

Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance

EPC269-19 / Version 1.14/ Date issued: 8 July 2021

Table of Contents

Executive Summary	15
1 Document Information	18
1.1 Structure of the document	18
1.2 References	19
1.3 Definitions	28
1.4 Abbreviations	38
1.5 Maintenance Process	40
2 General	41
2.1 Introduction	41
2.2 Vision	41
2.3 Scope	42
2.4 Objectives	43
2.5 Audience	44
3 High-level principles	45
4 SCT Inst and SCT scheme overview	47
4.1 Introduction	47
4.2 SCT Inst scheme	47
4.3 SCT Scheme	51
5 Mobile initiated SEPA (Instant) Credit Transfers	54
5.1 Introduction	54
5.2 MSCT Transaction	54
5.2.1 Introduction	54
5.2.2 MSCT modes	54
5.2.2.1 MSCTs based on payee-presented data	55
5.2.2.2 MSCTs based on payer-presented data	55
5.3 MSCT Provisioning and life cycle management	55
5.4 Relevant stakeholders in the MSCT ecosystems	56
6 MSCT service management	59
6.1 Introduction	59
6.2 MSCT application life-cycle	59



7 MSCT use cases.....	62
7.1 Introduction	62
7.2 Overview MSCT use cases.....	63
7.2.1 Introduction.....	63
7.2.2 Characteristics MSCT use cases.....	65
7.3 MSCT use cases	75
7.3.1 MSCT use case P2P-1: Mobile device – Payment with a proxy – SCA using an MSCT application involving a mobile code.....	75
7.3.2 MSCT use case P2P-2: Mobile device – Payment request with a proxy via messaging application – SCA using MSCT application involving a fingerprint.....	79
7.3.3 MSCT use case C2B-1: Mobile device - Payment of invoice with merchant-presented QR-code – SCA involving a mobile code	84
7.3.4 MSCT use case C2B-2: Mobile device – Payment at POI with merchant-presented QR-code – SCA using a dedicated authentication application (decoupled app-to-app) involving a fingerprint	88
7.3.5 MSCT use case C2B-3: Mobile device – m-commerce – mobile browser – PISP with embedded SCA involving a dynamic authenticator	93
7.3.6 MSCT use case C2B-4: Mobile device – transport ticketing – in-app payment - SCA involving fingerprint	98
7.3.7 MSCT use case C2B-5: Mobile device - Payment at a physical POI with consumer-presented QR-code - SCA using an MSCT application involving a mobile code	102
7.3.8 MSCT use case C2B-6: Mobile device - Offline use case – Payment at a physical POI using NFC and EMV-based SCA involving a fingerprint.....	107
7.3.9 MSCT use case C2B-7: Mobile device – Offline use case - Payment at a physical POI with consumer-presented QR-code involving a PISP – SCA via BLE using an MSCT app involving a fingerprint	112
7.3.10 MSCT use case C2B-8: Mobile device - Payment at a physical POI with consumer-presented QR-code - Unknown final amount with final amount being lower than pre-agreed amount – SCA of consumer using MSCT application involving a fingerprint	120
7.3.11 MSCT use case C2B-9: Mobile device – Payment at POI with merchant-presented QR-code – SCA via MSCT Inst application involving a mobile code.....	128
7.3.12 MSCT use case B2B-1: Mobile device - Payment request - SCA using MSCT application involving a fingerprint	133
7.4 Applicability of MSCTs.....	138
8 MSCT transaction aspects	139
8.1 Introduction	139
8.2 Payer authentication.....	142
8.2.1 Consumer Device User Verification Method	143
8.2.2 Authentication.....	143
8.3 Strong Customer Authentication (SCA)	145
8.4 Transaction authentication and dynamic linking.....	145
8.5 Transaction risk analysis	146
8.6 MSCT risk management	147
8.6.1 CDUVM Try Limit and Counter	148
8.6.2 Transaction Amount Limit.....	148



8.6.3 No-SCA Limit.....	148
8.6.4 Consecutive No-SCA Limit and Counter	149
8.6.5 Cumulative No-SCA Limit and Accumulator.....	149
8.7 Acknowledgements / Notifications	150
8.8 Transaction logging in the MSCT application	150
9 Generic security guidelines for the PSU-to-PSP space	151
9.1 Introduction	151
9.2 Threats	151
9.3 Generic security guidelines.....	153
9.4 Overview	155
10 Security considerations for the payer-to-payee space.....	158
10.1 Proximity technologies	158
10.1.1 QR-code.....	158
10.1.2 NFC	160
10.1.3 Bluetooth and Bluetooth Low Energy	161
10.2 Web-based payments	162
10.3 Merchant applications	162
10.4 Additional security measures	163
10.4.1 MSCT Tokenisation.....	163
10.4.2 Merchant Tokenisation	163
10.4.3 Securing the link payee name / IBAN_payee	163
11 Security of mobile devices.....	165
11.1 Introduction	165
11.2 Secure Element	165
11.3 Host Card Emulation	166
11.4 Trusted Execution Environment	166
11.5 Smart Secure Platform	167
11.6 Security guidelines for mobile devices	170
12 Security guidelines for MSCT applications	172
12.1 Software-based mobile applications	172
12.2 SE-based mobile applications	176
13 Security guidelines for CDUVMS	177
14 Security guidelines for PSU on-boarding.....	179
14.1 Introduction	179
14.2 Security guidelines	179
15 MSCT supporting services	182
15.1 Introduction	182
15.2 PISP payer authentication models.....	182
15.2.1 Redirection Model.....	182
15.2.2 Decoupled Model.....	182
15.2.3 Embedded Model.....	182



15.2.4 Delegated Model	183
15.3 SEPA Proxy Lookup Service	183
15.4 Request-to-Pay service	186
16 Overview MSCT interoperability aspects	190
16.1 Introduction	190
16.1.1 Current model for MSCTs based on payee-presented data	190
16.1.2 Current model for MSCTs based on payer-presented data	191
16.2 MSCT interoperability analysis	192
16.2.1 Person-to-Person (P2P) MSCTs	193
16.2.2 Customer-to-Business (C2B) MSCTs	193
16.2.3 Business-to-Business (B2B) MSCTs	193
16.3 MSCT interoperability layers	194
16.3.1 Introduction	194
16.3.2 PSU layer	195
16.3.3 MSCT service layer	195
16.4 MSCT interoperability model based on a HUB	195
17 Technical interoperability of MSCTs based on payee-presented data	197
17.1 Introduction	197
17.2 Exchange of MSCT transaction data	197
17.3 Acknowledgement/notification messages	198
17.3.1 Acknowledgement of receipt of MSCT instruction based on SCT to the payer	199
17.3.2 Notifications of successful MSCT transactions	199
17.3.2.1 MSCTs based on SCT Inst	199
17.3.2.2 MSCTs based on SCT	200
17.3.3 Notifications of unsuccessful transactions and rejects for MSCTs	202
17.3.3.1 MSCTs based on SCT Inst	202
17.3.3.2 MSCTs based on SCT	203
17.4 Request for recall by the payer	206
17.4.1 MSCTs based on SCT Inst	206
17.4.2 MSCTs based on SCT	206
17.5 Illustrative interoperability process flows for MSCTs based on payee-presented data	207
17.5.1 Introduction	207
17.5.2 Successful MSCT - P2P based on SCT Inst with proxy for payee	209
17.5.3 Successful MSCT - P2P based on SCT Inst with known payee data	215
17.5.4 Successful MSCT - C2B based on SCT Inst with merchant-presented QR-code containing a token	219
17.5.5 Successful MSCT - C2B based on SCT Inst with merchant-presented QR-code containing all transaction data in clear	225
17.5.6 Reject by the payer MSCT service provider – C2B based on SCT Inst with merchant-presented QR-code containing a token	230
17.5.7 Reject by the payer ASPSP – P2P based on SCT with payee-presented QR-code containing a proxy	234
17.5.8 Unsuccessful transaction – C2B based on SCT with merchant-presented QR-code containing a token	239



17.6	Minimum data set for MSCTs based on payee-presented data	244
17.7	Payee-presented QR-code for MSCTs.....	245
18	Technical interoperability of MSCTs based on payer-presented data	248
18.1	Introduction	248
18.2	Exchange of MSCT data.....	248
18.2.1	Exchange of payer-presented data	248
18.2.2	Exchange of transaction data.....	248
18.3	Acknowledgement/notification messages	250
18.3.1	Acknowledgement of receipt of payment request message for MSCTs based on SCT to the payee.....	250
18.3.2	Notifications of successful MSCT transactions	251
18.3.2.1	MSCTs based on SCT Inst	251
18.3.2.2	MSCTs based on SCT	252
18.3.3	Notifications of unsuccessful transactions and rejects for MSCTs	253
18.3.3.1	MSCTs based on SCT Inst	253
18.3.3.2	MSCTs based on SCT	256
18.4	Request for recall by the payer.....	259
18.4.1	MSCTs based on SCT Inst	259
18.4.2	MSCTs based on SCT	260
18.5	Illustrative interoperability process flows for MSCTs based on payer-presented data	261
18.5.1	Introduction	261
18.5.2	Successful MSCT – C2B based on SCT Inst with consumer-presented QR-code containing a token.....	263
18.5.3	Reject by payer ASPSP service provider – C2B based on SCT Inst with consumer-presented QR-code containing a token	268
18.5.4	Unsuccessful MSCT – C2B based on SCT Inst with consumer-presented QR-code containing consumer identification in clear	273
18.5.5	Reject by payer MSCT service provider – C2B based on SCT with consumer-presented QR-code containing consumer identification in clear	278
18.6	Minimum data set for MSCTs based on payer-presented data	281
18.7	Payer-presented QR-code for MSCTs	282
19	MSCT interoperability messages	284
19.1	Introduction	284
19.2	Overview MSCT interoperability messages	284
19.2.1	MSCTs based on payee-presented data.....	284
19.2.2	MSCTs based on payer-presented data	285
19.3	Entities involved in MSCT interoperability messages.....	286
20	New MSCT interoperability models	288
20.1	Introduction	288
20.2	Models involving a PISP	288
20.2.1	MSCTs based on merchant-presented data.....	288
20.2.2	MSCTs based on consumer-presented data	291
20.3	Models involving a Collecting PSP (CPSP)	295



21 MSCT standards, specifications and white papers.....	297
22 Challenges and opportunities.....	300
22.1 Challenges.....	300
22.2 Opportunities.....	303
23 Conclusions	305
Annex 1: Overview regulatory documents	308
Annex 2: Additional MSCT use cases	312
A2.1 MSCT use case P2P-3: Mobile device – Mobile banking via browser – Static customer authentication using on-line passcode.....	312
A2.2 MSCT use case P2P-4: Mobile device - Payment with a payee-presented QR-code - SCA using MSCT app involving facial recognition	316
A2.3 MSCT use case C2B-10: Mobile device – m-commerce – merchant application - PISP with redirection to consumer’s ASPSP - SCA involving a dynamic authenticator	320
A2.4 MSCT use case C2B-11: Mobile device - Payment at a physical POI with consumer-presented QR-code - SCA using a dedicated authentication application involving a fingerprint	324
A2.5 MSCT use case C2B-12: Mobile device – Payment at a physical POI with consumer-presented QR-code involving a PISP – SCA using a dedicated authentication application involving a fingerprint.....	329
A2.6 MSCT use case C2B-13: Smartwatch – Payment at a physical POI with consumer-presented QR-code involving a PISP – SCA using an embedded authentication via the POI involving an OTP and PIN	334
A2.7 MSCT use case C2B-14: Mobile device - Off-line use case – Payment at a physical POI with consumer-presented QR-code – SCA involving facial recognition	339
A2.8 MSCT use case C2B-15: Mobile device - Payment at a physical POI with consumer-presented QR-code - Unknown final amount with final amount is higher than pre-agreed amount – SCA using a dedicated authentication application involving a mobile code	344
Annex 3: Overview on errors with MSCTs	352
A3.1 MSCTs based on payee-presented data	352
A3.2 MSCTs based on payer-presented data.....	353
Annex 4: Minimum data sets for MSCT interoperability messages.....	356
A4.1 Introduction.....	356
A4.2 Transaction Information messages	356
A4.2.1 Transaction information request.....	356
A4.2.2 Transaction information response.....	357
A4.3 Lock Transaction messages	358
A4.3.1 Lock transaction request.....	358
A4.3.2 Lock transaction response	359
A4.4 Payment Request.....	359
A4.4.1 Payment request messages	361
A4.4.2 Confirmations of receipt of payment request	364
A4.5 Notification of Reject messages	365



A4.6 Notification of Successful/Unsuccessful Transaction messages	369
A4.7 Inquiry messages	375
A4.7.1 Inquiry request message.....	375
A4.7.2 Inquiry response message	376
Annex 5: The multi-stakeholder group	377

List of Tables

Table 1: Bibliography	28
Table 2: Terminology	37
Table 3: Abbreviation.....	40
Table 4: Overview mobile payments	62
Table 5: Overview illustrative MSCT use cases.....	64
Table 6: Main characteristics of MSCT use cases	74
Table 7: Analysis MSCT use case P2P-1	78
Table 8: Analysis MSCT use case P2P-2	83
Table 9: Analysis MSCT use case C2B-1	87
Table 10: Analysis MSCT use case C2B-2	92
Table 11: Analysis MSCT use case C2B-3	97
Table 12: Analysis MSCT use case C2B-4	101
Table 13: Analysis MSCT Use case C2B-5.....	106
Table 14: Analysis MSCT Use case C2B-6.....	111
Table 15: Analysis MSCT Use case C2B-7.....	119
Table 16: Analysis MSCT Use case C2B-8.....	127
Table 17: Analysis MSCT use case C2B-9	132
Table 18: Analysis MSCT use case B2B-1	138
Table 19: Applicability of MSCTs.....	138
Table 20: Risk parameters for MSCTs	147
Table 21: MSCT threats list in the PSU-to-PSP/MSCT service provider space.....	153
Table 22: Overview security guidelines for MSCTs in the PSU-to-PSP/MSCT service provider space	155
Table 23: Mapping security guidelines onto threats for MSCTs.....	157
Table 24: Security guidelines for mobile devices	171
Table 25: Overview potential attacks to mobile apps on a mobile device.....	175
Table 26: Required HUB functionalities for exchange of transaction data for MSCTs based on payee-presented data.....	198
Table 27: Overview of messages for notification to payee of successful MSCTs based on SCT Inst with payee-presented data.....	199
Table 28: Overview of messages for notification to payer of successful MSCTs based on SCT Inst with payee-presented data.....	200
Table 29: Overview of messages for notification to payee of successful MSCTs based on SCT with payee-presented data.....	200



Table 30: Overview of messages for notification to payer of successful MSCTs based on SCT with payee-presented data.....	201
Table 31: Required HUB functionalities for notification of successful transactions for MSCTs based on payee-presented data	201
Table 32: Overview of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data.....	202
Table 33: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data	203
Table 34: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data	203
Table 35: Overview of rejects and unsuccessful MSCTs based on SCT with payee-presented data	204
Table 36: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT with payee-presented data	204
Table 37: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data	205
Table 38: Required HUB functionalities for unsuccessful transactions and rejects for MSCTs based on payee-presented data	205
Table 39: Illustrative process flows for interoperability of MSCT transactions based on payee-presented data with mapping onto HUB functionalities.....	209
Table 40: Minimum data sets for MSCTs based on payee-presented data	244
Table 41: Coding of payee-presented QR-code for MSCTs	246
Table 42: Payload data for MSCTs based on payee-presented data.....	247
Table 43: Required HUB functionalities for exchange of payer identification and transaction data for MSCTs based on payer-presented data	250
Table 44: Overview of messages for acknowledgement of receipt of payment request to payee for MSCTs based on SCT with payer-presented data.....	251
Table 45: Overview of messages for notification to payee of successful MSCTs based on SCT Inst with payer-presented data	251
Table 46: Overview of messages for notification to payer of successful MSCTs based on SCT Inst with payer-presented data	252
Table 47: Overview of messages for notification to payee of successful MSCTs based on SCT with payer-presented data	252
Table 48: Overview of messages for notification to payer of successful MSCTs based on SCT with payer-presented data	253
Table 49: Required HUB functionalities for notification of successful transactions for MSCTs based on payer-presented data.....	253
Table 50: Overview of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data.....	254
Table 51: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data.....	255
Table 52: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data.....	256
Table 53: Overview of rejects and unsuccessful MSCTs based on SCT with payer-presented data	256



Table 54: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT with payer-presented data.....	257
Table 55: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data.....	258
Table 56: Required HUB functionalities for unsuccessful transactions and rejects for MSCTs based on payee-presented data	259
Table 57: Illustrative process flows for interoperability of MSCT transactions based on payer-presented data with mapping onto HUB functionalities.....	262
Table 58: Minimum data sets for MSCTs based on payer-presented data	282
Table 59: Coding of QR-code with payer-presented data	283
Table 60: Overview messages for MSCTs based on payee-presented data	285
Table 61: Overview messages for MSCTs based on payer-presented data.....	286
Table 62: Overview MSCT interoperability messages and entities involved.....	287
Table 63: Overview regulatory documents	311
Table 64: Analysis MSCT use case P2P-3	315
Table 65: Analysis MSCT use case P2P-4	319
Table 66: Analysis MSCT use case C2B-10	323
Table 67: Analysis MSCT Use case C2B-11.....	328
Table 68: Analysis MSCT Use case C2B-12.....	333
Table 69: Analysis MSCT Use case C2B-13.....	338
Table 70: Analysis MSCT Use case C2B-14.....	343
Table 71: Analysis MSCT Use case C2B-15.....	350
Table 72: Overview on errors for MSCTs based on payee-presented data.....	353
Table 73: Overview on errors for MSCTs based on payer-presented data	355
Table 74: Overview transaction information messages	356
Table 75: Dataset for transaction information request.....	357
Table 76: Dataset for transaction information response	358
Table 77: Overview lock transaction messages	358
Table 78: Dataset for lock transaction request message	359
Table 79: Dataset for lock transaction response message	359
Table 80: Overview of payment request messages.....	360
Table 81: Dataset for payment request message by the payee to the payee MSCT service provider.....	362
Table 82: Dataset for payment request message by the payee MSCT service provider to the payer MSCT service provider	363
Table 83: Dataset for confirmation of receipt of payment request by the payer MSCT service provider to the payee MSCT service provider	364
Table 84: Dataset for confirmation of receipt of payment request by the MSCT service provider to the payee	364
Table 85: Overview of notification of reject messages	365
Table 86: Dataset for notification of reject message by the payer ASPSP to the payer MSCT service provider	366
Table 87: Dataset for notification of reject message by the payer MSCT service provider to the payee MSCT service provider	367
Table 88: Dataset for notification of reject message by the payer MSCT service provider to the payer	368



Table 89: Dataset for notification of reject message by the payee MSCT service provider to the payee	369
Table 90: Overview of notification of successful / unsuccessful transaction messages	370
Table 91: Dataset for notification of successful / unsuccessful transaction message by the payer ASPSP to the payer MSCT service provider	371
Table 92: Dataset for notification of unsuccessful transaction message by the payer MSCT service provider to the payee MSCT service provider	372
Table 93: Dataset for notification of successful / unsuccessful transaction message by the payer MSCT service provider to the payer	373
Table 94: Dataset for notification of unsuccessful transaction message by the payee MSCT service provider to the payee	374
Table 95: Overview inquiry messages for MSCTs	375
Table 96: Dataset for inquiry request message between MSCT service providers	375
Table 97: Dataset for inquiry response message between MSCT service providers	376
Table 98: The multi-stakeholder group MSCT	378



List of Figures

Figure 1: Overview SCT Inst transaction process flow.....48

Figure 2: Overview SCT transaction process flow.....51

Figure 3: Actors in MSCT use case P2P-175

Figure 4: MSCT use case P2P-176

Figure 5: Actors in MSCT use case P2P-279

Figure 6: MSCT use case P2P-280

Figure 7: Actors in MSCT use case C2B-1.....84

Figure 8: MSCT use case C2B-185

Figure 9: Actors in MSCT use case C2B-2.....88

Figure 10: MSCT use case C2B-289

Figure 11: Actors in MSCT use case C2B-3.....93

Figure 12: MSCT use case C2B-394

Figure 13: Actors in MSCT use case C2B-4.....98

Figure 14: MSCT use case C2B-499

Figure 15: Actors in MSCT Use case C2B-5102

Figure 16: MSCT Use case C2B-5.....103

Figure 17: Actors in MSCT Use case C2B-6107

Figure 18: MSCT Use case C2B-6.....108

Figure 19: Actors in MSCT Use case C2B-7112

Figure 20: MSCT Use case C2B-7.....114

Figure 21: MSCT Use case C2B-7 – overview cryptography115

Figure 22: Actors in MSCT Use case C2B-8120

Figure 23: MSCT Use case C2B-8.....123

Figure 24: Actors in MSCT use case C2B-9.....128

Figure 25: MSCT use case C2B-9129

Figure 26: Actors in MSCT use case B2B-1.....133

Figure 27: MSCT use case B2B-1135

Figure 28: Decomposition of an MSCT based on SCT Inst into building blocks.....139

Figure 29: Decomposition of an MSCT based on SCT into building blocks141

Figure 30: Example of a TEE model.....167

Figure 31: Logical structure of an iSSP169

Figure 32: OWASP Security Verification Levels as per MASVS’173

Figure 33: The SEPA Proxy Lookup Service184

Figure 34: MSCT using the SEPA Proxy Lookup Service185

Figure 35: RTP process components and context.....187

Figure 36: RTP actors and information flow in 4-corner eco-system188

Figure 37: Model for MSCTs based on payee-presented data190

Figure 38: How to interconnect different MSCT services based on payee-presented data?191

Figure 39: Model for MSCTs based on payer-presented data.....191

Figure 40: How to interconnect different MSCT services based on payer-presented data? 192

Figure 41: MSCT interoperability layers194

Figure 42: Generic 4-corner MSCT interoperability model196

Figure 43: Actors for P2P – with proxy210

Figure 44: Process flow – P2P – with proxy212



Figure 45: Actors for P2P – without proxy215

Figure 46: Process flow – P2P – without proxy217

Figure 47: Actors for C2B - with token.....219

Figure 48: Process flow – C2B – merchant-presented QR-code with token221

Figure 49: Actors for C2B – without token225

Figure 50: Process flow – C2B – merchant-presented QR-code with full transaction data ..227

Figure 51: Actors for reject by consumer MSCT service provider for C2B payment context 230

Figure 52: Process flow – C2B – Reject by consumer MSCT service provider for MSCT based on merchant-presented QR-code with token.....231

Figure 53: Actors for reject by payer ASPSP for P2P payment context234

Figure 54: Process flow – P2P – Reject by payer ASPSP for MSCT based on payee-presented QR-code with proxy236

Figure 55: Actors for unsuccessful transaction for C2B payment context239

Figure 56: Process flow – C2B – Unsuccessful transaction for MSCT based on merchant-presented QR-code with token.....241

Figure 57: Actors for C2B - with consumer token.....263

Figure 58: Process flow – C2B – consumer-presented QR-code with token265

Figure 59: Actors for reject by consumer ASPSP for C2B payment context268

Figure 60: Process flow – C2B – Reject by consumer ASPSP for MSCT based on consumer-presented QR-code with token.....270

Figure 61: Actors for unsuccessful transaction for C2B payment context273

Figure 62: Process flow – C2B – Unsuccessful transaction for MSCT based on consumer-presented QR-code without token275

Figure 63: Actors for reject by consumer MSCT service provider for C2B payment context 278

Figure 64: Process flow – C2B – Reject by consumer MSCT service provider for MSCT based on consumer-presented QR-code without token.....279

Figure 65: Model for MSCTs based on merchant-presented data whereby PISP is consumer MSCT service provider289

Figure 66: Model for MSCT based on merchant-presented data whereby PISP is merchant MSCT service provider290

Figure 67: Model for MSCTs based on consumer-presented data whereby PISP is consumer MSCT service provider291

Figure 68: Model for MSCT based on consumer-presented data whereby PISP is merchant MSCT service provider / e- and m-commerce293

Figure 69: Model for MSCT based on consumer-presented data whereby PISP is merchant MSCT service provider / in-store294

Figure 70: Model involving a CPSP295

Figure 71: Actors in MSCT use case P2P-3312

Figure 72: MSCT use case P2P-3313

Figure 73: Actors in MSCT use case P2P-4316

Figure 74: MSCT use case P2P-4317

Figure 75: Actors in MSCT use case C2B-10.....320

Figure 76: MSCT use case C2B-10.....321

Figure 77: Actors in MSCT Use case C2B-11324

Figure 78: MSCT Use case C2B-11325

Figure 79: Actors in MSCT Use case C2B-12329



Figure 80: MSCT Use case C2B-12	330
Figure 81: Actors in MSCT Use case C2B-13	334
Figure 82: MSCT Use case C2B-13	335
Figure 83: Actors in MSCT Use case C2B-14	339
Figure 84: MSCT Use case C2B-14	340
Figure 85: Actors in MSCT Use case C2B-15	344
Figure 86: MSCT Use case C2B-15	346



Executive Summary

Mobile devices have achieved full market penetration and rich service levels in most, if not all, EU Member States, making the mobile channel ideal for leveraging and promoting the use of SEPA payment instruments.

This document provides interoperability guidance for Mobile Initiated SEPA (Instant) Credit Transfers (MSCTs). It aims to reflect the current state of the play and market situation at the time of writing while being brand and implementation model agnostic. On the other hand, it needs to be acknowledged that the MSCT ecosystem is rapidly evolving with many new entrants in the market. However, most of these are “closed-loop” solutions which are not interoperable. Clearly, market adoption will determine the success of each of these new entrants.

Cross-industry cooperation on specifications, guidelines and best practices has been identified as a critical success factor in this area. Therefore, the EPC has facilitated in 2018 the setting-up of a multi-stakeholder group covering the various sectors involved in the MSCT ecosystem to address the interoperability issues. The group developed the MSCT Interoperability Guidance (MSCT IG) that was published in 2019 (EPC269-19v1.0), following a public consultation. Over the past years, the multi-stakeholder group has analysed in further detail various MSCT interoperability issues that resulted in the publication of some additional documents (see EPC312-19 [27], EPC096-20 [20] and EPC031-21 [30]). The present document is a new version of the MSCT IG, which includes updates to various chapters, integrates the three documents mentioned above and also includes some new work by the MSG MSCT.

The document aims through the description of MSCT use cases to provide an insight into the main issues related to the initiation of (instant) SEPA credit transfers for different payment contexts such as person-to-person, consumer-to-business (retail payments including both in-store and m-commerce payments) and business-to-business payments. Next to the MSCT transaction aspects such as payer authentication, transaction authentication, risk management and payer/payee acknowledgements and notification messages, it focuses on the technology and security used in the customer-to-ASPSP space, since the SCT Inst and SCT transactions as such have already been specified in the respective scheme rulebooks (see [17] and [21]). It furthermore specifies various security guidelines for MSCTs (e.g. MSCT app, CDUVM, etc.). The document analyses in detail the technical interoperability of MSCTs based on payee- or payer-presented data and specifies the technical interoperability requirements between MSCT service providers, for successful, unsuccessful transactions and rejects, which are also depicted in some illustrative process flows. It defines the minimum data to be exchanged between the payer and payee to enable the initiation of an MSCT and specifies for this a payee- and payer-presented QR-code for MSCTs. It further specifies the minimum data sets for all interoperability messages between the respective MSCT service providers of the payer and the payee. New interoperability models involving a PISP (Payment Initiation Service Provider) or a CPSP (a collecting PSP on behalf of the merchant) have also been addressed. Finally, the document identifies the main interoperability challenges but also opportunities for MSCTs.



Note that subjects such as business cases and revenue models for the MSCT value chain are in the competitive space and therefore are not addressed in this document.

While producing this document, the multi-stakeholder group has noticed a number of “major challenges and barriers” that will need to be properly addressed to achieve full interoperability of MSCT transactions (see Chapter 22).

These include:

- The availability of a technical infrastructure to interconnect the different MSCT service providers notably for the support of token/proxy-based MSCTs and MSCT confirmation and notification messages to PSUs (payers and payees);
- The development of an implementation specification for the MSCT QR-codes specified in this document and the subsequent adoption by the market;
- Next to the technical aspects, also the operating rules, liabilities, adherence to these requirements and governance should be addressed. This could be achieved through the set-up of a dedicated “MSCT interoperability framework or MSCT scheme” to which the MSCT service providers (existing and new one) should participate to ensure interoperability of MSCT services;
- A recognition label for MSCTs. Some of the MSG MSCT members are of the opinion that the development of such a recognition label that shows to PSUs at the POI that an MSCT can be used for the payment of goods or services with a merchant, should be further analysed.
- Specifications for consumer selection of preferred payment instrument at the point of interaction.

Regarding the SEPA Proxy Lookup (SPL) scheme (see section 15.3) that has been developed for the support of MSCTs in P2P payment contexts, it should be noted that today it covers a mobile phone number for the payee but only mandates to return the payee’s IBAN for the proxy. However the payee’s name might not be known by the payer or by their MSCT app on their mobile device which might pose a problem in view of the dynamic linking for MSCTs as specified by the PSD2 and RTS (see section 8.4). A solution for this problem will need to be further investigated.

Clearly “Request-to-Pay” services could enhance the customer experience for MSCTs for all payment contexts. The work on the SRTP scheme [28] complements the current document and will further contribute to the PSU adoption of MSCTs.

Also the work done in the ERPB WG on SEPA API access scheme [37] complements the current document for MSCTs involving a PISP.



Other challenges for MSCT services include:

- Complexity and security of the different mobile platforms;
- Access restriction to mobile device features from some manufacturers;
- The co-existence of multiple proximity technologies, possibly linked to different payment instruments at the POI (see Chapter 22);
- Uncertainties regarding European rules and regulations (e.g.; PSD2 [5], RTS [6] and GDPR [7]), also related to their interplay with respect to MSCTs¹ (see also Chapters 7, 8 and 20).

The multi-stakeholder group has organised focused work on the technical interoperability issues through various technical expert work-streams. Note that also work on instant payments at POI has been conducted under the ERPB (see [33] and [35]) that has leveraged the documents developed by the MSG MSCT. Furthermore, a joint task force between the MSG MSCT and the ECSG is currently defining the requirements for the consumer selection of preferred payment instrument at the POI based on [36] with the aim to develop a report by November 2021.

By developing this interoperability guidance, the multi-stakeholder group aimed to contribute to a competitive MSCT market, by providing the different stakeholders an insight into the different service, technical and security aspects involved. The document could serve as a reference basis for making certain implementation choices.

In light of major new trends, and the rapidly changing market, the multi-stakeholder group recommends for the present document to be regularly updated in order to reflect the state of play related to MSCTs and to keep it aligned with the various documents referenced. More in particular, the usage of other proximity technologies than QR-codes for MSCTs, such as NFC and BLE, could be further specified (see Chapter 10.1).

¹ See EBA Q&A 2020_5365-5367, 5476, 5477, 5570-5573 and 5587.



1 Document Information

1.1 Structure of the document

This document contains a number of chapters and annexes, as follows:

- Chapter 1 includes the document information.
- Chapter 2 provides the vision on Mobile Initiated SEPA (Instant) Credit Transfers (MSCTs), including SCT Inst, as well as the scope and the objectives of this document;
- Chapter 3 defines the high-level principles;
- Chapter 4 gives an overview of the SCT Inst and SCT schemes;
- Chapter 5 introduces MSCTs and the stakeholders involved in the MSCT ecosystem;
- Chapter 6 briefly discusses the MSCT application life-cycle;
- Chapter 7 introduces some examples of MSCT use cases;
- Chapter 8 discusses MSCT transaction aspects;
- Chapter 9 defines security guidelines for the customer-to-PSP space;
- Chapter 10 discusses security for the payer-to-payee space;
- Chapter 11 provides security guidelines for mobile devices;
- Chapter 12 defines security guidelines for MSCT applications;
- Chapter 13 defines security guidelines for CDUVMS;
- Chapter 14 provides guidelines for customer on-boarding;
- Chapter 15 highlights some supporting services for MSCTs;
- Chapter 16 includes a high level analysis of technical interoperability aspects;
- Chapter 17 discusses the technical interoperability of MSCTs based on payee-presented data;
- Chapter 18 discusses the technical interoperability of MSCTs based on payee-presented data;
- Chapter 19 provides an overview on the MSCT interoperability messages;
- Chapter 20 discusses new MSCT interoperability models;
- Chapter 21 provides an overview on standard and industry bodies contributing to the interoperability of MSCTs;
- Chapter 22 provides an overview of additional challenges and opportunities;
- Chapter 23 includes the conclusions;
- Annex 1 provides an overview of relevant regulatory documents;
- Annex 2 provides additional MSCT use cases;
- Annex 3 includes an overview on errors with MSCTs;
- Annex 4 specifies the minimum data sates for MSCT interoperability messages;
- Annex 5 gives an overview of the different organisations and companies involved in the multi-stakeholder group that developed this document.



1.2 References

This section lists the references mentioned in this document. Square brackets throughout this document are used to refer to documents in this list.

[1]	EBA/GL/2014/12_rev1: Final guidelines on the security of internet payments (https://www.eba.europa.eu/sites/default/documents/files/documents/10180/934179/f27bf266-580a-4ad0-aaec-59ce52286af0/EBA-GL-2014-12%20%28Guidelines%20on%20the%20security%20of%20internet%20payments%29_Rev1.pdf?retry=1)	EBA
[2]	EBA/GL/2019/04: EBA Guidelines on ICT and security risk management (https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf)	EBA
[3]	Guideline for user-friendly payment terminals (https://www.oogvereniging.nl/wp-content/uploads/2013/07/Guideline-for-user-friendly-payment-terminals.pdf)	Dutch National Forum on the Payment System
[4]	eIDAS: Regulation (EU) No 910/2014 of the European parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN)	EC
[5]	PSD2: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN)	EC
[6]	Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (also referred to as "RTS") (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN)	EC
[7]	General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to	EC



	the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN)	
[8]	European Commission Report on existing remote on-boarding solutions in the banking sector – December 2019 (https://sb-bg.com/app/uploads/2020/08/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf)	EC
[9]	ECB/EuroSystem Assessment guide for the security of internet payments (https://www.ecb.europa.eu/pub/pdf/other/assessmentguide_securityinternetpayments201402en.pdf)	ECB
[10]	ECSG 001-17: SEPA Cards Standardisation Volume (https://www.e-csg.eu/scs-volume)	ECSG
[11]	EMV [®] QR-code Specification for Payment Systems (EMV QRCPS) - Merchant - Presented Mode (https://www.emvco.com/)	EMVCO
[12]	EMV [®] Mobile Payment: Software-based Mobile Payment Security Requirements (https://www.emvco.com/)	EMVCo
[13]	EMV [®] Software-based Mobile Payment Security Evaluation Process (https://www.emvco.com/)	EMVCo
[14]	EMV [®] Mobile Payment Consumer Device Cardholder Verification Method – Solution Evaluation and Registration (https://www.emvco.com/)	EMVCo
[15]	EMV [®] Mobile Payment Consumer Device Cardholder Verification Method Security Requirements (https://www.emvco.com/)	EMVCo
[16]	EMV [®] Consumer Device Cardholder Verification Method—Best Practices (https://www.emvco.com/)	EMVCo
[17]	EPC125-05 2019: SEPA Credit Transfer Scheme Rulebook (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2020-04/EPC125-05%202019%20SCT%20Rulebook%20version%201.1.pdf)	EPC
[18]	EPC115-06: SEPA Credit Transfer Scheme Interbank Implementation Guidelines (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2018-11/EPC115-06%20SCT%20Interbank%20IG%202019%20V1.0.pdf)	EPC
[19]	EPC342-08: Guidelines on algorithms usage and key management	EPC



	https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2021-03/EPC342-08%20v10.0%20Guidelines%20on%20Cryptographic%20Algorithms%20Usage%20and%20Key%20Management_0.pdf	
[20]	EPC492-09: White paper Mobile Payments (https://www.europeanpaymentscouncil.eu/sites/default/files/KB/files/EPC492-09%20v5.0%20White%20Paper%20Mobile%20Payments%20-%20edition%202017.pdf)	EPC
[21]	EPC004-16: SEPA Instant Credit Transfer Scheme Rulebook (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2020-10/EPC004-16%202019%20SCT%20Instant%20Rulebook%20v1.2_0.pdf)	EPC
[22]	EPC122-16: SEPA Instant Credit Transfer Scheme Interbank Implementation Guidelines (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2018-11/EPC122-16%20SCT%20Inst%20Interbank%20IG%202019%20V1.0_1.pdf)	EPC
[23]	EPC144-17: Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines (MCP IIG) (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2018-06/EPC144-17%20v1.0%20Mobile%20Contactless%20SEPA%20Card%20Payments%20Interoperability%20Implementation%20Guidelines.pdf)	EPC
[24]	EPC109-19: White Paper Non-NFC based Mobile SEPA Card Proximity Payments (MCPPs) (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2019-06/EPC109-19v1.0%20White%20paper%20MCPPs_final.pdf)	EPC
[25]	EPC244-20: 2020 Payment Threats and Fraud Trends Report (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2020-12/EPC244-20%20v1.0%202020%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf)	EPC
[26]	EPC250-18: The SEPA Proxy Lookup (SPL) Scheme Rulebook (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2020-03/EPC250-18%20v2.0%20SEPA%20Proxy%20Lookup%20Scheme%20Rulebook.pdf)	EPC
[27]	EPC312-19: Technical Interoperability of MSCTs based on payee-presented data (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2020-05/EPC312-	EPC



	19v1.0%20Technical%20interoperability%20of%20MSCTs%20based%20on%20payee-presented%20data_0.pdf)	
[28]	EPC014-20: SEPA RTP Scheme Rulebook https://www.europeanpaymentscouncil.eu/document-library/rulebooks/sepa-request-pay-srtp-scheme-rulebook	EPC
[29]	EPC096-20: Technical Interoperability of MSCTs based on payer-presented data (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2020-12/EPC096-20v1.0%20Technical%20interoperability%20of%20MSCTs%20based%20on%20payer-presented%20data%20%28003%29.pdf)	EPC
[30]	EPC031-21: New MSCT use cases and interoperability models https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/public-consultation-document-new-msct-use-cases-and	EPC
[31]	ERPB/2015/016: Final report on Mobile and card-based contactless proximity payments (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/4th-ERPB-meeting/2015-11-26_4th-ERPB_item_6_ERPB_CTLP_working_group_final_report.pdf?726f67769d37722de341702fe5f2387a)	ERPB
[32]	ERPB/2018/014: Report from the EPC EIPP multi-stakeholder group (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/10th-ERPB-meeting/Report from the EIPP Multi - Stakeholder Group.pdf?6fb4e75198566ea357712e02fad3a58e)	ERPB
[33]	ERPB/2019/012: Final report of the ERPB Working Group on Instant Payments at POI (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/12th-ERPB-meeting/Report from the ERPB WG on instant at POI.pdf?efe8385c4196f8094d5b6625f7ffdc79)	ERPB
[34]	ERPB/2019/013: Request-to-Pay - Specifications for a standardisation framework (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/12th-ERPB-meeting/Report from the RTP MSG.pdf?efe8385c4196f8094d5b6625f7ffdc79)	ERPB
[35]	ERPB/2020/026: Framework for interoperability of instant payments at the point of interaction (IPs at the POI) (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/14th-ERPB-	ERPB



	meeting/ERPB working group on instant at the POI - Framework for interoperability of instant payments at the POI.pdf?db00f43b17d4aeeb4a83ae82187d53c8)	
[36]	ERPB/2020/027: Specifications to enable consumer selection of preferred payment instrument(https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/14th-ERPB-meeting/ERPB working group on instant at the POI - Specifications for payment instrument selection.pdf?db00f43b17d4aeeb4a83ae82187d53c8)	ERPB
[37]	ERPB/2021/xx: Final report on SEPA API access scheme Awaiting publication	ERPB
[38]	ERPB/2021/xx: Final report of ERPB WG on transparency: to be published Awaiting publication	ERPB
[39]	ETSI TS 103 465: Smart Cards; Smart Secure Platform (SSP); Requirements Specification (https://www.etsi.org/deliver/etsi_ts/103400_103499/103465/15.00.00_60/ts_103465v150000p.pdf)	ETSI
[40]	ETSI TS 103 666-1, Smart Secure Platform (SSP); Part 1: General characteristics (https://www.etsi.org/deliver/etsi_ts/103600_103699/10366601/15.01.00_60/ts_10366601v150100p.pdf)	ETSI
[41]	ETSI TS 103 666-2, Smart Secure Platform (SSP); Part 2: Integrated SSP (iSSP) characteristics (https://www.etsi.org/deliver/etsi_ts/103600_103699/10366602/15.02.00_60/ts_10366602v150200p.pdf)	ETSI
[42]	ETSI TS 103 666-3, Smart Secure Platform (SSP); Part 3: Embedded SSP (eSSP) Type 1 characteristics (https://www.etsi.org/deliver/etsi_ts/103600_103699/10366603/16.00.00_60/ts_10366603v160000p.pdf)	ETSI
[43]	ETSI TS 103 666-4, Smart Secure Platform (SSP); Part 4: Embedded SSP (eSSP) Type 2 characteristics <i>Publication scheduled for end of 2021</i>	ETSI
[44]	ETSI TS 103 713, Smart Secure Platform (SSP); SPI interface (https://www.etsi.org/deliver/etsi_ts/103700_103799/103713/15.03.00_60/ts_103713v150300p.pdf)	ETSI
[45]	ETSI TS 103 813, Smart Secure Platform (SSP); Test Specification, SPI interface (https://www.etsi.org/deliver/etsi_ts/103800_103899/103813/15.00.00_60/ts_103813v150000p.pdf)	ETSI
[46]	ETSI TS 103 999-1, Smart Secure Platform (SSP); Part 1: General characteristics test specification	ETSI



	<i>Publication expected July 2021</i>	
[47]	ETSI TS 103 999-2, Smart Secure Platform (SSP); Part 2: Integrated SSP (iSSP) characteristics test specification <i>Publication scheduled for September 2021</i>	ETSI
[48]	Towards a better payment experience	Eye Association Netherlands
[49]	FIDO & PSD2 – Meeting the needs for Strong Customer Authentication (2017) (https://media.fidoalliance.org/wp-content/uploads/FIDO-PSD2-white-paper-FINAL.pdf)	FIDO Alliance
[50]	FIDO Authentication and the General Data Protection Regulation (GDPR) (May 2018) (https://fidoalliance.org/wp-content/uploads/FIDO Authentication and GDPR White Paper May2018-1.pdf)	FIDO Alliance
[51]	FIDO for PSD2 - Providing for a satisfactory customer journey (Sept. 2018) (https://media.fidoalliance.org/wp-content/uploads/FIDO-PSD2 Customer Journey White Paper.pdf)	FIDO Alliance
[52]	FIDO Privacy Principles (https://fidoalliance.org/fido-authentication/privacy-principles/)	FIDO Alliance
[53]	GPD_SPE_009: TEE System Architecture (https://globalplatform.org/wp-content/uploads/2017/01/GPD_TEE_SystemArch_v1.2_Public_Release.pdf)	GlobalPlatform
[54]	GPD_SPE_042: TEE TUI Extension: Biometrics API (https://globalplatform.org/wp-content/uploads/2018/05/GPD_TEE_TUI_Extn_Biometrics_API_v1.0_PublicRelease_2018_04_03.pdf)	GlobalPlatform
[55]	GPS_GUI_006: End-to-End Simplified Service Management Framework for payment (https://globalplatform.org/specs-library/end-to-end-simplified-service-management-framework-v1-1-2/)	GlobalPlatform
[56]	GPC_WPR_202: White paper- GlobalPlatform Technology – Virtual Primary Platform (VPP) https://globalplatform.org/wp-content/uploads/2020/10/GPC_VPP_WhitePaper_v1.0_Release.pdf	GlobalPlatform
[57]	GPC_FST_140: GlobalPlatform Technology - VPP - Network Protocol v1.0.1 https://globalplatform.org/specs-library/globalplatform-technology-virtual-primary-platform-v1-0-1/	GlobalPlatform
[58]	GPC_FST_142: GlobalPlatform Technology – VPP - Concepts and interfaces v1.0.1	GlobalPlatform



	https://globalplatform.org/specs-library/globalplatform-technology-virtual-primary-platform-v1-0-1/	
[59]	GSMA TS.26: NFC Handset Requirements (https://www.gsma.com/newsroom/wp-content/uploads//TS.26-v15.0.pdf)	GSMA
[60]	GSMA TS.27: NFC Handset Test Book (https://www.gsma.com/newsroom/wp-content/uploads//TS27-v14.1.pdf)	GSMA
[61]	GSMA SGP.21 RSP Architecture (https://www.gsma.com/newsroom/wp-content/uploads//SGP.21_v2.2.pdf)	GSMA
[62]	GSMA SGP.22 RSP Technical specification (https://www.gsma.com/esim/wp-content/uploads/2020/06/SGP.22-v2.2.2.pdf)	GSMA
[63]	NFC Functions and Security Certification overview (https://www.gsma.com/newsroom/wp-content/uploads//NFC-Functions-and-Security-Certification-Overview_v1.0.pdf)	GSMA
[64]	HCE and Tokenisation for Payment Services - Discussion paper	GSMA / Consult Hyperion
[65]	The Mobile Economy 2020 (https://www.gsma.com/mobileeconomy/)	GSMA
[66]	RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 (https://datatracker.ietf.org/doc/html/rfc8446)	IETF
[67]	ISO 9362: Business Identifier Code (BIC) (https://www.iso9362.org/isobic/overview.html)	ISO
[68]	ISO 13616: Financial services - International Bank account number (IBAN) -- Part 1: Structure of the IBAN (https://www.iso.org/standard/81090.html)	ISO
[69]	ISO 20022: Financial Services – Universal Financial Industry Message Scheme (https://www.iso20022.org/)	ISO
[70]	ISO 12812: Core banking - Mobile financial services - Parts 1-5 (https://www.iso.org)	ISO
[71]	ISO/IEC 14443: Identification cards - Contactless integrated circuit(s) cards - Proximity cards – Parts 1-4 (https://www.iso.org)	ISO
[72]	ISO/IEC 18004: Information technology -- Automatic identification and data capture techniques -- QR-code bar code symbology specification (https://www.iso.org/standard/43655.html)	ISO



[73]	ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems -- Near Field Communication - Interface and Protocol (NFCIP-1) (https://www.iso.org/standard/38578.html)	ISO
[74]	World Telecommunication/ICT Indicators Database 2018 (https://www.itu.int/pub/D-IND-WTID.OL-2018)	ITU
[75]	White Paper - Alternatives for Banks to offer Secure Mobile Payments (https://nfc-forum.org/resources/mobey-forum-nfc-white-paper-alternatives-for-banks-to-offer-secure-mobile-payments/)	Mobey Forum
[76]	Mobile wallet – Parts 1-5 (https://mobeyforum.org)	Mobey Forum
[77]	The Host Card Emulation in Payments - Options for Financial Institutions (https://mobeyforum.org/the-host-card-emulation-in-payments-options-for-financial-institutions-3/)	Mobey Forum
[78]	Biometrics in Payments – Touching convenience (https://mobeyforum.org/biometrics-in-payments-touching-convenience/)	Mobey Forum
[79]	NFC Activity Technical Specification (https://nfc-forum.org/product/activity-technical-specification-2/)	NFC Forum
[80]	NFC Digital Protocol Technical Specification (https://nfc-forum.org/product/digital-protocol-technical-specification-2-1/)	NFC Forum
[81]	NFC Controller Interface (NCI) Specifications (https://nfc-forum.org/product/nfc-controller-interface-nci-technical-specification-2-1/#:~:text=The%20NCI%20specification%20defines%20a,the%20device's%20main%20application%20processor.&text=The%20new%20version%20also%20includes,communicate%20with%20NFC%20Forum%20tags)	NFC Forum
[82]	NFC Analog Technical Specification (https://nfc-forum.org/product/analog-technical-specification-version-2-1/)	NFC Forum
[83]	Vetting the Security of Mobile Applications, NIST. Draft NIST Special publication 800-163, Revision 1, July 2018 (https://csrc.nist.gov/CSRC/media/Publications/sp/800-163/rev-1/error/documents/sp800-163r1-draft.pdf)	NIST
[84]	OMTP Trusted Environment TR0 v1.2 (https://www.gsma.com/newsroom/wp-content/uploads/2012/03/omtptrustedenvironmentomtptr0v12.pdf)	OMTP



[85]	OMTP Security Threats on Embedded Consumer Devices v1.1 (https://www.gsma.com/newsroom/wp-content/uploads/2012/03/omtpsecuritythreatsonembeddedconsumerdevicesv11.pdf)	OMTP
[86]	OMTP Advanced Trusted Environment TR1 v1.1 (https://www.gsma.com/newsroom/wp-content/uploads/2012/03/omtpadvancedtrustedenvironmentomtptr1v11.pdf)	OMTP
[87]	Open Banking Customer Experience Guidelines, version 1.0, September 2018 (https://www.openbanking.org.uk/wp-content/uploads/Customer-Experience-Guidelines.pdf)	Open Banking
[88]	OWASP Application Security Verification Standard (ASVS), Version 3.0.1, July 2016 (https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)	OWASP
[89]	OWASP Code Review Guide, Version 2.0, July 2017 (https://www.owasp.org/images/7/78/OWASP_AlphaRelease_CodeReviewGuide2.0.pdf)	OWASP
[90]	OWASP Mobile Application Security Verification Standard (MASVS), Version 1.1, July 2018 (https://github.com/OWASP/owasp-masvs)	OWASP
[91]	OWASP Mobile Security Testing Guide (MSTG). Version 1.1, 2018 (https://owasp.org/www-project-mobile-security-testing-guide/)	OWASP
[92]	OWASP Testing Guide. Version 4.0, 2014 (https://www.owasp.org/images/1/19/OTGv4.pdf)	OWASP
[93]	PCI Payment Application Data Security Standard, PA DSS (https://www.pcisecuritystandards.org/minisite/en/docs/PCI_DSS_v3.pdf)	PCI
[94]	Driving Forward with Tokenization and HCE - An SPA Position Paper (https://smartpaymentassociation.com/index.php/liste-documents/public-resources/position-papers/104-14-10-22-pp-tokenization-final-pdf/file)	SPA
[95]	Biometrics in Payment (https://www.smartpaymentassociation.com/images/easyblog_articles/18-05-15_SPA-Biometrics-For-Payments.pdf)	SPA
[96]	STET PSD2 API V1.4, January 2019 (https://www.stet.eu/assets/files/PSD2/1-4-1/api-dsp2-stet-v1.4.1.3-part-3-interaction-examples.pdf)	STET



[97]	Joint Initiative on a PSD2 Compliant XS2A Interface - NextGenPSD2 XS2A Framework Implementation Guidelines (https://www.berlin-group.org/nextgenpsd2-downloads)	The Berlin Group
[98]	Digital Payments Solutions Industry Considerations (http://www.theukcardsassociation.org.uk/wm_documents/Digital%20Wallets%20-%20Industry%20Considerations%20Outline.pdf)	The UK Cards Association
[99]	W3C Web Authentication: An API for accessing Public Key Credentials (https://www.w3.org/TR/webauthn/)	W3C
[100]	W3C Payment Request API (https://www.w3.org/TR/payment-request/)	W3C
[101]	W3C Securing the Web (https://www.w3.org/2001/tag/doc/web-https)	W3C

Table 1: Bibliography

1.3 Definitions

Throughout this document, the following terms are used. Their definitions are based on [5], [17] and [21].

Term	Definition
Account Servicing Payment Service Provider (ASPSP)	A PSP providing and maintaining a payment account for a payer (see [5]).
Account statement information	The information on the SCT payment (for the data elements to be provided, see [17], [21]) available to the Payee on the basis agreed between the Payee and their Payee ASPSP. This may include a paper account statement, an online account statement or a machine-readable statement.
Alias	For payments, an alias is basically a pseudonym for the customer that can be uniquely linked to the customer's name and IBAN in case of an SCT (Instant).
Authentication	The provision of assurance that a claimed characteristic of an entity is correct. The provision of assurance may be given by verifying an identity of a natural or legal person, device or process. ² (see ISO 12812 – Part 1 [70])
Authentication Application	An application accessed through the mobile device performing the functions related to a user authentication, as dictated by the Authentication Service Provider.

² Note that the PSD2 [5] uses a more restrictive definition: "authentication" means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials.



Authentication Service Provider	A service provider offering a customer authentication service typically in the context of this document, involving an Authentication Application accessed via the mobile device of the customer.
Authenticator	A security factor used in an authentication method such as: <ul style="list-style-type: none"> - Something you know, such as a password, PIN or passphrase - Something you have, such as a token device or smart card - Something you are, such as a biometric.
Beneficiary	See Payee.
Bluetooth Low Energy (BLE)	A wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications including beacons. Compared to classic Bluetooth, BLE is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range.
Business Identifier Code (BIC)	An 8 or 11 character ISO code assigned by SWIFT and used to identify a financial institution (see [83]).
Consumer	A natural person who, in payment service contracts covered by the PSD2, is acting for purposes other than his or her trade, business or profession [5].
Consumer Device UVM (CDUVM)	A UVM entered by or captured from the consumer (user) on the consumer device, i.e. a mobile device in the context of this document (see ISO 12812 – Part 1 [70]). In case the user is a cardholder this is also referred to as Consumer Device Cardholder Verification Method (CDCVM – see [10]).
Contactless Technology	A radio frequency technology operating at very short ranges so that the user has to perform a voluntary gesture in order that a communication is initiated between two devices by approaching them. It is a mobile payment acceptance technology at a POI device which is based on ISO/IEC 14443 (see [71]).
(Personalised Security) Credential(s)	Personalised feature(s) provided by the payment service provider to a payment service user for the purposes of authentication (see Article 4 in [5]).
Credit transfer	A payment service for crediting a payee’s payment account with a payment transaction or a series of payment transactions from a payer’s payment account by the PSP which holds the payer’s payment account, based on an instruction given by the payer (see [5]).
Credit Transfer instruction	An instruction given by a payer to a payer ASPSP requesting the execution of a credit transfer transaction, comprising such information as is necessary for the execution the credit transfer and is directly or indirectly initiated in accordance with the provisions of [5].



Credit Transfer Transaction	An instruction executed by a payer ASPSP by forwarding the Transaction to a CSM for forwarding the transaction to the payee ASPSP.
Customer	A payer or a payee which may be either a consumer or a business (merchant).
CustomerID	An identification of the payer, issued by their ASPSP for access to (a) customer facing user interface(s) (e.g. their on-line banking system), as required in the PSD2 API.
2D barcode	A two-dimensional barcode is a machine-readable optical label that contains digital information. They are also referred to as matrix barcodes. Examples include QR codes and tag barcodes.
Digital wallet	A service accessed through a consumer device which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications (e.g., value added services such as loyalty, couponing, etc.). A digital wallet is sometimes also referred to as an e-wallet.
Dynamic authentication	An authentication method that uses cryptography or other techniques to create a one-per-transaction random authenticator (a so-called “dynamic authenticator”).
EMVCo	An LLC formed in 1999 by Europay International, MasterCard International and Visa International to enhance the EMV Integrated Circuit Card Specifications for Payments Systems. It manages, maintains, and enhances the EMV specifications jointly owned by the payment systems. It currently consists of American Express, Discover, JCB, MasterCard, Union Pay and VISA.
Facial recognition	A technology capable of identifying or verifying a person from a digital image or a video frame from a video source. It is one of the CDUVM methods used for mobile payments.
Fingerprint	An impression left by the friction ridges of a human finger. It is one of the CDUVM methods used for mobile payments.
Funds	Cash, scriptural money or electronic money as defined in Article 4 in [5].
Host Card Emulation (HCE)	A technology that enables mobile devices to emulate a contactless card. HCE does not require the local usage of an SE on the mobile device for storage of sensitive data such as credentials, cryptographic keys, etc.
Identification of payee	A means of uniquely identifying the payee and their underlying account. Examples are the usage of IBAN, an alias, card number, dedicated, identifier, dedicated credentials, ...
Immediate(ly)	Synonym for Instant(ly).
Initiator Registry Provider (IRP)	An entity which makes a lookup request into the SPL service, in accordance with the SPL Rulebook (see [26]).
In-app payment	These are payments made directly from within a mobile application (e.g., a merchant app). The payment process is



	completed from within the app to enhance the consumer experience.
Instant(Iy)	At once, without delay.
Instant payment	Electronic retail payment solutions available 24/7/365 and resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee’s account with confirmation to the payer (within seconds of payment initiation). This is irrespective of the underlying payment instrument used (credit transfer, direct debit or payment card) and of the underlying clearing and settlement arrangements that make this possible (see [22]).
Intermediary PSP	A PSP which is neither that of the Payer nor that of the Payee and who participates in the execution of a credit transfer (see section 3.4 in [17]).
International Bank Account Number (IBAN)	An internationally agreed system of identifying bank accounts across national borders to facilitate the communication and processing of cross border transactions (see ISO 13616 [68]).
Merchant	A payee within a mobile payment scheme for payment of the goods or services purchased by the consumer. The merchant is a customer of their PSP.
Mobile code	An authentication credential used for user verification and entered by the consumer via the keyboard of the mobile device.
Mobile device	Personal device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth, etc. Examples of mobile devices include mobile phones, smart phones, tablets and wearables.
Mobile equipment	The mobile phone without the UICC (also referred to as mobile handset).
Mobile Network Operator (MNO)	A mobile phone operator that provides a range of mobile services, potentially including facilitation of NFC services. The MNO ensures connectivity Over the Air (OTA) between the consumer and their PSP using their own or leased network.
MSISDN	Mobile Station International Subscriber Directory Number. This is a number uniquely identifying a subscription in a GSM or a UMTS mobile network. It is the mapping of the telephone number to the SIM card in a mobile phone.
MSCT Application	A set of modules (application software) and/or data (application data) needed to provide functionality for an MSCT Inst or MSCT transaction as specified by the MSCT service provider in accordance with the SEPA SCT Inst or SCT scheme.
MSCT Application user interface	The user interface of a mobile payment application.
MSCT Service Provider	A service provider that offers or facilitates an MSCT service to a payer and/or payee based on a SCT Inst or SCT payment transaction. This may involve the provision of a dedicated MSCT



	application for download on the customer’s mobile device or the provision of dedicated software for the merchant POI. As an example, an MSCT service provider could be a PSP (e.g., an ASPSP or any party acting as a PISP under PSD2) or a technical service provider supporting a PSP.
Mobile payment service	A payment service made available by software/hardware through a mobile device.
Mobile service	A service such as identification, payment, ticketing, loyalty, etc., made available through a mobile device.
Mobile wallet	A digital wallet accessed through a mobile device. This service may reside on a mobile device owned by the consumer (i.e. the holder of the wallet) or may be remotely hosted on a secured server (or a combination thereof) or on a merchant website. Typically, the so-called mobile wallet issuer provides the wallet functionalities but the usage of the mobile wallet is under the control of the consumer.
Mobile wallet issuer	The service provider that issues mobile wallet functionalities to the customer (consumer or merchant).
NFC (Near Field Communication)	A contactless protocol for mobile devices specified by the NFC Forum for multi-market usage. NFC Forum specifications (see [81]) are based on ISO/IEC 18092 [73] but have been extended for harmonisation with EMVCo and interoperability with ISO/IEC 14443 [71].
Originator	See Payer.
Over The Air (OTA)	Any method of making data transfers or transactions wirelessly using the mobile network instead of a cable or other local connection. OTA refers to various kinds of distributing new software to mobile phones like device configuration settings, UICC and eSE configurations and even updating encryption keys. In the context of MSCTs it is used to provision and update the MSCT application, parameters and settings. For the information transfer, different protocols can be used, depending on used configuration such as SMS or remote application management over HTTPS.
Payee	A natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction (see [5]) (examples include merchant, business).
Payer	A natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order (see [5]).



Payment account	An account held in the name of one or more payment service users which is used for the execution of payment transactions (see [5]).
Payment Application Selection User Interface	The mobile phone user interface (component) enabling the consumer to Access the MSCT application User Interface on the mobile phone Select the preferred payment application.
Payment Initiation Service Provider (PISP)	A payment service provider pursuing business activities as referred to in Annex I of [5].
Payment Request	A message sent by the payee to their MSCT service provider and from the payee’s MSCT service provider to the payer MSCT service provider including all transaction data for presentation to the payer to enable them to initiate a transaction and perform SCA as needed.
Payment Service Provider (PSP)	An entity referred to in Article 1(1) of [5] or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33 of [5].
Payment scheme	A technical and commercial arrangement (often referred to as the “rules”) between parties in the payment value chain, which provides the organisational, legal and operational framework rules necessary to perform a payment transaction.
Payment system	A funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions (as defined in [5]).
Payment transaction	An act, initiated by the payer or on his/her behalf or by the payee (payee), of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee (as defined in [5]).
Personal data	Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (see [7]).
POI	“Point of Interaction”, the initial point in the merchant’s environment where data is exchanged with a consumer device (e.g., mobile phone, wearable, etc.) or consumer data is entered (e.g. physical POI, remote POI, QR-code on a poster) to initiate an SCT Inst or SCT.
Physical POI	A POI that is a physical device and consists of hardware and software, hosted in acceptance equipment to enable a consumer and/or merchant to perform an MCST. The merchant-controlled



	POI may be attended or unattended. Examples of POI include POS, vending machine.
Proximity Payment	A payment where the consumer and the merchant (and/or their equipment) are in the same location and where the communication between the mobile device and the Point of Interaction device takes place through a proximity technology (e.g., NFC, 2D barcodes, BLE, ultrasonic, etc.).
Proxy	Data required in order to retrieve a payment account identifier (e.g., mobile phone number, e-mail address, etc.). This is sometimes referred to as an “alias”. As an example, a proxy could be used to replace an IBAN which may be referred to as IBAN-proxy.
Remote POI	The initial point where card data enters the merchant’s domain for remote transactions. It exists in a variety of technical platforms which enable a cardholder (consumer) and/or a merchant to generate a remote payment (e.g. a payment page accessed via a merchant website or via a mobile app).
Remote transaction	In the context of this document, a transaction using a mobile device conducted over mobile internet.
Request-to-Pay	Set of rules and technical elements (including messages) that allow a payee to claim an amount of money from a payer for a specific transaction (see [28]).
Request-to-Pay message	Message sent by the Payee to the Payer, directly or through agents. It is used to request the movement of funds from the payer account to the payee account.
Reservation of the Amount	The Payer Bank Instantly, (i) either reserves the amount of the SCT Inst Instruction on the Payer’s Payment Account with this information being Instantly accessible to the Payer, (ii) or Immediately debits the amount of the SCT Inst Instruction from the Payer’s Payment Account; in both instances the Payer Bank thereafter sends a SCT Inst Transaction message to the relevant CSM.
Responder Registry Provider (RRP)	An entity which responds to a lookup request from the SPL service, in accordance with the SPL Rulebook (see [26]).
Risk-based Authentication	The use of statistical models via transaction, location, device and profile data to make a customer authentication decision without active customer participation in the decision-making process (see also Article 18.3 in [6]).
R-transaction	A transaction to reverse an initial SEPA (Instant) Credit Transfer and the subsequent messages. This refers to the exceptional processes flows, including Rejects, Return, Recalls and Request for Recall by the Payer, see section 4.4 in [17] and/or section 4.3.2 in [22].



Secured Server	A web server with secure remote access that enables the secure storage and processing of payment related data.
Secure Element (SE)	A tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g., key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. There are different form factors of SE including Universal Integrated Circuit Card (UICC), embedded SE (including eUICC and iSE) and microSD. Both the UICC and microSD are removable.
Secure Element (SE) Provider	A TTP which owns the original access rights to the SE. Typical examples are MNOs and mobile device manufacturers.
Sensitive payment data	Data including personalised security credentials which can be used to carry out fraud (see [5]).
SEPA Credit Transfer	The SEPA Credit Transfer is the payment instrument governed by the rules of the SEPA Credit Transfer Scheme for making credit transfer payments in euro throughout the SEPA from bank accounts to other bank accounts (see [17]).
SEPA Instant Credit Transfer	The SEPA Instant Credit Transfer is the payment instrument governed by the rules of the SEPA Instant Credit Transfer Scheme for making instant credit transfer payments in euro throughout the SEPA from bank accounts to other bank accounts (see [21]).
SEPA Proxy Lookup (SPL) Scheme	The SPL Scheme covers the exchange of the data necessary to initiate payments between proxy-based payment solutions on a pan-European level. It aims to facilitate interoperability between participating payment solutions. Initially the focus is on mobile payments whereby the mobile telephone number is used as a proxy to an IBAN. It is envisaged that the SPL scheme will evolve over time to support additional proxy types, account identifiers and use cases (see [26]).
SEPA Proxy Lookup (SPL) Service	A directory service which will initially forward to the IRP an IBAN associated to a mobile phone number provided by an RRP.
Settlement	An act that discharges obligations with respect to the transfer of Funds between Payer ASPSP and Payee ASPSP.
Strong customer authentication	An authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data (see Article 4 in [5]).
Third Party	This is an entity in the ecosystem that is different from an MNO or an MSCT service provider.



Third Party Payment Service Provider (TPP)	A third party that offers payment services which are different to the Account Servicing PSP (ASPSP) such as a Payment Initiation Service Provider (PISP), Account Information Service Providers (AISP) and Trusted Party Payment Instrument Issuer (TPII) (see [5]).
Token	Tokens can take on a variety of formats across the payments industry. They generally refer to a surrogate value for payment account, PSU identification data or transaction related data (e.g., the IBAN for SCT (Instant) payments). Payment Tokens must not have the same value as or conflict with the real payment account related data. If the token is included in the merchant-presented data it might be referred to as a merchant token; if the token is included in the consumer-presented data it might be referred to as a consumer token.
Tokenisation	Process of substituting payment account or transaction related data with a surrogate value, referred to as a token.
Token Requestor	An entity requesting a token to the Token Service
Token Service	A system comprised of the key functions that facilitate generation and issuance of tokens and maintain the established mapping of tokens to the payer account related data when requested by the token requestor. It may also include the capability to establish the token assurance level to indicate the confidence level of the payment token to the payer account related data / payer / merchant / device / environment binding. The service also provides the capability to support token processing of payment transactions submitted using tokens by de-tokenising the token to obtain the actual account related data.
Token Service Provider (TSP)	An entity that provides a Token Service.
Trusted Execution Environment (TEE)	A separate execution environment (as defined by Global Platform, see [53]) that runs alongside, but isolated from the main operating system. A TEE has security capabilities and meets certain security-related requirements: it protects TEE assets from general software attacks, defines rigid safeguards as to data and functions that a program can access, and resists a set of defined threats.
Trusted Platform Module (TPM)	A secure crypto processor (which is a dedicated microprocessor) that securely stores features used to authenticate a computer platform such as PC, laptop, or mobile device. These features can include passwords, certificates, or encryption keys. The TPM can also help to ensure that the platform remains trustworthy.
Trusted Third Party (TTP)	An entity which facilitates interactions between stakeholders of the ecosystem who all trust this third party (examples are SE provider, common infrastructure manager...).



User Interface (UI)	An application or part of an application enabling the user interactions, as permitted by the application issuer. It allows to provide information to the consumer (such as payment amount) and enables the consumer to interact in order to change preferences, perform queries, enter credentials, etc.
UICC	Universal Integrated Circuit Card - A generic and well standardised SE owned and issued by the MNOs.
Ultrasonic	Sound waves with frequencies higher than the upper audible limit of human hearing.
User Verification Method	A method for checking that a consumer is the one claimed (see [70]).

Table 2: Terminology



1.4 Abbreviations

Abbreviation	Term
ASPSP	Account Servicing PSP
API	Application Programming Interface
ATC	Application Transaction Counter
BIC	Business Identifier Code
BLE	Bluetooth Low Energy
CDCVM	Consumer Device Cardholder Verification Method
CDUVM	Consumer Device UVM
CSM	Clearing and Settlement Mechanism
2D barcode	Two dimensional barcode
DSS	Data Security Standards
EBA	European Banking Authority
EC	European Commission
ECSG	European Cards Stakeholders Group
eID	Electronic identity
EIPP	Electronic Invoice Presentment and Payment
EPC	European Payments Council
ERP	Enterprise Resource Planning
ERPB	Euro Retail Payments Board
eSE	Embedded Secure Element
eSSP	Embedded Smart Secure Platform
ETSI	European Telecommunications Standards Institute
FCI	File Control Information
FIDO Alliance	Fast IDentity Online Alliance
GDPR	General Data Protection Regulation
GSMA	The GSM Association
HCE	Host Card Emulation
HLOS	High-level Operating System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS
HSM	Hardware Security Module
IBAN	International Bank Account Number
I2C	Inter-Integrated Circuit
ID	Identifier
ICT	Information and Communication Technology
IoT	Internet of Things
IPR	Intellectual Property Rights
IRP	Initiator Registry Provider
iSE	Integrated Secure Element
ISO	International Organization for Standardization



ISP	Information Service Provider
iSSP	Integrated Smart Secure Platform
rSSP	Removable Smart Secure Platform
LCM	Lifecycle Management
LLOS	Low-Level Operating System
MA	Mobile Application
MACP	Mobile Application Cloud Platform
ME	Mobile Equipment
MIPI	Mobile Industry Processor Interface Alliance
MNO	Mobile Network Operator
MSCT (Instant)	Mobile initiated SCT (or SCT Inst)
MSISDN	Mobile Station International Subscriber Directory Number
NFC	Near-Field Communication
OEM	Original Equipment Manufacturer
OMTP	Open Mobile Terminal Platform
OS	Operating System
OTA	Over the Air
OTP	One-Time-Password
OWASP	Open Web Application Security Project
PCB	Printed Circuit Board
PCI	Payment Card Industry
PISP	Payment Initiation Service Provider
POI	Point of Interaction
POS	Point of Sale
PSD	Payment Services Directive
PSP	Payment Service Provider
PSU	Payment Service User
QR code	Quick Response code
RBA	Risk-Based Authentication
REE	Rich Execution Environment
RFID	Radio Frequency Identification
ROM	Read Only Memory
RRP	Responder Registry Provider
RSP	Remote SIM Provisioning
rSSP	Removable Smart Secure Platform
RTP	Request-To-Pay
RTS	Regulatory Technical Standard
SCL	Serial Clock
SCP	Smart Card Platform
SCT	SEPA Credit Transfer
SCT Inst	SEPA Instant Credit Transfer
SDD	SEPA Direct Debit
SE	Secure Element



SEPA	Single Euro Payments Area
SIM	Subscriber Identity Module
SoC	System on Chip
SP	Service Provider
SPA	Smart Payment Association
SPB	Secondary Platform Bundle
SPI	Serial Peripheral Interface
SPL	SEPA Proxy Lookup
SSL	Secure Sockets Layer
SSP	Smart Secure Platform
STET	
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TP	Third Party
TPM	Trusted Platform Module
TPP	Third Party Payment Service Provider
TSP	Token Service Provider
TTP	Trusted Third Party
UI	User Interface
UICC	Universal Integrated Circuit Card
URL	Uniform Resource Locator
UVM	User Verification Method
VPP	Virtual Primary Platform
XML	Extensible Markup Language

Table 3: Abbreviation

1.5 Maintenance Process

The EPC has established a dedicated multi stakeholder group (see Annex 5) for the development of this document. The multi stakeholder group recommends to regularly update the document to reflect the state of play in light of major new trends and developments related to MSCTs and to keep it aligned with the various documents referenced.



2 General

2.1 Introduction

In November 2019, the first edition of this document, developed by the multi-stakeholder group for mobile initiated SEPA (instant) credit transfers (MSG MSCT) was published on the EPC website, following a public consultation. In view of the rapidly changing market and evolving technology, the multi-stakeholder group has developed a new release of this guidance document.

This new edition is intended for readers who require detailed (technical) guidance on MSCTs. The document includes many updates to the first edition and integrates the various MSCT related documents that have subsequently been developed by the MSG MSCT and which have previously been published as separate documents on the EPC website, after a public consultation: EPC 312-19 [27], EPC096-20 [29] and EPC031-21[30].

The document aims through the description of MSCT use cases to provide an insight into the main issues related to the initiation of (instant) SEPA credit transfers for different payment contexts such as person-to-person, consumer-to-business (retail payments including both in-store and m-commerce payments) and business-to-business payments. Next to the MSCT transaction aspects such as payer authentication, transaction authentication, risk management and payer/payee acknowledgements and notification messages, it focuses on the technology and security used in the customer-to-ASPSP space, since the SCT Inst and SCT transactions as such have already been specified in the respective scheme rulebooks (see [17] and [21]). It furthermore specifies various security guidelines for MSCTs (e.g., MSCT app, CDUVM, PSU on-boarding, mobile device security, etc.). It contains a detailed analysis on the technical interoperability of MSCTs based on payee- or payer-presented data and defines the QR-codes for the exchange of these data. Illustrative examples are included for the interoperability of successful and unsuccessful MSCT transaction process flows using a so-called “HUB” between the payer’s and payee’s MSCT service providers. Additional interoperability models including a Payment Initiation Service Provider (PISP) or a Collecting PSP (on behalf of the merchant) are also included. It further specifies the minimum data sets for all MSCT interoperability messages. This guidance document concludes with a discussion on the main interoperability issues and barriers identified for MSCTs.

This interoperability guidance for MSCTs endeavour to reflect the current state of play and market situation at the time of publication while being brand and implementation model agnostic. On the other hand, it needs to be recognised that the MSCT ecosystem is rapidly evolving with many new entrants in the market. Clearly, market adoption will determine the success of each of these new entrants.

2.2 Vision

This document has been written by the multi-stakeholder group with the following vision:



“To ensure over time, across SEPA, a secure, convenient, consistent, efficient and trusted payment experience for the payer and payee for mobile initiated SEPA (instant) credit transfers, based on commonly accepted and standardised payment technologies.”

This vision is based on the following guiding principles:

- Technical interoperability of MSCTs across SEPA (based on common technical, functional and security standards and an appropriate certification and evaluation framework) both for PSU mobile devices and POIs;
- Full reachability for SCT Inst amongst PSPs;
- Wide availability and usability of appropriate POI equipment and mobile devices;
- Appropriate security and privacy measures to build and maintain trust in the MSCT ecosystem.

The aim is to lead to an enhanced payment experience – e.g., easy P2P payments, faster check out, user-friendliness, a better integration of value-added services with payment – and to cost-effectiveness for society.

This guidance aims to contribute to the creation of the necessary environment so that service providers, vendors and other stakeholders involved in the MSCT ecosystem can deliver secure, efficient and user-friendly MSCT solutions, in an integrated market.

The document contributes to the development of this integrated market for payments in Euro through the development and promotion of standards and guidelines.

This document focuses on the technical interoperability aspects of MSCTs. In the last chapter some non-technical challenges identified with respect to MSCT interoperability are briefly discussed.

2.3 Scope

The guidance focuses on interoperability between the different stakeholders involved in the MSCT ecosystem. In particular, they address the technical interoperability aspects related to the MSCT transaction across SEPA.

The document covers MSCTs, whereby an Instant SEPA Credit Transfer (SCT Inst) or a SEPA Credit Transfer (SCT) as specified in the respective rulebooks (see [21] and [17]) are the underlying SEPA payment instrument³.

More specifically, the document aims to provide information related to the following points:

- A description of MSCT use cases;

³ Note that the use cases and service models introduced in these guidelines may also be applied outside SEPA.



- The MSCT transaction aspects outside the inter-PSP space and the impact of new rules and regulations (PSD2 [5] and RTS [6] , GDPR [7]);
- The roles of the main stakeholders in the MSCT ecosystem;
- Lifecycle management aspects for MSCTs;
- Risk and security aspects related to MSCTs;
- Technical interoperability aspects for MSCTs (including QR-codes, messages, etc.);
- The main industry/standardisation bodies involved and their focus.
- The main challenges and barriers to interoperability within the MSCT ecosystem.

Finally, it is important to note that the document only addresses the aspects of MSCTs, which reside in the interoperability space of the stakeholders in the MSCT value chain. As such, the specification of business cases and a detailed analysis of the MSCT value chain fall outside the scope of the document.

2.4 Objectives

The purpose of this document is to provide interoperability guidance for MSCTs. In order to achieve this the document will

- Provide guidance so that all deployed operational and transactional processes directly related to MSCTs can be implemented while facilitating compliance with relevant rules and regulations (e.g., PSD2 & RTS, GDPR, see Annex 1)
- Describe how MSCTs can be implemented while maintaining appropriate methodologies for risk management, supporting adaptation to prevent fraud.
- Identify barriers to achieving an adequate level of technical interoperability for MSCTs.
- Strive for a harmonised customer experience across SEPA for MSCTs at the POI.
- Enhance the security of and trust in MSCTs.
- Provide guidance for the implementation of MSCTs which is complementary to the SCT and SCT Inst rulebooks (see [21] and [17]) and to the standards developed by standardisation and industry bodies in the MSCT ecosystem (see Chapter 21).



2.5 Audience

The document is primarily intended for the payment industry. It aims to create awareness within this industry about the various aspects to be considered in the development of MSCT solutions. The aim is also to help stakeholders to understand where the risks are, which aspects may become problematic in order to create / maintain an adequate level of trust in MSCTs. It could further be used as a reference by the payment industry to achieve a cohesive payment user experience.

It aims to provide information to stakeholders involved in implementations and deployment of MSCTs, including:

- Payment Service Providers;
- MSCT service providers;
- Other service providers such as MNOs, Tokenisation Providers, etc.;
- Equipment manufacturers;
- Security technology providers;
- Merchants and merchant organisations;
- Consumers and their associations;
- MSCT application developers;
- Regulators;
- Standardisation and industry bodies.



3 High-level principles

The following high-level principles have been employed for the specification of this guidance. They represent a more elaborate version of those contained in the EPC's White paper Mobile payments (see [20]) with a special emphasis on MSCTs.

1. To support the need for SEPA interoperability, the usage of SCT Inst or SCT as specified in the respective rulebooks (see [17] and [21]) is assumed.
2. The service models as described in Chapter 4 and infrastructures used for SCT Inst and SCT payments should be leveraged as much as appropriate.
3. Payment service providers (PSPs) should be able to differentiate their services offer with enough leeway such that the current effective competitive marketplace for payments is not hampered.
4. Creating ease, convenience and trust for PSUs (payers and payees), using a mobile device to initiate an MSCT, is regarded as critical for the further development within this area.
5. Payers shall be able to make MSCTs throughout SEPA, regardless of the original country where the MSCT service was subscribed to and / or provided (issued).
6. A consumer using a specific MSCT service should have a similar experience at the POI throughout SEPA. However, this experience may slightly differ depending on the existing infrastructure or other relevant environmental conditions (e.g., influenced by the risk management or POI environment).
7. Stakeholder (including payers and payees) payment liabilities should be clear, and in line with applicable regulations (see Annex 1).
8. PSPs should have the possibility to develop MSCT services on all the common mobile platforms⁴ in the market openly⁵.
9. The mobile device interface / wallet provider should enable the MSCT service provider to define the graphical interface to the PSU for their MSCT service, including brands and logos, MSCT solution brands, payment type, etc. as appropriate.
10. Payers should have the possibility for their MSCT services to switch mobile devices⁶ and should not be bound to a specific MNO.

⁴ Combination of different hardware and software on a mobile device.

⁵ See Chapter 22

⁶ From different providers (including MNOs, handset manufacturers, OS providers, etc.) subject to appropriate agreements.



11. Payers should be able to use all the MSCT services offered by multiple MSCT service providers using their mobile device⁷.
12. Payers should be able to select the relevant MSCT service on their mobile device to be used for a particular MSCT transaction.
13. All stakeholders involved in the MSCT ecosystem should comply with the mandatory provisions of relevant (EU) rules and regulations as applicable to them (see Annex 1).

⁷ subject to appropriate agreements and risk management considerations.



4 SCT Inst and SCT scheme overview

4.1 Introduction

In this chapter short descriptions are provided for the SEPA Instant Credit Transfer (SCT Inst) and the SEPA Credit Transfer (SCT) schemes. Further detailed information on both schemes may be found in [21], [22] and [17], [18] respectively.

4.2 SCT Inst scheme

An SCT Inst is a payment instrument for the execution of instant credit transfers in euro between PSU payment accounts in SEPA. The SCT Inst is executed on behalf of the payer holding a payment account with a payer ASPSP in favour of a payee holding a payment account with a payee ASPSP.

The execution of an SCT Inst payment involves four main actors:

- **The payer:** is the PSU who initiates directly or indirectly⁸ the instant credit transfer by providing the payer ASPSP with an instruction. The funds for such an SCT Inst are reserved from a specified payment account of which the payer is account holder.
- **The payer ASPSP:** is the participant that receives the SCT Inst Instruction from the payer and acts on the payment instruction by processing instantly the payment to the payee ASPSP in favour of the payee's payment account according to the information provided in the instruction and in accordance with the provisions of the scheme. The payer ASPSP is also obliged to inform immediately the payer in case the funds have not been made available to the payee.
- **The payee ASPSP:** is the participant that receives the SCT Inst transaction from the payer ASPSP and immediately makes the funds available to the payee, according to the information provided in the transaction and in accordance with the provisions of the scheme. The payee ASPSP is also obliged to send a confirmation message (positive or negative) immediately through the same CSM to the payer ASPSP to confirm whether the SCT Inst transaction has been accepted and funds have been made available immediately to the payee (positive confirmation) or not (negative confirmation).

Note: The payer ASPSP and payee ASPSP may be one and the same participant.

- **The payee:** is the PSU identified in the SCT Inst instruction to whom the funds are sent.

The payer ASPSPs and the payee ASPSPs are responsible for meeting their obligations under the SCT Inst scheme rulebook [21].

The operation of the scheme also involves other parties indirectly:

⁸ In compliance with PSD2 [5].



- **CSMs:** Such mechanisms could include the services of a clearing and settlement provider such as an automated clearing house or other mechanisms such as intra-PSP and intra-group arrangements and bilateral or multilateral agreements between participants. The term CSM does not necessarily connote one entity, for example, it is possible that the clearing function and the settlement functions are conducted by separate actors.
- **Intermediary PSPs:** PSPs offering intermediary services to payer and/or payee ASPSPs, for example in cases where they are not themselves direct participants in a CSM.
- **Payment initiation service providers (PISP):** Payers may make use of a PISP to initiate an instant credit transfer.

An SCT Inst payment under the SCT Inst scheme consists of the following steps as specified in [21] and illustrated in the figure below.

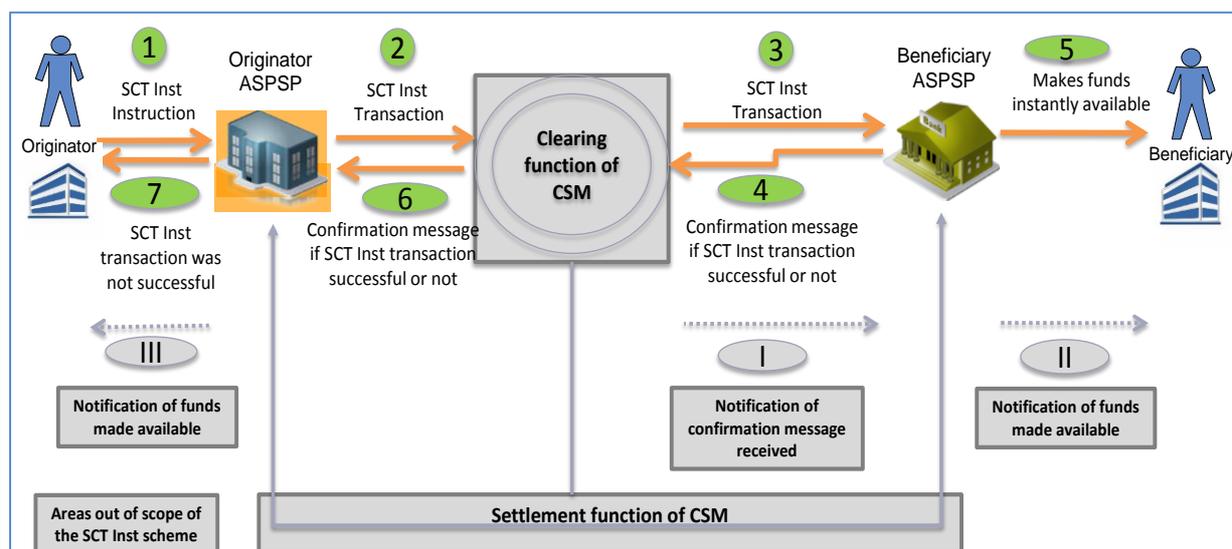


Figure 1: Overview SCT Inst transaction process flow

Notes:

- This figure taken from the SCT Inst scheme rulebook [21] refers to the payer as the originator and to the payee as the beneficiary.
- **Figure 1** displays the distinction between the clearing function and the settlement function of a CSM. The term “CSM” will be used to cover both functions.

Step 1: the payer ASPSP receives an SCT Inst instruction from the payer⁹. The payer ASPSP then instantly executes all processing conditions and funds availability checks. When these validation checks are successful, the payer ASPSP *instantly* makes a “Reservation of the amount”¹⁰ on the payer’s payment account with this information *instantly* accessible to the

⁹ Directly or indirectly initiated in compliance with the PSD2 [5].

¹⁰ See Chapter 7 in [21] for the definition of “Reservation of the amount”.



payer, *instantly* prepares an SCT Inst transaction based on the SCT Inst instruction and puts the time stamp in the created SCT Inst transaction.

Step 2: the payer ASPSP *instantly* sends the SCT Inst transaction message to the CSM of the payer ASPSP. Via this message, the payer ASPSP gives the authorisation to the CSM of the payer ASPSP to reserve funds on its account as cover for the SCT Inst transaction. This provides upfront settlement certainty.

Clearing function of CSM - out of scope of the scheme: the CSM of the payer ASPSP *instantly* reserves funds from the payer ASPSP as settlement cover for the SCT Inst transaction. The CSM of the payer ASPSP *instantly* sends the SCT Inst transaction to the CSM of the payee ASPSP.

Step 3: the CSM of the payee ASPSP *instantly* sends the SCT Inst transaction message to the payee ASPSP.

For the payee ASPSP, this message under step 3 implies that the payee ASPSP has *settlement certainty* for this SCT Inst transaction in case the payee ASPSP accepts the transaction for further processing.

The payee ASPSP *instantly* verifies if it can apply the SCT Inst transaction to the payee's payment account and executes various validation checks.

Step 4: the payee ASPSP sends the confirmation message to the CSM of the payee ASPSP indicating that the payee ASPSP

- has received the SCT Inst transaction and
- is able to *instantly* process the SCT Inst transaction (*positive confirmation*) or not (*negative confirmation with an immediate Reject*)

The CSM of the payee ASPSP gives a certainty of receipt for the confirmation message that the payee ASPSP has sent.

Clearing function of CSM: out of scope of the Scheme: based on the message received in Step 4:

- in case of a negative confirmation: the CSM of the payee ASPSP passes on this confirmation message to the CSM of the payer ASPSP. The CSM of the payer ASPSP releases the reservation of funds for the cover done between steps 2 and 3.
- in case of a positive confirmation:
 - **Step 1 - out of scope of the Scheme:** based on upfront technical arrangements (e.g., a technical acknowledgement, a special designed message) the CSM of the payee ASPSP notifies to the payee ASPSP that the message in step 4 has been successfully received.



- The CSM of the payee ASPSP initiates the final settlement processing for this specific SCT Inst transaction with the CSM of the payer ASPSP.

Step 5: only when the payee ASPSP has sent a positive confirmation via the message in Step 4 *and* the payee ASPSP has the *certainty* that the message under Step 4 has been *successfully delivered* to the CSM of the payee ASPSP, it *instantly makes the funds available* to the payee. The payee ASPSP relies on the settlement certainty covered by the message in Step 3.

The information about the new available funds is *instantly* accessible to the payee. This action means that the payee has immediate use of the funds subject to the terms and conditions governing the use of the payment account of the payee.

Step II - out of scope of the scheme: if agreed with the payee, the payee ASPSP may inform the payee about the *funds made available* to the payee. The information itself and the execution time for such information are not within the scope of the scheme.

Step 6: the CSM of the payer ASPSP instantly reports to the payer ASPSP if the SCT Inst transaction had been successful (or not). The basis for this report is the contents of the confirmation message in Step 4 which the CSM of the payer ASPSP had received via the CSM of the payee ASPSP.

Step 7: in case the payer ASPSP receives a negative confirmation about the SCT Inst transaction which indicates that *the funds have not been made available* to the payee, the payer ASPSP is *obliged to immediately* inform the payer. The payer ASPSP lifts the “Reservation of the amount” made in Step 1.

Step III - out of scope of the scheme: in case the payer ASPSP receives a positive confirmation about the SCT Inst transaction, it formally debits the payment account of the payer.

If agreed with the payer, the payer ASPSP informs the payer about the *funds made available* to the payee. The information itself and the execution time for such information are not within the scope of the scheme.

Settlement function of a CSM - out of scope of the scheme: when a positive confirmation is received, the amount of the SCT Inst transaction is included in the settlement procedure between the payer ASPSP and the payee ASPSP, and as such credited by the CSM to the payee ASPSP during the settlement process.

For the exception handling related to SCT Inst payments and the “*R-transactions*”, the reader is referred to section 4.3.2 in [21].



4.3 SCT Scheme

A SEPA Credit Transfer is a payment instrument for the execution of credit transfers in euro between PSU payment accounts located in SEPA. It involves the same actors as referred to in section 4.2.

An SCT payment under the SCT scheme consists of the following steps as specified in [17] and illustrated in the figure below.

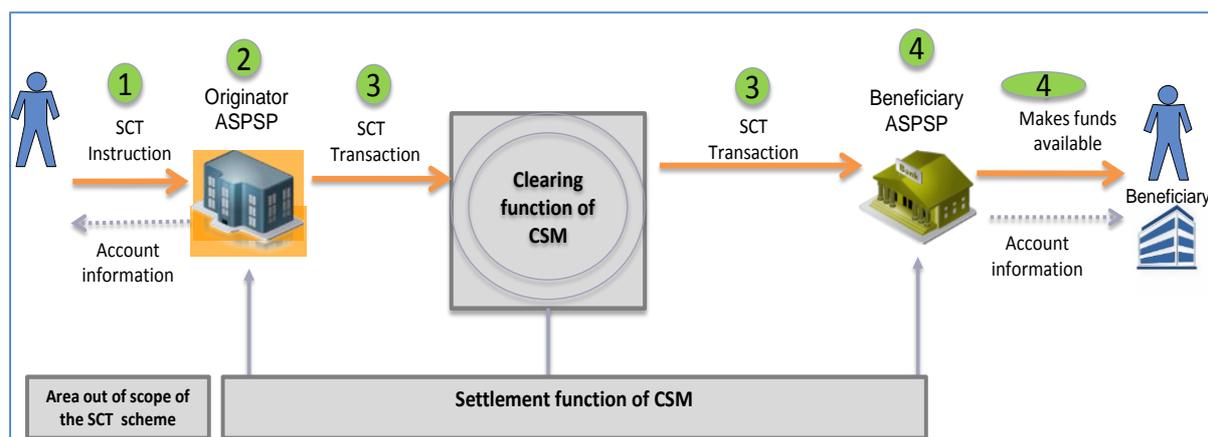


Figure 2: Overview SCT transaction process flow

Notes:

- This figure taken from the SCT scheme rulebook [17] refers to the payer as the originator and to the payee as the beneficiary.
- **Figure 2** displays the distinction between the clearing function and the settlement function of a CSM. The term “CSM” will be used to cover both functions.

Step 1: The payer¹¹ completes and forwards the credit transfer Instruction. The instruction will be submitted by any means agreed between the payer and the payer ASPSP. The data elements to be provided are defined in [17].

Step 2: The payer ASPSP receives and checks if it has sufficient information to execute a payment instruction and that the instruction fulfils the conditions required by its procedures as to execution of the instruction including the authenticity of the instruction, and the checking of the format and plausibility of the BIC and IBAN. The execution time for an SCT shall commence (Day “D”) at the point in time of receipt of the credit transfer Instruction, as defined in the PSD2¹².

¹¹ Directly or indirectly initiated in compliance with the PSD2 [5].

¹² The "Requested Execution Date" corresponds with a date requested by a payer for commencing the execution of the credit transfer instruction. The payer may choose to request a Requested Execution Date in the future and submit the credit transfer instruction to the payer ASPSP in accordance with its terms and conditions with the payer ASPSP. In such cases, the agreed date will be deemed to be the relevant date for commencing the execution of the credit transfer Instruction.



Step 3: On or following “D”, the payer ASPSP will debit the account of the payer¹³. This will be followed by the sending of the credit transfer Instruction to ensure receipt by the payee ASPSP via the selected CSM in accordance with the rules of the scheme. The data elements to be provided are defined in [17].

Step 4: The payee ASPSP should credit the account of the payee in accordance with the provisions of the PSD2 [5]. The payee ASPSP will make the information on the SCT payment (for the data elements to be provided, see [17]) available to the payee on the basis agreed between the payee and their payee ASPSP. This may include a paper account statement, an online account statement or a message readable statement. In the sequel of this document this will be referred to as “Account statement information”.

Credit transfer transactions are handled according to the time frame described above. If, for whatever reason, any party cannot handle the transaction in the normal way, the process of exception handling starts. The messages resulting from these situations are all handled in a standardised way, at process level as well as at dataset level. A brief overview of the possible processes is provided below while the reader is referred to section 4.4 in [17] for further details.

A “*Reject*” occurs when a credit transfer is not accepted for normal execution before interbank settlement. If the rejection is at the point at which the payer instructs the payer ASPSP, for the purposes of the scheme, the payer ASPSP need only to inform the payer of the reason.

A “*Return*” occurs when a credit transfer is diverted from normal execution after interbank settlement, and is sent by the payee ASPSP to the payer ASPSP for a credit transfer that cannot be executed for valid reasons such as wrong account number or account closed with the consequence that the payee account cannot be credited on the basis of the information contained in the original credit transfer message. The Return procedure must not be used in cases where the payee’s account has already been credited and the payee wishes to return the funds. Instead, the procedure of initiating a new credit transfer applies.

A “*Recall*” occurs when the payer ASPSP requests to cancel an SCT. The Recall procedure must be initiated by the payer ASPSP within 10 “Banking Business Days” after execution date of the SCT subject to the Recall. The Recall procedure can be initiated only by the payer ASPSP, which may do it on behalf of its PSU. Further details on the reasons for a Recall may be found in 4.3.2.2 in [17].

A “*Request for Recall by the Payer*” can be initiated by the payer ASPSP after a payer has requested the payer ASPSP to reverse a settled credit transfer for a reason other than duplicate sending, technical problems resulting in erroneous credit transfer(s) and a fraudulently originated credit transfer.

¹³ Payer ASPSPs are obliged to ensure that the amount of the Credit Transfer is credited to the account of the Payee ASPSP within one Banking Business Day (see [17]) following the point in time of receipt of the Credit Transfer Instruction in accordance with the provisions of the Payment Services Directive.



These four transaction processes described above will be referred to in the sequel of the document as “*R-transactions*” and associated messages.

In addition, “*SCT inquiries*” are defined which may be used when a scheme participant requests information or clarification about the status of an SCT. For further information on inquiries, the reader is referred to section 4.5 in [17].



5 Mobile initiated SEPA (Instant) Credit Transfers

5.1 Introduction

This chapter aims to provide a high-level overview about MSCTs, including both the MSCT transaction and the provisioning and life cycle management.

5.2 MSCT Transaction

5.2.1 Introduction

MSCT transactions are SCT Inst or SCT transactions that are initiated by the payer using a mobile device. They are based on the existing SCT Inst or SCT rulebooks (see [21] and [17] respectively) in the so-called “inter-PSP space” and are therefore using in that space the existing payment infrastructure. They typically use a mobile MSCT application or mobile browser on the payer’s mobile device to initiate the SCT Inst or SCT transaction, besides some features of the mobile device such as the support of a CDUVM, the mobile device screen to display transaction information, etc. Therefore, this document will mainly focus on the interactions outside the inter-PSP space such as between the mobile device and the POI, between the payer and payee, between the payer/payee and their MSCT service provider and between MSCT service providers (see also [Figure 1](#) and [Figure 2](#)).

5.2.2 MSCT modes

For MSCTs, basically two modes¹⁴ can be distinguished depending on how the data that enables the initiation of the payment is transferred between the payer and the payee:

- MSCTs based on payee-presented data: in this mode the data, i.e. the payee identification and, as needed, transaction data is provided by the payee to the payer and is either
 - presented by the payee and read by the payer’s mobile device (e.g. via proximity technology);
 - already shared by the payee with the payer beforehand (e.g. in P2P payment contexts);
- MSCTs based on payer-presented data: in this mode the data, i.e. the payer identification is provided by the payer to the payee and is either
 - presented by the payer and read by the payee’s device via a proximity technology (e.g. physical POI or mobile device);
 - entered by the payer into the payee’s POI (e.g. webpage of self-check-out);
 - already shared by the payer with the payee beforehand (e.g. entered by the payer during the on-boarding process and subsequently stored into a merchant app on the payer’s mobile device).

¹⁴ Note that when a proximity technology would be used in a bi-directional way between the payer and payee, MSCT transaction data could be exchanged in the two directions. However, currently there are no such implementations for MSCTs in the market.



5.2.2.1 MSCTs based on payee-presented data

Currently, there is a wider market adoption of MSCTs based on payee-presented data for all payment contexts; it is the most important mode used for P2P payments and for C2B payments at a physical POI, while for payments at a virtual POI there appears to be geographical differences. Moreover, payee-presented QR-codes seem to be the most important proximity technology adopted by the market for C2B payments. The payee-presented mode also facilitates the usage of MSCTs for paying invoices through the usage of a payee-presented QR-code.

From a payer perspective, the usage of an MSCT app on their mobile device that supports payee-presented data allows them to pay for all payment contexts (P2P, C2B and B2B), which leads to a consistent payment experience, enhanced trust and no need to share payer identification data with the payee. Moreover, it enables an easier risk management for the payer's MSCT service provider.

5.2.2.2 MSCTs based on payer-presented data

For C2B payment contexts, this mode enables merchants to issue a merchant app to their customers. It also gives them the opportunity to offer value-added services such as loyalty, couponing, etc. More in particular, large merchants appear to be interested in this mode in view of the consistent consumer experience for payments at a physical POI, being it account- or card-based. This mode could potentially¹⁵ also enable so-called off-line MSCTs whereby the payer's mobile device has no mobile network connectivity at the moment of the transaction.

However, this mode also comes with a number of challenges. Currently many POI terminals are not equipped yet for payer-presented mode (e.g. missing a QR-code reader). Moreover, there are some security concerns related to the generation of the payer-presented QR-code, e.g., if generated outside the control of the payer's MSCT service provider (see Chapter 10).

5.3 MSCT Provisioning and life cycle management

For MSCTs, the hosting of a dedicated MSCT application on the mobile device may be required. This MSCT application requires full life cycle management by the MSCT service provider, including provisioning, activation, personalisation, etc. (see Chapter 6). An MSCT application may be supported by complementary applications residing on the mobile device's "Read-Only Memory (ROM)", which are known as the MSCT application user interface and which are dedicated to interacting with the user. The MSCT service provider is responsible for this application, its security characteristics and the secure communication with the MSCT application.

Also a separate dedicated authentication application hosted on the payer's mobile device may be involved to conduct an MSCT. Likewise, if present, it requires a full life cycle management by the authentication application service provider, including provisioning, activation, personalisation, etc., in analogy to an MSCT app.

¹⁵ Subject to further clarifications to be provided by the EBA, see Q&A questions 2020_5365-5367.



If no MSCT application is present, the mobile device may be used to store static data/credentials for MSCTs (e.g., in a mobile wallet). If there are security requirements for these data (integrity and/or confidentiality), the data needs to be stored in a trusted environment with some access control.

5.4 Relevant stakeholders in the MSCT ecosystems

MSCTs involve some new stakeholders in the value chain compared to (instant) SEPA credit transfers.

The following stakeholders, in addition to the ones described in Chapter 4 may be involved:

- The MSCT service provider that offers an MSCT service to a payer and/or payee related to a SCT Inst or SCT payment transaction. This typically involves the provision of an MSCT application for download on the PSU's mobile device or the provision of dedicated software for the merchant POI. Examples include a mobile P2P payment service provider or a PISP. The MSCT service provider is linked to the payer's ASPSP and may be linked to the payee's ASPSP (this linkage includes both technical and contractual aspects). Note that an ASPSP may assume the role of an MSCT service provider.
- The Token Service Provider (TSP) is a TTP who is involved if tokens are used in MSCTs as surrogate values for the payer identification data (for a payer-presented token) or for payee identification data or transaction data such as transaction amount or transaction identifier (for payee-presented tokens) (see section 10.4 and Chapters 16 to 18). The TSP manages the generation and issuance of tokens, and maintains the established mapping of tokens to the related data when requested by the token requestor. The TSP also provides the capability to support token processing of MSCT transactions submitted using tokens by de-tokenising the token to obtain the transaction related data. In the document it is assumed that the role of TSP is covered by the MSCT service provider or is at least under the control of the MSCT service provider.
- The Mobile Wallet Issuer is a service provider that issues mobile wallet functionalities to the PSU (consumer or merchant).
- Other relevant new stakeholders include for example:
 - Secure Element (SE) providers, if the MSCT application /Authentication application is stored in an SE on the mobile device. This is the MNO in case of a UICC, the mobile equipment manufacturer, the MSCT service provider or a third party in case of an embedded SE, and the SE manufacturer.
 - Cloud service providers (which may be the MSCT service providers themselves or this service may be delegated to a TTP),
 - Application developers (MSCT application, user interface, mobile wallet ...),
 - Mobile Operating System (OS) suppliers,
 - Mobile equipment manufacturers,
 - Security technology developers,
 - Mobile Network Operators (MNOs),



- Organisations performing infrastructure certification (e.g., MSCT applications, POI, mobile devices, etc.).

At this stage, with the large number of stakeholders involved, alignment around key aspects of the ecosystem is crucial to move from fragmentation to harmonisation and to enable the development of SEPA-wide service offerings.

Numerous market studies available show that, besides strong market potential, mobile payments have really taken off (see for instance [65]). The major elements supporting a rationale for service providers to enter the mobile payments market include the following:

- Strong penetration of mobile devices: mobile phones have achieved full market penetration with enriched technology and service levels. More in particular in Europe, nowadays, “smart phones” have become ubiquitous¹⁶. Therefore, they are an ideal channel for increasing the usage of SEPA payment instruments. Moreover, more and more consumers are ready and are willing to use the mobile device for payments.
- The usage of the mobile device for payments allows to enhance the consumer purchase experience through value-added services such as loyalty, couponing, e-receipts, etc.
- Provisioning of user convenience by meeting proven needs of both consumers and merchants.
- The quick evolution and adoption of technology during the recent years.
- The need to foster innovation with competitive offerings to the customer’s benefit in a more complex ecosystem including new stakeholders, thereby growing the market for non-cash payments and migrating consumers to faster, more efficient and more convenient means of payments.

As mentioned above, it is not the purpose of this document to discuss the strategy for which a service provider may enter the market and the concrete service models including the various interactions among the different stakeholders in the value chain. However, a high-level description of various service models is provided in Chapters 16 and 20.

The main drivers identified for some of the stakeholders involved in the ecosystem for a potential adoption of mobile payments include the following:

Payer/Payee’ expectations and demands

- Efficiency: speed of payment, frictionless;
- Mobility: make cashless payments anywhere, anytime;
- Consistent user experience;
- Convenience: e.g. user-friendly payer authentication;
- Simplicity for enrolment and to conduct a payment;
- Merchant reimbursement¹⁷

¹⁶ More than 3 billion smart phone reported in March 2021 , see <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>

¹⁷ Referred to as “transfer back” in the respective SCT Inst and SCT scheme rulebooks ([21] and [17]).



- Confidence and trust;
- Notification of payment to payer and payee.
- Privacy and data protection;
- Wide merchant acceptance of MSCTs.

Note that value added services such as special offers or loyalty points are also part of consumers' expectations but are out of the scope of this document which solely focuses on the payment transaction.

Merchants' expectations

- Quick, efficient and secure process at point of payment;
- High availability and minimum latency;
- Cost effectiveness;
- Capable of supporting repayments (sometimes referred to as "refund" or "transfer-back");
- Consumer focused: The payment process needs to be quick, convenient and simple, easily understood by consumers who can see the benefits and "want to use it";
- Confidence and trust in the end to end process by both consumers and merchants;
- Availability of the funds: Either immediate payment or confirmation and/or assurance of payment to enable release of goods or services to the consumer;
- Capable of supporting alternative digital payments;
- Reachability of consumers through any mobile device (interoperability);
- Easy and low cost to implement and quick to market functionality;
- Standardisation of reporting from the ASPSP to the merchant to enable transaction and account statement reconciliation either through batch or individual transaction reporting;
- Optionally, subject to consumer consent, the provision of related additional services through consumer payment data collection to enable cross-selling and geo-based marketing services.

Service providers' expectations

- Customer retention/acquisition;
- Cost efficiency;
- Risk reduction / improved monitoring;
- Provision of related additional services;
- Desire for "cash displacement" and, in some countries, "cheque displacement";
- Compliance with regulations.

Clearly, MSCTs will co-exist with other means of payment on the mobile device while the mobile device will be an additional payment initiation channel co-existing with other channels. Other alternatives exist and the payments business is not limited to SEPA's geographical scope.



6 MSCT service management

6.1 Introduction

If an MSCT application is installed on the mobile device, dedicated processes need to be defined for its provisioning and life cycle management, which may vary depending on the implementation chosen (e.g. software or SE-based). In addition, while implementing these processes, the MSCT service provider should ensure compliance with relevant rules and regulations (see Annex 1).

If a separate dedicated authentication application is hosted on the payer's mobile device that is used to conduct an MSCT, a similar application life-cycle management would need to be applied by the authentication application service provider.

6.2 MSCT application life-cycle

Functions for application lifecycle management are triggered by one or several possible situations and require actions from the MNO and/or the MSCT service provider and/or a third party (e.g., an SE issuer). In some cases, actions may be required from the customer. The protocols used to execute the functions for MSCTP application lifecycle management will typically encompass acknowledgement/confirmation of the actions. This section provides the following non-exhaustive list of functions based on ISO 12812 [70]:

1. *Eligibility request*: The MSCT service provider requests an eligibility report from the MNO or a third party to ascertain that the customer's mobile device is technically capable of hosting the MSCT application and operating the related MSCT service;
2. *Installation of MSCT application*: The installation of the MSCT application on the mobile device, possibly in an SE;
3. *Installation of MSCT application user interface*: The installation of the mobile equipment application executing the user interactions related to the MSCT application, as permitted by the MSCT service provider. Depending on the implementation this might require user interaction. This function may also include the personalisation and activation¹⁸ of the MSCT application.
4. *Update of MSCT application parameters*: The update of MSCT application parameters and counters (e.g., for risk management) during the lifecycle of the application;
5. *Deletion of MSCT application*: The removal of the MSCT application and related data from the mobile device;
6. *Deletion of MSCT application user interface*: The removal of the MSCT application user interface and related data from the mobile device;

¹⁸ Note however that different implementations may exist where this is to be considered as a separate function.



7. *Blocking of MSCT application:* The MSCT service provider instructs the MSCT application to block itself either locally or remotely;
8. *Unblocking of MSCT application:* The MSCT service provider unblocks remotely the MSCT application;
9. *Blocking of mobile network connectivity:* The MNO blocks the network connectivity of the mobile device at the MNO server-side.
10. *Unblocking of mobile network connectivity:* The MNO re-installs the network connectivity of the mobile device at the MNO server-side.
11. *Audit of MSCT application:* The MSCT service provider retrieves MSCT application data from the MSCT application (e.g.; via OTA).
12. *Audit of SE:* If an MSCT application is stored in an SE, the MSCT service provider may request the SE issuer information about the SE resources, state of their MSCT application(s), etc.

Each phase of the MSCT application lifecycle (subscription, installation, usage and termination) is carried out by the execution of the processes listed hereafter. A process may be covered by functions described above.

- *Subscription (on-boarding)*
 1. Inquiry to MSCT service provider
 2. Inquiry to SE issuer (if MSCT application is hosted on an SE)
 3. Subscription to MSCT service (application);
 4. Renewal of MSCT service (application);
 5. Mobile device eligibility check;
- *Installation*
 6. Installation of MSCT application;
 7. Installation of MSCT application user interface;
- *Usage*
 8. Audit MSCT application;
 9. Update MSCT application parameters;
 10. Change SE (if applicable);
 11. Change mobile phone number;
 12. Change mobile equipment;
 13. Lost/stolen mobile device – contact MNO;
 14. Lost/stolen mobile device – contact MSCT service provider;



15. Recovery of mobile device (contact MNO/MSCT service provider);
16. New mobile device after lost/stolen;
17. Change MNO;
18. Temporary mobile services suspension;
19. Resume mobile services;
20. Temporary MSCT application suspension;
21. Resume MSCT application;
22. MSCT service provider customer relationship management;
23. MNO customer relationship management;

- *Termination*

24. Mobile service termination by customer;
25. Mobile service termination by MNO;
26. MSCT application termination by customer;
27. MSCT application termination by the MSCT service provider.



7 MSCT use cases

7.1 Introduction

The table below provides an overview of mobile payments based on the underlying payment instruments.

Mobile payments		
Payment context	Card-based	Account-based (SCT Inst or SCT)
Person-to-Person (P2P)		
<ul style="list-style-type: none"> • Mobile banking <ul style="list-style-type: none"> ○ Browser ○ Dedicated application • Dedicated MSCT application 	EPC White paper mobile payments [20]	EPC White paper mobile payments [20] MSCT IG
Consumer-to-Business (C2B) or Business-to-Business (B2B)		
m-Commerce <ul style="list-style-type: none"> • Browser-based (on mobile device) • Dedicated MSCT app • Merchant app (App-to-App, In-App) 	SEPA Cards Standardisation Volume [10] EPC White paper mobile payments [20]	EPC White paper mobile payments [20] MSCT IG
Proximity payments (physical interaction) <ul style="list-style-type: none"> • NFC • QR-codes • BLE • 	SEPA Cards Standardisation Volume [10] MCP IG [23] White paper non-NFC mobile SEPA card proximity payments [24]	EPC White paper mobile payments [20] MSCT IG

Table 4: Overview mobile payments

The light purple part in the table above marks the scope of this document.



7.2 Overview MSCT use cases

7.2.1 Introduction

In this document, MSCT use cases will be described with a diagram depicting the different actors involved and with a decomposition into the different steps of the MSCT transaction which are also shown in a figure. Each MSCT use case is followed by a short evaluation on the interoperability aspects for deployment across SEPA and a short list of the main challenges.

Note that these MSCT use cases are presented for *illustrative purposes*, in other words, the list of MSCT use cases described is not meant to be exhaustive but should be seen as examples for specific payment contexts. Some of the MSCT use cases are included in section 7.3 of this chapter while the remaining ones may be found in Annex 2.

Payment context	#	MSCT use case description
Person-to-Person (P2P) payments	P2P-1	Mobile device - Payment with proxy - SCA using MSCT application involving mobile code
	P2P-2	Mobile device - Payment request with proxy via messaging application - SCA using MSCT application involving fingerprint
	P2P-3	Mobile device - Mobile banking via browser - Static customer authentication with on-line passcode
	P2P-4	Mobile device - Payment with payee-presented QR-code - SCA using MSCT application involving a facial recognition
Consumer-to-Business (C2B) payments	C2B-1	Mobile device - Payment of invoice with merchant-presented QR-code – SCA involving mobile code
	C2B-2	Mobile device - Payment at a physical POI with merchant-presented QR-code - MSCT application with SCA using a dedicated authentication application (decoupled app-to-app) involving fingerprint
	C2B-3	Mobile device - m-commerce - Mobile browser - PISP with embedded SCA involving dynamic authenticator
	C2B-4	Mobile device - Transport ticketing - In-app payment - SCA involving fingerprint
	C2B-5	Mobile device - Payment at a physical POI with consumer - presented QR-code - SCA using an MSCT application involving mobile code
	C2B-6	Mobile device - Off-line use case - Payment at a physical POI using NFC and EMV-based SCA involving fingerprint (a so-called hybrid use case)
	C2B-7	Mobile device - Off-line use case - Payment at a physical POI with consumer-presented QR-code involving a PISP - SCA via BLE using an MSCT app involving fingerprint
	C2B-8	Mobile device - Payment at a physical POI with consumer-presented QR-code - Unknown final amount with final amount



		being lower than pre-agreed amount - SCA of consumer using MSCT application involving fingerprint
	C2B-9	Mobile device - Payment at a physical POI with merchant-presented QR-code - SCA using an MSCT application involving mobile code
	C2B-10	Mobile device - m-commerce - Merchant application - PISP with redirection to consumer ASPSP for SCA involving dynamic authenticator
	C2B-11	Mobile device - Payment at a physical POI involving consumer-presented QR-code - SCA using a dedicated authentication application involving fingerprint
	C2B-12	Mobile device - Payment at a physical POI with consumer-presented QR-code involving a PISP - SCA using a dedicated authentication application involving fingerprint
	C2B-13	Smartwatch - Payment at a physical POI with consumer-presented QR-code involving a PISP - SCA using an embedded authentication via the POI involving OTP and PIN
	C2B-14	Mobile device - Off-line use case - Payment at a physical POI with consumer-presented QR-code - SCA involving facial recognition
	C2B-15	Mobile device - Payment at a physical POI with consumer-presented QR-code - Unknown final transaction amount with final amount being higher than pre-agreed amount - SCA using a dedicated authentication app involving mobile code
Business-to-Business (B2B) payment	B2B-1	Mobile device - Payment request ¹⁹ - SCA involving mobile code

Table 5: Overview illustrative MSCT use cases

Notes:

- The MSCT use cases in the table above for m-commerce that refer to the usage of an MSCT application may also be implemented using a dedicated web page.
- In the MSCT use cases below a specific strong customer authentication (SCA) method has been described for illustrative purposes. Note that alternative SCA methods, including CDCVMs exist and are discussed in Chapter 8.
- In all the descriptions of the MSCT use cases for C2B payment contexts, reference is made to the merchant name; this refers to the merchant trade name and/or, if not available, at least the merchant legal name.
- Although no examples have been included for car-on-board units, acting as interactive devices, the description of an MSCT using a car-on-board unit as a payer device, would

¹⁹ See section 15.4 for the SEPA RTP scheme that supports this MSCT use case.



be similar to the MSCT use cases already included in this Chapter. Often, although implementation dependent, the payment use case with a car-on-board unit will be an MSCT based on payer-presented data.

7.2.2 Characteristics MSCT use cases

A more detailed overview on the main characteristics of the MSCT use cases described in this document (as listed in **Table 5**) are presented in the table below.



Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance
 EPC269-19 Version 1.14

MSCT Use case #	Mobile Technology	Payer interface provider (s)	PSU experience	Type of data exchanged between payer and payee	Authentication	Description of the underlying service
P2P-1	MSCT app	ASPSP	Payer selects a functionality made available by a previously downloaded MSCT app and sends funds to a payee who holds an account with the same or with a different ASPSP.	Payee proxy (SPL) - mobile phone number	SCA involving a mobile code and authentication code calculated using a dedicated key in the MSCT app	The MSCT (P2P) app enables the payer to select a payee from the list of contacts and prepares an SCT (Inst) instruction using the mobile number of the payee as an alias. The MSCT app uses the SPL service to retrieve the payee account data.
P2P-2	MSCT app + messaging app	MSCT service provider + Messaging service provider	Payee selects a functionality made available by a previously downloaded MSCT app, enters the amount that is split amongst # payers and enters personal message. Payee sends a payment request via the messaging app and selects the payers in the address book. The message contains the amount, the personal	Payee proxy (SPL) - mobile phone number	SCA involving a fingerprint and authentication code calculated using a dedicated key in the MSCT app	The MSCT (P2P) app enables the payer to split the amount and connect to a messaging service that also holds an address book to select the payers. The MSCT Inst application uses the SPL service to retrieve the payee account



			message and the mobile phone number of the payee. The payers click on the request and opens their MSCT app. The MSCT app uses the SPL service to retrieve payee's account and sends funds.			
P2P-3	Mobile browser	ASPSP	Payer uses a mobile browser to access their mobile banking service and sends funds to a payee who holds an account with the same or with a different ASPSP.	IBAN_payee in full or pre-registered	Static authentication involving a CustomerID and passcode	The payer accesses their mobile banking environment, authenticates and sends a SCT (Inst) instruction.
P2P-4	MSCT app + QR-code scanner	ASPSP	The payee selects a functionality made available by the MSCT app and enters the amount to be paid. The MSCT app generates a QR code containing payee name, IBAN and amount. Payer scans the QR-code and acquires the payee data	Payee-presented QR-code	SCA involving facial recognition and authentication code calculated by MSCT app using a dedicated key	The payee uses an MSCT app to generate a QR-code containing the transaction details for the payer to scan.



			and confirms the operation.			
C2B-1	MSCT app + QR-code scanner	ASPSP	Consumer selects a functionality made available by the MSCT app and scans a QR-code printed on an invoice containing payee data, the amount and the invoice nr.	Merchant-presented QR-code	SCA involving a mobile code and authentication code calculated using a dedicated key by the MSCT app	The merchant generates a QR-code containing payment details and prints it on an invoice for the consumer to scan.
C2B-2	MSCT app + QR-code scanner + dedicated SW on POI	MSCT service provider + Authentication service provider	Same as above, only the payer authentication is performed through a dedicated authentication application in the payer's mobile wallet.	Merchant-presented QR-code	SCA using an Authentication app (decoupled or app-to-app redirect) involving a fingerprint and authentication code using a dedicated key calculated by the Authentication app	The consumer has a separate authentication application on their mobile device that has been previously linked to the MSCT Inst application, which allows the calculation of an authentication code.
C2B-3	Mobile browser	PISP through the merchant virtual POI	The consumer can stay on the merchant website and authenticate /authorise	IBAN_merch	SCA using embedded authentication model with PISP –	The consumer is shopping on a merchant webpage which embeds an iFrame provided by the PISP, enabling



			the payment without redirection		involving CustomerID + passcode and OTP provided by payer's ASPSP.	authentication/authorisation of the payments without any re-direction.
C2B-4	Merchant (Transport) app + MSCT app	ASPSP + Transport Ticketing company	The merchant provides consumers with an app that redirects to the MSCT app for payment. The merchant app is used to purchase a transport ticket. Once the journey is confirmed, the consumer is redirected to the MSCT app to confirm the transaction.	IBAN_merch	In-app payment – SCA involving fingerprint and authentication code calculated using a dedicated key by the MSCT app	The MSCT app and the transport app have been previously linked. Once the consumer decides to pay, the two apps exchange the following data: IBAN_merch, transport company name and transaction amount.
C2B-5	MSCT app	MSCT service provider	Consumer selects the MSCT app that provides a QR-code with consumer-presented data scanned by the POI.	Consumer-presented QR-code with token	SCA involving a mobile code and authentication code calculated by MSCT app using a dedicated key	The merchant uses a payment request message to the MSCT service provider containing the consumer token and transaction data.



C2B-6	EMV contactless app	PISP through the merchant physical POI	Consumer device holds an contactless EMV app, consumer IBAN is transformed into PAN	Consumer PAN	SCA using embedded authentication model with PISP – involving fingerprint and cryptogram calculated by EMV contactless authentication app	Offline use case The merchant uses an EMV authentication request message (cryptogram) to the PISP which is transferred to the payer ASPSP.
C2B-7	MSCT app	PISP through the merchant physical POI	Consumer downloads MSCT app. MSCT app generates QR-code containing keying material that enables to establish a secure link with the POI via BLE	Consumer-presented QR-code containing a public key used to encrypt all other data exchanged with the POI	SCA using embedded authentication model with PISP – involving fingerprint and cryptogram calculated by MSCT app using a dedicated key	Offline use case The merchant uses a payment request message to the PISP containing the cryptogram calculated by the MSCT app which is transferred to the payer ASPSP.
C2B-8	MSCT app	MSCT service provider	Consumer downloads MSCT app and performs SCA via the MSCT app Consumer is reimbursed for part of	Consumer-presented QR-code with token	<i>Original payment:</i> SCA involving a fingerprint and authentication code calculated by MSCT app in the consumer’s mobile device using a dedicated key	The merchant uses a payment request message to the MSCT service provider containing the consumer token and transaction data



			the transaction amount and is notified in MSCT app		<p><i>Repayment:</i> SCA involving dedicated merchant code and authentication code calculated by merchant platform using a dedicated key</p>	
C2B-9	MSCT app + QR-code scanner + MSCT app on POI	MSCT service provider	Consumer selects a functionality made available by the MSCT app and scans a QR-code displayed by the POI. The QR-code contains merchant data and the amount. The payee has downloaded a specific application on the POI. ASPSPs need to be registered with the same MSCT Inst service provider.	Merchant-presented QR-code	SCA involving a mobile code and authentication code calculated by MSCT app using a dedicated key	The merchant POI can produce a dynamic QR-code containing all data necessary to request an SCT Inst payment.



C2B-10	Merchant app + PISP service	ASPSP + Merchant + PISP	<p>The merchant provides consumers with an app and consumers have enrolled with their account data. Consumer opens merchant app and navigates to purchase goods/services, then confirms and selects PISP payment solution. The consumer is redirected to the ASPSP mobile banking app to authenticate/authorise the transaction.</p>	Pre-registered consumer IBAN	SCA using redirection model with PISP involving CustomerID + passcode and dynamic authenticator provided by payer's ASPSP.	<p>The merchant app enables in app shopping. An SCT Inst instruction is forwarded to the consumer's ASPSP through the PISP. The user is redirected to their mobile banking app to authenticate/authorise the payment.</p>
C2B-11	MSCT app + Auth. app	MSCT service provider and Authentication service provider	<p>Consumer selects the MSCT app that provides a QR-code with consumer-presented data scanned by the POI. The consumer is re-directed to the authentication app for SCA.</p>	Consumer-presented QR-code with token	SCA using an Authentication app (decoupled app-to-app) involving a fingerprint and authentication code calculated by Authentication app using a dedicated key	<p>The merchant uses a payment request message to the MSCT service provider containing the consumer token and transaction data</p> <p>The MSCT app is linked to the authentication app on the consumer mobile device to provide the transaction data.</p>



C2B-12	Auth app	PISP and Authentication service provider	Consumer provides a QR-code stored on their mobile device and uses an Authentication app for the SCA	Consumer-presented QR-code with identification data “in clear”	SCA using decoupled model with PISP – involving fingerprint and authentication code calculated by Authentication app using a dedicated key	The merchant uses a payment request message to the PISP containing the consumer identification data and transaction data which is transferred to the payer ASPSP, which then triggers a decoupled SCA via the Authentication service provider.
C2B-13	Smartwatch with QR-code	PISP through the merchant physical POI	Consumer provides a QR-code stored on their smartwatch	Consumer-presented QR-code with identification data “in clear”	SCA using embedded authentication model with PISP – involving PIN and OTP provided by payer’s ASPSP.	The merchant uses a payment request message to the PISP containing the consumer identification data and transaction data which is transferred to the payer ASPSP. Authentication is done into PISP software on the merchant POI
C2B-14	MSCT app	MSCT service provider	Consumer downloads MSCT app and pre-downloads dynamic tokens in this app	Consumer-presented QR-code with token	SCA using Authentication involving facial recognition and pre-loaded dynamic token	The merchant uses a payment request message to the MSCT service provider containing the consumer token and transaction data.
C2B-15	MSCT app + Auth app	MSCT service provider + Authentication service provider	Consumer downloads MSCT app and Authentication app Consumer is re-directed to the	Consumer-presented QR-code with token	SCA using an Authentication app (decoupled app-to-app) involving a mobile code and authentication	The merchant uses a payment request message to the MSCT service provider containing the consumer token and transaction data



			Authentication app for SCA for the two transactions		code calculated by Authentication app using a dedicated key	The MSCT app is linked to the authentication app on the consumer mobile device to provide the transaction data.
B2B-1	eIPP app + MSCT app	ASPSP + MSCT provider + eIPP solution provider	The payee sends an e-invoice to their EIPP provider that forwards it to the payer's EIPP provider. The Request-to-Pay includes an e-invoice reference, transaction amount and IBAN_payee. The payer receives the Request-to-Pay in their EIPP app and clicks on the request. This opens the MSCT app that retrieves and displays the invoice information. The payer confirms the transaction.	IBAN_payee	SCA involving a fingerprint and authentication code calculated by MSCT app using a dedicated key	The payee and the payer use different eIPP solutions that are able to exchange information. The MSCT App is linked to the payer's eIPP App. Once the payer decides to pay, the two Apps exchange the following data: invoice reference, transaction amount, payee name and IBAN_payee.

Table 6: Main characteristics of MSCT use cases



7.3 MSCT use cases

7.3.1 MSCT use case P2P-1: Mobile device – Payment with a proxy – SCA using an MSCT application involving a mobile code

This use case presents an example of user experience whereby the payer uses an MSCT application on their mobile device to conduct an MSCT (Inst) from their own payment account to the payment account of a payee.

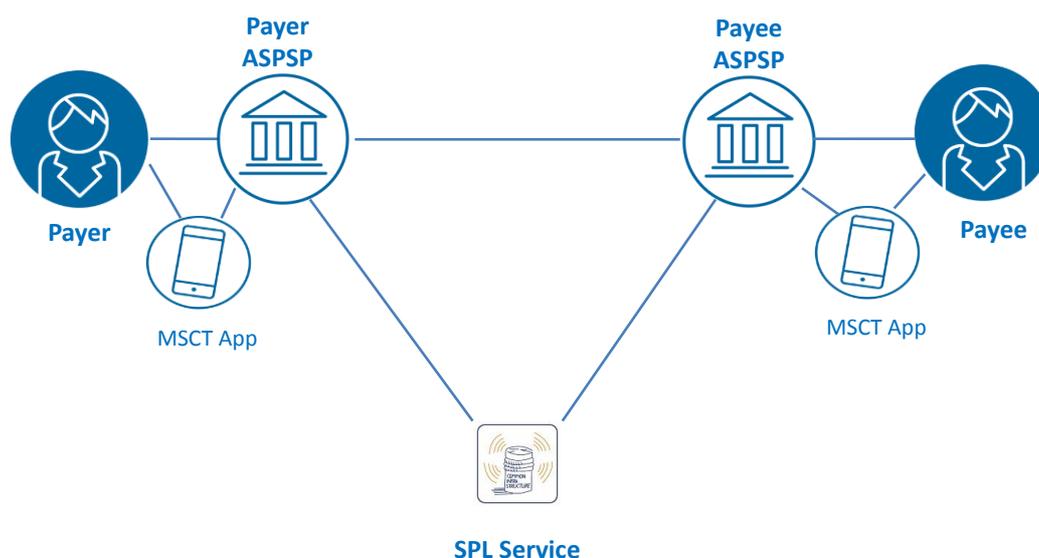


Figure 3: Actors in MSCT use case P2P-1

Payer and payee may, and frequently will, hold their payment accounts with different ASPSPs and have downloaded different MSCT (Inst) applications²⁰ (so-called mobile P2P applications) from their ASPSP on their mobile device.

A payee proxy (e.g., mobile phone number) will be in place, making the input of the payee details considerably more convenient for the payer. A strong customer authentication (see section 8.3) in accordance to PSD2 [5] is performed, involving the entry of a mobile code by the payer (see section 8.2) and the calculation of an authentication code using a dedicated key by the MSCT application on the payer's mobile device.

In view of the usage of a proxy, the so-called SEPA Proxy Lookup (SPL) Service is used to link the payee's proxy as to their account details. For more information on the SPL service, the reader is referred to section 15.3.

²⁰ The MSCT application may also be downloaded from an MSCT service provider. The payer and payee may have different MSCT service providers.



MSCT use case P2P-1 Mobile device – Proxy - SCA using MSCT app and mobile code

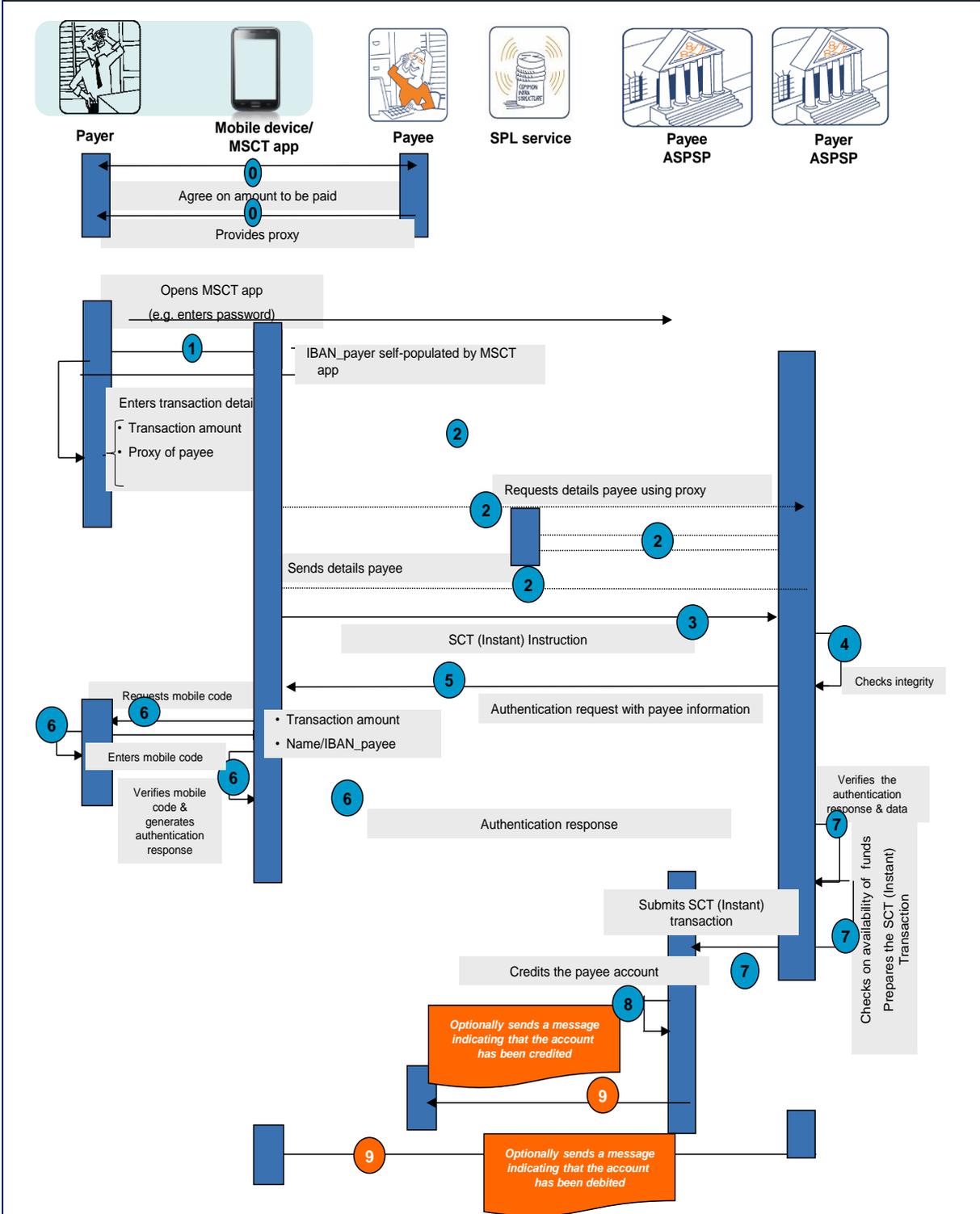


Figure 4: MSCT use case P2P-1



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, the payer would need to be subscribed to the MSCT service and have downloaded a dedicated MSCT (Inst) application²¹ from their ASPSP on their mobile device. This MSCT application is typically linked to a specific payer account.
- The payee also needs to be subscribed to the MSCT service and have downloaded a dedicated MSCT (Inst) application from their ASPSP on their mobile device.
- The payer and the payee agree upon the amount to be paid to the payee. The payee provides their proxy (e.g., mobile phone number) to the payer, if not previously known to the payer.
- The payer's ASPSP and payee's ASPSP are (directly or indirectly) participants in the SPL Service.
- During the payment transaction, a mobile internet connection is required.

Step 1

The payer selects and opens the MSCT (Inst) application on their mobile device, which possibly involves the entry of a password.

Step 2

- Once the MSCT (Inst) application is selected, the IBAN_payer is self-populated.
- The payer enters the details of the transaction via their mobile device:
 - The transaction amount,
 - The payee's proxy (e.g., mobile phone number); this information may be manually entered by the payer on the mobile device or selected e.g., via the mobile device address book in case of a pre-registered payee.
- The MSCT (Inst) application uses the SPL service to retrieve the payee account data based on the payee's mobile phone number received.

Step 3

The SCT (Inst) instruction including the payee name, the IBAN_payee and the transaction amount, is transmitted to the payer's ASPSP.

Step 4

The payer's ASPSP checks the integrity of the SCT (Inst) instruction.

Step 5

Subsequently, the payer's ASPSP sends an authentication request, including the payee's name/IBAN_payee, transaction amount and a challenge, to the MSCT (Inst) application on the mobile device of the payer.

²¹ Typically a mobile P2P application.



Step 6

- The authentication request is handled automatically by the MSCT (Inst) application on the payer's mobile device.
- The payee's name/IBAN_payee and the transaction amount are displayed on the mobile device.
- The payer is requested to enter their mobile code on the mobile device to authenticate and to confirm the transaction.
- Upon successful verification of the mobile code by the MSCT (Inst) application, it calculates an authentication code which is transmitted to the payer's ASPSP.

Step 7

- The payer's ASPSP verifies the authentication code.
- The payer's ASPSP checks the availability of funds on the payer's account,
- The payer's ASPSP prepares and submits the SCT (Inst) transaction to the payee's ASPSP.

Step 8

- In case of an SCT Inst, a confirmation message is returned from the payee's ASPSP to the payer's ASPSP (not shown on the figure).
- The payee's ASPSP makes the funds available to the payee.

Step 9

- The payee is optionally notified by their ASPSP that their account has been credited through their MSCT application.
- The payer is optionally notified by their ASPSP that their account has been debited through their MSCT application.

Analysis MSCT Use case P2P-1	
Interoperability	<ul style="list-style-type: none"> • The payer and payee may have different ASPSPs and different MSCT applications. • The SPL service is needed and both the payer's ASPSP and payee's ASPSP need to be participants in the SPL service (directly or indirectly).
Challenges	<ul style="list-style-type: none"> • How to handle the cases where the payee's account data could not be retrieved from the SPL service because the payee's ASPSP is not registered in the SPL service. • The notification messages in step 9 are not included in the SCT Inst and SCT schemes. • In case of an SCT there is no immediate, irrevocable crediting of the funds. How to inform the payee that the payment has been initiated (after step 8) if we do not have an SCT Inst?

Table 7: Analysis MSCT use case P2P-1



Notes:

- The acknowledgement to the payer about the receipt of the MSCT instruction based on SCT is addressed in Chapter 17 and Annex 4.
- The minimum data elements in the notification messages are defined in Annex 4.

7.3.2 MSCT use case P2P-2: Mobile device – Payment request with a proxy via messaging application – SCA using MSCT application involving a fingerprint

This use case presents an example of user experience whereby a bill for a lunch is split amongst friends by the payee (who previously paid the bill). The friends are invited through a payment request via a messaging application to pay with an MSCT Inst using different MSCT services.

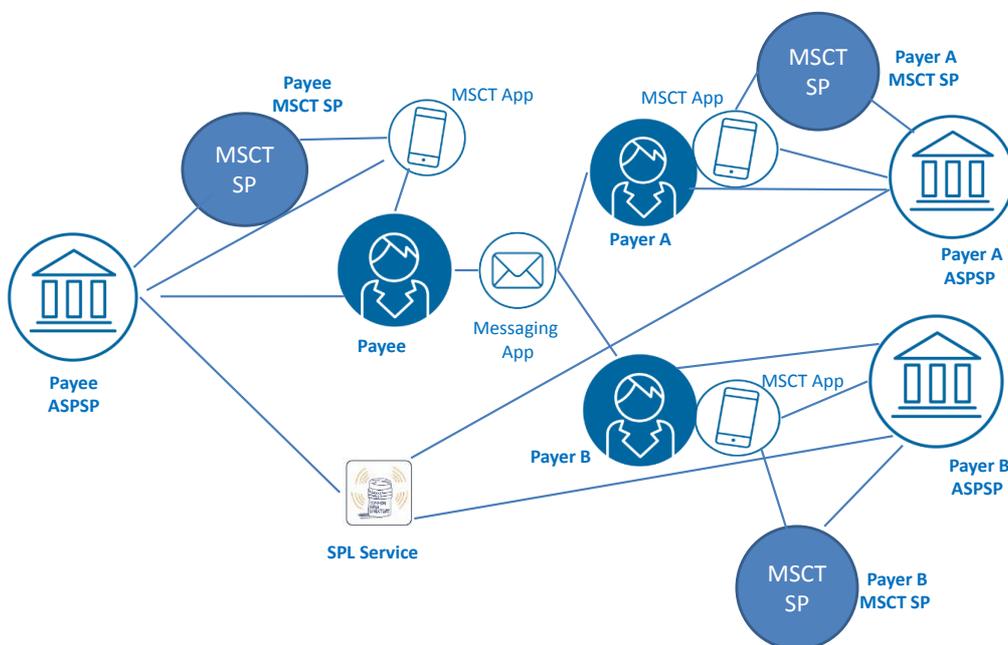


Figure 5: Actors in MSCT use case P2P-2

Payers and payee may, and frequently will, hold their payment accounts with different ASPSPs and have downloaded different MSCT Inst applications from potentially different MSCT service providers. Each ASPSP is a participant in an MSCT service (not necessarily the same). A strong customer authentication (see section 8.3) in accordance with PSD2 [5] is performed, involving the presentation of a fingerprint by the payer (see section 8.2) and the calculation of an authentication code using a dedicated key by the MSCT application on the payer’s mobile device.

In case the MSCT Inst application is provided to the payer by an MSCT service provider instead of the payer’s ASPSP, an agreement is needed between the payer’s ASPSP and the MSCT service provider concerning the MSCT application.



Note that in the figure below for simplification, both payer and payee have the same MSCT service provider.

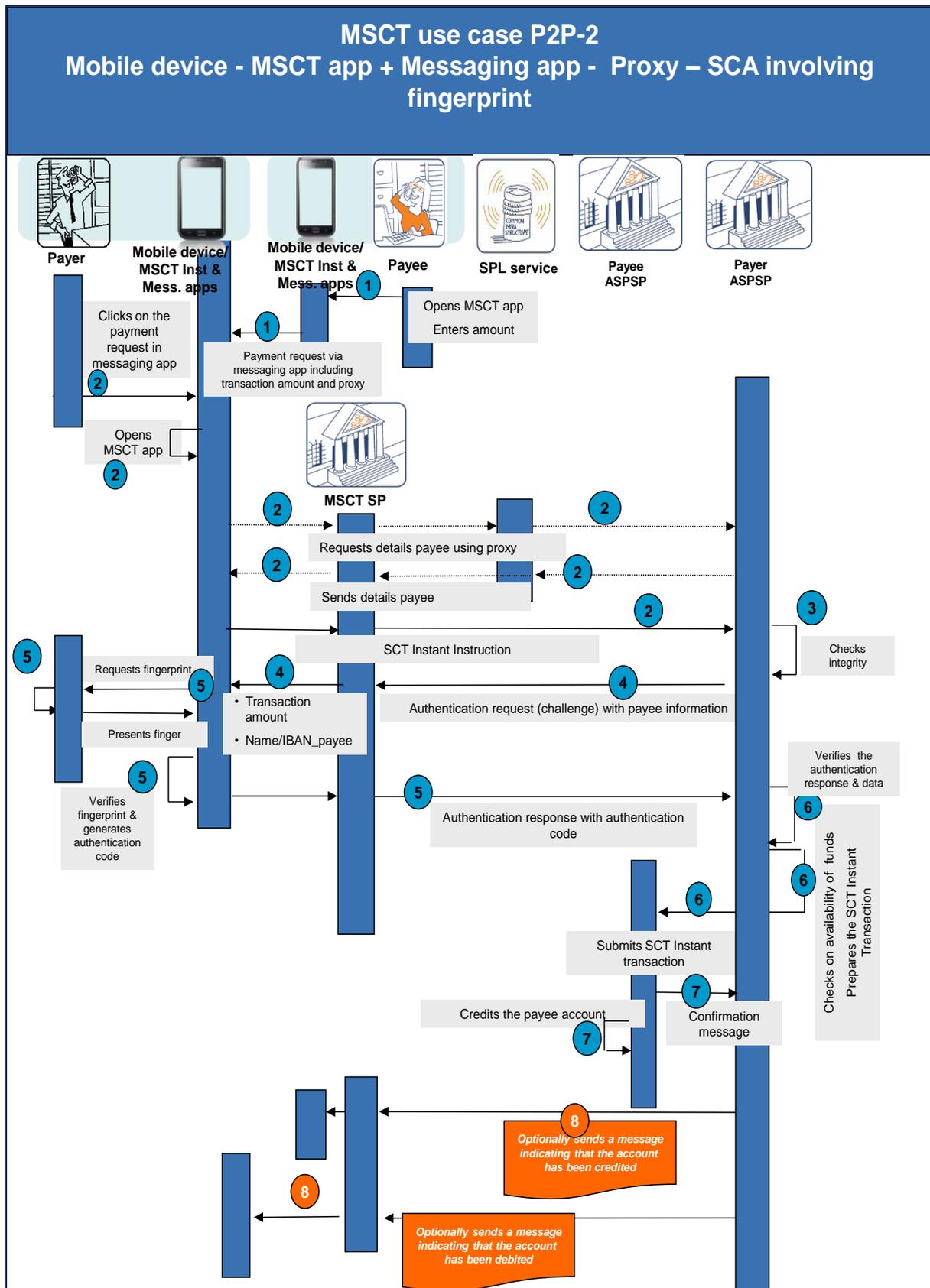


Figure 6: MSCT use case P2P-2



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, all payers and the payee would need to be subscribed to an MSCT Inst service and have downloaded a dedicated MSCT Inst application from their MSCT service provider on their mobile device.
- All payers and the payee need to be subscribed to the same messaging service provider and have downloaded the dedicated messaging application on their mobile device. Moreover, this messaging service should be supported by all MSCT Inst applications.
- The ASPSPs of the payers and the payee are participants in the respective chosen MSCT Inst services and are participants in the SPL service.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The payee opens their MSCT Inst application on their mobile device and enters the amount to be paid, the split of the amount and a personal message.
- The payee shares the payment request(s) via a messaging application and selects the payer(s) in the address book of the messaging application. The payment request only contains the amount, the personal message and the mobile phone number of the payee.²²
- The payee can check in their MSCT Inst application the payment request(s) sent.

Step 2

- Each payer receives the payment request in their messaging application and clicks on this request.
- This automatically opens the MSCT Inst application of their MSCT service provider. (The selection of the ASPSP has already been done during the registration process).
- The MSCT Inst application uses the SPL service to retrieve the payee account data based on the payee's mobile phone number received.
- The SCT Inst instruction including the payee name, the IBAN_payee and the transaction amount, is transmitted to the payer's ASPSP via the MSCT service provider.

Step 3

The payer's ASPSP checks the integrity of the SCT Inst instruction.

²² Note that no payment data will be sent due to low security level of the messaging application.



Step 4

Subsequently, the payer's ASPSP sends an authentication request including the payee's name/IBAN_payee, the transaction amount and a challenge to the MSCT Inst application in the mobile device of the payer via the MSCT service provider.

Step 5

- The authentication request is handled automatically by the MSCT (Inst) application on the payer's mobile device.
- The payee's name/IBAN_payee and the transaction amount are displayed on the mobile device.
- The payer is requested to present a fingerprint to their mobile device to authenticate and to confirm the transaction.
- Upon successful fingerprint verification by the mobile device, the MSCT Inst application calculates an authentication code which is transmitted to the payer's ASPSP via the MSCT service provider.

Step 6

- The payer's ASPSP verifies the authentication code.
- The payer's ASPSP checks the availability of funds on the payer's account.
- The payer's ASPSP prepares and submits the SCT Inst transaction to the payee's ASPSP.

Step 7

- A confirmation message is returned from the payee's ASPSP to the payer's ASPSP.
- The payee's ASPSP makes the funds available to the payee.

Step 8

- The payee is optionally notified by their MSCT service provider (information provided by the payee's ASPSP) that their account has been credited.
- The payer is optionally notified by their MSCT service provider that their account has been debited (information provided by the payer's ASPSP).

Note: This use case is also valid for an SCT.



Analysis MSCT Use case P2P-2	
Interoperability	<ul style="list-style-type: none"> • All payers and the payee have to be subscribed to the same messaging service provider and use the same messaging application. • All payers and the payee may have different ASPSPs. • All payers and the payee may have different MSCT service providers and different MSCT applications. • The SPL service is needed and all payer ASPSPs and the payee's ASPSP need to be participants in the SPL service (directly or indirectly).
Challenges	<ul style="list-style-type: none"> • How to handle the cases where the payee's account data could not be retrieved from the SPL service because the payee's ASPSP is not registered in the SPL network. • Standard for the interface between the messaging application and the MSCT services providers. • The notification messages in step 8 are not included in the SCT Inst and SCT schemes. • In case of an SCT there is no immediate, irrevocable crediting of the funds. How to inform the payee that the payment has been initiated (after step 6)?

Table 8: Analysis MSCT use case P2P-2

Notes:

- The interoperability in case different MSCT service providers are involved is discussed in Chapter 16 and 18.
- The acknowledgement to the payer about the receipt of the MSCT instruction based on SCT is addressed in Chapter 17 and Annex 4.
- The minimum data elements in the notification messages are defined in Annex 4.



7.3.3 MSCT use case C2B-1: Mobile device - Payment of invoice with merchant-presented QR-code – SCA involving a mobile code

This use case presents an example of consumer experience whereby their mobile device is used to pay an invoice using an MSCT (Inst) from their own payment account to the payment account of a merchant (payee). Hereby a dedicated MSCT (Inst) application on the consumer's mobile device is used, provided by their ASPSP²³.

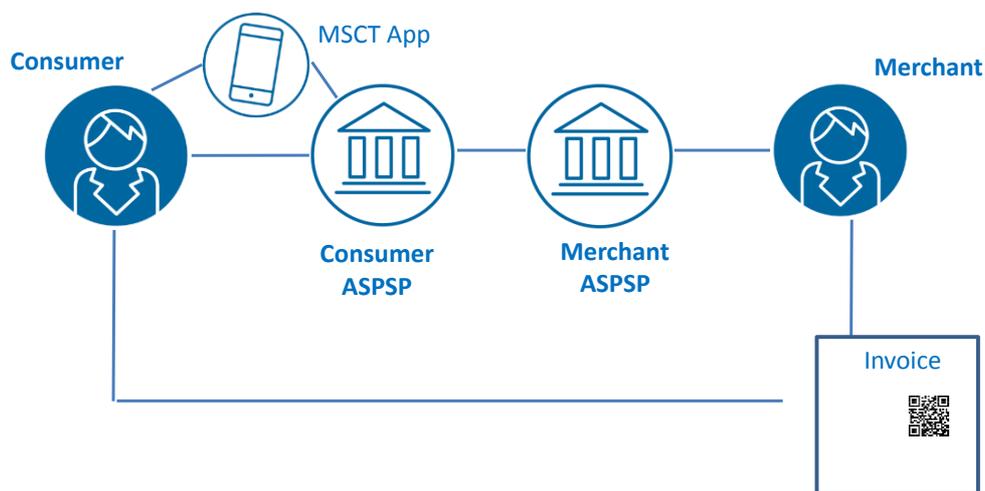


Figure 7: Actors in MSCT use case C2B-1

Furthermore, a merchant-presented QR-code on the invoice will be in place, making the input of the merchant details considerably more convenient for the consumer.

In this payment transaction, a strong payer authentication (see section 8.3) in accordance with PSD2 [5] is performed involving a mobile code (see section 8.2) and the calculation of an authentication code using a dedicated key by the MSCT application.

²³ The MSCT application may also be downloaded from an MSCT service provider.

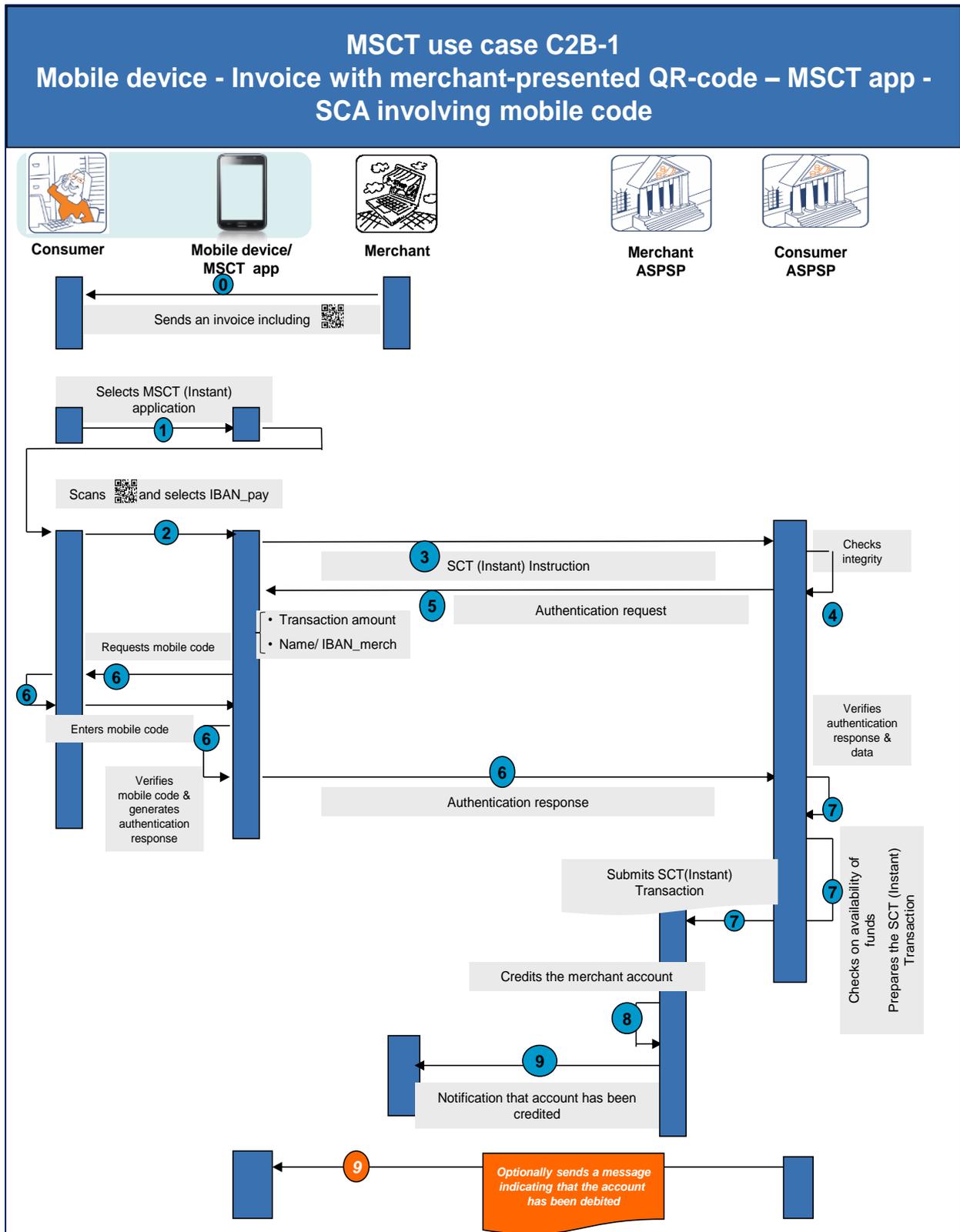


Figure 8: MSCT use case C2B-1



In the figure above, the following steps are illustrated:

Step 0

- As a pre-requisite, the merchant sends an invoice to the consumer containing a QR-code (which includes the merchant name, the transaction amount, invoice number and the IBAN_merch).
- The consumer has registered for the MSCT (Inst) service with their ASPSP and has downloaded a dedicated MSCT (Inst) application on their mobile device.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The consumer selects and opens the MSCT (Inst) application on their mobile device which possibly involves the entry of a password.
- The consumer scans the QR-code from the merchant invoice.

Step 2

- The consumer may select the IBAN_payer they want to use in case there are several eligible payment accounts.
- The transaction amount, the merchant name and IBAN_merch are automatically retrieved from the QR-code and displayed to the consumer.
- An SCT (Inst) instruction is generated by the MSCT (Inst) application.

Step 3

The SCT (Inst) instruction is transmitted to the consumer's ASPSP.

Step 4

The consumer's ASPSP checks the integrity of the SCT (Inst) instruction.

Step 5

Subsequently, the consumer's ASPSP sends an authentication request including the payee's name/IBAN_merch, the transaction amount and a challenge to the MSCT (Inst) application on the mobile device of the payer.

Step 6

- The authentication request is handled automatically by the MSCT (Inst) application on the consumer's mobile device.
- The payee's name/IBAN_merch and the transaction amount are displayed on the mobile device.
- The consumer is requested to enter their mobile code on the mobile device to authenticate and to confirm the transaction.
- Upon successful mobile code verification by the MSCT (Inst) application on mobile device, it calculates an authentication code which is transmitted to the consumer's ASPSP.



Step 7

- The consumer's ASPSP verifies the authentication code.
- The consumer's ASPSP checks the availability of funds on the payer's account,
- The consumer's ASPSP prepares and submits the SCT (Inst) transaction to the payee's ASPSP.

Step 8

- In case of an SCT Inst, a confirmation message is returned from the merchant's ASPSP to the consumer's ASPSP (not shown on the figure).
- The merchant's ASPSP makes the funds available to the merchant.

Step 9

- The merchant is notified by their ASPSP that their account has been credited.
- The consumer is optionally notified by their ASPSP that their account has been debited.

Analysis MSCT Use case C2B-1	
Interoperability	<ul style="list-style-type: none"> • The consumer and the merchant may have different ASPSPs and MSCT (Inst) applications.
Challenges	<ul style="list-style-type: none"> • Standardisation of a "QR-code", ensuring the correct payee name/IBAN_merch link. • Integrity of the QR-code. • The notification messages in step 9 are not included in the SCT Inst and SCT schemes.

Table 9: Analysis MSCT use case C2B-1

Notes:

- The payee-presented QR-codes are specified in Chapter 17.
- The security of QR-codes is addressed in Chapter 10.

The minimum data elements for the notification messages are defined in Annex 4.



7.3.4 MSCT use case C2B-2: Mobile device – Payment at POI with merchant-presented QR-code – SCA using a dedicated authentication application (decoupled app-to-app) involving a fingerprint

This use case presents an example of consumer experience whereby their mobile device is used to pay in-store by reading a merchant-presented QR-code on the POI. Hereby a dedicated MSCT Inst application on the mobile device of the consumer is used that they have downloaded from an MSCT service provider into their mobile wallet.

The consumer authentication is performed through a dedicated Authentication application²⁴ in the consumer’s mobile wallet²⁵.

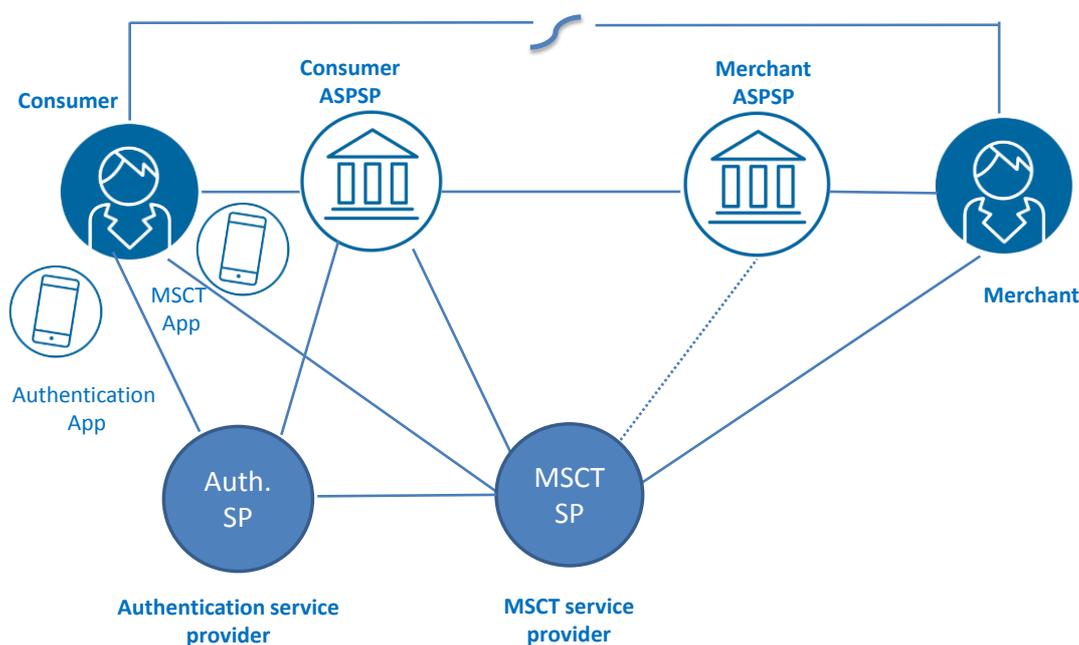


Figure 9: Actors in MSCT use case C2B-2

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. Both ASPSPs are participants in the same MSCT Inst service²⁶. Also, the merchant needs to be subscribed to the MSCT Inst service and have downloaded dedicated software on their POI.

In this payment transaction a strong customer authentication (see section 8.3) in accordance to PSD2 [5] is performed involving a fingerprint (see section 8.2) and the calculation of an authentication code using a dedicated key by the Authentication application.

²⁴ An application accessed through the mobile device performing the functions related to a user authentication, as dictated by the Authentication service provider.

²⁵ In this case there is a delegated authentication from the payer’s ASPSP to the Authentication service provider. Also, an agreement between the payer’s ASPSP and the Authentication service provider is required.

²⁶ This refers to the current MSCT solutions in the market.

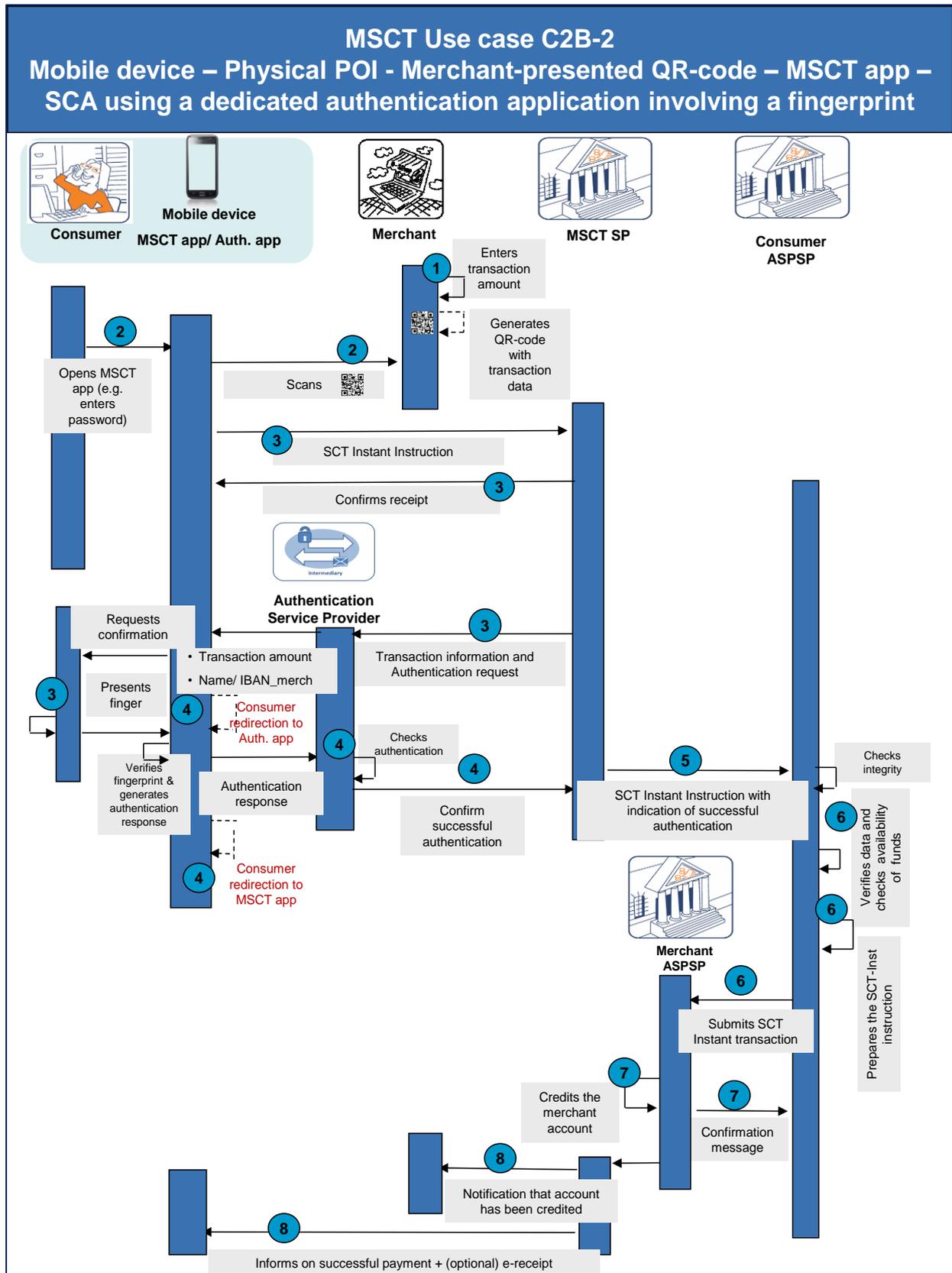


Figure 10: MSCT use case C2B-2

In the figure above, the following steps are illustrated:



Step 0

- As a prerequisite, the consumer would need to first subscribe to the MSCT Inst service and download a dedicated MSCT Inst application from the MSCT Inst service provider on their mobile device. Furthermore, they have a separate Authentication application from an Authentication service provider on their mobile device that has been previously linked to the MSCT Inst application.
- The consumer's ASPSP relies on the Authentication service provider for the consumer authentication.
- The merchant also needs to be subscribed to the MSCT Inst service, e.g., through their ASPSP or the MSCT Inst service provider directly.
- The MSCT Inst service provider is linked to both ASPSPs.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The merchant enters the transaction amount on the POI.
- The transaction amount is displayed on the merchant's POI with a QR-code, which includes the merchant's name, IBAN_merch, merchant transaction identifier and the transaction amount.

Step 2

- The consumer selects and opens the MSCT Inst application on their mobile device which possibly involves the entry of a password.
- A message is displayed on the mobile device inviting the consumer to scan the QR-code from the POI.

Step 3

- The MSCT Inst application retrieves the merchant name, IBAN_merch, merchant transaction identifier and the transaction amount from the QR-code and sends an SCT Inst instruction to the MSCT Inst service provider.
- The consumer is informed about the receipt of the MSCT Inst instruction by the MSCT Inst provider.
- The consumer is invited to confirm the transaction and is redirected to their Authentication application which displays the merchant name/IBAN_merch and the transaction amount.
- The consumer authenticates and confirms the transaction by presenting their finger to the mobile device.



Step 4

- Upon successful fingerprint verification by the mobile device, the dedicated Authentication app will calculate an authentication code²⁷ which is transmitted in the authentication response to the Authentication service provider.
- The Authentication service provider checks the authentication response.
- The MSCT Inst service provider is informed by the Authentication service provider about the successful authentication.
- The consumer is redirected to the MSCT Inst application.

Step 5

The SCT Inst instruction including the including the merchant's name, IBAN_merch, the transaction amount and the merchant transaction identifier with a flag indicating the successful authentication are transmitted from the MSCT service provider to the consumer's ASPSP.

Step 6

- The consumer's ASPSP checks the integrity of the SCT Inst instruction.
- The consumer's ASPSP checks the availability of funds on the consumer's account.
- The consumer's ASPSP prepares and submits the SCT Inst transaction to the merchant's ASPSP.

Step 7

- A confirmation message is returned from the merchant's ASPSP to the consumer's ASPSP.
- The merchant's ASPSP makes the funds available to the merchant.

Step 8

- The merchant is notified by the MSCT service provider (information provided by the consumer's ASPSP) that the transaction was successfully executed.
- The consumer is notified by the MSCT service provider that the transaction has been successfully executed (information provided by the consumer's ASPSP) and may optionally receive an e-receipt.

²⁷ Or alternatively a cryptogram or digital signature.



Analysis MSCT Use case C2B-2	
Interoperability	<ul style="list-style-type: none"> • The consumer and the merchant need to be subscribed to the same MSCT service. • The consumer’s ASPSP and the merchant’s ASPSP need be linked to the same MSCT service. If the MSCT service provider is a PISP, the link between the PISP and the merchant’s ASPSP is not needed. • For a truly “open” approach and a SEPA-wide interoperability, if the MSCT service provider of the payer is different to the MSCT service provider of the merchant, a framework needs to be specified that interconnects the different MSCT service providers.
Challenges	<ul style="list-style-type: none"> • Standardisation of messages including data elements between MSCT service provider back-ends • Standardisation of a “QR-code”, ensuring the correct payee name/IBAN_merch link. • Integrity of the QR-code. • How is the transaction reconciled with the purchase (e.g., transaction identifier)? • The notification messages in step 8 are not included in the SCT Inst scheme.

Table 10: Analysis MSCT use case C2B-2

Notes:

- The standardisation of the payee-presented QR-code is addressed in Chapter 17.
- The security of QR-codes is addressed in Chapter 10.
- The interoperability of MSCTs based on payee-presented data whereby different MSCT service providers are involved for the consumer and merchant is addressed in Chapter 17.
- The minimum data elements in the notification messages are defined in Annex 4.



7.3.5 MSCT use case C2B-3: Mobile device – m-commerce – mobile browser – PISP with embedded SCA involving a dynamic authenticator

This use case presents an example of consumer (payer) experience whereby they use their mobile device to pay for goods or services they purchased via a webshop (m-commerce). Hereby an SCT Inst is used from the consumer's payment account to the payment account of the merchant (payee) which is initiated using a mobile browser.

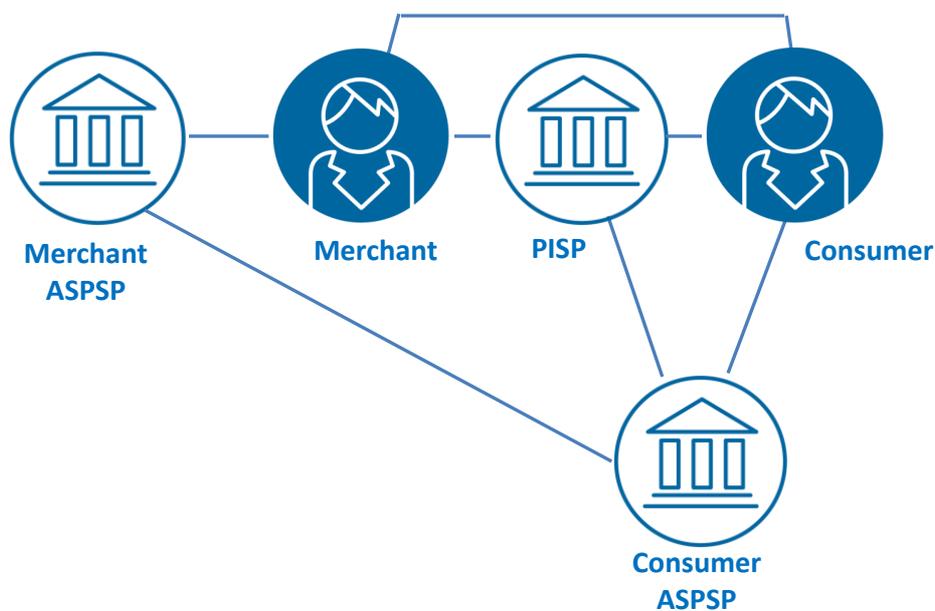


Figure 11: Actors in MSCT use case C2B-3

Consumer and merchant may, and frequently will, hold their payment accounts with different ASPSPs.

Furthermore, a strong customer authentication (see section 8.3) involving a passcode and dynamic authenticator (e.g. an OTP - see section 8.2) is performed in accordance with PSD2 [5] via a PISP i-frame on the merchant's website (embedded model).

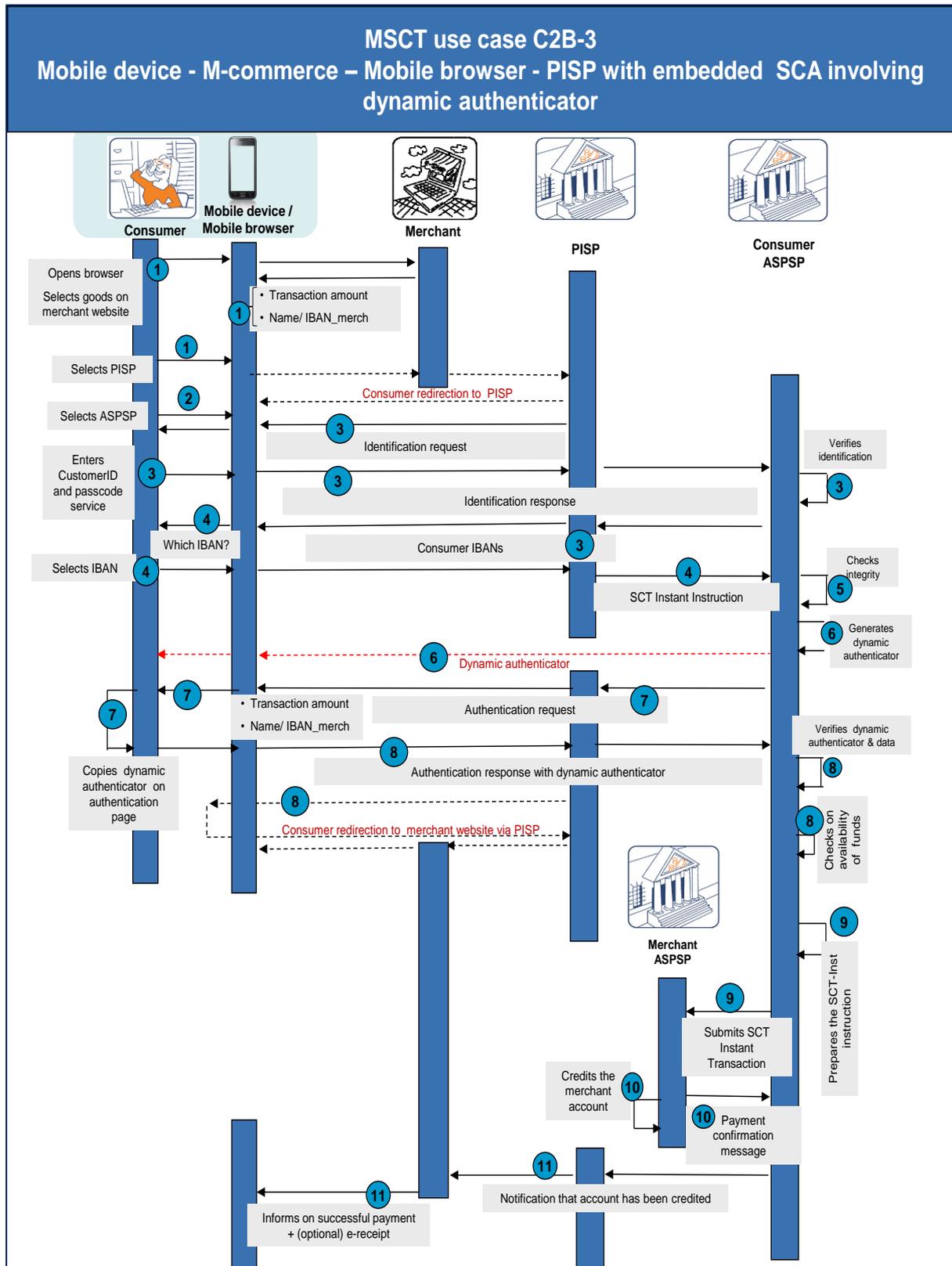


Figure 12: MSCT use case C2B-3



In the figure above, the following steps are illustrated:

Step 0

- The merchant needs to be registered with a PISP.
- The PISP has access to the PSD2 account interface of the consumer's ASPSP.
- The consumer is registered with their ASPSP for the online banking service.
- As a prerequisite, a mobile internet connection is required during the purchase.

Step 1

- The consumer navigates using the browser of their mobile device to a merchant's website and selects the goods or services they want to buy. After having accepted the general purchase conditions, they are invited to confirm the purchase.
- The checkout section of the merchant website displays the transaction details including the merchant name, the transaction amount and the payment options to the consumer.
- The consumer selects their preferred PISP payment solution in this checkout section.

Step 2

The consumer is invited to select their preferred ASPSP on the PISP's iframe on the merchant's website for this transaction.

Step 3

- The consumer is invited to enter their CustomerID and passcode in accordance with the security policy of their ASPSP.
- The consumer identification data is transmitted through the PISP to the consumer's ASPSP.
- After successful identification of the consumer by the ASPSP, the different consumer IBANs are provided to the PISP²⁸.

Step 4

- The consumer is invited to select the IBAN they want to use for this purchase on the PISP's iframe.
- An SCT Inst instruction including the transaction amount, the merchant's name and IBAN_merch are forwarded by the PISP to the consumer's ASPSP.

Step 5

The consumer's ASPSP checks the integrity of the SCT Inst instruction.

²⁸ Note that this functionality may require an AISP license for the PISP.



Step 6

The consumer's ASPSP transmits a dynamic authenticator (e.g., an OTP linked to the transaction amount and merchant - see section 8.3) to the consumer.

Step 7

The consumer is subsequently requested to copy this dynamic authenticator into a dedicated field on the PISP's iframe on the merchant's website.

Step 8

- The PISP transmits the dynamic authenticator to the consumer's ASPSP.
- The consumer's ASPSP verifies the dynamic authenticator.

Step 9

- The consumer's ASPSP checks the availability of funds on the consumer's account.
- The consumer's ASPSP prepares and submits the SCT Inst transaction to the merchant's ASPSP.

Step 10

- A confirmation message is returned from the merchant's ASPSP to the consumer's ASPSP.
- The merchant's ASPSP makes the funds available to the merchant.

Step 11

- The merchant is notified by the PISP (information provided by the consumer's ASPSP) that their account has been credited.
- The consumer is informed by the merchant that the payment has been successfully executed and may optionally receive an e-receipt.

Note: If an SCA is not requested by the ASPSP (see section 8.3), steps 6 through 8 may be omitted.

Analysis MSCT Use case C2B-3	
Interoperability	<ul style="list-style-type: none"> • The merchant needs to have a contractual relationship with the PISP. • Interoperable due to the underlying SCT Inst scheme.
Challenges	<ul style="list-style-type: none"> • PISP needs to connect to # ASPSPs. • In view of the lack of an MSCT app and pre-onboarding, the consumer identification / authentication process involves more consumer interactions. • From a consumer experience, they may have to enter credentials in "new" environments.



	<ul style="list-style-type: none">• The notification messages in Step 11 are not included in the SCT Inst scheme.• The ASPSP's API needs to make the consumer IBANs available to the PISPs – this issue may require an AISP license for the PISP.• Consumer consent with respect to usage of the PISP subject to EBA clarifications ((PSD 2 Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30))²⁹.
--	---

Table 11: Analysis MSCT use case C2B-3

Notes:

- The interoperability of MSCTs involving a PISP is analysed in Chapter 20.
- The minimum data elements in the notification messages are defined in Annex 4.

²⁹ Subject to clarification by EBA on questions EBA Q&A 2020_5570 and 2020_5573.



7.3.6 MSCT use case C2B-4: Mobile device – transport ticketing – in-app payment - SCA involving fingerprint

This use case presents an example of consumer experience whereby their mobile device is used to pay for a transport ticket purchased via a dedicated transport application stored in a mobile wallet on their mobile device. Furthermore they have downloaded an MSCT application from their ASPSP in their wallet that has been previously linked to the transport application.

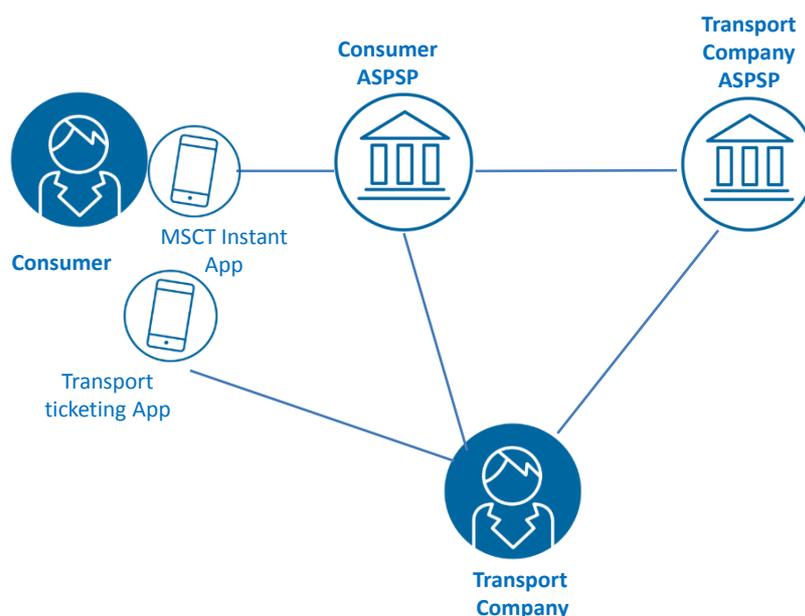


Figure 13: Actors in MSCT use case C2B-4

Consumer and merchant (transport service) may, and frequently will, hold their payment accounts with different ASPSPs.

In this payment transaction a strong customer authentication (see section 8.3) in accordance to PSD2 [5] is performed involving a fingerprint (see section 8.2) and the calculation of an authentication code by the MSCT application.

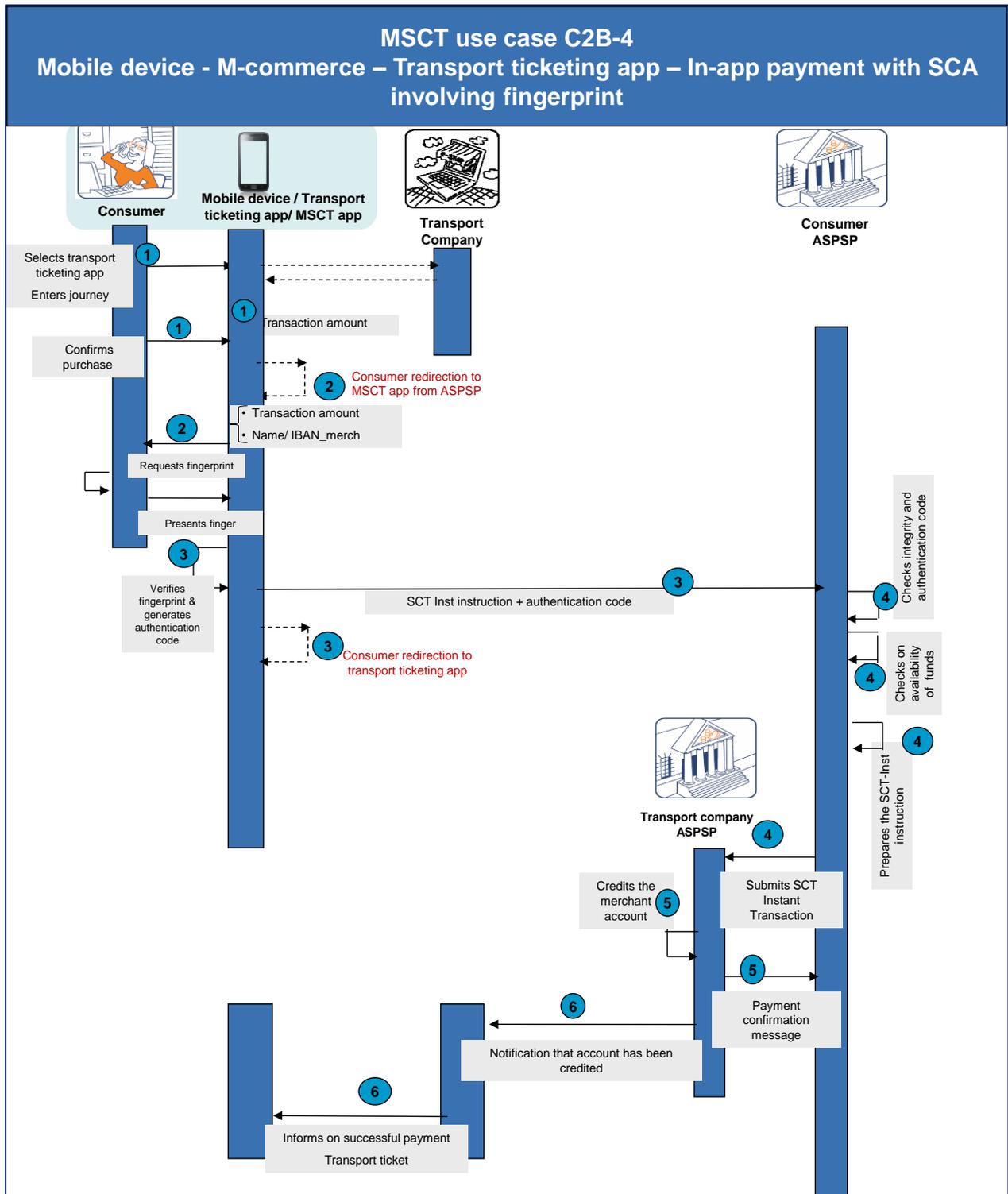


Figure 14: MSCT use case C2B-4



In the figure above, the following steps are illustrated:

Step 0 (Pre-requisite)

- The consumer has downloaded an MSCT Inst application provided by their ASPSP and linked to a specific consumer account on their mobile device.
- The consumer has also downloaded a transport ticketing application on their mobile device that has been previously linked to the MSCT Inst application.
- As a prerequisite, a mobile internet connection is required during the purchase.

Step 1

- The consumer selects a transport ticketing application on their mobile device to buy a ticket.
- The consumer enters their journey and the ticketing application displays the transaction amount with an invitation to confirm and pay the journey.
- Upon confirmation by the consumer via the mobile device, the consumer is redirected to their MSCT Inst application that automatically opens and is provided with the transport company name, IBAN_merch and the transaction amount.

Step 2

- The merchant (the transport company) name/IBAN_merch and the transaction amount are displayed by the MSCT Inst application.
- The consumer authenticates and confirms the transaction by presenting their finger to the mobile device.

Step 3

- Upon successful verification of the fingerprint by the mobile device, the MSCT Inst application calculates an authentication code.
- The SCT Inst instruction and the authentication code are transmitted to the consumer's ASPSP.
- The consumer is redirected to the transport ticketing application.

Step 4

- The consumer's ASPSP checks the authentication code and the integrity of the SCT Inst instruction.
- The consumer's ASPSP checks the availability of funds on the consumer's account.
- The consumer's ASPSP prepares and submits the SCT Inst transaction to the transport company's ASPSP.



Step 5

- A confirmation message is returned from the transport company’s ASPSP to the consumer’s ASPSP.
- The merchant’s ASPSP makes the funds available to the merchant.

Step 6

- The transport company is notified their ASPSP about the successful SCT Inst payment.
- The consumer is notified about the successful transaction and receives the electronic transport ticket from the transport company they can store in their mobile wallet.

Analysis MSCT Use case C2B-4	
Interoperability	<ul style="list-style-type: none"> • The transport company needs to be linked with the consumer’s ASPSP. • The MSCT application needs to be linked to the transport ticketing application.
Challenges	<ul style="list-style-type: none"> • The notification messages in step 6 are not included in the SCT Inst scheme.

Table 12: Analysis MSCT use case C2B-4

Note: The minimum data elements in the notification messages are specified in Annex 4.



7.3.7 MSCT use case C2B-5: Mobile device - Payment at a physical POI with consumer-presented QR-code - SCA using an MSCT application involving a mobile code

This use case presents an example of consumer experience whereby their mobile device is used to pay in-store by presenting a consumer-presented QR-code to the POI. Hereby a dedicated MSCT Inst application on the mobile device of the consumer is used that they have downloaded from an MSCT service provider into their mobile wallet.

The consumer authentication is performed through the MSCT application in the consumer's mobile wallet.

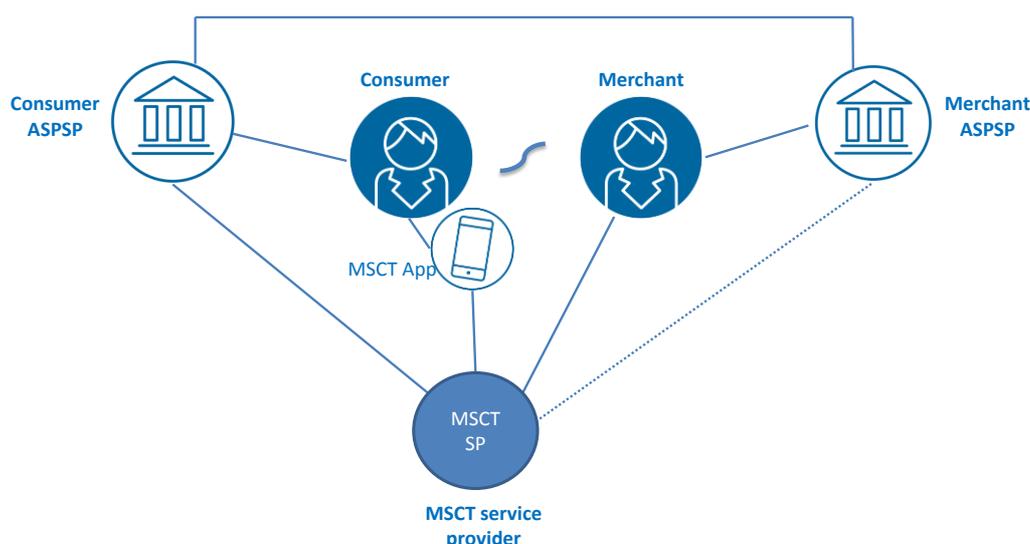


Figure 15: Actors in MSCT Use case C2B-5

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. Both ASPSPs are participants in the same MSCT Inst Service³⁰.

Also, the merchant needs to be subscribed to the MSCT Inst service and have downloaded dedicated software on their POI.

In this payment transaction a strong customer authentication (see section 8.3) in accordance with the relevant PSD2 [5] requirements is performed involving a mobile code³¹ (see section 8.2) and the calculation of an authentication code using a dedicated key by the MSCT application. Note that hereby an agreement is needed between the MSCT service provider and the consumer's ASPSP concerning the MSCT application.

³⁰ This refers to the current MSCT solutions in the market.

³¹ Note that also PSU verification methods may be used.

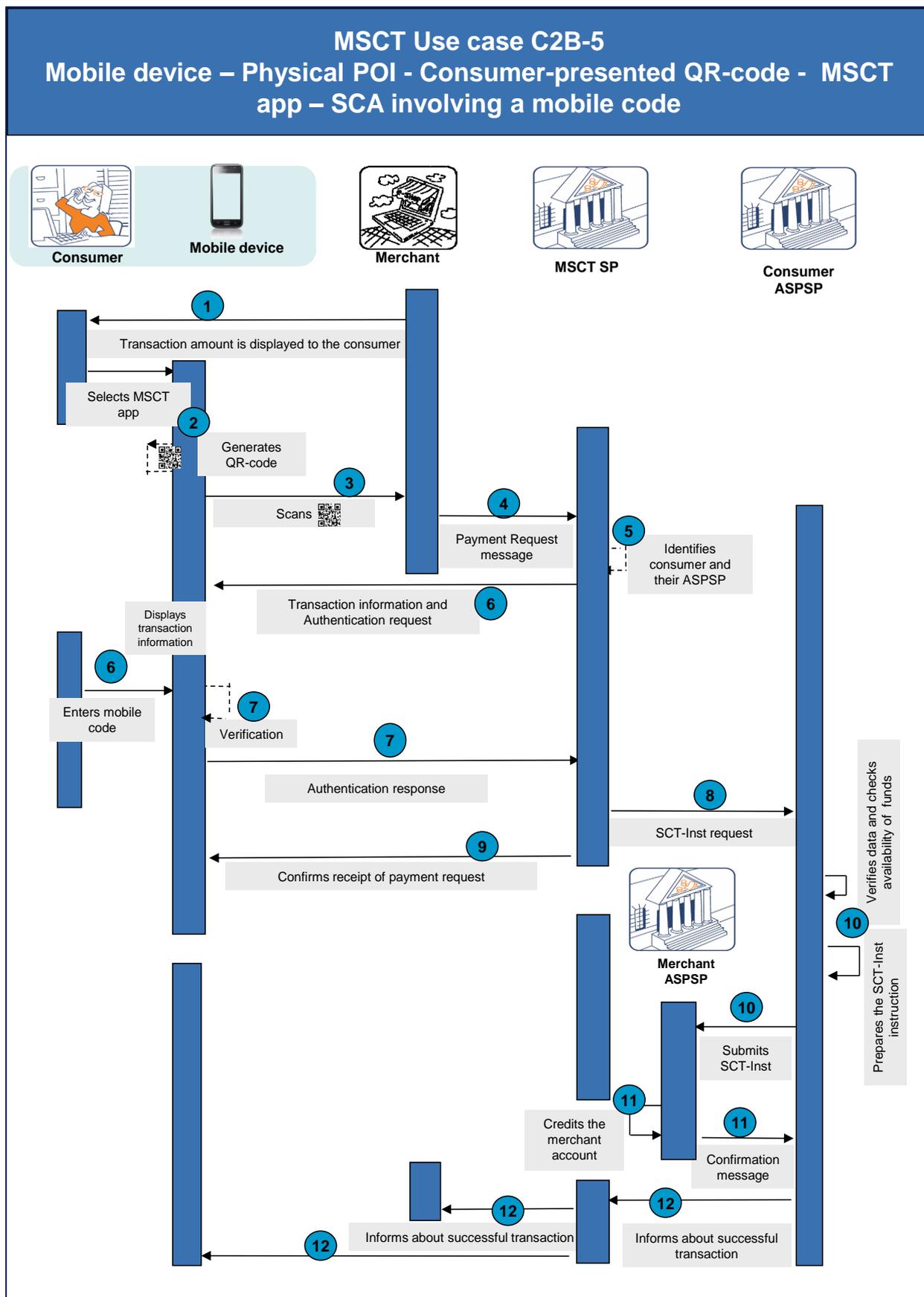


Figure 16: MSCT Use case C2B-5



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, the consumer would need to first subscribe to the MSCT Inst service and download a dedicated MSCT Inst application from the MSCT service provider on their mobile device.
- The consumer's ASPSP delegates the authentication of the consumer to the MSCT service provider.
- The merchant also needs to be subscribed to the MSCT Inst service, e.g., through their ASPSP or the MSCT service provider directly and has downloaded dedicated software and has the appropriate equipment to scan QR-codes in their POI environment.
- The MSCT service provider is linked to the consumer's ASPSP.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The merchant enters the transaction amount which is displayed on the POI.³²

Step 2

- The consumer selects and opens the MSCT Inst application on their mobile device which possibly involves the entry of a password.
- A QR-code containing a token for the consumer is generated by the MSCT Inst application on the mobile device.

Step 3

The consumer presents the QR-code which is scanned by the merchant's POI.

Step 4

The merchant retrieves the consumer's token from the QR-code and sends a Payment Request message to their MSCT service provider, including the merchant's name, IBAN_merchant³³, merchant transaction identifier, the transaction amount and the consumer identifier.

Step 5

The MSCT service provider identifies the consumer's IBAN and ASPSP from the consumer token.

³² The display of the transaction amount by the POI may happen after step 3, since the customer identification might have an impact on the final transaction amount.

³³ Instead of the IBAN_merchant a proxy may be used.



Step 6

- The MSCT service provider forwards the transaction information to the MSCT Inst app on the consumer's mobile device.
- The MSCT Inst application pops-up a window with the transaction details including the merchant name/ IBAN_merchant and transaction amount.
- The consumer authenticates and confirms the transaction by entering a mobile code on the mobile device.

Step 7

Upon successful verification of the mobile code by the MSCT Inst application, an authentication code is calculated by the MSCT application.

Step 8

The SCT Inst instruction, including the merchant's name, IBAN_merchant, the transaction amount and the merchant transaction identifier and the authentication code are transmitted to the consumer's ASPSP via the MSCT service provider.

Step 9

The MSCT service provider acknowledges successful receipt of the SCT Inst instruction to the consumer.

Step 10

- The consumer's ASPSP checks the integrity of the SCT Inst instruction and verifies the authentication code.
- The consumer's ASPSP checks the availability of funds on the payer's account.
- The consumer's ASPSP prepares and submits the SCT Inst transaction to the merchant's ASPSP.

Step 11

- A confirmation message is returned from the merchant's ASPSP to the consumer's ASPSP.
- The merchant's ASPSP makes the funds available to the merchant.

Step 12

- The merchant is notified by the MSCT service provider (information provided by the consumer's ASPSP) that their account has been credited.
- The consumer is notified by the MSCT service provider in their MSCT app that the transaction has been successfully executed (information provided by the consumer's ASPSP) and may optionally receive an e-receipt.

Note: For virtual POIs, the MSCT use case will be similar except that the consumer token will need to be transferred to the merchant in a different way (e.g., entered manually by the consumer into the merchant's website or payment page).



Analysis MSCT Use case C2B-5	
Interoperability	<ul style="list-style-type: none"> • The consumer and the merchant are subscribed to the same MSCT service while the consumer’s ASPSP needs be linked to the corresponding MSCT service provider. • For a truly “open” approach and a SEPA-wide interoperability, if the MSCT service provider of the consumer is different to the MSCT service provider of the merchant, a framework will need to be specified that interconnects the different MSCT service providers.
Challenges	<ul style="list-style-type: none"> • Standardisation of messages including data elements between MSCT service provider back-ends. • Standardisation of a “QR-code” and identification of consumers. • Standardisation of the Payment Request messages. • Security of the QR-code/consumer token. • Standardisation of interface between MSCT providers and ASPSPs • How is the transaction reconciled with the purchase (e.g., transaction identifier)? • The notification messages in step 12 are not included in the SCT Inst scheme.

Table 13: Analysis MSCT Use case C2B-5

Notes:

- The standardisation of the QR-code for payer-presented data is addressed in Chapter 18.
- The security of QR-codes and their data is addressed in Chapter 10.
- The interoperability of MSCTs based on payer-presented data whereby different MSCT service providers are involved for the consumer and merchant is addressed in Chapters 16 and 18 .
- The minimum data elements in the payment request and notification messages are defined in Annex 4.



7.3.8 MSCT use case C2B-6: Mobile device - Offline use case – Payment at a physical POI using NFC and EMV-based SCA involving a fingerprint

This MSCT use case presents an example for an in-store payment based on consumer-presented data and relying on EMV technology for the authentication of the consumer by their ASPSP.

Benefitting from the bi-directional NFC communication capability, the consumer's mobile device and the POI exchange the data requested to build the payload, while performing SCA using a mobile EMV contactless authentication app issued by the consumer's ASPSP. The result of this SCA mechanism is a cryptogram generated by the EMV app which is transmitted by the POI, together with the other transaction data via the merchant's MSCT service provider to the consumer's ASPSP which will then verify this cryptogram. In the described example, the merchant's MSCT service provider acts as a PISP for the exchanges with the consumer's ASPSP.

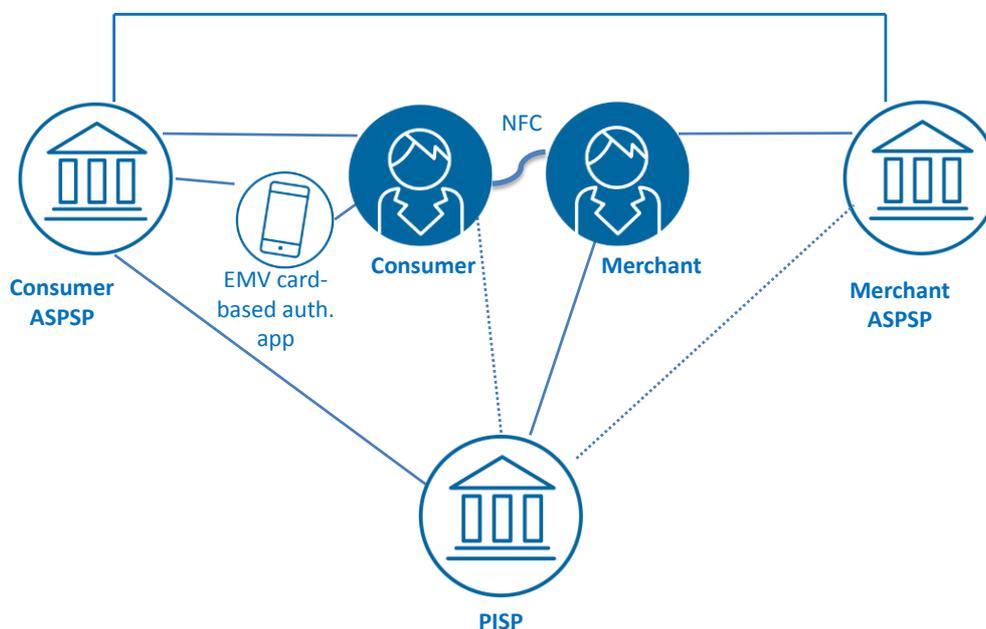


Figure 17: Actors in MSCT Use case C2B-6

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. The merchant has a contract with a PISP (= merchant MSCT service provider) that supports the PSD2 API, have downloaded dedicated software on their POI and agreed to make the PSD2 Art. 45(2) required PISP information available to the payer. Moreover, the consumer needs to provide appropriate consent to the usage of the PISP by the merchant.³⁴ In this payment transaction a strong customer authentication (see section 8.3) in accordance with the relevant PSD2 [5] requirements is performed involving a fingerprint (see section 8.2) and the calculation of a cryptogram by the EMV application using a dedicated key.

³⁴ Subject to clarification by EBA on questions EBA Q&A 2020_5570 and 2020_5573.



No mobile network connectivity of the mobile handset is required in this use case, except for the possible notification to the consumer of the transaction execution (see Chapter 18).

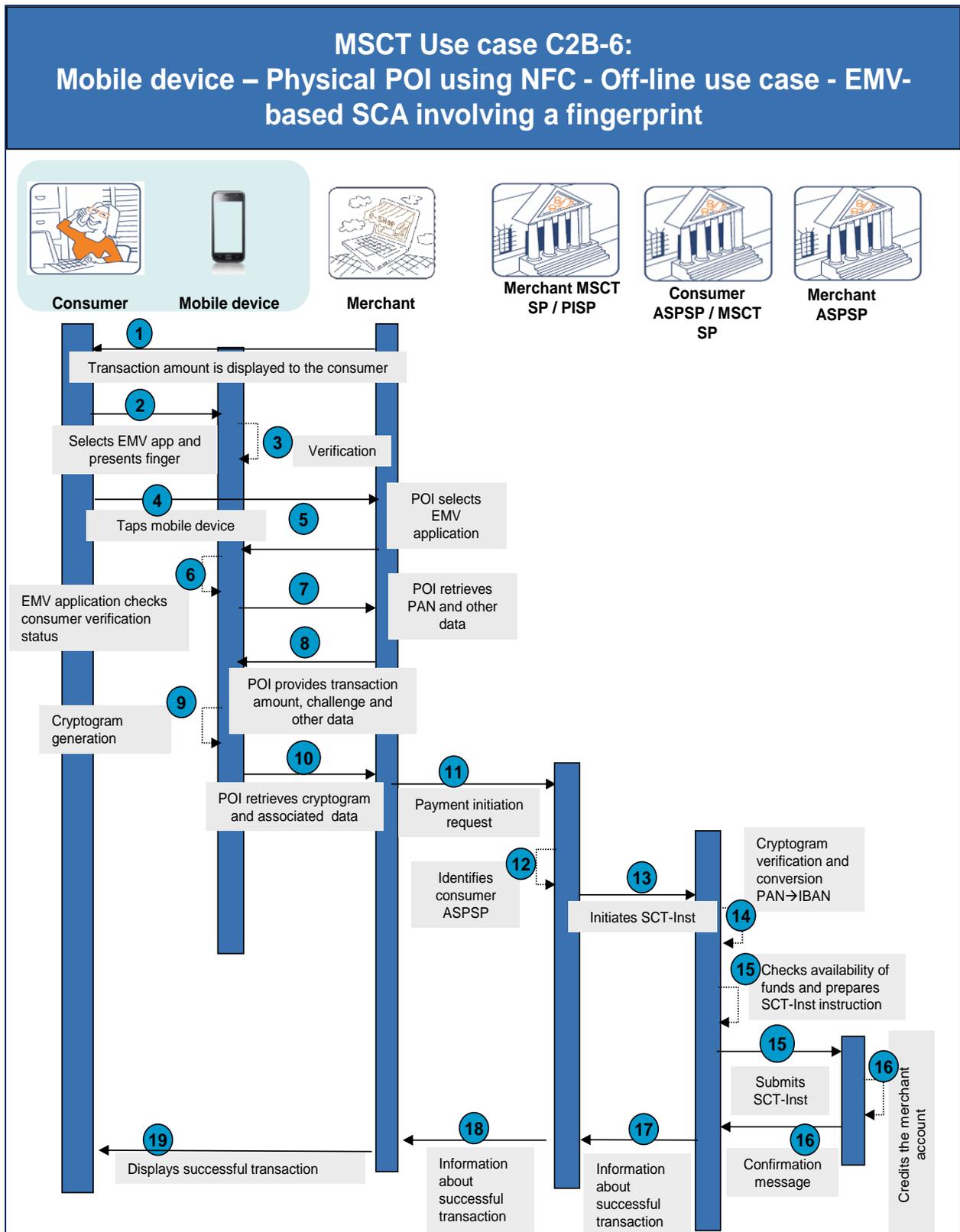


Figure 18: MSCT Use case C2B-6



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, the consumer has downloaded a mobile EMV contactless authentication app from their ASPSP on their mobile device. They have further registered their IBAN to be converted into a consumer_PAN and this consumer_PAN has been provisioned to the authentication app.
- The merchant has contracted with the MSCT service provider (=PISP) and installed their software on the POI.

Step 1

The merchant enters the transaction amount which is displayed on the POI.

Step 2

The consumer selects and opens the EMV authentication application on their mobile device and presents a fingerprint.³⁵

Step 3

The fingerprint is verified by the mobile device and the verification result is stored in the mobile device.

Step 4

The consumer taps their mobile device on the POI. This gesture may represent the consumer's consent to use the PISP services³⁶.

Step 5

While the mobile device is in the NFC field, the POI selects the EMV authentication application.

Step 6

While the mobile handset is in the NFC field, the EMV application checks the status of the consumer verification that was stored on the mobile device and stores this result in an EMV parameter (Card Verification Result).

Step 7

While the mobile handset is in the NFC field, the POI retrieves from the EMV authentication app the PAN and possibly other data.

Step 8

While the mobile handset is in the NFC field, the POI sends to the EMV application the transaction amount, a challenge and other transaction data such as date, country code, etc.

³⁵ Other consumer verification methods may be applied, see section 8 in the MSCT IG.

³⁶ Subject to clarification by EBA on questions EBA Q&A 2020_5570 and 2020_5573.



Step 9

While the mobile handset is in the NFC field, the EMV application generates a cryptogram. This cryptogram signs the transaction amount, challenge, the Card Verification Result and other data.³⁷

Step 10

While the mobile handset is in the NFC field, the POI retrieves the cryptogram and other associated data from the EMV application.

Step 11

The POI sends a payment initiation request to the merchant's MSCT service provider (=PISP). The payment initiation request message includes the transaction amount, name and IBAN_merchant³⁸, transaction identifier, consumer_PAN, the cryptogram and other associated data.

Step 12

The merchant's MSCT service provider identifies the consumer's ASPSP from the Issuer Identification Number present in the consumer_PAN (typically the first 6 digits).

Step 13

The merchant MSCT service provider, in its role of PISP, initiates a payment with the consumer ASPSP via the PSD2 API, and sends the full transaction data to the consumer's ASPSP, including the transaction amount, consumer_PAN, merchant name, merchant_IBAN, transaction identifier, cryptogram.

Step 14

- The consumer ASPSP, upon receipt of the payload, checks the cryptogram using some of the associated data. They may also perform other optional controls (spending limits, risk management...).
- Subsequently to the successful verification of the cryptogram, the consumer ASPSP converts the consumer_PAN back to the IBAN of the consumer.

Step 15

- The consumer's ASPSP checks the availability of funds on the payer's account.
- The consumer ASPSP prepares and submits the SCT Inst transaction to the merchant ASPSP.

Step 16

- A confirmation message is returned from the merchant's ASPSP to the consumer's ASPSP.
- The merchant's ASPSP makes the funds available to the merchant.

³⁷ Subject to further clarification by the EBA on the need for dynamic linking (see EBA Q&A 2020_5247).

³⁸ Alternatively, the name and IBAN of the merchant may also be added by the merchant MSCT service provider.



Step 17

The consumer's ASPSP sends a notification message to the PISP about the execution of the SCT Inst transaction.

Step 18

The PISP (= merchant MSCT service provider) sends a notification message to the merchant about the successful transaction.

Step 19

The merchant POI displays to the consumer that the transaction has been successfully executed.

Analysis MSCT Use case C2B-6	
Interoperability	<ul style="list-style-type: none"> • Based on and governed by PSD2. • The EMV contactless kernel could serve as a basis for interoperability for the communication with the consumer's mobile device.
Challenges	<ul style="list-style-type: none"> • The PSD2 API needs to support the functionalities needed (e.g. PAN, cryptogram and other associated data, notification message). • Use of NFC in certain phones is currently restricted to the phone vendor's proprietary payment wallet but solution is "compatible" with this wallet. • Requires a contract between the merchant and the PISP (= merchant MSCT service provider) covering the liabilities around payment status confirmations. • Consumer consent with respect to usage of the PISP subject to EBA clarifications ((PSD 2 Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30))³⁹. • Clarification on the need for SCA with dynamic linking⁴⁰. • Impact of using the EMVCo specifications for an authentication app for MSCTs.

Table 14: Analysis MSCT Use case C2B-6

Note: The interoperability models for MSCTs involving a PISP are analysed in Chapter 20.

³⁹ Subject to clarification by EBA on questions EBA Q&A 2020_5570 and 2020_5573.

⁴⁰ Subject to clarification by EBA on question EBA Q&A 2020_5247.



7.3.9 MSCT use case C2B-7: Mobile device – Offline use case - Payment at a physical POI with consumer-presented QR-code involving a PISP – SCA via BLE using an MSCT app involving a fingerprint

This use case presents an example of consumer experience whereby their mobile device has no mobile network connection⁴¹ and is used for a payment at a physical POI. In this use case two proximity technologies are used: a consumer-presented QR-code and BLE.

The consumer has preloaded a dedicated MSCT app onto their mobile device provided by their ASPSP that supports the generation of an Advanced Electronic Signature (AdES) as specified under the eIDAS framework⁴² based on a dedicated asymmetric key pair⁴³. It is further assumed that the QR-code provided by the MSCT app⁴⁴ contains the necessary information to establish a secure connection (cross refer section in the MSCT IG) between this app and the merchant POI via BLE for performing the SCA.

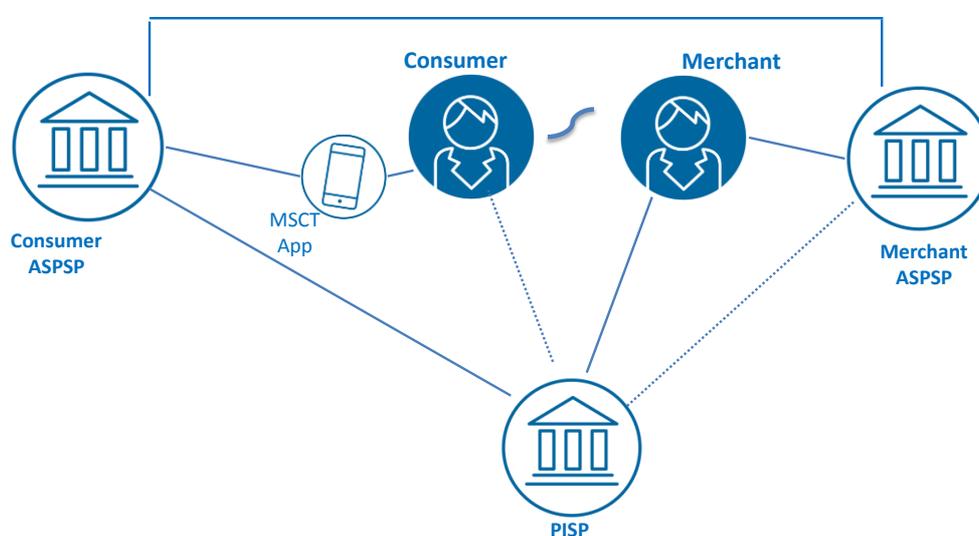


Figure 19: Actors in MSCT Use case C2B-7

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs.

The merchant has a contract with a PISP (= merchant MSCT service provider) that supports the PSD2 API, has downloaded dedicated software on their POI and agreed to make the PSD2 Art. 45(2) required PISP information available to the consumer. Moreover, the consumer needs to provide appropriate consent to the usage of the PISP by the merchant.⁴⁵

⁴¹ If the mobile device of the consumer has internet connection, a similar use case could be considered whereby the QR-code could be used to establish an internet connection between the MSCT app and the merchant or the PISP to conduct the transaction.

⁴² See <https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014>

⁴³ See also the EU Retail Payments Strategy including the use of EUID, eIDAS signatures and e-receipts, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0592&from=EN>.

⁴⁴ Unlike in some other MSCT use cases whereby an MSCT app is involved and the SCT Inst is initiated by the MSCT service provider, in this use case it is initiated by a PISP, involved on the merchant side.

⁴⁵ Subject to clarification by EBA on the questions EBA Q&A 2020_5570 and 2020_5573.



The PISP also has a dedicated asymmetric key pair to generate a QSEAL in accordance with the eIDAS framework.

The exchange of data between the MSCT app on the consumer's mobile device and the PISP is protected through symmetric encryption using a secret key derived from dedicated session Elliptic Curve Diffie-Hellman (ECDH) key pairs that are generated for each transaction both by the MSCT app and by the PISP (see **Figure 21**) for an overview of the cryptography) from the respective public keys of the MSCT app and the PISP.

In this payment transaction a strong customer authentication (see section 8.3) in accordance with PSD2 [5] is performed involving a fingerprint that unlocks a cryptographic private key held within the "separate secure execution environment" of the consumer's mobile device to create the AdES (see section 8.2).

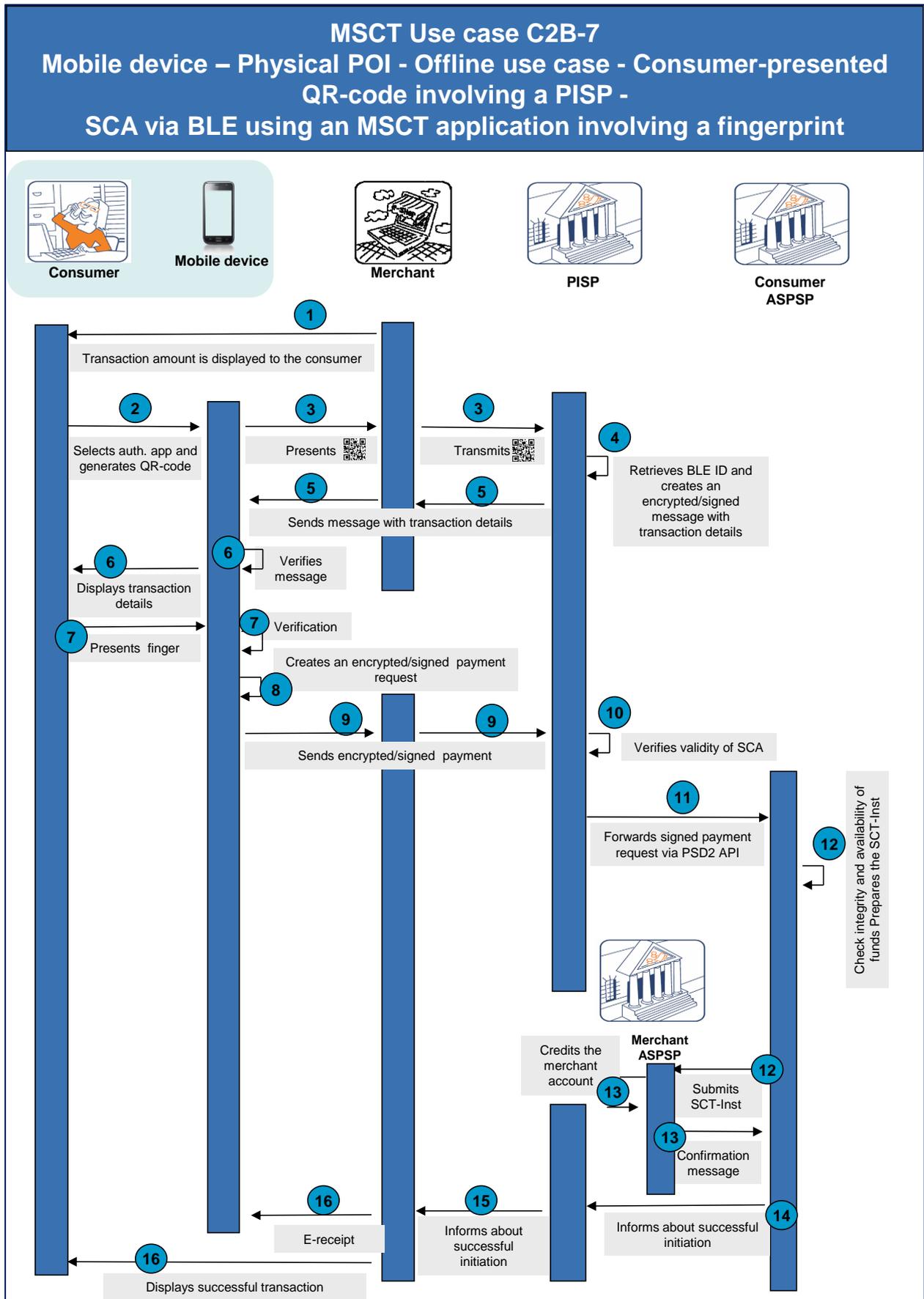


Figure 20: MSCT Use case C2B-7

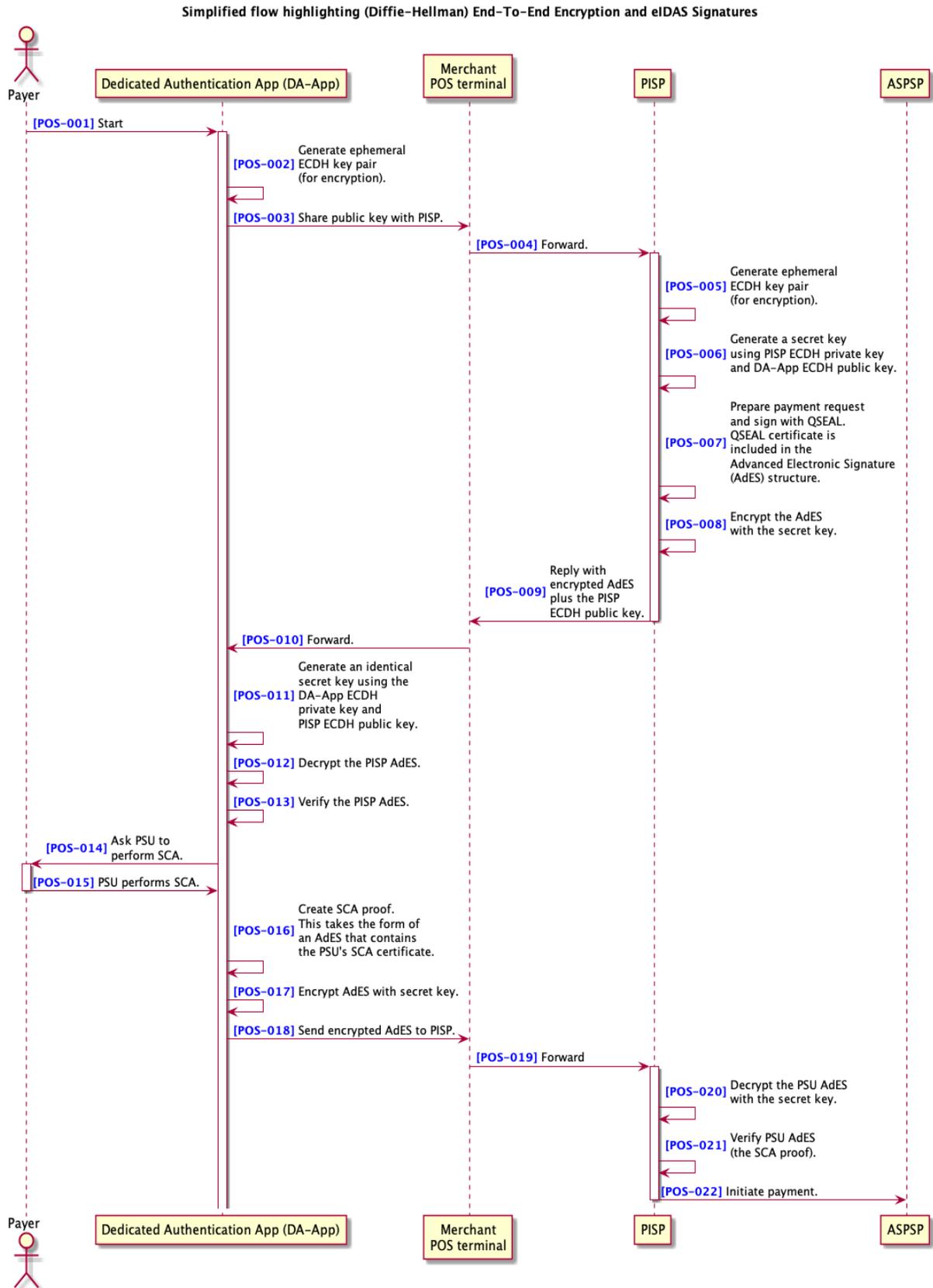


Figure 21: MSCT Use case C2B-7 – overview cryptography



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, consumers would need to download an MSCT app from their ASPSP that supports the generation of AdES under the eIDAS framework and the yet to be defined interoperability standard between these apps and PISPs, including the generation of ECDH session keys. Moreover, the app stores all eIDAS country root keys to enable public key certificate verifications.
- The merchant is subscribed to the PISP and has installed their software on the POI.
- The PISP also supports the generation of QSEALs under the eIDAS framework and the yet to be defined interoperability standard including the generation of ECDH session keys. It is further enabled to use the consumer ASPSP's PSD2 Access to the Account interface (PSD2 API).
- During the payment transaction, there is no internet nor OTA connection required for the consumer's mobile device.

Step 1

The merchant enters the transaction amount which is displayed on the POI⁴⁶.

Step 2

- The consumer selects and opens the MSCT app on their mobile device.
- The app generates a session ECDH_app key pair and a dynamic QR code-containing the ECDH_app public key.

Step 3

- The consumer presents their QR-code, which is scanned by the merchant's POI.
- The POI retrieves the necessary information to establish a BLE connection with the MSCT app on the consumer's mobile device.
- The information contained in the QR-code is provided to the PISP.

Step 4

- The PISP retrieves the ECDH_app public key and checks the merchant.
- The PISP generates an ECDH_PISP key pair and creates a message containing the transaction details, including - as a minimum - the merchant's name, IBAN_merchant, merchant transaction identifier and the transaction amount. This message is signed with a PISP QSEAL and encrypted with a secret session key derived from the ECDH public keys of the MSCT app and the PISP.

Step 5

The encrypted/signed message, including the PISP QSEAL public key certificate and the ECDH_PISP public key is transferred to the merchant and from the merchant's POI to the MSCT app on the consumer's mobile device using BLE.

⁴⁶ The display of the transaction amount by the POI may happen after step 3, since the customer identification might have an impact on the final transaction amount.



Step 6

- The MSCT app on the consumer's mobile device also generates the same secret session key from the ECDH public keys of the MSCT app and the PISP and decrypts the message.
- Next the app verifies the PISP QSEAL public key certificate and subsequently the PISP QSEAL (hereby implicitly authenticating the PISP).
- The transaction details (including as a minimum the transaction amount and merchant name/IBAN) are displayed to the consumer by the MSCT app.
- The MSCT app optionally offers the consumer to select a payment account or presents a default account for approval.

Step 7

- The consumer authenticates and confirms the transaction by presenting a finger to their device.
- The mobile device verifies the fingerprint.

Step 8

- Upon successful verification of the fingerprint, the MSCT app on the consumer's mobile device further completes the message received with the IBAN_consumer, CustomerID and the ASPSP's HostID (uri).
- The app generates an AdES on the message (dynamically linked to all data elements).
- The app subsequently encrypts the signed data using the secret session key.

Step 9

The encrypted/signed message including the AdES public key certificate is transferred from the app via BLE to the POI and further transferred to the PISP.

Step 10

- The PISP checks the message received by decrypting the message using the secret session key.
- Next the PISP optionally verifies the AdES public key certificate and subsequently the AdES, and can thereby verify the validity of the SCA.
- The PISP retrieves the ASPSP's HostID (uri).

Step 11

The PISP provides the consumer-signed message as a "signed payment request" to the consumer's ASPSP via their PSD2 API.

Step 12

- The consumer ASPSP checks the integrity of all the information provided including the verification of the AdES.
- The consumer ASPSP checks the availability of funds on the consumer's account.
- The consumer ASPSP prepares and submits the SCT Inst transaction to the merchant ASPSP.



Step 13

- A confirmation message is returned from the merchant’s ASPSP to the consumer’s ASPSP.
- The merchant’s ASPSP makes the funds available to the merchant.

Step 14

The consumer ASPSP sends a notification message to the PISP about the execution of the SCT Inst transaction.

Step 15

The PISP sends a notification message to the merchant about the successful transaction.

Step 16

The merchant POI displays the successful transaction and provides an e-receipt to the consumer’s mobile device via BLE.

Analysis MSCT Use case C2B-7	
Interoperability	<ul style="list-style-type: none"> • Based on and governed by PSD2 • EC eIDAS framework • Yet to be defined proximity connection standard between the MSCT app and the PISP software on the POI.
Challenges	<ul style="list-style-type: none"> • The MSCT app from the consumer ASPSP must support the generation of AdES under the eIDAS framework and the proximity connection standard (including the generation of the session key). • The PISP needs to support the generation of QSEALs under the eIDAS framework. • Requires a contract between the merchant and the PISP. • Consumer consent with respect to usage of the PISP subject to EBA clarifications ((PSD 2 Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30))⁴⁷. • Support for the proximity connection standard both by the MSCT app and the POI. • Lack of common specification for usage of BLE for payments at the POI. • Liability aspects need to be clarified. • Standardisation of the QR-code and identification of consumers. • Integrity of the QR-code. • The notification messages in steps 14 and 15 are not included in the SCT Inst scheme. • The PSD2 API needs to support the functionalities required (e.g. payment request, notification message, etc.).

⁴⁷ Subject to clarification by EBA on the questions EBA Q&A 2020_5570 and 2020_5573.



Table 15: Analysis MSCT Use case C2B-7

Notes:

- All MSCT use cases described include the performance of an SCA. Obviously, if SCA is not required when an exemption is applied in accordance with PSD2 and the RTS, the corresponding steps will be omitted and the consumer would just confirm the transaction, e.g. by pressing a button on the consumer device.
- The standardisation of the QR-code for consumer-presented data is addressed in Chapter 18.
- The interoperability models for MSCTs involving a PISP are analysed in Chapter 20.
- The integrity of QR-codes is addressed in Chapter 10.
- The minimum data elements in the payment request and notification messages are defined in Annex 4.



7.3.10 MSCT use case C2B-8: Mobile device - Payment at a physical POI with consumer-presented QR-code - Unknown final amount with final amount being lower than pre-agreed amount – SCA of consumer using MSCT application involving a fingerprint

This use case presents an example of consumer experience whereby their mobile device is used to pay in-store by presenting a consumer-presented QR-code to the POI. Hereby a dedicated MSCT Inst application on the mobile device of the consumer is used that they have downloaded from an MSCT service provider into their mobile wallet.

The consumer authentication is performed through the MSCT application in the consumer mobile device.

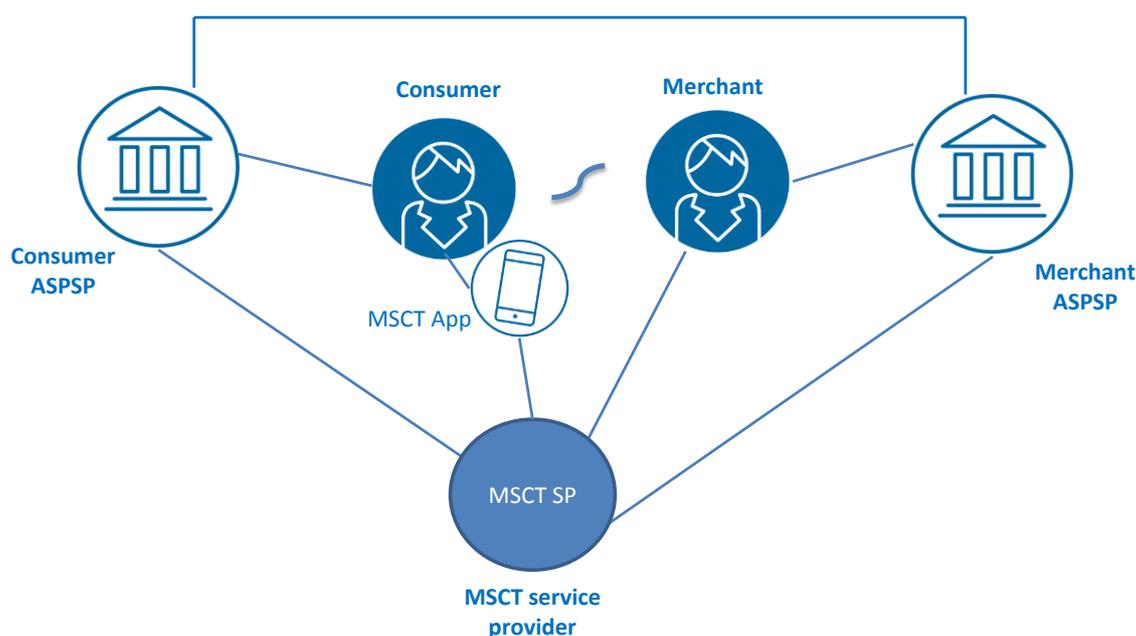


Figure 22: Actors in MSCT Use case C2B-8

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. Both ASPSPs are participants in the same MSCT Inst Service⁴⁸.

Also, the merchant needs to be subscribed to the MSCT Inst service and have downloaded dedicated software on their POI.

In this payment transaction a strong customer authentication (see section 8.3) of the consumer on the pre-agreed amount in accordance with the relevant PSD2 requirements is performed involving a fingerprint⁴⁹ (see section 8.2) and the calculation of an authentication code by the consumer's MSCT application using a dedicated key.

Furthermore, a strong customer authentication (see section 8.3) of the merchant on the repayment⁵⁰ amount in accordance with the relevant PSD2 requirements is performed

⁴⁸ This refers to the current MSCT solutions in the market.

⁴⁹ Note that also other biometric methods may be used.

⁵⁰ This is referenced as a "transfer back" in the SCT Inst rulebook (EPC004-16/2019 Version1.2).



involving a merchant code⁵¹ (see section 8.2) and the calculation of an authentication code by the merchant platform using a dedicated key.

Note that for both authentications delegation needs to be given to the MSCT service provider by the respective ASPSPs.

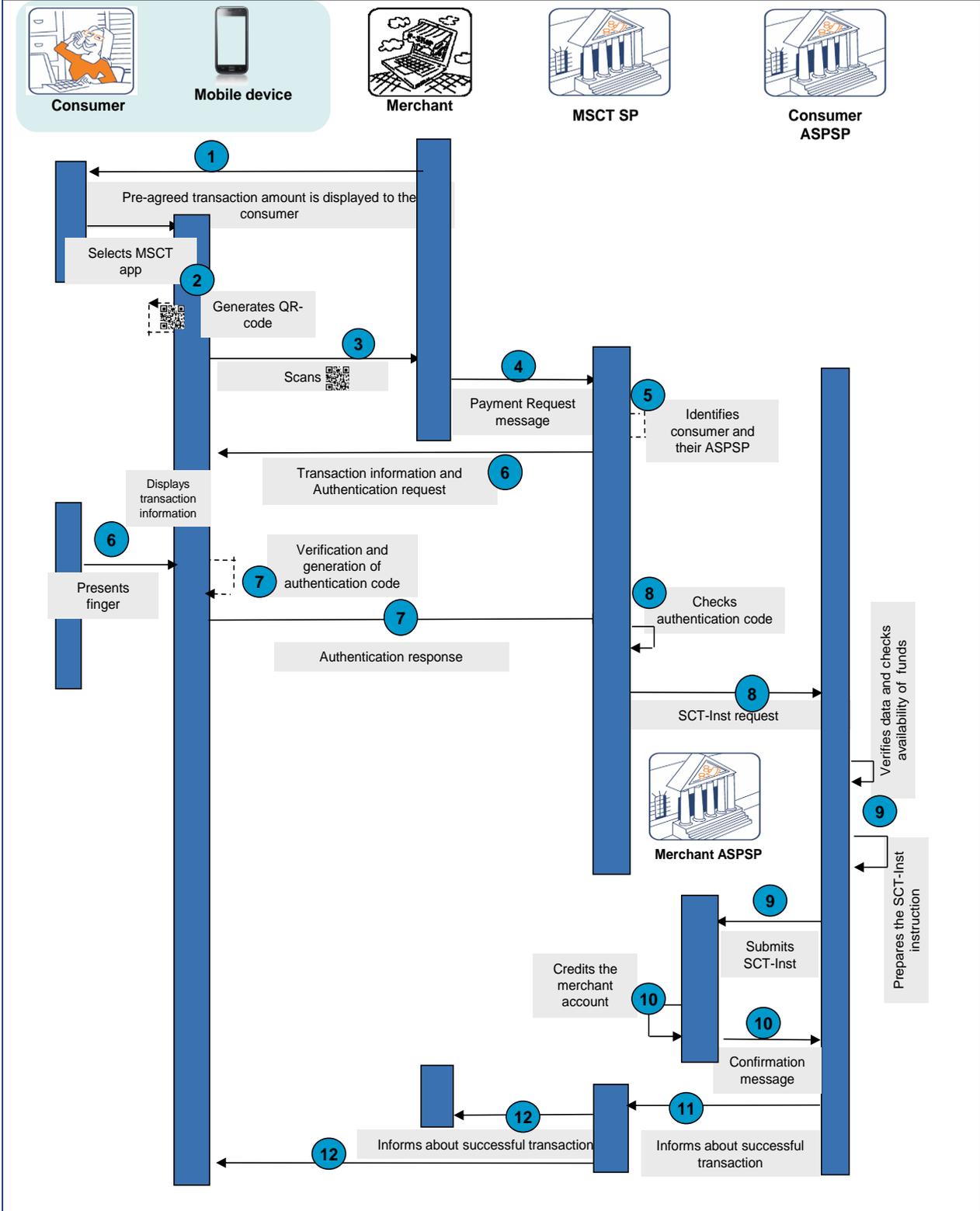
Note that the transaction flow for the repayment (covering part of the original transaction amount) illustrated in this use case remains valid even if a repayment is done for a reimbursement of the full original transaction amount.

⁵¹ Note that also biometric methods may be used.



MSCT Use case C2B-8 (1)

Mobile device – Physical POI - Consumer-presented QR-code – Unknown final transaction amount with final amount lower than pre-agreed amount SCA using an MSCT application involving a fingerprint



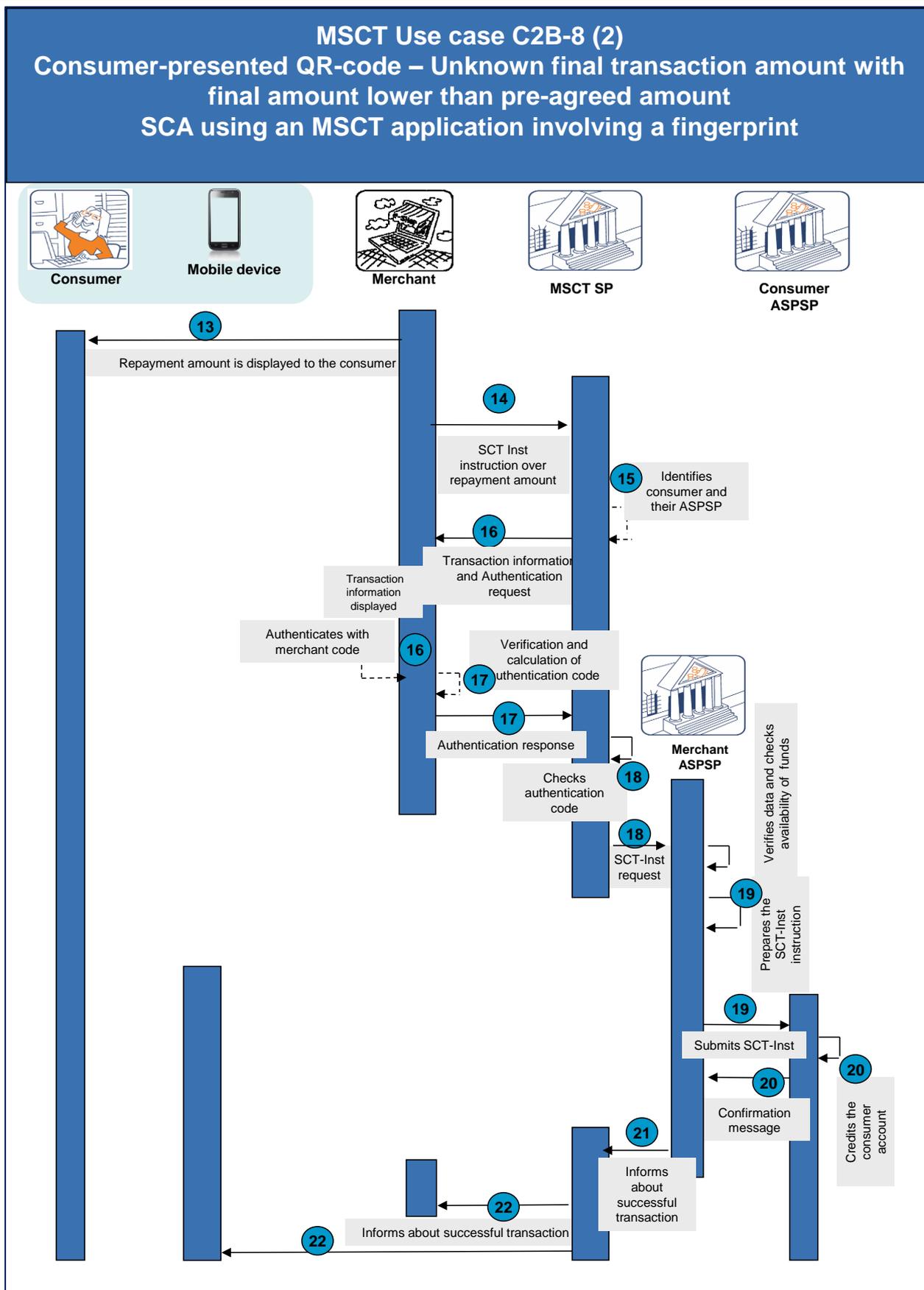


Figure 23: MSCT Use case C2B-8



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, the consumer would need to subscribe to the MSCT Inst service and download a dedicated MSCT Inst application from the MSCT service provider on their mobile device.
- The consumer ASPSP delegates the authentication of the consumer to the MSCT service provider.
- The merchant also needs to be subscribed to the MSCT Inst service, e.g., through their ASPSP or the MSCT service provider directly and has downloaded dedicated software and has the appropriate equipment to scan QR-codes in their POI environment.
- The MSCT service provider is linked to the consumer ASPSP.
- During the payment transaction, a mobile internet connection by the consumer device is required.

Step 1

The merchant enters the pre-agreed transaction amount⁵² which is displayed on the POI.⁵³

Step 2

- The consumer selects and opens the MSCT Inst application on their mobile device which possibly involves the entry of a password.
- A QR-code containing a token for the consumer is generated by the MSCT Inst application on the mobile device.

Step 3

The consumer presents the QR-code which is scanned by the merchant POI.

Step 4

The merchant retrieves the consumer token from the QR-code and sends a Payment Request message to their MSCT service provider, including the merchant name, IBAN_merchant⁵⁴, merchant transaction identifier, the pre-agreed amount and the consumer token.

Step 5

The MSCT service provider identifies the consumer IBAN and ASPSP from the consumer token.

Step 6

- The MSCT service provider forwards the transaction information to the MSCT Inst app on the consumer mobile device.
- The MSCT Inst application pops-up a window with the transaction details including the merchant name/ IBAN_merchant and the pre-agreed transaction amount.
- The consumer authenticates and confirms the transaction by presenting a fingerprint to the mobile device.

⁵² E.g. for car rental, hospitality,

⁵³ The display of the transaction amount by the POI may happen after step 3, since the customer identification might have an impact on the final transaction amount.

⁵⁴ Instead of the IBAN_merchant a proxy may be used.



Step 7

Upon successful verification of the fingerprint by the mobile device, an authentication code is calculated by the MSCT application.

Step 8

- The authentication response is transmitted to the MSCT service provider.
- The MSCT service provider checks the authentication code.
- The SCT Inst instruction, including the merchant name, IBAN_merchant, the pre-agreed transaction amount, the merchant transaction identifier and the flag indicating a successful verification are transmitted to the consumer ASPSP via the MSCT service provider.

Step 9

- The consumer ASPSP checks the integrity of the SCT Inst instruction.
- The consumer ASPSP checks the availability of funds on the payer account.
- The consumer ASPSP prepares and submits the SCT Inst transaction over the pre-agreed amount to the merchant ASPSP.

Step 10

- A confirmation message is returned from the merchant ASPSP to the consumer ASPSP.
- The merchant ASPSP makes the funds available to the merchant.

Step 11

The consumer ASPSP sends a notification message to the MSCT service provider about the successful execution of the SCT Inst transaction over the pre-agreed amount.

Step 12

- The merchant is informed by the MSCT service provider that their account has been credited.
- The consumer is informed by the MSCT service provider in their MSCT app that the payment has been successfully executed and may optionally receive an e-receipt.

Step 13

- After offering the service, the final transaction amount is lower than the pre-agreed amount by the consumer.
- The merchant enters the repayment amount (i.e. difference between the pre-agreed amount and the final amount) on the POI which is displayed to the consumer, if present.

Step 14

The merchant POI sends an SCT Inst instruction to their MSCT service provider, including the merchant name, IBAN_merchant⁵⁵, merchant transaction identifier, the repayment amount and the merchant transaction identifier of the original transaction.

⁵⁵ Instead of the IBAN_merchant a proxy may be used.



Step 15

The MSCT service provider identifies the consumer name/IBAN and consumer ASPSP from the consumer token in the original transaction and the merchant ASPSP from the IBAN_merchant.

Step 16

- The MSCT service provider forwards the transaction information with a challenge to the merchant POI.
- The transaction information including the consumer name/IBAN and repayment amount are displayed to the merchant with a request for authentication⁵⁶.
- The merchant authenticates (e.g. using a dedicated merchant code) and confirms the transaction.

Step 17

Upon successful verification of the merchant, an authentication code is calculated and transmitted to the MSCT service provider.

Step 18

- The MSCT service provider checks the authentication code.
- Upon successful verification, the SCT Inst instruction including the consumer name, IBAN_consumer, the repayment amount and a transaction identifier with a flag indicating the successful authentication are transmitted from the MSCT service provider to the merchant ASPSP.

Step 19

- The merchant ASPSP checks the integrity of the SCT Inst instruction.
- The merchant ASPSP checks the availability of funds for the final transaction amount on the merchant account.
- The merchant ASPSP prepares and submits the SCT Inst transaction (on the repayment amount) to the consumer ASPSP.

Step 20

- A confirmation message is returned from the consumer ASPSP to the merchant ASPSP.
- The consumer ASPSP makes the funds available to the consumer.

Step 21

The merchant ASPSP sends a notification message to the MSCT service provider about the successful execution of the SCT Inst transaction.

Step 22

- The consumer is informed by the MSCT service provider that their account has been credited.
- The merchant is informed by the MSCT service provider that the payment has been successfully executed and may optionally receive an e-receipt.

⁵⁶ This transaction may be exempted from SCA based on Articles 16 or 17 of the RTS.



Analysis MSCT Use case C2B-8	
Interoperability	The consumer and the merchant are subscribed to the same MSCT service while both the consumer ASPSP and the merchant ASPSP need to be linked to the MSCT service provider. For a truly “open” approach and a SEPA-wide interoperability, if the MSCT service provider of the consumer is different from the MSCT service provider of the merchant, a framework will need to be specified that interconnects the different MSCT service providers.
Challenges	<ul style="list-style-type: none"> • Standardisation of messages between MSCT service providers (e.g., Payment Request messages, Notification messages, ...). • Standardisation of the QR-code. • Security of the QR-code. • Authority to staff for repayment at merchant side. • How to link the two transactions. • How can the merchant link the two transactions? • How can the consumer link the two transactions? • The notification messages in steps 11 and 22 are not included in the SCT Inst scheme.

Table 16: Analysis MSCT Use case C2B-8

Notes:

- For virtual POIs, the MSCT use case will be similar except that the consumer token will need to be transferred to the merchant in a different way (e.g., entered manually by the consumer into the merchant website or payment page).
- The standardisation of the QR-code for consumer-presented data is addressed in Chapter 18.
- The interoperability of MSCTs based on consumer-presented data whereby different MSCT service providers are involved for the consumer and merchant is addressed in Chapters 16 and 18.
- The security of QR-codes is addressed in Chapter 10.
- The minimum data elements in the payment request and notification messages are defined in Annex 4.



7.3.11 MSCT use case C2B-9: Mobile device – Payment at POI with merchant-presented QR-code – SCA via MSCT Inst application involving a mobile code

This use case presents an example of consumer experience whereby their mobile device is used to pay in-store by reading a merchant-presented QR-code on the POI. Hereby both the consumer and merchant are subscribed to the same MSCT Inst service⁵⁷. The consumer has downloaded a dedicated MSCT Inst application from the MSCT service provider on their mobile device. The merchant has downloaded dedicated software on their POI from the MSCT service provider.

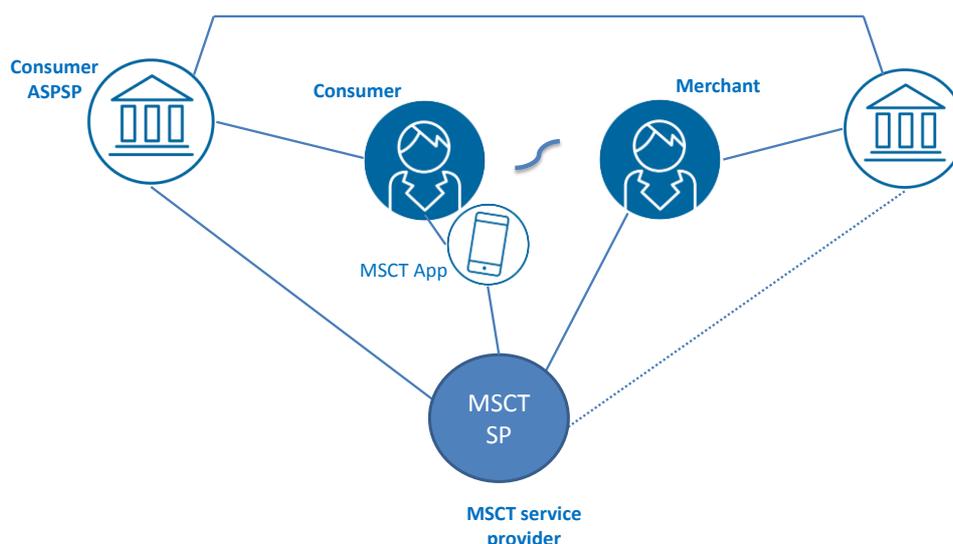


Figure 24: Actors in MSCT use case C2B-9

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. Both ASPSPs need to be registered with the same MSCT Inst service provider.

In this payment transaction a strong customer authentication (see section 8.3) in accordance with PSD2 [5] is performed involving a mobile code (see section 8.2) and the calculation of an authentication code by the MSCT application using a dedicated key. Since the MSCT application is provided to the consumer by an MSCT service provider instead of the consumer's ASPSP, a delegation for payer authentication from the consumer's ASPSP to their MSCT service provider is required. However, this requires an agreement between the consumer's ASPSP and the consumer's MSCT service provider.

⁵⁷ This refers to the current MSCT solutions in the market.

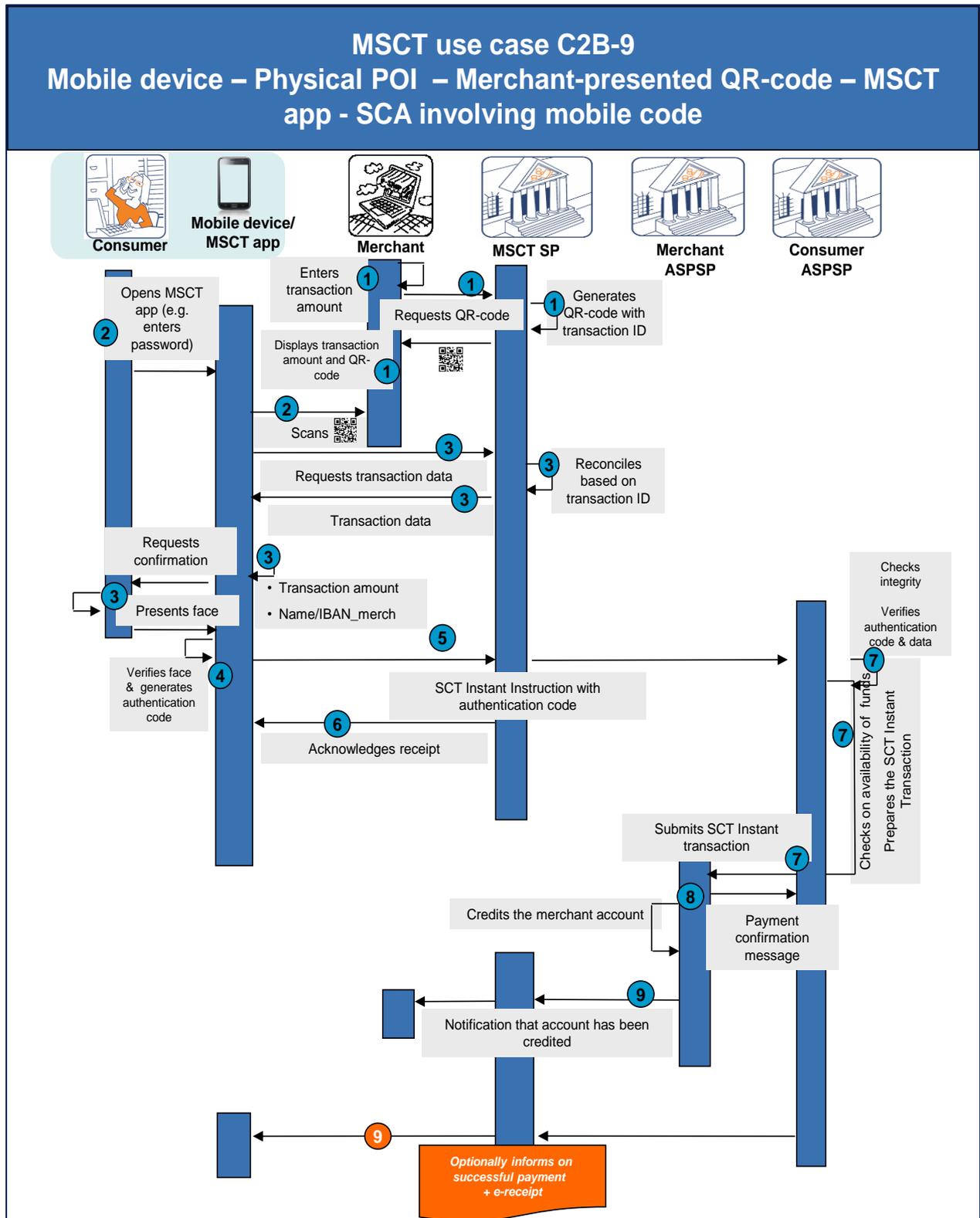


Figure 25: MSCT use case C2B-9



In the figure above, the following steps are illustrated:

Step 0

- The consumer needs to be subscribed to an MSCT Inst service and needs to have downloaded a dedicated MSCT Inst application from the MSCT Inst service provider, linked to a specific payment account of their ASPSP.
- The merchant needs to be subscribed to the same MSCT Inst service with a specific account from their ASPSP and have downloaded dedicated software on their POI.
- The MSCT service provider needs to be linked to both ASPSPs.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The merchant enters the transaction amount on the POI.
- The POI provides the transaction amount to the MSCT service provider.
- The MSCT service provider generates a QR-code, including the merchant transaction identifier.
- The transaction amount is displayed on the merchant's POI with the QR-code, which includes the merchant transaction identifier.

Step 2

- The consumer selects and opens the MSCT Inst application on their mobile device which possibly involves the entry of a password.
- A message is displayed on the mobile device inviting the consumer to scan the QR-code from the POI.

Step 3

- The mobile device retrieves the merchant transaction identifier from the QR-code and transmits the information to the MSCT service provider.
- The MSCT service provider reconciles this with the information received from the POI.
- The MSCT Inst application pops-up a window with the transaction details including the merchant name/IBAN_merch and transaction amount.
- The consumer authenticates and confirms the transaction by entering a mobile code on the mobile device.

Step 4

- Upon successful verification of the mobile code by the MSCT Inst application, an authentication code is calculated by the MSCT application.



Step 5

The SCT Inst instruction, including the merchant’s name, IBAN_merch, the transaction amount and the merchant transaction identifier and the authentication code are transmitted to the consumer’s ASPSP via the MSCT service provider.

Step 6

The MSCT service provider acknowledges successful receipt of the SCT Inst instruction to the consumer.

Step 7

- The consumer's ASPSP checks the integrity of the SCT Inst instruction and verifies the authentication code.
- The consumer’s ASPSP checks the availability of funds on the payer's account,
- The consumer’s ASPSP prepares and submits the SCT Inst transaction to the payee's ASPSP.

Step 8

- A confirmation message is returned from the merchant’s ASPSP to the consumer’s ASPSP.
- The merchant’s ASPSP makes the funds available to the merchant.

Step 9

- The merchant is notified by the MSCT service provider (information provided by the consumer’s ASPSP) that their account has been credited.
- The consumer is optionally notified by the MSCT service provider that the payment has been successfully executed (information provided by the consumer’s ASPSP) and may optionally receive an e-receipt.

Analysis MSCT Use case C2B-9	
Interoperability	<ul style="list-style-type: none"> • The consumer and the merchant need to be subscribed to the same MSCT service • The consumer’s ASPSP and the merchant’s ASPSP need be linked to the same MSCT service. If the MSCT service provider is a PISP, the link between the PISP and the merchant’s ASPSP is not needed. • For a truly “open” approach and a SEPA-wide interoperability, if the MSCT service provider of the payer is different to the MSCT service provider of the merchant, a framework needs to be specified that interconnects the different MSCT service providers.
Challenges	<ul style="list-style-type: none"> • Standardisation of a “QR-code”, ensuring the correct payee name/IBAN_merch link.



	<ul style="list-style-type: none">• Integrity of the QR-code.• Standardisation of merchant transaction identifier.• The notification messages in step 9 are not included in the SCT Inst scheme.
--	--

Table 17: Analysis MSCT use case C2B-9

Notes:

- The standardisation of the QR-code for payee-presented data is addressed in Chapter 17.
- The security of QR-codes is addressed in Chapter 10.
- The interoperability in case different MSCT service providers are involved for the consumer and the merchant is addressed in Chapters 16 and 17.
- The minimum data elements in the notification messages are specified in Annex 4.



7.3.12 MSCT use case B2B-1: Mobile device - Payment request - SCA using MSCT application involving a fingerprint

This use case presents an example of user experience whereby a business (payer) is requested via an EIPP service (see [32]) to pay an invoice from a payee. The invoice is paid with an MSCT. The payment request message included in the EIPP service contains the elements to initiate a payment to the payee and the transaction amount.

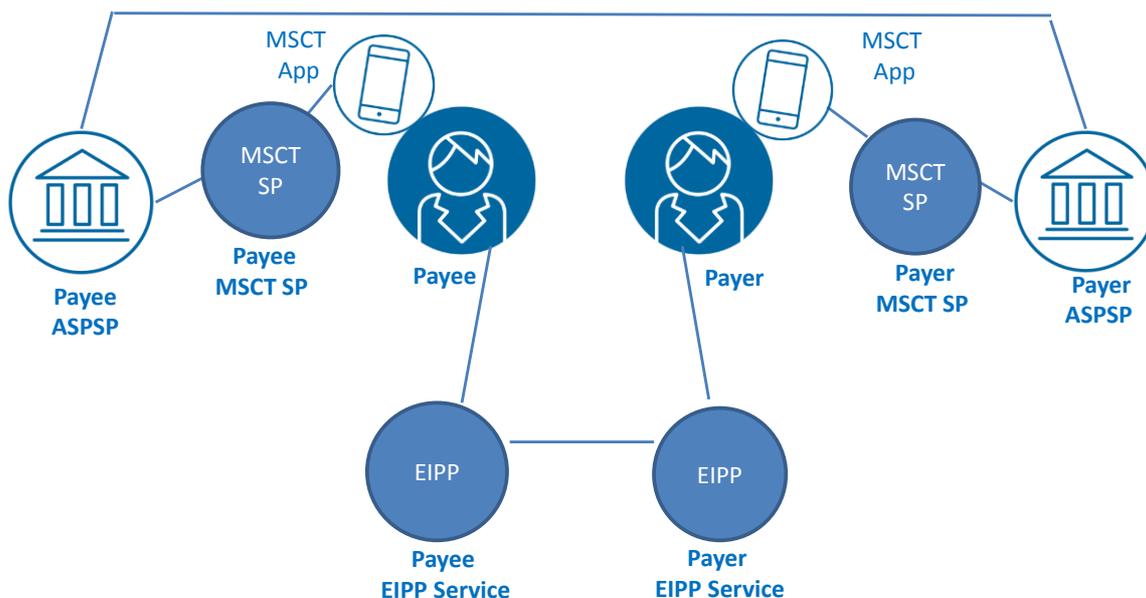


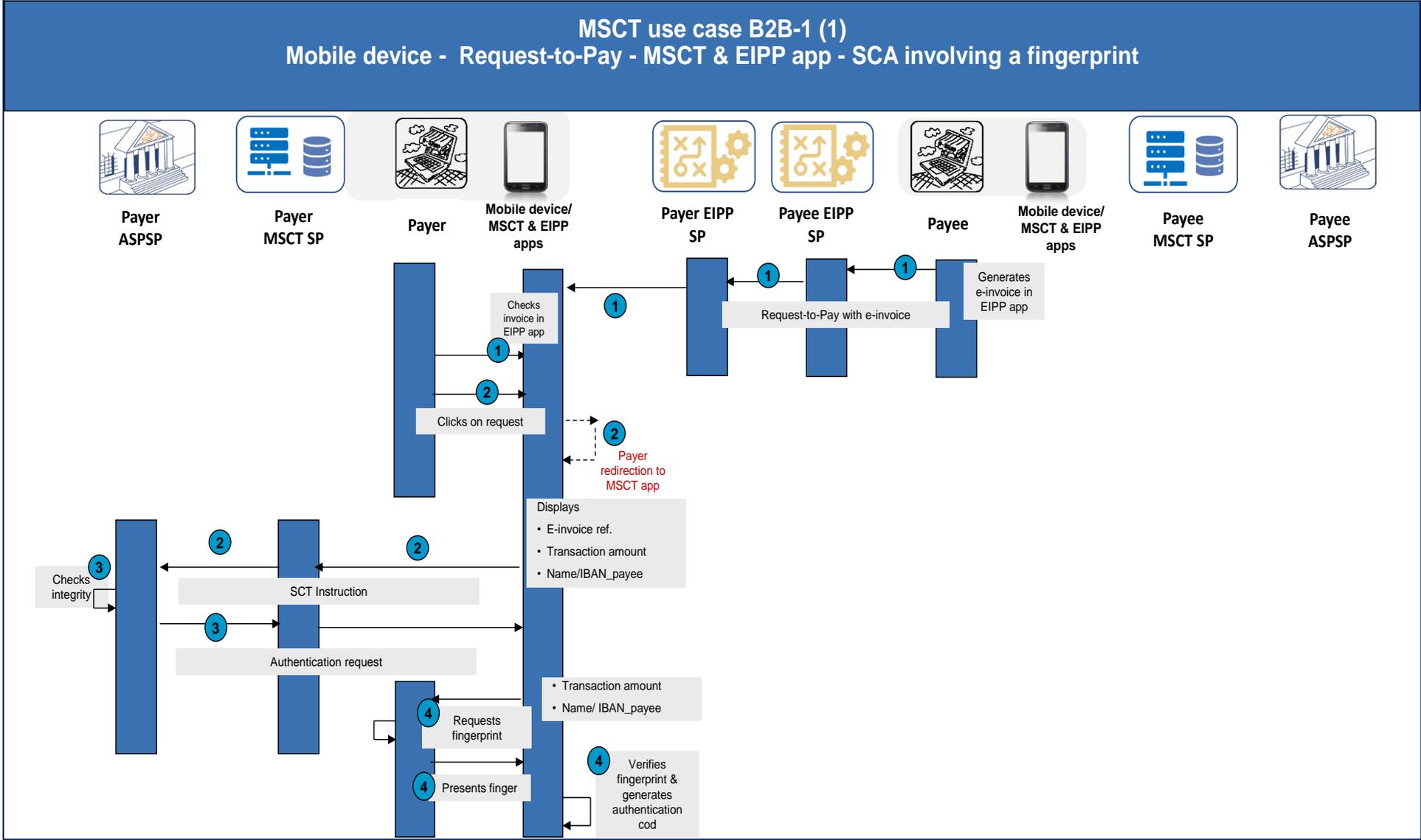
Figure 26: Actors in MSCT use case B2B-1

Payer and payee have subscribed to potentially different EIPP solution providers (see [32]).

Payer and payee may, and frequently will, hold their payment accounts with different ASPSPs and have downloaded different MSCT applications from potentially different MSCT service providers. Each ASPSP is a participant in an MSCT service (not necessarily the same).

A strong customer authentication (see section 8.3) in accordance to PSD2 [5] is performed, involving the presentation of a fingerprint⁵⁸ (see section 8.2) by the payer and the calculation of an authentication code by the payer's MSCT application.

⁵⁸ Note that other biometric methods may be used, see section 8.2.



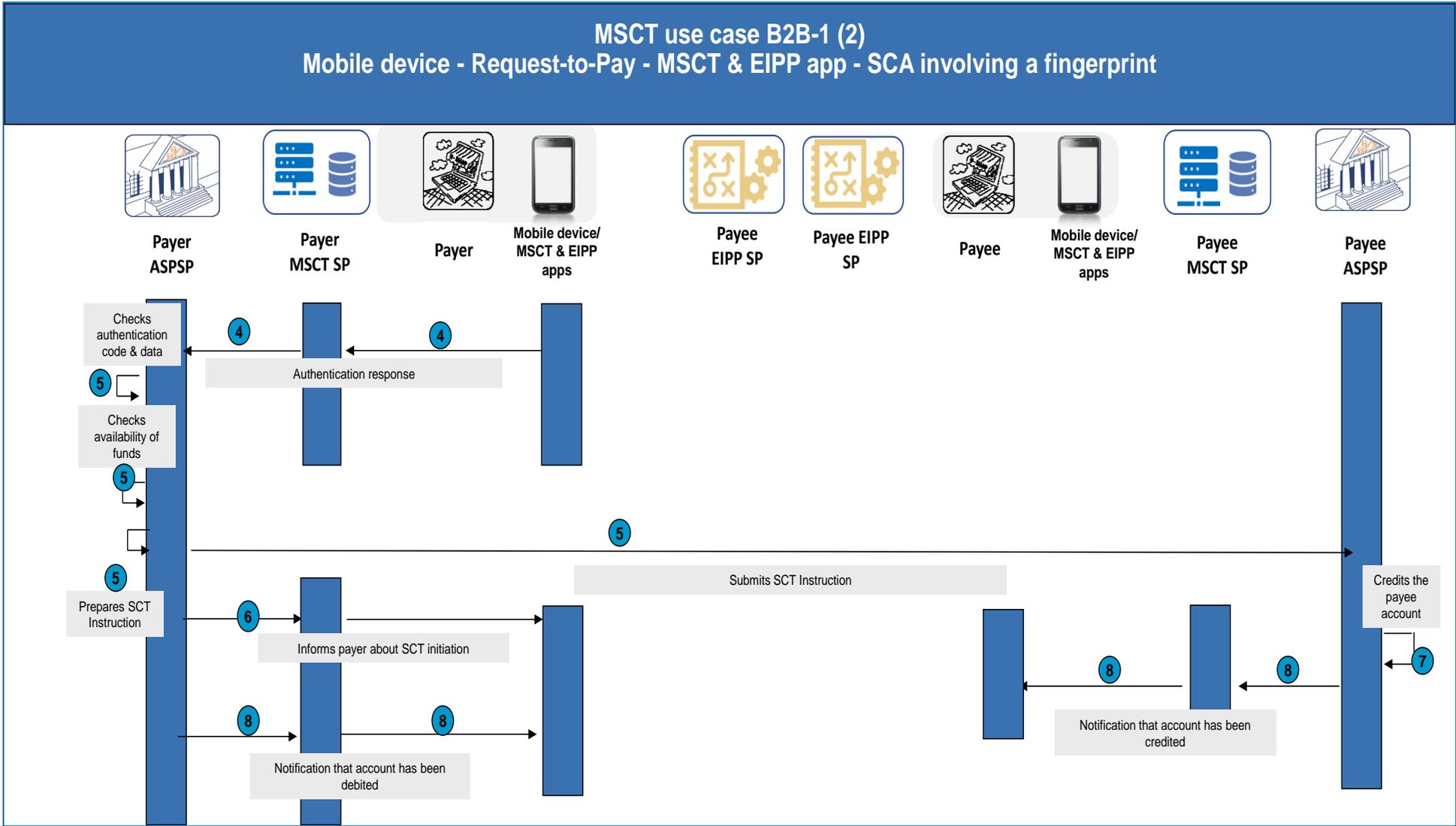


Figure 27: MSCT use case B2B-1



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, the payer and the payee would need to be subscribed to a (potentially different) EIPP solution provider and downloaded a dedicated EIPP application on their mobile devices.
- The payer has activated the EIPP service with the payee through their respective EIPP solution providers. Such activation occurs through a servicing message sent by the EIPP solution provider of the payer to the EIPP solution provider of the payee, that delivers to the payee and their EIPP solution provider all the information required to deliver e-invoices and related Request-to-Pay messages from the payee to the payer.
- The payer and the payee would need to be subscribed to potentially different MSCT services and have downloaded dedicated MSCT applications on their mobile devices including a link to the EIPP application offered by their EIPP solution provider. These MSCT applications are linked to the payer and payee accounts.
- The ASPSPs of the payer and the payee are participants in the chosen MSCT services.
- As a prerequisite, a mobile internet connection is required during the transaction.

Step 1

- The payee sends a payment request message, containing an e-invoice as an annex, to their EIPP solution provider.
- The payee's EIPP solution provider forwards the payment request message to the payer's EIPP solution provider.
- The payer's EIPP solution provider sends the e-invoice and the payment request including an e-invoice reference, transaction amount and IBAN_payee, to the payer.
- The payer can check in their EIPP solution provider application the invoice received.

Step 2

- The payer receives the payment request in their EIPP solution provider application and clicks on the request.
- This opens the MSCT application of their MSCT service provider. (The selection of the ASPSP has already been done during the registration process).
- The MSCT application retrieves and displays the e-invoice reference, transaction amount, payee name and IBAN_payee.
- The SCT instruction including the necessary payment data is transmitted to the payer's ASPSP via the MSCT service provider.

Step 3

- The payer's ASPSP checks the integrity of the SCT instruction.



- Subsequently, the payer's ASPSP sends an authentication request including the payee's name, transaction amount and a challenge to the MSCT application in the mobile device of the payer via the MSCT service provider.

Step 4

- The payee's name, the transaction amount and possibly a personal message are displayed on the mobile device while the payer is invited to present a fingerprint to their mobile device for their authentication.
- Upon successful fingerprint verification by the mobile device, an authentication code is calculated by the MSCT application which is transmitted to the payer's ASPSP via the MSCT service provider.

Step 5

- The payer's ASPSP checks the authentication code and the data received.
- The payer's ASPSP checks the availability of funds on the payer's account
- The payer's ASPSP prepares and submits the SCT transaction to the payee's ASPSP.

Step 6

The payer is informed by their MSCT service provider that the payment has been successfully initiated (information provided by the payer's ASPSP).

Step 7

The payee's ASPSP makes the funds available to the payee merchant.

Step 8

- The payee receives a notification message from their MSCT service provider (information provided by the payee's ASPSP) that the funds related to their payment request have been received.
- The payer receives a notification message from their MSCT service provider that their account has been debited (information provided by the payer's ASPSP).

Notes:

- This example is also valid for SCT Inst. In this case, in step 7 there is a confirmation message sent from the payee's ASPSP to the payer's ASPSP.
- This use case is also valid for C2B.
- In the B2B environment, the MSCT applications could be linked to the e-banking or ERP application, which would require the appropriate agreements.



Analysis MSCT Use case B2B-1	
Interoperability	<ul style="list-style-type: none"> • The payer and the payee may have different MSCT service providers and EIPP solution providers. • The payer and the payee may have different ASPSPs.
Challenges	<ul style="list-style-type: none"> • Standardisation of messages between MSCT service providers (e.g., Payment Request messages, Notification messages, ...). • The notification messages in step 8 are not included in the SCT schemes.

Table 18: Analysis MSCT use case B2B-1

Note: The minimum data elements in the payment request and notification messages are defined in Annex 4.

7.4 Applicability of MSCTs

In the table below the applicability of SCT Inst and SCT payments for MSCTs are shown versus the different payment contexts.

Payment Context	SCT Inst	SCT
Person-to-Person (P2P)	X	X
Consumer-to-Business (C2B)	X	X - but an additional service is needed to offer guarantee of payment
Business-to-Business	X	X - but an additional service is needed to offer guarantee of payment

Table 19: Applicability of MSCTs



8 MSCT transaction aspects

8.1 Introduction

In the following figures, the decomposition of an MSCT into building blocks are illustrated, both for SCT Inst and SCT transactions.

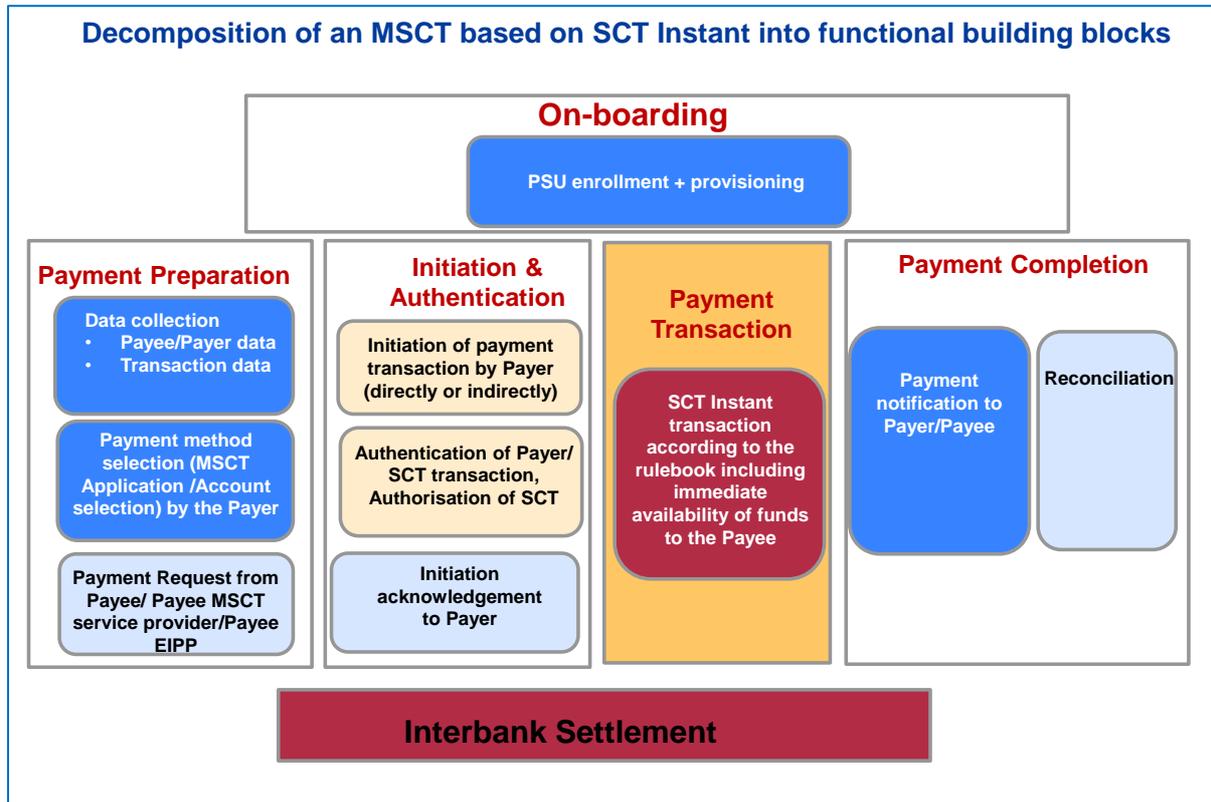


Figure 28: Decomposition of an MSCT based on SCT Inst into building blocks

Dark blue	Light blue	Dark amber	Light amber

The dark amber box in the above is covered by the SCT Inst scheme rulebook [22] and supporting documents ([see https://www.europeanpaymentscouncil.eu/what-we-do/sepa-schemes/sepa-instant-credit-transfer/sepa-instant-credit-transfer-rulebook-and](https://www.europeanpaymentscouncil.eu/what-we-do/sepa-schemes/sepa-instant-credit-transfer/sepa-instant-credit-transfer-rulebook-and)) and falls outside the scope of the MSCT IG. However, they form the basis on which this document is built. The immediacy of payment offered by SCT Inst includes an immediate, irrevocable availability of the funds.

This document focuses on the interoperability outside the inter-PSP space such as between the payer mobile device and the payee equipment (e.g. POI, mobile device), between the payer and their MSCT service provider(s), between the payee and their MSCT service



provider(s)⁵⁹, etc. (see dark blue boxes in the Payment Preparation and Payment Completion phases).

The light blue boxes in the figure are features which may or may not be present in an MSCT based on SCT Inst. This may depend on the payment context (e.g., a Payment Request from the merchant / merchant IP service provider for C2B payments based on consumer-presented data, see Chapters 17 and 18). Since these features are impacting the interoperability of MSCTs, they will be covered in this document.

“On-boarding” (see dark blue box) refers to the registration process of a PSU with an MSCT service provider or a merchant for a specific MSCT service, before using the service for actual payment transactions. Since the security of the on-boarding process is a cornerstone for the trust in MSCT services and for fraud mitigation, specific security requirements are defined in this guidance document (see Chapter 14).

The light amber boxes refer to functionalities which are not impacting the interoperability if different MSCT service providers or different MSCT services for the payer and the payee are involved (see also Chapter 16).

In case of P2P payments, a mobile phone number of the payee may be used which may require the support by the SPL service⁶⁰ (see section 15.3) for the linking with the IBAN_payee.

⁵⁹ In so far that they impact the interoperability of IPs at the POI.

⁶⁰ https://www.europeanpaymentscouncil.eu/sites/default/files/infographic/2018-05/How%20the%20SPL%20service%20works%20%28May%202018%29_1.pdf

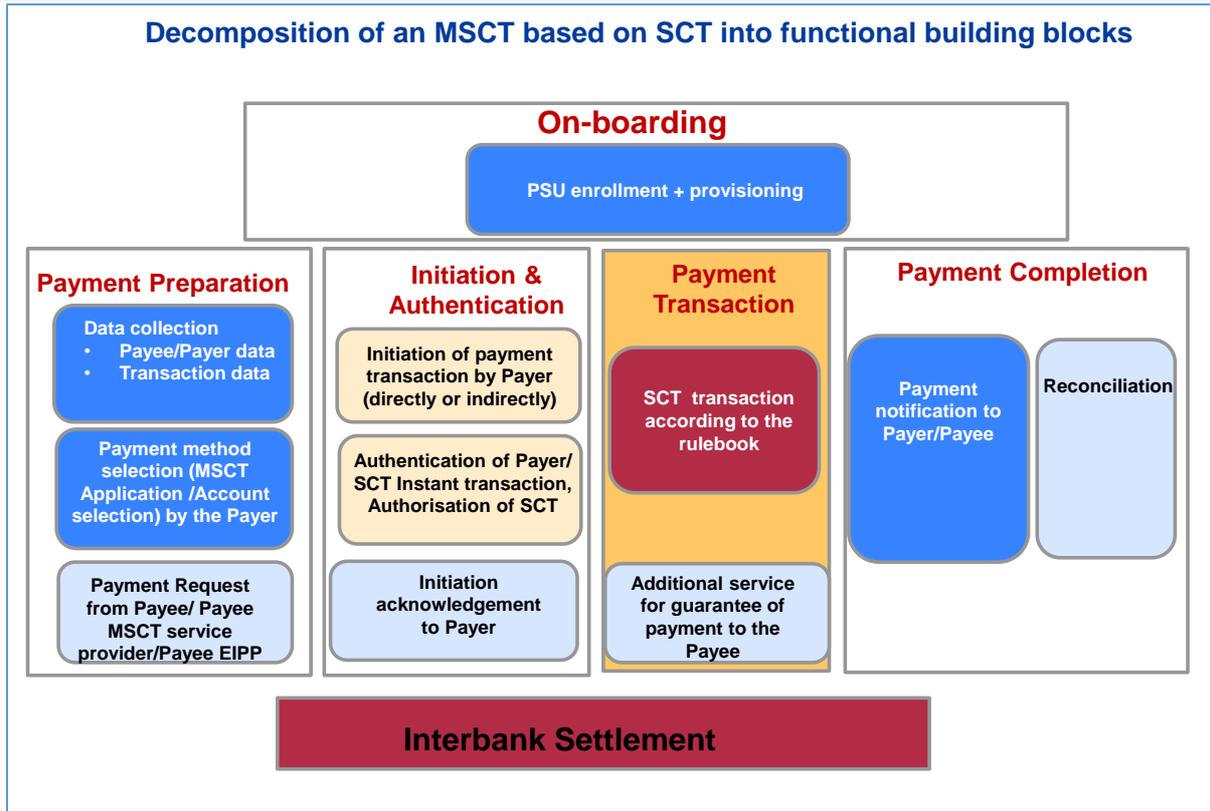


Figure 29: Decomposition of an MSCT based on SCT into building blocks

Dark blue	Light blue	Dark amber	Light amber

The dark amber box in the figure above is covered by the SCT scheme rulebook [17] and supporting documents ([see https://www.europeanpaymentscouncil.eu/what-we-do/sepa-schemes/sepa-credit-transfer/sepa-credit-transfer-rulebook-and-implementation](https://www.europeanpaymentscouncil.eu/what-we-do/sepa-schemes/sepa-credit-transfer/sepa-credit-transfer-rulebook-and-implementation)) and falls outside the scope of the MSCT IG. However, they form the basis on which this document is built. Contrary to an SCT Inst transaction, the SCT scheme does not include an immediate availability of funds to the payee.

This document focuses on the interoperability of MSCTs, based on SCT Inst or SCT, outside the inter-PSP space such as between the payer mobile device and the payee equipment (e.g. POI, mobile device), between the payer and their MSCT service provider(s), between the payee and their MSCT service provider(s)⁶¹, etc. (see dark blue boxes in the Payment Preparation and Payment Completion phases).

The light blue boxes in the two figures above are features which may or may not be present in an MSCT based on SCT Inst or SCT. This may depend on the payment context (e.g., a Payment Request from the merchant / merchant MSCT service provider for C2B payments

⁶¹ In so far that they impact the interoperability of IPs at the POI.



based on consumer-presented data, see Chapter 18). Since these features are impacting the interoperability of MSCTs, they will be covered in this document.

“On-boarding” (see dark blue box) refers to the registration process of a PSU with an MSCT service provider or a merchant for a specific MSCT service, before using the service for actual payment transactions. Since the security of the on-boarding process is a cornerstone for the trust in MSCT services and for fraud mitigation, specific security requirements are defined in this guidance document (see Chapter 14).

The light amber boxes refer to functionalities which are not impacting the interoperability if different MSCT service providers or different MSCT services for the payer and the payee are involved (see also Chapter 16).

In case of P2P payments, a mobile phone number of the payee may be used which may require the support by the SPL service⁶² (see section 15.3) for the linking with the IBAN payee. On-boarding refers to the process of registration of a payer (consumer) with an MSCT service provider (including ASPSPs, PISPs) or a merchant.

The following sections in this chapter will focus on the different aspects of the blocks “Initiation and Authentication” and “Payment Completion” in the figures above, while aspects related to the block “Payment Preparation” are treated in Chapters 17 and 18.

8.2 Payer authentication

The term payer authentication in an MSCT transaction refers to the methods used for the authentication of the payer/consumer.

The usage of a payer authentication method is related to the transaction risk management and is for MSCT transactions at the discretion of the payer’s ASPSP, in accordance with PSD2 [5] and the Commission Delegated Regulation, supplementing PSD2, with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (also referred to as “RTS”, see [6]).

The mobile environment offers already today a number of features which can be utilised for MSCTs with respect to customer identification / authentication. This includes for example the keyboard of the mobile device or a biometric sensor (e.g., fingerprint, facial recognition, voice recognition, heartbeat, iris scan, etc. (see for instance [78] and [95])).

⁶² https://www.europeanpaymentscouncil.eu/sites/default/files/infographic/2018-05/How%20the%20SPL%20service%20works%20%28May%202018%29_1.pdf



8.2.1 Consumer Device User Verification Method

For MSCTs, the payer authentication method used typically involves a Consumer Device User Verification Method⁶³ (CDUVM). It is entered by or captured from the payer on the mobile device. Typical methods used include

- Biometrics, verified by the mobile device OS.
 - Mobile code⁶⁴: entered on the mobile device.
 - The verification of the mobile code is done by an application on the mobile device;
- or
- Implicit validation of the correct entry of the mobile code through a cryptographic derivation, verified on-line by the payer's ASPSP.

Different types of biometrics may be used for mobile payments such as fingerprint, facial recognition, etc. More information on the usage of biometrics for payments may be found in [78] and [95].

On a mobile device, a distinction may be made between a CDUVM verified by the ASPSP, and a so-called "shared" CDUVM, which is a CDUVM used by multiple mobile (payment) applications accessible via the mobile device. This "shared" CDUVM may be verified by another mobile service provider than a PSP, in which case there is a formal agreement needed between the two parties. A similar approach has been taken for the Customer Device Cardholder Verification Method (CDCVM) by EMVCo (see [15]). The reader is referred to Chapter 13 for specific guidelines for CDUVMs.

The usage of a CDUVM is often linked to the transaction risk management and may be used as one of the "authentication elements" in the context of Strong Customer Authentication (see section 8.3), being it a knowledge (e.g., mobile code) or an inherence factor (biometrics).

For MSCTs, other factors, such as the consumer choice, may influence the usage of a CDUVM.

8.2.2 Authentication

For the authentication the following methods may be distinguished:

Static authentication method

This method uses a static authenticator such as a log-in, identification number, a passcode, password, mobile code, etc. The static authenticator is typically provided (as a knowledge factor) through manual entry by the payer on the mobile device.

⁶³ ISO 12812-1 defines "user verification method" as a method verifying that the person (payer) who uses the mobile financial service is the legitimate customer of the mobile financial service provider

⁶⁴ For security reasons, in case of a mobile code, this is a dedicated mobile code (also referred to as mobile PIN, mobile passcode, etc.).



- The static authenticator may be verified off-line in the mobile device (e.g. by a dedicated MSCT or Authentication application on the mobile device);
- The static authenticator may be verified on-line in an ASPSP environment (e.g. via the on-line banking system).

Dynamic authentication method

This method uses a dynamic authenticator which may be a One Time Password (OTP) or the result of a challenge / response mechanism.

One-time password (OTP)

The following methods may be distinguished:

- An OTP generated by the ASPSP and sent to the payer via a different communication channel which is manually entered by the payer on their mobile device and verified online by the ASPSP;
- An OTP generated by a dedicated (separate) payer's authentication device and which is entered by the payer on their mobile device and verified online by the payer's ASPSP.

The OTP is considered as a proof of possession by the payer of the device on which the OTP was received or generated.

Challenge/response method

In case a dedicated MSCT or a separate Authentication application⁶⁵ is accessible via the mobile device, a dynamic authentication method (e.g., challenge/response method secured by a dedicated key in the MSCT or Authentication application – possession factor) is initiated by the MSCT service provider/ASPSP/Authentication service provider and is handled automatically by this application on the mobile device. Typically, the payer is requested to enter their CDUVM (e.g., mobile code, fingerprint, etc. – knowledge or inherence factor) once during the MSCT transaction process. The response is considered as a proof of possession by the payer of the device on which the response was generated.

In case an Authentication Application is used for MSCTs for the authentication of the payer, there needs to be a delegation of authority by the payer's ASPSP to the Authentication Service Provider, in case the latter is a different entity than the ASPSP.

⁶⁵ A dedicated application issued by an Authentication Service Provider to support the authentication process for mobile services, including an MSCT payment transaction. Typical examples are eID-based solutions. The Authentication Application is accessed via the mobile device and may be hosted on the mobile device or on a remote server.



More information on the usage of an Authentication application may be found in [51].

8.3 Strong Customer Authentication (SCA)

PSD2 [5] defines in Article 4 Strong Customer Authentication as “*an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data*”.

Article 97 of the PSD2 [5] mandates the usage of strong customer authentication for MSCT transactions, except for the exemptions (Article 98)⁶⁶ defined in Article 12 [Unattended terminals for transport fares and parking fees], Article 13 [Trusted beneficiaries], Article 14 [Recurring transactions], Article 15 [Credit transfers between accounts held by the same natural or legal person] and Article 17 [Secure corporate payment processes and protocols] of the RTS [6]. However, the payer’s ASPSP may still apply SCA in case of risk for these exemptions.

Note: For payer convenience, the usage of a CDUVM verification should be combined with the strong customer authentication.

8.4 Transaction authentication and dynamic linking

The usage of a transaction authentication method is related to the transaction risk management and is for MSCT transactions at the discretion of the payer’s ASPSP, in accordance to PSD2 [5] and the RTS [6].

As transaction authentication methods, similar mechanisms as those described in the previous section may be used. Typically, the transaction related data that is input to the authentication mechanism are the transaction amount, the payee and their account and possibly a time factor.

Moreover, the payer authentication is often a combined method with the transaction authentication for payer convenience, which implicitly provides payer consent. As an example, a challenge / response method as described in section 8.2 may involve transaction related data as well as a payer authentication (CDUVM)⁶⁷.

For MSCTs that are conducted as electronic remote transactions⁶⁸, whereby the connectivity via mobile internet from the payer’s mobile device is used to conduct the transaction, Article 97(2) of the PSD2 [5] applies in this context.

⁶⁶ For those MSCT transactions that may be considered as contactless payments, the exemption mentioned under Article 11 of the RTS would apply. This needs to be clarified through the replies to the EBA Q&A questions 2020_5365 to 2020_5367.

⁶⁷ see also requirement 12 in <https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/api-evaluation-group-recommended-functionalities-psd2rts>

⁶⁸ Subject to further clarification of EBA on the questions 2020_5365 to 2020_5367.



This Article mandates for electronic remote payment transactions, that payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee, except for the exemptions (Article 98), defined in Article 16 [Low value transactions] and Article 18 [Transaction risk analysis] of the RTS [6].

Strong customer authentication with dynamic linking requires that:

- “...The authentication code generated shall be specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction.
- the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the payee agreed to by the payer.
- Any change to the amount or the payee shall result in the invalidation of the authentication code generated.” (Article 5 of the RTS [6][6]).

Further guidance on strong customer authentication and dynamic linking are provided in the EBA opinion document on the implementation of the RTS (see [10] in Annex 1).

The combination of a dynamic authentication method (see section 8.2), including the transaction amount and payee name/IBAN_payee with a CDUVM provided by the payer (see section 8.2) is a means to enable “strong customer authentication with dynamic linking”. Examples are also provided in [51].

8.5 Transaction risk analysis

Transaction risk analysis refers to the use of statistical models via transaction, location, device and profile data, without active payer participation, in the decision-making process for strong customer authentication (see also Article 18.3 in [6]) by the payer’s ASPSP. This is sometimes referred to as Risk-Based Authentication (RBA).

It may include:

- Verification of characteristics of the mobile device being used by the payer,
- Verification of the location of the mobile device, e.g., as per a geo-location facility on the mobile device,
- Verification of the true IP address of the mobile device being used.

Transaction specifics may include amount, date, payee/merchant name, etc.

Notes:

- To perform a transaction risk analysis in case a PISP is involved, the necessary data needs to be transmitted to the payer’s ASPSP.
- It is to be noted that some of the data or parameters used for transaction risk analysis, may be subject to data protection regulation such as the GDPR (see [7]).



Additional considerations may be taken into account such as:

- The payer is a repeat customer and was authenticated on previous occasions;
- The payer is using the same account;
- The payer is requesting delivery of the goods or services to the same address.

All these factors could serve as input to the transaction risk analysis for the application of the exemption specified in Article 18 of the RTS [6] and could be used for fraud mitigation purposes. It should however be noted, in case a PISP is involved for the initiation of an MSCT, that the necessary data to perform transaction risk analysis should be transferred from the PISP to the payer’s ASPSP to enable the ASPSP to apply an exemption.

8.6 MSCT risk management

The purpose of this section is to present risk management parameters for MSCTs that can be applied if an MSCT application or an Authentication application on the mobile device is used to conduct an MSCT. The risk parameters are set up at the discretion of the service provider (e.g., MSCT service provider or Authentication service provider). This involves counters and limits that are described below.

Depending on the particular MSCT service, the MSCT dedicated data may range from pure payment credentials which may or may not be stored on the mobile device (e.g., in a wallet) to an Authentication application or a dedicated MSCT application. Obviously, the applicability of MSCT risk parameters is dependent on the type of dedicated MSCT data used, as shown in the table below. It is at the discretion of the MSCT service provider to make a choice on which parameters will be supported⁶⁹ or to add any other risk parameter they seem to be appropriate. The risk parameters are described in further detail below.

Risk parameters	MSCT data type		
	MSCT application	Authentication application	Credentials
CDUVM Try Limit and Counter	X	X	
Transaction Amount Limit	X		
No-SCA Limit	X		X
Consecutive No-SCA Limit and Counter	X		X
Cumulative No-SCA Limit and Accumulator	X		X

Table 20: Risk parameters for MSCTs

⁶⁹ subject to an agreement with the payer’s ASPSP in case the MSCT service provider received delegation of authority for strong customer authentication.



Note: The last three counters are usually implemented in the payer's ASPSP back-end but may be implemented in the MSCT application in case of full delegation of all functions to the MSCT application, if present.

8.6.1 CDUVM Try Limit and Counter

The *CDUVM Try Limit* is a parameter indicating the maximum number of consecutive incorrect CDUVM trials allowed (see section 8.2).

The number of CDUVM trials is recorded and the *CDUVM Try Counter* represents the remaining number of trials allowed. The *CDUVM Try Counter* is reset to the *CDUVM Try Limit* after a successful CDUVM verification.

If the *CDUVM Try Counter* is equal to zero, indicating no remaining CDUVM trials are left, all further MSCT transactions requiring a CDUVM and optionally all MSCT transaction or authentications are refused until the *CDUVM Try Counter* is reset by the service provider. Optionally, the service provider may implement a fall-back CDUVM method for consumer convenience.

The value of the *CDUVM Try Limit* is set in the MSCT application or in the Authentication application as appropriate, and defined by the MSCT service provider.

8.6.2 Transaction Amount Limit

A *Transaction Amount Limit* may be used to mitigate risks and additionally allows control of high value transactions.

The value of the *Transaction Amount Limit*⁷⁰ is set in the MSCT application and defined by the MSCT service provider or by the payer but subject to the MSCT service provider limit.

When the transaction amount is above the *Transaction Amount Limit*, the MSCT transaction initiation is refused.

8.6.3 No-SCA Limit

The *No-SCA Limit* is a risk management parameter indicating the maximum value of a transaction which does not require an SCA according to PSD 2 [5] (see section 8.3).

Transactions for which the value is less than, or equal to, the *NO-SCA Limit* are typically low risk payments (e.g., low value) where convenience is important and the usage of an SCA may not be required (see Article 16 of the RTS [6]). Transactions for which the value is greater than the *No-SCA Limit* require the usage of an SCA.

⁷⁰ The MSCT *Transaction Amount Limit* may be different to the limit that the payer's ASPSP may apply on their side when a transaction initiation is received. However, the MSCT Transaction Amount Limit should not exceed the payer's ASPSP limit.



The value of the *No-SCA Limit* is set by the payer's ASPSP and shall be compliant with the dedicated Regulation (see [5] and [6]).

8.6.4 Consecutive No-SCA Limit and Counter

The *Consecutive No-SCA Limit* is a parameter indicating the number of consecutive MSCT transactions which can be performed before an SCA according to PSD 2 [5] is required.

The total number of No-SCA transactions is recorded in the *Consecutive No-SCA Counter* which is managed by the payer's ASPSP. When a transaction is performed and the resulting *Consecutive No-SCA Counter* is greater than the *Consecutive No-SCA Limit*, then an SCA (see section 8.3) is required.

The value of the *Consecutive No-SCA Limit* is set and defined by the payer's ASPSP in accordance to Article 16 of the RTS [6] and taking into account:

- The risk of fraudulent transaction (e.g. in case of loss or theft of the mobile device).
- The convenience from the payer's perspective.

and is used in conjunction with the *No-SCA Limit* risk parameter.

The *Consecutive No-SCA Counter* is managed by the payer's ASPSP and will be reset after the successful SCA verification.

8.6.5 Cumulative No-SCA Limit and Accumulator

The *Cumulative No-SCA Limit* is a parameter indicating the maximum total value of MSCT transactions (amounts) which can be performed before an SCA in accordance to PSD 2 [5] is required.

The total amount of No-SCA transactions is recorded in the *Cumulative No-SCA Amount Accumulator* which is managed by the payer's ASPSP. When a transaction is performed and the resulting *Cumulative No-SCA Amount Accumulator* reaches the *Cumulative No-SCA Limit*, then an SCA (see section 8.3) is required.

The value of the *Cumulative No-SCA Limit* is set and defined by the payer's ASPSP in accordance to Article 16 of the RTS [6] and taking into account:

- The risk of fraudulent transaction (e.g. in case of loss or theft of the mobile device);
- The credit risk;
- The convenience from the payer's perspective;

and is used in conjunction with the *No-SCA Limit* risk parameter.

The *Cumulative No-SCA Amount Accumulator* is managed by the payer's ASPSP and will be reset after the successful SCA verification.



8.7 Acknowledgements / Notifications

The following messages can be identified in that respect:

- Acknowledgement of receipt to the payer by their MSCT service provider of the instruction for MSCTs based on SCT involving payee-presented data;
- Acknowledgement of receipt to the payee by their MSCT service provider of the payment request for MSCTs based on SCT involving payee-presented data;
- Notification of reject/successful/unsuccessful transaction to the payee by their MSCT service provider;
- Notification of reject/successful/unsuccessful transaction to the payer by their MSCT service provider.

In addition, all messages related to exception handling which are in the technical interoperability space should be addressed as well.

All these technical interoperability messages will be analysed in detail in Chapters 17 and 18 in this document.

8.8 Transaction logging in the MSCT application

Each MSCT application on the mobile device could have its own transaction logging function to allow the payer to check the latest MSCTs initiated. The transaction details should be stored in a log file, accessible by the MSCT application. At a minimum, the last 10 transactions initiated should be displayable to the payer while the number of transactions stored in the log file remains at the discretion of the MSCT service provider. Hereby a dedicated flag could be implemented to indicate whether the transaction was acknowledged, successful or failed. Every time an MSCT is initiated, a new record⁷¹ is created and the transaction logging is updated whereby the chronological order is respected.

The record in the log file could contain the following data:

- Transaction date and time;
- Transaction amount;
- Transaction identifier⁷²;
- Payer IBAN
- Payee identification (e.g., name/trade name).

An access control to this transaction logging display may be implemented (e.g., by requesting a CDUVM). Payers may be allowed to enable or disable this access control themselves.

⁷¹ Considering the integrity and security data aspect, the data within the MSCT transaction log is not considered to be protected.

⁷² This is an end-to-end reference which enables the identification of the MSCT transaction by the payer and the payee.



9 Generic security guidelines for the PSU-to-PSP space

9.1 Introduction

This chapter deals with the security in the “PSU-to-ASPSP/MSCT service provider space/PISP space” for MSCTs based on SCT Inst or SCT payments. This includes the communication between the payer and their ASPSP/MSCT service provider/PISP and the communication between the payee and their ASPSP/MSCT service provider/PISP.

9.2 Threats

The following generic threats may be considered in relation to MSCTs in this space:

Ref.	Threat
T1	<p>Payer impersonation</p> <p>This occurs when an attacker poses as the payer when transmitting the SCT (Instant) Instruction to the payer ASPSP/MSCT service provider/PISP. The attacker may pose as a genuine payer by initiating an MSCT to the payer ASPSP/MSCT service provider/PISP with a valid IBAN.</p>
T2	<p>Spoofed payer ASPSP / MSCT service provider/PISP towards payer</p> <p>This occurs when an attacker poses as the genuine payer ASPSP/MSCT service provider/PISP towards the payer in order to</p> <ul style="list-style-type: none"> • Intercept SCT (instant) instructions; • Capture sensitive data (e.g. credentials) or other personal data from payers; • Create fraudulent MSCT related messages⁷³ or information to the payer.
T3	<p>Tampering with SCT (Instant) instruction messages</p> <p>An SCT (Instant) instruction message may be deliberately and maliciously tampered with while in transfer between the parties involved. An attacker may intercept the messages and modify their content.</p>
T4	<p>Tampering with MSCT interoperability messages (i.e. MSCT related messages such as notification messages, acknowledgements, etc.)</p> <p>This message may be deliberately and maliciously tampered with while in transfer between the parties involved. An attacker may intercept the messages and modify their content.</p>
T5	<p>Tampering with account statement information</p> <p>Account statement information may be deliberately and maliciously tampered with while in transfer between the payee ASPSP and the payee, or between the payer ASPSP and the payer.</p>
T6	<p>Tampering with R-transaction messages or Payment Request messages</p> <p>These messages may be deliberately and maliciously tampered with while in transfer between the parties involved. An attacker may intercept or modify the message content or cancel the message.</p>

⁷³ For more details on these messages see Chapter 19.



T7	<p>Unauthorised access to MSCT services of ASPSP/MSCT service provider/PISP Unauthorised access to the MSCT service of an ASPSP / MSCT service provider occurs when an attacker tries to perform unauthorised operations on these MSCT services.</p>
T8	<p>(D)DoS of the MSCT service of the ASPSP/MSCT service provider/PISP A (distributed) denial of service of the MSCT service of an ASPSP/MSCT service provider/PISP occurs when an attacker exhausts the MSCT service infrastructure resources (e.g., disk space, network bandwidth, CPU, etc.); rendering it unusable and thus negating effective service.</p>
T9	<p>Repudiation by payer</p> <ul style="list-style-type: none"> • A payer may refute SCT (Instant) Instructions which they have previously initiated; • A payer may deny receipt of MSCT related messages from the payer ASPSP/MSCT service provider.
T10	<p>Repudiation by payer ASPSP/MSCT service provider/PISP</p> <ul style="list-style-type: none"> • A payer ASPSP/MSCT service provider/PISP may refute the receipt of an SCT (Instant) Instruction; • A payer ASPSP/MSCT service provider/PISP may refute sending/ deny the receipt of MSCT related messages.
T11	<p>Disclosure of payer or payee personal data/sensitive payment data This occurs when sensitive personal information about the payer or the payee becomes known to anyone other than the intended parties. The attacker may intercept and capture the exchanged data (e.g., credentials or name, address, phone number, IBAN, etc.) (see also T2, T7 and T13).</p>
T12	<p>Timing attacks (message, confirmation, etc.) This occurs when there are intentional delays in the delivery of the messages or if there is de-synchronisation between two parties and time differences are leading to time-outs.</p>
T13	<p>Spoofed payee ASPSP/ PISP/MSCT service provider towards payee This occurs when an attacker poses as the genuine payee ASPSP/PISP/MSCT service provider towards the payee in order to</p> <ul style="list-style-type: none"> • Create fraudulent MSCT related messages or information to the payee; • Capture sensitive data (e.g. credentials) or other personal data from payees.
T14	<p>Payee impersonation This occurs when an attacker poses as the payee when transmitting the transaction data to their MSCT service provider, PISP or the payer. The attacker may pose as a genuine payee when creating fraudulent QR-codes, payment request messages, MSCT related messages, etc.</p>



T15	<p>Repudiation by payee</p> <ul style="list-style-type: none"> • A payee may refute payment request messages which they have previously initiated; • A payee may deny receipt of MSCT related messages from the payee ASPSP/MSCT service provider/PISP.
T16	<p>Repudiation by payee ASPSP/MSCT service provider/PISP</p> <ul style="list-style-type: none"> • A payee ASPSP/MSCT service provider/PISP may deny the receipt of a payment request message; • A payee ASPSP/MSCT service provider/PISP may refute the sending/deny the receipt of MSCT related messages.

Table 21: MSCT threats list in the PSU-to-PSP/MSCT service provider space

9.3 Generic security guidelines

To address the threats described in the previous section, the following generic security guidelines should be followed as mitigating measures.

Ref	Security guidelines
G-SG1	All stored personal data about payers, payees and sensitive payment data related to SCT (Instant) transactions or R-transactions and related messages they hold should be protected in strict accordance with the legal and regulatory requirements [5] and [7] and used solely for the purposes explicitly allowed by the respective "data subject" (natural person, see [7]).
G-SG2	A secure communication channel between the payer and the payer ASPSP/MSCT service provider/PISP, should be made available. Examples include a website connection via TLS1.2 or higher (according to the state of the art) or a dedicated app with endpoint security on the payer's mobile device.
G-SG3	A secure communication channel between the payee and the payee ASPSP/MSCT service provider/PISP, should be made available. Examples include a website connection via TLS1.2 or higher (according to the state of the art) or a dedicated app with endpoint security on the payee's mobile device.
G-SG4	The payer ASPSP/MSCT service provider/PISP should provide the payer access to the MSCT instruction functionalities only through strong customer authentication (see section 8.3) using an authentication code that is dynamically linked to the transaction amount and the payee unless the payer's ASPSP decides to apply an exemption in accordance to the PSD 2 [5] and RTS [6] (see Chapter 8).
G-SG5	All personalised security credentials issued to the payer should meet the security requirements and be protected according to the requirements specified in the RTS [6].



G-SG6	The payer ASPSP/MSCT service provider/PISP should protect the messages to the Payer in order to ensure the origin and integrity of the message and the confidentiality of sensitive payment data as appropriate. In addition, the payer ASPSP/MSCT service provider/PISP should take measures to ensure the authenticity of the payer as receiver of the message (e.g., using the same session as the SCT (Instant) instruction).
G-SG7	Given the importance of security, entities with direct relationships with payers should promote security and data protection awareness, training and education wherever possible including warnings for phishing attacks, encouragements to adopt security measures on their consumer device, including firewalls, antivirus, antispyware, etc. Moreover, the payers should adequately protect their personal security credentials.
G-SG8	The payee ASPSP/MSCT service provider/PISP should protect the messages to the payee in order to ensure the origin and integrity of the message, and the confidentiality of sensitive payment data as appropriate. In addition, the payee ASPSP/MSCT service provider/PISP should take measures to ensure the authenticity of the payee as receiver of the message.
G-SG9	<p>Given the importance of security, entities with direct relationships with payees should promote security and data protection awareness, training and education wherever possible including warnings for phishing attacks, encouragements to adopt security measures in their environments (platforms, devices and systems), including firewalls, antivirus, antispyware, etc. Moreover, the payees should adequately protect their personal security credentials.</p> <p>Merchants should handle sensitive payment data of relevance for (Instant) Credit Transfers in accordance with the PSD2, the RTS and the EBA Guidelines (see Annex 1).</p>
G-SG10	The secure communication between the entities involved in an MSCT should be kept open only for the minimum time needed to perform the action concerned.
G-SG11	Audit trails should be generated for all relevant operations. They should include sufficient information to fully trace back a given operation and shall be stored in a secure way such that unauthorised addition is prevented and that tampering or deletion of trails is detectable.
G-SG12	A trusted time source is recommended to be used to ensure reasonable time accuracy on exchanged timestamps and audit trails.
G-SG13	All service providers should implement internal measures (e.g., separation of good/bad traffic; shut off of certain information streams) or external measures (e.g., multiple ISP contracts, scrubbing service) against (D)DoS attacks.



G-SG14	The payer ASPSP/payee ASPSP/MSCT service provider/PISP should implement adequate fraud monitoring systems to detect fraudulent SCT (Instant) transactions/R-transactions and MSCT related messages.
---------------	---

Table 22: Overview security guidelines for MSCTs in the PSU-to-PSP/MSCT service provider space

9.4 Overview

The table below shows the relationships between the threats identified (see **Table 21**) and the security guidelines (see **Table 22**).



	Threats															
Generic Security Guidance	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16
G-SG1	x						x				x			x		
G-SG2	x	x	x	x	x	x					x					
G-SG3				x	x	x					x		x	x		
G-SG4	x					x			x							
G-SG5	x										x					
G-SG6		x		x	x	x					x					
G-SG7	x		x	x	x	x					x					
G-SG8				x	x	x					x		x			
G-SG9				x	x	x					x			x		
G-SG10	x	x	x	x	x	x	x	x				x	x			
G-SG11							x		x	x		x			x	x



G-SG12										x		x				x
G-SG13								x								
G-SG14	x	x	x	x	x	x	x						x			

Table 23: Mapping security guidelines onto threats for MSCTs



10 Security considerations for the payer-to-payee space

In this chapter different technologies used for the interface between the payer and the payee are considered.

10.1 Proximity technologies

Different proximity technologies have entered the market over the past years to conduct mobile payments. In this document the technologies most widely used, being QR-codes, BLE and NFC are briefly described below. It is noticed that other new technologies such as ultrasonic, BLE beacons, etc., are emerging but the payment market adoption is still in its early days. They are therefore not described in this document.

10.1.1 QR-code

A two-dimensional code consists of modules arranged in a square pattern on a white background. A Quick Response (QR) code is an example of a 2D code as specified in ISO/IEC 18004 [72]. In the context of MSCTs, the QR-code is used as a means of payment initiation, in one of two modes:

- Payee-presented QR-code - where the code contains data to identify the payee and transaction
- or
- Payer-presented QR-code – where the code contains data to identify the payer.

In the case of a payee-presented QR-code, the payer needs to have an MSCT application or another application linked to the MSCT application on their mobile device that has the capability of scanning the QR-code of the payee. Typically, from this QR-code the data will be retrieved to enable the initiation of the MSCT using the MSCT application.

In the case of a payer-presented QR-code, the payer can make purchases using data associated with themselves or their account and previously provisioned to their mobile device. This data may range from payer identification data, over credentials to a token which are used to calculate a QR-code (static or dynamic). The consumer typically has to select the QR-code option within their MSCT application, which will result in the display of the QR-code on the mobile device. The QR-code is scanned by the payee at the time of payment to complete the purchase.

A QR-code may contain both sensitive and non-sensitive payment data that can be used by different entities involved in the processing of the MSCT transaction.

A QR-code code may be static, e.g., payee account data and related payment details for a fixed transaction amount (typical use case of a transport ticket) or may be dynamic to initiate/identify a single specific MSCT transaction (e.g., at a POI).

Tampering a QR-code data may lead to fraudulent transactions or data leakage. Therefore the sensitive payment data in the QR-code should be adequately protected while also the integrity of the data elements in the QR-code should be ensured to avoid any service disruptions.



Non-sensitive data may be related to the application information such as, name, download url, etc. - this kind of data can remain in clear, to be available for a plain QR-code scanner also for marketing or user information purposes.

Below a more detailed analysis is made for each of the two modes used for MSCTs.

Payee-presented QR-codes

Proxy and payload information that is present “in clear” in the QR-code needs an integrity protection to avoid manipulations with the intention to initiate fraudulent transactions (e.g., to a fake payee or with a wrong transaction amount).

Depending on the outcome of EBA Q&A 5477, the IBAN of the payee, if present “in clear”, may also require additional security protection outside the inter-PSP space, e.g. in the QR-code.

It should further be noted that in certain countries (e.g., France, Sweden, ...), there are recommendations to protect the IBAN outside the inter-PSP space. This means that in some countries it is recommended that the IBAN is not included “in clear” into the payee-presented QR-code.

In addition, to protect the data contained in the QR-code, the MSCT application on the payer’s mobile device must enforce a properly encrypted and authenticated connection to the payer’s MSCT service provider (as already specified in Chapter 9).

Payer-presented QR-codes

Customer IDs, IBANs and proxies that are present “in clear” in the QR-code need an integrity protection to avoid mistakes with the initiation of transactions (e.g. using the wrong payer).

The CustomerID might be a payer credential (e.g. for access to online banking system). Capture of the CustomerID and IBAN could lead to impersonation attacks and initiation of fraudulent transactions (see for example [25]) and reputational damage while also contaminating other payment instruments such as SDD. Depending on the outcome of EBA Q&A 5476, if the CustomerID is considered to be sensitive payment data, it needs to be properly protected to ensure its confidentiality.

Depending on the outcome of EBA Q&A 5477, the IBAN of the payer may also require additional security protection outside the inter PSP space, e.g. in the QR-code.

It should further be noted that in certain countries (e.g., France, Sweden, ...), there are recommendations to protect the IBAN outside the inter-PSP space. This means that in some countries it is recommended that the IBAN is not included “in clear” into the payer-presented QR-code.



Also the link between the CustomerID and the IBAN should be guaranteed and the correct generation of the payer-presented QR-code ensured – in other words appropriate security measures should be applied by the entity/application creating the QR-code.

If the payer-presented QR-code is static (e.g., a static token) the same risk as described above applies, namely it could lead to impersonation attacks and initiation of fraudulent transactions (see for example [25]) and reputational damage.

In addition, to protect the data contained in the QR-code, the MSCT application on the payee's POI must enforce a properly encrypted and authenticated connection to the payee MSCT service provider (as already specified in Chapter 9).

10.1.2 NFC

NFC (Near Field Communication) is a contactless protocol for mobile devices specified by the NFC Forum for multi-market usage and by EMVCo for mobile card payment applications. NFC Forum specifications (see [81]) are based on ISO/IEC 18092 [73] but have been extended for harmonisation with EMVCo and interoperability with ISO/IEC 14443 [71] infrastructures.

NFC is a radio frequency technology operating within the RF band of 13.56 MHz at rates ranging from 106 to 424 kbit/s. It operates at very short ranges of up to 4 cm ("proximity") so that the user has to perform a voluntary gesture to initiate a communication between two devices by approaching them.

Each full NFC-enabled device can work in three modes:

- NFC card emulation: enabling the devices to act like smart cards (either using a Secure Element, or Host Card Emulation).
- NFC reader/writer: enabling the device to read information stored on NFC tags embedded in labels or smart posters. NFC tags are passive data stores which can be read, and under some circumstances written to, by an NFC device.
- NFC peer-to-peer: enabling two NFC-enabled devices to communicate with each other to exchange information in an ad-hoc fashion.

The NFC Data Exchange Format (NDEF) is a standardised data format maintained by the NFC Forum⁷⁴ that can be used to exchange information in reader/writer or peer-to-peer mode.

In the context of MSCT, if a mobile device OS only allows operation in NFC reader mode⁷⁵, the NFC technology could be utilised uni-directionally to read data from an NFC tag, e.g. merchant name and IBAN. If allowed by the mobile device OS, the NFC technology could be utilised for a bi-directional exchange of payer/payee identification and transaction data.

⁷⁴ <https://nfc-forum.org/product/nfc-data-exchange-format-ndef-technical-specification/>

⁷⁵ An example is the Core NFC framework of iOS 11.



The usage of the NFC technology for mobile payments remains still somewhat challenging since terms and conditions for accessing the NFC antenna might apply on certain mobile phone platforms (see also Chapter 22).

10.1.3 Bluetooth and Bluetooth Low Energy

Bluetooth

Bluetooth is an industry standard according to IEEE 802.15.1 for bidirectional data transmission between devices over relatively short distances using radio technology. They may be operated worldwide without approval but robustness against interference (e.g., by WLANs or cordless telephones) needs to be implemented⁷⁶. The actual achievable range depends not only on the transmission power but also on several further parameters such as for example, the sensitivity of a receiver and the designs of the transmitting and receiving antennas used by radio communication modules, or obstacles between transmitter and receiver. There are different range classes: Class 1 (max. 100 m), Class 2 (max. 10 m), Class 3 (max. 1 m).

Pairing

The establishment of a connection always takes place under the protocol architecture according to the specifically supported Bluetooth release version. A connection can originate from any Bluetooth enabled device. As soon as Bluetooth devices are put into operation, the individual Bluetooth controllers identify themselves within two seconds. Since this connection time for payment application at the POI is much too long, currently only the variant "Bluetooth Low Energy (BLE)" is applied in payment contexts.

Bluetooth Low Energy

Bluetooth Low Energy (BLE), is a radio technology with which devices in an environment up to about 10 meters can be networked. Compared to "classic" Bluetooth, BLE offers significantly shorter connection times. Based on the protocol Bluetooth version Low Energy V4.0 (and later) a "connectionless" (non-statically paired) operation can be established in only 3 ms and data transmission can be completed after 6 ms.

BLE transmissions can be made secure against unauthorised intrusion if they are operated as a connection with multi-level dynamic key allocation. Static key assignment limits security. When the key is transmitted, exactly this part of the communication is particularly at risk, since only the successful exchange of the key protects a BLE connection.

Unlike NFC, with radio ranges of typically < 10 cm, BLE has ranges of many meters, depending on its range class. This causes practical problems for use at the POIs, as several mobile devices can be in the reception range of the POI. As a consequence, an MSCT payment must be explicitly confirmed by the consumer on the mobile device once the connection has been successfully established.

⁷⁶To achieve robustness against interference, frequency hopping is used, in which the frequency band is divided into 79 channels at 1 MHz intervals, which are changed up to 1600 times per second.



In analogy to NFC technology (see below), the usage of the BLE technology for making proximity payments requires that the Bluetooth functionality on the consumer's mobile device is switched on, which should be handled by the MSCT application. BLE is available on most mobile phones but the technology as such is challenging to secure proximity. Different phones have different characteristics so if no additional technology is used to secure the proximity for instance the wrong person might get the payment request. There are different technologies provided by different vendors to secure (which might involve patents) which creates a dependency on third party providers. It usually also requires some extra software to be integrated into the payment application.

10.2 Web-based payments

Creating a secure Web (payment) experience involves too many considerations to address briefly in this document. However, it is worth highlighting some key points and recent developments.

- Require the use of "https" URLs. This leverages Transport Layer Security (TLS) with the HTTP protocol (see [66]).
- Ensure end-to-end TLS encryption. TLS 1.3 was completed in 2018. It enhances communication over the Internet "in a way that is designed to prevent eavesdropping, tampering, and message forgery" (see [66]). Web application developers should look at adopting TLS 1.3, but with attention to fallback mechanisms to TLS 1.2 where version 1.3 is not yet supported (see also [19]).
- Consider the use of emerging Web standards to mitigate major security risks such as the OWASP top 10 application security risks⁷⁷. For example:
 - To prevent against scripting attacks by leveraging the specifications of the W3C Web Application Security Working Group⁷⁸. This includes development of a content security policy and leveraging the browser's new capabilities to verify the integrity of included resources ("subresource integrity").
 - To reduce the risks involved with phishable passwords, consider using W3C's Web Authentication API (see [99]), part of the FIDO2 suite of specifications⁷⁹.
 - To reduce data exposure, move in the direction of tokenised payments. W3C anticipates this will become easier through new browser-based standards for payments: the Payment Request API (see [100]).

Additional guidance may also be found in "Securing the Web," a finding of the W3C Technical Architecture Group see [101].

10.3 Merchant applications

For MSCTs based on merchant application on the mobile device, the reader is referred to Chapter 12 for security guidance.

⁷⁷ See https://www.owasp.org/index.php/Top_10-2017_Top_10

⁷⁸ <https://www.w3.org/2011/webappsec/>

⁷⁹ <https://fidoalliance.org/fido2/>



10.4 Additional security measures

10.4.1 MSCT Tokenisation

In order to enhance the security of mobile payment transactions, so-called tokens may be used. In the context of this document, they generally refer to a surrogate value for sensitive payment data such as payer or payee identification data (e.g., CustomerID, IBAN) or transaction data which are used in MSCT transactions. These tokens are designed to provide additional protection of data in communications and storage and are typically used when exchanging data between the payer and the payee (e.g., via a proximity technology such as a QR-code) or during the processing of MSCT transactions (e.g., in MSCT service provider back-ends).

Tokenisation is the process of replacing for example an IBAN and payee name with a unique MSCT token that is restricted in its usage. They are issued by so-called “Token Service Providers”, on the request of a PSP (a so-called Token Requestor).

An MSCT token provides improved protection when its use is limited to a specific domain(s), such as a specific merchant, form factor (including mobile phones, wearables, etc.) or channel such as different proximity technologies. The application of these underlying usage controls, known as the “Token Domain Restriction Controls”, is a primary component and benefit of tokens. The Token Domain Restriction Controls can be used to limit the use of a token to its intended use (for example, prevention of the successful use of a token outside of a specific proximity technology).

From an operational perspective it should however be noted that applying any tokenisation process introduces a dependency on the Token Service Provider to conduct an MSCT in view of the de-tokenisation process needed.

10.4.2 Merchant Tokenisation

In case consumers have on-boarded with merchants, the merchants need to implement specific security measures to protect these data. Merchants may decide to deploy tokenisation solutions to implement some use cases and value-added services while avoiding entering into processing of consumer data. This enables them to increase the level of security of their payment solution and to facilitate their compliance with security requirements.

Such merchant tokens are used in closed loop environments between a subset of ecosystem participants for specified purpose and do not enter into the interoperability domain. They are used where transaction data are stored, but sensitive payment data have substitute values (tokens). Typical use cases include fraud management, merchant analytics, added-value services (loyalty, couponing, etc.).

Merchant tokens are to be seen as a process reducing the amount of consumer data stored in merchant environments and may enable merchants to address security requirements compliance.

10.4.3 Securing the link payee name / IBAN_payee

For (instant) credit transfers, it is crucial that the link payee name/IBAN_payee is correct. Several methods may be employed to ensure this.



In a number of SEPA countries it has been implemented as an additional service (e.g. in the Netherlands, UK, etc.), where before the initiation of the credit transfer this link is checked by the payer's ASPSP.

Another means of securing this link is the addition of a digital signature on the payee name/IBAN_payee which may be added for example in a QR-code or a payment request message and checked by the payer's ASPSP before the (instant) credit transfer.

However, since this issue is not specific to mobile initiated (instant) credit transfers it will not be further analysed in this document.



11 Security of mobile devices

11.1 Introduction

Within the SEPA region, most of the deployed general-purpose mobile phones include the appropriate communication capabilities such as fast and reliable internet access to support mobile financial services. They use a so-called “UICC” (Universal Integrated Circuit Card), which is a tamper-resistant component, owned and provided by the MNOs, and fully standardised by ETSI. Whereas the UICC already manages the necessary confidential and cryptographic data to identify the user to the mobile network, the UICC can potentially also host mobile payment applications such as an MSCT application under the control of the MSCT service provider or an authentication application under the control of the authentication service provider.

The usage of a mobile phone for MSCTS is depending on the requirements set by the MSCT service provider. For example, an MSCT service provider may only require the storage of a QR-code whereas another MSCT service provider may require the download of their MSCT app to the mobile phone on a specific platform. The requirements on the mobile phones may become complex: an NFC controller, BLE, a Secure Element (SE) and appropriate interfaces to enable secure MSCT or authentication applications. In the absence of an SE (see section 11.2), MSCTs may make use of other security features offered by the mobile phones such as Host Card Emulation (HCE – see section 11.3) and a Trusted Execution Environments (TEE – see section 11.4).

11.2 Secure Element

A Secure Element (SE) is a tamper-resistant module capable of hosting applications in a secure manner. The SE provides a protection of the applications including separation of the applications. The SE may appear in different form factors in the mobile equipment for usage in the context of MSCTs:

- UICC (a removable SE);
- Embedded SE (eSE, including eUICC);
- Integrated SE (iSE).

Typically such a SE contains

- An Operating System (OS) which supports the secure execution of applications and secure storage of application data. The operating system may also support the secure loading of applications.
- Communication interfaces:
 - A device (contact) interface which enables commands and responses to be exchanged between the SE and authorised mobile applications in the mobile equipment.
 - It may contain an antenna (contactless) interface which enables the exchange of commands and responses between an application in the SE and a POI via the NFC controller of the mobile equipment.
- A so-called “manager” that maintains a list of applications on the SE, the status of the applications and the associated data. The status of an application indicates if the application is available for selection on the contactless interface.



The main factors driving the choice of SE in this context could be:

- Control and management of the SE;
- Intrinsic security properties;
- Eligibility for formal security certification;
- Integration within the mobile phone and connections to external interfaces such as contactless or remote protocols;
- Availability (timelines and geographical market);
- Support infrastructure (personalisation tools);
- Possibility of deployment within the existing commercial supply chains for mobile phones;
- Establishment of business and technical relationships between stakeholders (SE owner, MSCT service provider, etc.);
- Cost-effectiveness and economies of scale.

The choice of the type of SE has an impact on the mobile payment service model.

11.3 Host Card Emulation

Until a few years ago, SE-based NFC was the only practical and interoperable technology option to enable mobile contactless payments. Today, for all the mobile device operating systems that support Host Card Emulation (HCE), any application in the mobile device can directly access the NFC capabilities to communicate with a merchant's contactless POI. HCE eliminates any dependencies on having an SE and enables cloud-based payments. This provides a simpler option for the adoption of NFC by enabling mobile payment providers, merchants, and third party application developers to provide consumer experiences without the technical or commercial integrations required for the SE-based model.

Previously, an NFC application on a mobile device communicating with a contactless reader would have to be coded for and executed in an SE, but nowadays mobile device operating systems (OS) and implementations allow the application that receives and processes the payment transaction commands sent from the contactless reader to be coded for and executed in the application processor of the mobile device.

To enhance the security, HCE-based solutions may be offered in combination with tokenisation, see section 10.4.1.

For further information on HCE the reader is referred to [64] and [77].

11.4 Trusted Execution Environment

In a mobile device, applications typically are executed in an environment provided and managed by a Rich OS, the so-called REE (Rich Execution Environment) which is outside the Trusted Execution Environment (TEE). This environment and applications running on it are considered un-trusted.

A TEE can be defined as a dedicated execution environment providing security features such as isolated execution, integrity of applications along with confidentiality of their assets for the deployment of sensitive services. It complements SEs / TPMs for handling sensitive assets, brings security to interaction with the user and has the potential to control data flows in the consumer device.



The TEE runs alongside the Rich OS and provides security services to that rich environment and applications running inside the environment. A set of TEE APIs allows the communication from the REE to run Trusted Applications within the TEE.

The interfaces between the main components are represented in the figure below.

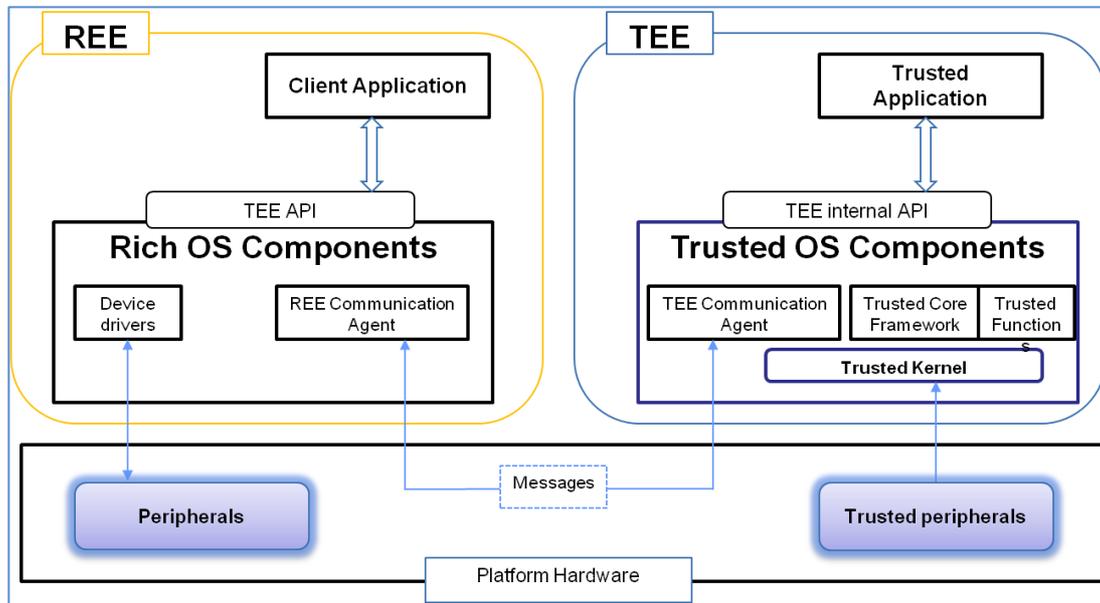


Figure 30: Example of a TEE model

The model identifies API interfaces and a communication agent within the REE:

These APIs allow access to some TEE services, such as cryptography or trusted storage and enable the execution of a Client Application in the Rich OS to access and exchange data with a Trusted Application running inside a TEE. The TEE API in the REE enables the standard communication with the TEE and is used by the Client Application.

The REE Communication Agent provides REE support for messaging between the Client Application and the Trusted Application.

For the security guidelines on TEE and MSCT related data, the reader is referred to the dedicated section in Book 4 of the SEPA Card Standardisation Volume (see [10]) which provides similar guidance in the context of card-based payments.

11.5 Smart Secure Platform

Mobile devices are constantly being enhanced and feature an ever-increasing number of capabilities. However, those also introduce new challenges such as an increasing complexity and dependencies.

MSCT service providers face a huge complexity with different solutions for each handset and/or mobile OS. This means that they need to develop their applications for a large number of different mobile platforms (combinations of different hardware and software) in view of the current platform incompatibilities. This obviously comes with a cost impact and may in some cases also lead to consumer confusion. The fact that there are multiple solutions on the market which are different - read not compatible - makes it challenging for the supply side. Moreover, once the devices are in



usage by the consumer, there are a number of additional challenges which remain to be addressed; security and privacy are the most relevant ones.

Already recommendation 13 of the ERPB Statement in November 2015⁸⁰, requested ETSI the development of a “Smart Secure Platform” (SSP), taking into account the requirements for mobile payments. This platform should enable the provision of value-added services relying on authentication of the user, regardless of the mobile device, communication channel and underlying technology.

ETSI Technical Committee *Smart Card Platform* (TC SCP) started the work in April 2016 by collecting and define requirements to be used for the development of a more generic secure element to be used in various fields of application taking into account state of the art technologies (e.g., replacing outdated protocols). A major design topic was the possibility to adapt the generic configuration of the SSP so that it could easily be adjusted to optimally fit the requirements of its envisaged application (e.g., for IoT, banking, eID) and to provide the possibility for a certification against existing SE certification schemes.

A multi-part specification was developed TS 103 666 ([40] to [43]) under the general title *Smart Secure Platform (SSP)*. Part 1 *General Characteristics* and Part 2 *Integrated SSP (iSSP) characteristics* were first published half a year after the requirements in November 2019. Part 3 on the embedded SSP (Type 1) followed in July 2020 while Part 4 on the embedded SSP (Type 2) is expected end 2021.

Priority was set on developing a solution for an integrated SSP. The integrated solution radically changes the distribution model, as the integrated SSP comes as an integral part of the customer device (e.g., mobile device) and will not be distributed (and owned) by the service provider anymore as, for instance, in the case of SIM which is owned and distributed by an MNO. This concept requires a system which allows a service provider to download their application, including the operating system (OS). The solution developed (see Figure 31 below) uses a separation of hardware and software based on the concept of the Virtual Primary Platform (VPP) of GlobalPlatform (see [56] to [58]). The primary platform, the hardware, includes a minimal OS, the so-called Low-Level Operating System (LLOS), providing just the necessary capabilities to communicate with it. The secondary platform contains the OS of the application and is called the High-Level Operating System (HLOS). On top of the secondary platform one or more applications may reside which provide the service providers’ specific functionality. The combination of a secondary platform and its application(s) is called a Secondary Platform Bundle (SPB). Such SPB can be loaded and also remotely downloaded to a primary platform, thus providing a way to distribute applications independently. For example, a mobile payment application can be downloaded to an SSP independently of an MNO application; there is no need for any agreement between the respective service providers. The same concept has been extended to be supported also on embedded SSPs.

⁸⁰ https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/4th-ERPB-meeting/2015-11-26_4th-ERPB_meeting_final_statement.pdf?25029cf94b5c5d93e555201f86981bb4

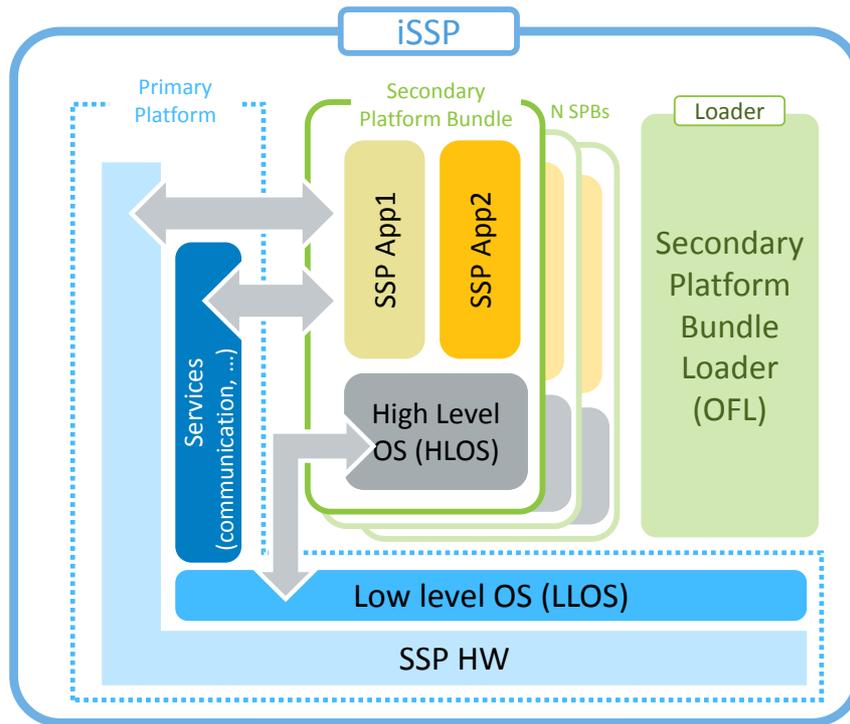


Figure 31: Logical structure of an iSSP⁸¹

ETSI SCP also developed a new specification of the Serial Peripheral Interface using the SCL interface. SPI is an interface being widely used in the industry to communicate between different chips on the same Printed Circuit Board (PCB). As the integrated SSP is basically a chip inside a System on Chip (SoC), SPI was the first choice for the communication protocol for the integrated SSP (see TS 103 713 [44]).

Other work currently pursued by TC SCP are enhancements of the requirements and the removable SSP (rSSP). The latter could be the advanced platform for applications residing on say, a payment card format or a smaller physical size of card as used for mobile communication.

As for all their specifications ETSI TC SCP are striving to provide test specifications also for their SSP specifications. To support TC SCP in this effort ETSI is funding a so-called “Testing Task Force” under the guidance of TC SCP. The first test specification, the one for the SPI interface, has already been published (see [45]) and the one for the SSP General Characteristics is expected for publication in July 2021 (see [46]).

Though not all work has been completed yet one can summarise the new Smart Secure Platform by saying that SSP⁸² is a new, open platform for multiple applications, including mobile payments, providing a clear separation of layers, enhanced security, new interfaces and a new filesystem. It is

⁸¹ Figure provided by courtesy of ETSI; all rights reserved.

⁸² The presentations given at the ETSI Security Week in 2020 provide detailed material covering the various topics, from the reasons for developing SSP and the requirements via testing and certificates to the technical realisation of the various types, see https://docbox.etsi.org/Workshop/2020/202006_ETSISECURITYWEEKGOESVIRTUAL/SSP_THREAD



faster and more flexible than the UICC, giving a choice of hardware but is still supporting existing features of the UICC such as NFC and toolkit.

11.6 Security guidelines for mobile devices

The following security guidelines for mobile devices should be applied regarding their usage for MSCT transactions. Note that these guidelines are aligned with the security requirements for mobile device included in Book 4 of the SEPA Cards Standardisation Volume (see [10]).

Reference	Mobile Device Security Guidelines
MD-SG1	Only authorised applications entities (e.g., MSCT service provider, Authentication service provider, etc.) should be able to access and communicate to the MSCT/ Authentication application or credentials residing in a secure environment on the mobile device.
MD-SG2	There should be generic enablers for a secure environment (e.g. for controlled access to sensitive peripherals, secure storage, flexible secure boot) to verify the integrity of the mobile device firmware, run-time integrity checking, firewalls and anti-virus software (for further guidance, see for instance the OMTP documents [84], [85], [86] and the GlobalPlatform documents [53], [54]).
MD-SG3	There should be a mechanism to: <ul style="list-style-type: none"> • Prevent unauthorised capture of data • Prevent unauthorised use of the mobile device (e.g. a lock function).
MD-SG4	It is recommended that the MSCT service provider educates and informs the payer on the risks associated with the use of mobile devices and how to protect themselves against the risks associated with e.g., <ul style="list-style-type: none"> • Rooting / jailbreaking a mobile device • App downloading from untrusted sources. It is recommended that the MSCT service provider provides information to the PSU on antivirus products/regular updates to be downloaded and installed onto the mobile device.
MD-SG5	It is recommended that stronger rules are put in place to ensure verification of MSCT application codes and the origin of the MSCT application, when distributed via an application store.



MD-SG6	It is recommended that MSCT application developers incorporate best practices such as <ul style="list-style-type: none">• Clearer messaging of permissions requested by given MSCT application• Reduce set of permissions to only the necessary ones.
---------------	--

Table 24: Security guidelines for mobile devices

In addition, the following mitigating security measures on the mobile device could be taken into account, subject to the overall risk approach of the MSCT service provider.

Malware detection

An application developer can include detection of traces or signatures of malware installed on the PSU mobile device. This detection is limited by the capabilities provided by the device and its operating system.

Mobile device fingerprinting

A PSU mobile device can be (uniquely) identified by using device parameters (e.g., IP-address, geo-location, etc.). This can facilitate the detection of the “usual” mobile devices which may increase the trust in the legitimate usages of the payer credentials.

Mobile device binding

Mobile device binding refers to a reliable and consistent verification of the mobile device used for MSCTs by registering the mobile device and binding it with a personalised security credential, e.g. as part of the PSU on-boarding process (see also Chapter 14). This then helps to validate the returning mobile device on subsequent MSCT transactions.

Rooting / Jailbreaking detection

Special measures can be implemented to detect rooted or jailbroken mobile devices. They use a version of the operating system that is not the original version provided by the device manufacturer or operating system provider. This increases the risk of unauthorised access to the device which could impact the full mobile device ecosystem.

Further security requirements for mobile devices may also be found in [59] and [63].



12 Security guidelines for MSCT applications

12.1 Software-based mobile applications

The security of mobile applications (e.g., MSCT application, Authentication application) facilitating payment transactions is a major concern to the stakeholders in the payment ecosystem. It is “key” for the market players to have a solid foundation for building their mobile payment services with an adequate level of security embedded.

In the context of MSCT payments, the MSCT/Authentication applications residing on the mobile devices support the critical functionality such as:

- Implementation of CDUVM,
- Implementation of Strong Customer Authentication;
- Hosting and transmitting sensitive payment information (e.g. personal data, preloaded payment tokens, etc.);
- Accessing components of local (i.e. host institution-wide) and interbank payment infrastructure (SPL service, distributed CSM infrastructure of the SCT (Instant) scheme, etc.).
- Collecting and processing payment initiation data (e.g., Request-to-Pay, merchant-presented QR-code, etc.).

In addressing risks around secure mobile applications design, the current guidelines are aiming to provide up-to-date references to the most advanced standards and best practices in designing this type of software-based mobile applications, taking into account their specific operational role within the MSCT service context. Nonetheless, it must be clearly articulated that along with evolution of the technologies the current and prospective software-based mobile payments are built upon, the forms and number of threats to the security will also evolve. This makes it obligatory to the MSCT service providers delivering this type of services to be compliant to the forefront developments in the area of mobile application security best practices and guidelines underpinned by the respective standards.

As stated in [12], the security of the overall mobile payments solution relies heavily on the effectiveness of the *server-side components and backend system* in handling credential verification and detecting potential compromise of the mobile application and/or device integrity either from information provided directly by the mobile application, device attestation, or inferred from transactional analysis. Hence, the above list includes references to standards outlining design and testing principles for traditional web-applications underscoring their crucial role in ensuring security of the overall MSCT payment solution. Furthermore, being considered in the operational context, the end-to-end mobile payment solution needs to cater for other security requirements such as preventing the QR-codes or other payment initiation instruction medium from being tampered, secure transmission of sensitive data from POI to the backend system of either PSP or ASPSP, etc.

As introduced in [90], there are three OWASP levels of security verification associated with corresponding sets of requirements for mobile applications depending on the context they operate in. The operational context includes data sensitivity, the degree of impact on users’ wellbeing and consequences to the infrastructure in case of a security breach.

These OWASP levels read as follows:



L1 – Standard Security. The level of security which guarantees implementation of security best practice while designing mobile applications resulting in countering most common security vulnerabilities;

L2 – Defense-in-Depth. The level of security which provides additional defence-in-depth controls such as SSL pinning, resulting in a mobile application design which is resilient against more sophisticated attacks, assuming the security controls of the mobile operating system are intact and the end user is not viewed as a potential adversary;

R – Resiliency against reverse engineering and tampering. This level of security verification requirements once implemented in full or partially, impedes specific client-side threats where the end user is malicious and/or the mobile OS is compromised.

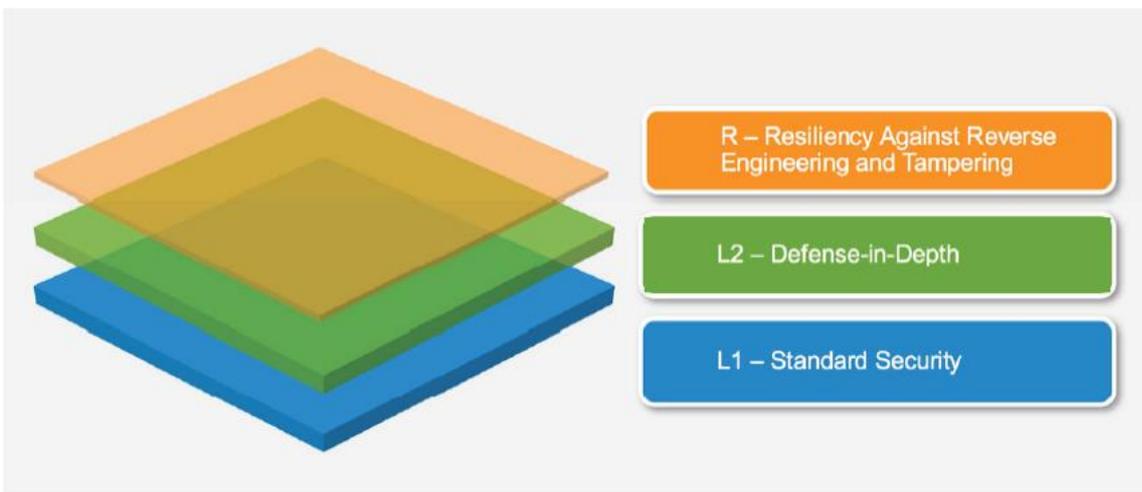


Figure 32: OWASP Security Verification Levels as per MASVS^{83, 84}

Considering the context of the MSCT applications, it is appropriate to request at least the security verification level L2 + R as the baseline while designing these applications and testing their functionality.

The following table represents a classification of potential attacks on Mobile applications (e.g., MSCT or Authentication applications) hosted on a mobile device (mobile platform) device), which are based on [12].

Attack	Description	Attack Path
Bypass mobile platform (e.g. OS) security controls	Gain privileged access to mobile application processing and assets	A malware infection uses a published exploit or zero-day attack targeted at a specific platform vulnerability which

⁸³ MASVS – Mobile Application Security Verification Standard, see [90].

⁸⁴ The figure is courtesy of OWASP.



		can be used to escalate privilege
Reverse engineer mobile application source code	Recover sensitive source code and extract sensitive mobile application assets, such as payments sensitive data or cryptographic constants and ciphers	Download the app from an app store and analyse it within their own local environment, performing code disassembly, Java code de-compilation, code structure analysis and asset extraction
Tampering of mobile application code	Alter behavior of mobile application and possible modification of payment transaction data	Code is modified or malicious code injected, for example to present false information to the user using malicious forms of the app hosted in a third-party app store, or installed through a phishing attack
Exploit interfaces between components	Abuse the interfaces between the components that make up the payment application	Masquerade as a legitimate payment application while interacting with a trusted application in the TEE. Compromise the results of user authentication, thereby fooling the mobile application into believing that the user identity has been successfully validated. Compromise payment application functionality to relay sufficient information to a remote endpoint, enabling payment to occur with that remote endpoint
Extract assets in runtime	Recover assets from an application running under the attacker's control	The application is executed under debugger, emulator, or dynamic binary instrumentation. The attacker intercepts plaintext assets at the time they are being processed in memory.
Modify mobile application code flow	Manipulate critical mobile application functionality	The application is executed under debugger, emulator or dynamic binary instrumentation. The attacker injects malicious code that



		alters the logic of the application in order to perform fraudulent payments directly on the device, facilitate recovery of assets for off-device attacks, suppress reporting to backend, etc.
Insecure communication	<p>When application transmits its data, it must traverse the internet. Threat agents might exploit vulnerabilities to intercept sensitive data while being transferred across the path.</p> <p>When the application receives or collects data for a payment initiation e.g., Request-to-Pay, QR-code) it could be altered.</p>	<p>This flaw exposes an individual user's data and can lead to account theft.</p> <p>Payment initiation transaction data may be tampered and funds redirected.</p> <p>A “man in the middle” proxy redirect might be in place.</p>
Exploiting vulnerability of improperly secured API exposed	Exploiting vulnerabilities such as not timely revoking clients’ certificates or failure in processing exceptions arising from unsuccessful attempt to access the directory service in case of cross-border PSD2 transaction.	<p>Masquerade as a legitimate payment initiation service provider to facilitate low-amount payments not requiring SCA.</p> <p>A “man in the middle” attack targeting customer credentials.</p>
Exploiting vulnerability of public API architecture flaws	Exploiting vulnerabilities such as tightly bounded code performing controller, data management, and data dispatching API functionalities; allowing for insecure cookie for authentication endpoints; caching sensitive data; HTTP specific security requirements not implemented in full (e.g. refer to [89] for the list of baseline requirements)	Vulnerability originating from architecture design flaws leading to attackers being able to exploit the tight-coupled code to get access to the data stored in the host backend system, or to collect as much as possible details on the API design via random penetration requests and making use of this knowledge set to shape their attack strategy.

Table 25: Overview potential attacks to mobile apps on a mobile device



The standards referenced above are supposed to be considered jointly so that they would guide MSCT/Authentication application development process throughout the entire software development lifecycle, since they are cross-referencing each other.

One of the options as to how to put them in practice would be working out a threat model relevant to a particular business case of MSCT payment flow context (the POI bound data exchange technologies, transaction risk analysis being enforced on both application and the backend system's side of the MSCT solution, etc.). Provided the operational context is set up, the security verification standards for mobile and web-applications [88], [90] as well as the dedicated sections of the test guides [91] and [92] could provide valuable insights on the best practice in designing the respective parts of the MSCT/Authentication application-based payment solution. Finally, to ensure that the desired level of security of the MSCT payment solution is achieved, a comprehensive testing covering all the security requirements should be undertaken. The guides [91] and [92] are instrumental for providing the baseline test requirements.

As an illustration to this approach, the following example shows how the end-to-end mobile application development cycle might look like leveraging the aforementioned standards:

The results of threat modelling are to be used as the starting point in designing secure functionality of a mobile application, e.g., the threat originating from *“exploiting interfaces between mobile application components”*. If one refers to [90], they would be able to figure out that in the *“Data Storage and Privacy Requirements”* section there is a reference to a dedicated security requirement, which is *“2.6. No sensitive data is exposed via inter process communication mechanisms”*. To get a baseline recommendation out of the standards prepared by the expert community, it is worthwhile to look up the Mobile Security Testing Guide [91], which is referencing to both best practice details and descriptions of how to perform static and dynamic tests to ensure sensitive data is not exposed via inter process communication mechanisms. These details are provided in [91] in the section on *“Data Storage”* for both Android and iOS.

12.2 SE-based mobile applications

Since for implementations whereby the MSCT/Authentication application is hosted in an SE, the guidelines are similar as those for Mobile Contactless SEPA Card Applications, the reader is referred to the SEPA Card Standardisation Volume - Book 4 (see [10]) for further security guidance.



13 Security guidelines for CDUVMs

In [15], although focused on card-based mobile payments, the general concept of a “*mobile payment using a Consumer Device Cardholder Verification Method (CDCVM)*” is described in a generic way and hence can be applied to CDUVMs in the MSCT context. Therefore this document is considered to provide a good reference to get an overview of the security objectives and goals, the threats, the CDUVM assets to be protected, and the security requirements that need to be followed to meet the security objectives.

A short overview and summary of the main topics for CDCVM is given below while reference is made to [15] for further in-depth reading.

A *CDCVM solution* may be provided at *application level* and/or at *mobile device or OS level* as a mobile platform authentication mechanism for use by mobile applications on the device (“shared CDCVM”).

It has to be ensured that the CDCVM solution cannot be maliciously abused, disabled or bypassed; and that its assets are adequately protected. The key security goals and objectives for the steps involved in CDCVM processing (e.g. biometry, mobile code) are:

- *Capture*: Secure processing of the (raw) entry data, secure channel for transfer of UVM data
- *Feature extraction*: Secure extraction / conversion of input into a format suitable for matching with a reference; secure channel for transfer of sample (if applicable).
- *Match*: Secure channel for transfer of stored reference data, secure matching process; and secure channel for transfer of the result of the matching process through the Authenticator APIs.

An attacker may try to retrieve sensitive (e.g. biometric) data, or identify and exploit vulnerabilities, by gaining *remote or physical access* to the mobile device. The goal of an attacker will be to compromise secret data on the physical device or to create an artefact as part of a presentation attack. In [15] some threat examples are provided, e.g., in the context of biometric CDCVM typical threats are:

- Presentation of a fake artefact to spoof the sensor;
- Firmware is replaced by malware;
- The raw image is used to create an artefact;
- Replay of raw or processed image; capture of transmitted data (interception) for replay;
- The biometric template database is manipulated;
- A spoofed result of biometric processing is transmitted;
- Introduce transient faults during CDCVM processing (glitch attacks).

A number of *CDCVM assets* must be protected, depending on the CDCVM solution. Assets can be categorized as requiring one or more security services: confidentiality (e.g. biometric image),



integrity (e.g. verification result), and Integrity with the addition of accountability/authentication (e.g. biometric processing firmware).

In [15] almost 50 dedicated security requirements are listed which should be followed in the design of a CDCVM solution and its architecture. The main topics covered by these requirements are:

- Document the protection of the CDCVM Solution security assets and their dependencies;
- Protect the CDCVM solution security assets to meet the minimum required security objective;
- Protect the CDCVM solution against unauthorised modification and usage;
- Provide strong access control measures;
- Provide accurate verification results to “relying applications”;
- Provide reliable and secure reporting information (if applicable);
- If communicating between multiple CDCVM solution components over insecure interfaces, use secure and industry accepted cryptographic protocols and methods;
- Develop the CDCVM Solution at a secure site with configuration management, version control, and secure coding practices.

Further best practices for CDCVM may also be consulted in [16].



14 Security guidelines for PSU on-boarding

14.1 Introduction

MSCT service providers and merchants should take appropriate measures to identify and register PSUs to whom they deliver their services.

It is essential for payment service providers to confirm that a particular communication, transaction, or access request is legitimate. Accordingly, MSCT service providers should use reliable methods for verifying the identity and authorisation of new PSUs. PSPs should furthermore use reliable methods for authenticating the identity and authorisation of established PSUs seeking to register for new MSCT services. Also merchants that on-board consumers to facilitate MSCT services (e.g., by offering a dedicated app or storing consumer related data related to MSCTs) should use similar reliable methods for this process.

In case an authentication application is involved on the PSU mobile device for the MSCT, similar guidelines apply with respect to the on-boarding of the PSU by the Authentication service provider.

14.2 Security guidelines

PSUs may be registered for MSCT services by MSCT service providers or merchants using one of the following means:

- Electronically via a dedicated application (e.g. an on-line banking app or merchant app) or via a website;
- Physical presence.

PoB-GL1	In case of remote electronic registration, appropriate measures should be in place to control the connection (communication channel) between the MSCT service provider or the merchant and the PSU such that unknown third parties cannot displace PSUs (see also Chapter 9).
----------------	---

A secure communication channel ensuring integrity and confidentiality as needed between the PSU and their MSCT service provider or the merchant shall be made available. Examples include a website connection via TLS1.2 or higher (according to the state of the art) or a dedicated app with endpoint security on the PSU's mobile device.

PoB-GL2	MSCT service providers and merchants ⁸⁵ who are not ASPSPs, should rely on the PSU identification and authentication method used by the PSU's ASPSP for the on-boarding of the PSU for the MSCT service and the linking to the PSU account.
----------------	--

Electronic identification and "Know Your Customer" (KYC) processes used by ASPSPs are set out by regulatory authorities and are based on robust customer identification and authentication processes applied for the registration of customers⁸⁶. These are particularly important in the cross-

⁸⁵ Or a third party acting on behalf of them.

⁸⁶ For example, Annexes 2 and 3 in [4] provide insights into the different KYC methods used.



border context given the additional difficulties that may arise from doing business electronically with customers across national borders, including the increased risk for identity impersonation (see [6] and [25]) and the greater difficulty in conducting effective credit checks on potential customers.

In case PSUs use PKI certificates for their electronic identification when registering for an MSCT service, the PSU identification used by the certificate authority should be accepted by the ASPSP and supervised by the competent authorities. In case eIDAS electronic identification means for PSUs are used, the mutual recognition for the usage of these means is laid down in the eIDAS Regulation [4], which enhances cross-border trust.

In case a third party is involved e.g., on behalf of a merchant, appropriate agreements should be in place that cover the security requirements and liabilities.

PoB-GL3	PSUs should explicitly register for an MSCT service, linked to one or more accounts from their ASPSPs. The guideline remains valid for any re-registration ⁸⁷ or de-registration process.
----------------	--

This explicit registration aims to raise PSU awareness and stresses the trust factor involved in conducting MSCT payments. This may also involve the download and activation of a dedicated MSCT application on the PSU device.

PoB-GL4a	To ensure that the request was made by the legitimate consumer and their registered mobile device, without disrupting the user experience, consumer mobile device binding should be implemented by ASPSPs, MSCT service providers and merchants as appropriate. The procedure implemented should also cater for loss or renewal of the consumer mobile device.
PoB-GL4b	To ensure that the request was made by the legitimate merchant and their POI, the POI platform used should be identified and possibly platform binding applied as appropriate ⁸⁸ . The procedure implemented should also cater in case of upgrades of the POI platform.

PSU mobile device binding refers to a reliable and consistent verification of the PSU's mobile device used for MSCT services by registering the PSU's mobile device and binding it with a PSU credential, e.g. as part of the PSU on-boarding process. This enables to validate this PSU mobile device used in subsequent MSCT transactions (see also section 11.5).

For achieving this binding, the trust of existing PSU mobile devices could be leveraged. As an example a strong PSU mobile device ID could be used. This is a unique tamper resistant identifier that cryptographically binds a specific PSU mobile device to a PSU identity, leveraging PKI capabilities.

⁸⁷ As examples, a re-registration process is needed in case of change of payment account or loss of the consumer device.
⁸⁸ Depending on the type of POI platform.



PoB-GL5	MSCT service providers, if involved, should implement controls to ensure that credentials as appropriate are distributed to PSUs in a way that is trustworthy. The level of trust in the PSU's identity shall be maintained throughout the MSCT service lifecycle, including the re-issuance of credentials.
----------------	--

MSCT service providers should keep control of addressing information (physical or online) which are used for communication with the PSU. MSCT service center staff should be well informed and educated in the procedures that are used for distributing credentials. All distributions of new credentials or downloading of the MSCT application / POI software should be logged, and the MSCT service provider should consider giving the PSU a notification through a dual communication channel (see [9] in Annex 1).

PoB-GL6	All stored personal data about PSUs and (sensitive) payment data related to MSCT transactions and related messages MSCT service providers hold should be protected in strict accordance with the legal and regulatory requirements (PSD2 [5], GDPR[7]) and used solely for the purposes explicitly allowed by the respective "data subject".
----------------	--



15 MSCT supporting services

15.1 Introduction

This chapter is devoted to an overview on some of the supporting services that may be involved in the execution of an MSCT, namely a Payment Initiation Service Provider (PISP), the SEPA Proxy Lookup (SPL) service and a Request-to-Pay (RTP) service.

15.2 PISP payer authentication models

As illustrated in some of the MSCT use cases in Chapter 7, a Payment Initiation Service Provider (PISP) may be used for the initiation of an MSCT. In this chapter a high level description will be provided on the PISP payer authentication models supported by the PSD2 [5] and the RTS [6], including references to additional information on these models.

15.2.1 Redirection Model

The redirection model is an approach whereby the payer starts interacting with the PISP, merchant or MSCT application on their mobile device and is then redirected to either their ASPSP's on-line banking website or to an MSCT application or a dedicated Authentication application (app-to-app redirection model) that has been issued or adopted by the payer's ASPSP for their authentication. In this model, the payer's ASPSP will remain in full control of the strong customer authentication.

In order to allow this, the PISP has to redirect the payer to the ASPSP authentication service, meaning the payer will leave temporarily the PISP interface for authenticating towards the ASPSP interface. After finalisation of the payer authentication, the ASPSP redirects the payer PSU back to the PISP interface.

The currently published API standards, for example from the Berlin Group (see [97]), Open Banking Implementation Entity (OBIE) (see [87]) and STET (see [96]) enable the redirection model.

15.2.2 Decoupled Model

The decoupled model is similar to the redirection approach, but here not the PISP, but the ASPSP requests the payer to authenticate via the ASPSP's authentication application. Typically, the MSCT transaction would be handled through a browser, a merchant app or POS terminal (not designed to make a payer authentication), while the payer authentication would remain under the control of the payer's ASPSP - executed in parallel (decoupled) through a dedicated Authentication application on the payer's mobile device or a dedicated authentication device.

The currently published API standards, for example from the Berlin Group (see [97]), Open Banking Implementation Entity (OBIE) (see [87]) and STET (see [96]) enable the decoupled model.

15.2.3 Embedded Model

In the embedded model, the payer authentication is performed via the payer's ASPSP API provided to the PISP. This means that the SCA of the payer is performed through the PISP user interface and the authentication factor(s) are transmitted via the API from the PISP to the payer's ASPSP for verification.

In this model, the payer's ASPSP has control over the payer's authentication, however the payer's credentials may be visible to the PISP, depending on the authentication method used.



The currently published API standards, for example from the Berlin Group (see [97]) and STET (see [96]) enable the embedded model.

15.2.4 Delegated Model

In the delegated model, the strong customer authentication is performed by the PISP, not the payer's ASPSP. However, this model requires an (outsourcing) agreement between the payer's ASPSP and the PISP, defining inter alia the liabilities as well as the on-boarding of the payer by the PISP, including the issuance of the payer credentials.

The required functionalities for the API between the payer's ASPSP and the PISP to cover all four models, hereby striving to the best payer journey, have been addressed in the dedicated ERPB Working Group on a SEPA API access scheme (see [37]).

15.3 SEPA Proxy Lookup Service

The mobile P2P payment services in the market today are mostly domestic solutions that require both payer and payee to be registered with the same mobile P2P payment service provider or that at least require the payer to know the payment details of the payee (e.g. the IBAN).

It is also recognised that the success of the mobile P2P payment services strongly depends on the underlying user experience for the payer and the payee. Here the manual exchange of payment information such as the IBAN makes the payment process very uncomfortable. Furthermore, there is the need to enable cross-border and cross-community mobile P2P payments.

The EPC facilitated interoperability between the existing mobile P2P payment services by the set-up of a new scheme, the so-called SEPA Proxy Lookup (SPL) scheme that operates based on a dedicated scheme rulebook (see [26]).

To support interoperability amongst different European mobile P2P payment services, this SPL service, accessible by mobile P2P payment service providers, offers the retrieval of the correct up-to-date IBAN of the payee based on their mobile phone number, if the payee is not registered in their own mobile P2P payment service. As such it enables MSCTs based upon the mobile phone number of the payee, between a payer and payee that are registered with different mobile P2P payment service providers.

The SPL service provides a mapping of a mobile phone number to an IBAN, so the mobile P2P payment service provider of the payer can request for the IBAN based on the payee's mobile phone number. Subsequently, the payer's mobile payment service provider can initiate an MSCT to the payee. The EPC has defined an SPL scheme⁸⁹ for managing this SPL service. Interested mobile P2P payment service providers have to register for this SPL scheme with the EPC.

In case the mobile number of the payee could not be found in the local directory of the payer's mobile P2P payment service provider, the latter will send an appropriate request to the SPL service provider. The SPL service provider will transfer the incoming IBAN request to the network of registered mobile P2P payment service providers.

⁸⁹ see <https://www.europeanpaymentscouncil.eu/what-we-do/other-schemes/sepa-proxy-lookup-scheme>



The request will be sent in parallel, based on the mobile phone (MSISDN) structure, to a subset of the registered mobile P2P payment service providers and the system will cope with the time-out behavior to ensure a total maximum response time. Some of the requested MSCT service providers will return a positive answer, whereby the SPL service provider will select the most recent entry to be presented to the payer’s mobile P2P payment service provider. This means that the SPL service provider is in fact operating as a routing network (also sometimes referred to as a “switch”) and is not a dedicated central IBAN database.

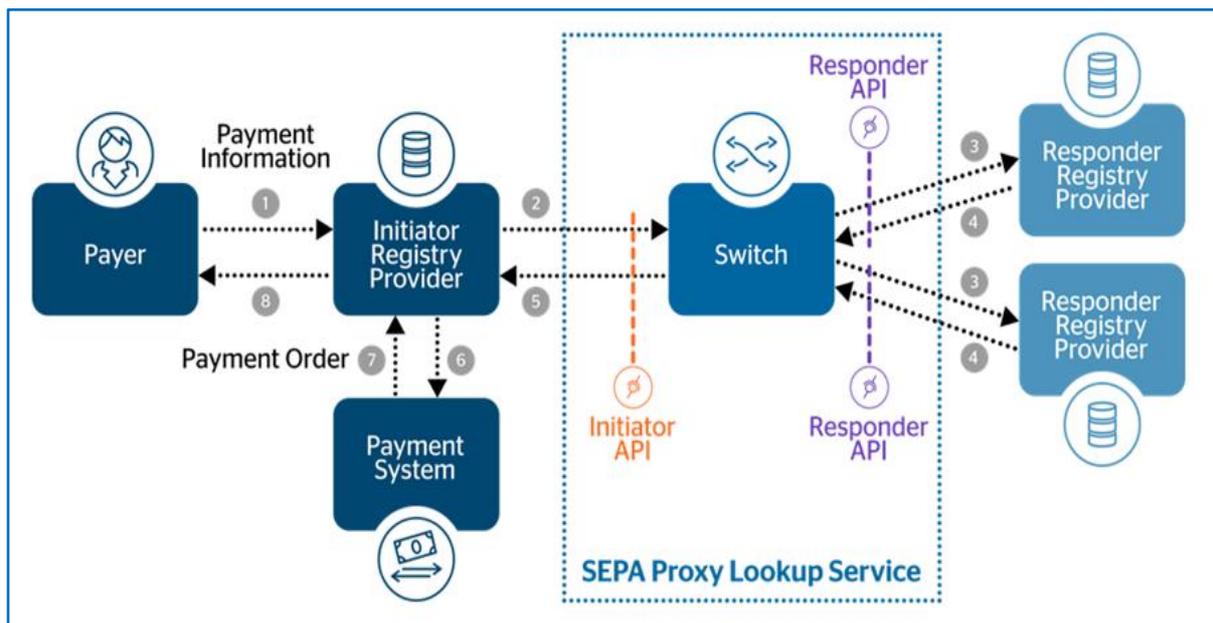


Figure 33: The SEPA Proxy Lookup Service

The major functionalities of the SPL service are the management of the participants, namely the Initiator Registry Provider (IRPs) and the Responder Registry Providers (RRPs), the implementation of the APIs to IRPs and RRP, the implementation of the mapping (mobile number to IBAN). Besides that, the SPL service also contains support functions like reporting, statistics and billing. The IRPs can also offer, as an optional feature, to perform a “Reachability Check” as part of their on-boarding process of (new) customers. This would allow the IRP to inform their customers about which contacts included in their mobile device are reachable via the SPL service.

The following figure illustrates the customer experience and flow for a standard MSCT transaction using the SPL service. The steps 8 through 10 show the execution of the MSCT transaction which is outside the scope of the SPL service.

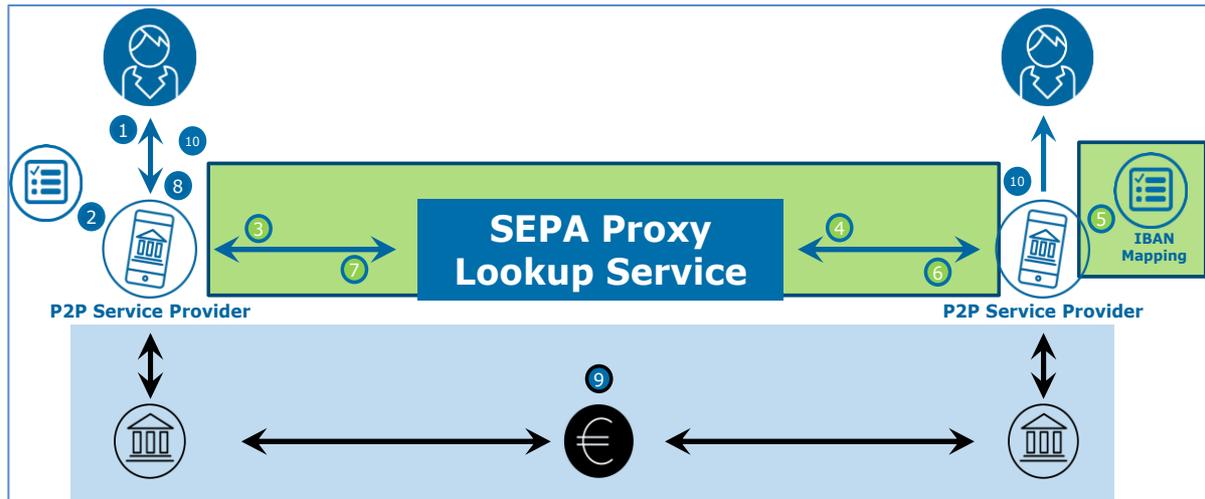


Figure 34: MSCT using the SEPA Proxy Lookup Service

In the figure above, the following steps are illustrated:

Step 0 (prerequisites)

Both the payer's and the payee's mobile P2P service providers should be registered participants in the SPL service.

Both the payer and payee have been on-boarded with their respective mobile P2P service providers with their respective mobile phone number for the respective mobile P2P service.

Step 1 (outside the SPL scheme)

The payer opens the mobile application of their mobile P2P service provider to transfer funds to the payee. The mobile P2P application checks the phone book of the payer on their mobile device to retrieve the mobile number of the payee.

Step 2 (outside the SPL scheme)

Subsequently based on this mobile phone number, the payer's mobile P2P payment service provider checks first if the payee is a known customer in their local directory, in which case the IBAN and name of the payee are retrieved. If not, it checks the phone book of the payer to get the mobile number of the payee.

Step 3

If not present in their local directory, the payer's mobile P2P payment service provider sends a request to the SPL service provider with the payee's mobile phone number.



Step 4

The SPL service provider transfers in parallel the request to a subset of registered mobile P2P payment service providers, based on the country code included in the mobile phone number

Step 5

Each mobile P2P payment service provider checks its customer base if the mobile phone number is known.

Step 6

The mobile P2P payment service provider returns the corresponding IBAN if a match is found.

Step 7

The SPL chooses the payee's account data based on the SPL scheme rules if multiple replies are received.

Step 8 (outside the SPL scheme)

The payer's mobile P2P payment service provider requests the payer a strong customer authentication based on the payee account data and transaction amount.

Step 9 (outside the SPL scheme)

The (instant) credit transfer is initiated by the payer's mobile P2P payment service provider and the funds are transferred towards the payee's ASPSP.

Step 10 (outside the SPL scheme)

- The payee is optionally informed by their mobile P2P payment service provider that their account has been credited.
- The payer is optionally informed by their mobile P2P payment service provider that their account has been debited.

In further developments (see Chapter 16) also different mappings could possibly be requested from the SPL service provider (e.g., payee name, mail addresses as proxy). The technical solution used for the SPL service has been designed to cope with potential new functionalities.

15.4 Request-to-Pay service

The "Request-to-Pay" (RTP) was first defined in the E-invoicing Presentment and Payment (EIPP) context as a technical message representing a claim for payment sent by a payee (payee) to a payer, which provides the necessary information for the initiation of a payment by the payer. The ERPB Working Group on EIPP solutions identified the RTP in 2017⁹⁰ as the key linkage and integration component in EIPP solutions. Following-up on the conclusions of this group, the EPC coordinated a multi-stakeholder group on EIPP (EIPP MSG) which identified an ISO 20022 message pair for RTP (pain.013 and pain.014) and updated these messages to support the attachment of e-invoice documents and other business requirements specific to EIPP (see [32]).

⁹⁰ see https://www.ecb.europa.eu/paym/retpaym/shared/pdf/8th-ERPB-meeting/EIPP_working_group_report.pdf?522a05eb9fde0192136bc7fdf062ac4f



In parallel the EPC has observed that initiatives have been launched which enable the use of the RTP in business contexts beyond e-invoicing, for any claim of payment by a creditor/ payee, sent to a debtor/payer. As reflected in the statement published after the ERPB meeting of November 2018⁹¹, the EPC was invited to coordinate the necessary work in this area and as a result, the RTP multi-stakeholder group (RTP MSG) was created in the beginning of 2019. The objective of this group was to analyse and prepare the concrete and rapid exploitation of the RTP functionality from a broader perspective, also based on the outcome of the work of the EIPP MSG in relation with the RTP and on the results of the work performed by the EPC Multi-Stakeholder Group on mobile initiated SCT and SCT Inst (MSCT MSG).

In addition to requesting the payment of the invoices, the broader perspective for RTP will cover the request of payment for goods and services in the retail context, both for in-store and e-and m-commerce, as well as in P2P context. The scope of work of the RTP MSG includes several topics. The first is the analysis of how the existing ISO 20022 RTP messages can be used in this extended context as additional layers to the SCT Inst and SCT payment schemes. Another topic is the analysis for complementing the MSCT use-cases (see Chapter 7) with RTP functionality when the need for such functionality is identified. Subsequently, the RTP MSG will assess the different options how to extend the RTP functionality to other environments than the inter-PSP network, such as messaging platforms for P2P, proximity communications, e- and m-commerce applications. Providing guidelines for secure and trustworthy interoperability between various types of actors within ecosystems using the RTP functionality, is also in the scope of the RTP MSG. As such the outcome of this RTP work will enhance the customer experience for MSCTs and will complement the MSCT interoperability guidance.

The RTP is a messaging functionality. It is not a payment means or a payment instrument, but a way to request a payment initiation.

In a simplified view, the RTP-related process components can be illustrated as follows:



Figure 35: RTP process components and context

From the transmission perspective, the SRTP scheme [28] is channel-agnostic and the RTP can be transmitted from the payee to the payer, through the RTP service provider participants to the scheme by any secured channel. In addition, the payer can directly receive an RTP by the payee through various environments such as proximity technologies, messaging applications, dedicated APIs, etc.

Both payee and payer use their own RTP service provider. The payee can send RTPs to the reachable payers through routing entities. In any case, the identifier of the payer and the payer's RTP service

⁹¹ see <https://www.ecb.europa.eu/paym/retpaym/shared/pdf/10th-ERPB-meeting/Statement.pdf?32cf8f15483d29182fc1d72f40bbf7b4>



provider has to be known by the payee or the payee’s RTP service provider (prior to issuing an RTP), so that the payee’s RTP service provider is able to route the RTP to the payer’s RTP service provider.

For simplification and as out of scope for the SRTP rulebook, the payment flows are not presented in the below diagram. It should be noted that in a more complex scenario, the PSPs of the payee and/or payer could be different entities from the RTP service providers.

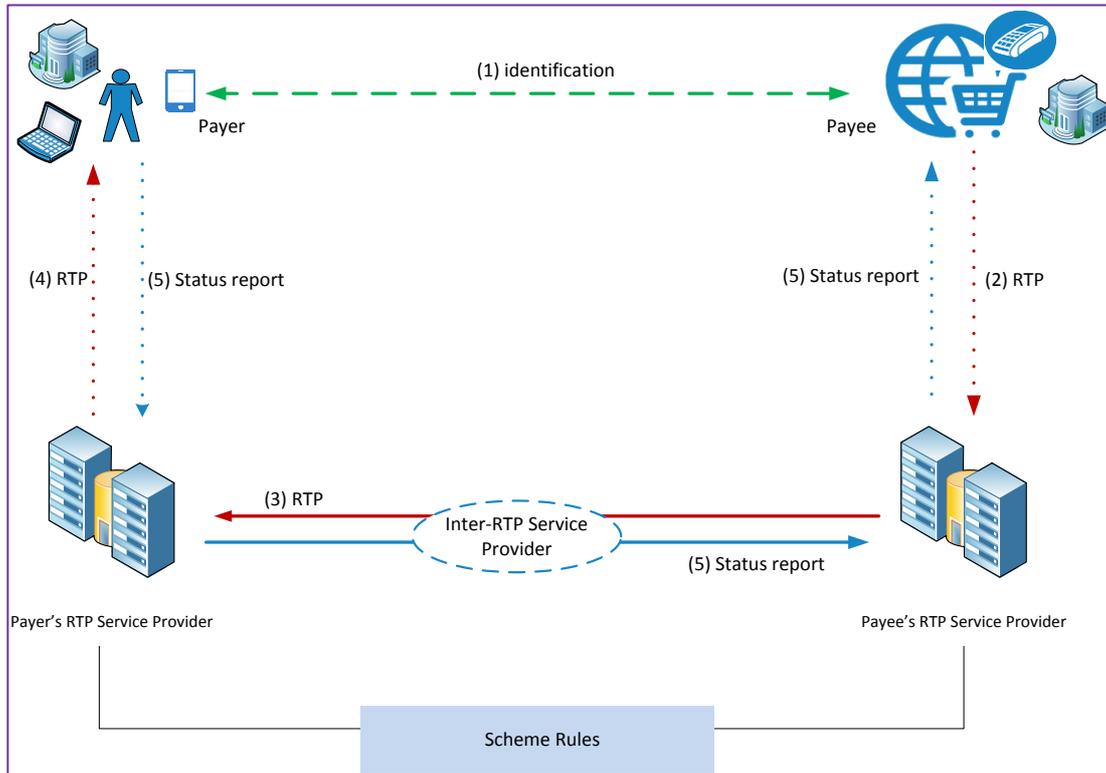


Figure 36: RTP actors and information flow in 4-corner eco-system

Step 1

A first interaction enables the communication of the payer’s identifier and payer’s RTP service provider identifier.

Note: The identification and authentication are agreed between the payer/payee and their respective RTP service providers.

Step 2

The RTP is sent by the payee to its RTP service provider. It contains all RTP core data, including the payer’s identifier.

Step 3

The RTP is sent through the inter-RTP service provider network.

Step 4

The RTP is presented to the payer on its agreed channel or device (e.g. smartphone, web browser, etc.).



Step 5

The acceptance/refusal of the RTP by the payer is sent back to the payee through the inter-RTP service provider environment.

It is envisaged that the SRTP Scheme will evolve further over time to support more elaborated functionalities.



16 Overview MSCT interoperability aspects

16.1 Introduction

As illustrated in various MSCT use cases (see Chapter 7), implementations for MSCTs in the market today, being based on payee- or payer-presented data, involve often the same MSCT service provider, both on the payer and payee side. They are sometimes referred to as a “closed loop” models, whereby both the payer and the payee are customers of the same MSCT service provider. These MSCT models are applicable for P2P, C2B (in this case the payer is a consumer and the payee is a merchant) and B2B (instant) payment contexts and typically cover a certain geography (e.g., within (part of) a country).

16.1.1 Current model for MSCTs based on payee-presented data

In the figure below, the model is depicted for MSCTs based on payee-presented data that are currently in the market, whereby both the payer and payee are customers of the same MSCT service provider.

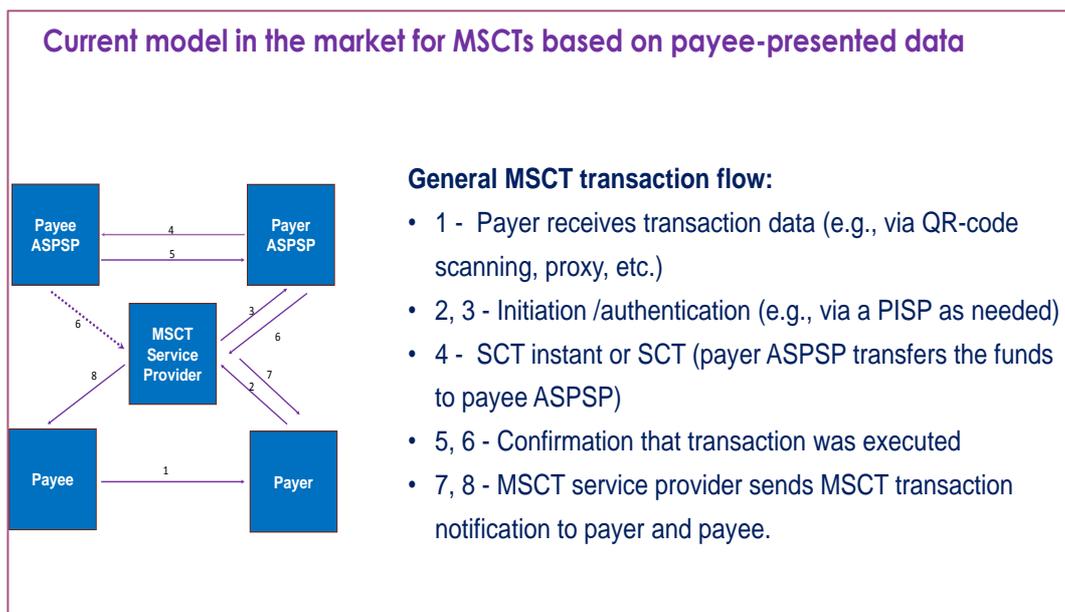


Figure 37: Model for MSCTs based on payee-presented data

Note: The dotted line between the MSCT service provider and the payee ASPSP means that for some MSCT services, this link may be present, in others there is no link.

In order to achieve interoperability for MSCTs, the main issue is how to interconnect these different (closed loop) MSCT services as illustrated in the figure below.



How to interconnect different MSCT services based on payee-presented data?

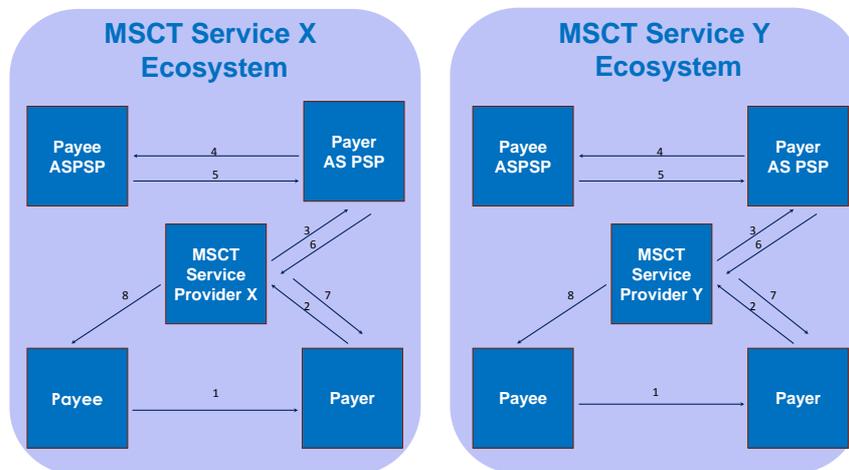


Figure 38: How to interconnect different MSCT services based on payee-presented data?

16.1.2 Current model for MSCTs based on payer-presented data

In the figure below, the model is depicted for MSCTs based on payee-presented data that are currently in the market, whereby both the payer and payee are customers of the same MSCT service provider.

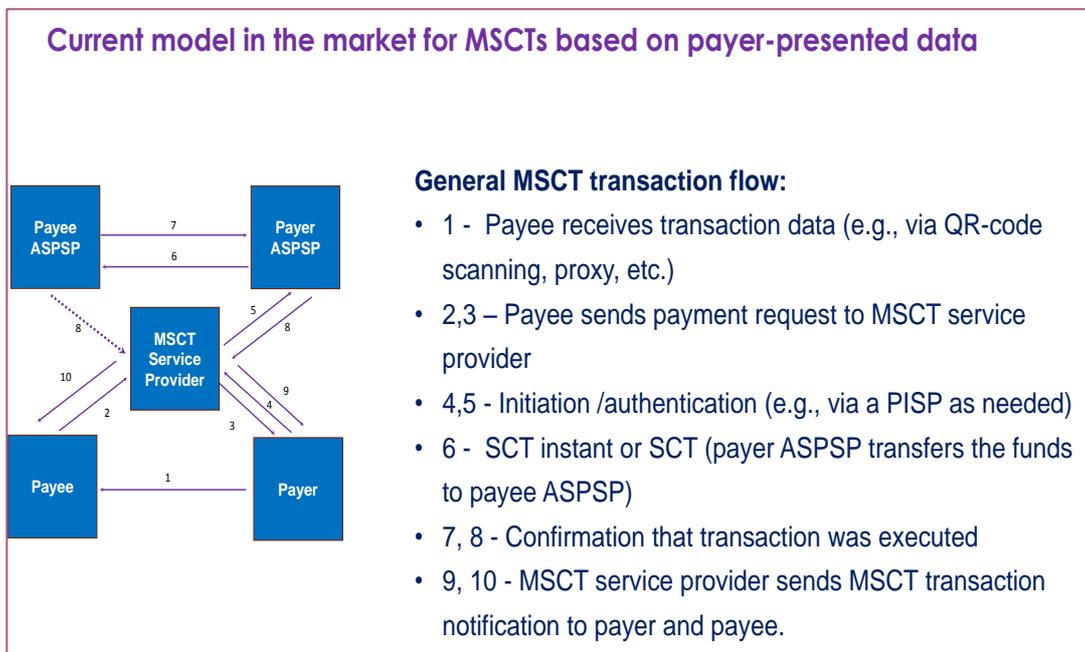


Figure 39: Model for MSCTs based on payer-presented data

Note: The dotted line between the MSCT service provider and the payee ASPSP means that for some MSCT services, this link may be present, in others there is no link.



In order to achieve interoperability for MSCTs, the main issue is how to interconnect these different (closed loop) MSCT services as illustrated in the figure below.

How to interconnect different MSCT services based on payer-presented data?

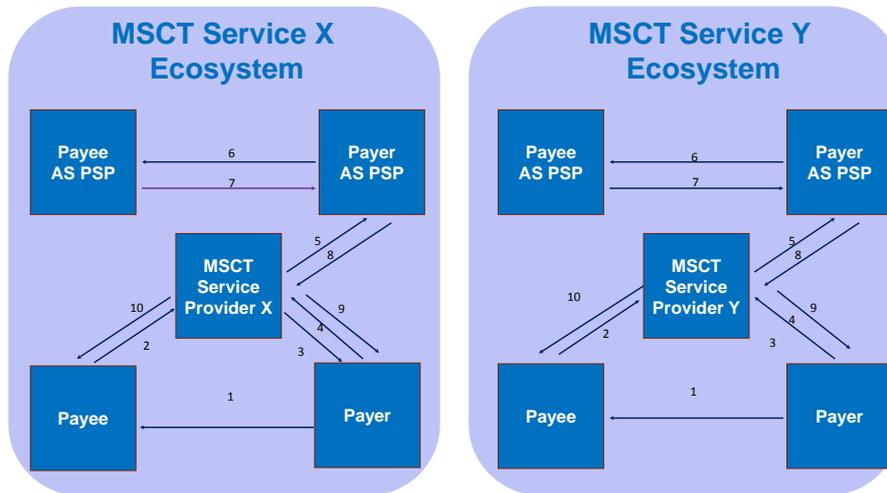


Figure 40: How to interconnect different MSCT services based on payer-presented data?

16.2 MSCT interoperability analysis

In this section a brief analysis will be performed on the main interoperability aspects for MSCTs. For both models, the MSCT service provider X is already connected to the payer’s ASPSP. The interconnection needed during the execution of the Instant SCT or SCT transfer⁹², to ensure interoperability across SEPA, is already covered in the SCT Inst and SCT rulebooks (EPC004-16 and EPC125-05 respectively).

As a consequence, this document will focus for an MSCT transaction on what is referred to in **Figure 28** and **Figure 29** in Chapter 8 as *Payment Preparation (or prepayment), Initiation and Authentication* and *Payment Completion* phases related to an Instant SCT or SCT transaction.

It should further be noted that for mobile initiated SCT Inst or SCT transactions, the strong customer authentication of the payer by their ASPSP is in the payer-to-payer’s ASPSP domain and is as such not impacting the interoperability. Neither is the interoperability impacted if the payer’s ASPSP has delegated the strong customer authentication to the payer’s MSCT service provider or to a so-called authentication service provider.

For MSCTs whereby a PISP is involved which is different to the MSCT service provider, the functionality needed to enable the requirements identified in this document for interconnectivity amongst MSCT service providers should be ensured. However these functionalities will not be discussed in further detail in this document.

⁹² This means after the transaction has been sent by the payer’s ASPSP following the receipt of the SCT Inst or SCT initiation request and the subsequent authentication of/confirmation by the payer.



16.2.1 Person-to-Person (P2P) MSCTs

P2P payments are mostly based on payee-presented data. For these MSCTs, the interoperability between the different P2P MSCT solutions, when a proxy is used for the payee such as a mobile phone number or e-mail address, the interoperability is ensured by the implementation of the SPL scheme (see section 15.3). The SPL scheme covers already today various proxy types and mandates the return of the payee's IBAN for the proxy but not necessarily the payee's name. This may be an issue in case the payee's name is not known by the payer or by the MSCT app on their mobile device, more in particular related to the dynamic linking required for MSCTs (see section 8.4).

The implementation and success of the SPL scheme is crucial for ensuring a SEPA-wide interoperability for these P2P MSCT payments. In principle this scheme could be considered sufficient from a pure "technical perspective" if the payee is known by the payer, to achieve full interoperability.

For P2Ps based on payer-presented data, a payment request message from the payee will be involved – a further analysis is conducted in Chapter 18.

16.2.2 Customer-to-Business (C2B) MSCTs

As said before, most current market solutions are all based on the models depicted in whereby both the payer and the payee have on-boarded (registered) with the same MSCT service provider.

In view of the fact that many SEPA countries have already adopted these "closed loop" MSCT solutions today and the critical time to market, it is considered to be challenging to specify one single SEPA-wide MSCT solution where all existing countries would have to migrate to, and this from different perspectives: competitiveness, cost-effectiveness, customer experience and timeliness to market.

To achieve SEPA-wide interoperability, one should rather look how to connect the multiple existing MSCT solutions. Hereby, two main areas would need to be addressed:

- How to "standardise" the transfer of merchant/transaction data to the consumer – ideally, independently of the technology, while ensuring the security of the link merchant name – IBAN_merchant?
- How to interconnect the MSCT service provider back-end systems so that when a consumer that is on-boarded with MSCT service "X" can make a purchase with a merchant that takes part in MSCT service "Y"?

16.2.3 Business-to-Business (B2B) MSCTs

For B2B, the reconciliation on the payee side appears to be a major issue – more in particular for SCT Inst payments; although it should be recognised that this problem reaches obviously beyond MSCTs. Immediate information on the incoming payments, processed by the payee's ASPSP (individual transaction, push) or on request by the corporate (individual transaction, pull) are strongly demanded features in view of the usability of SCT Inst by corporates. With SCT Inst, the EPC has defined messages from initiator to ASPSP, from ASPSP to ASPSP (pacs.008) and ASPSP to initiator



but not from ASPSP to payee. Corporates would like to see an immediate “ASPSP to payee message” in the context of SCT Inst closing the chain of information from initiator to payee.

In addition, for all payment contexts described, and as already mentioned in section 8.7, the following *acknowledgement and notification messages* have been identified as being key factors for PSU adoption:

- Acknowledgement of receipt to the payer by their MSCT service provider of the instruction for an MSCT based on SCT involving payee-presented data;
- Acknowledgement of receipt to the payee by their MSCT service provider of the payment request message for MSCTs based on SCT involving payer-presented data
- Notification of reject/successful/unsuccessful transaction to the payee by their MSCT service provider;
- Notification of reject/successful/unsuccessful transaction to the payer by their MSCT service provider.

The interoperability aspects related to these messages will be further analysed in the Chapters 17 and 18.

16.3 MSCT interoperability layers

16.3.1 Introduction

The different technical interoperability aspects described in the previous sections could be represented in a 3-layer approach as shown in the figure below. Since the interoperability in the inter-PSP space is already covered in the respective scheme rulebooks, this document will focus on the interoperability aspects related to MSCTs in the PSU and MSCT service provider layers as depicted in the figure below.

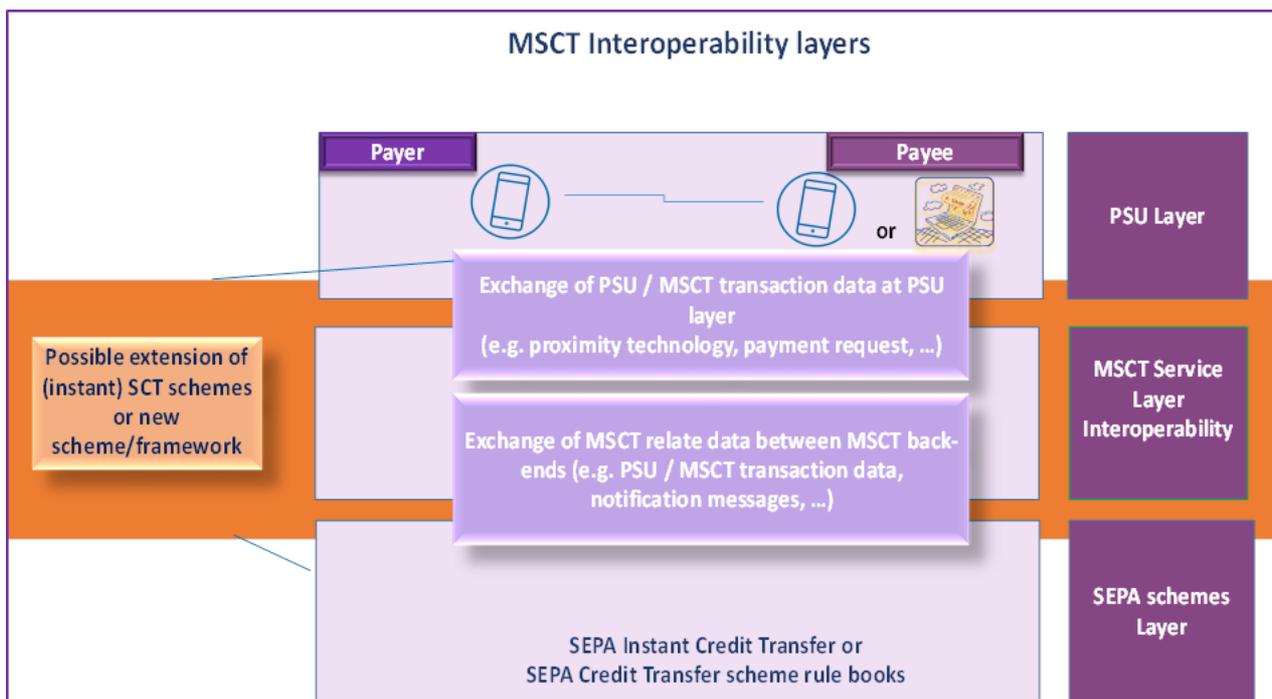


Figure 41: MSCT interoperability layers



In what follows, a high level overview will be provided on potential solutions for this interoperability gaps.

16.3.2 PSU layer

It is generally recognised that the PSU layer, being it the MSCT application on the payer's mobile device or the MSCT application on the merchant's POI, is in the competitive space of the MSCT service. However, a minimum standardisation would be needed on how the PSU/ transaction data are exchanged between the payer and the payee.

In case the payee's name, IBAN and transaction amount are known/ entered on the mobile device by the payer, the respective SCT Inst and SCT schemes would ensure interoperability for MSCTs. In all other cases, e.g. if proximity technologies, payment request messages, proxies or tokens are used to exchange this data, interoperability issues arise. Those issues will be further analysed in Chapters 17 and 18.

16.3.3 MSCT service layer

The interoperability solutions at this layer will depend on the type of PSU/transaction data that has been exchanged between the payer and payee at the PSU layer.

In case, the full PSU/transaction data needed for the initiation of an SCT Inst or SCT is exchanged directly in clear between the payee and the payer, the MSCT transaction can be immediately initiated by the payer while the SCT Inst and SCT scheme rules ensure the interoperability.

In case the transaction data exchanged contains a token or proxy, the corresponding transaction data in clear-text needs to be retrieved via the appropriate entity (e.g. payer's or payee's MSCT service provider) before the MSCT transaction can be initiated. Moreover, the appropriate transaction data including the payee name / trade name / IBAN and transaction amount need to be displayed to the consumer for authentication of the MSCT transaction. This means that dedicated messages will need to be exchanged between the MSCT service provider back-ends to cover for these functionalities.

Also the infrastructure needed to exchange the notification messages⁹³ to the payer and payee (see sections 8.7 and 16.2) would need to be developed as well as the standardisation of the minimum data elements required in the message flows between MSCT service providers (see Chapter 19).

16.4 MSCT interoperability model based on a HUB

To achieve MSCT interoperability for a generic basic 4-corner model, the concept of a HUB is introduced in this document to interconnect the respective MSCT service providers as shown in the figure below.

Hereby it is assumed that both payer and payee have different ASPSPs that are SCT Inst or SCT scheme participants (see Chapter 4), while the entities assuming the role of MSCT service provider are depicted as separate entities that are different for the payer and the payee.

⁹³Currently the SCT Inst Scheme rulebook only requires the transmission of the negative confirmation message as notification by the payer's ASPSP to the payer (see [21]).



The term HUB is used to indicate an “infrastructure” that enables interconnectivity between the respective MSCT service providers but it is meant to be agnostic to the way it might be implemented – different implementation models may be possible (centralised or de-centralised (e.g. a direct API)).

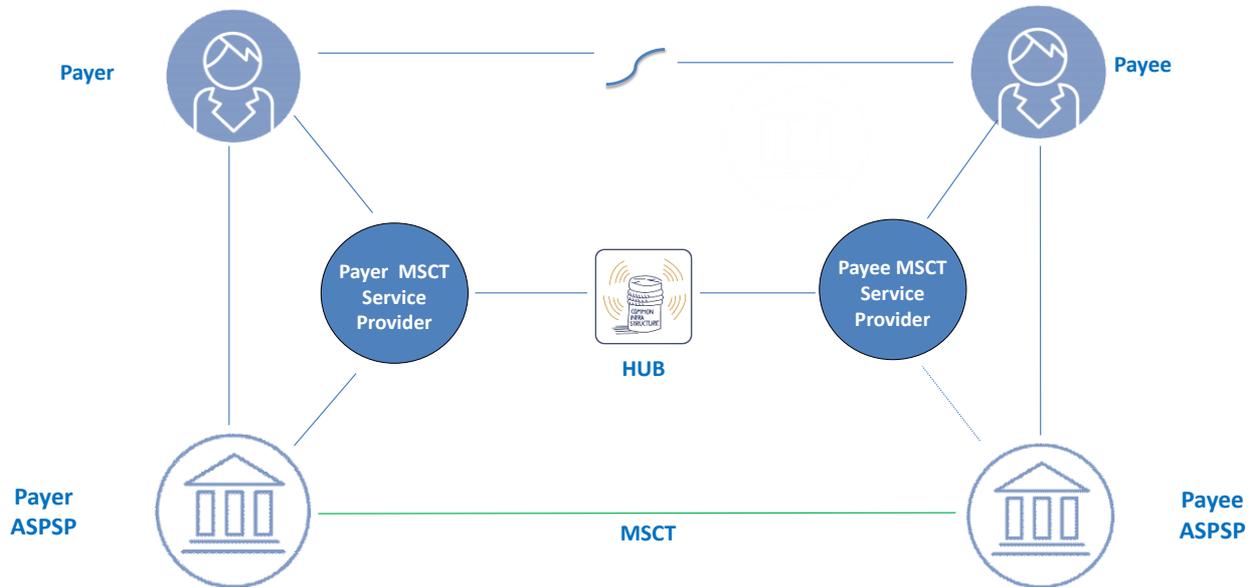


Figure 42: Generic 4-corner MSCT interoperability model

Obviously, if the role of MSCT service provider would be assumed by an ASPSP the model below would simplify. Alternatively, if multiple PSPs (such as a PISP licensed under PSD2 or a Collecting PSP on behalf of the merchant (CPSP)) would be involved between the PSU and their MSCT service provider / ASPSP, this model might become more complex.

Note: The payer’s MSCT service provider is linked to the payer’s ASPSP and the payee’s MSCT service provider may⁹⁴ be linked to the payee’s ASPSP (this linkage may include both technical and contractual aspects).

The forthcoming chapters specify the requirements on the HUB to achieve interoperability of MSCTs, respectively for MSCTs based on payee-presented data (Chapter 17) and payer-presented data (Chapter 18). The models involving a PISP or CPSP are analysed in Chapter 20.

⁹⁴ represented by a dotted line.



17 Technical interoperability of MSCTs based on payee-presented data

17.1 Introduction

This chapter analyses in more detail the interoperability of MSCTs based on payee-presented data. As mentioned before it focuses on the interoperability of MSCT at the PSU layer and the MSCT service (provider) layer. Hereby two main functionalities will be covered:

- The exchange of the transaction data that enables the initiation of the MSCT;
- The acknowledgement/notification messages sent to the payer and payee after a successful/unsuccessful transaction or a reject.

Next to the specification of the MSCT interoperability requirements for the HUB, based on the generic 4-corner model, illustration of transaction process flows involving the HUB for successful transactions, rejects and unsuccessful transactions are included.

The chapter further defines the minimum data set to be exchanged between payee and payer for this type of MSCTs and specifies a payee-presented QR-code for MSCTs, followed by some examples of payload data for this QR-code.

17.2 Exchange of MSCT transaction data

With respect to the availability of the transaction data (payee data and payment data) needed by the payer for the initiation of the MSCT transaction the following cases need to be considered:

- *Part of the payee data is not known by the payer and a proxy is used instead (e.g., for P2P payment, a mobile phone number is used as a proxy instead of an IBAN):* in this case, the MSCT service provider of the payer needs to be able to retrieve the payee's IBAN/name from the proxy used. This generally requires the support of the payee's MSCT service provider and/or ASPSP.
- *The transaction data (payee and payment data) is exchanged through a proximity technology (QR-code, NFC, BLE, etc.)* between the payee and the payer.

Hereby the following distinctions need to be made:

- The payee-presented data includes a "token": in this case, a de-tokenisation process needs to take place such that the transaction data can be derived from the token and provided to the payer via their MSCT service provider. This generally requires the support of the payee's MSCT service provider (see *Transaction information request/Transaction information response* messages in section below) prior to the initiation of the MSCT transaction.
- The payee-presented data includes all transaction data in "clear" (e.g. the payee's name, trade name, IBAN of the payee, transaction amount, transaction identifier, etc.). This enables the immediate initiation of the MSCT transaction.
- Only part of the transaction data is exchanged between the payee and the payer through a proximity technology or only part of the transaction data exchanged is in clear (e.g. payee-presented data contains a proxy). In this case the complete transaction data needs to be provided by the payee's MSCT service provider upon



request from the payer’s MSCT service provider (see *Transaction information request/Transaction information response* messages in section 17.5 below) prior to the initiation of the MSCT transaction.

From the analysis made above, requirements can be derived for the HUB to support the transaction data exchange needed for the interoperability of MSCTs based on payee-presented data. The table below list the required functionalities for the HUB for this exchange of transaction data

MSCT transaction feature	Requirements on HUB
Exchange of transaction data Payment Preparation phase (see Figure 28 and Figure 29)	MSCTs based on SCT Inst or on SCT
All transaction data is available “in clear” to the payer (e.g. in clear in QR-code or known to the payer) ⁹⁵	Not applicable
Payer uses a proxy for the payee	Translation of proxy into payee’s name and IBAN <i>Transaction information request</i> and <i>Transaction Information response</i> messages between MSCT service providers
Payee-presented transaction data includes a token (It is hereby assumed that the tokenisation/de-tokenisation is handled by or via the payee’s MSCT service provider)	De-tokenisation into transaction data is needed <i>Transaction information request</i> and <i>Transaction information response</i> messages between MSCT service providers
Payee-presented transaction data is incomplete (e.g. contains part of the transaction data “in clear”)	Completion of the transaction data is needed by the payee’s MSCT service provider <i>Transaction information request</i> and <i>Transaction information response</i> messages between MSCT service providers

Table 26: Required HUB functionalities for exchange of transaction data for MSCTs based on payee-presented data

17.3 Acknowledgement/notification messages

The following messages have already been identified in sections 8.7 and 16.2 in this respect:

- Acknowledgement of receipt of the SCT instruction provided to the payer by their MSCT service provider;
- Notification of payment to the payee by their MSCT service provider;
- Notification of payment to the payer by their MSCT service provider.

⁹⁵ In this case, another mechanism would need to be implemented to ensure the integrity of the data.



Note: The acknowledgement of receipt of the SCT Inst instruction to the payer is not considered in view of the immediacy of the MSCT transaction.

17.3.1 Acknowledgement of receipt of MSCT instruction based on SCT to the payer

For MSCTs that are based on SCT⁹⁶, where there is no immediacy of payment, it might be useful for the payer to receive a confirmation that the MSCT instruction has been well-received by their MSCT service provider. However, since this acknowledgement message is not impacting the interoperability of MSCTs because it is in the payer-to-payer ASPSP space, it will not be further discussed in this document.

17.3.2 Notifications of successful MSCT transactions

This section describes the *notification of successful transaction* messages that need to be supported to duly inform the payee and the payer for MSCTs based on payee-presented data.

17.3.2.1 MSCTs based on SCT Inst

Notification to payee

For all payment contexts, the *notification to the payee* about a *successful MSCT transaction based on SCT Inst* (i.e. after the receipt of the confirmation 6 by the payer's ASPSP in **Figure 1**) requires the following messages to be supported:

Notification to payee	
Successful transactions for MSCTs based on SCT Inst with payee-presented data	
1.	<i>Notification of successful transaction</i> by the payer ASPSP to the payer MSCT service provider.
2.	<i>Notification successful transaction</i> by the payer MSCT service provider to the payee MSCT service provider.
3.	<i>Notification successful transaction</i> by the payee MSCT service provider to the payee.
	Or
	<i>Notification of successful transaction</i> by the payee ASPSP to the payee (for specific cases only).

Table 27: Overview of messages for notification to payee of successful MSCTs based on SCT Inst with payee-presented data

⁹⁶ For MSCTs based on SCT Inst, this acknowledgement is not needed in view of the immediacy of the payment.



Notification to payer

For all payment contexts, the *notification to the payer* about a *successful MSCT transaction based on SCT Inst* (i.e. after the receipt of the confirmation 6 by the payer’s ASPSP in **Figure 1**) requires the following messages to be supported:

Notification to payer	
Successful transactions for MSCTs based on SCT Inst with payee-presented data	
	<ol style="list-style-type: none"> 1. <i>Notification of successful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of successful transaction</i> by the payer MSCT service provider to the payer.

Table 28: Overview of messages for notification to payer of successful MSCTs based on SCT Inst with payee-presented data

17.3.2.2 MSCTs based on SCT

Notification to payee

For all payment contexts, the *notification to the payee* about a *successful initiation of an MSCT transaction based on SCT* (i.e. after the transfer of the SCT transaction message 3 by the payer’s ASPSP in **Figure 2**) requires the following messages to be supported:

Notification to payee	
Successful transaction initiation for MSCTs based on SCT with payee-presented data	
	<ol style="list-style-type: none"> 1. <i>Notification of successful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification successful transaction</i> by the payer MSCT service provider to the payee MSCT service provider. 3. <i>Notification successful transaction</i> by the payee MSCT service provider to the payee. <p>Or</p> <p><i>Notification of successful transaction</i> by the payee ASPSP to the payee (for specific cases only).</p>

Table 29: Overview of messages for notification to payee of successful MSCTs based on SCT with payee-presented data



Notification to payer

For all payment contexts, the *notification to the payer* about a *successful MSCT transaction based on SCT* (i.e. after the receipt of the confirmation 6 by the payer’s ASPSP in **Figure 2**) requires the following messages to be supported:

Notification to payer	
Successful transactions for MSCTs based on SCT Inst with payee-presented data	
	<ol style="list-style-type: none"> 1. <i>Notification of successful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of successful transaction</i> by the payer MSCT service provider to the payer.

Table 30: Overview of messages for notification to payer of successful MSCTs based on SCT with payee-presented data

For MSCTs based on SCT, also a guarantee of payment⁹⁷ could be considered, but falls outside the scope of this document⁹⁸.

From the analysis made above, requirements can be derived for the HUB to support the notification of successful transactions needed for the interoperability of MSCTs based on payee-presented data. The table below list the required functionalities for the HUB for this.

MSCT transaction feature	Requirements on HUB	
	SCT Inst	SCT
Notification messages Payment Completion phase, (see Figure 28 and Figure 29)		
Notification to payee about successful transaction	Notification from payer’s MSCT service provider to payee’s MSCT service provider	Notification from payer’s MSCT service provider to payee’s MSCT service provider
Notification to payer about successful transaction	Not applicable	Not applicable

Table 31: Required HUB functionalities for notification of successful transactions for MSCTs based on payee-presented data

⁹⁷ This could potentially be addressed by a dedicated MSCT interoperability framework.

⁹⁸ Note that this is planned to be addressed in phase 2 of the SEPA RTP scheme under development.



17.3.3 Notifications of unsuccessful transactions and rejects for MSCTs

17.3.3.1 MSCTs based on SCT Inst

For MSCTs with payee-presented data based on SCT Inst, the following categories for rejects and unsuccessful transactions could be distinguished.

Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payee-presented data	
Cat 1	Reject by the payer MSCT service provider (before initiation to payer ASPSP)
Cat 2	Reject by payer ASPSP before execution of the SCT Inst (i.e. before message 2 in Figure 1)
Cat 3	Unsuccessful transaction - receipt by the payer ASPSP of negative confirmation message 6 in Figure 1

Table 32: Overview of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data

Annex 3 provides an overview on errors with MSCTs based on payee-presented data with a mapping on the three categories mentioned above.

The messages in the inter-PSP space related to these *rejects* and *unsuccessful transactions* have been specified in the SCT Inst scheme rule book [21] and the SCT Instant interbank implementation guidelines [22].

Notification to payee

For all payment contexts, the *notification to the payee* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payee	
Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payee-presented data	
Cat 1	<ol style="list-style-type: none"> 1. <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. 2. <i>Notification of reject</i> by the payee MSCT service provider to the payee.
Cat 2	<ol style="list-style-type: none"> 1. <i>Notification of reject</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. 3. <i>Notification of reject</i> by the payee MSCT service provider to the payee.



Cat 3	<ol style="list-style-type: none"> 1. <i>Notification of unsuccessful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification unsuccessful transaction</i> by the payer MSCT service provider to the payee MSCT service provider. 3. <i>Notification unsuccessful transaction</i> by the payee MSCT service provider to the payee. <p>Or</p> <p><i>Notification of unsuccessful transaction</i> by the payee ASPSP to the payee (for specific cases only).</p>
--------------	---

Table 33: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data

***Notification to payer**

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payer	
Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payee-presented data	
Cat 1	<i>Notification of reject</i> by the payer MSCT service provider to the payer.
Cat 2	<ol style="list-style-type: none"> 1. <i>Notification of reject</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of reject</i> by the payer MSCT service provider to the payer.
Cat 3	<ol style="list-style-type: none"> 1. <i>Notification of unsuccessful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of unsuccessful transaction</i> by the payer MSCT service provider to the payer.

Table 34: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data

17.3.3.2 MSCTs based on SCT

For MSCTs with payee-presented data based on SCT, the following categories for rejects and unsuccessful transactions could be distinguished.

Rejects and unsuccessful transactions for MSCTs based on SCT with payee-presented data	
Cat 1	Reject by the payer MSCT service provider (before initiation to payer ASPSP)
Cat 2	Reject by payer ASPSP before execution of the SCT (i.e. before message 3 in Figure 2)



Cat 3	Unsuccessful transaction - receipt by the payer ASPSP of a “Reject” or “Return” message ⁹⁹ (see DS-03 in the SCT scheme rulebook)
--------------	--

Table 35: Overview of rejects and unsuccessful MSCTs based on SCT with payee-presented data

Note: For MSCTs based on SCT transactions, the notification messages for unsuccessful transactions after the receipt of a “Return” may only be sent up to three days after the settlement date (Cat 3 in the table above).

Annex 3 provides an overview on errors with MSCTs based on payee-presented data with a mapping on the three categories mentioned above.

The messages in the inter-PSP space related to these *rejects and returns* have been specified in the SCT scheme rule book [17] and the SCT interbank implementation guidelines [18].

Notification to payee

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payee	
Rejects and unsuccessful transactions for MSCTs based on SCT with payee-presented data	
Cat 1	<ol style="list-style-type: none"> <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. <i>Notification of reject</i> by the payee MSCT service provider to the payee.
Cat 2	<ol style="list-style-type: none"> <i>Notification of reject</i> by the payer ASPSP to the payer MSCT service provider. <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. <i>Notification of reject</i> by the payee MSCT service provider to the payee.
Cat 3	<ol style="list-style-type: none"> <i>Notification of unsuccessful transaction</i> by the payer ASPSP to the payer MSCT service provider. <i>Notification unsuccessful transaction</i> by the payer MSCT service provider to the payee MSCT service provider. <i>Notification unsuccessful transaction</i> by the payee MSCT service provider to the payee. <p>Or</p> <p><i>Notification of unsuccessful transaction</i> by the payee ASPSP to the payee (for specific cases only).</p>

Table 36: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT with payee-presented data

⁹⁹ Note that a “Return” may be up to three days after the settlement date.



Notification to payer

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payer	
Rejects and unsuccessful transactions for MSCTs based on SCT with payee-presented data	
Cat 1	<i>Notification of reject</i> by the payer MSCT service provider to the payer.
Cat 2	<ol style="list-style-type: none"> <i>Notification of reject</i> by the payer ASPSP to the payer MSCT service provider. <i>Notification of reject</i> by the payer MSCT service provider to the payer.
Cat 3	<ol style="list-style-type: none"> <i>Notification of unsuccessful transaction</i> by the payer ASPSP to the payer MSCT service provider. <i>Notification of unsuccessful transaction</i> by the payer MSCT service provider to the payer.

Table 37: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data

From the analysis made above, requirements can be derived for the HUB to support the notification of unsuccessful transactions and rejects needed for the interoperability of MSCTs based on payee-presented data. The table below list the required functionalities for the HUB for this.

MSCT transaction feature	Requirements on HUB
Notification messages	MSCTs based on payee-presented data
	SCT Inst or SCT
<i>Notification of reject</i> to payee (Table 33 and Table 36 : Cat 1 and 2)	<i>Notification of reject</i> message by payer MSCT service provider to payee MSCT service provider
<i>Notification of unsuccessful transaction</i> to payee (Table 33 and Table 36 : Cat 3)	<i>Notification of unsuccessful transaction</i> message by payer MSCT service provider to payee MSCT service provider
<i>Notification of reject</i> to payer (Table 34 and Table 37 : Cat 1 and 2)	Not applicable
<i>Notification of unsuccessful transaction</i> to payer (Table 34 and Table 37 : Cat 3)	Not applicable

Table 38: Required HUB functionalities for unsuccessful transactions and rejects for MSCTs based on payee-presented data



17.4 Request for recall by the payer

17.4.1 MSCTs based on SCT Inst

The SCT Inst scheme rulebook [21] describes in section 4.3.2.2 “Exception process handling” an “SCT Inst recall” under the R-transactions as follows:

*“An **SCT Inst recall** occurs when the payer ASPSP requests to cancel an SCT Inst transaction. The recall procedure can be initiated only by the payer ASPSP which may do it on behalf of the payer. Before initiating the Recall procedure, the payer ASPSP has to check if the SCT Inst transaction is subject to one of the following reasons only:*

- *Duplicate sending;*
- *Technical problems resulting in erroneous SCT Inst transaction(s);*
- *Fraudulent originated SCT Inst instruction.”*

In the inter-PSP space this procedure is handled via the “Recall of an SCT Inst” (DS-05) and “Answer to a recall of SCT Inst” messages which are specified respectively in sections 4.5.6 and 4.5.7 of SCT Inst rulebook [21]. The rulebook also specifies in section 4.3.2.2 the main characteristics of the “Recall of an SCT Inst” and the “Answer to a recall”.

The SCT Inst rulebook further defines in section 4.3.2.3 a “Request for recall by the payer” as follows:

*“A **Request for recall by the payer** can be initiated by the payer ASPSP after a payer has requested the payer ASPSP to get the reimbursement of a settled SCT Inst transaction for a reason **other than** duplicate sending, technical problems resulting in erroneous SCT Inst transactions or a fraudulently originated SCT Inst instruction.*

The payer ASPSP is obliged to inform the payer that such Request for recall does not guarantee that the payer will effectively receive back the funds of the initial SCT Inst transaction. It will depend on the consent of the payee whether to turn back the funds to the payer.”

The payer shall always be informed by their MSCT service provider (if involved in the Request for recall by the payer) or by their ASPSP about the result of the recall. The payee will typically be contacted directly by their ASPSP if a recall is received from the payer ASPSP, as described in the SCT Inst scheme rulebook ([21], section 4.3.2.2).

17.4.2 MSCTs based on SCT

The SCT scheme rulebook [17] describes in section 4.3.2.3 “Exception process handling” a “Recall” under the R-transactions as follows:

*“A **Recall** occurs when the payer ASPSP requests to cancel an SCT transaction. The recall procedure can be initiated only by the payer ASPSP which may do it on behalf of the payer. Before initiating the Recall procedure, the payer ASPSP has to check if the SCT transaction is subject to one of the following reasons only:*

- *Duplicate sending;*
- *Technical problems resulting in an erroneous SEPA Credit Transfer Transaction;*
- *Fraudulent originated SEPA Credit Transfer Instruction.”*



In the inter-PSP space this procedure is handled via the “Request for Recall” (DS-07) and “Response to request for Recall” (DS-07) messages which are specified respectively in sections 4.5.7 and 4.5.8 of the SCT scheme rulebook [17]. The rulebook also specifies in section 4.3.2.3 the main characteristics of the “Recall” and the “Response to Recall”.

The SCT rulebook further defines in section 4.3.2.4 a “Request for recall by the payer” as follows:

“A Request for recall by the payer can be initiated by the payer ASPSP after a payer has requested the payer ASPSP to get the reimbursement of a settled SCT transaction for a reason other than duplicate sending, technical problems resulting in an erroneous SCT transaction and a fraudulently originated SCT instruction.

The payer ASPSP is obliged to inform the payer that such Request for Recall does not guarantee that the payer will effectively receive back the funds of the initial SCT transaction. It will depend on the consent of the payee whether to turn back the funds to the payer.”

The payer shall always be informed by their MSCT service provider (if involved on the Request for recall by the payer) or by their ASPSP about the result of the recall. The payee will typically be contacted directly by their ASPSP if a recall is received from the payer ASPSP, as described in the SCT scheme rulebook ([17], section 4.3.2.3).

Since these are very exceptional processes both for SCT Inst and SCT for which different communication channels could be used between the PSU and their MSCT service provider or ASPSP, that is not impacting the interoperability amongst MSCT service providers, this *Request for recall by the payer* will not be further analysed in this document.

17.5 Illustrative interoperability process flows for MSCTs based on payee-presented data

17.5.1 Introduction

In this section the full process flows between the HUB and respective MSCT service provider back-ends for a few examples will be described. These examples are provided for illustrative purposes only. Note that as mentioned before, an MSCT service provider could be an ASPSP. This means that in the process flows below, one or both MSCT providers could be one or both of the respective ASPSPs in which case the process flows would simplify.

Seven cases will be considered as listed in the table below.



MSCT transactions	Support from the HUB ¹⁰⁰	Reference
P2P – successful MSCT based on SCT Inst Payer uses a proxy for the payee	<ul style="list-style-type: none"> Retrieval of the payee data from the proxy¹⁰¹ (see section 17.2) Notification of successful transaction (see section 17.3)¹⁰² 	Section 17.5.2
P2P – successful MSCT based on SCT Inst IBAN payee and name payee is known by the payer	Not applicable	Section 17.5.3
C2B – successful MSCT based on SCT Inst Merchant-presented QR-code contains a token	<ul style="list-style-type: none"> Retrieval of the transaction data from the token (see section 17.2) Conditional transaction lock messages (see below) Notification of successful transaction (see section 17.3) 	Section 17.5.4
C2B - successful MSCT based on SCT Inst Merchant-presented QR-code contains all transaction data in clear ¹⁰³	<ul style="list-style-type: none"> Conditional transaction lock messages (see below) Notification of successful transaction (see section 17.3) 	Section 17.5.5
C2B - reject by the payer (consumer) MSCT service provider for MSCT based on SCT Inst Merchant-presented QR-code contains including a token (Table 32: Cat 1)	<ul style="list-style-type: none"> Retrieval of the transaction data from the token (see section 17.2) Notification of reject (see section 17.3) 	Section 17.5.6
P2P - reject by the payer ASPSP service provider for MSCT based on SCT Payee-presented QR-code including a proxy (Table 35: Cat 2)	<ul style="list-style-type: none"> Retrieval of the payee data from the proxy (see section 17.2) Notification of reject (see section 17.3) 	Section 17.5.7
C2B - unsuccessful transaction following a “Return” for MSCT based on SCT Merchant-presented data including a token	<ul style="list-style-type: none"> Retrieval of the transaction data from the token (see section 17.2) Notification of unsuccessful transaction (see section 17.3) 	Section 17.5.8

¹⁰⁰ Depicted by the green arrows in the illustrative process flows below.

¹⁰¹ As an example, this functionality is already covered by the SEPA Proxy Lookup (SPL) Scheme defined by the EPC (see section 15.3).

¹⁰² The functionality to cover for these notification messages could be considered by the SPL scheme as a possible service extension for P2P payments.

¹⁰³ Obviously in this case additional measures should be taken to ensure the security of the data exchanged (see Chapter 10).



(Table 35: Cat 3).		
--------------------	--	--

Table 39: Illustrative process flows for interoperability of MSCT transactions based on payee-presented data with mapping onto HUB functionalities

All process flows for C2B payment contexts in the next sections are illustrated for physical POIs. Note however that the process flows would remain the same if the QR-code is shown on a payment page of an e-merchant.

The QR-code may be static or dynamic. In case dynamic QR-codes are used, a *conditional transaction lock function* is defined as follows. The function consists of conditional lock transaction messages that are sent between the consumer's MSCT service provider and the merchant's MSCT service provider via the HUB to prevent that multiple consumers from different MSCT service providers pay the same transaction after strong customer authentication (see section 8.3). The transaction lock function is required in case the QR-code stays active for a certain time window that would enable multiple scans and related payments and its need is specified in the dedicated Lock Transaction Indicator (LT Indicator as defined in section 17.6 in this document). If two consumers would perform SCA on the same transaction, the consumer with successful SCA for which the lock function sent by their MSCT service provider reaches as first the MSCT service provider of the merchant is the one for which the transaction is locked.

For P2P transactions whereby the payee presents a QR-code on their mobile device to the payer and for C2B transactions involving QR-codes on invoices, the process flow will be similar as for C2B transactions with merchant-presented QR-codes.

Note also that in the process flows below, the representation and description of strong customer authentication (SCA) is simplified since the focus is on the interconnectivity between the respective MSCT service providers. More details on SCA are provided in section 8.3 and are illustrated in the MSCT use cases in Chapter 7.

Furthermore, the process flows do not include potential exchanges needed between MSCT service provider back-ends for applicable remuneration to support a business model.

17.5.2 Successful MSCT - P2P based on SCT Inst with proxy for payee

The process flow below illustrates the usage of the HUB in the case the payer uses a proxy for the payee.

In this MSCT transaction type, the following actors and interconnectivity are required as depicted below.

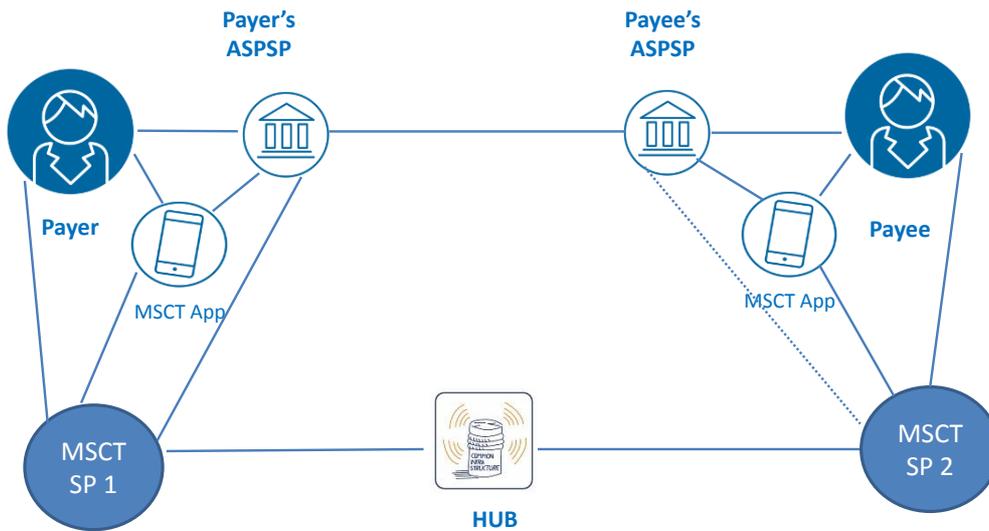
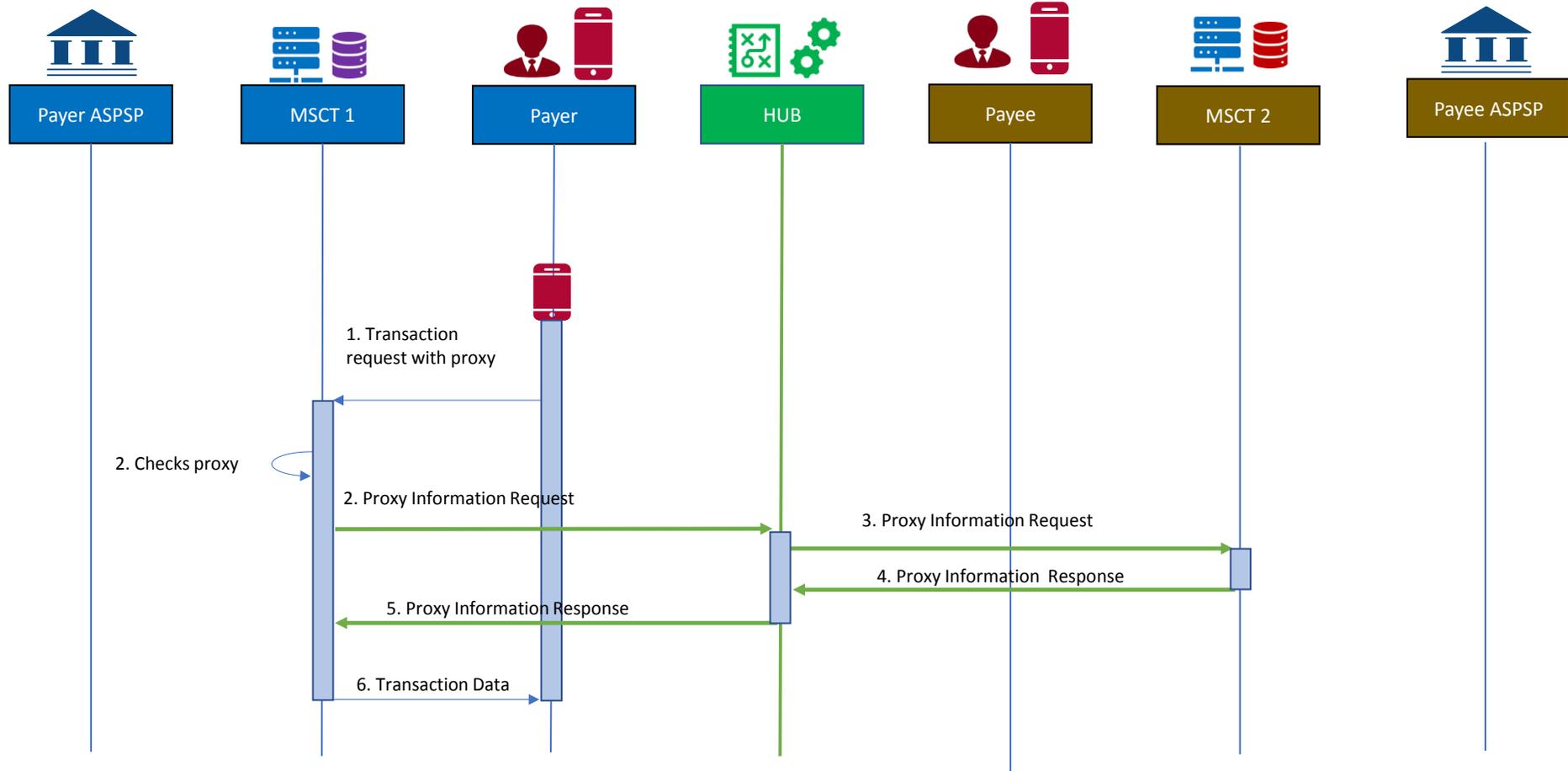


Figure 43: Actors for P2P – with proxy

The detailed process flows between the different actors involved for this MSCT transaction type are shown in the next figure.



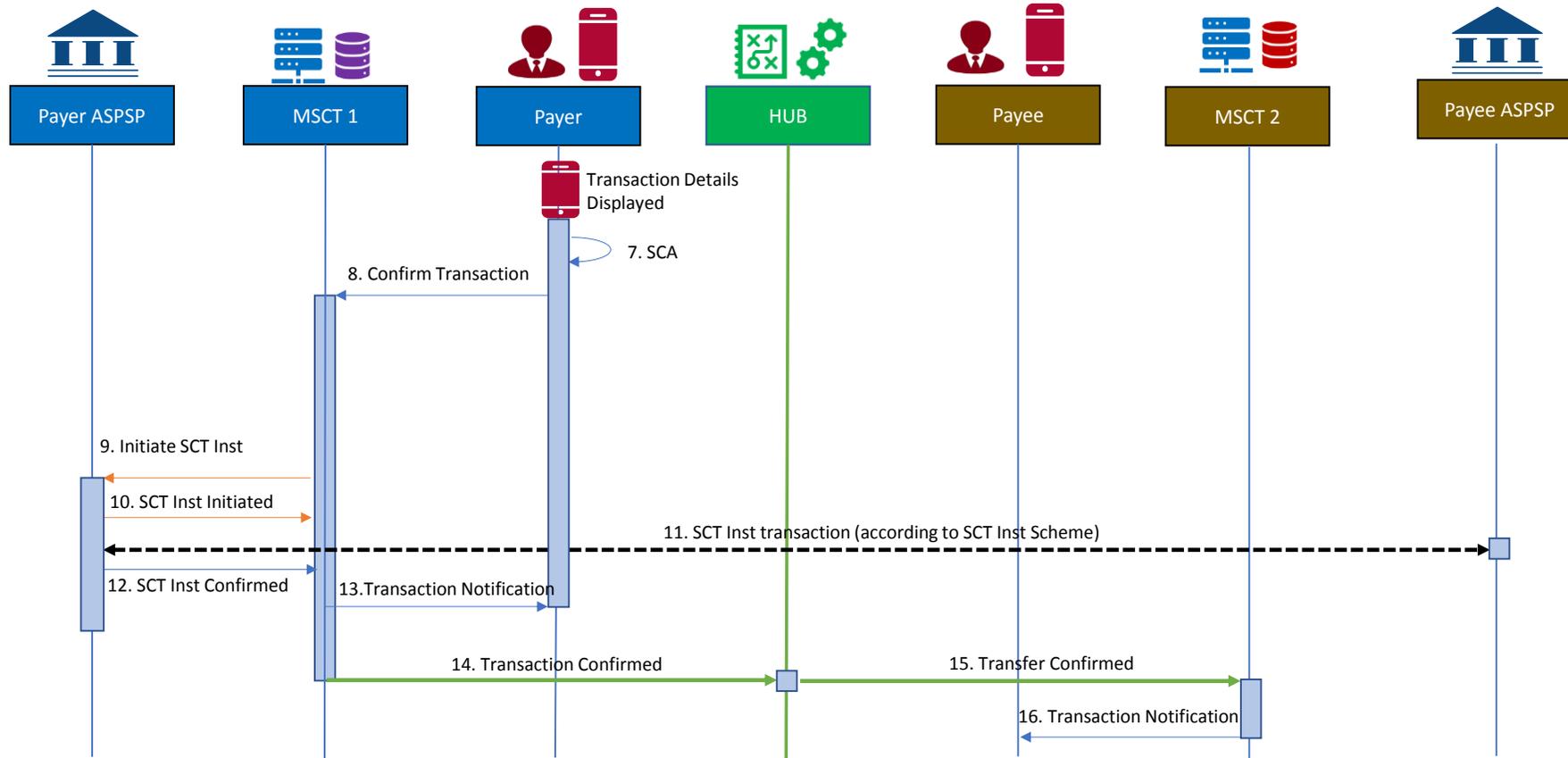


Figure 44: Process flow – P2P – with proxy



In the figure above the following steps are involved:

Step 1:

The payer initiates a new transaction in their MSCT application including the transaction amount and a proxy of the payee which is provided to their MSCT service provider.

Step 2:

The MSCT service provider checks the transaction request received and retrieves the proxy. Next the proxy received is checked in their own directory

- If the IBAN/name of the payee can be retrieved, they are provided to the MSCT app of the payer;
- If the proxy is not available in their own directory, a Proxy Information Request including the proxy is forwarded by the payers' MSCT service provider to the HUB.¹⁰⁴ Note that this is the case illustrated in the figure above.

Step 3:

The HUB forwards the Proxy Information Request to the payee's MSCT service provider.

Step 4:

The payee's MSCT service provider checks the Proxy Information Request, prepares the Proxy Information Response including the IBAN/name of the payee and sends the Proxy Information Response to the HUB.

Step 5:

The HUB forwards the Proxy Information Response to the payer's MSCT service provider.

Step 6:

The payer's MSCT service provider retrieves the payee's details from the Proxy Information Response and provides them to the payer with a request for an SCA.

Step 7:

The payer performs an SCA on the transaction details displayed (see section 8.3).

Step 8:

The confirmation including the authentication response is provided to the payer's MSCT service provider.¹⁰⁵

Step 9:

The payer's MSCT service provider sends an SCT Inst instruction to the payer's ASPSP including the transaction details.

¹⁰⁴ It is assumed, in case the HUB is provided by the SPL service that both the payer's and the payee's MSCT service providers are registered as IRP and RRP respectively into the SPL scheme [26].

¹⁰⁵ This description assumes that the payer's MSCT service provider has received delegation from the payer's ASPSP for SCA. Otherwise additional steps are needed for the SCA as described in Chapter 7.



Step 10:

The payer's ASPSP sends a message to the payer's MSCT service provider confirming the initiation of the SCT Inst transaction.

Step 11:

The payer's ASPSP sends the SCT Inst transaction to the payee's ASPSP and the transaction flow is handled according to the SCT Inst scheme.

Step 12:

The payer's ASPSP sends a confirmation message to the payer's MSCT service provider about the execution of the SCT Inst transaction.

Step 13:

The payer's MSCT service provider sends a transaction notification message to the payer.

Step 14:

The payer's MSCT service provider sends a transaction notification message to the HUB.

Step 15:

The HUB forwards the transaction notification message to the payee's MSCT service provider.

Step 16:

The payee's MSCT service provider sends a transaction notification message to the payee.



17.5.3 Successful MSCT - P2P based on SCT Inst with known payee data

The process flow below illustrates that the usage of the HUB is not needed in the case the payer knows the payee name and IBAN, in other words, in case no proxy is used.

In this MSCT transaction type the following actors and interconnectivity are required as depicted below.

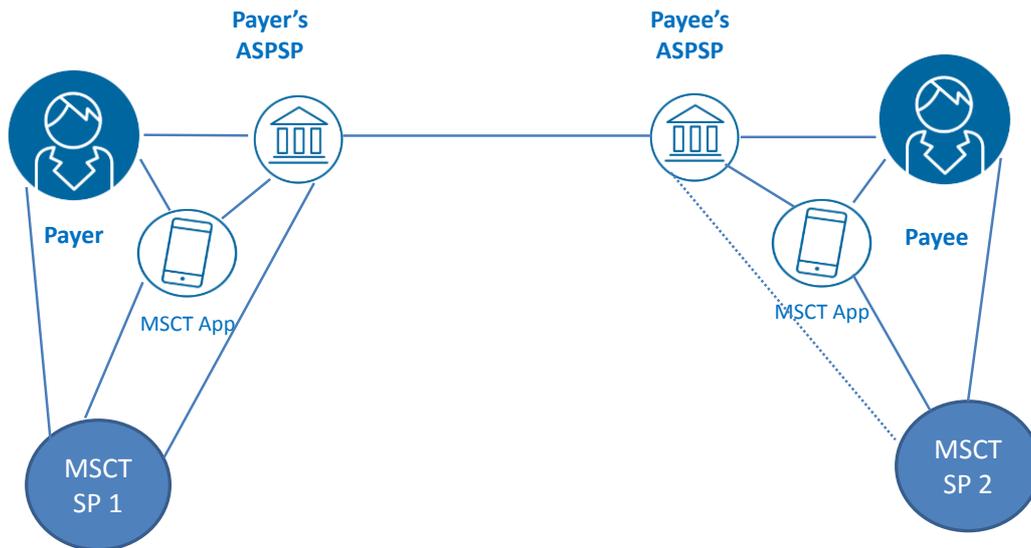
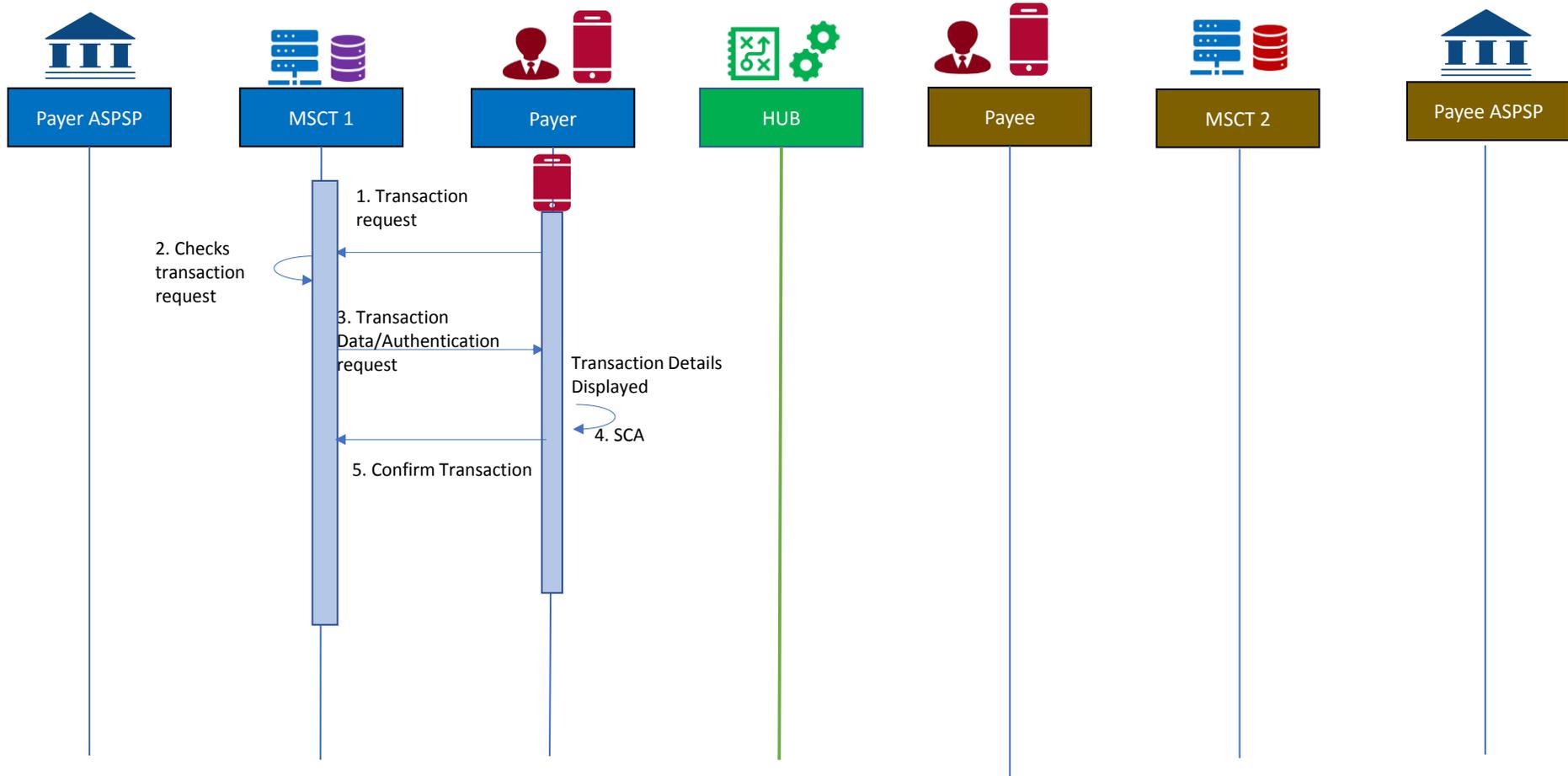


Figure 45: Actors for P2P – without proxy

The detailed process flows between the different actors involved for this MSCT transaction type are shown in the next figure.



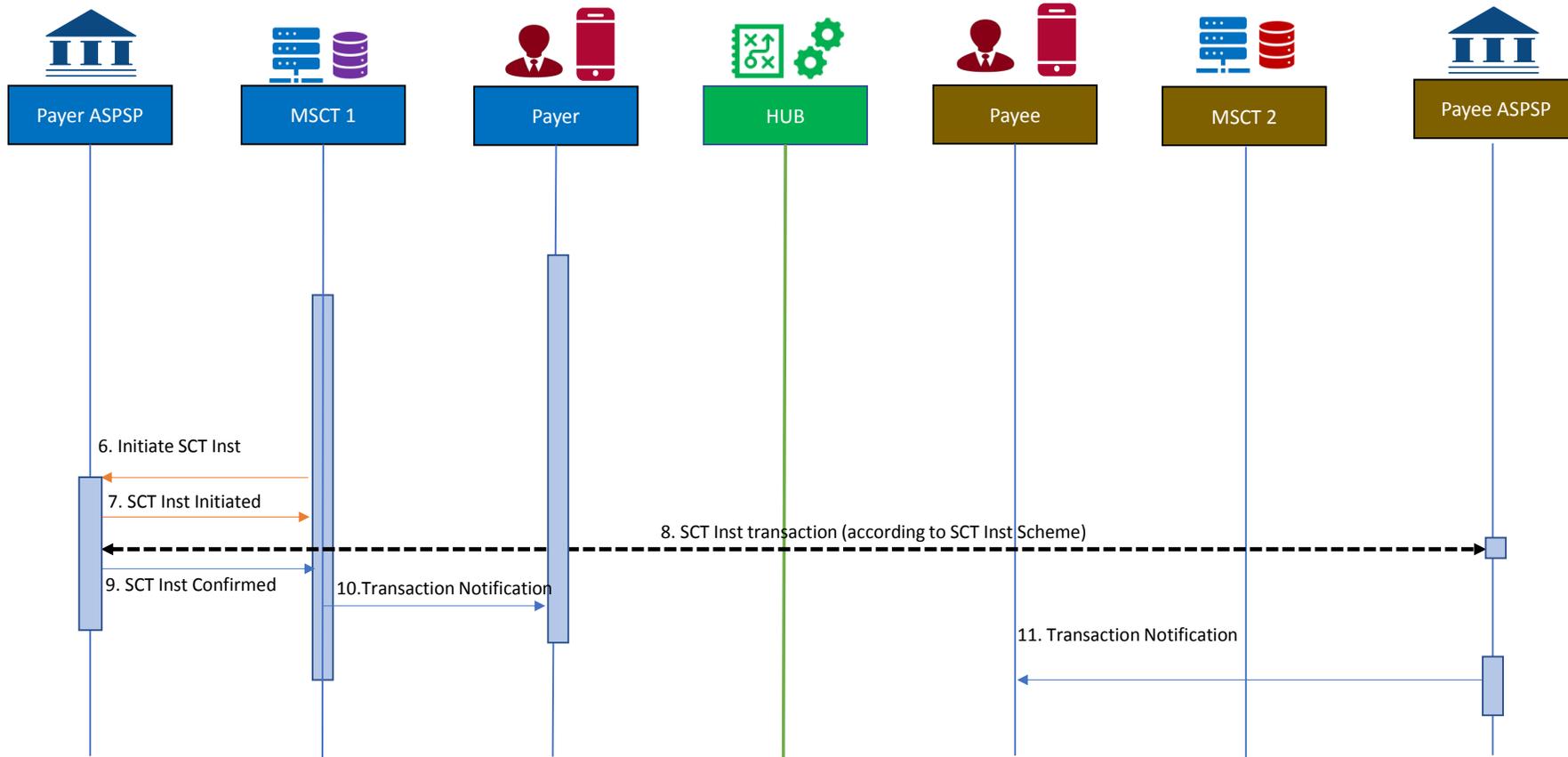


Figure 46: Process flow – P2P – without proxy



In the figure above the following steps are involved:

Step 1:

The payer initiates a new transaction in their MSCT application including the transaction amount and payee details which is provided to their MSCT service provider.

Step 2:

The MSCT service provider checks the transaction initiation request received.

Step 3:

The payer's MSCT service provider sends an SCA request based on the transaction details to the payer.

Step 4:

The payer performs an SCA on the transaction details displayed.

Step 5:

The confirmation including the authentication response is provided to the payer's MSCT service provider.¹⁰⁶

Step 6:

The payer's MSCT service provider sends an SCT Inst instruction to the payer's ASPSP including the transaction details.

Step 7:

The payer's ASPSP sends a message to the payer's MSCT service provider confirming the initiation of the SCT Inst.

Step 8:

The payer's ASPSP sends the SCT Inst transaction to the payee's ASPSP and the transaction flow is handled according to the SCT Inst scheme.

Step 9:

The payer's ASPSP sends a confirmation message to the payer's MSCT service provider about the execution of the SCT Inst transaction.

Step 10:

The payer's MSCT service provider sends a transaction notification message to the payer.

Step 11:

The payee's ASPSP sends a transaction notification message to the payee.

¹⁰⁶ This description assumes that the payer's MSCT service provider has received delegation from the payer's ASPSP for SCA. Otherwise additional steps are needed for the SCA as described in Chapter 7.



17.5.4 Successful MSCT - C2B based on SCT Inst with merchant-presented QR-code containing a token

The process flow below illustrates the usage of the HUB in case the merchant-presented data does not contain the necessary transaction data “in clear” and a token is used instead. This may be a dynamic or a static token. It is hereby assumed that the tokenisation/de-tokenisation of (part of) the transaction data is handled by or via the merchant’s MSCT service provider.

In this case the following actors and interconnectivity are required as depicted below.

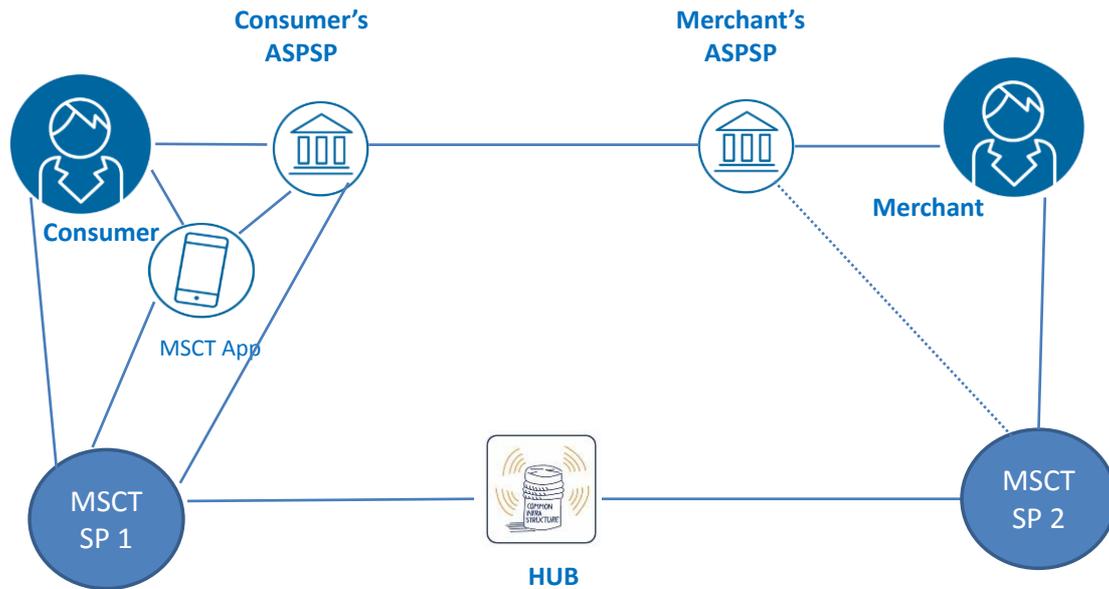
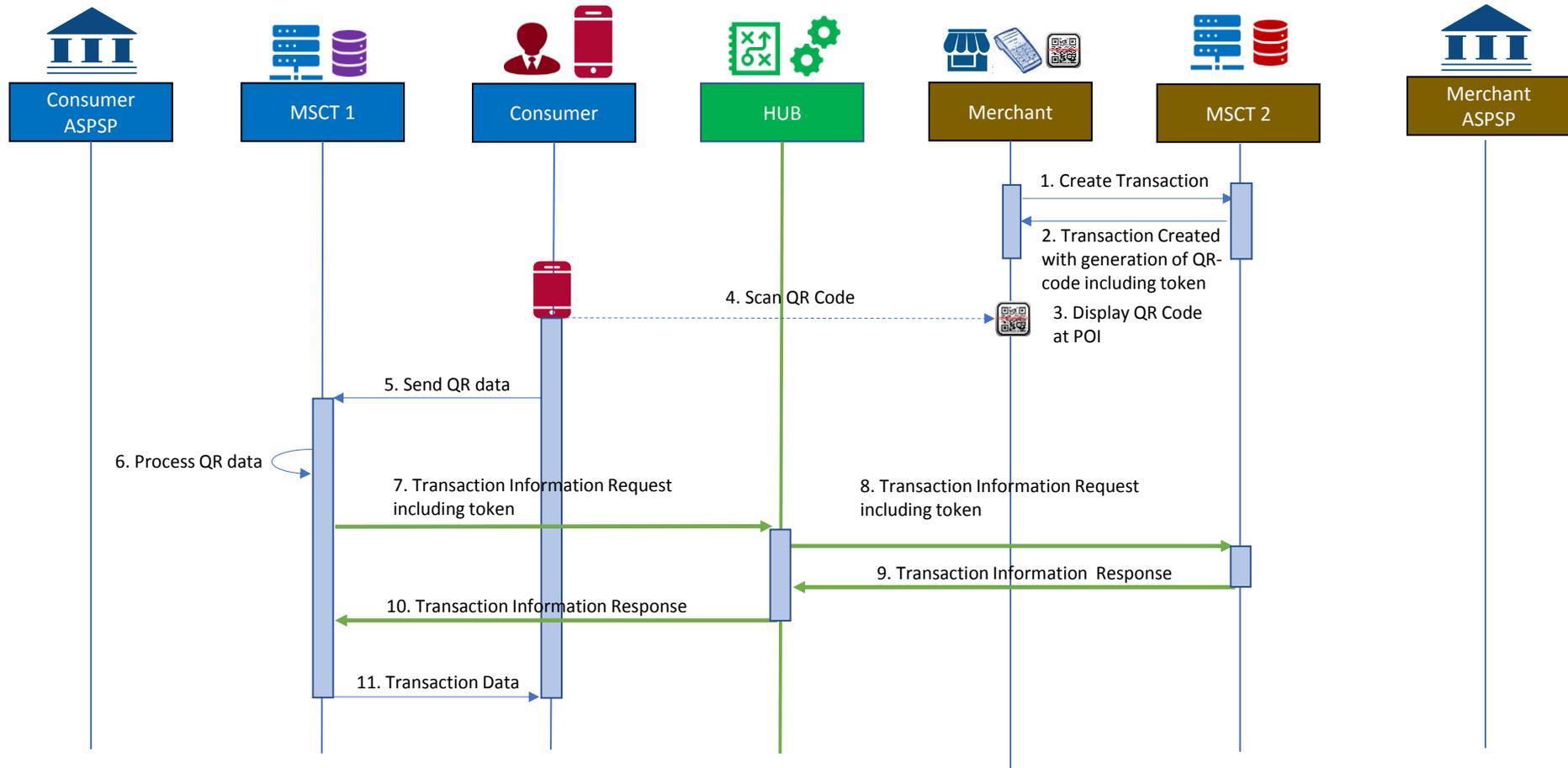


Figure 47: Actors for C2B - with token

The detailed process flows between the different actors involved for this MSCT transaction type are shown in the next figure.



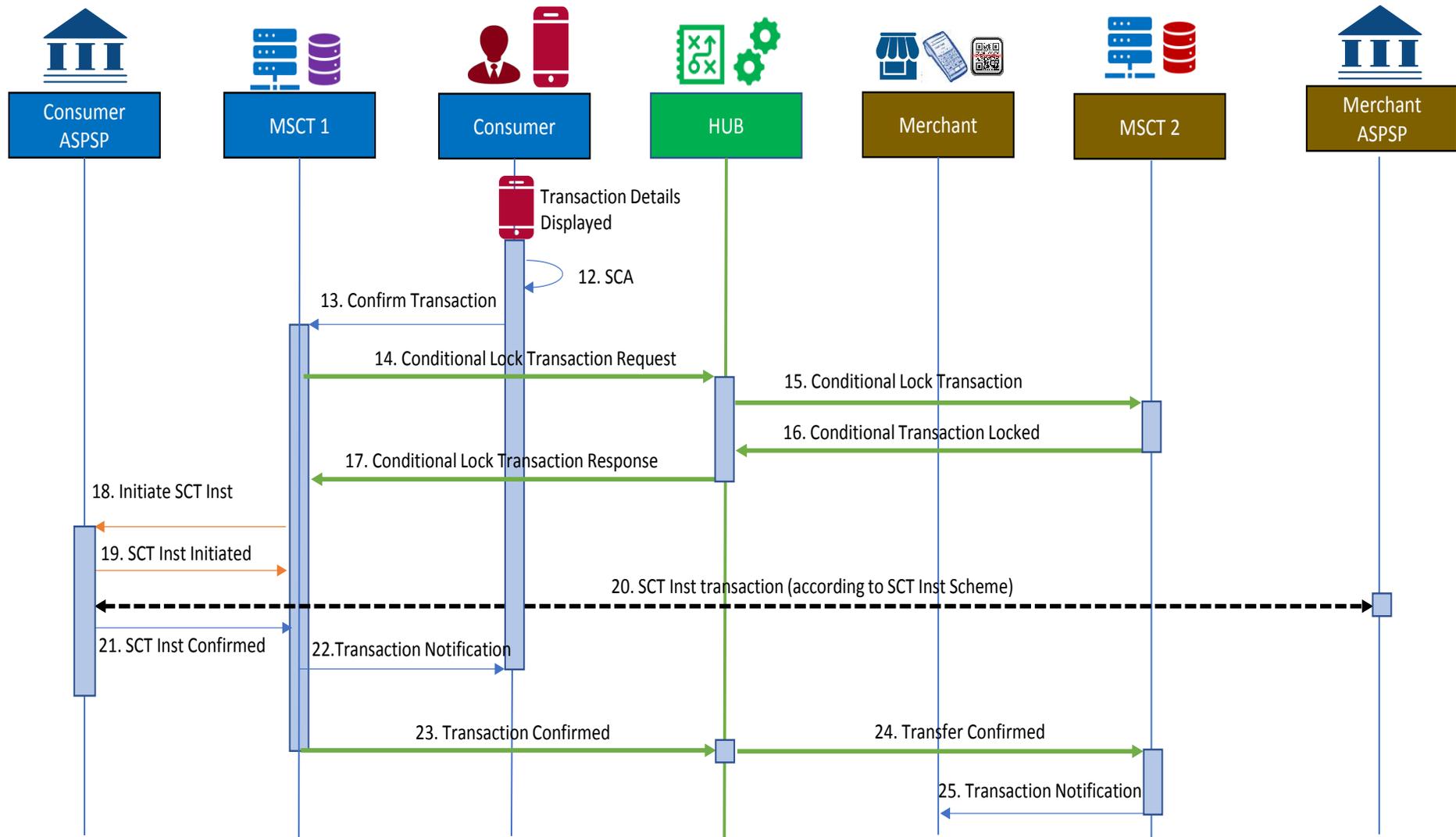


Figure 48: Process flow – C2B – merchant-presented QR-code with token



In the figure above the following steps are involved:

Step 1:

The merchant creates a new transaction and provides a new transaction request with the transaction details, including the transaction amount to their MSCT service provider.

Step 2:

The merchant's MSCT service provider returns a QR-code including a dedicated token based on the transaction details (transaction amount, IBAN_merchant, transaction identifier) and their MSCT service provider identifier to the merchant.¹⁰⁷

Step 3:

The merchant POI displays the transaction amount with the QR-code.

Step 4:

The consumer opens their MSCT application and scans the QR-code.

Step 5:

The data, including the token and MSCT service provider identifier is retrieved from the QR-code and provided to the consumer's MSCT service provider.

Step 6:

The consumer's MSCT service provider checks the QR-code data and prepares a Transaction Information Request including the token.

Step 7:

The Transaction Information Request including the merchant's MSCT service provider identifier is sent to the HUB.

Step 8:

The HUB identifies the merchant's MSCT service provider and forwards them the Transaction Information request.

Step 9:

The merchant's MSCT service provider checks the request, prepares the response and sends the Transaction Information Response to the HUB.

Step 10:

The HUB forwards the Transaction Information Response to the consumer's MSCT service provider.

¹⁰⁷ As an alternative, the MSCT service provider could also return the token to the merchant and their POI generates the QR-code.



Step 11:

The consumer's MSCT service provider retrieves the transaction details from the Transaction Information Response and sends them to the consumer with a request for an SCA.

Step 12:

The consumer performs an SCA on the transaction details displayed.

Step 13:

The confirmation including the authentication response is provided to the consumer's MSCT service provider.¹⁰⁸

Step 14 (conditional)^{109:}

The consumer's MSCT service provider sends a Lock Transaction Request to the HUB including the merchant's MSCT service provider identifier.

Step 15 (conditional):

The HUB forwards a "Lock Transaction" to the merchant's MSCT service provider.

Step 16 (conditional):

The merchant's MSCT service provider sends a "Transaction Locked" to the HUB.

Step 17 (conditional):

The HUB forwards the Lock Transaction Response to the consumer's MSCT service provider.

Step 18:

The consumer's MSCT service provider sends an SCT Inst instruction to the consumer's ASPSP including the transaction details.

Step 19:

The consumer's ASPSP sends a message to the consumer's MSCT service provider confirming the initiation of the SCT Inst.

Step 20:

The consumer's ASPSP sends the SCT Inst transaction to the merchant's ASPSP and the transaction flow is handled according to the SCT Inst scheme.

Step 21:

The consumer's ASPSP sends a confirmation message to the consumer's MSCT service provider about the execution of the SCT Inst transaction.

¹⁰⁸ This description assumes that the consumer's MSCT service provider has received delegation from the consumer's ASPSP for SCA. Otherwise additional steps are needed for the SCA as described in Chapter 7.

¹⁰⁹ See sections 17.5.1 and 17.6. In case the LT Indicator does not require a lock transaction function, steps 14 through 17 will not be present.



Step 22:

The consumer's MSCT service provider sends a transaction notification message to the consumer.

Step 23:

The consumer's MSCT service provider sends a transaction notification message to the HUB with the merchant's MSCT service provider identifier.

Step 24:

The HUB forwards the transaction notification message to the merchant's MSCT service provider.

Step 25:

The merchant's MSCT service provider sends a transaction notification message to the merchant.



17.5.5 Successful MSCT - C2B based on SCT Inst with merchant-presented QR-code containing all transaction data in clear

The process flow below illustrates the usage of the HUB in the case the merchant-presented data does contain all the necessary transaction data “in clear”. This will typically occur for a QR-code on an invoice as illustrated below.

In this MSCT transaction type the following actors and interconnectivity are required as depicted below.

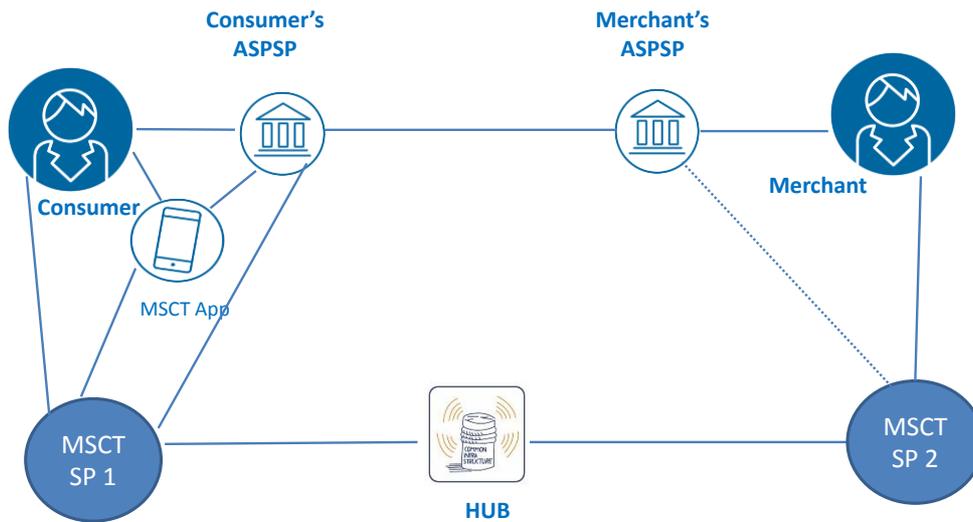
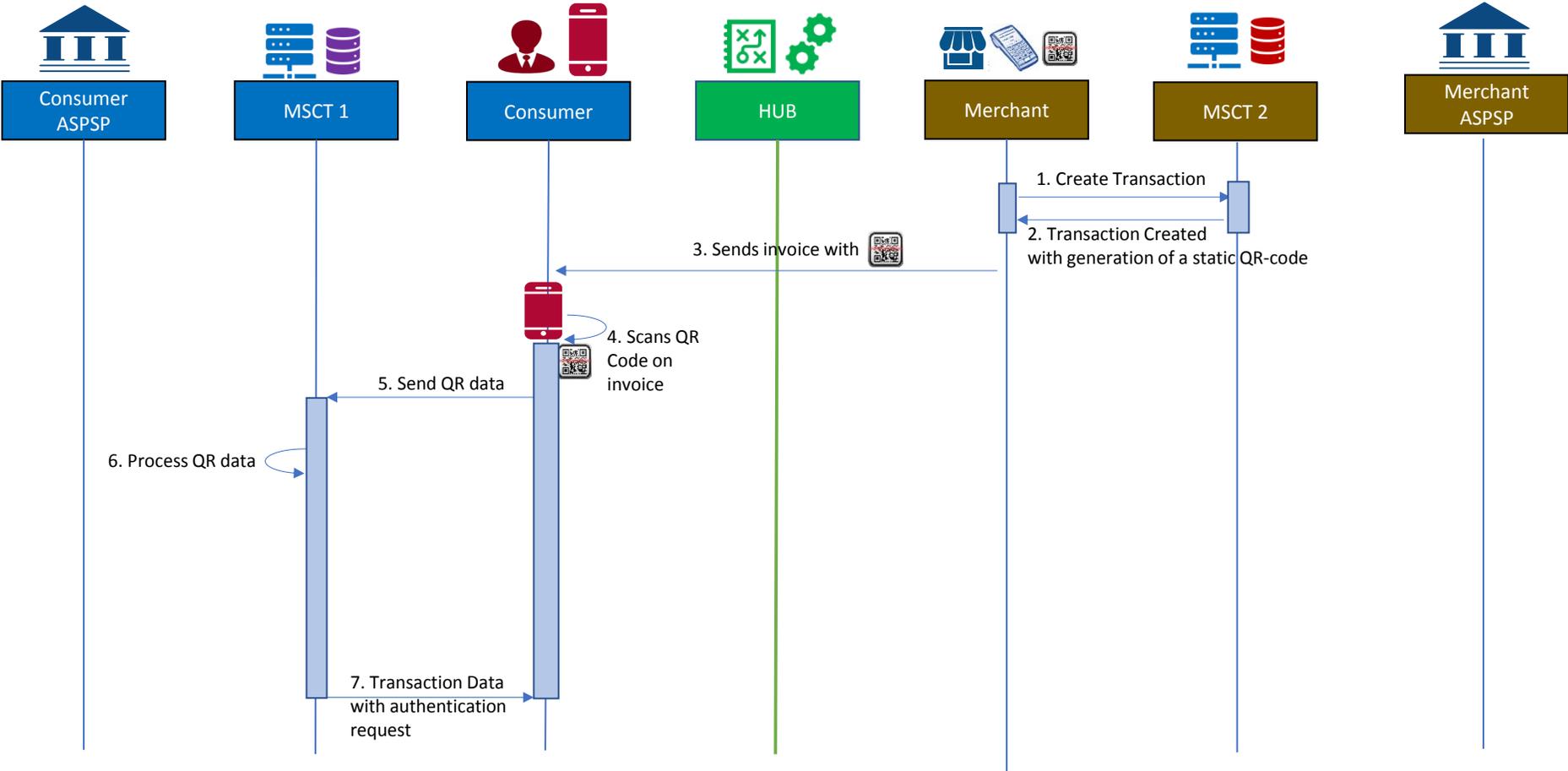


Figure 49: Actors for C2B – without token

The detailed process flows between the different actors involved for this MSCT transaction type are shown in the next figure. In case of an invoice, the LT indicator in the QR-code will not require a lock function and therefore the related messages are not shown in the process flow below.



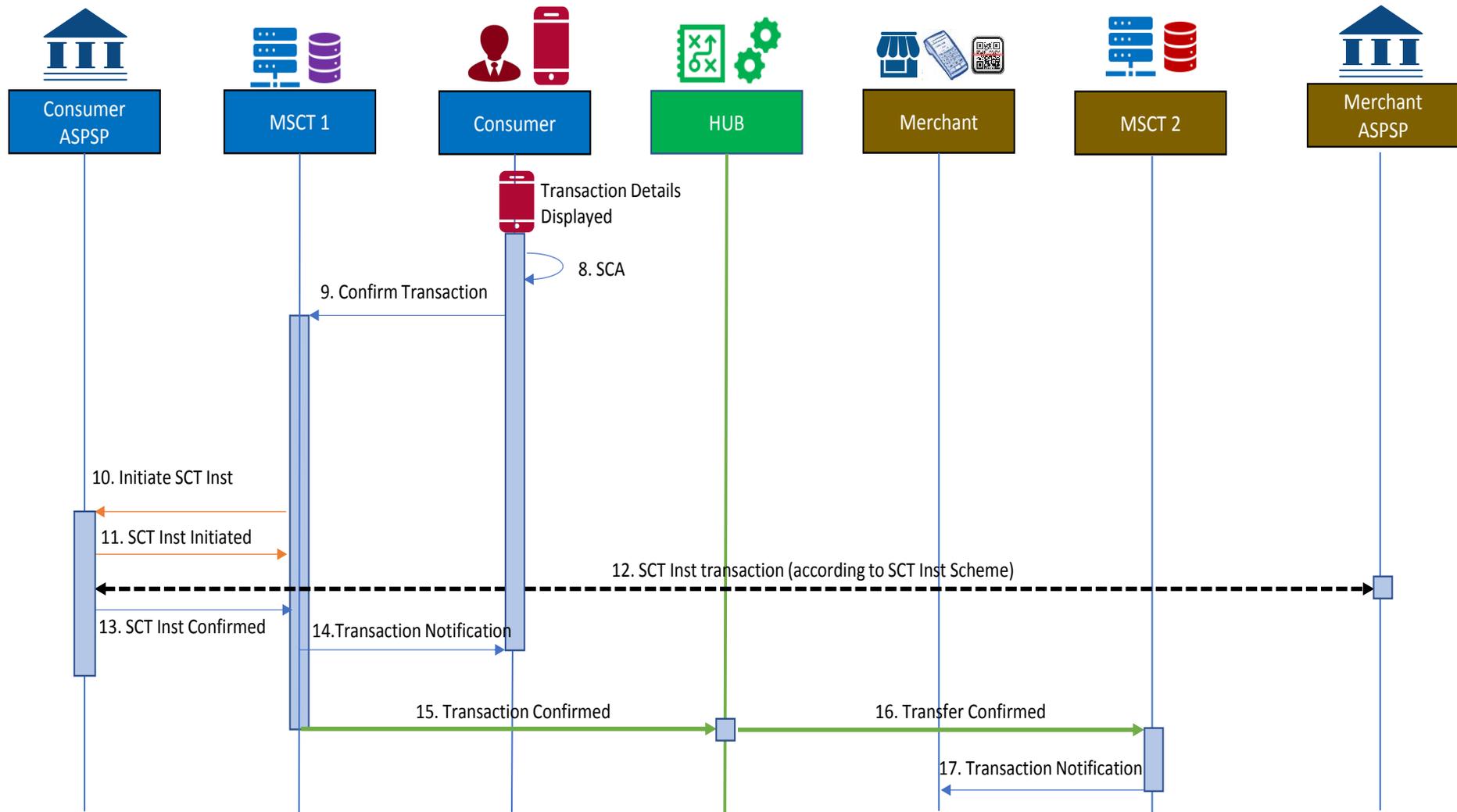


Figure 50: Process flow – C2B – merchant-presented QR-code with full transaction data



In the figure above the following steps are involved:

Step 1:

The merchant creates a new transaction and provides a new transaction request with the transaction details, including the transaction amount to their MSCT service provider.

Step 2:

The merchant's MSCT service provider returns a QR-code based on the transaction details (transaction amount, IBAN_merchant, transaction identifier) and an MSCT service provider identifier to the merchant.¹¹⁰

Step 3:

The merchant prepares the invoice, displaying the QR-code and provides the invoice to the consumer.

Step 4:

The consumer opens their MSCT application and scans the QR-code from the invoice.

Step 5:

The transaction data and merchant's MSCT service provider identifier are retrieved from the QR-code and provided to the consumer's MSCT service provider.

Step 6:

The MSCT service provider checks the QR-code data.

Step 7:

The MSCT service provider sends an authentication request to the consumer.

Step 8:

The consumer performs an SCA on the transaction details displayed.

Step 9:

The confirmation including the authentication response is provided to the consumer's MSCT service provider.¹¹¹

Step 10:

The consumer's MSCT service provider sends an SCT Inst instruction to the consumer's ASPSP including the transaction details.

¹¹⁰ As an alternative, the MSCT service provider could also return the transaction identifier to the merchant and their POI generates the QR-code.

¹¹¹ This description assumes that the consumer's MSCT service provider has received delegation from the consumer's ASPSP for SCA. Otherwise additional steps are needed for the SCA as described in Chapter 7.



Step 11:

The consumer's ASPSP sends a message to the consumer's MSCT service provider confirming the initiation of the SCT Inst.

Step 12:

The consumer's ASPSP sends the SCT Inst transaction to the merchant's ASPSP and the transaction flow is handled according to the SCT Inst scheme.

Step 13:

The consumer's ASPSP sends a confirmation message to the consumer's MSCT service provider about the execution of the SCT Inst transaction.

Step 14:

The consumer's MSCT service provider sends a transaction notification message to the consumer.

Step 15:

The consumer's MSCT service provider sends a transaction notification message to the HUB with the merchant's MSCT service provider identifier.

Step 16:

The HUB forwards the transaction notification message to the merchant's MSCT service provider.

Step 17:

The merchant's MSCT service provider sends a transaction notification message to the merchant.



17.5.6 Reject by the payer MSCT service provider – C2B based on SCT Inst with merchant-presented QR-code containing a token

The process flow below illustrates the usage of the HUB in the case of a reject by the consumer (payer) MSCT service provider for an MSCT based on merchant-presented data using a QR-code including a token. This may be a dynamic or a static token. It is hereby assumed that the tokenisation/de-tokenisation of (part of) the transaction data is handled by or via the merchant MSCT service provider. In this illustration it is assumed that the consumer MSCT service provider rejects the MSCT after having received requested the de-tokenisation to the merchant MSCT service provider (e.g. due to the fact that incomplete data related to the token is provided).

In this MSCT transaction type, the following actors and interconnectivity are required as depicted below.

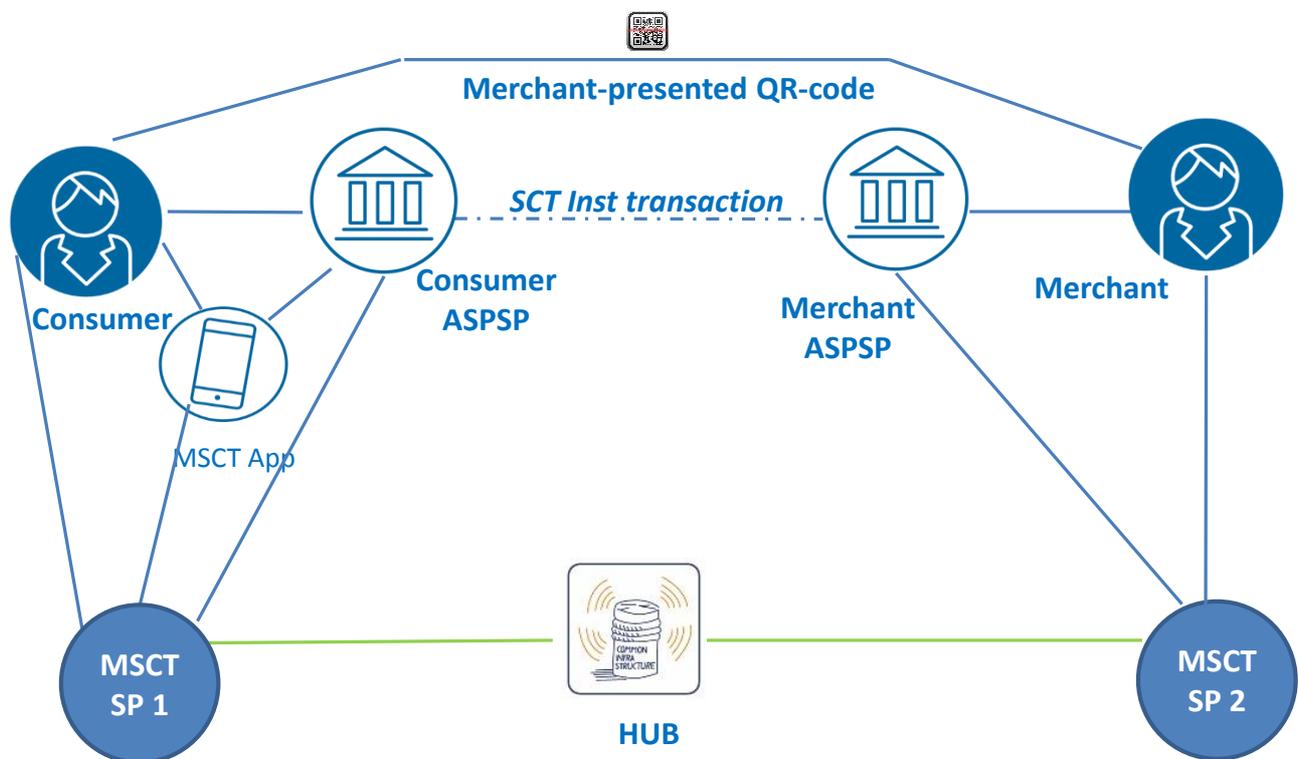


Figure 51: Actors for reject by consumer MSCT service provider for C2B payment context

The detailed process flows between the different actors involved in this MSCT transaction are shown in the next figure.

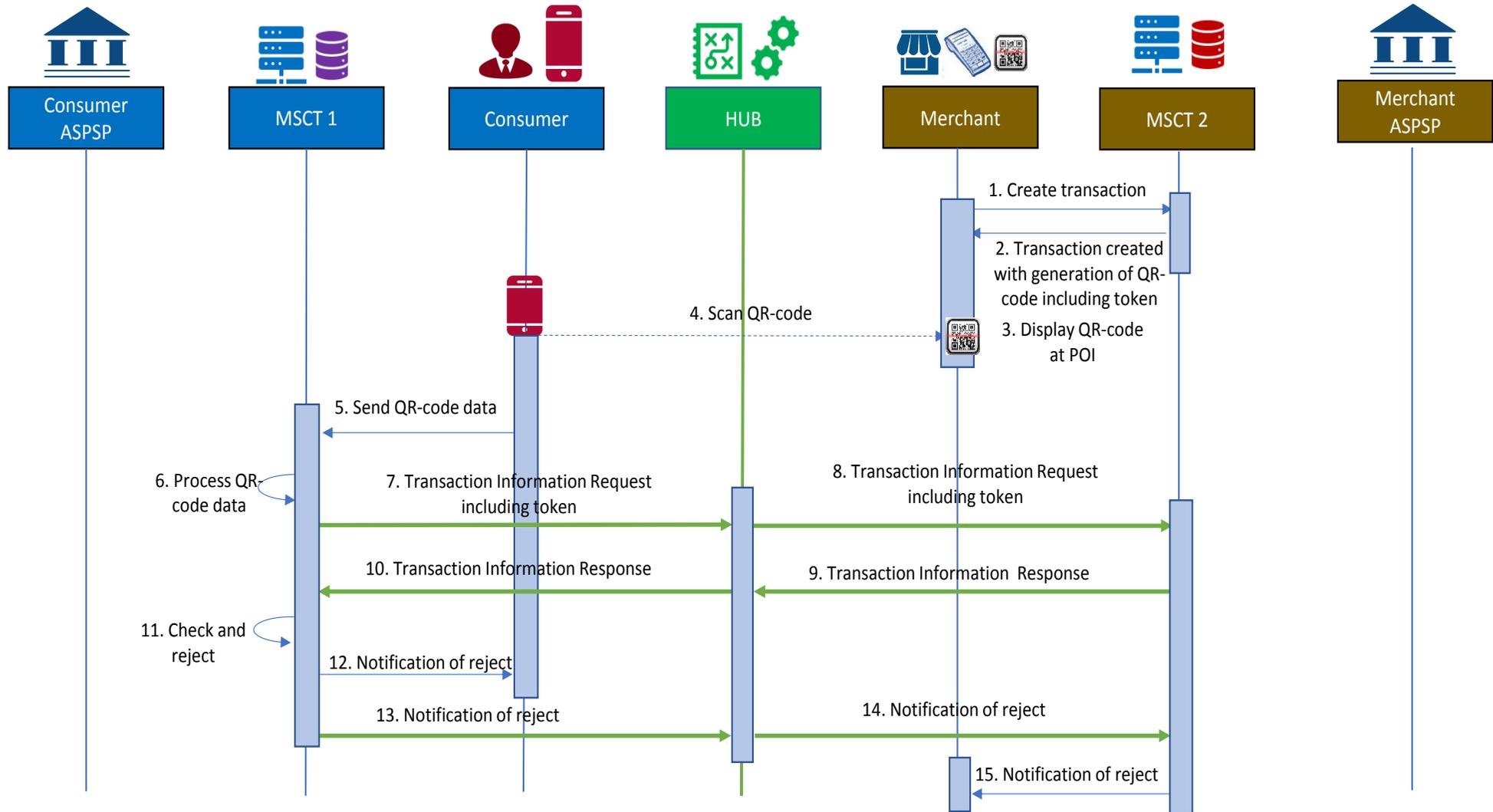


Figure 52: Process flow – C2B – Reject by consumer MSCT service provider for MSCT based on merchant-presented QR-code with token



In the figure above the following steps are involved:

Step 1:

The merchant creates a new transaction and provides a new transaction request with the transaction details, including the transaction amount to their MSCT service provider.

Step 2:

The merchant MSCT service provider returns a QR-code including a dedicated token based on the transaction details (transaction amount, IBAN_merchant, name/trade name merchant, transaction identifier) and their MSCT service provider identifier to the merchant.¹¹²

Step 3:

The merchant POI displays the transaction amount with the QR-code.

Step 4:

The consumer opens their MSCT application and scans the QR-code.

Step 5:

The data, including the token and merchant MSCT service provider identifier, is retrieved from the QR-code and provided to the consumer MSCT service provider.

Step 6:

The consumer MSCT service provider checks the QR-code data and prepares a Transaction Information Request including the token.

Step 7:

The Transaction Information Request including the merchant MSCT service provider identifier is sent to the HUB.

Step 8:

The HUB identifies the merchant MSCT service provider and forwards them the Transaction Information request.

Step 9:

The merchant MSCT service provider checks the request, prepares the response and sends a Transaction Information Response to the HUB.

Step 10:

The HUB forwards the Transaction Information Response to the consumer MSCT service provider.

Step 11:

¹¹² As an alternative, the MSCT service provider could also return the token to the merchant and their POI generates the QR-code.



The consumer MSCT service provider retrieves the transaction details from the Transaction Information Response and notices that the information is “invalid” or “incomplete” so that they cannot proceed with the transaction.

Step 12:

The consumer MSCT service provider sends a notification of reject to the consumer.

Step 13:

The consumer MSCT service provider sends a notification of reject to the HUB with the merchant MSCT service provider identifier.

Step 14:

The HUB forwards the notification of reject to the merchant's MSCT service provider.

Step 15:

The merchant MSCT service provider sends the notification of reject to the merchant.



17.5.7 Reject by the payer ASPSP – P2P based on SCT with payee-presented QR-code containing a proxy

The process flow below illustrates the usage of the HUB in the case of a reject by the payer ASPSP for an MSCT in a P2P payment context, based on payee-presented data using a QR-code including a proxy. It is hereby assumed that retrieval of the payee data is handled by or via the payee MSCT service provider. In this illustration it is assumed that the payer ASPSP rejects the MSCT after an unsuccessful SCA.

In this example, the following actors and interconnectivity are required as depicted below.

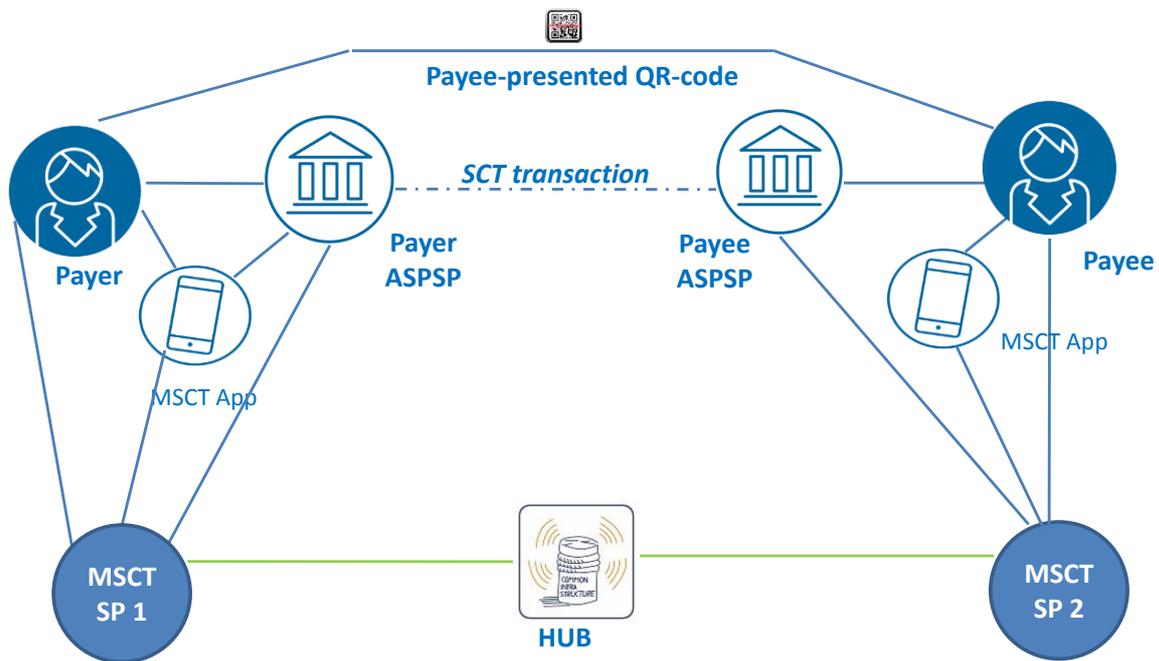


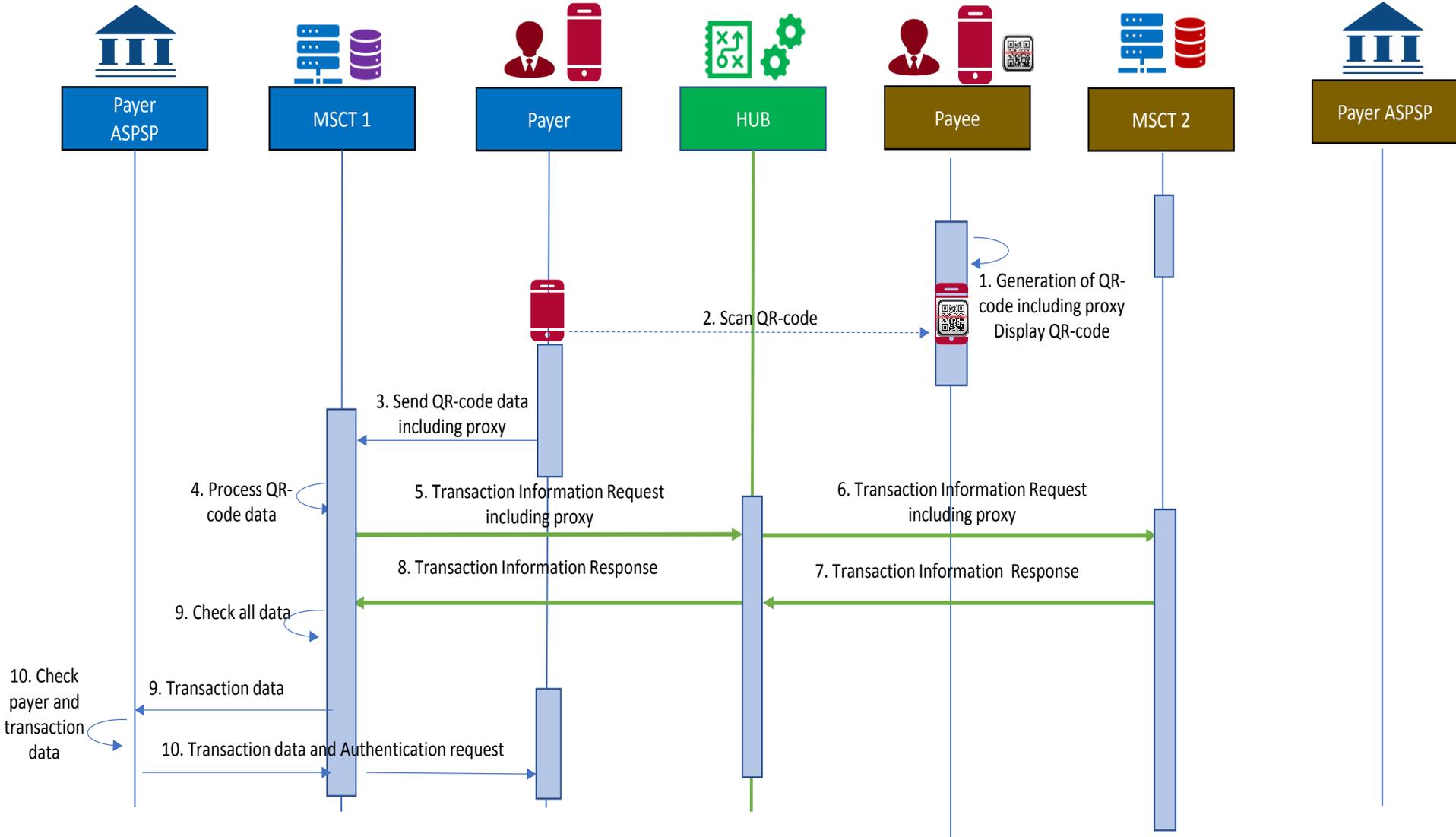
Figure 53: Actors for reject by payer ASPSP for P2P payment context

The detailed process flows between the different actors involved in this MSCT transaction type are shown in the next figure.



Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance

EPC269-19 Version 1.14



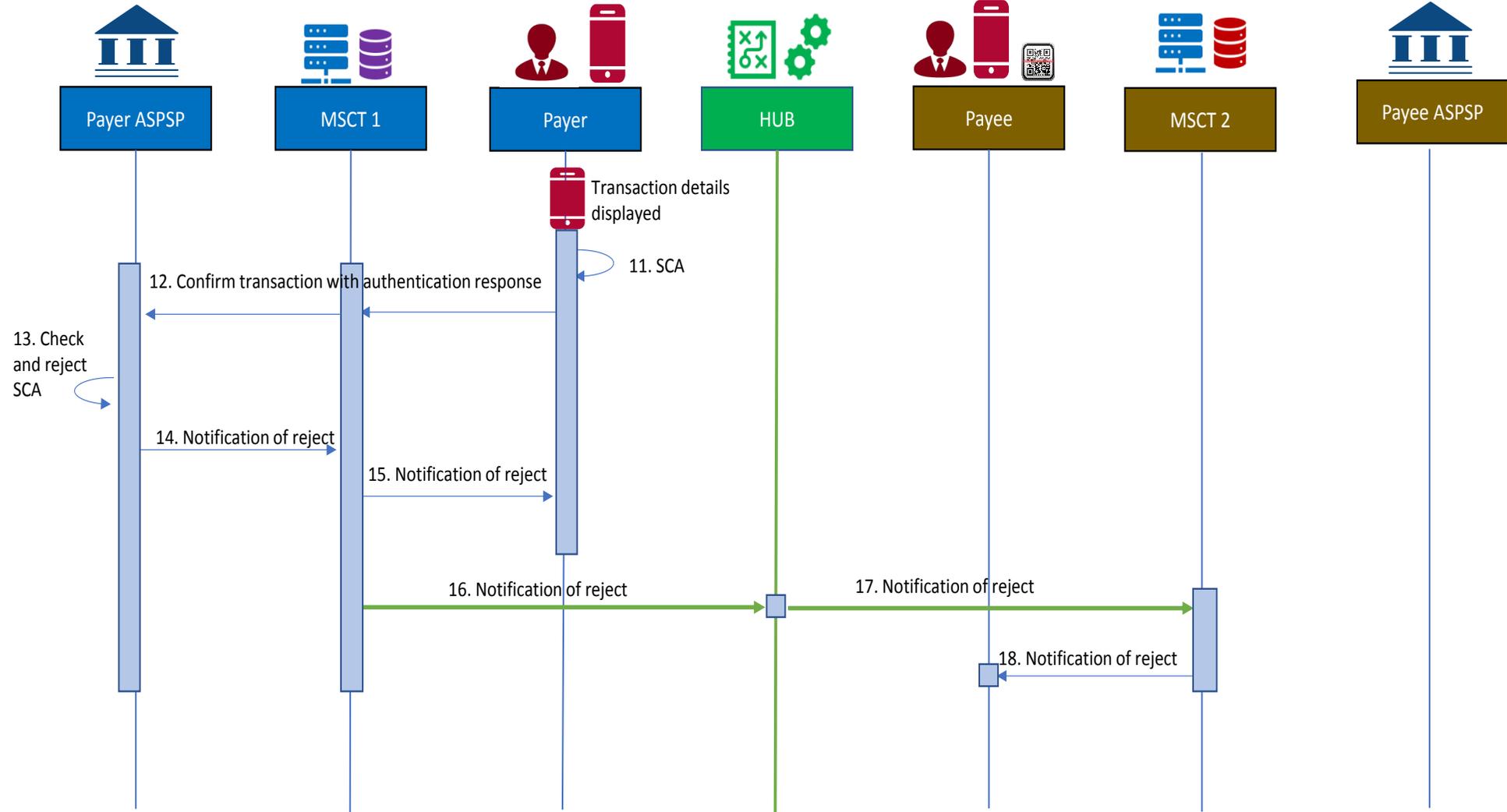


Figure 54: Process flow – P2P – Reject by payer ASPSP for MSCT based on payee-presented QR-code with proxy



In the figure above the following steps are involved:

Step 1

- The payee opens the MSCT application on their mobile device, which possibly involves the entry of a password and enters the amount to be paid.
- The MSCT application on the payee's mobile device generates a QR-code including the payee name, a proxy_IBAN, and the amount to be paid which is displayed to the payer.

Step 2

- The payer selects and opens the MSCT application on their mobile device, which possibly involves the entry of a password.
- The payer scans the QR-code from the payee's mobile device.

Step 3

The data, including the proxy and the payee MSCT service provider identifier, is retrieved from the QR-code and provided to the payer MSCT service provider.

Step 4

The payer MSCT service provider checks the QR-code data and prepares merchant retrieves the Transaction information Request including the proxy_IBAN of the payee.

Step 5:

The Transaction Information request including the proxy_IBAN of the payee and the payee provider identifier is sent to the HUB.

Step 6:

The HUB identifies the payee MSCT service provider and forwards them the Transaction Information Request containing the proxy_IBAN of the payee.

Step 7:

The payee MSCT service provider checks the request, prepares and sends Transaction Information Response including the IBAN_payee to the HUB.

Step 8:

The HUB forwards the Transaction Information Response to the payer MSCT service provider.

Step 9:

- The payer MSCT service provider checks the Transaction Information Response and retrieves the IBAN_payee.
- The payer MSCT service provider sends all transaction data to the payer ASPSP.



Step 10:

- The payer ASPSP checks the all the transaction details.
- The payer ASPSP sends the transaction details with an authentication request to the payer via the payer MSCT service provider.

Step 11:

The payer consents to the transaction based on the details displayed and performs SCA.

Step 12:

The confirmation including the authentication response is provided to the payer ASPSP via the payer MSCT service provider.

Step 13:

The payer ASPSP checks the authentication response which is incorrect and rejects the transaction¹¹³.

Step 14:

The payer ASPSP sends a notification of reject to the payer MSCT service provider.

Step 15:

The payer MSCT service provider sends a notification of reject to the payer.

Step 16:

The payer MSCT service provider sends a notification of reject to the HUB with the payee MSCT service provider identifier.

Step 17:

The HUB forwards the notification of reject to the payee MSCT service provider.

Step 18:

The payee MSCT service provider sends the notification of reject to the payee.



17.5.8 Unsuccessful transaction – C2B based on SCT with merchant-presented QR-code containing a token

The process flow below illustrates the usage of the HUB in the case of an unsuccessful transaction (after receipt by the consumer ASPSP of a Return message (see section 4.1) for an MSCT based on merchant-presented data using a QR-code including a token.

In this example, the following actors and interconnectivity are required as depicted below.

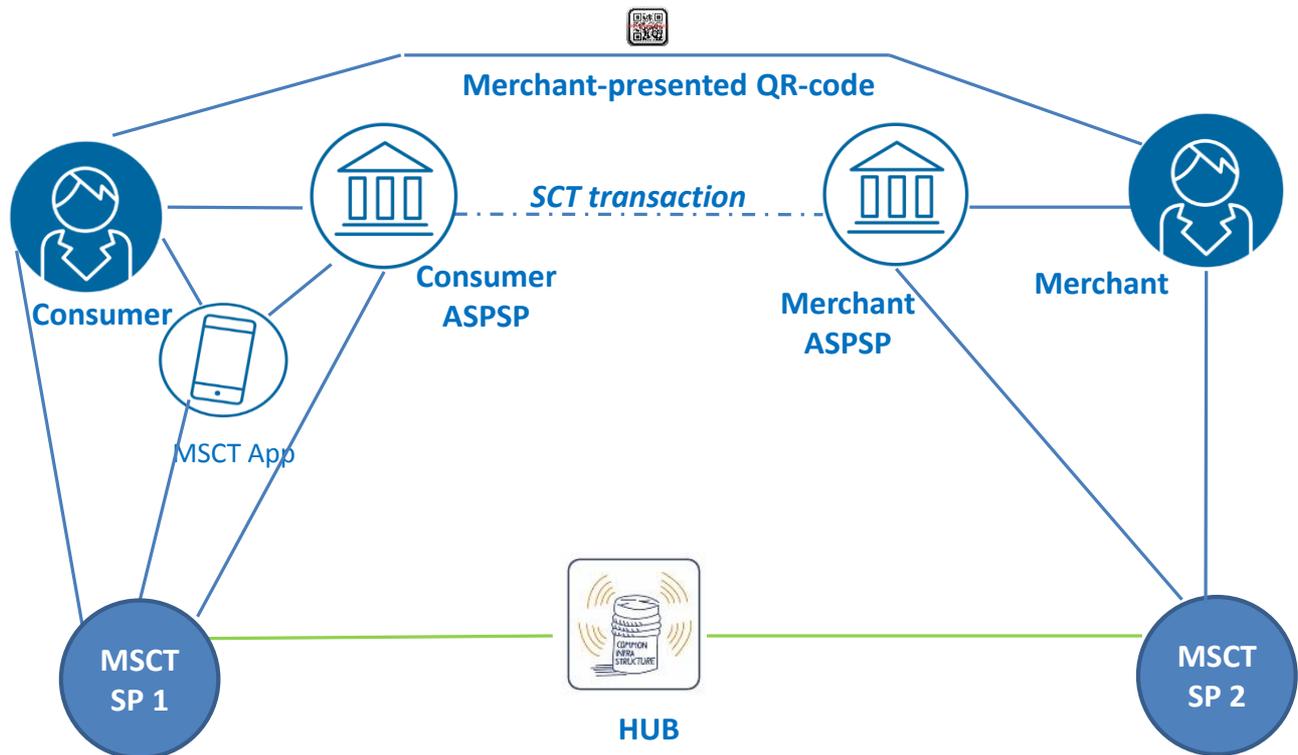


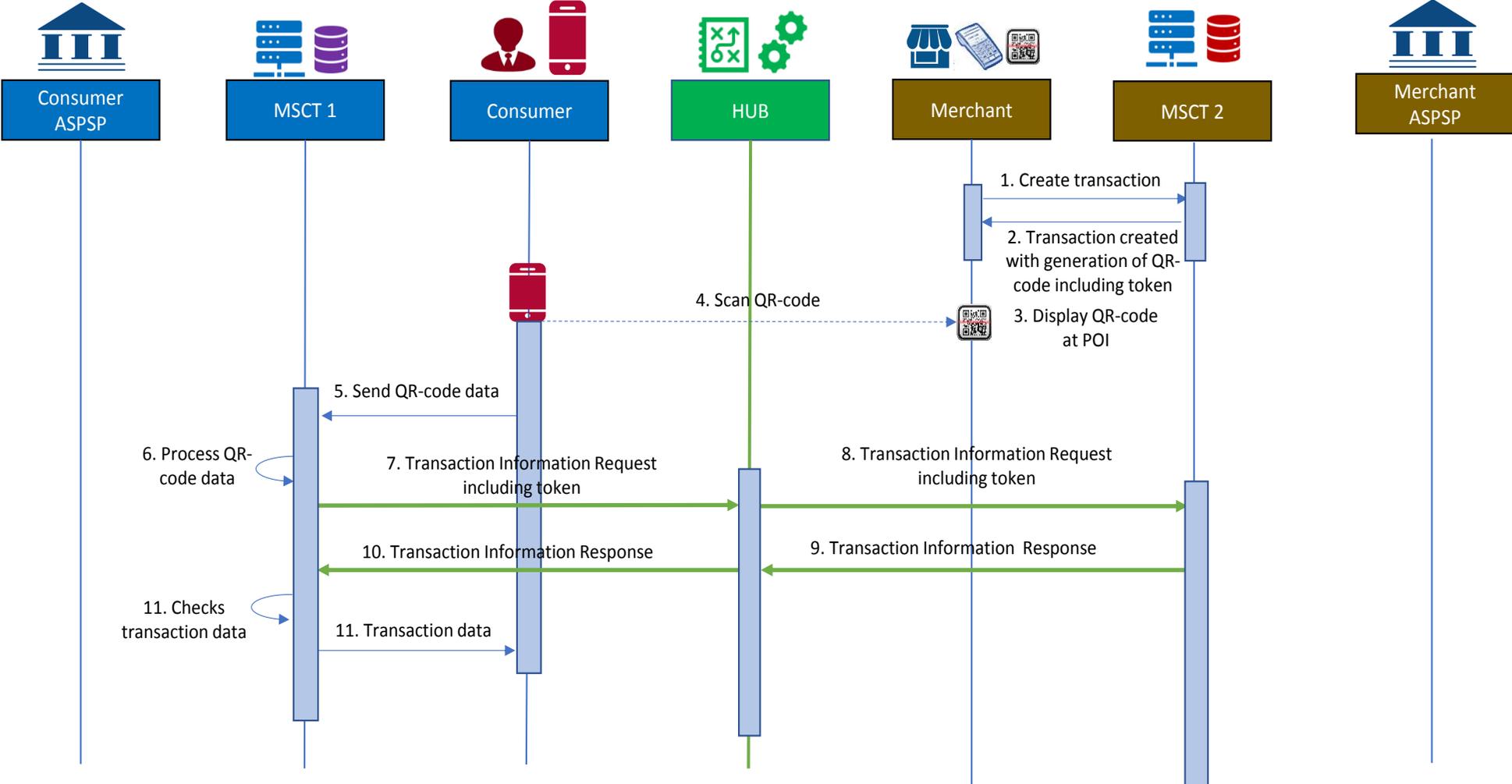
Figure 55: Actors for unsuccessful transaction for C2B payment context

The detailed process flows between the different actors involved in this MSCT transaction type are shown in the next figure.



Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance

EPC269-19 Version 1.14



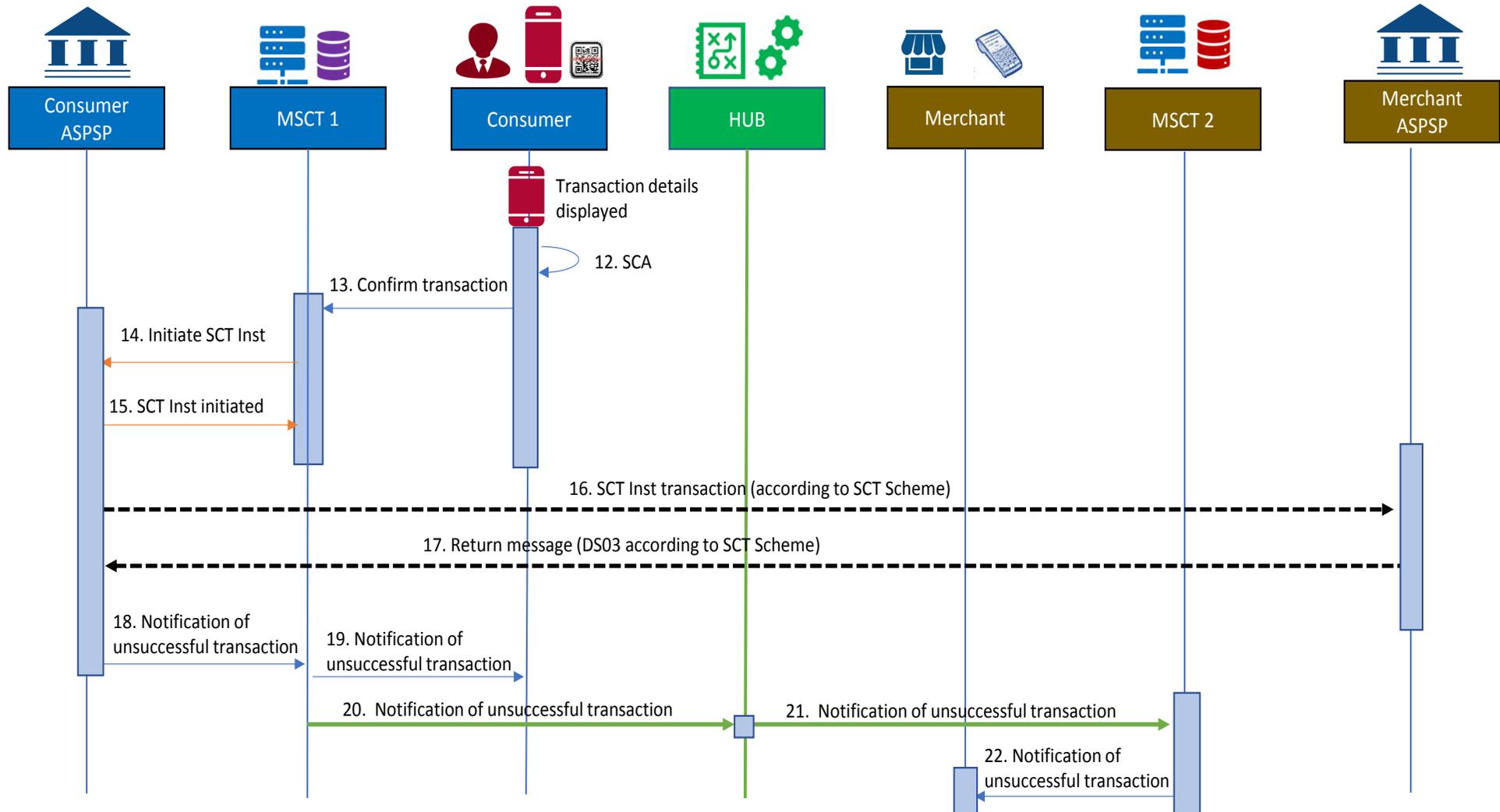


Figure 56: Process flow – C2B – Unsuccessful transaction for MSCT based on merchant-presented QR-code with token



In the figure above the following steps are involved:

Step 1:

The merchant creates a new transaction and provides a new transaction request with the transaction details, including the transaction amount to their MSCT service provider.

Step 2:

The merchant MSCT service provider returns a QR-code including a dedicated token based on the transaction details (transaction amount, IBAN_merchant, name/trade name merchant, transaction identifier) and their MSCT service provider identifier to the merchant.¹¹⁴

Step 3:

The merchant POI displays the transaction amount with the QR-code.

Step 4:

The consumer opens their MSCT application and scans the QR-code.

Step 5:

The data, including the token and MSCT service provider identifier is retrieved from the QR-code and provided to the consumer MSCT service provider.

Step 6:

The consumer MSCT service provider checks the QR-code data and prepares a Transaction Information Request including the token.

Step 7:

The Transaction Information Request including the merchant MSCT service provider identifier is sent to the HUB.

Step 8:

The HUB identifies the merchant MSCT service provider and forwards them the Transaction Information request.

Step 9:

The merchant MSCT service provider checks the request, prepares the response and sends a Transaction Information Response to the HUB.

Step 10:

The HUB forwards the Transaction Information Response to the consumer MSCT service provider.

Step 11:

- The consumer MSCT service provider retrieves the transaction details from the Transaction Information Response.
- The consumer MSCT service provider sends the transaction details to the consumer.

¹¹⁴ As an alternative, the MSCT service provider could also return the token to the merchant and their POI generates the QR-code.



Step 12:

The consumer consents to the transaction based on the details displayed and performs SCA¹¹⁵.

Step 13:

The confirmation including the authentication response is provided to the consumer MSCT service provider.

Step 14:

After checking the authentication response, the consumer MSCT service provider sends an SCT Inst instruction to the consumer ASPSP including the transaction details.

Step 15:

The consumer ASPSP sends a message to the consumer MSCT service provider confirming the initiation of the SCT Inst.

Step 16:

The consumer ASPSP sends the SCT Inst transaction to the merchant ASPSP and the transaction flow is handled according to the SCT Inst scheme.

Step 17:

After a few days, the consumer ASPSP receives a “Return message” from the merchant ASPSP.

Step 18:

The consumer ASPSP sends a notification of unsuccessful transaction to the consumer MSCT service provider.

Step 19:

The consumer MSCT service provider sends a notification of unsuccessful transaction to the consumer.

Step 20:

The consumer MSCT service provider sends a notification of unsuccessful transaction to the HUB with the merchant MSCT service provider identifier.

Step 21:

The HUB forwards the notification of unsuccessful transaction to the merchant MSCT service provider.

Step 22:

The merchant MSCT service provider sends the notification of unsuccessful transaction to the merchant.

¹¹⁵ The SCA may be performed by the consumer’s MSCT service provider or by their ASPSP. This may involve additional steps which are not illustrated in this process flow since they do not impact the interoperability (see Chapter 8). Here it is assumed that the consumer’s MSCT service provider has received delegation from the consumer’s ASPSP for SCA subject to appropriate agreements.



17.6 Minimum data set for MSCTs based on payee-presented data

To achieve interoperability for MSCTs, an agreement on a minimum data set is required for the data to be exchanged between the payer/consumer and payee/merchant. Any future specification of the data needed for the messages between the respective MSCT service providers, through the HUB, will need to take this minimum data set into account.

The minimum data set to be exchanged between the payee and the payer, will rely on the MSCT transaction feature, such as described in **Table 26** in section 17.2 in this document:

1. If the transaction data is available “in clear” to the payer (e.g. in clear in QR-code or known to the payer), the minimum data set will consist of both routing info and necessary payload data.
2. If the payer uses a proxy for the payee, the minimum data will consist of both routing info and necessary payload data, including the proxy. The translation of the proxy into the payee’s name and IBAN will be done through the interconnection between the payer’s and payee’s MSCT service providers through the HUB.
3. If the payee-presented transaction data includes a token, the minimum data will consist of both routing info and a token as payload. The translation of the token into the transaction data will be done through the interconnection between the payer’s and payee’s MSCT service providers through the HUB.

The proposed minimum data sets for these 3 cases will include:

<p>For case 1 above: <i>transaction data is available “in clear” to the payer:</i> [Version]+[Type]+ [Routing info] + [a clear-text name/value string]</p> <p>For case 2 above: <i>the payer uses a proxy for the payee:</i> [Version]+[Type]+ [Routing info] + [proxy] + [a clear-text name/value string]</p> <p>For case 3 above: <i>the payee-presented transaction data includes a token:</i> [Version]+[Type]+ [Routing info] + [token]</p>
--

Table 40: Minimum data sets for MSCTs based on payee-presented data

The version refers to the specification version of the format of the proximity technology used (e.g. QR-code).

The type may refer to the Payment Context and the Lock Transaction (LT) Indicator.

As an example, the routing info and payload data for MSCTs based on payee-presented QR-codes are described in the section below.



17.7 Payee-presented QR-code for MSCTs

To enable MSCT interoperability across SEPA, for the data exchange between the payee and payer for all payment contexts, an MSCT QR-code shall be standardised based on the minimum data set defined in section 17.6 of this document.

This standardised MSCT QR-code should be adopted by all MSCT service providers and supported by the MSCT apps in the payer's mobile device, either in the MSCT app (direct reading of the QR-code by the MSCT app) or via a link between the MSCT app and the QR-reader on the mobile device to achieve interoperability across SEPA.

For the development of a standardised MSCT QR-code the following four principles will be followed:

- A. Mobile wallets will often support multiple payment methods. The wallet user will often select and set a default payment method;
- B. Merchants will often support multiple payment methods. The merchant could set a preferred (prioritised) payment method;
- C. Avoid any special actions from merchant personnel at POI (e.g. in a store -all extra actions generate friction, such as asking what kind of wallet or what kind of payment instrument the consumer would like to use);
- D. Avoid any special actions from the wallet user at POI (more in particular in stores- e.g. swiping through a POS-menu to find your wallet generates friction).

When following the principles above, a payee-generated QR-code format for MSCTs for data exchange between the payee and the payer could be based on the following preconditions:

1. Make a generic routing/payload data-exchange at POI between the payee and the payer;
2. Routing goes directly or via (a) HUB(s) between MSCT service providers;
3. Avoid having specific details about merchant and transaction in the data exchange¹¹⁶ in order to
 - a. Reduce privacy/security concerns;
 - b. Reduce maintenance concerns related to QR-code distribution;
 - c. Increase readability of the QR-code.

¹¹⁶ A typical exception would be QR-codes on invoices.



Type

The type contains the Payment Context and could contain the Lock Transaction Indicator.

The Payment Context should enable to differentiate between the three cases mentioned under section 5 above.

As an example, the Payment Context could read as follows:

- /m/ merchant POI (physical POI in-store);
- /e/ merchant POI (e-or m-commerce);
- /i/ invoice payment;
- /p/ P2P payment.

The Lock Transaction Indicator is used to inform about the need of the Lock Transaction Function to mitigate the risk about unwanted multiple payments for the same QR-code (see also section 17.5 in this document).

QR-code format

The QR-code is based on the following format:

- A URL based on https:// structure
- First part of the URL: ordinary domain structure
- Second part of the URL: version
- Third part: type
- Fourth part: routing information
- Fifth part: payload information.

<code>HTTPS://<Domain_name>/<Version>/<Type><Payee MSCT service provider_ID>/<Payload></code>

Table 41: Coding of payee-presented QR-code for MSCTs

The Domain name could be used to refer to a dedicated MSCT interoperability framework (see Chapter 23).

Content in payload related to the Payment Contexts

The different payment contexts could require different payload requirements. As examples,

- POI situations should avoid having clear-text information (such as IBAN_merchant) in the QR-code.
- For invoice payments, the QR-code could include clear-text information that is visual anyway on the invoices.



In the table below, the payload data for the three use cases defined in section 17.2 in this document are listed.

Payload Data		
Case 1 <i>transaction data is available "in clear" to the payer</i>	Name payee (account holder)	
	Trade name	
	IBAN payee	
	MCC	Merchant Category Code
	Purpose of credit transfer (includes e.g. merchant transaction identifier)	Data for reconciliation purposes at payee – is included from initiation through entire transaction payment chain
	Remittance information structured or Remittance information unstructured	
	Currency	
Transaction amount		
Case 2 <i>the payer uses a proxy for the payee</i>	Proxy	
	MCC	Merchant Category Code
	Purpose of credit transfer (includes e.g. merchant transaction identifier)	Data for reconciliation purposes at payee – is included from initiation through entire transaction payment chain)
	Remittance information structured or Remittance information unstructured	
	Currency	
	Transaction amount	
Case 3 <i>the payee-presented transaction data includes a token</i>	Token	

Table 42: Payload data for MSCTs based on payee-presented data



18 Technical interoperability of MSCTs based on payer-presented data

18.1 Introduction

This chapter analyses in more detail the interoperability of MSCTs based on payer-presented data. As mentioned before it focuses on the interoperability of MSCT at the PSU layer and the MSCT service (provider) layer. Hereby two main functionalities will be covered:

- The exchange of the payer identification and transaction data that enables the initiation of the MSCT;
- The acknowledgement/notification messages sent to the payer and payee after a successful/unsuccessful transaction or a reject.

Next to the specification of the MSCT interoperability requirements for the HUB, based on the generic 4-corner model, illustration of transaction process flows involving the HUB for successful transactions, rejects and unsuccessful transactions are included.

The chapter further defines the minimum data set to be exchanged between payer and payee for this type of MSCTs and specifies a payer-presented QR-code for MSCTs.

18.2 Exchange of MSCT data

For MSCTs based on payer-presented data, both the payer identification data and transaction data need to be exchanged to enable the initiation of an MSCT.

18.2.1 Exchange of payer-presented data

To achieve interoperability of MSCTs based on payer-presented data, at least *payer identification data* (which enables the payer MSCT service provider to identify the payer) and an *identifier of the payer MSCT service provider* are needed in this payer-presented data.

The *payer identification data* is defined by the payer MSCT service provider, may take a variety of forms and may be static or dynamic. This payer identification data will need to be transferred as part of the Payment Request message from the payee to their MSCT service provider and further to the payer MSCT service provider, see section 18.2.2 below.

The *identifier of the payer MSCT service provider* is needed by the payee MSCT service provider and subsequently by the HUB to know where to route the Payment Request message, see section 18.2.2 below.

18.2.2 Exchange of transaction data

The transaction data (payee data and payment data) needed by the payer for the initiation of the MSCT transaction is to be exchanged between the payee and the payer via their respective MSCT service providers¹¹⁷ as follows:

¹¹⁷ If a bi-directional proximity technology is used between the payer's mobile device and the payee's device, a direct transfer of the transaction data may be possible but will not be further investigated in this document, since the process flows would be similar to MSCT use cases based on payee-presented data (see Chapter 17).



- The transaction data is provided by the payee to their MSCT service provider via a Payment Request message. Thereby the payer identification data and the identifier of the payer MSCT service provider will need to be retrieved from the payer-presented data by the payee and included, next to the transaction data, in the Payment Request message. The Payment Request message between the payee and their MSCT service provider should further at least contain a transaction identifier, the name and the IBAN¹¹⁸ of the payee and the transaction amount.
- The Payment Request message is transferred by the payee MSCT service provider via the HUB to the payer MSCT service provider using the identifier of the payer MSCT service provider received.
- The payer MSCT service provider identifies the payer and possibly their IBAN from the token included in the Payment Request message and provides the transaction data (at least the transaction amount and the name/trade name and the IBAN of the payee) to the payer for authentication purposes.

From the analysis made above, requirements can be derived for the HUB to support the payer identification and transaction data exchange needed for the interoperability of MSCTs based on payer-presented data. The table below list the required functionalities for the HUB for this exchange of transaction data

MSCT transaction feature	Requirements on HUB
<p>Exchange of data Payment Preparation phase (see Figure 28 and Figure 29)</p>	<p>MSCTs based on SCT Inst or on SCT</p>
<p>Payer-presented data</p>	
<p>Transfer of payer <i>MSCT service provider identifier</i> to payee MSCT service provider</p>	<p>The payer MSCT service provider identifier is used by the payee MSCT service provider and the HUB for routing purposes and is included in the Payment Request message.</p>
<p>Transfer of payer token to payer MSCT service provider as <i>payer identification data</i></p>	<p>Transfer of the payer token between the respective MSCT service providers – but included in the Payment Request message</p>
<p>Transfer of CustomerID¹¹⁹ and IBAN to payer MSCT service provider as <i>payer identification data</i>¹²⁰</p>	<p>Transfer of the CustomerID and IBAN between the respective MSCT service</p>

¹¹⁸ This may vary and is implementation dependent, e.g., if the IBAN is already known by the payee’s MSCT service provider it may be omitted.

¹¹⁹ In the context of this document, a CustomerID is an identification of the payer (consumer), issued by their ASPSP for access to (a) customer facing user interface(s) (e.g. their on-line banking system), as required in the PSD2 API.

¹²⁰ In this case additional protection of the data might be required, subject to further clarifications to be provided by the EBA on questions 2020_5476 and 2020_5477.



	providers – but included in the Payment Request message
Transfer of CustomerID ¹²¹ and IBAN-proxy to payer MSCT service provider as <i>payer identification data</i>	Transfer of the CustomerID and IBAN-proxy between the respective MSCT service providers – but included in the Payment Request message
Transaction data	
Transfer of <i>transaction data</i> to the payer MSCT service provider	Transfer of Payment Request message between MSCT service providers that includes the transaction data

Table 43: Required HUB functionalities for exchange of payer identification and transaction data for MSCTs based on payer-presented data

18.3 Acknowledgement/notification messages

The following messages have already been identified in sections 8.7 and 16.2 in this respect:

- Acknowledgement of receipt of the payment request message for MSCTs based on SCT to the payee by their MSCT service provider;
- Notification of payment to the payee by their MSCT service provider;
- Notification of payment to the payer by their MSCT service provider.

Note: The acknowledgement of receipt of the Payment Request message for MSCTs based on SCT Inst to the payee is not considered in view of the immediacy of the MSCT transaction.

18.3.1 Acknowledgement of receipt of payment request message for MSCTs based on SCT to the payee

For MSCTs that are based on SCT¹²², where there is no immediacy of payment, it might be useful for the payee to receive a confirmation that the payment request message has been well-received by the payer’s MSCT service provider. The acknowledgement of receipt needs to be supported by the HUB to support the interoperability of MSCTs.

¹²¹ In this case additional protection of the CustomerID might be required, subject to further clarifications to be provided by the EBA on question 2020_5476.

¹²² For MSCTs based on SCT Inst, this acknowledgement is not needed in view of the immediacy of the payment.



Acknowledgement of receipt of payment request to payee MSCTs based on SCT with payer-presented data	
	<ol style="list-style-type: none"> 1. <i>Acknowledgement of receipt of payment request</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Acknowledgement of receipt of payment request</i> by the payer MSCT service provider to the payee MSCT service provider. 3. <i>Acknowledgement of receipt of payment request</i> by the payee MSCT service provider to the payee.

Table 44: Overview of messages for acknowledgement of receipt of payment request to payee for MSCTs based on SCT with payer-presented data

18.3.2 Notifications of successful MSCT transactions

This section describes the *notification of successful transaction* messages that need to be supported to duly inform the payee and the payer for MSCTs based on payer-presented data.

18.3.2.1 MSCTs based on SCT Inst

Notification to payee

For all payment contexts, the *notification to the payee* about a *successful MSCT transaction based on SCT Inst* (i.e. after the receipt of the confirmation 6 by the payer’s ASPSP in **Figure 1**) requires the following messages to be supported:

Notification to payee Successful transactions for MSCTs based on SCT Inst with payer-presented data	
	<ol style="list-style-type: none"> 4. <i>Notification of successful transaction</i> by the payer ASPSP to the payer MSCT service provider. 5. <i>Notification successful transaction</i> by the payer MSCT service provider to the payee MSCT service provider. 6. <i>Notification successful transaction</i> by the payee MSCT service provider to the payee. <p>Or</p> <p><i>Notification of successful transaction</i> by the payee ASPSP to the payee (for specific cases only).</p>

Table 45: Overview of messages for notification to payee of successful MSCTs based on SCT Inst with payer-presented data



Notification to payer

For all payment contexts, the *notification to the payer* about a *successful MSCT transaction based on SCT Inst* (i.e. after the receipt of the confirmation 6 by the payer's ASPSP in **Figure 1**) requires the following messages to be supported:

Notification to payer	
Successful transactions for MSCTs based on SCT Inst with payer-presented data	
	<ol style="list-style-type: none"> 1. <i>Notification of successful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of successful transaction</i> by the payer MSCT service provider to the payer.

Table 46: Overview of messages for notification to payer of successful MSCTs based on SCT Inst with payer-presented data

18.3.2.2 MSCTs based on SCT

Notification to payee

For all payment contexts, the *notification to the payee* about a *successful initiation of an MSCT transaction based on SCT* (i.e. after the transfer of the SCT transaction message 3 by the payer's ASPSP in **Figure 2**) requires the following messages to be supported:

Notification to payee	
Successful transaction initiation for MSCTs based on SCT with payer-presented data	
	<ol style="list-style-type: none"> 1. <i>Notification of successful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification successful transaction</i> by the payer MSCT service provider to the payee MSCT service provider. 3. <i>Notification successful transaction</i> by the payee MSCT service provider to the payee. <p>Or</p> <p><i>Notification of successful transaction</i> by the payee ASPSP to the payee (for specific cases only).</p>

Table 47: Overview of messages for notification to payee of successful MSCTs based on SCT with payer-presented data

Notification to payer

For all payment contexts, the *notification to the payer* about a *successful MSCT transaction based on SCT* (i.e. after the receipt of the confirmation 6 by the payer's ASPSP in **Figure 2**) requires the following messages to be supported:



Notification to payer	
Successful transactions for MSCTs based on SCT Inst with payer-presented data	
1.	Notification of successful transaction by the payer ASPSP to the payer MSCT service provider.
2.	Notification of successful transaction by the payer MSCT service provider to the payer.

Table 48: Overview of messages for notification to payer of successful MSCTs based on SCT with payer-presented data

For MSCTs based on SCT, also a guarantee of payment¹²³ could be considered, but falls outside the scope of this document¹²⁴.

From the analysis made above, requirements can be derived for the HUB to support the notification of successful transactions needed for the interoperability of MSCTs based on payer-presented data. The table below list the required functionalities for the HUB for this.

MSCT transaction feature	Requirements on HUB	
	SCT Inst	SCT
Notification messages Payment Completion phase, (see Figure 28 and Figure 29)		
Notification to payee about successful transaction	Notification from payer’s MSCT service provider to payee’s MSCT service provider	Notification from payer’s MSCT service provider to payee’s MSCT service provider
Notification to payer about successful transaction	Not applicable	Not applicable

Table 49: Required HUB functionalities for notification of successful transactions for MSCTs based on payer-presented data

18.3.3 Notifications of unsuccessful transactions and rejects for MSCTs

18.3.3.1 MSCTs based on SCT Inst

For MSCTs with payer-presented data based on SCT Inst, the following categories for rejects and unsuccessful transactions could be distinguished.

¹²³ This could potentially be addressed by a dedicated MSCT interoperability framework.

¹²⁴ Note that this is planned to be addressed in phase 2 of the SEPA RTP scheme under development.



Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payer-presented data	
Cat 1	Reject by the payee MSCT service provider (before the sending of the Payment Request message to the payer MSCT service provider)
Cat 2	Reject by the payer MSCT service provider (before initiation to the payer ASPSP)
Cat 3	Reject by the payer ASPSP before execution of the SCT Inst (i.e. before message 2 in Figure 1)
Cat 4	Unsuccessful transaction - receipt by the payer ASPSP of negative confirmation message 6 in Figure 1

Table 50: Overview of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data

Annex 3 provides an overview on errors with MSCTs based on payer-presented data with a mapping on the four categories mentioned above.

The messages in the inter-PSP space related to these *rejects* and *unsuccessful transactions* have been specified in the SCT Inst scheme rule book [21] and the SCT Inst Implementation Guidelines [22].

Notification to payee

For all payment contexts, the *notification to the payee* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payee Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payer-presented data	
Cat 1	<i>Notification of reject</i> by the payee MSCT service provider to the payee.
Cat 2	<ol style="list-style-type: none"> <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. <i>Notification of reject</i> by the payee MSCT service provider to the payee.
Cat 3	<ol style="list-style-type: none"> <i>Notification of reject</i> by the payer ASPSP to the payer MSCT service provider. <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. <i>Notification of reject</i> by the payee MSCT service provider to the payee.



Cat 4 ¹²⁵	<ol style="list-style-type: none"> 1. <i>Notification of unsuccessful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of unsuccessful transaction</i> by the payer MSCT service provider to the payee MSCT service provider. 3. <i>Notification of unsuccessful transaction</i> by the payee MSCT service provider to the payee. <p>Or</p> <p><i>Notification of unsuccessful transaction</i> by the payee ASPSP to the payee (for specific cases only).</p>
-----------------------------	---

Table 51: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data

Notification to payer

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payer	
Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payer-presented data	
Cat 1	<ol style="list-style-type: none"> 1. <i>Notification of reject</i> from the payee MSCT service provider to the payee. 2. <i>Notification of reject</i> from the payee to the payer about the reject for C2B and B2B payment contexts (e.g. via display on the POI).
Cat 2	<p><i>Notification of reject</i> by the payer MSCT service provider to the payer.</p> <p>Or (for C2B or B2B payment contexts only¹²⁶)</p> <ol style="list-style-type: none"> 1. <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. 2. <i>Notification of reject</i> by the payee MSCT service provider to the payee. 3. <i>Notification of reject</i> from the payee to the payer (e.g. via display on the POI).
Cat 3	<ol style="list-style-type: none"> 1. <i>Notification of reject</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of reject</i> by the payer MSCT service provider to the payer. <p>Or (for C2B or B2B payment contexts only)</p> <ol style="list-style-type: none"> 1. <i>Notification of reject</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. 3. <i>Notification of reject</i> by the payee MSCT service provider to the payee. 4. <i>Notification of reject</i> from the payee to the payer (e.g. via the POI).

¹²⁵ As already specified in EPC096-20v1.0

¹²⁶ This will typically be used for off-line MSCT use cases whereby the payer's device has no mobile network connectivity.



Cat 4¹²⁷	<ol style="list-style-type: none"> 1. <i>Notification of unsuccessful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of unsuccessful transaction</i> by the payer MSCT service provider to the payer. <p>Or (for C2B or B2B payment contexts only)</p>
	<ol style="list-style-type: none"> 1. <i>Notification of unsuccessful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of unsuccessful transaction</i> by the payer MSCT service provider to the payee MSCT service provider. 3. <i>Notification of unsuccessful transaction</i> by the payee MSCT service provider to the payee. 4. <i>Notification of unsuccessful transaction</i> from the payee to the payer (e.g. via the POI).

Table 52: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data

18.3.3.2 MSCTs based on SCT

For MSCTs with payer-presented data based on SCT, the following categories for rejects and unsuccessful transactions could be distinguished.

Rejects and unsuccessful transactions for MSCTs based on SCT with payer-presented data	
Cat 1	Reject by the payee MSCT service provider (before the sending of the Payment Request message to the payer MSCT service provider)
Cat 2	Reject by the payer MSCT service provider (before initiation to the payer ASPSP)
Cat 3	Reject by the payer ASPSP before execution of the SCT (i.e. before message 3 in Figure 2)
Cat 4	Unsuccessful transaction - receipt by the payer ASPSP of a “Reject” or “Return” message ¹²⁸ (see DS-03 in the SCT scheme rulebook)

Table 53: Overview of rejects and unsuccessful MSCTs based on SCT with payer-presented data

Note: For MSCTs based on SCT transactions, the notification messages for unsuccessful transactions after the receipt of a “Return” may only be sent up to three days after the settlement date (Cat 4 in the table above).

¹²⁷ As already specified in EPC096-20v1.0.

¹²⁸ Note that a “Return” may be up to three days after the settlement date.



Annex 3 provides an overview on errors with MSCTs based on payer-presented data with a mapping on the four categories mentioned above.

The messages in the inter-PSP space related to these *rejects and returns* have been specified in the SCT Scheme rule book [17] and the SCT Interbank implementation guidelines [18].

Notification to payee

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payee	
Rejects and unsuccessful transactions for MSCTs based on SCT with payer-presented data	
Cat 1	<i>Notification of reject</i> by the payee MSCT service provider to the payee.
Cat 2	<ol style="list-style-type: none"> <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. <i>Notification of reject</i> by the payee MSCT service provider to the payee.
Cat 3	<ol style="list-style-type: none"> <i>Notification of reject</i> by the payer ASPSP to the payer MSCT service provider. <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. <i>Notification of reject</i> by the payee MSCT service provider to the payee.
Cat 4	<ol style="list-style-type: none"> <i>Notification of unsuccessful transaction</i> by the payer ASPSP to the payer MSCT service provider. <i>Notification of unsuccessful transaction</i> by the payer MSCT service provider to the payee MSCT service provider. <i>Notification of unsuccessful transaction</i> by the payee MSCT service provider to the payee. <p>Or</p> <p><i>Notification of unsuccessful transaction</i> by the payee ASPSP to the payee (for specific cases only).</p>

Table 54: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT with payer-presented data

Notification to payer

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payer	
Rejects and unsuccessful transactions for MSCTs based on SCT with payer-presented data	
Cat 1	1. <i>Notification of reject</i> from the payee MSCT service provider to the payer.



	2. <i>Notification of reject</i> from the payee to the payer about the reject for C2B and B2B payment contexts (e.g. via display on the POI).
Cat 2	<p><i>Notification of reject</i> by the payer MSCT service provider to the payer.</p> <p>Or (for C2B or B2B payment contexts only¹²⁹)</p> <ol style="list-style-type: none"> 1. <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. 2. <i>Notification of reject</i> by the payee MSCT service provider to the payee. 3. <i>Notification of reject</i> from the payee to the payer (e.g. via display on the POI).
Cat 3	<ol style="list-style-type: none"> 1. <i>Notification of reject</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of reject</i> by the payer MSCT service provider to the payer. <p>Or (for C2B or B2B payment contexts only)</p> <ol style="list-style-type: none"> 1. <i>Notification of reject</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of reject</i> by the payer MSCT service provider to the payee MSCT service provider. 3. <i>Notification of reject</i> by the payee MSCT service provider to the payee. 4. <i>Notification of reject</i> from the payee to the payer (e.g. via the POI).
Cat 4	<ol style="list-style-type: none"> 1. <i>Notification of unsuccessful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of unsuccessful transaction</i> by the payer MSCT service provider to the payer. <p>Or (for C2B or B2B payment contexts only)</p> <ol style="list-style-type: none"> 1. <i>Notification of unsuccessful transaction</i> by the payer ASPSP to the payer MSCT service provider. 2. <i>Notification of unsuccessful transaction</i> by the payer MSCT service provider to the payee MSCT service provider. 3. <i>Notification of unsuccessful transaction</i> by the payee MSCT service provider to the payee. 4. <i>Notification of unsuccessful transaction</i> from the payee to the payer (e.g. via the POI).

Table 55: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data

From the analysis made above, requirements can be derived for the HUB to support the notification of unsuccessful transactions and rejects needed for the interoperability of MSCTs based on payer-presented data. The table below list the required functionalities for the HUB for this.

¹²⁹ This will typically be used for off-line MSCT use cases whereby the payer’s device has no mobile network connectivity.



MSCT transaction feature	Requirements on HUB
Notification messages	MSCTs based on payer-presented data
	SCT Inst or SCT
Notification of reject to payee (Table 51 and Table 54: Cat 1)	Not applicable
Notification of reject to payee (Table 51 and Table 54: Cat 2 and 3)	Notification of reject message by payer MSCT service provider to payee MSCT service provider
Notification of unsuccessful transaction to payee (Table 51 and Table 54: Cat 4)	Notification of unsuccessful transaction by payer MSCT service provider to payee MSCT service provider
Notification of reject to payer (Table 52 and Table 55: Cat 1)	Not applicable
Notification of reject to payer (Table 52 and Table 55: Cat 2)	Notification of reject message by payee MSCT service provider to payer MSCT service provider
Notification of reject to payer (Table 52 and Table 55: Cat 3 for C2B and B2B payment contexts only)	Notification of reject message by payer MSCT service provider to payee MSCT service provider
Notification of unsuccessful transaction to payer (Table 52 and Table 55: Cat 4 for C2B and B2B payment contexts only)	Notification of unsuccessful transaction by payer MSCT service provider to payee MSCT service provider

Table 56: Required HUB functionalities for unsuccessful transactions and rejects for MSCTs based on payee-presented data

18.4 Request for recall by the payer

18.4.1 MSCTs based on SCT Inst

The SCT Inst scheme rulebook [21] describes in section 4.3.2.2 “Exception process handling” an “SCT Inst recall” under the R-transactions as follows:

“An SCT Inst recall occurs when the payer ASPSP requests to cancel an SCT Inst transaction. The recall procedure can be initiated only by the payer ASPSP which may do it on behalf of the payer. Before initiating the Recall procedure, the payer ASPSP has to check if the SCT Inst transaction is subject to one of the following reasons only:

- Duplicate sending;
- Technical problems resulting in erroneous SCT Inst transaction(s);
- Fraudulent originated SCT Inst instruction.”

In the inter-PSP space this procedure is handled via the “Recall of an SCT Inst” (DS-05) and “Answer to a recall of SCT Inst” messages which are specified respectively in sections 4.5.6 and 4.5.7 of SCT Inst scheme rulebook [21]. The rulebook also specifies in section 4.3.2.2 the main characteristics of the “Recall of an SCT Inst” and the “Answer to a recall”.



The SCT Inst rulebook further defines in section 4.3.2.3 a “Request for recall by the payer” as follows:

*“A Request for recall by the payer can be initiated by the payer ASPSP after a payer has requested the payer ASPSP to get the reimbursement of a settled SCT Inst transaction for a reason **other than** duplicate sending, technical problems resulting in erroneous SCT Inst transactions or a fraudulently originated SCT Inst instruction.*

The payer ASPSP is obliged to inform the payer that such Request for recall does not guarantee that the payer will effectively receive back the funds of the initial SCT Inst transaction. It will depend on the consent of the payee whether to turn back the funds to the payer.”

The payer shall always be informed by their MSCT service provider (if involved in the Request for recall by the payer) or by their ASPSP about the result of the recall. The payee will typically be contacted directly by their ASPSP if a recall is received from the payer ASPSP, as described in the SCT Inst scheme rulebook ([21], section 4.3.2.2).

18.4.2 MSCTs based on SCT

The SCT scheme rulebook [17] describes in section 4.3.2.3 “Exception process handling” a “Recall” under the R-transactions as follows:

*“A **Recall** occurs when the payer ASPSP requests to cancel an SCT transaction. The recall procedure can be initiated only by the payer ASPSP which may do it on behalf of the payer. Before initiating the Recall procedure, the payer ASPSP has to check if the SCT transaction is subject to one of the following reasons only:*

- Duplicate sending;
- Technical problems resulting in an erroneous SEPA Credit Transfer Transaction;
- Fraudulent originated SEPA Credit Transfer Instruction.”

In the inter-PSP space this procedure is handled via the “Request for Recall” (DS-07) and “Response to request for Recall” (DS-07) messages which are specified respectively in sections 4.5.7 and 4.5.8 of the SCT scheme rulebook [17]. The rulebook also specifies in section 4.3.2.3 the main characteristics of the “Recall” and the “Response to Recall”.

The SCT rulebook further defines in section 4.3.2.4 a “Request for recall by the payer” as follows:

“A Request for recall by the payer can be initiated by the payer ASPSP after a payer has requested the payer ASPSP to get the reimbursement of a settled SCT transaction for a reason other than duplicate sending, technical problems resulting in an erroneous SCT transaction and a fraudulently originated SCT instruction.

The payer ASPSP is obliged to inform the payer that such Request for Recall does not guarantee that the payer will effectively receive back the funds of the initial SCT transaction. It will depend on the consent of the payee whether to turn back the funds to the payer.”



The payer shall always be informed by their MSCT service provider (if involved on the Request for recall by the payer) or by their ASPSP about the result of the recall. The payee will typically be contacted directly by their ASPSP if a recall is received from the payer ASPSP, as described in the SCT scheme rulebook ([17], section 4.3.2.3).

Since these are very exceptional processes both for SCT Inst and SCT for which different communication channels could be used between the PSU and their MSCT service provider or ASPSP, that is not impacting the interoperability amongst MSCT service providers, this *Request for recall by the payer* will not be further analysed in this document.

18.5 Illustrative interoperability process flows for MSCTs based on payer-presented data

18.5.1 Introduction

In this section the full process flows between the HUB and respective MSCT service provider back-ends for a few examples will be described. These examples are provided for illustrative purposes only. Note that as mentioned before, an MSCT service provider could be an ASPSP. This means that in the process flows below, one or both MSCT providers could be one or both of the respective ASPSPs in which case the process flows would simplify.

Four cases will be considered as listed in the table below.

MSCT transactions	Support from the HUB ¹³⁰	Reference
C2B – successful transaction based on SCT Inst Consumer-presented QR-code contains a token	<ul style="list-style-type: none"> • Payment request messages (see section 18.2) • Notification of successful transaction (see section 18.3) 	Section 18.5.2
C2B - reject by the payer (consumer) ASPSP service provider for MSCT based on SCT Inst Consumer-presented QR-code including a token (Table 50: Cat 3)	<ul style="list-style-type: none"> • Retrieval of the payee data from the proxy (see section 18.2) • Notification of reject (see section 18.317.3) 	Section 18.5.3
C2B - unsuccessful transaction for MSCT based on SCT Inst Consumer-presented data including CustomerID and IBAN (Table 50: Cat 4).	<ul style="list-style-type: none"> • Retrieval of the transaction data from the token (see section 18.2) • Notification of unsuccessful transaction (see section 18.3) 	Section 18.5.4
C2B – reject by the payer (consumer) MSCT service provider for MSCT based on SCT	<ul style="list-style-type: none"> • Payment request messages (see section 18.2) • Notification of reject (see section 18.3) 	Section 18.5.5

¹³⁰ Depicted by the green arrows in the illustrative process flows below.



<p>Consumer-presented data including CustomerID and IBAN (Table 53: Cat 2)</p>		
---	--	--

Table 57: Illustrative process flows for interoperability of MSCT transactions based on payer-presented data with mapping onto HUB functionalities

All process flows for C2B payment contexts in the next sections are illustrated for physical POIs. Note however that the process flows would remain the same if the QR-code is shown on a payment page of an e-merchant.

The QR-code may be static or dynamic. In case dynamic QR-codes are used, a *conditional transaction lock function* is defined as follows. The function consists of conditional lock transaction messages that are sent between the consumer’s MSCT service provider and the merchant’s MSCT service provider via the HUB to prevent that multiple consumers from different MSCT service providers pay the same transaction after strong customer authentication (see section 8.3). The transaction lock function is required in case the QR-code stays active for a certain time window that would enable multiple scans and related payments and its need is specified in the dedicated Lock Transaction Indicator (LT Indicator as defined in section 17.6 in this document). If two consumers would perform SCA on the same transaction, the consumer with successful SCA for which the lock function sent by their MSCT service provider reaches as first the MSCT service provider of the merchant is the one for which the transaction is locked.

For P2P transactions whereby the payee presents a QR-code on their mobile device to the payer and for C2B transactions involving QR-codes on invoices, the process flow will be similar as for C2B transactions with merchant-presented QR-codes.

Note also that in the process flows below, the representation and description of strong customer authentication (SCA) is simplified since the focus is on the interconnectivity between the respective MSCT service providers. More details on SCA are provided in section 8.3 and are illustrated in the MSCT use cases in Chapter 7.

Furthermore, the process flows do not include potential exchanges needed between MSCT service provider back-ends for applicable remuneration to support a business model.



18.5.2 Successful MSCT – C2B based on SCT Inst with consumer-presented QR-code containing a token

In this section the process flow for a successful in-store payment between a consumer (payer) and merchant (payee) using the HUB is illustrated. In this example, it is assumed that the consumer-presented data does not contain the consumer identification “in clear” but that a token is used instead (see section 18.2). It is hereby assumed that the tokenisation/de-tokenisation process is handled by or via the consumer’s MSCT service provider. The consumer-presented data includes the identifier of the consumer’s MSCT service provider “in clear” so that it can be retrieved by the merchant and provided to their MSCT service provider in the payment request message.

In this example, the following actors and interconnectivity are required as depicted below.

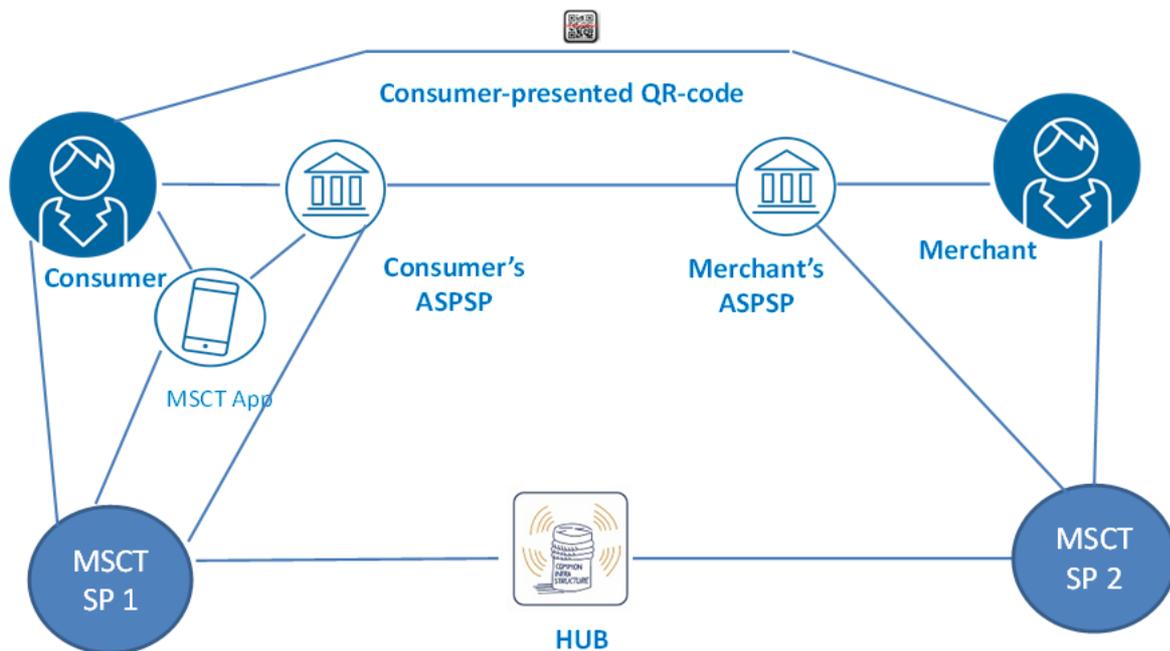


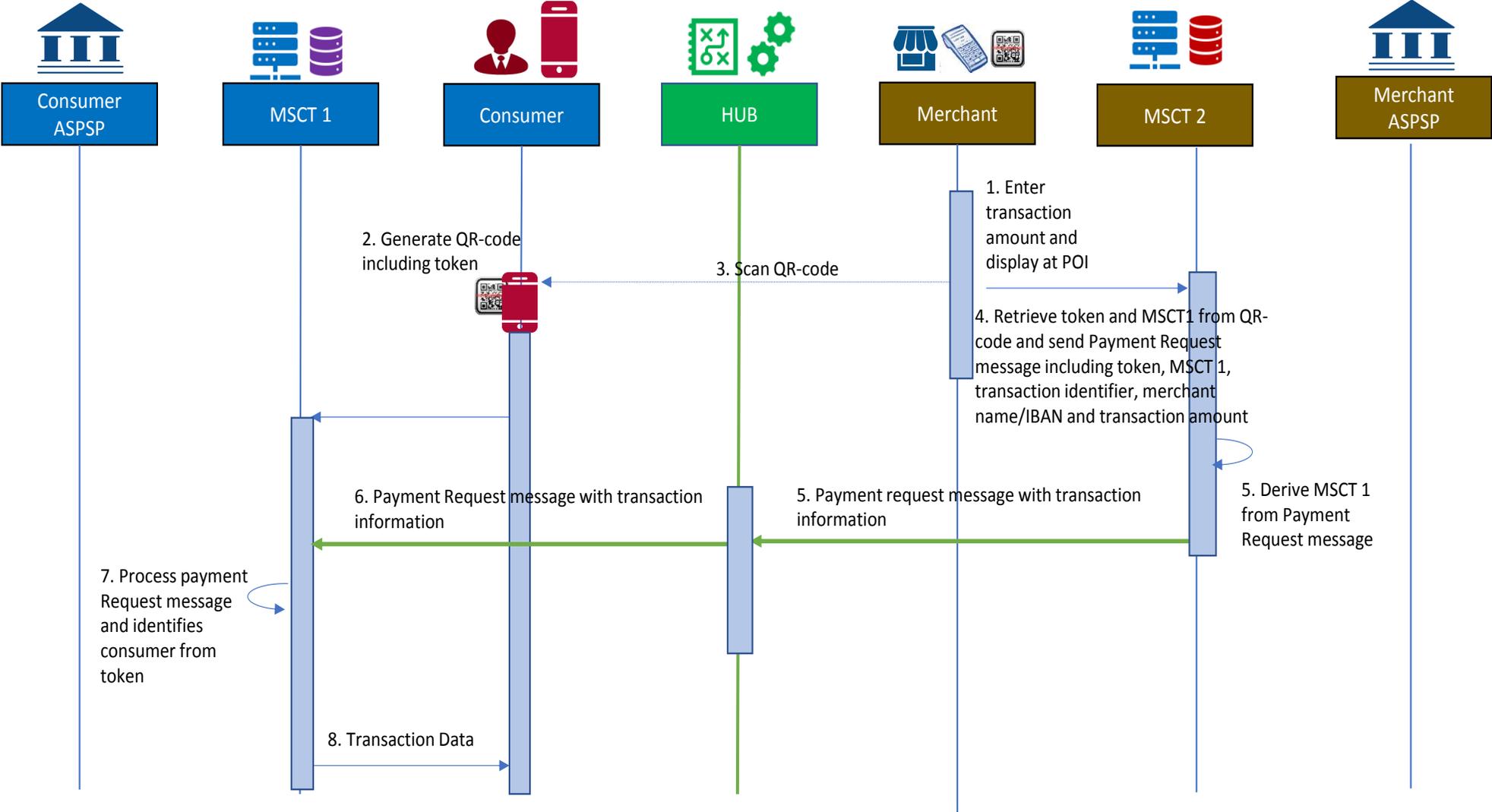
Figure 57: Actors for C2B - with consumer token

The detailed process flows between the different actors involved for this MSCT transaction type are shown in the next figure.



Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance

EPC269-19 Version 1.14





Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance
EPC269-19 Version 1.14

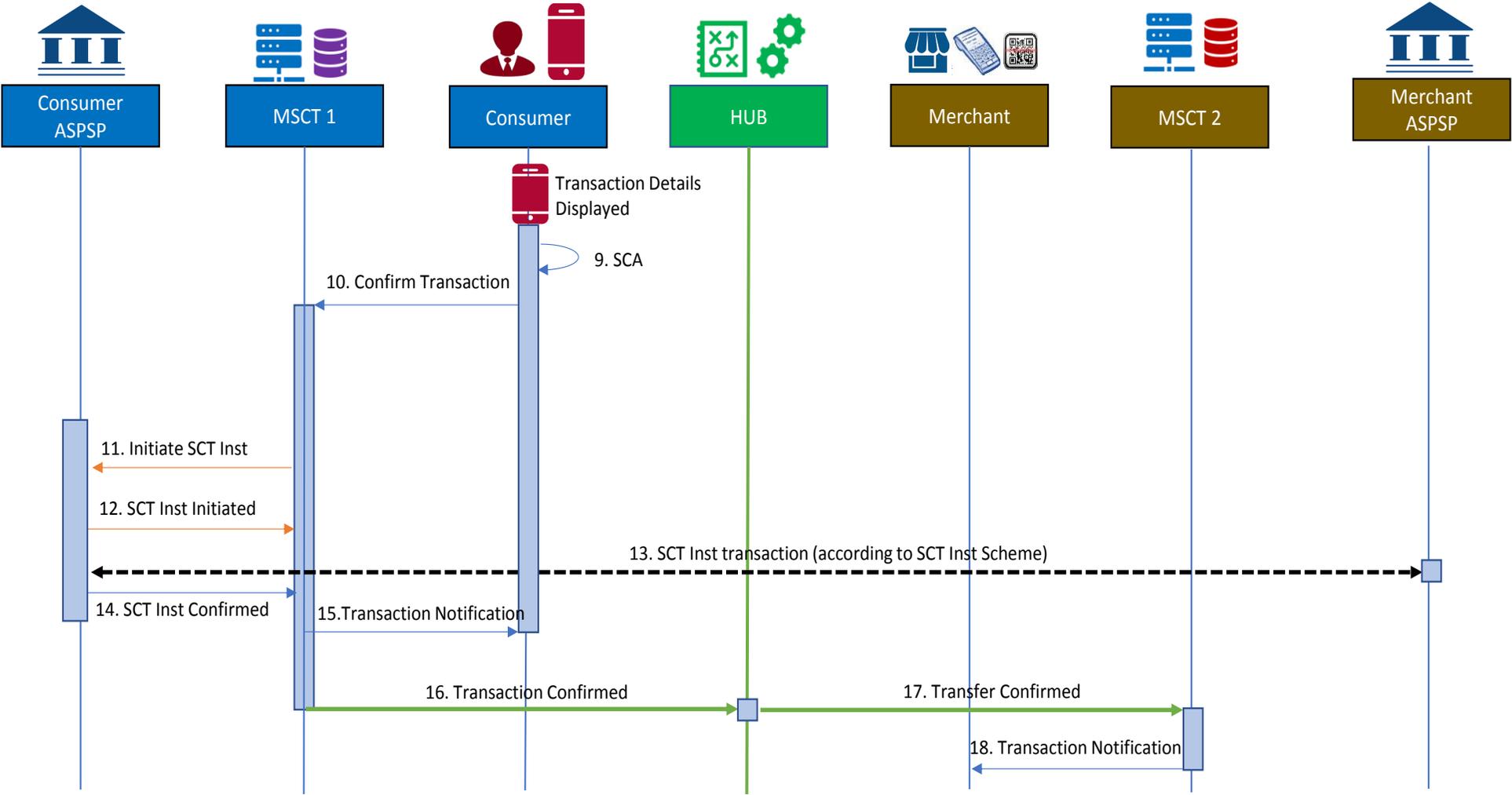


Figure 58: Process flow – C2B – consumer-presented QR-code with token



In the figure above the following steps are involved:

Step 1

- The merchant enters the transaction amount which is displayed on the POI¹³¹.

Step 2

- The consumer selects and opens the MSCT Inst application on their mobile device which possibly involves the entry of a password.
- A QR-code containing a consumer token and their MSCT service provider identifier is generated by the MSCT Inst application on the mobile device.

Step 3

The consumer presents the QR-code which is scanned by the merchant's POI.

Step 4

The merchant retrieves the consumer's token and the consumer's MSCT service provider identifier from the QR-code and sends a Payment Request message to their MSCT service provider, including the merchant's name, IBAN_merchant¹³², merchant transaction identifier, the transaction amount, the consumer's MSCT service provider identifier and the consumer token.

Step 5:

The Payment Request message including the consumer's MSCT service provider identifier is sent to the HUB.

Step 6:

The HUB identifies the consumer's MSCT service provider and forwards them the Payment Request message containing the consumer token and transaction data.

Step 7:

The consumer's MSCT service provider checks the Payment Request message, retrieves the transaction data and the consumer's name and possibly IBAN from the consumer token.

Step 8:

The consumer's MSCT service provider sends the transaction details to the consumer.

Step 9:

The consumer consents to the transaction based on the details displayed and performs SCA¹³³.

¹³¹ The display of the transaction amount by the POI may happen at a later stage since the payer indemnity might have an impact on the final transaction amount (e.g., discounts). However this could require additional steps to obtain the payer identification from the token received. This would need to be analysed in forthcoming work by the MSG MSCT.

¹³² Instead of the IBAN_merchant a proxy may be used.

¹³³ The SCA may be performed by the consumer's MSCT service provider or by their ASPSP. This may involve additional steps which are not illustrated in this process flow since they do not impact the interoperability. Here it is assumed that the consumer's MSCT service provider has received delegation from the consumer's ASPSP for SCA subject to appropriate agreements.



Step 10:

The confirmation including the authentication response is provided to the consumer's MSCT service provider.

Step 11:

After checking the authentication response, the consumer's MSCT service provider sends an SCT Inst instruction to the consumer's ASPSP including the transaction details.

Step 12:

The consumer's ASPSP sends a message to the consumer's MSCT service provider confirming the initiation of the SCT Inst.

Step 13:

The consumer's ASPSP sends the SCT Inst transaction to the merchant's ASPSP and the transaction flow is handled according to the SCT Inst scheme.

Step 14:

The consumer's ASPSP sends a confirmation message to the consumer's MSCT service provider about the execution of the SCT Inst transaction.

Step 15:

The consumer's MSCT service provider sends a transaction notification message to the consumer.

Step 16:

The consumer's MSCT service provider sends a transaction notification message to the HUB with the merchant's MSCT service provider identifier.

Step 17:

The HUB forwards the transaction notification message to the merchant's MSCT service provider.

Step 18:

The merchant's MSCT service provider sends a transaction notification message to the merchant.



18.5.3 Reject by payer ASPSP service provider – C2B based on SCT Inst with consumer-presented QR-code containing a token

The process flow below illustrates the usage of the HUB in the case of a reject by the consumer (payer) ASPSP for an MSCT based on consumer-presented data using a QR-code including a token. This may be a dynamic or a static token. It is hereby assumed that the tokenisation/de-tokenisation of (part of) the transaction data is handled by or via the consumer MSCT service provider. In this illustration it is assumed that the payer ASPSP rejects the MSCT after an unsuccessful SCA.

In this example, the following actors and interconnectivity are required as depicted below.

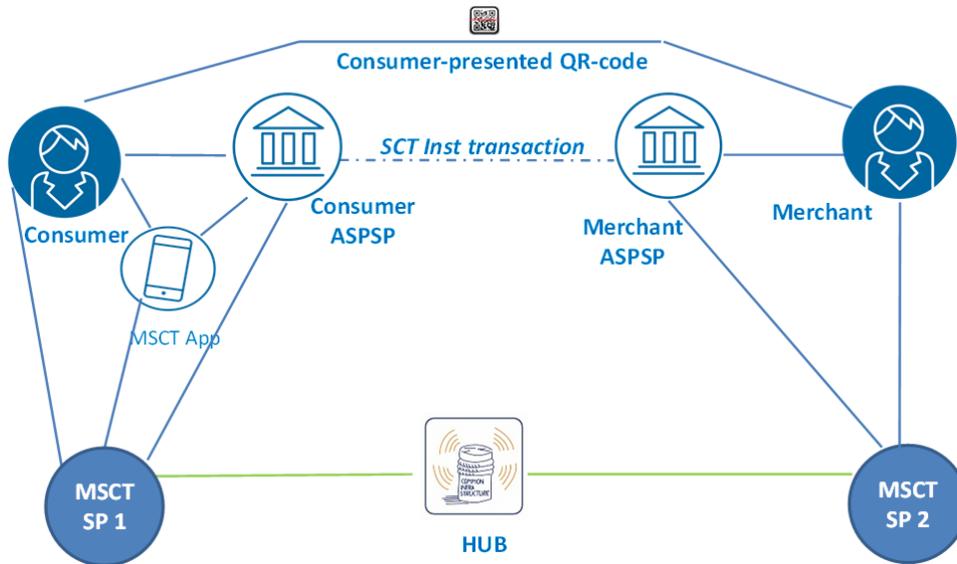
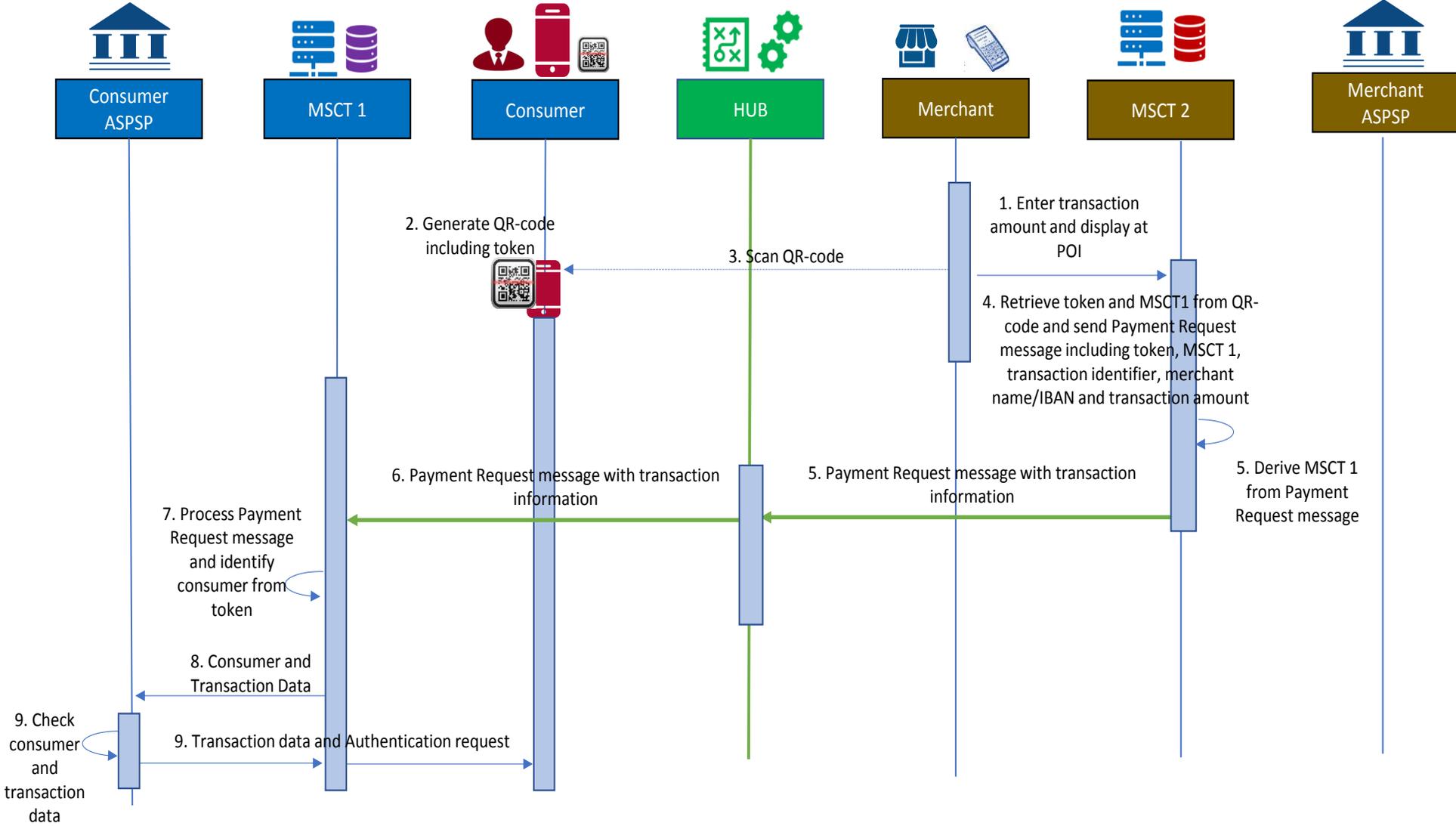


Figure 59: Actors for reject by consumer ASPSP for C2B payment context

The detailed process flows between the different actors involved in this MSCT transaction type are shown in the next figure.



Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance
EPC269-19 Version 1.14



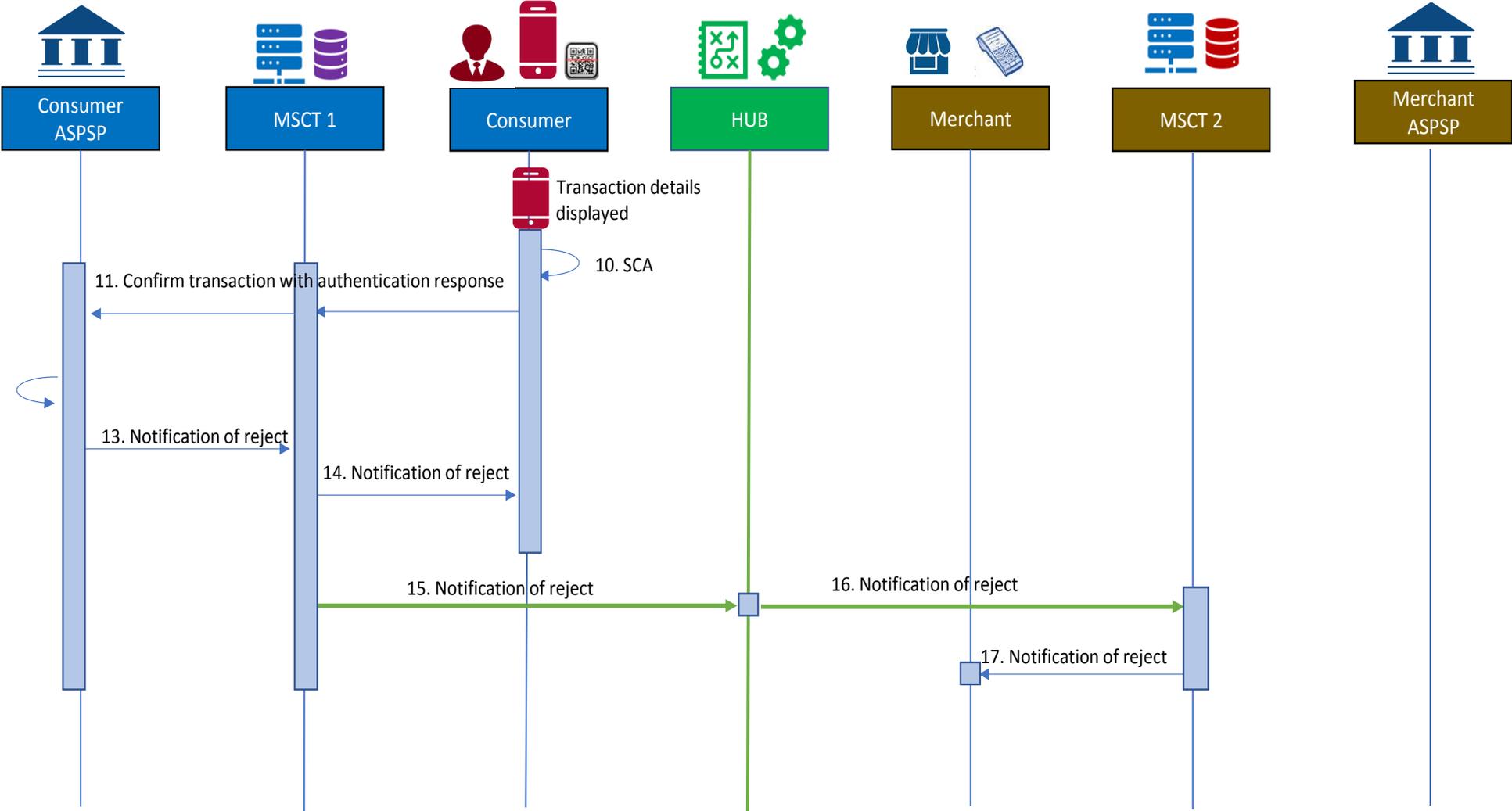


Figure 60: Process flow – C2B – Reject by consumer ASPSP for MSCT based on consumer-presented QR-code with token



In the figure above the following steps are involved:

Step 1

The merchant enters the transaction amount which is displayed on the POI¹³⁴.

Step 2

- The consumer selects and opens the MSCT Inst application on their mobile device which possibly involves the entry of a password.
- A QR-code containing a consumer token and their MSCT service provider identifier is generated by the MSCT Inst application on the mobile device.

Step 3

The consumer presents the QR-code which is scanned by the merchant POI.

Step 4

The merchant retrieves the consumer token and the consumer MSCT service provider identifier from the QR-code and sends a Payment Request message to their MSCT service provider, including the merchant name/trade name, IBAN_merchant18F135, merchant transaction identifier, the transaction amount, the consumer MSCT service provider identifier and the consumer token.

Step 5:

The Payment Request message including the consumer MSCT service provider identifier is sent to the HUB.

Step 6:

The HUB identifies the consumer MSCT service provider and forwards them the Payment Request message containing the consumer token and transaction data.

Step 7:

The consumer MSCT service provider checks the Payment Request message, retrieves the transaction data and the consumer name and possibly IBAN from the consumer token.

Step 8:

The consumer MSCT service provider sends the consumer and transaction details to the consumer ASPSP.

Step 9:

- The consumer ASPSP checks the consumer and transaction details
- The consumer ASPSP sends the transaction details with an authentication request to the consumer via the consumer MSCT service provider.

Step 10:

The consumer consents to the transaction based on the details displayed and performs SCA.

¹³⁴ The display of the transaction amount by the POI may happen at a later stage since the payer indemnity might have an impact on the final transaction amount (e.g., discounts). However this could require additional steps to obtain the payer identification from the token received. This would need to be analysed in forthcoming work by the MSG MSCT.

¹³⁵ Instead of the IBAN_merchant a proxy may be used.



Step 11:

The confirmation including the authentication response is provided to the consumer ASPSP via the consumer MSCT service provider.

Step 12:

The consumer ASPSP checks the authentication response which is incorrect and rejects the transaction¹³⁶.

Step 13:

The consumer ASPSP sends a notification of reject to the consumer MSCT service provider.

Step 14:

The consumer MSCT service provider sends a notification of reject to the consumer.

Step 15:

The consumer MSCT service provider sends a notification of reject to the HUB with the merchant MSCT service provider identifier.

Step 16:

The HUB forwards the notification of reject to the merchant MSCT service provider.

Step 17:

The merchant MSCT service provider sends the notification of reject to the merchant.



18.5.4 Unsuccessful MSCT – C2B based on SCT Inst with consumer-presented QR-code containing consumer identification in clear

The process flow below illustrates the usage of the HUB in the case of an unsuccessful transaction (after receipt by the consumer ASPSP of the negative confirmation message 6 in **Figure 1**) for an MSCT based on consumer-presented data using a QR-code including the CustomerID and IBAN_Consumer in “clear”.

In this example, the following actors and interconnectivity are required as depicted below.

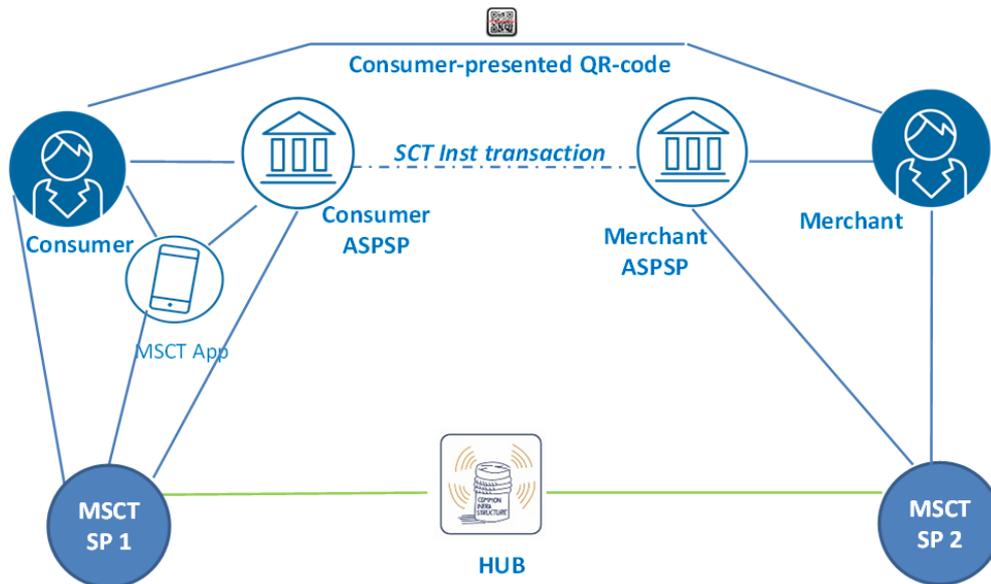
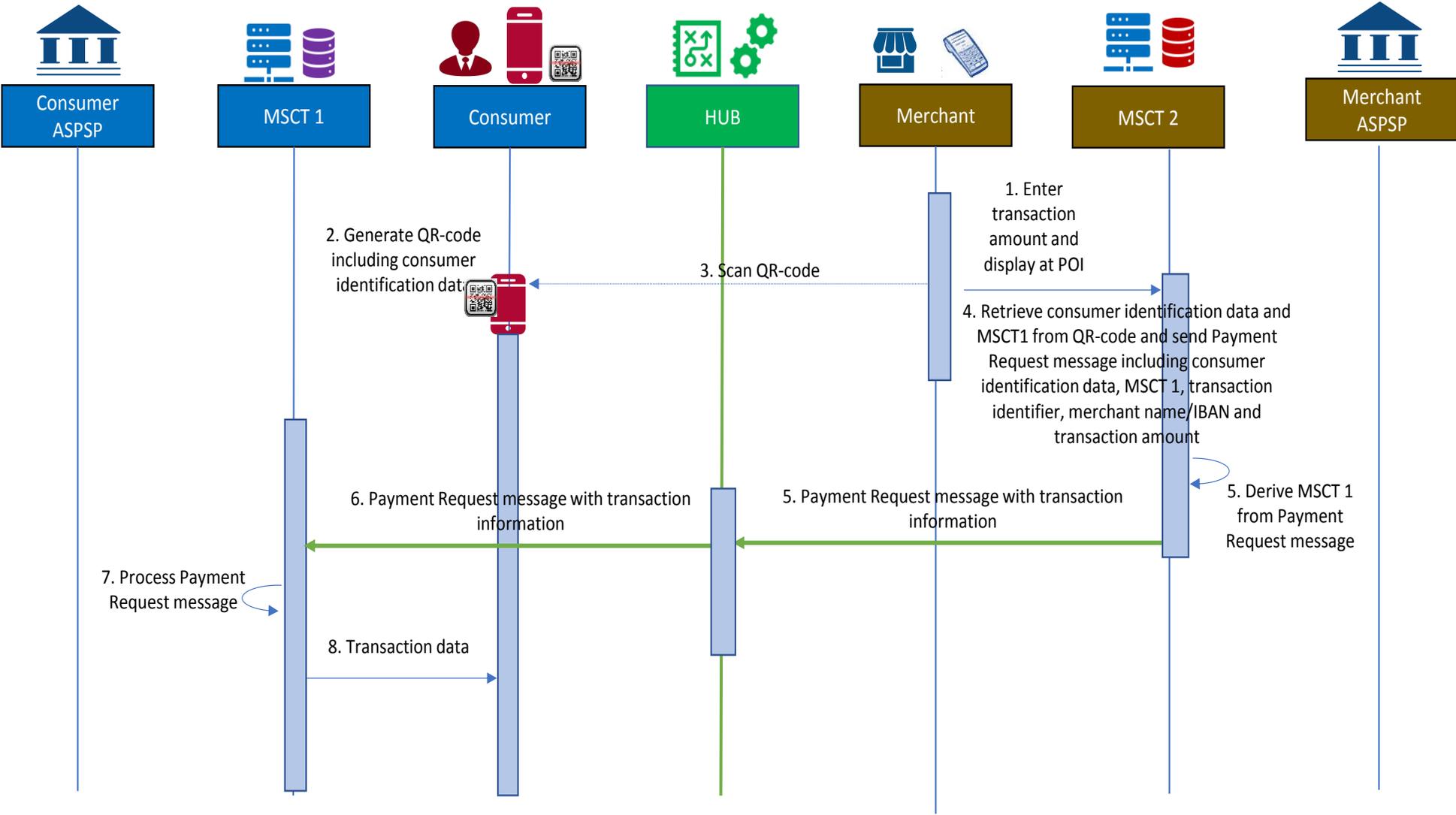


Figure 61: Actors for unsuccessful transaction for C2B payment context

The detailed process flows between the different actors involved in this MSCT transaction type are shown in the next figure.



Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance
EPC269-19 Version 1.14



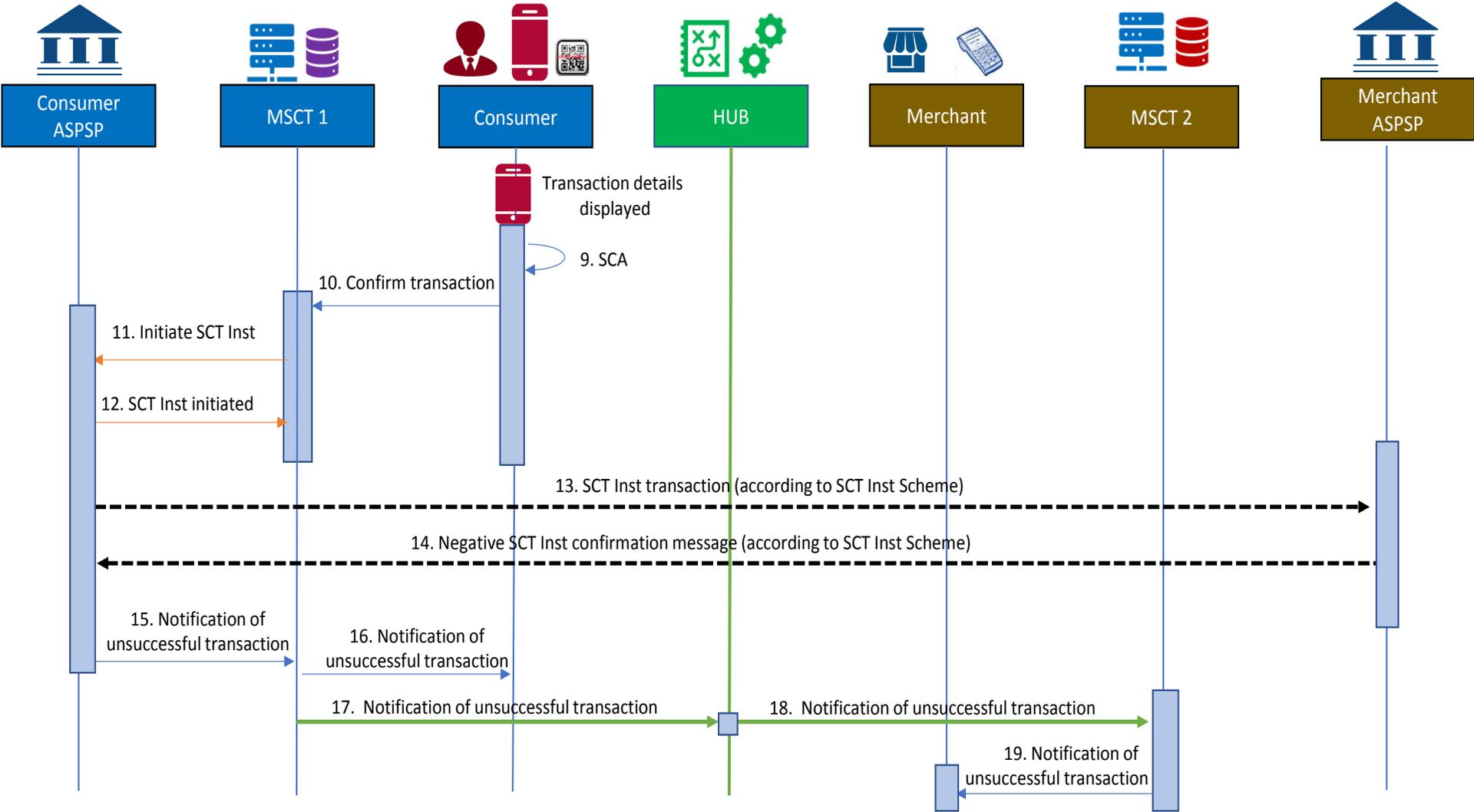


Figure 62: Process flow – C2B – Unsuccessful transaction for MSCT based on consumer-presented QR-code without token



In the figure above the following steps are involved:

Step 1

The merchant enters the transaction amount which is displayed on the POI¹³⁷.

Step 2

- The consumer selects and opens the MSCT Inst application on their mobile device which possibly involves the entry of a password.
- A QR-code containing the CustomerID and IBAN_consumer and their MSCT service provider identifier is generated by the MSCT Inst application on the mobile device.

Step 3

The consumer presents the QR-code which is scanned by the merchant POI.

Step 4

The merchant retrieves the consumer data and the consumer MSCT service provider identifier from the QR-code and sends a Payment Request message to their MSCT service provider, including the merchant name/trade name, IBAN_merchant¹³⁸, merchant transaction identifier, the transaction amount, the consumer's MSCT service provider identifier, the CustomerID and IBAN_consumer.

Step 5:

The Payment Request message including the consumer MSCT service provider identifier is sent to the HUB.

Step 6:

The HUB identifies the consumer MSCT service provider and forwards them the Payment Request message containing the consumer and transaction data.

Step 7:

The consumer MSCT service provider checks the Payment Request message and retrieves the consumer and transaction data.

Step 8:

The consumer MSCT service provider sends the transaction details to the consumer.

Step 9:

The consumer consents to the transaction based on the details displayed and performs SCA¹³⁹.

Step 10:

The confirmation including the authentication response is provided to the consumer MSCT service provider.

¹³⁷ The display of the transaction amount by the POI may happen at a later stage since the payer indemnity might have an impact on the final transaction amount (e.g., discounts). However this could require additional steps to obtain the payer identification from the token received. This would need to be analysed in forthcoming work by the MSG MSCT.

¹³⁸ Instead of the IBAN_merchant a proxy may be used.

¹³⁹ The SCA may be performed by the consumer's MSCT service provider or by their ASPSP. This may involve additional steps which are not illustrated in this process flow since they do not impact the interoperability (see Chapter 8). Here it is assumed that the consumer's MSCT service provider has received delegation from the consumer's ASPSP for SCA subject to appropriate agreements.



Step 11:

After checking the authentication response, the consumer MSCT service provider sends an SCT Inst instruction to the consumer ASPSP including the transaction details.

Step 12:

The consumer ASPSP sends a message to the consumer MSCT service provider confirming the initiation of the SCT Inst.

Step 13:

The consumer ASPSP sends the SCT Inst transaction to the merchant ASPSP and the transaction flow is handled according to the SCT Inst scheme.

Step 14:

The consumer ASPSP receives a negative confirmation message from the merchant ASPSP.

Step 15:

The consumer ASPSP sends a notification message of unsuccessful transaction to the consumer MSCT service provider.

Step 16:

The consumer MSCT service provider sends a notification of unsuccessful transaction to the consumer.

Step 17:

The consumer MSCT service provider sends a notification of unsuccessful transaction to the HUB with the merchant MSCT service provider identifier.

Step 18:

The HUB forwards the notification of unsuccessful transaction to the merchant MSCT service provider.

Step 19:

The merchant MSCT service provider sends a notification of unsuccessful transaction to the merchant.



18.5.5 Reject by payer MSCT service provider – C2B based on SCT with consumer-presented QR-code containing consumer identification in clear

The process flow below illustrates the usage of the HUB in the case of a reject by the consumer (payer) MSCT service provider for an MSCT in a C2B payment context, based on consumer-presented data using a QR-code including a the CustomerID and IBAN. In this illustration it is assumed that the consumer MSCT service provider rejects the MSCT after having received the payment request message from the merchant MSCT service provider (e.g., due to the fact that incomplete or incorrect data is provided).

In this MSCT transaction type, the following actors and interconnectivity are required as depicted below.

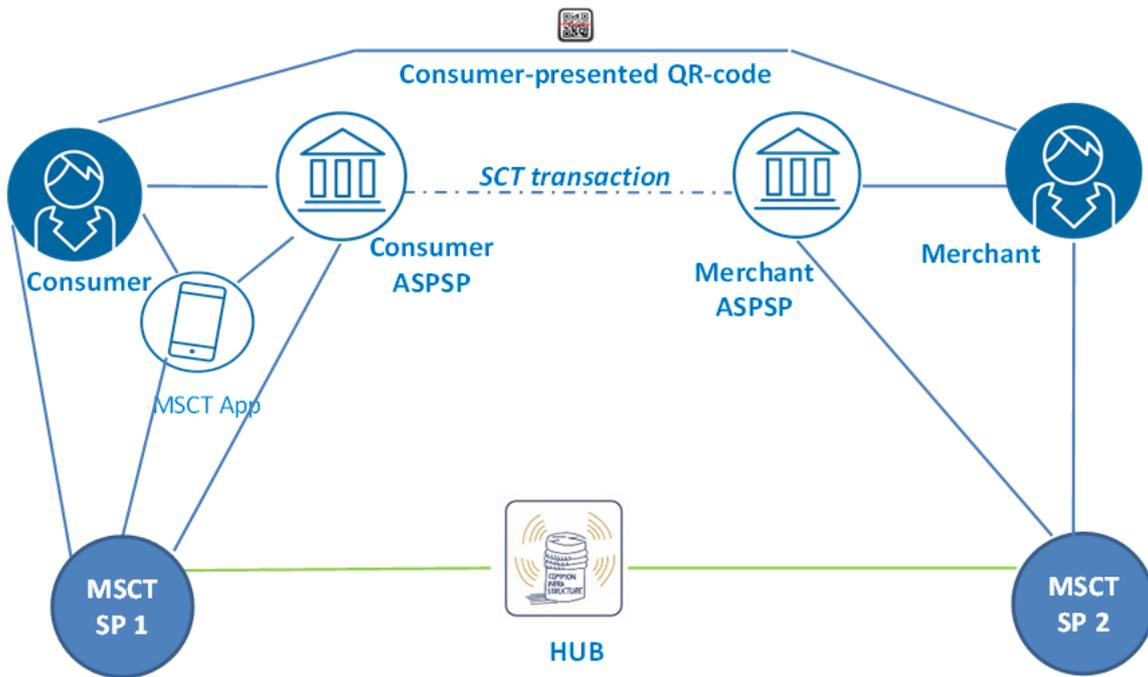


Figure 63: Actors for reject by consumer MSCT service provider for C2B payment context

The detailed process flows between the different actors involved in this MSCT transaction are shown in the next figure.

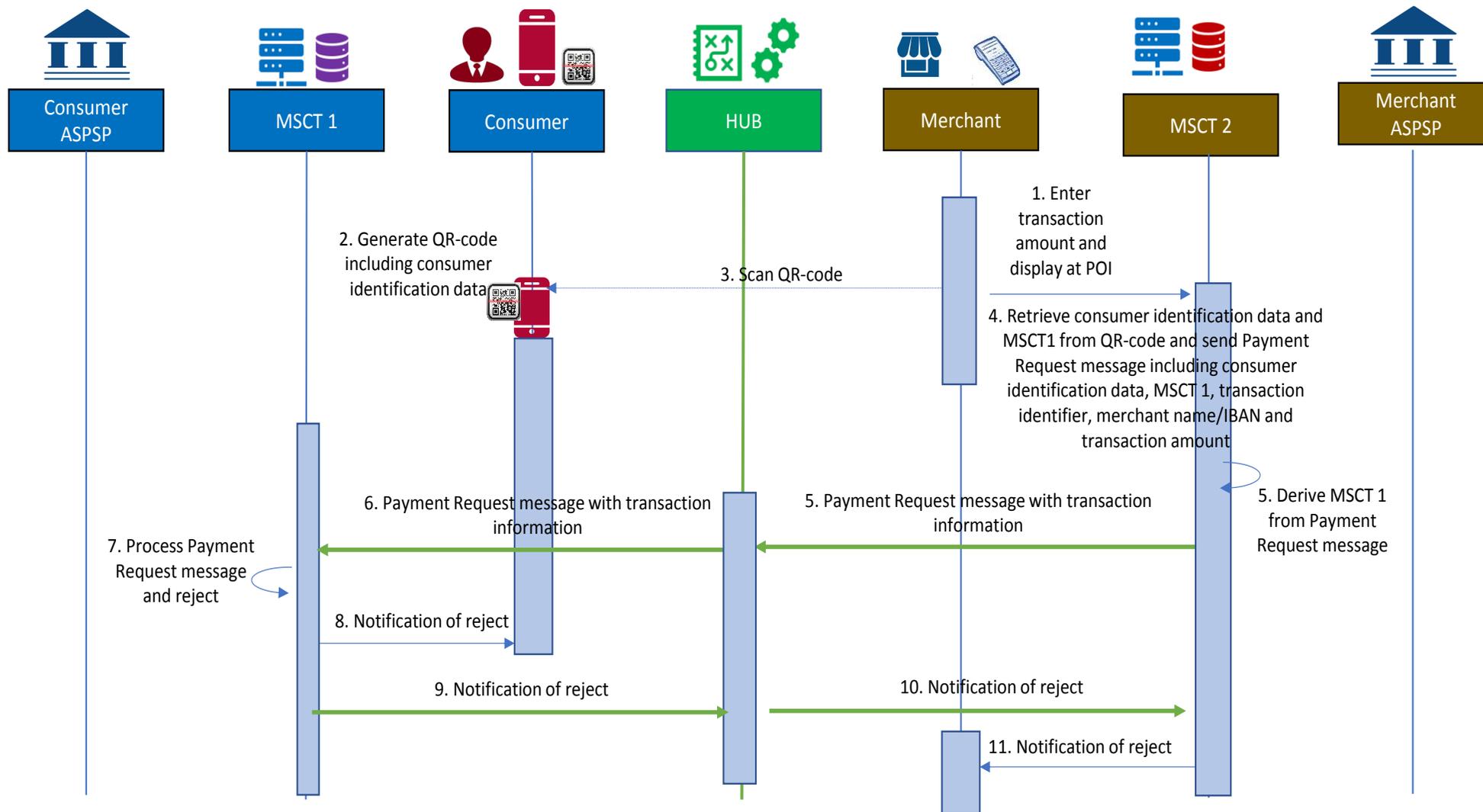


Figure 64: Process flow – C2B – Reject by consumer MSCT service provider for MSCT based on consumer-presented QR-code without token



In the figure above the following steps are involved:

Step 1

The merchant enters the transaction amount which is displayed on the POI¹⁴⁰.

Step 2

- The consumer selects and opens the MSCT Inst application on their mobile device which possibly involves the entry of a password.
- A QR-code containing the CustomerID and IBAN_consumer and their MSCT service provider identifier is generated by the MSCT Inst application on the mobile device.

Step 3

The consumer presents the QR-code which is scanned by the merchant's POI.

Step 4

The merchant retrieves the consumer data and the consumer MSCT service provider identifier from the QR-code and sends a Payment Request message to their MSCT service provider, including the merchant's name, IBAN_merchant18F141, merchant transaction identifier, the transaction amount, the consumer's MSCT service provider identifier, the CustomerID and IBAN_consumer.

Step 5:

The Payment Request message including the consumer MSCT service provider identifier is sent to the HUB.

Step 6:

The HUB identifies the consumer MSCT service provider and forwards them the Payment Request message containing the consumer and transaction data.

Step 7:

- The consumer MSCT service provider checks the Payment Request message and retrieves the consumer and transaction data.
- The consumer MSCT service provider rejects the transaction due to incomplete or incorrect data provided in the Payment Request message.

Step 8:

The consumer MSCT service provider sends a notification of reject to the consumer.

Step 9:

The consumer MSCT service provider sends a notification of reject to the HUB to the HUB with the merchant MSCT service provider identifier.

Step 10:

¹⁴⁰ The display of the transaction amount by the POI may happen at a later stage since the payer indemnity might have an impact on the final transaction amount (e.g., discounts). However this could require additional steps to obtain the payer identification from the token received. This would need to be analysed in forthcoming work by the MSG MSCT.

¹⁴¹ Instead of the IBAN_merchant a proxy may be used.



The HUB forwards the notification of reject to the merchant MSCT service provider.

Step 11:

The merchant MSCT service provider sends the notification of reject to the merchant.

18.6 Minimum data set for MSCTs based on payer-presented data

To achieve interoperability for MSCTs, an agreement on a minimum data set is required for the data to be exchanged between the payer/consumer and payee/merchant, being it in the payer-presented data or in the payment request messages exchanged (see section 18.2).

The minimum data set to be exchanged between the payee and the payer, will rely on the MSCT transaction feature, such as described in **Table 43** in section 18.2 in this document:

1. If the payer-presented data provided to the payee contains a (*payer*) token, the minimum data will consist of both routing info (i.e. the identifier of the payer MSCT service provider) and the (*payer*) token as payload. The minimum data will be forwarded in the Payment Request message through the HUB from the payee MSCT service provider to the payer MSCT service provider for de-tokenisation into the payer identification data, together with the other transaction data.
2. If the payer-presented data provided to the payee contains the *CustomerID* and *IBAN* “in clear” (e.g. in clear in a QR-code) of the payer, the minimum data set will consist of both routing info (i.e. the identifier of the payer MSCT service provider) and the *CustomerID* and *IBAN*. The minimum data will be forwarded in the Payment Request message through the HUB from the payee MSCT service provider to the payer MSCT service provider together with the other transaction data.
3. If the payer-presented data provided to the payee contains the *CustomerID* (“in clear”) and an *IBAN-proxy* of the payer, the minimum data set will consist of both routing info (i.e. the identifier of the payer MSCT service provider) and the *CustomerID* and *IBAN-proxy*. The minimum data will be forwarded in the Payment Request message through the HUB from the payee MSCT service provider to the payer MSCT service provider together with the other transaction data. The *IBAN* will need to be derived from the *IBAN-proxy* by the payer MSCT service provider.

The minimum data sets for these 3 cases are as follows:

For case 1 - the payer-presented data includes a token:

[Version]+[Type]+[payer MSCT service provider ID]+[(payer) token]

For case 2 – the payer-presented data contains the CustomerID and IBAN “in clear”

[Version]+[Type]+[payer MSCT service provider ID]+[CustomerID + IBAN_payer]



For case 3 – the payer-presented data contains the CustomerID “in clear” and a proxy

[Version]+[Type]+[payer MSCT service provider ID]+[CustomerID + IBAN-proxy]

Table 58: Minimum data sets for MSCTs based on payer-presented data

Note: There might be a need for the merchant, in C2B payment contexts, to identify the consumer to offer additional services or benefits. For interoperability, the consumer identification means would need to be standardised in future work and could be added to the payload information (see Table 59).

The version refers to the specification version of the format of the proximity technology used (e.g., the QR-code, see section 18.7).

The type may refer to the cases above and may enable to add other services¹⁴².

The payer MSCT service provider identifier is used in the interoperability space for routing purposes, therefore a standardisation of this data element will be necessary.

The payer identification data (that is part of the payload) needs to be included in the Payment Request message. Therefore, a predefined length and character set need to be specified.

18.7 Payer-presented QR-code for MSCTs

To enable MSCT interoperability across SEPA, for the data exchange between the payer and payee for all payment contexts, an MSCT QR-code shall be standardised based on the minimum data set defined in section 18.6 of this document.

This standardised MSCT QR-code should be adopted by all MSCT service providers and supported by the MSCT apps in the payer’s mobile device, either in the MSCT app (direct reading of the QR-code by the MSCT app) or via a link between the MSCT app and the QR-reader on the mobile device to achieve interoperability across SEPA.

For the development of a standardised MSCT QR-code the following three principles will be followed:

- A. Mobile wallets will often support multiple payment methods. The wallet user will often select and set a default payment method;
- B. Avoid any special actions from merchant personnel at POI (e.g. in a store - all extra actions generate friction, such as asking what kind of wallet or what kind of payment instrument the consumer would like to use);
- C. Avoid any special actions from the wallet user at POI (more in particular in stores - e.g. swiping through a POS-menu to find your wallet generates friction).

When following the principles above, a payer-generated QR-code format for MSCTs for data exchange between the payer and the payee could be based on the following preconditions:

¹⁴² An example may be a repayment (transfer back).



1. Make a generic routing/payload data-exchange at POI between the payer and the payee;
2. Routing goes directly or via (a) HUB(s) between MSCT service providers;
3. Avoid having specific details about the payer in the data exchange in order to
 - a. Reduce privacy/security concerns;
 - b. Reduce maintenance concerns related to QR-code distribution;
 - c. Increase readability of the QR-code.

QR-code format:

The QR-code is based on the following format:

- A URL based on https:// structure
- First part of the URL: ordinary domain structure
- Second part of the URL: version
- Third part: type
- Fourth part: routing information
- Fifth part: payload information which is the payer identification data.

<code>HTTPS://<Domain_name>/<Version>/<Type><Payer MSCT_service provider ID>/<Payload></code>

Table 59: Coding of QR-code with payer-presented data

The Domain name refers to a dedicated MSCT interoperability framework (see Chapter 23).



19 MSCT interoperability messages

19.1 Introduction

Through the analysis of the technical interoperability of MSCTs, either based on payee- or on payer-presented data, made in the Chapters 17 and 18 in this document, a number of MSCT interoperability messages have been specified to be supported by the MSCT service providers and the HUB. Note that the messages in the inter-PSP space for SCT Inst and SCT have already been specified in the respective scheme rulebooks (see [21] and [17] respectively) and implementation guidelines (see [22] and [18] respectively).

This chapter provides an overview of these MSCT interoperability messages for which the minimum data sets are defined in Annex 4 to this document.

19.2 Overview MSCT interoperability messages

This section provides an overview of all the MSCT interoperability messages identified in the Chapters 17 and 18 in this document.

Since several errors (e.g. execution errors, failures in notification messages, etc.) may occur during the exchange of messages between the respective MSCT service providers (see also Annex 3), there is also a need to define a so-called “*Inquiry request message*” and an “*Inquiry response message*” between the respective MSCT service providers of the payer and the payee. Also for these messages the minimum data elements are defined in Annex 4.

19.2.1 MSCTs based on payee-presented data

The following messages that need to be supported by the HUB have been identified in this document for MSCTs based on payee-presented data.

Message type	Description
Transaction information request	Message sent by the payer MSCT service to the payee MSCT service provider to request (missing) transaction data.
Transaction information response	Message sent by the payee MSCT service to the payer MSCT service provider to provide (missing) transaction data.
Lock transaction request	Message sent by the payer MSCT service to the payee MSCT service provider to request the locking of a transaction for a given payer.
Lock transaction response	Message sent by the payee MSCT service to the payer MSCT service provider to confirm the locking of a transaction for a given payer.
Notification of reject	<ul style="list-style-type: none"> Notification to the payer about the reject of the MSCT. This involves the payer, the payer MSCT service provider and may involve the payer ASPSP. Notification to the payee about the reject of the MSCT. This involves the payee, the payer MSCT



	service provider, the HUB and the payee MSCT service provider and may involve the payer ASPSP.
Notification of successful / unsuccessful transaction	<ul style="list-style-type: none"> • Notification to the payer about the successful/unsuccessful execution of the MSCT. This involves the payer, the payer ASPSP and the payer MSCT service provider. • Notification to the payee about the successful/unsuccessful execution of the MSCT. This involves the payee, the payer ASPSP, the payer MSCT service provider, the HUB and the payee MSCT service provider.
Inquiry request message	Message exchanged between MSCT service providers to request a special investigation concerning a specific MSCT
Inquiry response message	Message exchanged between MSCT service providers to reply to an inquiry request message concerning a specific MSCT

Table 60: Overview messages for MSCTs based on payee-presented data

Notes: The following messages will not be covered in this document since they are not impacting the interoperability of MSCTs based on payee-presented data.

- MSCT initiation request message from the payer to the payer MSCT service provider and from the payer MSCT service provider to the payer ASPSP;
- Acknowledgement of receipt of the MSCT instruction based on SCT from the payer ASPSP to the payer MSCT service provider and from the payer MSCT service provider to the payer.

However, the data sets of the MSCT initiation request messages should be aligned with the data sets of the initiation messages DS-01 defined in the SCT Inst and SCT scheme rulebooks ([21] and [17]).

19.2.2 MSCTs based on payer-presented data

The following messages that need to be supported by the HUB have been identified in the document for MSCTs based on payer-presented data.

Message type	Description
Payment request message	Message sent by the payee via their MSCT service provider and the HUB to the payer MSCT service provider.
Confirmation of receipt of payment request message (for MSCTs based on SCT)	Confirmation to the payee about the receipt of the payment request message. This involves the payee, the payer MSCT service provider, the HUB, the payee MSCT service provider and the payee.
Notification of reject message	<ul style="list-style-type: none"> • Notification to the payer about the reject of the MSCT. This involves the payer, the payer MSCT service provider and may involve the payer ASPSP,



	<p>the HUB, the payee MSCT service provider and the payee.</p> <ul style="list-style-type: none"> • Notification to the payee about the reject of the MSCT. This involves the payee, the payee MSCT service provider and may involve the HUB, the payer MSCT service provider and the payer ASPSP.
Notification of successful / unsuccessful transaction	<ul style="list-style-type: none"> • Notification to the payer about the successful/unsuccessful execution of the MSCT. This involves the payer, the payer ASPSP, the payer MSCT service provider and may involve the HUB and the payee MSCT service provider. • Notification to the payee about the successful/unsuccessful execution of the MSCT. This involves the payee, the payer ASPSP, the payer MSCT service provider, the HUB and the payee MSCT service provider.
Inquiry request message	Message exchanged between MSCT service providers to request a special investigation concerning a specific MSCT
Inquiry response message	Message exchanged between MSCT service providers to reply to an inquiry request message concerning a specific MSCT

Table 61: Overview messages for MSCTs based on payer-presented data

Note: The MSCT initiation message from the payer MSCT service provider to the payer ASPSP will not be covered in this document since it is not impacting the interoperability of MSCTs based on payer-presented data. However, it should be aligned with the data sets of the instruction message DS-01 defined in the SCT Inst and SCT scheme rulebooks ([21] and [17]).

19.3 Entities involved in MSCT interoperability messages

The table below presents a mapping of the various MSCT interoperability messages defined in this chapter versus the entities involved in sending/receiving these messages. Hereby the abbreviations for the messages are used between the respective entities as they are defined in Annex 4 to this document.



Message type	Entities involved in the exchange of the MSCT interoperability message									
	Payer/ Payer MSCT service provider		Payer MSCT service provider/ Payer ASPSP		Payer MSCT service provider/HUB		Payee MSCT service provider/HUB		Payee/Payee MSCT service provider	
	Payee-presented data	Payer-presented data	Payee-presented data	Payer-presented data	Payee-presented data	Payer-presented data	Payee-presented data	Payer-presented data	Payee-presented data	Payer-presented data
Transaction information request					TIRQ		TIRQ			
Transaction information response					TIRP		TIRP			
Lock Transaction Request					LTRQ		LTRQ			
Lock Transaction Response					LTRP		LTRP			
Payment Request message						PR2		PR2		PR1
Confirmation of receipt payment request message						CRPR1		CRPR1		CRPR2
Notification of reject message	NR1	NR1	NR3	NR3	NR2	NR2	NR2	NR2	NR4	NR4
Notification of successful/ unsuccessful transaction message	NT3	NT3	NT1	NT1	NT2	NT2	NT2	NT2	NT4	NT4
Inquiry request message					IRQ	IRQ	IRQ	IRQ		
Inquiry response message					IRP	IRP	IRP	IRP		

Table 62: Overview MSCT interoperability messages and entities involved



20 New MSCT interoperability models

20.1 Introduction

This section studies models involving a Payment Initiation Service Provider (PISP) or a Collecting PSP (CPSP). Next to a brief description of the most important models identified, a brief analysis is made of how the interoperability requirements that have been specified in this document are impacted.

20.2 Models involving a PISP

PISPs as specified in the PSD2 [5] and the RTS [6] could be involved to facilitate MSCTs.

This section analyses models for MSCTs involving a PISP, impacting the interoperability. Hereby the focus will be on C2B payment contexts and a distinction will be made between MSCTs based on merchant-presented data and MSCTs based on consumer-presented data. Although the MSCT transaction in the figures below is depicted as and SCT Inst, the analyses made below remain valid if the MSCT is based on SCT. Likewise, the analyses also remain valid for other payment contexts, although for P2P payments, a PISP will only be involved on the payer side.

Note that according to Article 94.2 of PSD2, if a PISP is involved between the PSU and their ASPSP, *they shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the PSU.*

20.2.1 MSCTs based on merchant-presented data

Two different cases could be distinguished concerning the involvement of a PISP:

- *Case 1:* The PISP is the consumer MSCT service provider and the consumer has a dedicated MSCT application on their consumer device to initiate the payment after receiving the merchant-presented data from the POI;
- *Case 2:* The PISP is the merchant MSCT service provider. The consumer has no dedicated MSCT application on their device but the merchant-presented data is read by a generic application (e.g. a QR-code reader) on the consumer device and a redirection to a merchant website or merchant app takes place. On this webpage/ merchant app the consumer confirms or selects a PISP and provides their consumer identification data.

Below a brief analysis will be made for both cases and their impact on the technical interoperability requirements. Also, the challenges for these two cases will be identified.



Case 1 – PISP is consumer MSCT service provider

This model is represented in the figure below.

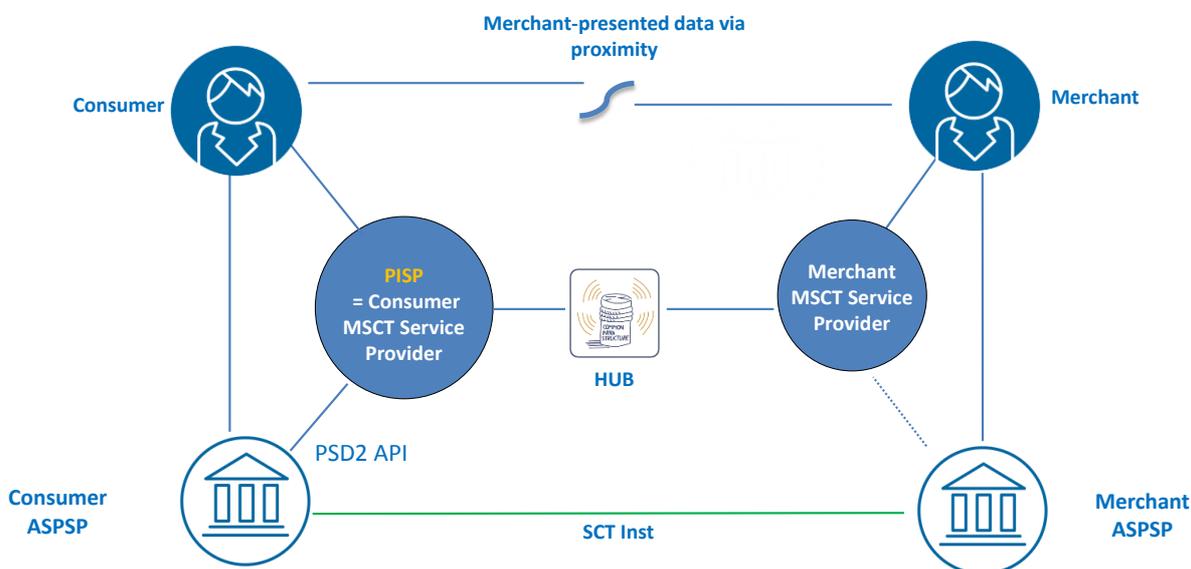


Figure 65: Model for MSCTs based on merchant-presented data whereby PISP is consumer MSCT service provider

In this model, the consumer has on-boarded with the PISP and downloaded an MSCT application on their mobile device, hereby providing the necessary consent with respect to the PISP according to PSD2 (Arts. 51 through 58, 64, 66 and 94) and RTS (Art. 30)¹⁴³. The technical interoperability requirements specified in Chapter 17 apply for the PISP as MSCT service provider of the consumer. Also note that to enable the PISP to use the PSD2 API for the communication with the consumer ASPSP, the consumer should have registered their CustomerID and IBAN during the on-boarding process with the PISP, hereby meeting the appropriate security guidelines (see Chapter 14).

Challenge: Complementing the usage of the PSD2 API, an additional feature (beyond PSD2 and RTS) should be supported, namely the notification from the consumer ASPSP to the PISP (= consumer MSCT service provider) about the successful/unsuccessful transaction or reject in support of the notifications to the consumer and the merchant (see section 17.3).

¹⁴³ Subject to further clarifications to be provided by the EBA on the following four questions: EBA Q&A 2020_5570 to 5573.



Case 2 – PISP is merchant MSCT service provider

This model is represented in the figure below.

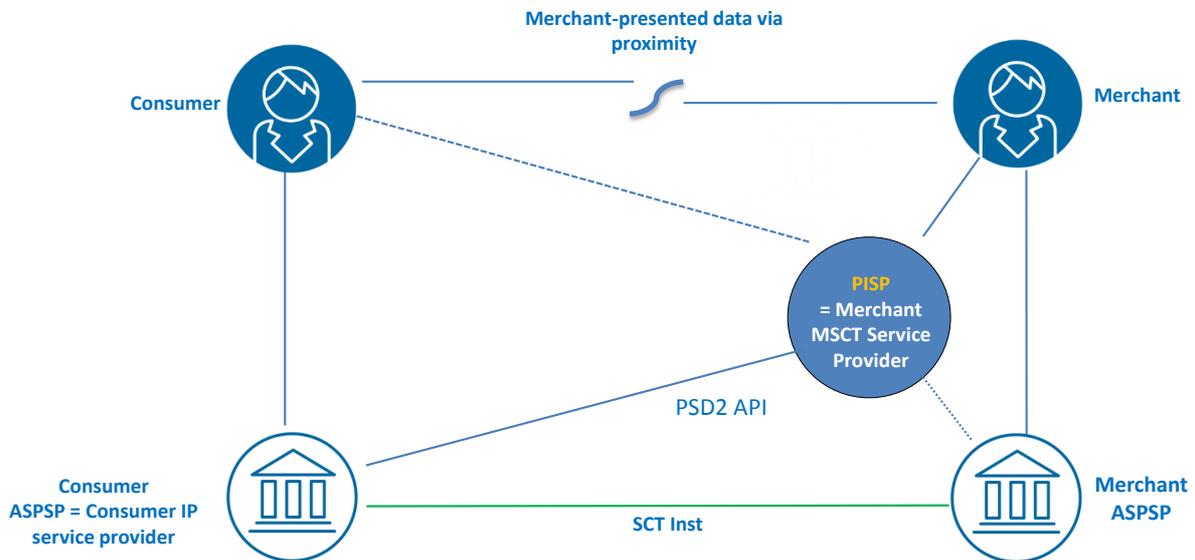


Figure 66: Model for MSCT based on merchant-presented data whereby PISP is merchant MSCT service provider

In this model, it is assumed that the consumer ASPSP is their MSCT service provider while a PISP is involved on the merchant side as the merchant MSCT service provider. The merchant-presented data provided to the consumer at the POI (e.g. via a QR-code read by a “generic QR-code reader” on the consumer device) and re-directs the consumer to a merchant webpage/ merchant application¹⁴⁴. To proceed with the payment, the consumer confirms the PISP or is invited to select a PISP hereby giving the appropriate consent to the PISP for the initiation of the MSCT according to PSD2 (Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30). The consumer should subsequently provide their CustomerID and IBAN to the PISP i-frame to enable the PISP to initiate the MSCT via the PSD2 API¹⁴⁵.

Since the PISP is the MSCT service provider of the merchant, the interoperability requirements described in Chapter 18 apply as the transaction data available to the PISP would be the same as in the case of an MSCT based on consumer-presented data. However, the functional requirements for the HUB as listed in this chapter with respect to the transfer of the Payment Request messages could be covered by the PSD2 API; this model is in fact reduced to a 3-corner model.

¹⁴⁴ Care should be taken concerning the security of the information included in the QR-code for the redirect (e.g. to avoid man-in-the middle attacks).

¹⁴⁵ Alternative methods exist such as enabling the consumer to select their ASPSP and being redirected towards an ASPSP hosted webpage to enter their identification data.



Challenges:

- Complementing the usage of the PSD2 API, an additional feature (beyond PSD2 and RTS) should be supported, namely the notification from the consumer ASPSP (= consumer MSCT service provider) to the PISP (= merchant MSCT service provider) about the successful/unsuccessful transaction or reject in support of the notification to the merchant (see section 18.3).
- Consumer consent with respect to usage of the PISP (= merchant MSCT service provider) subject to EBA clarifications ((PSD2 Arts. 44, 45, 51 through 58, 64, 66 and 94) and RTS (Art. 30))¹⁴⁶.
- Consumer and merchant experience.

20.2.2 MSCTs based on consumer-presented data

Two different main cases could be distinguished concerning the involvement of a PISP:

- *Case 1:* The PISP is the consumer MSCT service provider and the consumer has a dedicated MSCT application on their consumer device. The consumer-presented data includes the identifier to route the Payment Request message via the HUB to the PISP (see Chapter 18).
- *Case 2:* The PISP is the merchant MSCT service provider. Hereby a dedicated agreement will be needed between the merchant and the PISP.

Both cases will now be further analysed below.

Case 1 – PISP is consumer MSCT service provider

This model is represented in the figure below.

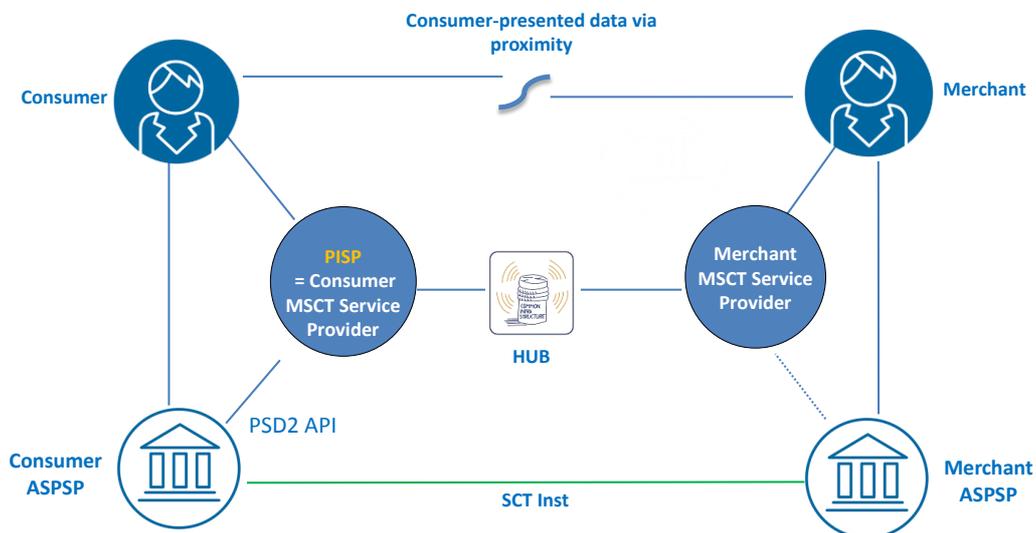


Figure 67: Model for MSCTs based on consumer-presented data whereby PISP is consumer MSCT service provider

¹⁴⁶ Subject to further clarifications to be provided by the EBA on the questions EBA Q&A 2020_5570 and 2020_5573.



In this model, the consumer has on-boarded with the PISP and downloaded an MSCT application on their mobile device, hereby providing the necessary consent with respect to the PISP according to PSD2 (Arts. 51 through 58, 64, 66 and 94) and RTS (Art. 30)¹⁴⁷. The technical interoperability requirements specified in Chapter 18 apply for the PISP as MSCT service provider of the consumer. Also note that to enable the PISP to use the PSD2 API for the communication with the consumer ASPSP, the consumer should have registered their CustomerID and IBAN during the on-boarding process with the PISP, hereby meeting the appropriate security guidelines (see Chapter 14).

Challenge: Complementing the usage of the PSD2 API, an additional feature (beyond PSD2 and RTS) should be supported, namely the notification from the consumer ASPSP to the PISP (= consumer MSCT service provider) about the successful/unsuccessful transaction or reject in support of the notifications to the consumer and the merchant (see section 18.3).

Note: This model remains valid for e- and m- commerce if the consumer data is entered on a merchant webpage / merchant app whereby the consumer selects or confirms the PISP.

Case 2 – PISP is merchant MSCT service provider

Typically, the consumer-presented data is provided by the consumer to the merchant POI and forwarded together with the transaction data (transaction amount, name/IBAN merchant, etc.) to the merchant MSCT service provider = PISP for the initiation of the MSCT. In order to enable the PISP to use the PSD2 API for the communication with the consumer ASPSP, the CustomerID and IBAN of the consumer should be made available “in clear” to the PISP¹⁴⁸.

One of the main challenges however with the involvement of a PISP on the merchant side is how the consumer can give the appropriate consent for the usage of a PISP in accordance with the PSD2 (Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30)¹⁴⁹.

In what follows, two different sub-cases could be distinguished concerning the involvement of a PISP as merchant MSCT service provider:

- *Subcase 2.1:* A PISP involved on the merchant side for e- and m-commerce;
- *Subcase 2.2:* A PISP involved on the merchant side for in-store payments.

Note that for the two subcases above, if the PISP is at the same time also the consumer MSCT service provider, which means that the consumer has on-boarded with this PISP (see also the case 1 in this section), then the model becomes effectively a 3-corner model that will not be further discussed in this document.

Below a brief analysis will be made of each of the two subcases distinguished above and their impact on the technical interoperability requirements. Also, the challenges for these two subcases will be identified.

¹⁴⁷ Subject to further clarifications to be provided by the EBA on the questions EBA Q&A 2020_5570 and 2020_5573.

¹⁴⁸ Subject to further clarifications to be provided by the EBA on the questions EBA Q&A 2020_5476 and 2020_5477.

¹⁴⁹ Subject to further clarifications to be provided by the EBA on the questions EBA Q&A 2020_5570 and 2020_5573.



Subcase 2.1 – PISP on merchant side for e- or m-commerce

This model is represented in the figure below.

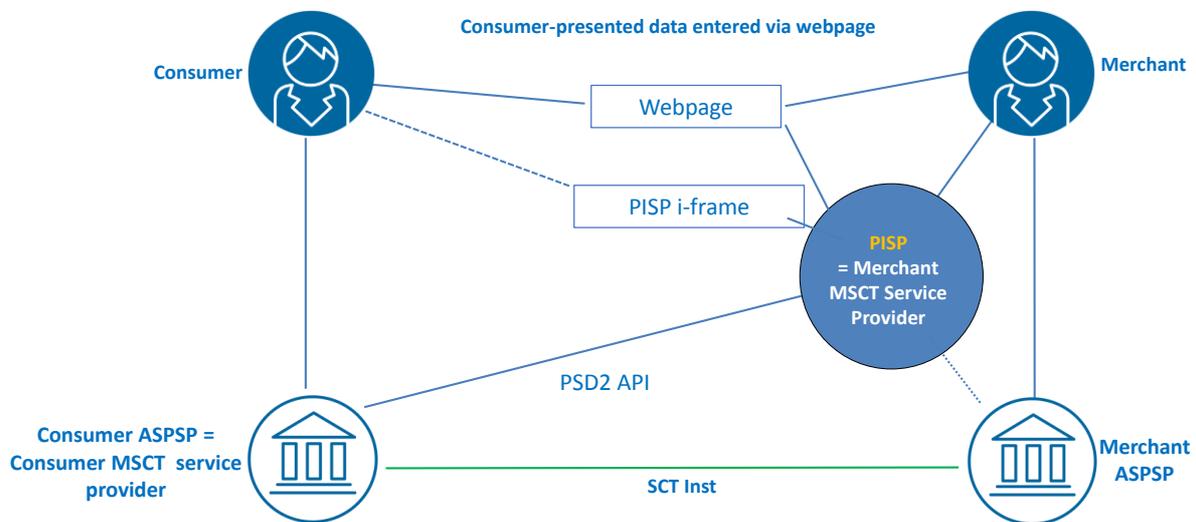


Figure 68: Model for MSCT based on consumer-presented data whereby PISP is merchant MSCT service provider / e- and m-commerce

In this model, it is assumed that the consumer ASPSP is their MSCT service provider while a PISP is involved on the merchant side as the merchant MSCT service provider. To proceed with the payment, the consumer is invited to confirm or select a PISP on the merchant webpage / merchant app, whereby they are able to access the appropriate PISP information. They subsequently give the appropriate request and consent to the PISP for the initiation of the MSCT according to PSD2 (Arts. 44, 45, 64, 66 and 94), by providing their CustomerID and IBAN to the PISP i-frame to enable the PISP the initiation of the MSCT via the PSD2 API to the consumer ASPSP.

Since the PISP is the MSCT service provider of the merchant, the interoperability requirements specified in Chapter 18 apply. However, the functional requirements for the HUB with respect to the transfer of the Payment Request messages could be covered by the PSD2 API; this model is in fact reduced to a 3-corner model.

Challenges:

- Complementing the usage of the PSD2 API, an additional feature (beyond PSD2 and RTS) should be supported, namely the notification from the consumer ASPSP (= consumer MSCT service provider) to the PISP (= merchant MSCT service provider) about the successful/unsuccessful transaction or reject in support of the notification to the merchant (see section 18.3).
- Protection of CustomerID and IBAN subject to EBA clarifications¹⁵⁰.

¹⁵⁰ Subject to further clarifications to be provided by the EBA on the questions EBA Q&A 2020_5476 and 2020_5477.



- Consumer consent with respect to usage of the PISP (= merchant MSCT service provider) subject to EBA clarifications ((Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30))¹⁵¹.

Subcase 2.2 – PISP on merchant side for in-store

This model is represented in the figure below.

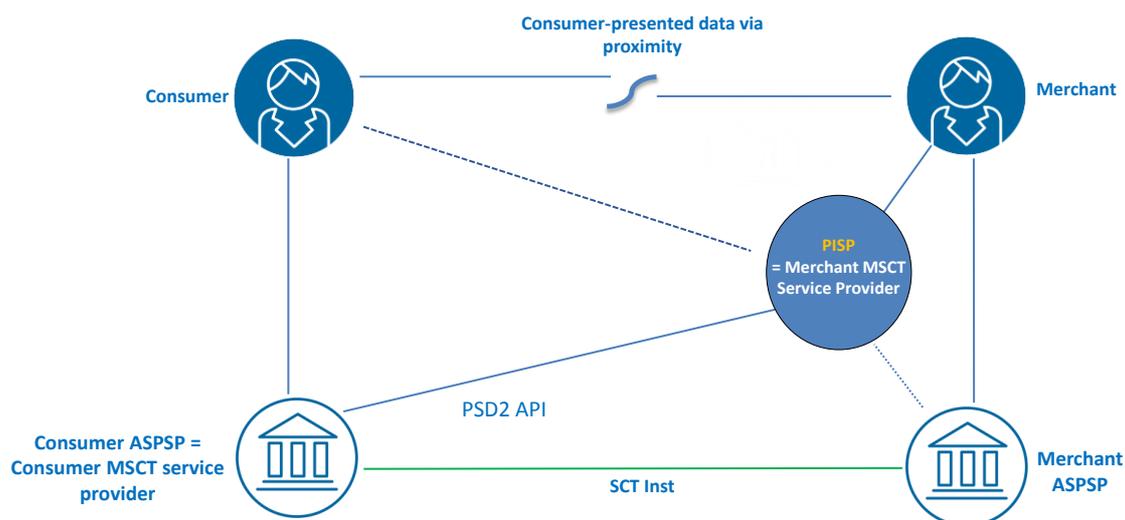


Figure 69: Model for MSCT based on consumer-presented data whereby PISP is merchant MSCT service provider / in-store

In this model, it is assumed that the consumer ASPSP is their MSCT service provider while a PISP is involved on the merchant side as the merchant MSCT service provider. To proceed with the payment, the consumer provides their consumer-presented data to the merchant, e.g. via a QR-code. The consumer should also provide the appropriate consent via the merchant on the usage of a PISP for the initiation of the MSCT according to PSD2 (Arts. 44, 45, 64, 66 and 94). Moreover, it is hereby assumed that the consumer identification data, i.e. CustomerID and IBAN are provided “in clear” to enable the PISP to use the PSD2 API for the communication with the consumer ASPSP.

Since the PISP is the MSCT service provider of the merchant, the interoperability requirements specified in Chapter 18 apply. However, the functional requirements for the HUB with respect to the transfer of the Payment Request messages could be covered by the PSD2 API; this model is in fact reduced to a 3-corner model.

Challenges:

- Complementing the usage of the PSD2 API, an additional feature (beyond PSD2 and RTS) should be supported, namely the notification from the consumer ASPSP (= consumer MSCT service provider) to the PISP (= merchant MSCT service provider)

¹⁵¹ Subject to further clarifications to be provided by the EBA on the questions EBA Q&A 2020_5570 and 2020_5573.



about the successful/unsuccessful transaction or reject in support of the notification to the merchant (see section 18.3).

- Protection of CustomerID and IBAN subject to EBA clarifications¹⁵².
- Consumer consent with respect to usage of the PISP subject to EBA clarifications ((Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30))¹⁵³.

20.3 Models involving a Collecting PSP (CPSP)

This annex analyses models for MSCTs at POI involving a *Collecting Payment Service Provider* (CPSP) on the merchant side which acts as a collector of payment transactions on behalf of the merchant (the ultimate beneficiary) and their impact on the interoperability of MSCTs at the POI. This CPSP has their own ASPSP.

The model is represented in the figure below.

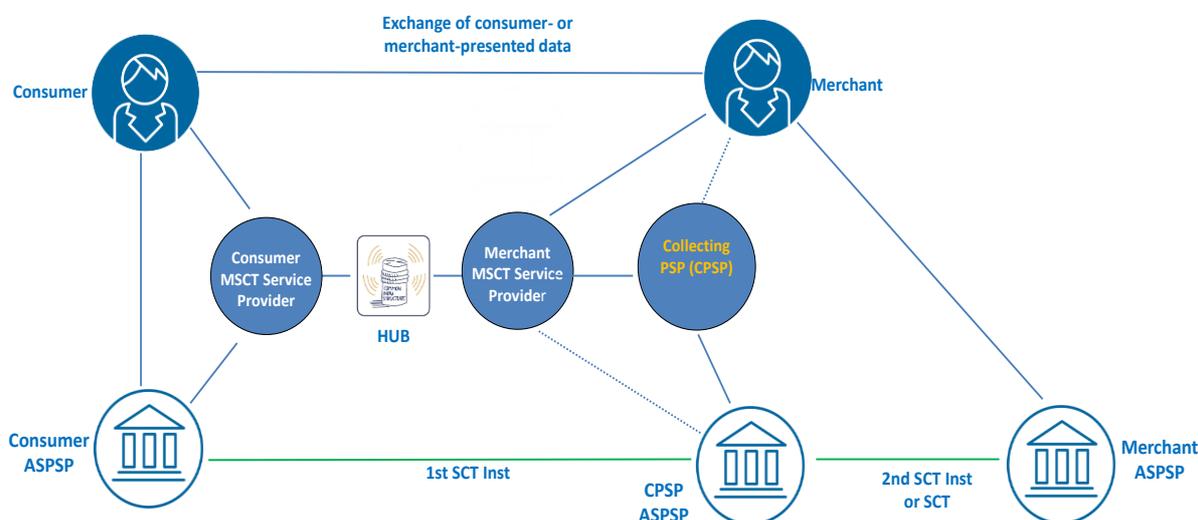


Figure 70: Model involving a CPSP

In this model, the transaction at the POI is an MSCT, typically based on SCT Inst, from the consumer to the CPSP (as the payee), followed by a second payment, either through an SCT Inst or an SCT transaction, from the CPSP (the payer) to the merchant. The merchant needs to have contracts with both the CPSP and their ASPSP. After the first SCT Inst payment, the merchant shall be informed of the execution by the merchant MSCT service provider (via the notification message, see sections 17.3 and 18.3) so that the goods or services can be released.

The payee in this first transaction is the CPSP. Hence the consumer shall be duly informed that the MSCT is conducted to this CPSP, related to the merchant, and not to the actual merchant¹⁵⁴. This will also impact, if performed, the SCA with dynamic linking. Therefore, the

¹⁵² Subject to further clarifications to be provided by the EBA on the questions EBA Q&A 2020_5476 and 2020_5477.

¹⁵³ Subject to further clarifications to be provided by the EBA on the questions EBA Q&A 2020_5570 and 2020_5573.

¹⁵⁴This relates to the work by the ERPB WG on Transparency (see [38]).



notion of “payee reference party” has been introduced in the messages exchanged between the respective MSCT service providers (see Annex 4) to include the merchant next to the payee that is the CPSP.

From a technical interoperability perspective, the interoperability requirements specified in Chapter 17, in case of merchant-presented data, and in Chapter 18, in case of consumer-presented data, apply. The subsequent interactions related to the second (instant) credit transfer transaction from the CPSP to the merchant are to follow the SCT Inst or SCT scheme rulebooks, as relevant.

Furthermore, it is to be noted that different implementation models may exist, e.g., the MSCT service provider on the merchant side could be the CPSP MSCT service provider. The flow of the notification message to the merchant may depend on the actual implementation model and will need to be further analysed in future work.

Also note that often the roles of the merchant MSCT service provide and the CPSP are assumed by a single entity. If this is not the case, there is no technical interface between the CPSP and the merchant but there is a need for an appropriate contract between the two parties.



21 MSCT standards, specifications and white papers

MSCTs require the careful coordination of standards and specifications defined within several disciplines and issued by a heterogeneous group of industry bodies and global organisations.

The most relevant are:

Bluetooth Special Interest Group (SIG)

The Bluetooth Special Interest Group (SIG) is a network of member organisations that are the caretakers and innovators of Bluetooth® technology. The standards organisation oversees the development of Bluetooth standards and the licensing of the Bluetooth technologies and trademarks to manufacturers. The SIG is a not-for-profit, non-stock corporation founded in September 1998 (<https://www.bluetooth.com/>).

ECSG

The European Cards Stakeholders Group is a multi-stakeholder association supporting and promoting European card standardisation with market driven implementation. Its mission is to maintain and evolve the SEPA Cards Standardisation Volume [10] in line with market needs, reflecting the evolution of card payment technology, and to promote Volume conformance throughout the card payments value chain, to enable a more harmonised SEPA card payment ecosystem (www.e-csg.eu).

EMVCo

EMVCo exists to facilitate worldwide interoperability and acceptance of secure payment transactions. It accomplishes this by managing and evolving the EMV® Specifications and related testing processes. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues. Today there are EMV® Specifications based on contact chip, contactless chip, EMV® 2nd Generation, Common Payment Application (CPA), card personalisation, Payment Tokenisation, and 3-D Secure. EMVCo has also specified some documents for QR-code based payments. Relevant EMVCo documents are listed in [11] through [16] (www.emvco.com).

EPC

The European Payments Council (EPC), an international not-for-profit association, representing payment service providers, supports and promotes European payments integration and development, notably the Single Euro Payments Area (SEPA). The EPC is committed to contribute to safe, reliable, efficient, convenient, economically balanced and sustainable payments, which meet the needs of payment service users and support the goals of competitiveness and innovation in an integrated European economy. It pursues this purpose through the development and management of pan-European payment schemes and the formulation of positions and proposals on European payment issues in constant dialogue with other stakeholders and regulators at the European level and taking a strategic and holistic perspective. The primary task of the EPC is to manage the SEPA Credit Transfer and Direct Debit schemes in close dialogue with all stakeholders. The EPC is also active in the fields of cards, mobile payments, including Person-to-Person, e-invoicing-related payments, cash and payment security. Relevant EPC documents are listed in [17] through [30] (www.epc-cep.eu).

**ETSI**

The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies, including fixed, mobile, radio, converged, broadcast and internet technologies. ETSI defines GSM, UMTS telecommunication protocols and the UICC including all the access protocols. ETSI SCP has recently specified the requirements for a “Smart Secure Platform” (see section 11.5). Relevant ETSI documents are listed in [39] through [47] (www.etsi.org).

FIDO Alliance

The FIDO Alliance is an open industry association with a focused mission: authentication standards to help reduce the world’s over-reliance on passwords. The mission of the FIDO alliance includes developing technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users; operating industry certification programs to help ensure successful worldwide adoption of the specifications and submitting mature technical specification(s) to recognised standards development organisation(s) for formal standardisation. Relevant FIDO Alliance documents are listed in [49] through [52] (www.fidoalliance.org).

GlobalPlatform

GlobalPlatform (GP) is an international association focused on establishing and maintaining an interoperable and sustainable infrastructure for smart card deployments. Its technology supports multi-application, multi-actor and multi-service model implementations, which delivers benefits to issuers, service providers and technology suppliers. Relevant GlobalPlatform documents are listed in [53] through [58] (www.globalplatform.org).

GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences (www.gsma.com).

ISO

The International Organization for Standardization (ISO) is a developer and publisher of International Standards. ISO has different committees which specify technical standards used in mobile payments such as standards for integrated circuit cards, QR-codes, communication protocols such as NFC, security mechanisms and is also involved with mobile payments in ISO TC68 SC2 and SC9. More in particular the current work conducted by SC 2 regarding “Customer identification and authentication technologies” and “Code-scanning payment security” is related to the security of MSCTs. Relevant ISO documents are listed in [67] through [73] (www.iso.org).

Mobey Forum

Mobey Forum is a global, financial industry driven forum, whose mission is to facilitate PSPs to offer mobile financial services through insight from pilots, cross-industry collaboration, analysis, experience-sharing, experiments and co-operation and communication with



relevant external stakeholders. Relevant Mobey Forum documents are listed in [75] through [78] (www.mobeyforum.org).

NFC Forum

The Near Field Communication Forum is a non-profit industry association that specifies and certifies the use of NFC short-range wireless interaction. NFC Forum's specifications are used for NFC-chipsets, NFC mobile devices and NFC tags. NFC Forum specifications are based on ISO/IEC 18092 (see [73]) and support interoperability with the relevant specifications for public transport infrastructures. NFC Forum specifications are harmonised with EMVCo specifications and are referenced by GSMA and the Global Certification Forum (GCF) for SE-based NFC. Relevant NFC Forum specifications are listed in [79] to [82] (www.nfcforum.org).

OWASP

The OWASP Foundation was established as a not-for-profit charitable organisation in the United States in 2004, to ensure the ongoing availability and support for the OWASP initiative. OWASP is an open community dedicated to enabling organisations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. OWASP advocates approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas. Relevant OWASP specifications are listed in [88] through [92] (www.owasp.org).

PCI

The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS, see [93]) (www.pcisecuritystandards.org).



22 Challenges and opportunities

By analysing the different MSCT solutions that are currently available in the market, the following challenges in addition to the technical interoperability requirements specified in Chapters 16 to 20 were identified. Here a special focus was given to both consumer and merchant experience. These challenges would need to be sufficiently addressed for a SEPA-wide take-up of MSCTs.

22.1 Challenges

Proximity technologies

In various countries, the proximity solutions described in this document have been introduced by the local MSCT service providers and the retailers to be able to reach their customers. However, because of the lack of standardisation, many different MSCT solutions exist in the market today. This means that consumers who would like to purchase across a range of merchants or cross-border may need to download many different MSCT applications on their mobile device in view of their “closed-loop” implementations.

The usage of these proximity technologies also come for the retailers with a cost for the adaptation of their POI terminal. Here a distinction is to be noted between the adoption of BLE technology at POIs that may require a hardware change versus the adoption of QR-codes which may require only a software update.

BLE is a potential alternative to NFC for electronic payments with mobile devices at the POI. Both transmission methods work bidirectional and have a sufficiently fast transmission rate.

BLE transmissions can be made secure against unauthorised intrusion if they are operated as a connection with multi-level dynamic key allocation. Static key assignment limits security. When the key is transmitted, exactly this part of the communication is particularly at risk, since only the successful exchange of the key protects a BLE connection.

In analogy to NFC technology, the usage of the BLE technology for making proximity payments requires that the Bluetooth functionality on the consumer’s mobile device is switched on, which should be handled by the MSCT app.

Finally, there is a lack of standardisation for the adoption of BLE technology for MSCTs (e.g. common specification for radio range on POI, transaction processing) and “common” customer experience guidelines.

Another challenge may appear when the POI supports multiple proximity technologies. In such an environment, the consumer’s mobile device may perform a transaction over an unintended interface. However, this problem could potentially be avoided by appropriate implementation measures and has been detected in the ERPB report on Instant Payments at the Point of Interaction [33] and by the ECSG in their November 2019 stocktake report to the ERPB¹⁵⁵.

¹⁵⁵ See <https://www.ecb.europa.eu/paym/groups/erpb/html/index.en.html>



There is currently work undertaken by a joint task force between the MSG MSC and the ECSG for the development of standards, business and technical requirements for the consumer selection of preferred payment instrument (card payment or SCT Inst) to conduct a payment transaction at the POI (physical or virtual POI), addressing Recommendation B of the ERPB November 2020 Statement¹⁵⁶. This should contribute to an improved PSU experience at the POI and ensure that the consumer's choice of a given payment instrument to conduct a payment transaction at the POI is respected.

Mobile competitive landscape

Currently it is unclear what will be the prevailing mobile proximity payment technology in the future, which results into difficult decisions with respect to investments to be made. It is precisely the competition between the different technologies that leads to a fragmented market.

However, there is a strong demand for more openness of the (new) solutions which are entering or are on the market today to support competitiveness; examples are an open and free access to the mobile device capabilities (including the NFC antenna, any component being it the SE or HCE).

It has to be noted that numerous mobile offerings are gaining consumer attention, interest and preference. Nevertheless, consumer awareness of mobile device usage for payment services initiation is in some countries still low. In the absence of an MSCT interoperability framework or scheme, the will from MSCT service providers to conquer the consumer preference, leads into a movement towards the use of "closed loop" solutions, which hinders widespread use and pan-European interoperability of MSCT services, leading to market fragmentation and PSU dissatisfaction.

Complexity and security of mobile devices

A mobile device may be considered as a quite complex piece of equipment with many different components, including the baseband, operating system, firmware, software, multiple external interfaces (including the NFC controller), possibly a Trusted Execution Environment (TEE) and one or multiple Secure Elements (SEs). Moreover, the production of these components involves different manufacturers before integration in the mobile device. This means that functional and security standards should be ensured throughout the whole production cycle. Also the presence of different software on the mobile device, developed by diverse vendors or service providers, poses a significant challenge to the integrity of the mobile device ecosystem. The versatility of the mobile devices leaves stakeholders in the ecosystem (including MSCT providers, merchants, other service providers, ...) with major challenges with respect to the development of strategies / road maps with a viable business case and market reach.

¹⁵⁶ See <https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/14th-ERPB-meeting/Statement.pdf?352d20823cd2f48606069c77372be042>.



For MSCT service providers there is a strong dependency on the handset manufacturers and mobile OS providers, which is a highly competitive space with little cooperation on standardisation. Therefore they face a huge complexity with different solutions for each handset and/or mobile OS. This means that they need to develop their applications for a large number of different mobile platforms (combinations of different hardware and software) in view of the current platform incompatibilities. This obviously comes with a cost impact and may in some cases also lead to consumer confusion. The fact that there are multiple solutions on the market which are different - read not compatible - makes it challenging for the supply side. Moreover, once the devices are in usage by the consumer, there are a number of additional challenges which remain to be addressed; security and privacy are the most relevant ones.

Several organisations (see Chapter 21) have already developed specifications and standards for securing the mobile contactless payment environment. Furthermore, they have also created some testing and certification activities in accordance with those standards and specifications.

In this context it is also important to mention the development of the specifications by ETSI of the “Smart Secure Platform” (SSP) that addresses some of the concerns raised above (see Chapter 11). However, availability and market adoption of this new platform is still to be achieved.

Lack of clarity of European rules and regulations

There is still lack of clarity regarding EU rules and regulations such as the PSD2 [5], the RTS [6] and the GDPR [7], also related to their interplay, that might have an impact on the take-up of MSCTs in view of different interpretations with respect to strong customer authentication with dynamic linking and the applicability of the exemptions (see Chapter 8), consumer consent (see Chapters 7 and 20), the involvement of a PISP, or the transfer and processing of sensitive payment data (e.g. related to risk-based authentication - see section 8.5)¹⁵⁷.

PSU on-boarding

The trust in MSCTs, more in particular for cross-border payments, strongly relies on the mutual recognition and trust in PSU on-boarding procedures and mechanisms. Weak customer on-boarding procedures may lead to PSU impersonation and fraudulent transactions. More in particular, related to mobile initiated instant SCTs this is perceived as an important risk to be adequately addressed (see Chapter 14).

Recognition of payee name

It is important for trust and transparency that the commercial brand name of the payee is provided to the payer’s MSCT provider so that it can be properly used in any communication (MSCT app, bank account statements, ...) towards the payer. It might also facilitate every further communication between the payer and the payee.

¹⁵⁷ See EBA Q&A 2020_5365-5367, 5476, 5477, 5570-5573 and 5587.



In this context, the work done by the ERPB WG on Transparency for retail payments end-users should be mentioned [21].

Currency conversion

SCTs have to be denominated in Euros. For retail payments, if the consumer and/ or the merchant are located in non-Euro countries and only their non-Euro account is linked to the MSCT service with their respective ASPSPs, MSCT transactions may be more cumbersome and additional costs may be involved in view of the currency conversion. Transparency to the customer is expected by regulation¹⁵⁸.

22.2 Opportunities

Whilst there are challenges to achieve interoperability for MSCTs as described in Chapter 16 to 20 and above, the introduction of these solutions also offers a number of opportunities to PSUs. More in particular, the immediate availability of funds for MSCTs based on SCT Instant is an attractive feature for the payee. For P2P payments, it is attractive for the payer that they can initiate an MSCT anywhere and anytime. Moreover, the migration of the SCT (instant) schemes to the new version of ISO 20022 payment messages (see [69]), would enable a richer and consistent information exchange between the payee and the payer, and as such provide more transparency to the payer for MSCTs.

For some MSCT payments, the initiation of the payment involves an exchange of data that allows the identification of a known consumer with the merchant's backend system, allowing reconciliation with a merchant's loyalty program or other additional services. The consumer identification can be used for instance to trigger the collection or redemption of loyalty points in combination with the payment transaction. This may provide value added benefits for a retailer and their customer base.

The BLE technology is available on the majority of mobile phones. Almost all iOS and Android devices (as well as emerging platforms) support the technology. BLE also has the potential to eliminate line-ups at the check-out, giving customers the freedom to pay anywhere in-store.

As an example, a beacon could be installed at the entrance of a shop that identifies the consumer. If the consumer scans the goods they purchase using a dedicated MSCT application on their mobile device, the overall transaction amount could be displayed by the mobile device to the consumer once they have finished shopping. They could be subsequently invited on their mobile device to confirm the payment by entering a CDUVM. In addition, BLE beacons and sensors are able to form connections with more than one device at a time.

Depending on market demand, mobile payments based on SCT (Instant) could support more use cases and features, including new ones, subject to appropriate business cases.

¹⁵⁸ See Regulation (EU) 2019/518 of the European Parliament and of the Council of 19 March 2019 amending Regulation (EC) No 924/2009 as regards certain charges on cross-border payments in the Union and currency conversion charges (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2019:091:TOC>)



Last but not least, the take-up of MSCTs would enhance the PSU choice (both for the consumer and the merchant) with respect to payment instruments available for retail payments.



23 Conclusions

This document provides interoperability guidance for MSCTs. It aims to reflect the current state of play and market situation at the time of writing while being brand and implementation model agnostic. On the other hand, it needs to be recognised that the MSCT ecosystem is rapidly evolving with lots of new entrants in the market. Clearly, market adoption will determine the success of each of these new entrants.

The document aims through the description of MSCT use cases to provide an insight into the main issues related to the initiation of (instant) SEPA credit transfers for different payment contexts such as person-to-person, consumer-to-business (retail payments including both in-store and m-commerce payments) and business-to-business payments. Next to the MSCT transaction aspects such as payer authentication, transaction authentication, risk management and payer/payee acknowledgements and notification messages, it focuses on the technology and security used in the customer-to-ASPSP space, since the SCT Inst and SCT transactions as such have already been specified in the respective scheme rulebooks (see [17] and [21]). It furthermore specifies various security guidelines for MSCTs (e.g. MSCT app, CDUVM, etc.). The document analyses in detail the technical interoperability of MSCTs based on payee- or payer-presented data and specifies the technical interoperability requirements between MSCT service providers, for successful, unsuccessful transactions and rejects, which are also depicted in some illustrative process flows. It defines the minimum data to be exchanged between the payer and payee to enable the initiation of an MSCT and specifies for this a payee- and payer-presented QR-code for MSCTs. It further specifies the minimum data sets for all interoperability messages between the respective MSCT service providers of the payer and the payee. New interoperability models involving a PISP or a CPSP have also been addressed. Finally, the document identifies the main interoperability challenges but also opportunities for MSCTs.

Note that subjects such as business cases and revenue models for the MSCT value chain are in the competitive space and therefore are not addressed in this document.

While producing this document, the multi-stakeholder group has noticed a number of “challenges and barriers” that will need to be properly addressed to achieve full interoperability of MSCT transactions (see Chapter 22).

This includes:

- The availability of a technical infrastructure to interconnect the different MSCT service providers notably for the support of token/proxy-based MSCTs and MSCT confirmation and notification messages to PSUs (payers and payees);
- The development of an implementation specification for the MSCT QR-codes specified in this document and the subsequent adoption by the market;
- Next to the technical aspects, also the operating rules, liabilities, adherence to these requirements and governance should be addressed. This could be achieved through the set-up of a dedicated “MSCT interoperability framework or MSCT scheme” to



which the MSCT service providers (existing and new ones) should participate to ensure interoperability of MSCT services;

- A recognition label for MSCTs. Some of the MSG MSCT members are of the opinion that the development of such a recognition label that shows to PSUs at the POI that an MSCT can be used for the payment of goods or services with a merchant, should be further analysed.
- Consumer selection of preferred payment instrument, including addressing the conflicts arising from the usage of multiple proximity technologies at the POI.

Related to the challenges listed above the following should be noted:

- A report on an interoperability framework for instant payments at the POI has been developed by the dedicated ERPB working group (see [35]).
- A joint task force between the MSG MSCT and the ECSG is currently defining the requirements for the consumer selection of preferred payment instrument at the POI based on [36] with the aim to develop a report by November 2021.

Regarding the SEPA Proxy Lookup (SPL) scheme (see section 15.3) that has been developed for the support of MSCTs in P2P payment contexts, it should be noted that today it covers a mobile phone number for the payee but only mandates to return the payee's IBAN for the proxy. However the payee's name might not be known by the payer or by their MSCT app on their mobile device which might pose a problem in view of the dynamic linking for MSCTs as specified by the PSD2 and RTS (see section 8.4). A solution for this problem will need to be further investigated.

Clearly "Request-to-Pay" services could enhance the PSU experience for MSCTs for all payment contexts. The work on the SRTP scheme [28] complements the current document and will further contribute to the customer adoption of MSCTs.

Also the work done in the ERPB WG on SEPA API access scheme [37] complements the current document for MSCTs involving a PISP.

Another challenge for MSCT service providers remains the support of the different mobile platforms. Mobile devices have different operating systems with different execution environments which directly impacts the "secure" communication between different components in the device. Therefore the development of the "Smart Secure Platform" (enabling the provision of value-added services relying on authentication of the user, regardless of the mobile device, communication channel and underlying technology) by ETSI is of utmost importance. The multi-layered functional and security approach taken by ETSI will ensure, subject to sufficient market take-up, more flexibility and portability for mobile payment providers.

There is still a dependency for the consumer on the type of mobile device with respect to the choice of MSCT services. Therefore access to all resources needed on the mobile device, in



order to ensure that the consumer can have a choice amongst payment applications from different mobile payment providers (e.g. the mobile device contactless interface), independently of the mobile device and the operating system used, should be ensured by all handset manufacturers and mobile OS developers (see also [31]).

The impact of the PSD2 [5] with the RTS [6] and the GDPR [7] on payments and more in particular the uncertainty regarding some provisions as well as their interplay when applied to MSCTs might be a barrier for the quick take-up of MSCTs¹⁵⁹ (see Chapters 7, 8 and 20).

By developing this guidance the multi-stakeholder group aimed to contribute to a competitive MSCT market, by providing the different stakeholders an insight into the different service, technical and security aspects involved. The document could serve as a reference basis for making certain implementation choices.

In light of major new trends, and the rapidly changing market, the multi-stakeholder group recommends for the present document to be regularly updated in order to reflect the state of play related to MSCTs and to keep it aligned with the various documents referenced. More in particular, the usage of other proximity technologies than QR-codes for MSCTs, such as NFC and BLE, could be further specified (see Chapter 10.1).

¹⁵⁹ See EBA Q&A 2020_5365-5367, 5476, 5477, 5570-5573 and 5587.



Annex 1: Overview regulatory documents

The following regulatory documents apply in the context of MSCTs (non-exhaustive list):

[1]	Electronic Money Directive (EMD) Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision on the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=en
[2]	Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0847&from=EN
[3]	4 th Anti-Money Laundering Directive (AML4) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC	http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN
[4]	Payment Services Directive (PSD2) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC	http://ec.europa.eu/finance/payments/framework/index_en.htm
[5]	Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (also referred to as ‘RTS’) ¹⁶⁰	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.ENG&toc=OJ:L:2018:069:TOC

¹⁶⁰ See also EBA-Op-2018-04: Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, (<https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf>)



[6]	General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC	http://ec.europa.eu/justice/data-protection/
[7]	PCOM(2017) 489 final - 2017/0226 (COD) Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0489&from=EN
[8]	EBA/GL/2014/12_rev1 Final guidelines on the security of internet payments	https://www.eba.europa.eu/sites/default/documents/files/documents/10180/934179/f27bf266-580a-4ad0-aaec-59ce52286af0/EBA-GL-2014-12%20%28Guidelines%20on%20the%20security%20of%20internet%20payments%29_Rev1.pdf
[9]	EBA/GL/2017/10 Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)	http://www.eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf
[10]	EBA/GL/2017/17 Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)	https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2/-/regulatory-activity/consultation-paper;jsessionid=9E970E4AE798781510FF63999C8067ED
[11]	EBA-Op-2018-04 Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC	https://eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf
[12]	EBA/GL/2018/05	https://www.eba.europa.eu/documents/10180/2281937/Gui



	Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2)	delines+on+fraud+reporting+under+Article+96%286%29%20PSD2+%28EBA-GL-2018-05%29.pdf/5653b876-90c9-476f-9f44-507f5f3e0a1e
[13]	EBA/GL/2018/07 Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)	https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2570450/2f7b1d78-48bd-44fa-bf86-35274e253129/Final%20Report%20on%20Guidelines%20on%20the%20exemption%20to%20the%20fall%20back%20EN.pdf?retry=1
[14]	EBA/GL/2019/04 Guidelines on ICT and security risk management	https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf
[15]	EBA/Op/2019/06 Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2	https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf
[16]	EBA/Op/2020/10 Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC	https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2020/884569/EBA%20Opinion%20on%20obstacles%20under%20Art.%2032%283%29%20RTS%20on%20SCA%20CSC.pdf
[17]	EBA/Op/2021/02 Opinion of the European Banking Authority on supervisory actions to ensure the removal of obstacles to account access under PSD2	https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963372/Opinion%20on%20supervisory%20actions%20for%20removal%20of%20obstacles%20to%20accou



		nt%20access%20under%20PSD 2.pdf
[18]	EDPB: Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 2.0	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services_en
[19]	ESA JC/GL/2017-16/ Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information	https://esas-joint-committee.europa.eu/Publications/Guidelines/Joint%20Guidelines%20to%20prevent%20terrorist%20financing%20and%20money%20laundering%20in%20electronic%20fund%20transfers%20(JC-GL-2017-16).pdf

Table 63: Overview regulatory documents



Annex 2: Additional MSCT use cases

This annex includes the MSCT use cases that have been listed in **Table 5** but were not included in Chapter 7.

A2.1 MSCT use case P2P-3: Mobile device – Mobile banking via browser – Static customer authentication using on-line passcode

This use case presents an example of user experience whereby the payer uses their mobile device to conduct an MSCT (Inst) from their payment account to the payment account of a payee using a mobile browser.

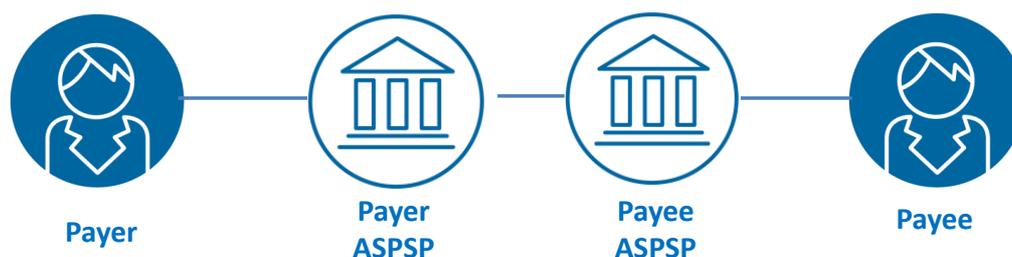


Figure 71: Actors in MSCT use case P2P-3

Payer and payee may, and frequently will, hold their payment accounts with different ASPSPs. Furthermore, it concerns a low value payment whereby a static authentication is applied in view of the exemption of strong customer authentication in accordance with PSD2 (see[5]), involving an online passcode. Further information on the possible application of exemptions for SCA may be found in section 8.3.

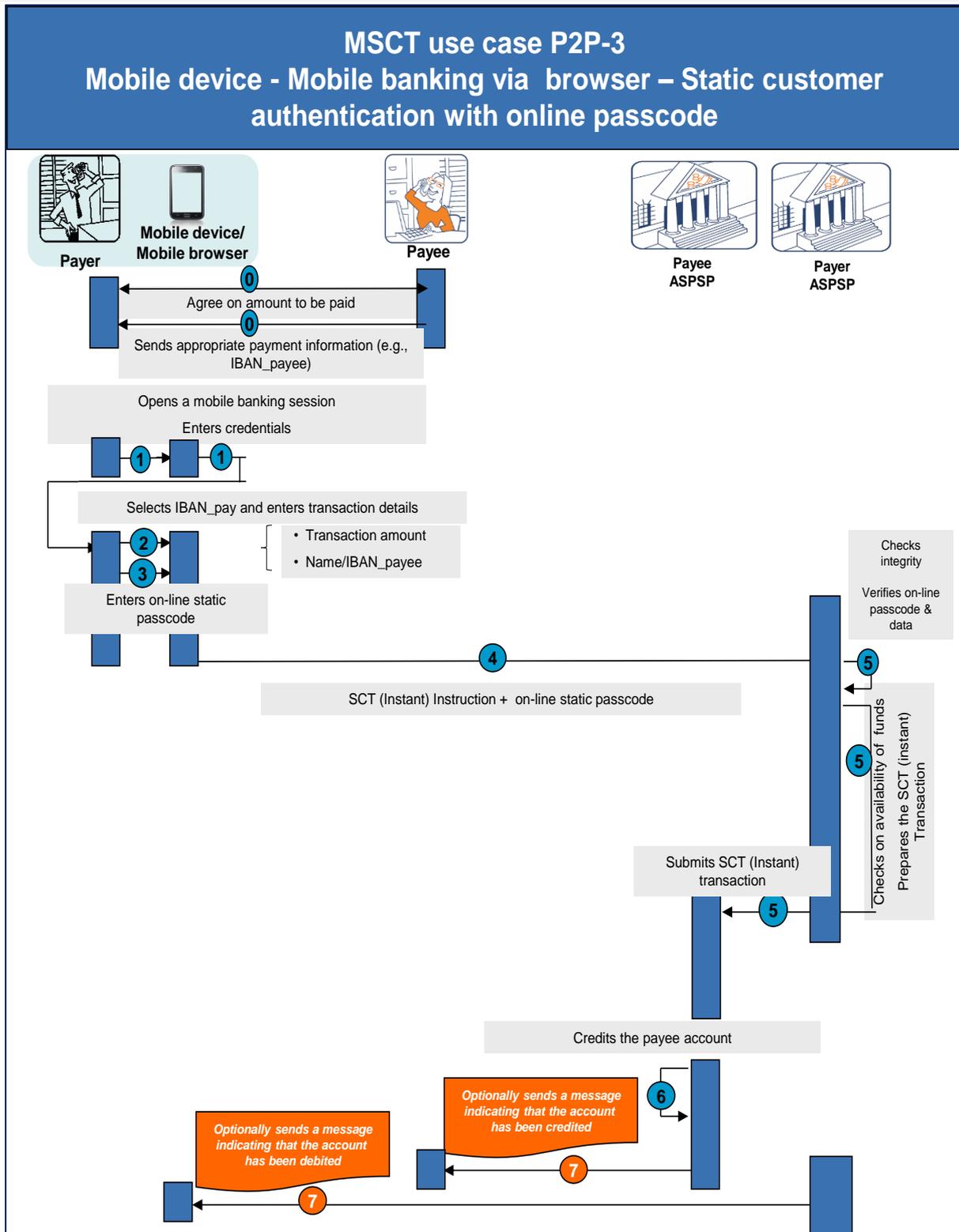


Figure 72: MSCT use case P2P-3



In the figure above, the following steps are illustrated:

Step 0

- The payer and the payee agree upon the amount to be paid to the payee (which is assumed to be low value¹⁶¹). Subsequently, the payee provides all the appropriate payment information to the payer, including their IBAN, as needed.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The payer opens a mobile banking session with their ASPSP in accordance with the security policy of their ASPSP (e.g., by entering a CustomerID and passcode) via a mobile browser on their mobile device
- The payer's credentials are checked by the payer's ASPSP.
- The payer selects the SCT (Inst) service.

Step 2

Next, the payer selects the account (IBAN_payer) they want to use in case they hold several eligible payment accounts and enters the details of the transaction via their mobile device including at least:

- The transaction amount,
- The identification (payee name, IBAN_payee) of the payee's account to be credited; this information can be put in full by the payer or by accessing a pre-registered payee.

and

- Optionally, a value date and remittance data (structured or unstructured).

Step 3

The payer confirms the SCT (Inst) instruction on the webpage via their mobile device.

Step 4

The SCT (Inst) instruction including the payee name, the IBAN_payee, the transaction amount and possibly a value date, is transmitted to the payer's ASPSP.

Step 5

- The payer's ASPSP checks the integrity of the SCT (Inst) instruction and verifies the on-line passcode.
- The payer's ASPSP checks the availability of funds on the payer's account.
- The payer's ASPSP prepares and submits the SCT (Inst) transaction to the payee's ASPSP.

¹⁶¹ Exempted from SCA according to Article 16 of the RTS [6].



Step 6

- In case of an SCT Inst, a confirmation message is returned from the payee’s ASPSP to the payer’s ASPSP (not shown on the figure).
- The payee’s ASPSP makes the funds available to the payee.

Step 7

- The payee is optionally notified by their ASPSP that their account has been credited.
- The payer is optionally notified by their ASPSP that their account has been debited.

Analysis MSCT Use case P2P-3	
Interoperability	<ul style="list-style-type: none"> • The payer and the payee may have different ASPSPs. • Interoperable in view of SCT and SCT Inst rulebooks.
Challenges	<ul style="list-style-type: none"> • The payee needs to provide their IBAN to the payer. • Cumbersome for the payer to enter the IBAN of the payee. • ASPSPs in certain countries or entire communities of ASPSPs may not support a trusted beneficiary list. • In case of an SCT there is no immediate, irrevocable crediting of the funds. • The notification messages in step 7 are not included in the SCT Inst and SCT schemes.

Table 64: Analysis MSCT use case P2P-3

Note: The minimum data elements in the notification messages are defined in Annex 4.



A2.2 MSCT use case P2P-4: Mobile device - Payment with a payee-presented QR-code - SCA using MSCT app involving facial recognition

This use case presents an example of payer experience using their mobile device to pay a payee (e.g. for sharing costs), whereby the details of the payee and the amount to be paid are retrieved from a QR-code scanned from the payee's mobile device.

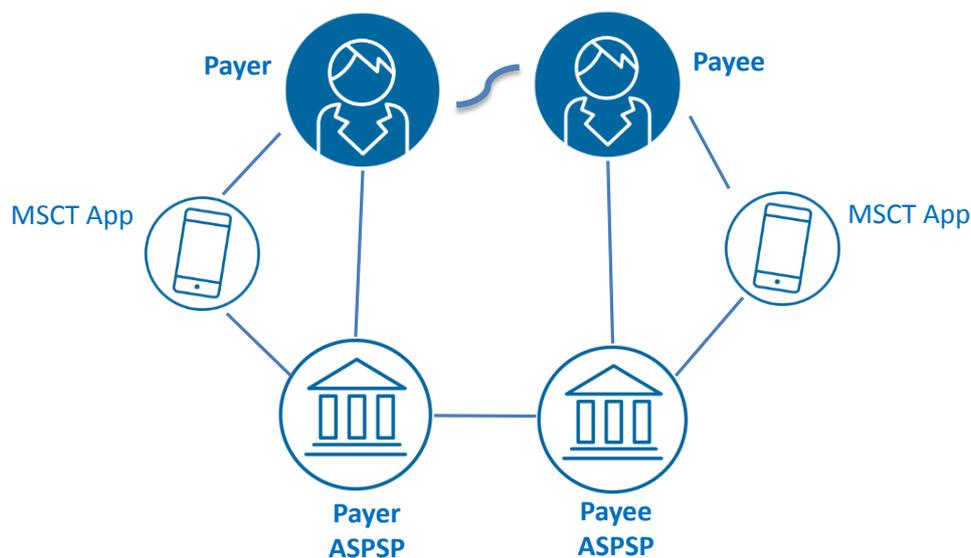


Figure 73: Actors in MSCT use case P2P-4

Payer and payee may, and frequently will, hold their payment accounts with different ASPSPs and have downloaded a dedicated MSCT (Inst) application from their ASPSP¹⁶². A strong payer authentication (see section 8.3) in accordance with PSD2 [5] is performed, involving a facial recognition¹⁶³ of the payer (see section 8.2) and the calculation of an authentication code by the MSCT application using a dedicated key.

¹⁶² The MSCT application may also be downloaded from an MSCT service provider. The payer and payee may have different MSCT service providers.

¹⁶³ Note that other biometric methods may be used, see section 8.2.

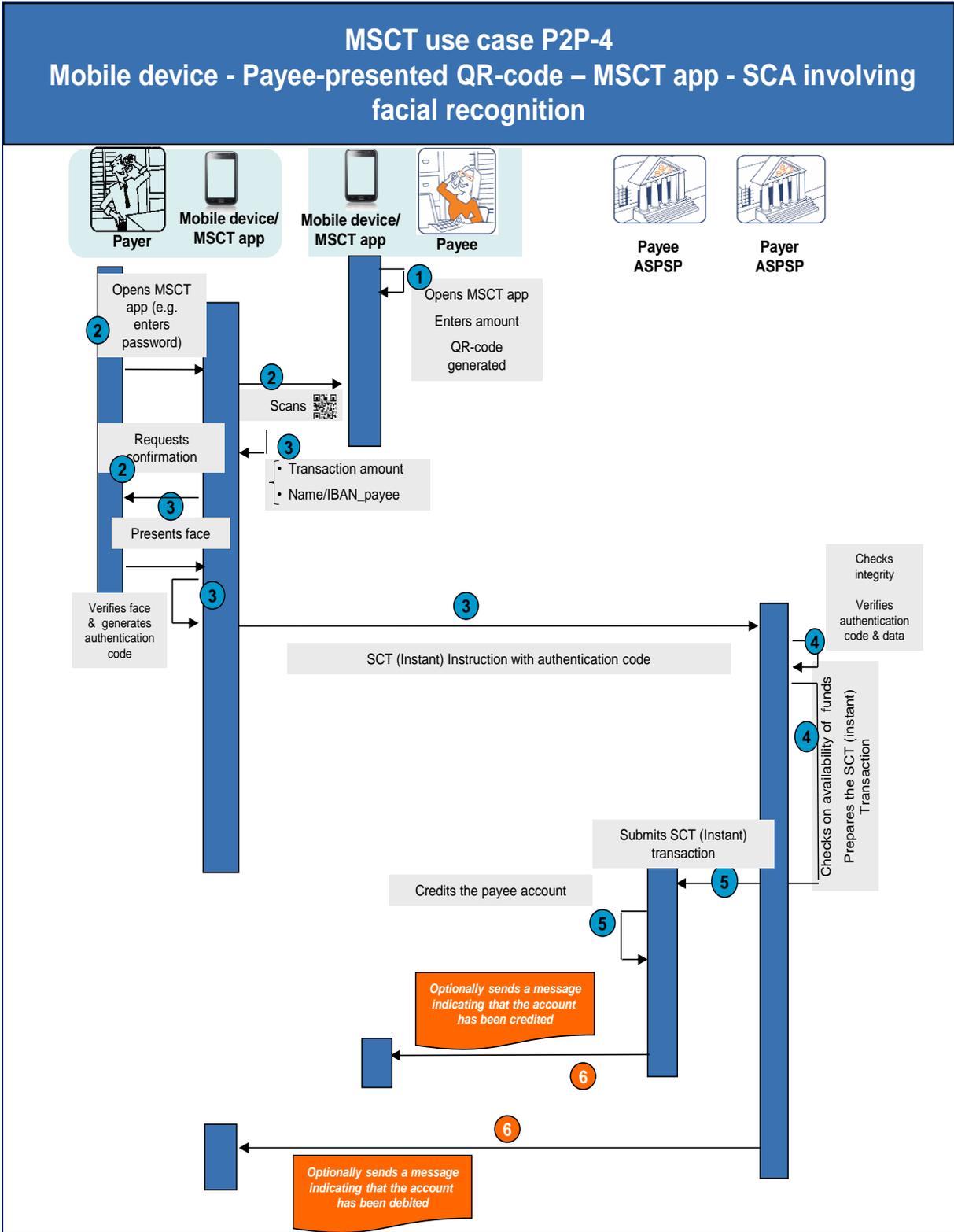


Figure 74: MSCT use case P2P-4



In the figure above, the following steps are illustrated:

Step 0

- The payee needs to be subscribed to the MSCT (Inst) service of their ASPSP and has downloaded an MSCT (Inst) application that is enabled to generate QR- codes.
- The payer needs to be subscribed to the MSCT (Inst) service of their ASPSP and has downloaded an MSCT (Inst) application that is enabled to read QR-codes.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The payee opens their MSCT (Inst) application on their mobile device and enters the amount to be paid.
- The MSCT application on the payee's mobile device generates a QR-code including the payee name, the IBAN_payee, and the amount to be paid.

Step 2

- The payer selects and opens the MSCT (Inst) application on their mobile device, which possibly involves the entry of a password.
- The payer scans the QR-code from the payee's mobile device.
- The MSCT application retrieves the name of the payee, the IBAN_payee, and the amount to be paid from the QR-code which are displayed to the payer.

Step 3

- Next, the payer is invited to present their face to the camera of their mobile device for their authentication and to confirm the payment.
- Upon successful face verification by the mobile device, an authentication code is generated by the MSCT (Inst) application¹⁶⁴ and transmitted with the SCT (Inst) instruction to the payer's ASPSP.

Step 4

- The payer's ASPSP checks the integrity of the SCT (Inst) instruction and verifies the authentication code received.
- The payer's ASPSP checks the availability of funds on the payer's account
- The payer's ASPSP prepares and submits the SCT (Inst) transaction to the payee's ASPSP.

¹⁶⁴ In case the MSCT application is provided to the payer by an MSCT service provider instead of the payer's ASPSP, a delegation for payer authentication from the payer's ASPSP to the MSCT service provider is required. However, this requires an agreement between the payer's ASPSP and the MSCT provider.



Step 5

- In case of an SCT Inst, a confirmation message is returned from the payee’s ASPSP to the payer’s ASPSP (not shown on the figure).
- The payee’s ASPSP makes the funds available to the payee.

Step 6

- The payee is optionally notified by their ASPSP that their account has been credited.
- The payer is optionally notified by their ASPSP that their account has been debited.

Analysis MSCT Use case P2P-4	
Interoperability	<ul style="list-style-type: none"> • The payer and the payee may have different ASPSPs and MSCT (Inst) applications.
Challenges	<ul style="list-style-type: none"> • Standardisation of a “QR-code”, ensuring the correct payee name/IBAN_payee link. • Integrity of the QR-code. • The notification messages in step 6 are not included in the SCT Inst and SCT schemes. • In case of an SCT there is no immediate, irrevocable crediting of the funds. How to inform the payee that the payment has been initiated?

Table 65: Analysis MSCT use case P2P-4

Notes:

- The payee-presented QR-code is specified in Chapter 17.
- The security of QR-codes is addressed in Chapter 10.
- The minimum data sets for the notification messages are defined in Annex 4.
- The acknowledgement of receipt of the MSCT instruction based on SCT is addressed in Chapter 17 and Annex 4.



A2.3 MSCT use case C2B-10: Mobile device – m-commerce – merchant application - PISP with redirection to consumer's ASPSP - SCA involving a dynamic authenticator

This use case presents an example of consumer experience whereby a merchant application on their mobile device is used to purchase goods and subsequently pay with an MSCT Inst. For this case it is assumed that the consumer is redirected to the mobile banking app of their ASPSP.

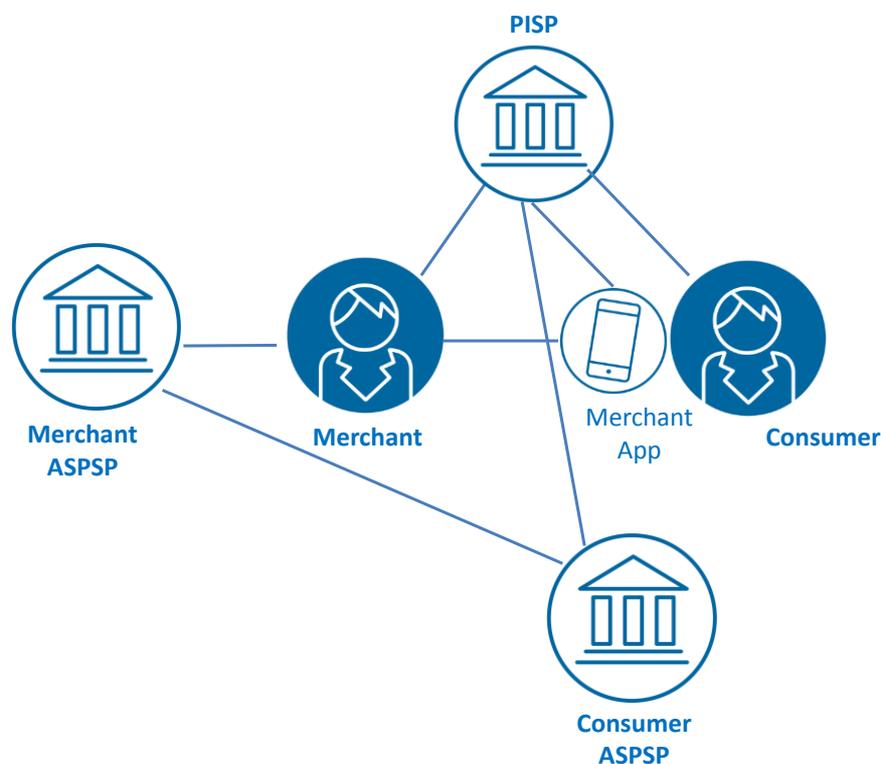


Figure 75: Actors in MSCT use case C2B-10

Consumer and merchant may, and frequently will, hold their payment accounts with different ASPSPs. The consumer have on-boarded with a merchant including their bank account and have downloaded a merchant application on their mobile device. The merchant is pre-registered with a PISP that is linked to the merchant application (this linkage includes both technical and contractual aspects).

Furthermore, the consumer is redirected via the PISP from the merchant application through the PISP to their ASPSP's online banking service where a strong customer authentication (see section 8.3) involving a passcode and dynamic authenticator (e.g. an OTP - see section 8.2) is performed in accordance to PSD2 [5].

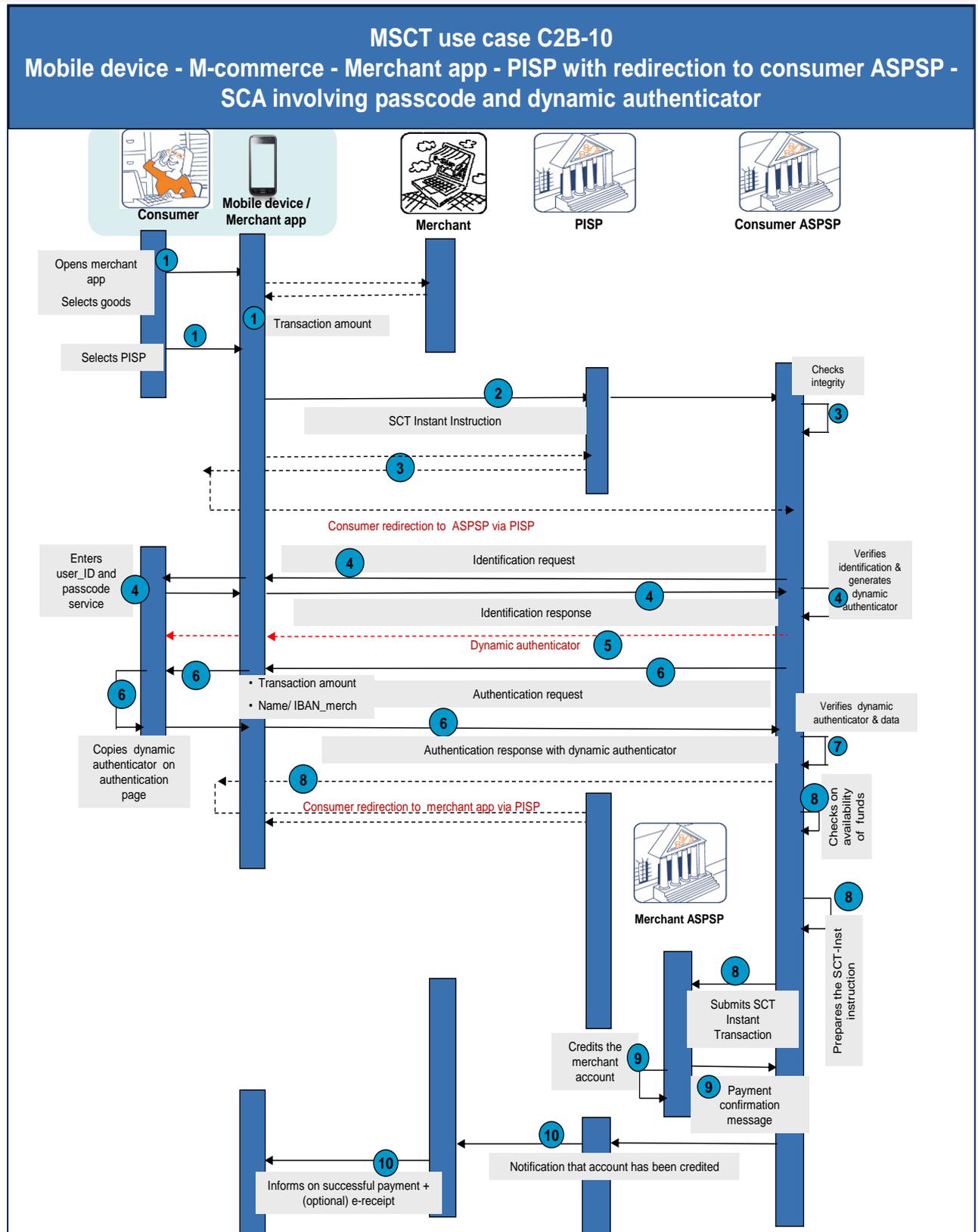


Figure 76: MSCT use case C2B-10



In the figure above, the following steps are illustrated:

Step 0

- The merchant needs to be registered with a PISP with a dedicated payment account.
- The PISP has a communication channel to the consumer's ASPSP.
- The consumer has downloaded a merchant application on their mobile device and has on-boarded with their account details. The consumer has also downloaded a mobile banking app.
- As a prerequisite, a mobile internet connection is required during the purchase.

Step 1

- The consumer selects and opens the merchant application, subsequently navigates and selects the goods or services they want to buy. After having accepted the general purchase conditions, they are invited to confirm the purchase.
- The checkout section of the merchant application displays the transaction details including the transaction amount and the payment options to the consumer.
- The consumer selects their preferred PISP payment solution in this checkout section.

Step 2

An SCT Inst instruction including the transaction amount, the merchant's name, IBAN_merch and merchant transaction identifier are forwarded to the consumer's ASPSP through the PISP.

Step 3

- The consumer's ASPSP checks the integrity of the SCT Inst instruction.
- The consumer is redirected from the merchant application through the PISP to the mobile banking app of their ASPSP.

Step 4

- The consumer is invited to enter their CustomerID and passcode in accordance with the security policy of their ASPSP.
- After successful identification by the ASPSP, the transaction details including the transaction amount and merchant name/IBAN_merch are displayed to the consumer.

Step 5

The consumer's ASPSP transmits a dynamic authenticator (e.g., an OTP linked to the transaction amount and merchant - see section 8.2) to the consumer.

Step 6

The consumer is subsequently requested to enter this dynamic authenticator into a dedicated authentication page to authorise the SCT Inst instruction.

Step 7

The consumer's ASPSP verifies the dynamic authenticator.

.

Step 8



- The consumer is redirected back, based on previously received referral information by their ASPSP, via the PISP to the merchant application.
- The consumer’s ASPSP checks the availability of funds on the consumer’s account.
- The consumer’s ASPSP prepares and submits the SCT Inst transaction to the merchant’s ASPSP.

Step 9

- A confirmation message is returned from the merchant’s ASPSP to the consumer’s ASPSP.
- The merchant’s ASPSP makes the funds available to the merchant.

Step 10

- The merchant is notified by the PISP (information provided by the consumer’s ASPSP) that their account has been credited.
- The consumer is notified by the merchant that the payment has been successfully executed and may optionally receive an e-receipt in their merchant application.

Note: If an SCA is not requested by the ASPSP (see Chapter 8.3) steps 5 through 7 may be omitted.

Analysis MSCT Use case C2B-10	
Interoperability	<ul style="list-style-type: none"> • The merchant needs to have a contractual relationship with the PISP. • Interoperable due to the underlying SCT Inst scheme • Consumer authenticates in “known” on-line banking environment.
Challenges	<ul style="list-style-type: none"> • The PISP needs to connect to # ASPSPs. • In view of the lack of an MSCT application and prior on-boarding, the consumer authentication process is less convenient. • The notification messages in step 10 are not included in the SCT Inst scheme. • Consumer consent with respect to usage of the PISP subject to EBA clarifications ((PSD 2 Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30))¹⁶⁵.

Table 66: Analysis MSCT use case C2B-10

Notes:

- The interoperability of MSCTs involving a PISP is analysed in Chapter 20.
- The minimum data elements in the notification messages are defined in Annex 4.

¹⁶⁵ Subject to clarification by EBA on questions EBA Q&A 2020_5570 and 2020_5573.

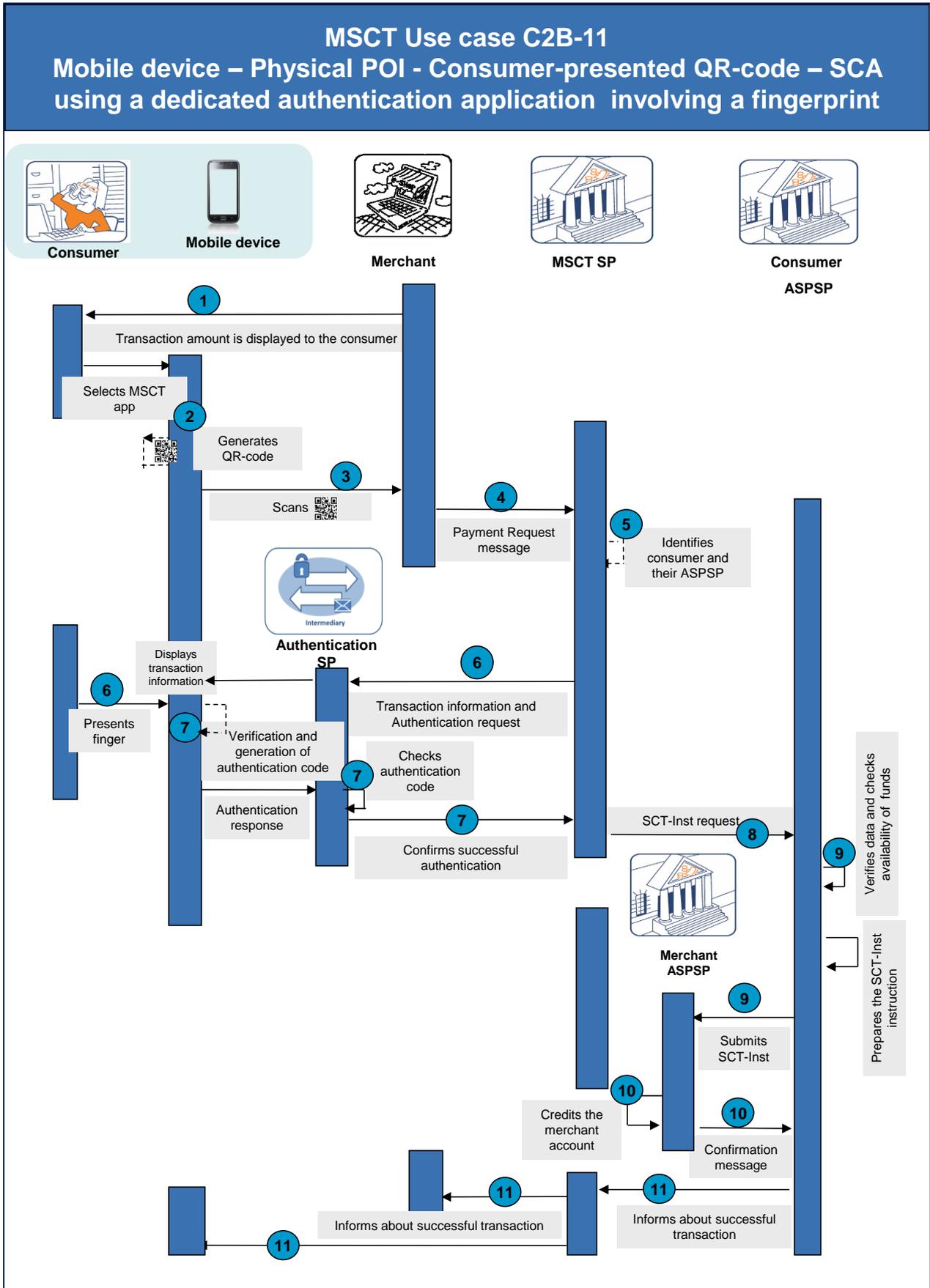


Figure 78: MSCT Use case C2B-11



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, the consumer would need to first subscribe to the MSCT Inst service and download a dedicated MSCT Inst application from the MSCT service provider on their mobile device. Furthermore, they have a separate Authentication application from an Authentication service provider on their mobile device that has been previously linked to the MSCT Inst application.
- The consumer's ASPSP delegates the authentication of the consumer to the Authentication service provider.
- The merchant also needs to be subscribed to the MSCT Inst service, e.g., through their ASPSP or the MSCT service provider directly, has downloaded dedicated software and has the appropriate equipment to scan QR-codes in their POI environment.
- The MSCT service provider is linked to the consumer's ASPSP.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The merchant enters the transaction amount which is displayed on the POI¹⁶⁸.

Step 2

- The consumer selects and opens the MSCT Inst application on their mobile device which possibly involves the entry of a password (or other means of authentication).
- A QR-code containing a token for the consumer is generated by the MSCT Inst application on the mobile device.

Step 3

The consumer presents the QR-code which is scanned by the merchant's POI.

Step 4

The merchant retrieves the consumer's token from the QR-code and sends a payment Request message to their MSCT service provider, including the merchant's name, IBAN_merchant¹⁶⁹, merchant transaction identifier, the transaction amount and the consumer token.

¹⁶⁸ The display of the transaction amount by the POI may happen after step 3, since the customer identification might have an impact on the final transaction amount.

¹⁶⁹ Instead of the IBAN_merchant a proxy may be used.



Step 5

The MSCT service provider identifies the consumer's IBAN and ASPSP from the consumer token.

Step 6

- The MSCT service provider forwards the transaction information to the MSCT Inst app on the consumer's mobile device.
- The consumer is invited to confirm the transaction and is redirected to their Authentication application which displays the merchant name/ IBAN_merchant and the transaction amount.
- The consumer authenticates and confirms the transaction by presenting their finger to the mobile device.

Step 7

- Upon successful fingerprint verification by the mobile device, an authentication code is calculated by the dedicated Authentication application.
- The authentication code is provided to the Authentication service provider for verification.
- Upon successful verification, the MSCT service provider is informed by the Authentication service provider.

Step 8

The SCT Inst instruction including the merchant's name, IBAN_merchant, the transaction amount and the merchant transaction identifier with a flag indicating the successful authentication are transmitted from the MSCT service provider to the consumer's ASPSP.

Step 9

- The consumer's ASPSP checks the integrity of the SCT Inst instruction.
- The consumer's ASPSP checks the availability of funds on the consumer's account.
- The consumer's ASPSP prepares and submits the SCT Inst transaction to the merchant's ASPSP.

Step 10

- A confirmation message is returned from the merchant's ASPSP to the consumer's ASPSP.
- The merchant's ASPSP makes the funds available to the merchant.

Step 11

- The merchant is notified by the MSCT service provider (information provided by the consumer's ASPSP) that their account has been credited.
- The consumer is notified by the MSCT service provider in their MSCT app that the payment has been successfully executed (information provided by the consumer's ASPSP) and may optionally receive an e-receipt.



Note: For virtual POIs, the MSCT use case will be similar except that the consumer token will need to be transferred to the merchant in a different way (e.g., entered manually by the consumer into the merchant’s website or payment page).

Analysis MSCT Use case C2B-11	
Interoperability	<ul style="list-style-type: none"> • The consumer and the merchant are subscribed to the same MSCT service while the consumer’s ASPSP needs be linked to the corresponding MSCT service provider. • For a truly “open” approach and a SEPA-wide interoperability, if the MSCT service provider of the consumer is different to the MSCT service provider of the merchant, a framework will need to be specified that interconnects the different MSCT service providers.
Challenges	<ul style="list-style-type: none"> • Standardisation of messages including data elements between MSCT service provider back-ends. • Standardisation of a “QR-code” and identification of consumers. • Standardisation of the Payment Request messages. • Security of the QR-code/consumer token. • Standardisation of interface between MSCT providers and ASPSPs. • How is the transaction reconciled with the purchase (e.g., transaction identifier)? • The notification messages in step 11 are not included in the SCT Inst scheme.

Table 67: Analysis MSCT Use case C2B-11

Notes:

- The standardisation of the QR-code for payer-presented data is addressed in Chapter 18.
- The security of QR-codes is addressed in Chapter 10.
- The interoperability of MSCTs based on payer-presented data whereby different MSCT service providers are involved for the consumer and merchant is addressed in Chapters 16 and 18.
- The minimum data elements in the payment request and notification messages are defined in Annex 4.



A2.5 MSCT use case C2B-12: Mobile device – Payment at a physical POI with consumer-presented QR-code involving a PISP – SCA using a dedicated authentication application involving a fingerprint

This use case presents an example of consumer experience whereby their mobile device is used to pay in-store by presenting a consumer-presented QR-code to the POI. It is assumed that the QR-code contains the CustomerID and the consumer IBAN in clear text¹⁷⁰. Hereby a dedicated authentication application on the mobile device of the consumer is used that they have downloaded. The consumer authentication is performed through a decoupled¹⁷¹ authentication using a fingerprint code via the dedicated authentication application on the consumer’s mobile device.

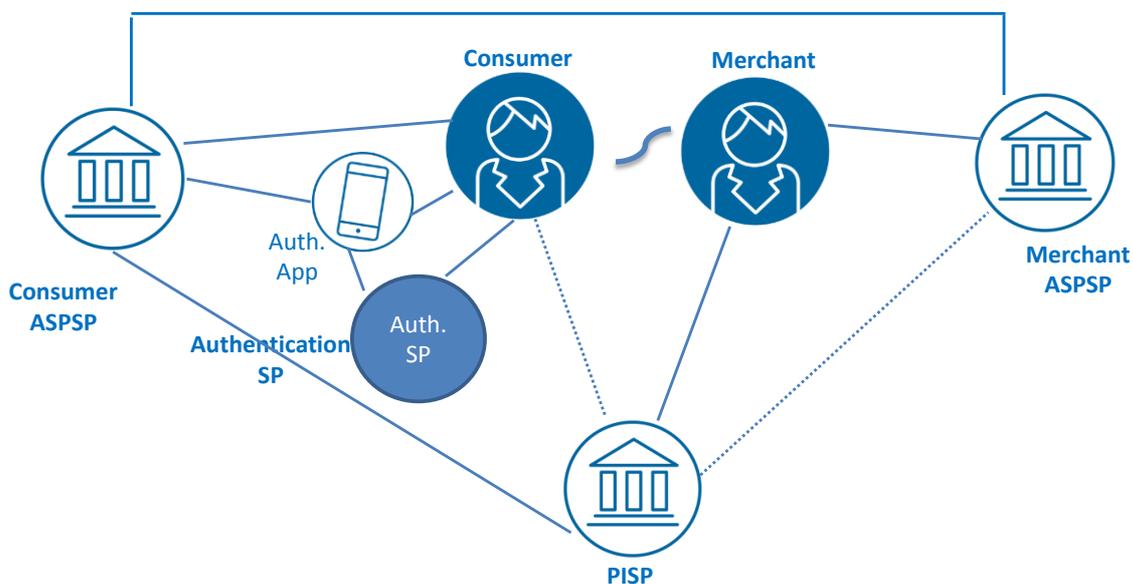


Figure 79: Actors in MSCT Use case C2B-12

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. In this use case the consumer’s ASPSP is their MSCT service provider. The merchant has a contract with a PISP (= merchant MSCT service provider) that supports the PSD2 API, has downloaded dedicated software on their POI and agreed to make the PSD2 Art. 45(2) required PISP information available to the consumer. Moreover, the consumer needs to provide appropriate consent to the usage of the PISP by the merchant.¹⁷²

In this payment transaction a strong customer authentication (see section 8.3) in accordance with the relevant provisions of PSD2 [5] is performed involving a fingerprint (see section 8.2) and the calculation of an authentication code by a authentication application using a dedicated key

For a virtual POI, this MSCT use case would be similar except that the CustomerID and IBAN will need to be transferred to the PISP in a different way (e.g., entered manually by the consumer into the PISP’s i-frame after selection/confirmation of the PISP on the merchant’s website or payment page).

¹⁷⁰ Subject to clarification by EBA on questions EBA Q&A 2020_5476 and 2020_5477.

¹⁷¹ Decoupled from the device used to make the transaction (the POI). See section 15.2 in the MSCT IG.

¹⁷² Subject to clarification by EBA on questions EBA Q&A 2020_5570 and 2020_5573.

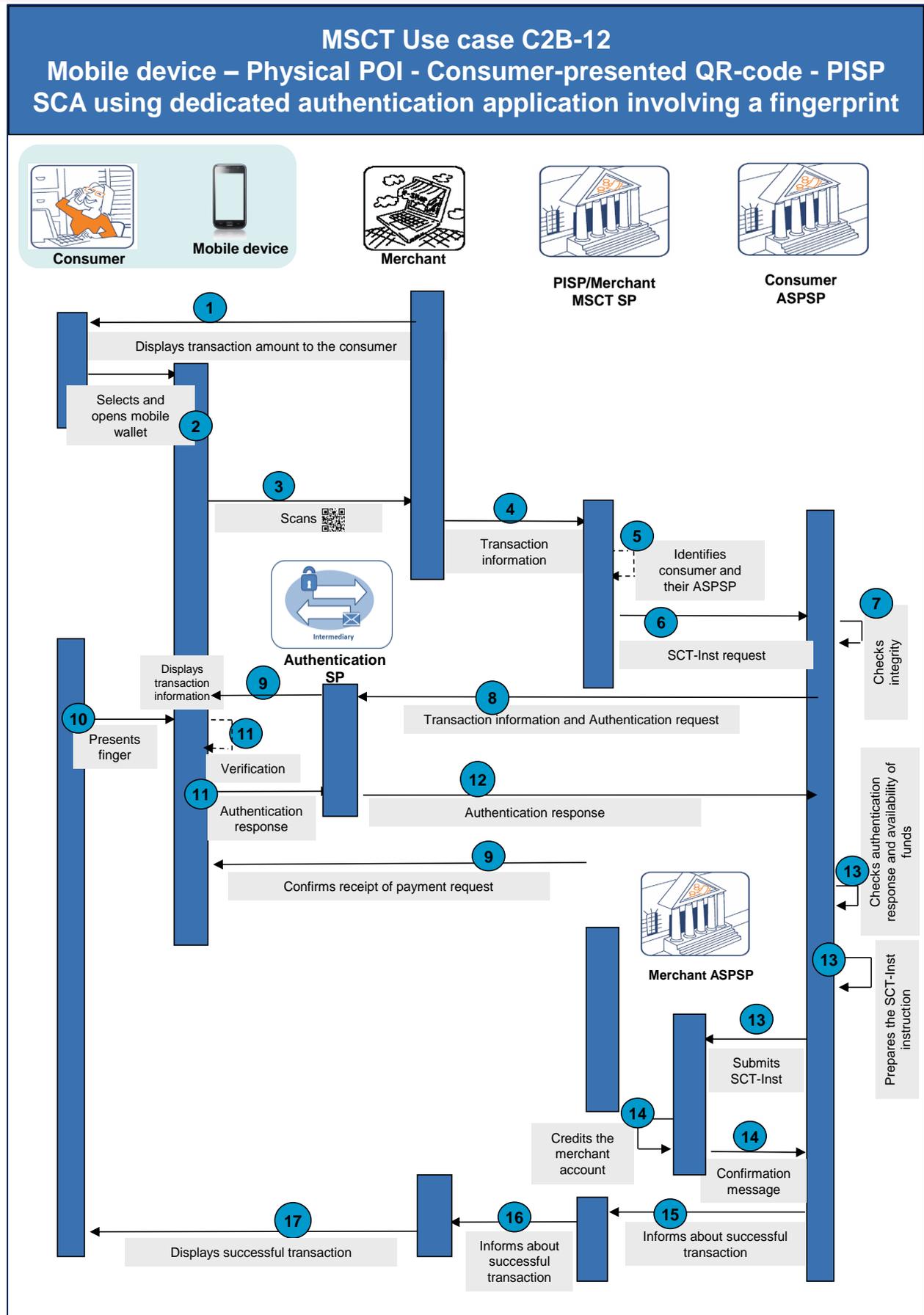


Figure 80: MSCT Use case C2B-12



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, consumers would need to download a dedicated authentication app of an Authentication Service Provider. This Authentication Service Provider needs to have an appropriate agreement with the consumer's ASPSP that covers the liabilities, delegation for authentication, on-boarding of consumer and their device (with linkage to the consumer account) and certification of the authentication app.
- The consumer creates a static QR code containing their IBAN and CustomerID (issued by the consumer's ASPSP) in an open standardised (reversible) format. This QR code can be printed on a sticker or stored in a mobile wallet (in analogy to a mobile boarding pass).
- The merchant is subscribed to the PISP and installed their software on the POI.
- The PISP is enabled to use the consumer ASPSP's PSD2 Access to the Account interface (PSD2 API).
- During the payment transaction, a mobile internet connection of the consumer device is required for the customer authentication.

Step 1

The merchant enters the transaction amount which is displayed on the POI¹⁷³.

Step 2

The consumer selects and opens their mobile wallet containing the QR code.

Step 3

The consumer presents their QR code, which is scanned by the merchant's POI.

Step 4

The merchant's POI software retrieves the CustomerID and IBAN from the QR-code and provides the transaction details, including the merchant's name, IBAN_merchant, merchant transaction identifier, the transaction amount, the CustomerID and IBAN to the PISP.

Step 5

The PISP identifies the consumer's ASPSP BIC from the consumer's IBAN and their PSD2 access point.

Step 6

The PISP accesses the consumer's ASPSP PSD2 interface and initiates an SCT Inst transaction by providing the transaction data including the CustomerID and IBAN, the merchant's name/IBAN, the transaction amount and the merchant transaction identifier.

Step 7

The consumer's ASPSP checks the integrity of the SCT Inst instruction.

¹⁷³ The display of the transaction amount by the POI may happen after step 3, since the customer identification might have an impact on the final transaction amount.



Step 8

The consumer's ASPSP forwards the transaction information to the Authentication Service Provider and requests a decoupled SCA.

Step 9

- The Authentication Service Provider forwards the transaction information to their dedicated authentication application on the consumer's mobile device.
- The authentication application pops-up a window with the transaction details including the merchant name/IBAN_merch and transaction amount and requests an authentication.

Step 10

The consumer authenticates and confirms the transaction by presenting a finger¹⁷⁴ to the mobile device.

Step 11

The authentication application verifies the fingerprint and provides upon successful verification the authentication response to the Authentication Service Provider.

Step 12

The Authentication Service Provider provides the authentication response to the consumer's ASPSP.

Step 13

- The consumer's ASPSP checks the authentication response.
- The consumer's ASPSP checks the availability of funds on the payer's account.
- The consumer ASPSP prepares and submits the SCT Inst transaction to the merchant ASPSP.

Step 14

1. A confirmation message is returned from the merchant's ASPSP to the consumer's ASPSP.
2. The merchant's ASPSP makes the funds available to the merchant.

Step 15

The consumer's ASPSP sends a notification message to the PISP about the execution of the SCT Inst transaction.

Step 16

The PISP (= merchant MSCT service provider) sends a notification message to the merchant about the successful transaction.

¹⁷⁴ Note that other authentication means may be used, see chapter 8 in the MSCT IG.



Step 17

The merchant POI displays to the consumer that the transaction has been successfully executed.

Analysis MSCT Use case C2B-12	
Interoperability	Based on and governed by PSD2.
Challenges	<ul style="list-style-type: none"> • Standardisation of the QR-code and identification of consumers. • Security of the QR code. • Protection of CustomerID and IBAN¹⁷⁵. • Consumer consent with respect to usage of the PISP subject to EBA clarifications ((PSD 2 Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30))¹⁷⁶. • The PSD2 API needs to support the functionalities required (e.g. decoupled SCA, notification message, etc.). • Requires a contract between the merchant and the PISP. • The notification messages in steps 15 and 16 are not included in the SCT Inst scheme.

Table 68: Analysis MSCT Use case C2B-12

Notes:

- The standardisation of the QR-code for consumer-presented data is addressed in Chapter 18.
- The interoperability models for MSCTs involving a PISP are analysed in section 3 of this document.
- The security of QR-codes is addressed in Chapter 10.
- The minimum data elements in the notification messages are specified in Annex 4.

¹⁷⁵ Subject to clarification by EBA on questions EBA Q&A 2020_5476 and 2020_5477.

¹⁷⁶ Subject to clarification by EBA on questions EBA Q&A 2020_5570 and 2020_5573.



A2.6 MSCT use case C2B-13: Smartwatch – Payment at a physical POI with consumer-presented QR-code involving a PISP – SCA using an embedded authentication via the POI involving an OTP and PIN

This use case presents an example of consumer experience whereby their smartwatch is used to pay in-store by presenting a consumer-presented QR-code to the POI. It is assumed that the QR-code contains the CustomerID and the consumer IBAN in clear text¹⁷⁷. The consumer authentication is performed through an embedded authentication¹⁷⁸ using a PIN and one-time password (OTP) entered on the POI.

The merchant is connected to a PISP (= merchant MSCT service provider) that supports the PSD2 interface of the consumer’s ASPSP (= consumer MSCT service provider).

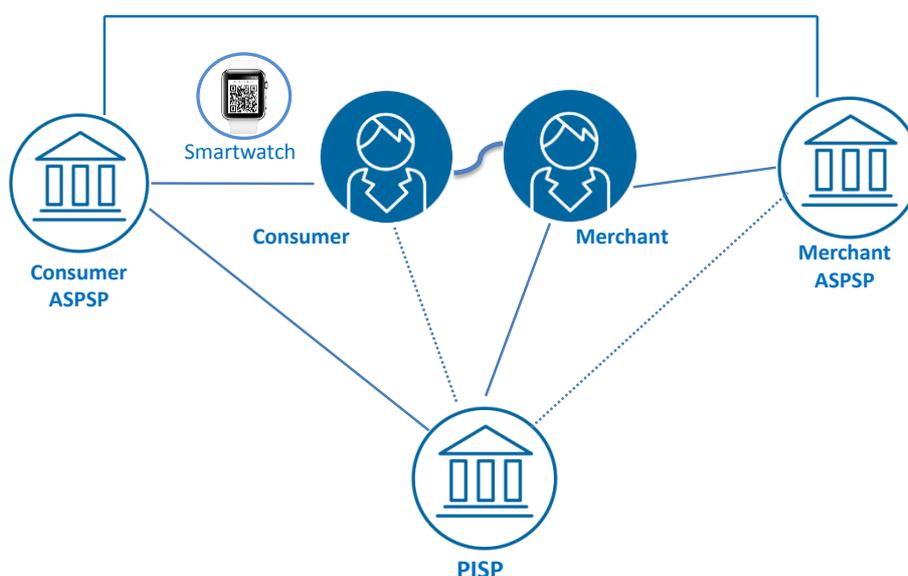


Figure 81: Actors in MSCT Use case C2B-13

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs.

The merchant has a contract with a PISP that supports the PSD2 API, has downloaded dedicated software on their POI and agreed to make the PSD2 Art. 45(2) required PISP information available to the consumer. Moreover, the consumer needs to provide appropriate consent to the usage of the PISP by the merchant.¹⁷⁹

In this payment transaction a strong customer authentication (see section 8.3) in accordance with PSD2 [5] is performed involving a PIN and OTP (see section 8.2).

Note that compliance with the EBA Opinion paper¹⁸⁰ may be dependent on the actual implementation.

¹⁷⁷ Subject to clarification by EBA on questions EBA Q&A 2020_5476 and 2020_5477.

¹⁷⁸ See section 15.2 in the MSCT IG.

¹⁷⁹ Subject to clarification by EBA on questions EBA Q&A 2020_5570 and 2020_5573.

¹⁸⁰ See EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ([see https://www.eba.europa.eu/file/104475/](https://www.eba.europa.eu/file/104475/)).



For a virtual POI, this MSCT use case would be similar except that the CustomerID and IBAN will need to be transferred to the PISP in a different way (e.g., entered manually by the consumer into the PISP's i-frame after selection/confirmation of the PISP on the merchant's website or payment page).

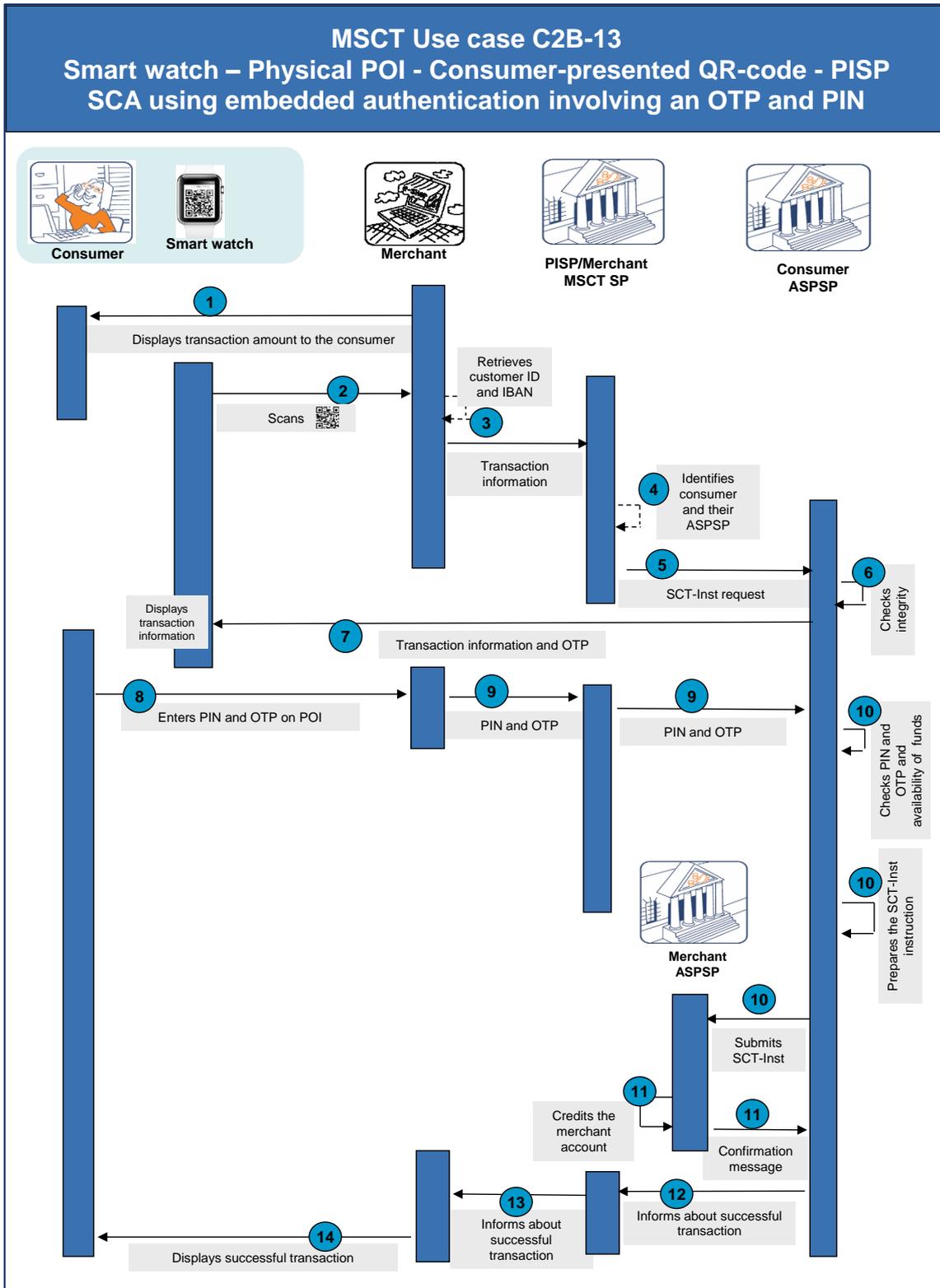


Figure 82: MSCT Use case C2B-13



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, consumers would need to be subscribed to a “classic” ASPSP SCA method using a PIN knowledge factor and a possession factor of a device, i.e. the smartwatch in this case, which were securely bound to their account.
- The consumer creates a static QR code containing their IBAN and CustomerID in an open standardised (reversible) format. This QR code is stored on a smartwatch (in analogy to a mobile boarding pass).
- The merchant is subscribed to the PISP and installed their software on the POI.
- The PISP is enabled to use the consumer ASPSP’s PSD2 Access to the Account interface (PSD2 API).
- Depending on the OTP creation method, a mobile SMS connection with the consumer may or may not be required during the payment transaction.

Step 1

The merchant enters the transaction amount which is displayed on the POI.

Step 2

The consumer presents their QR code, which is scanned by the merchant.

Step 3

The merchant’s POI software retrieves the CustomerID and IBAN from the QR-code and provides the transaction details, including the merchant's name, IBAN_merchant, merchant transaction identifier, the transaction amount, the CustomerID and IBAN to the PISP.

Step 4

The PISP identifies the consumer’s ASPSP BIC from the consumer’s IBAN and their PSD2 access point.

Step 5

The PISP accesses the consumer’s ASPSP PSD2 interface and initiates an SCT Inst transaction by providing the transaction data including the CustomerID and IBAN, the merchant’s name/ IBAN, the transaction amount and the merchant transaction identifier.

Step 6

The consumer’s ASPSP checks the integrity of the SCT Inst instruction.

Step 7

The consumer’s ASPSP provides the transaction information (e.g. via SMS) and a one-time password (OTP) to the registered consumer’s device, i.e. the smartwatch.

Step 8

The consumer reviews and confirms the transaction by entering their PIN and the OTP onto the merchant’s POI terminal.



Step 9

The PISP reads and securely transmits the PIN and OTP to the consumer ASPSP's server via their PSD2 API (embedded authentication).

Step 10

- The consumer's ASPSP checks the PIN and OTP.
- The consumer's ASPSP checks the availability of funds on the payer's account.
- The consumer ASPSP prepares and submits the SCT Inst transaction to the merchant ASPSP.

Step 11

3. A confirmation message is returned from the merchant's ASPSP to the consumer's ASPSP.

4. The merchant's ASPSP makes the funds available to the merchant.

Step 12

The consumer's ASPSP sends a notification message to the PISP about the execution of the SCT Inst transaction.

Step 13

The PISP (= merchant MSCT service provider) sends a notification message to the merchant about the successful transaction.

Step 14

The merchant POI displays to the consumer that the transaction has been successfully executed.

Analysis MSCT Use case C2B-13	
Interoperability	5. Based on and governed by PSD2
Challenges	<ul style="list-style-type: none"> • Standardisation of the QR-code and identification of consumers • Security of the QR code. • Protection of CustomerID and IBAN¹⁸¹. • Consumer consent with respect to usage of the PISP subject to EBA clarifications ((PSD 2 Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30))¹⁸². • Communication of OTP to smart watch. • The PSD2 API needs to support the functionalities required (e.g. embedded SCA, notification message, etc.) • Requires a contract between the Merchant and the PISP. • Requires the merchant's POS terminal to enable the entry of a numeric PIN+OTP code and to implement appropriate security measures

¹⁸¹ Subject to clarification by EBA on questions EBA Q&A 2020_5476 and 2020_5477.

¹⁸² Subject to clarification by EBA on questions EBA Q&A 2020_5570 and 2020_5573.



	<ul style="list-style-type: none">• The notification messages in steps 12 and 13 are not included in the SCT Inst scheme• Customer experience
--	--

Table 69: Analysis MSCT Use case C2B-13

Notes:

- The standardisation of the QR-code for consumer-presented data is addressed in Chapter 18.
- The interoperability models for MSCTs involving a PISP are analysed in Chapter 20.
- The security of QR-codes is addressed in Chapter 10.
- The minimum data elements in the notification messages are specified in Annex 4.



A2.7 MSCT use case C2B-14: Mobile device - Off-line use case – Payment at a physical POI with consumer-presented QR-code – SCA involving facial recognition

This use case presents an example of consumer experience whereby their mobile device is used to pay in-store by presenting a consumer-presented QR-code¹⁸³ to the POI. This example covers an offline-use case whereby the consumer’s mobile device has generally online capability but has no connectivity at the time of transaction. Hereby a dedicated MSCT Inst application on the mobile device of the consumer is used that they have downloaded from an MSCT service provider into their mobile wallet.

The consumer authentication is performed offline through the MSCT application in the consumer’s mobile wallet.

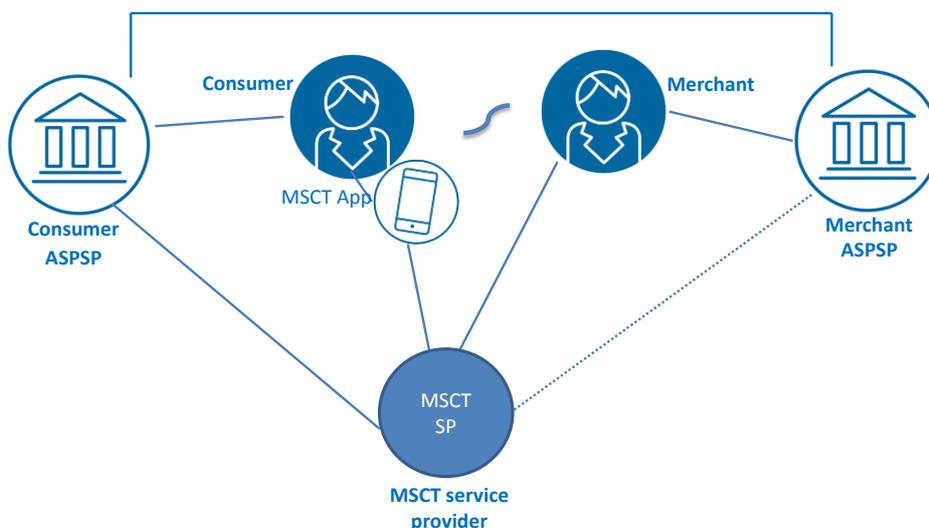


Figure 83: Actors in MSCT Use case C2B-14

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. Both ASPSPs are participants in the same MSCT Inst service¹⁸⁴.

Also, the merchant needs to be subscribed to the MSCT Inst service and have downloaded dedicated software on their POI.

In this payment transaction a strong customer authentication (see section 8.3) in accordance with PSD2 [5] is performed involving a token/unique ID and facial recognition (see section 8.2). Note that hereby delegation for the consumer authentication needs to be given to the MSCT service provider by the payer’s ASPSP.

The tokens used in this example in the QR-codes are valid only once (dynamic tokens). Based on risk considerations, the offline usability of those may be restricted.

Note that although in the description of this use case, an optical token is used, the use case remains valid for other proximity technologies such as NFC or BLE.

¹⁸³ This use case remains valid for any other optical format used to present the consumer data (e.g., barcode).

¹⁸⁴ This refers to the current MSCT solutions in the market.



MSCT Use case C2B-14
Mobile device – Physical POI - Off-line use case – Consumer-presented QR-code - SCA involving facial recognition

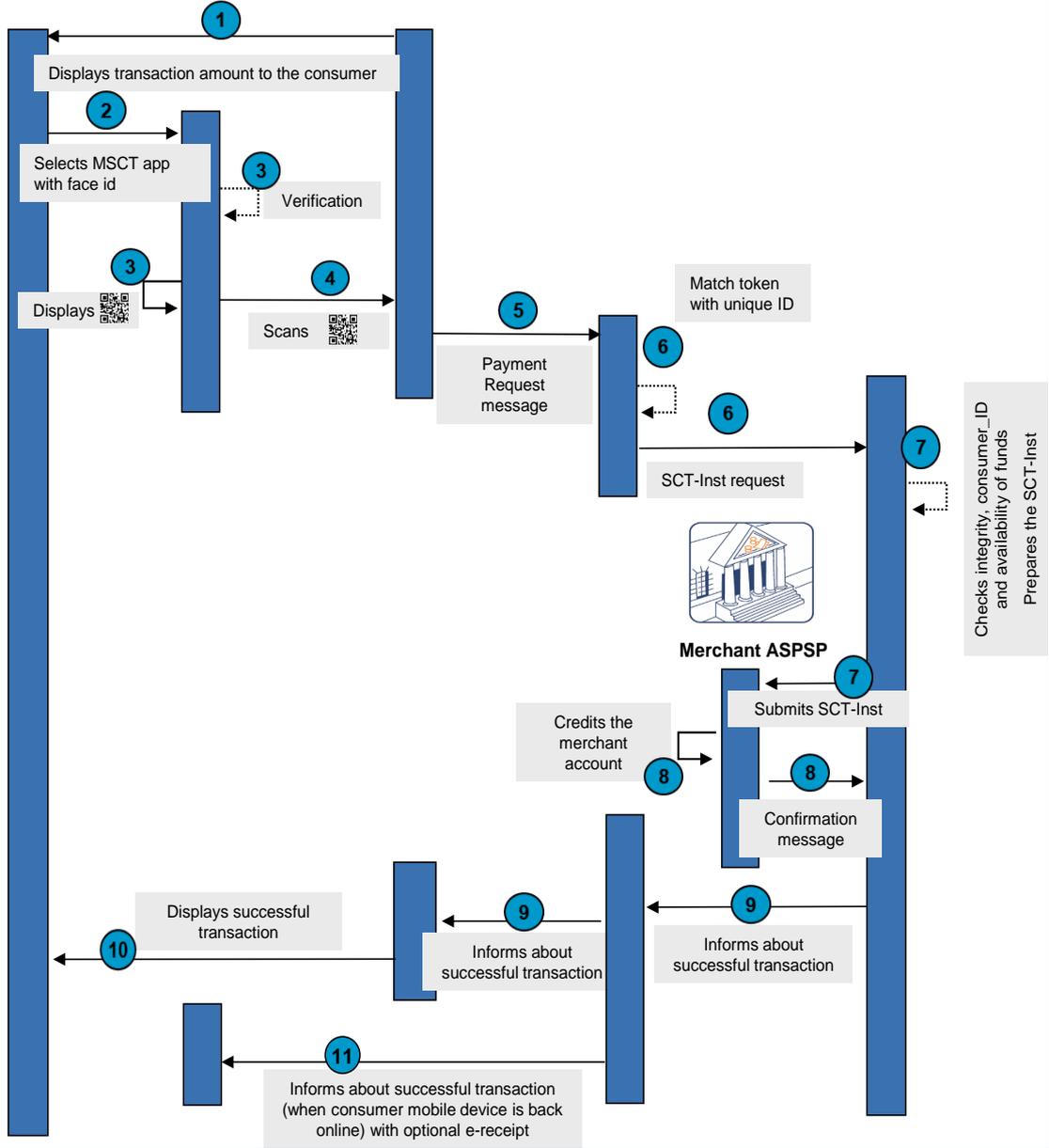
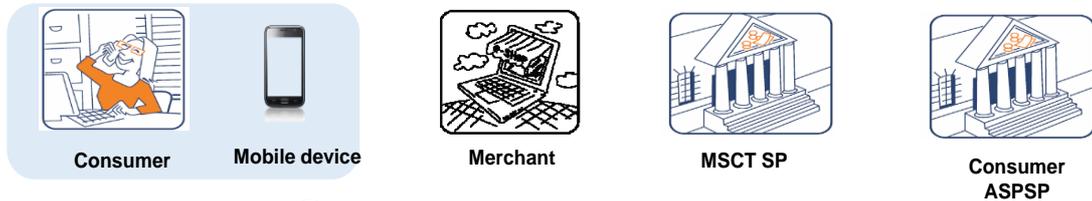


Figure 84: MSCT Use case C2B-14



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, the consumer would need to first subscribe to the MSCT Inst service and download a dedicated MSCT application from the MSCT service provider on their mobile device. During an on-boarding process, where the consumer will be authenticated online (see Chapter 14), the MSCT app receives a unique ID and the consumer will have agreed with their MSCT service provider an authentication method during the on-boarding process to open the MSCT app (e.g. facial recognition). The unique ID may be linked directly to the consumer or, for enhanced security, to the dedicated MSCT app, with a linking to the consumer in the MSCT service provider back-end system.
- The consumer's ASPSP delegates the authentication of the consumer to the MSCT service provider.
- The merchant also needs to be subscribed to the MSCT Inst service, e.g., through their ASPSP or the MSCT service provider directly and install a dedicated API for communication with the MSCT service provider.
- The MSCT service provider is linked to both ASPSPs.
- When the MSCT app on the consumer's mobile device has an online connection to the MSCT service provider, dedicated offline transaction tokens are being stored in an OS secured keychain by the MSCT app on the mobile device.

Step 1

The merchant enters the transaction amount which is displayed on the POI.

Step 2

The consumer selects and opens the MSCT application on their mobile device by authenticating¹⁸⁵ themselves via a facial identity.

Step 3

- The facial identity of the consumer is verified by the mobile device.
- Upon successful verification, a QR-code is displayed that contains a transaction token taken out from the secured keychain on the mobile device.

Step 4

The consumer presents their QR code, which is scanned by the merchant.

Step 5

The merchant retrieves the data from the QR-code and sends a Payment Request message to the MSCT service provider, including the merchant's name, IBAN_merchant¹⁸⁶, merchant transaction identifier, the transaction amount and the transaction token.

¹⁸⁵ Subject to clarification by EBA on questions EBA Q&A 2020_5366 and 2020_5367.

¹⁸⁶ Instead of the IBAN_merchant a proxy may be used.



Step 6

The MSCT service provider matches the transaction token with the unique ID and transmits an SCT Inst instruction, including the merchant name, IBAN_merchant, transaction data and unique ID to the consumer ASPSP.

Step 7

- The consumer ASPSP checks the integrity of the SCT Inst instruction and verifies the unique ID.
- The consumer ASPSP checks the availability of funds on the consumer account.
- The consumer ASPSP prepares and submits the SCT Inst transaction to the merchant ASPSP.

Step 8

- A confirmation message is returned from the merchant ASPSP to the consumer ASPSP.
- The merchant ASPSP makes the funds available to the merchant.

Step 9

- The consumer's ASPSP sends a notification message to the MSCT service provider about the successful execution of the SCT Inst transaction.
- The merchant receives a notification from their MSCT service provider that their account has been credited.

Step 10

The merchant POI displays to the consumer that the transaction has been successfully executed.

Step 11

The consumer is notified by the MSCT service provider in their MSCT app as soon as the app is back online again that the payment has been successfully executed and may optionally receive an e-receipt.

Analysis MSCT Use case C2B-14	
Interoperability	<ul style="list-style-type: none"> • The consumer and the merchant are subscribed to the same MSCT service while the consumer ASPSP needs be linked to the corresponding MSCT service provider. • For a truly “open” approach and a SEPA-wide interoperability, if the MSCT service provider of the consumer is different to the MSCT service provider of the merchant, a framework will need to be specified that interconnects the different MSCT service providers.
Challenges	<ul style="list-style-type: none"> • Standardisation of messages including data elements between MSCT service provider back-ends. • Standardisation of the QR-code. • Standardisation of the Payment Request messages.



	<ul style="list-style-type: none">• Security of the QR-code.• Clarification on the compliance concerning SCA with dynamic linking as specified in the PSD2 and RTS187.• Standardisation of interface between MSCT service providers and ASPSPs.• The notification messages in step 9 are not included in the SCT Inst scheme.
--	--

Table 70: Analysis MSCT Use case C2B-14

Notes:

- The standardisation of the QR-code for payer-presented data is defined in Chapter 18.
- The interoperability of MSCTs based on consumer-presented data whereby different MSCT service providers are involved for the consumer and merchant is addressed in Chapters 16 and 18.
- The security of QR-codes is addressed in Chapter 10.
- The minimum data elements in the payment request and notification messages are defined in Annex 4.

¹⁸⁷ Subject to clarification by EBA on questions EBA Q&A 2020_5366 and 2020_5367.



A2.8 MSCT use case C2B-15: Mobile device - Payment at a physical POI with consumer-presented QR-code - Unknown final amount with final amount is higher than pre-agreed amount – SCA using a dedicated authentication application involving a mobile code

This MSCT use case presents an example of consumer experience whereby their mobile device is used to pay in-store by presenting a consumer-presented QR-code to the POI. Hereby a dedicated MSCT Inst application on the mobile device of the consumer is used that they have downloaded from an MSCT service provider into their mobile device.

The consumer authentications are performed through a dedicated Authentication application in the consumer mobile device.

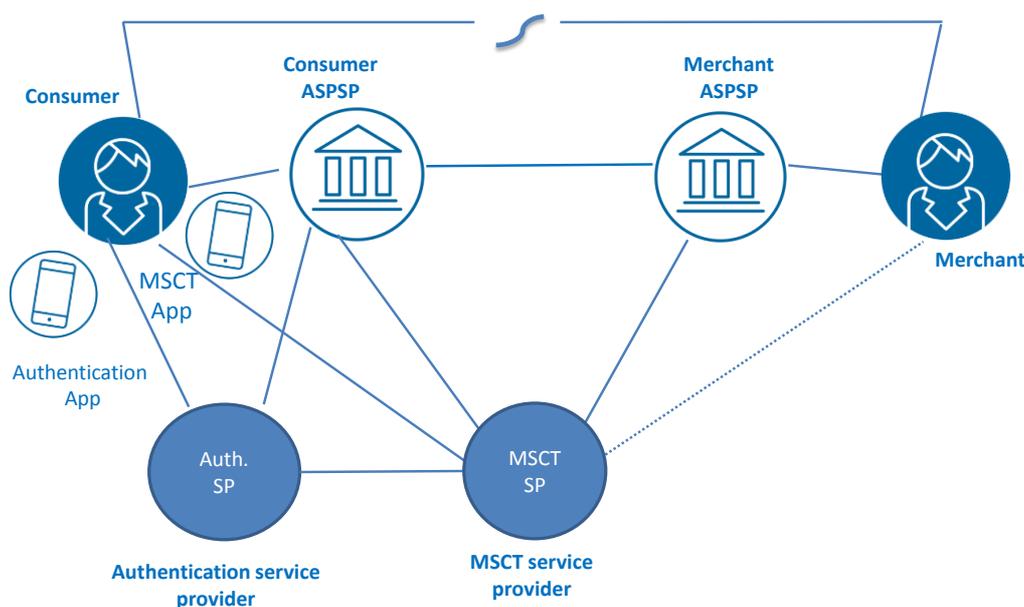


Figure 85: Actors in MSCT Use case C2B-15

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. Both ASPSPs are participants in the same MSCT Inst Service.

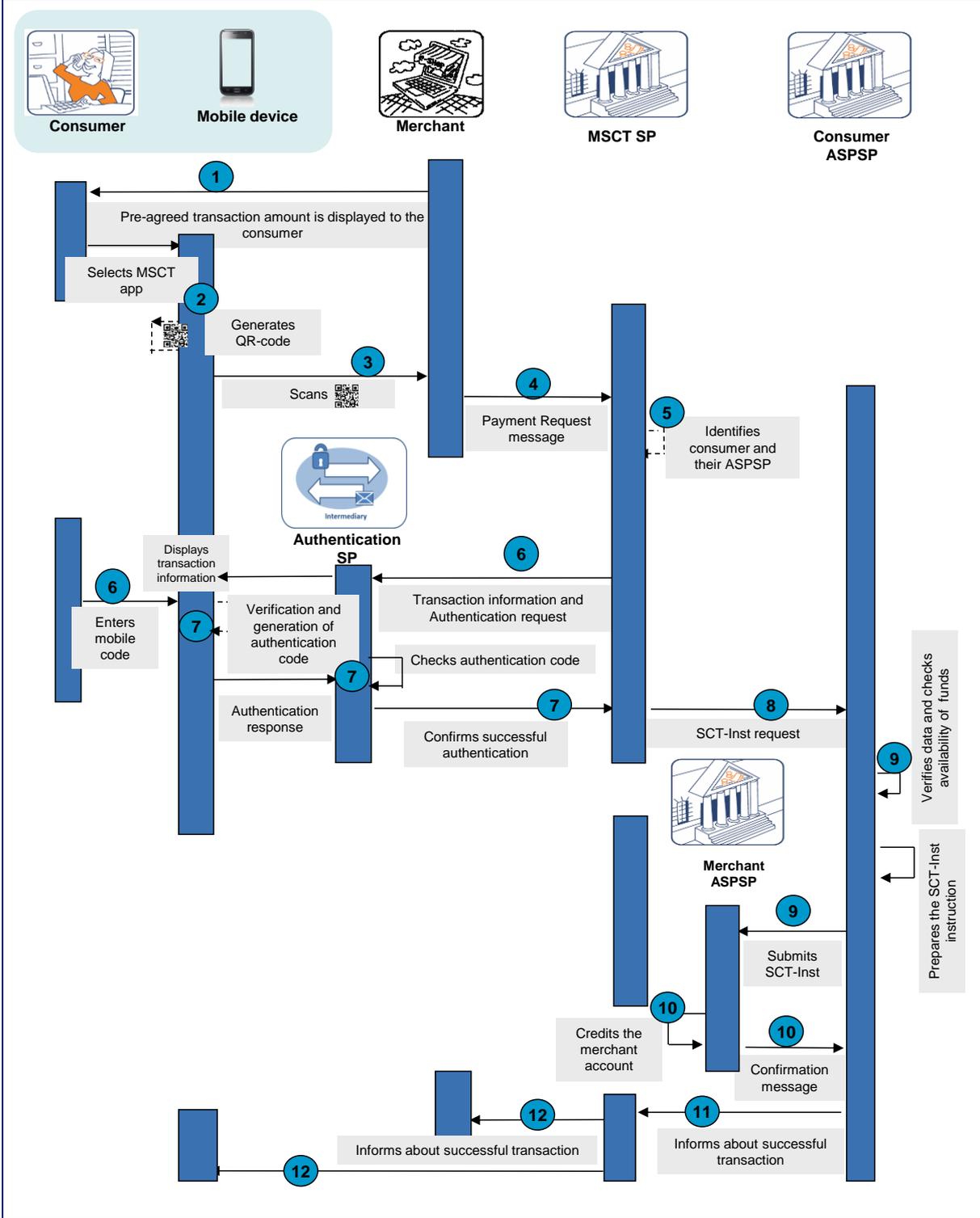
Also, the merchant needs to be subscribed to the MSCT Inst service and have downloaded dedicated software on their POI.

In this payment transaction strong customer authentication (see section 8.3) in accordance with the relevant PSD2 [5] requirements is performed involving a mobile code (see section 8.2) and the calculation of an authentication code by the authentication application using a dedicated key.

Note that hereby delegation for the consumer authentication needs to be given by the consumer ASPSP to the Authentication service provider. This requires an agreement between the consumer ASPSP and the Authentication service provider.



MSCT Use case C2B-15 (1)
Mobile device – Physical POI - Consumer-presented QR-code –
Unknown final transaction amount with final amount higher than pre-
agreed amount
SCA using a dedicated authentication application involving a mobile
code





MSCT Use case C2B-15 (2)
Mobile device – Physical POI - Consumer-presented QR-code – Unknown final transaction amount with final amount higher than pre-agreed amount
SCA using a dedicated authentication application involving a mobile code

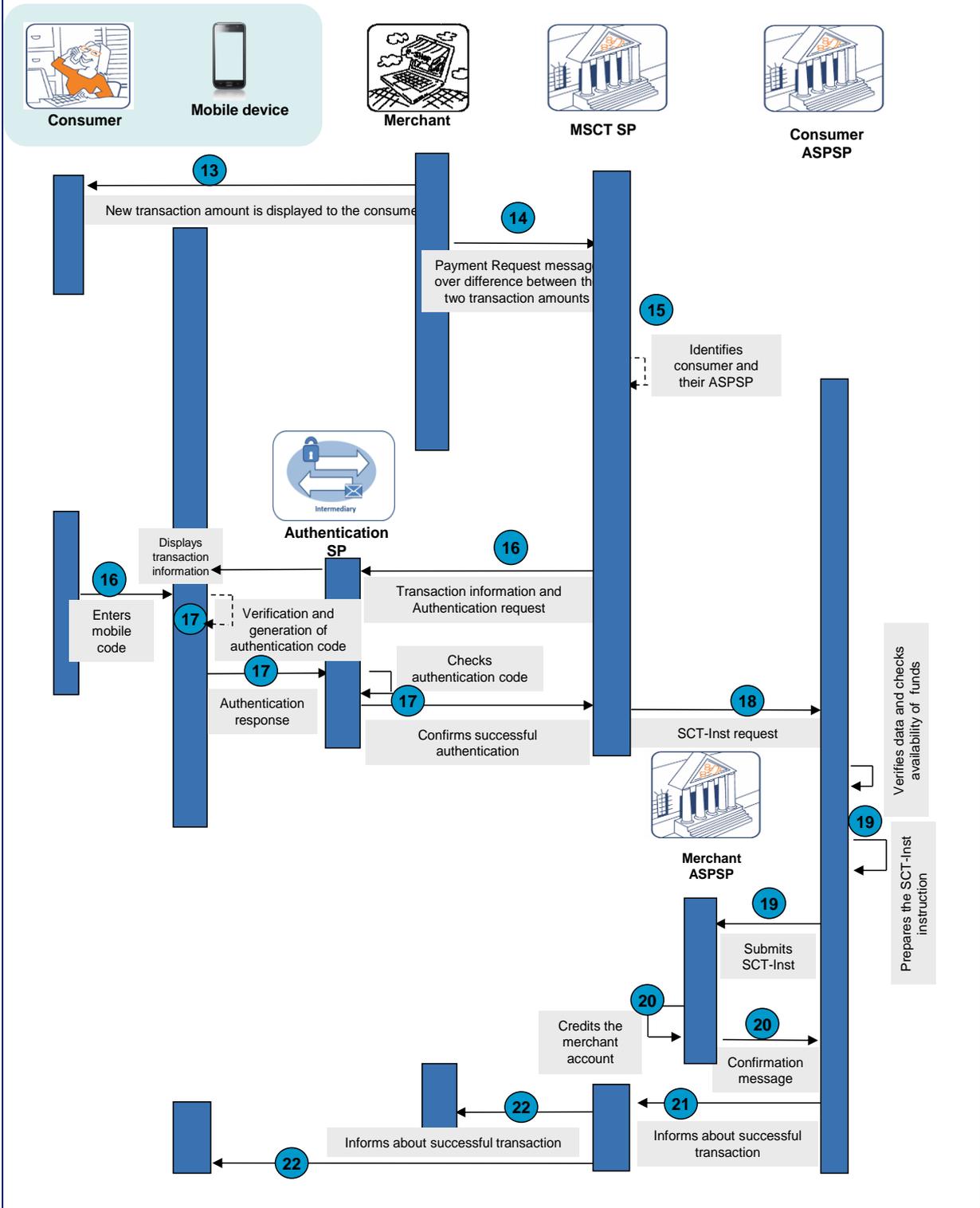


Figure 86: MSCT Use case C2B-15



In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, the consumer would need to first subscribe to the MSCT Inst service and download a dedicated MSCT Inst application from the MSCT service provider on their mobile device. Furthermore, they have a separate Authentication application from an Authentication service provider on their mobile device that has been previously linked to the MSCT Inst application.
- The consumer ASPSP delegates the authentication of the consumer to the Authentication service provider.
- The merchant also needs to be subscribed to the MSCT Inst service, e.g., through their ASPSP or the MSCT service provider directly, has downloaded dedicated software and has the appropriate equipment to scan QR-codes in their POI environment.
- The MSCT service provider is linked to the consumer ASPSP.
- During the payment transaction, a mobile internet connection by the consumer device is required.

Step 1

The merchant enters the pre-agreed¹⁸⁸ transaction amount which is displayed on the POI¹⁸⁹.

Step 2

- The consumer selects and opens the MSCT Inst application on their mobile device which possibly involves the entry of a password (or other means of authentication).
- A QR-code containing a token for the consumer is generated by the MSCT Inst application on the mobile device.

Step 3

The consumer presents the QR-code which is scanned by the merchant POI.

Step 4

The merchant retrieves the consumer token from the QR-code and sends a Payment Request message to the MSCT service provider, including the merchant name, IBAN_merchant¹⁹⁰, merchant transaction identifier, the pre-agreed transaction amount and the consumer token.

Step 5

The MSCT service provider identifies the consumer IBAN and ASPSP from the consumer token.

¹⁸⁸ E.g. for rental, hospitality, e-com food, ...

¹⁸⁹ The display of the pre-agreed transaction amount by the POI may happen after step 3, since the customer identification might have an impact on the final transaction amount.

¹⁹⁰ Instead of the IBAN_merchant a proxy may be used.



Step 6

- The MSCT service provider forwards the transaction information to the MSCT Inst app on the consumer mobile device.
- The consumer is invited to confirm the transaction and is redirected to their Authentication application which displays the merchant name/ IBAN_merchant and the pre-agreed transaction amount.
- The consumer authenticates and confirms the transaction by entering their mobile code on the mobile device.

Step 7

- Upon successful mobile code verification by the mobile device, an authentication code is calculated by the Authentication application.
- The authentication code is transmitted for verification to the Authentication service provider.
- Upon successful verification, the MSCT service provider is informed by the Authentication service provider.

Step 8

The SCT Inst instruction including the merchant name, IBAN_merchant, the pre-agreed transaction amount and the merchant transaction identifier with a flag indicating the successful authentication are transmitted from the MSCT service provider to the consumer ASPSP.

Step 9

- The consumer ASPSP checks the integrity of the SCT Inst instruction.
- The consumer ASPSP checks the availability of funds on the consumer account.
- The consumer ASPSP prepares and submits the SCT Inst transaction (on the pre-agreed transaction amount) to the merchant ASPSP.

Step 10

- A confirmation message is returned from the merchant ASPSP to the consumer ASPSP.
- The merchant ASPSP makes the funds available to the merchant.

Step 11

The consumer ASPSP sends a notification message to the MSCT service provider about the successful execution of the SCT Inst transaction.

Step 12

- The merchant is informed by the MSCT service provider that their account has been credited.
- The consumer is informed by the MSCT service provider in their MSCT app that the payment has been successfully executed and may optionally receive an e-receipt.



Step 13

- After offering the service, the final transaction amount is higher than the pre-agreed amount by the consumer.
- The merchant enters the difference between the two transaction amounts on the POI¹⁹¹ which is displayed as a new transaction amount on the POI to the consumer, if present.

Step 14

The merchant sends a new Payment Request message to their MSCT service provider, including the merchant name, IBAN_merchant¹⁹², merchant transaction identifier, the new transaction amount and the merchant transaction identifier of the original transaction.

Step 15

The MSCT service provider identifies the consumer IBAN and ASPSP from the consumer token in the original transaction.

Step 16

- The MSCT service provider forwards the transaction information to the MSCT Inst app on the consumer mobile device.
- The consumer is invited to confirm the transaction and is redirected to their Authentication application¹⁹³ which displays the merchant name/ IBAN_merchant and the new transaction amount.
- The consumer authenticates and confirms the transaction by entering their mobile code on the mobile device.

Step 17

- Upon successful mobile code verification by the mobile device, an authentication code is calculated by the Authentication application.
- The authentication code is transmitted for verification to the Authentication service provider.
- Upon successful verification, the MSCT service provider is informed by the Authentication service provider.

Step 18

The SCT Inst instruction including the merchant name, IBAN_merchant, the new transaction amount and the merchant transaction identifier with a flag indicating the successful authentication are transmitted from the MSCT service provider to the consumer ASPSP.

Step 19

- The consumer ASPSP checks the integrity of the SCT Inst instruction.
- The consumer ASPSP checks the availability of funds for the new transaction amount on the consumer account.

¹⁹¹ The display of the transaction amount by the POI may happen after step 3, since the customer identification might have an impact on the final transaction amount.

¹⁹² Instead of the IBAN_merchant a proxy may be used.

¹⁹³ This 2nd transaction may be exempted from SCA in which case the consumer would not be invited to enter a mobile code.



- The consumer ASPSP prepares and submits the SCT Inst transaction (on the new transaction amount) to the merchant ASPSP.

Step 20

6. A confirmation message is returned from the merchant ASPSP to the consumer ASPSP.
7. The merchant ASPSP makes the funds available to the merchant.

Step 21

The consumer ASPSP sends a notification message to the MSCT service provider about the successful execution of the SCT Inst transaction.

Step 22

- The merchant is informed by the MSCT service provider that their account has been credited.
 - The consumer is informed by the MSCT service provider in their MSCT app that the payment has been successfully executed and may optionally receive an e-receipt.
- 8.

Notes:

- For virtual POIs, the MSCT use case will be similar except that the consumer token will need to be transferred to the merchant in a different way (e.g., entered manually by the consumer into the merchant website or payment page).
- This use case could also be described for MSCTs based on merchant-presented QR-codes whereby two consecutive transactions will need to be executed, the first one based on a QR-code including the pre-agreed amount, the second one covering the difference between the two transaction amounts.

- 9.
- 10.

Analysis MSCT Use case C2B-15	
Interoperability	The consumer and the merchant are subscribed to the same MSCT service while the consumer ASPSP needs be linked to this MSCT service provider. For a truly “open” approach and a SEPA-wide interoperability, if the MSCT service provider of the consumer is different from the MSCT service provider of the merchant, a framework will need to be specified that interconnects the different MSCT service providers.
Challenges	<ul style="list-style-type: none"> • Standardisation of messages between MSCT service providers (e.g., Payment Request messages, Notification messages, ...). • Standardisation of the QR-code. • Security of the QR-code. • How can the two transactions be linked? • How can the merchant link the two transactions? • How can the consumer link the two transactions? • The notification messages in steps 11 and 22 are not included in the SCT Inst scheme.

Table 71: Analysis MSCT Use case C2B-15



Notes:

- The standardisation of the QR-code for payer-presented data is specified in Chapter 18.
- The interoperability of MSCTs based on consumer-presented data whereby different MSCT service providers are involved for the consumer and merchant is addressed in Chapters 16 and 18.
- The security of QR-codes is addressed in Chapter 10.
- The minimum data elements in the payment request and notification messages are defined in Annex 4.



Annex 3: Overview on errors with MSCTs

This annex provides an overview on the main errors for MSCTs based on respectively payee- and payer-presented data.

A3.1 MSCTs based on payee-presented data

The table below identifies the different errors which may occur with MSCTs based on payee-presented data for SCT Inst or SCT. For the relevant cases, a mapping is made to the different categories identified in Table 32 and Table 35 in this document.

Error cases for MSCTs based on payee-presented data					
#	Issue description	Mapping on Table 32 and Table 35			Inquiry – Table 60
		Cat 1 - Reject by payer MSCT SP	Cat 2 - Reject by payer ASPSP	Cat 3 – Unsuccessful transaction	
Communication errors between the parties					
1	TLS mutual authentication issues	X	X	X	X
2	Incorrect message syntax	X	X	X	X
3	No server response, timeouts, etc.	X	X	X	X
4	Communication interruptions/failures	X	X	X	X
Issues with the payer MSCT app					
5	MSCT app not recognised by payer MSCT service provider server	X			
6	Payer device not properly personalised (e.g., missing credentials)	X			
QR-code scanning issues					
7	Incorrect QR-code (syntax issue, invalid checksum/signature, etc.)				
8	QR-code impossible to read/partially read				
Payer authentication failure					
9	Incorrect user verification (mobile code, biometrics) by mobile device	X	X		
10	Blocked payer mobile device due to too many consecutive user verification errors	X	X		
11	Incorrect authentication code	X	X		
Dynamic linking errors					
12	Payee data received in authentication request does not match payee data received in payment initiation request	X	X		
13	Dynamic linking verification failure	X	X		
Issues with tokens/proxies					
14	Payee token/proxy not found or invalid	X			X
Payer ASPSP verification issues (other than failed SCA)					
15	Sanction screening / AML/ Fraud controls by payer ASPSP		X		



16	Invalid payer IBAN		X		
17	Insufficient funds		X		
18	Spending limits reached or other risk assessment errors		X		
SCT Inst /SCT execution errors					
19	Sanction screening / AML/ Fraud controls by payee ASPSP			X	
20	Invalid payee IBAN			X	
21	Other SCT Inst /SCT processing issue			X	X
Notification errors					
22	Failure to notify the payee of the correct SCT Inst / SCT execution				X
23	Failure to notify the payee of issues/errors prior to SCT Inst / SCT execution				X
24	Failure to notify the payee of issues/errors with the SCT Inst / SCT execution				X
25	Failure to notify the payer of the correct SCT Inst / SCT execution				X
26	Failure to notify the payer of issues/errors prior to SCT Inst / SCT execution				X
27	Failure to notify the payer of issues/errors with the SCT Inst / SCT execution				X

Table 72: Overview on errors for MSCTs based on payee-presented data

A3.2 MSCTs based on payer-presented data

The table below identifies the different errors which may occur with MSCTs based on payer-presented data for SCT Inst or SCT. For the relevant cases, a mapping is made to the different categories identified in Table 50 and Table 53 in this document.

Error cases for MSCTs based on payer-presented data						
#	Issue description	Mapping on Table 50 and Table 53				Inquiry Table 61
		Cat 1 - Reject by payee MSCT SP	Cat 2 - Reject by payer MSCT SP	Cat 3 - Reject by payer ASPSP	Cat 4 - Unsuccessful transaction	
Communication errors between the parties						
1	TLS mutual authentication issues	X	X	X	X	X
2	Incorrect message syntax	X	X	X	X	X
3	No server response, timeouts, etc.	X	X	X	X	X
4	Communication interruptions/failures	X	X	X	X	X
Issues with the payer MSCT app						
5	MSCT app not recognised by payer MSCT service provider server		X			



6	Payer device not properly personalised (e.g., missing credentials, invalid payer token)		X			
QR-code scanning issues						
7	Incorrect QR-code (syntax issue, invalid checksum/signature, etc.)	X				
8	QR-code impossible to read/partially read	X				
Payer authentication failure						
9	Incorrect user verification (mobile code, biometrics) by mobile device		X	X		
10	Blocked payer mobile device due to too many consecutive user verification errors		X	X		
11	Incorrect authentication code		X	X		
Dynamic linking errors						
12	Payee data received in authentication request does not match payee data received in payment initiation request		X	X		
13	Dynamic linking verification failure		X	X		
Issues with tokens/proxies						
14	Payer token/proxy not found or invalid		X	X		X
Payer ASPSP verification issues (other than failed SCA)						
15	Sanction screening / AML/ Fraud controls by payer ASPSP			X		
16	Invalid payer IBAN			X		
17	Insufficient funds			X		
18	Spending limits reached or other risk assessment errors			X		
SCT Inst /SCT execution errors						
19	Sanction screening / AML/ Fraud controls by payee ASPSP				X	
20	Invalid Payee IBAN				X	
21	Other SCT Inst /SCT processing issue				X	X
Notification errors						
22	Failure to notify the payee of the correct SCT Inst / SCT execution					X
23	Failure to notify the payee of issues/errors prior to SCT Inst / SCT execution					X
24	Failure to notify the payee of issues/errors with the SCT Inst / SCT execution					X
25	Failure to notify the payer of the correct SCT Inst / SCT execution					X



26	Failure to notify the payer of issues/errors prior to SCT Inst / SCT execution					X
27	Failure to notify the payer of issues/errors with the SCT Inst / SCT execution					X

Table 73: Overview on errors for MSCTs based on payer-presented data



Annex 4: Minimum data sets for MSCT interoperability messages

A4.1 Introduction

This section specifies the minimum data sets for the MSCT interoperability messages listed in Chapter 19. The messages cover both MSCTs based on SCT Inst or SCT. For each type identified in these tables, an overview table with the messages involved is provided, followed by tables detailing the minimum data set for each message, with an indication for each data element whether it is mandatory (M), optional (O) or conditional (C)¹⁹⁴.

A4.2 Transaction Information messages

This section provides the *Transaction Information messages* for MSCTs based on SCT Inst or SCT using payee-presented data as defined in Chapter 17. The minimum data elements to be included in these messages are specified below.

Transaction information messages	
TIRQ	Transaction Information request message by payer MSCT service provider to payee MSCT service provider
TIRP	Transaction Information response message by payee MSCT service provider to payer MSCT service provider

Table 74: Overview transaction information messages

A4.2.1 Transaction information request

TIRQ	Inter-MSCT service provider transaction information request by payer MSCT service provider to payee MSCT service provider
Description	This dataset describes the content of the transaction information request by the payer MSCT service provider to the payee MSCT service provider via the HUB.
Attributes contained	<ul style="list-style-type: none"> • The payee proxy or token (M) • The payer MSCT service provider identifier (M)

¹⁹⁴ This means that it is dependent on certain conditions, e.g., if it the MSCT is successful, unsuccessful or a reject.



TIRQ	Inter-MSCT service provider transaction information request by payer MSCT service provider to payee MSCT service provider
	<ul style="list-style-type: none"> • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • The expiry date of the Transaction information request (O) • Type of payment instrument (SCT or SCT Inst) (O) • Date and Time stamp (M)

Table 75: Dataset for transaction information request

A4.2.2 Transaction information response

TIRP	Inter-MSCT service provider transaction information response by payee MSCT service provider to payer MSCT service provider
Description	This dataset describes the content of the transaction information response by the payee MSCT service provider to the payer MSCT service provider via the HUB.
Attributes contained	<ul style="list-style-type: none"> • The payee proxy or token (M) • The name / trade name of the payee (M) • The name / trade name of the payee reference party (O) • The IBAN of the payee (C) • The transaction amount (C) • The currency (C) • The Merchant Category Code (C) • The payer MSCT service provider identifier (M) • The payee MSCT service provider identifier (M)



TIRP	Inter-MSCT service provider transaction information response by payee MSCT service provider to payer MSCT service provider
	<ul style="list-style-type: none"> • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (O) • Place holder for charging (O) • Date and Time stamp (M)

Table 76: Dataset for transaction information response

A4.3 Lock Transaction messages

This section provides the *Conditional Lock Transaction messages* for MSCTs, based on SCT Inst or SCT, using payee-presented data. These conditional messages may be used to lock a specific MSCT transaction for a given payer in C2B payment contexts as defined in Chapter 17. The minimum data elements to be included in these messages are specified below.

Lock transaction messages	
LTRQ	Lock transaction request message by payer MSCT service provider to payee MSCT service provider
LTRP	Lock transaction response message by payee MSCT service provider to payer MSCT service provider

Table 77: Overview lock transaction messages

A4.3.1 Lock transaction request

LTRQ	Inter MSCT service provider lock transaction request by payer MSCT service provider to payee MSCT service provider
Description	This dataset describes the content of the lock transaction request by the payer MSCT service provider to the payee MSCT service provider via the HUB.



LTRQ	Inter MSCT service provider lock transaction request by payer MSCT service provider to payee MSCT service provider
Attributes contained	<ul style="list-style-type: none"> • The payer name/trade name (M) • The transaction amount (M) • The currency (M) • The payer MSCT service provider identifier (M) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (M) • Date and Time stamp (M)

Table 78: Dataset for lock transaction request message

A4.3.2 Lock transaction response

LTRP	Inter-MSCT service provider lock transaction response by payee MSCT service provider to payer MSCT service provider
Description	This dataset describes the content of the lock transaction response by the payee MSCT service provider to the payer MSCT service provider via the HUB.
Attributes contained	<ul style="list-style-type: none"> • Lock transaction status (M) • Date and Time stamp (M) • A copy of the mandatory minimum data elements in LTRQ to which is being responded (M)

Table 79: Dataset for lock transaction response message

A4.4 Payment Request

This section provides an overview on the different messages for the *Payment Request* for MSCTs, based on SCT Inst or SCT, using payer-presented data as defined in Chapter 18. The minimum data elements to be included in these messages are specified below.



Payment Request messages	
PR1	Payment request message by payee to payee MSCT service provider
PR2	Payment request message by payee MSCT service provider to payer MSCT service provider
CRPR1	Confirmation of receipt of payment request message by payer MSCT service provider to payee MSCT service provider
CRPR2	Confirmation of receipt of payment request message by payee MSCT service provider to payee

Table 80: Overview of payment request messages



A4.4.1 Payment request messages

From payee to their MSCT service provider

PR1	Payment request message by payee to payee MSCT service provider
Description	This dataset describes the content of the Payment Request message as presented by the payee to the payee MSCT service provider.
Attributes contained	<ul style="list-style-type: none"> • The payer identification data (M) • The transaction amount (M) • The currency (M) • The remittance Information sent by the payee to the payer (O) • The payer MSCT service provider identifier (M) • The Requested Execution Date/Time of the Payment Request (M) • The IBAN of the payee (M) • The name of the payee (M) • The trade name of the payee (M for C2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The address of the payee (O) • The BIC code of the payee ASPSP (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • The purpose of the Payment Request (O) • The Merchant Category Code (MCC) (M for C2B) • The expiry date of the Payment Request (O)



PR1	Payment request message by payee to payee MSCT service provider
	<ul style="list-style-type: none"> • Type of payment instrument requested by the payee (SCT or SCT Inst) (M) • Flag notification message required (O) • Place holder for charging (O)

Table 81: Dataset for payment request message by the payee to the payee MSCT service provider

Between MSCT service providers

PR2	Inter-MSCT service provider payment request message by payee MSCT service provider to payer MSCT service provider
Description	This dataset describes the content of the Payment Request presentment by the payee MSCT service provider to the payer MSCT service provider via the HUB.
Attributes contained	<ul style="list-style-type: none"> • The payer identification data (M) • The transaction amount (M) • The currency (M) • The remittance information (O) • The payer MSCT service provider identifier (M) • The Requested Execution Date/Time of the Payment Request (M) • The IBAN of the payee (M) • The name of the payee (M) • The trade name of the payee (M for C2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The address of the payee (O)



PR2	Inter-MSCT service provider payment request message by payee MSCT service provider to payer MSCT service provider
	<ul style="list-style-type: none"> • The BIC code of the payee ASPSP (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • The purpose of the Payment Request (O) • The Merchant Category Code (MCC) (M for C2B) • The expiry date of the Payment Request (O) • Type of payment instrument requested by the payee (SCT or SCT Inst) (M) • Flag notification message required (O) • Additional unique reference provided by the payee MSCT service provider (O) • Type of payment instrument (SCT or SCT Inst) (M) • Place holder for charging (O)

Table 82: Dataset for payment request message by the payee MSCT service provider to the payer MSCT service provider



A4.4.2 Confirmations of receipt of payment request

Between MSCT service providers

CRPR1	Inter-MSCT service provider confirmation of receipt of payment request by payer MSCT service provider to payee MSCT service provider
Description	This dataset describes the content of the confirmation of receipt of a Payment Request message by the payer MSCT service provider to the payee MSCT service provider via the HUB.
Attributes contained	<ul style="list-style-type: none"> • Confirmation of receipt (M) • Date and Time stamp (M) • A copy of the mandatory minimum data elements in PR2 which is being confirmed (M)

Table 83: Dataset for confirmation of receipt of payment request by the payer MSCT service provider to the payee MSCT service provider

From payee MSCT service provider to payee

CRPR2	Confirmation of receipt of payment request by payee MSCT service provider to payee
Description	This dataset describes the content of the confirmation of receipt of a payment request message by the payee MSCT service provider to the payee.
Attributes contained	<ul style="list-style-type: none"> • Confirmation of receipt (M) • Date and Time Stamp (M) • A copy of the mandatory minimum data elements in PR2 which is being confirmed (M)

Table 84: Dataset for confirmation of receipt of payment request by the MSCT service provider to the payee



A4.5 Notification of Reject messages

This section provides an overview on the different messages for the *Notification of Reject* for MSCTs based on SCT Inst or SCT, using payer- or payee-presented data as defined in Chapter 17 and Chapter 18. The minimum data elements to be included in these messages are specified below.

Notification of reject messages	
NR1	Notification of reject message by payer ASPSP to payer MSCT service provider
NR2	Notification of reject message by payer MSCT service provider to payee MSCT service provider
NR3	Notification of reject message by payer MSCT service provider to payer
NR4	Notification of reject message by payee MSCT service provider to payee

Table 85: Overview of notification of reject messages

From payer ASPSP to payer MSCT service provider

NR1	Notification of reject by payer ASPSP to payer MSCT service provider
Description	This dataset describes the content of the notification of reject message from the payer ASPSP to the payer MSCT service provider.
Attributes contained	<ul style="list-style-type: none"> • Type of reject (M) • The BIC code of the payer ASPSP (M) • The name of the payer (M) • The transaction amount (M) • The currency (M) • The remittance Information (O)



NR1	Notification of reject by payer ASPSP to payer MSCT service provider
	<ul style="list-style-type: none"> • The payer MSCT service provider identifier (M) • The IBAN of the payee (M) • The name of the payee (M) • The trade name of the payee (M for C2B and B2B) • The payee reference party (O) • The trade name of the payee reference party (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Reason code for reject (M) • Type of payment instrument (SCT or SCT Inst) (M) • Date and Time stamp (M)

Table 86: Dataset for notification of reject message by the payer ASPSP to the payer MSCT service provider

Between MSCT service providers

NR2	Inter-MSCT service provider notification of reject by payer MSCT service provider to payee MSCT service provider
Description	This dataset describes the content of the notification of reject by the payer MSCT service provider to the payee MSCT service provider via the HUB.
Attributes contained	<ul style="list-style-type: none"> • Type of reject (M) • The name of the payer (M) • The transaction amount (M) • The currency (M) • The remittance Information (O)



NR2	Inter-MSCT service provider notification of reject by payer MSCT service provider to payee MSCT service provider
	<ul style="list-style-type: none"> • The payer MSCT service provider identifier (M) • The IBAN of the payee (M) • The name of the payee (M) • The trade name of the payee (M for C2B and B2B) • The payee reference party (O) • The trade name of the payee reference party (O) • The BIC code of the payer ASPSP (O) • The BIC code of the payee ASPSP (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Reason code for reject (M) • Additional unique reference provided by the payer MSCT service provider (O) • Type of payment instrument (SCT or SCT Inst) (M) • Date and Time stamp (M) • Place holder for charging (O)

Table 87: Dataset for notification of reject message by the payer MSCT service provider to the payee MSCT service provider



Between payer MSCT service provider and payer

NR3	Notification of reject by payer MSCT service provider to payer
Description	This dataset describes the content of the notification of reject from the payer MSCT service provider to the payer.
Attributes contained	<ul style="list-style-type: none"> • Type of reject (M) • The transaction amount (M) • The currency (M) • The IBAN of the payer (O) • The remittance Information (O) • The name of the payee (M) • The trade name of the payee (M for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (O) • Reason code for reject (M) • Date and Time stamp (M)

Table 88: Dataset for notification of reject message by the payer MSCT service provider to the payer

Between payee MSCT service provider and payee

NR4	Notification of reject by payee MSCT service provider to payee
Description	This dataset describes the content of the notification of reject by the payee MSCT service provider to the payee.
Attributes contained	<ul style="list-style-type: none"> • Type of reject (O)



NR4	Notification of reject by payee MSCT service provider to payee
	<ul style="list-style-type: none"> • The name of the payer (M) • The transaction amount (M) • The currency (M) • The remittance Information (O) • The name of the payee (O) • The IBAN of the payee (O) • The trade name of the payee (O for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (O) • Date and Time stamp (M)

Table 89: Dataset for notification of reject message by the payee MSCT service provider to the payee

A4.6 Notification of Successful/Unsuccessful Transaction messages

This section provides an overview on the different messages for the *Notification of Successful / Unsuccessful transaction* for MSCTs, based on SCT Inst or SCT, using payer- or payer-presented data as defined in Chapter 17 and Chapter 18. The minimum data elements to be included in these notification messages are specified below.

Notification of successful / unsuccessful transaction messages	
NT1	Notification of successful / unsuccessful transaction message by payer ASPSP to payer MSCT service provider
NT2	Notification of successful /unsuccessful transaction message by payer MSCT service provider to payee MSCT service provider



NT3	Notification of successful /unsuccessful transaction message by payer MSCT service provider to payer
NT4	Notification of successful /unsuccessful transaction message by payee MSCT service provider to payee

Table 90: Overview of notification of successful / unsuccessful transaction messages

From payer ASPSP to payer MSCT service provider

NT1	Notification of successful / unsuccessful transaction by payer ASPSP to payer MSCT service provider
Description	This dataset describes the content of the notification of successful / unsuccessful transaction by the payer ASPSP to the payer MSCT service provider.
Attributes contained	<ul style="list-style-type: none"> • The BIC code of the payer ASPSP (M) • Transaction status (M) • The name of the payer (M) • The transaction amount (M) • The currency (M) • The remittance information (O) • The Payer MSCT service provider identifier (M) • The IBAN of the payee (M) • The name of the payee (M) (account holder) • The trade name of the payee (M for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The payee MSCT service provider identifier (M)



NT1	Notification of successful / unsuccessful transaction by payer ASPSP to payer MSCT service provider
	<ul style="list-style-type: none"> • The Identification code of the MSCT scheme (M) • The transaction identifier (M) • Reason code for unsuccessful transaction (C) • Identification of party not accepting the transaction (C) • Additional unique reference provided by the payer MSCT service provider (O) • Type of payment instrument (SCT or SCT Inst) • The settlement date of the transaction (C) • Date and Time stamp (M) • Place holder for charging (O)

Table 91: Dataset for notification of successful / unsuccessful transaction message by the payer ASPSP to the payer MSCT service provider

Between MSCT service providers

NT2	Inter-MSCT service provider notification of successful / unsuccessful transaction between payer MSCT service provider and payee MSCT service provider
Description	This dataset describes the content of the notification of successful / unsuccessful transaction by the payer MSCT service provider to the payee MSCT service provider via the HUB.
Attributes contained	<ul style="list-style-type: none"> • Transaction status (M) • The name of the payer (M) • The transaction amount (M) • The currency (M)



NT2	Inter-MSCT service provider notification of successful / unsuccessful transaction between payer MSCT service provider and payee MSCT service provider
	<ul style="list-style-type: none"> • The remittance information (O) • The payer MSCT service provider identifier (M) • The IBAN of the payee (M) • The name of the payee (M) (account holder) • The trade name of the payee (M for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Reason code for unsuccessful transaction (C) • Identification of party not accepting the transaction (C) • Additional unique reference provided by the Payer MSCT service provider (O) • Type of payment instrument (SCT or SCT Inst) • The settlement date of the transaction (C) • Date and Time stamp (M) • Place holder for charging (O)

Table 92: Dataset for notification of unsuccessful transaction message by the payer MSCT service provider to the payee MSCT service provider



Between payer MSCT service provider and payer

NT3	Notification of successful / unsuccessful transaction by payer MSCT service provider to payer
Description	This dataset describes the content of the notification of successful / unsuccessful transaction by the payer MSCT service provider to the payee MSCT service provider.
Attributes contained	<ul style="list-style-type: none"> • Transaction status (M) • The transaction amount (M) • The currency (M) • The remittance Information (O) • The payer MSCT service provider identifier (M) • The IBAN of the payer (O) • The name of the payee (M) • The trade name of the payee (M for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (O) • Reason code for unsuccessful transaction (M) • The settlement date of the transaction (C) • Date and Time stamp (M)

Table 93: Dataset for notification of successful / unsuccessful transaction message by the payer MSCT service provider to the payer



Between payee MSCT service provider and payee

NT4	Notification of successful / unsuccessful transaction by payee MSCT service provider to payee
Description	This dataset describes the content of the notification of successful / unsuccessful transaction by the payee MSCT service provider to the payee.
Attributes contained	<ul style="list-style-type: none"> • Transaction status (M) • The name of the payer (M) • The transaction amount (M) • The currency (M) • The remittance Information (O) • The name of the payee (O) • The IBAN of the payee (M) • The trade name of the payee (O for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The payee MSCT service provider identifier (O) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (O) • The settlement date of the transaction (C) • Date and Time stamp (M)

Table 94: Dataset for notification of unsuccessful transaction message by the payee MSCT service provider to the payee



A4.7 Inquiry messages

This section provides an overview on the different messages for the *Inquiry messages* between MSCT service providers for MSCTs, based on SCT Inst or SCT, using payer- or payer-presented data as defined in Chapter 19. The minimum data elements to be included in these notification messages are specified below.

Inquiry messages	
IRQ	Inquiry request message between MSCT service providers
IRP	Inquiry response message between MSCT service providers

Table 95: Overview inquiry messages for MSCTs

A4.7.1 Inquiry request message

IRQ	Inter-MSCT service provider inquiry request message
Description	This dataset describes the content of the inquiry request message exchanged between the payer and the payee MSCT service providers via the HUB.
Attributes contained	<ul style="list-style-type: none"> • Check status request (M) • The payer MSCT service provider identifier (M) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Date and Time stamp (M)

Table 96: Dataset for inquiry request message between MSCT service providers



A4.7.2 Inquiry response message

IRP	Inter-MSCT service provider inquiry response message
Description	This dataset describes the content of the inquiry response message exchanged between the payer and the payee MSCT service providers via the HUB.
Attributes contained	<ul style="list-style-type: none"> • Check status response information (M) • Date and Time stamp (M) • A copy of the mandatory data elements of IRQ to which is responded (M)

Table 97: Dataset for inquiry response message between MSCT service providers

Notes:

- The different status to be reflected in the data field Check status response would need to be defined under an MSCT interoperability framework.
- The reply to an Inquiry request may be a re-sending of a previous message instead of an Inquiry response message.



Annex 5: The multi-stakeholder group

The following organisations have contributed to the development of the 2nd release of this document through participation in the multi-stakeholder group Mobile Initiated SEPA (Instant) Credit Transfers (MSG MSCT):

AIB on behalf of Banking & Payments Federation Ireland (BPFI) - representing EPC
BP
BEUC - European Consumer Organisation
BlueCode
Carrefour - representing EuroCommerce
Circle K
Colruyt - representing EuroCommerce
Crédit Mutuel - representing EPC
DnB Bank – representing EPC
EACT - European Association of Corporate Treasurers
EquensWorldline
Estonian Banking Association- representing EPC
EMPSA - European Mobile Payment Systems Association
ETTPA - European Third Party Providers Association
Fiserv
Getswish
Huawei
Idemia - representing Smart Payment Association
IKEA - representing EuroCommerce
Intesa Sanpaolo on behalf of Italian Banking Association (ABI) – representing EPC
KBC - representing EPC
La Banque Postale - representing EPC
Mastercard
Millennium bcp – representing EPC
Monei
National Clearing House KIR
Nordea
OpenWay
Orange - representing GSMA
Payconiq
Rabo bank - representing EPC
SIA S.p.A.
TAS Group
Thales – representing Smart Payment Association
Vipps
Visa
W3C
Eurosystem – as observer



European Central Bank (ECB) – as observer

European Commission – as observer

Table 98: The multi-stakeholder group MSCT

The multi-stakeholder group further wishes to thank EMVCo and ETSI Smart Secure Platform (SCP) for their contributions delivered as input to this document.

The multi-stakeholder group wishes to inform that this document is provided "as is" without warranty of any kind, whether expressed or implied, including, but not limited to, the warranties of merchantability and fitness for a particular purpose. Any warranty of non-infringement is expressly disclaimed. Any use of this document shall be made entirely at the user's own risk, and neither the multi-stakeholder group nor any of its members shall have any liability whatsoever to any implementer for any damages of any nature whatsoever, directly or indirectly, arising from the use of this document, nor shall the multi-stakeholder group or any of its members have any responsibility for identifying any IPR.

End of Document
