European Payments Council

Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance

Table of Contents

List of Tables

List of Figures

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 the setting-up of a multi-stakeholder group covering the various sectors involved in the MSCT ecosystem to develop this document and to address the interoperability issues. The present version of this document has been produced following a public consultation in Q2-Q3 2019.

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 in 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/beneficiary acknowledgements and notification messages it focuses on the technology and security used in the customer-to-ASPSP space, since the SCT Instant and SCT transactions as such have already been specified in the respective rulebooks (see [13] and [19]). It furthermore specifies various security guidelines for MSCTs (e.g. MSCT app, CDUVM, etc.). Finally, the document identifies the main interoperability issues and barriers detected 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 17).

These include:

- the standardisation of beneficiary/transaction data between the payer and beneficiary, e.g. by the specification of an MSCT QR-code, enabling multiple payment contexts;

- the development of a dedicated infrastructure to interconnect the different MSCT providers notably for the support of token/proxy-based MSCTs and MSCT confirmation and notification messages to customers (payers and beneficiaries);

- 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 scheme" to which the (existing) MSCT providers would participate to ensure interoperability of MSCT services.

Regarding the SEPA Proxy Lookup (SPL) scheme that has been developed for the support of P2P MSCTs, it should be noted that today it covers a mobile phone number as proxy for the beneficiary and only mandates to return the beneficiary's IBAN for the mobile phone number. However the beneficiary'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 by the new multi-stakeholder group on this topic [18] will complement the current document and will further contribute to the customer adoption of MSCTs.

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 18);

- Certain unclarities in European rules and regulations (e.g.; PSD2 [2], RTS [3] and GDPR [4]), also related to their interplay (see chapter 8).

The multi-stakeholder group has organised focused work on the interoperability issues through a dedicated technical expert work-stream. Note that also the ERPB has established a working group for instant payments at POI that further looked into the major challenges for this type of payments.

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.

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 Instant, 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 Instant 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-beneficiary 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 provides an overview on MSCT standards, specifications and white papers;
- Chapter 17 discusses MSCT interoperability aspects;
- Chapter 18 provides an overview of additional challenges and opportunities;
- Chapter 19 includes the conclusions;
- Annex 1 provides an overview of relevant regulatory documents;
- Annex 2 provides an overview of characteristics of the MSCT use cases presented in chapter 6;
- Annex 3 gives an overview of the different organisations 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.

N°	Title	Issued by
[1]	Guideline for user-friendly payment terminals	Dutch National Forum on the Payment System
[2]	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	EC
[3]	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")	EC
[4]	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	EC
[5]	ECB/EuroSystem Assessment guide for the security of internet payments	ECB
[6]	ECSG001-17: SEPA Cards Standardisation Volume	ECSG
[7]	EMV® QR-code Specification for Payment Systems (EMV QRCPS) - Merchant - Presented Mode	EMVCO
[8]	EMV® Contactless Mobile Payment – Software- based Mobile Payment (SBMP) Security Requirements	EMVCo
[9]	EMV® SBMP Security Evaluation Process	EMVCo
[10]	EMV® Consumer Device Cardholder Verification Method – Solution Evaluation and Registration	EMVCo
[11]	EMV® Consumer Device Cardholder Verification Method Security Requirements	EMVCo
[12]	EMV® Consumer Device Cardholder Verification Method— Best Practices	EMVCo
[13]	EPC125-05: SEPA Credit Transfer Scheme Rulebook	EPC
[14]	EPC115-06: SEPA Credit Transfer Scheme Interbank Implementation Guidelines	EPC

[15]	EPC342-08: Guidelines on algorithms usage and key management	EPC
[16]	EPC492-09: White paper Mobile Payments	EPC
[17]	EPC163-13: White Paper Mobile Wallet Payments	EPC
[18]	EPC 251-18: Terms of Reference – Request-to-Pay Multi-Stakeholder Group (RTP MSG)	EPC
[19]	EPC004-16: SEPA Instant Credit Transfer Scheme Rulebook	EPC
[20]	EPC122-16: SEPA Instant Credit Transfer Scheme Interbank Implementation Guidelines	EPC
[21]	EPC211-18: 2018 Payment Threats and Fraud Trends Report	EPC
[22]	EPC250-18: The SEPA Proxy Lookup (SPL) Scheme Rulebook	EPC
[23]	ERPB Final report on Mobile and card-based contactless proximity payments (https://www.ecb.europa.eu/paym/retpaym/shared/pdf/4th-ERPB-meeting/2015-11-26_4th-ERPB_item_6_ERPB_CTLP_working_group_final_report.pdf?726f67769d37722de341702fe5f2387a)	ERPB
[24]	Report from the EPC EIPP multi-stakeholder group (https://www.ecb.europa.eu/paym/retpaym/shared/pdf/10th-ERPB-meeting/Report_from_the_EIPP_Multi_-_Stakeholder_Group.pdf?6fb4e75198566ea357712e02fad3a58e)	ERPB
[25]	ETSI TS 103 465: Smart Cards; Smart Secure Platform (SSP); Requirements Specification – to be published	ETSI
[26]	Towards a better payment experience	Eye Association Netherlands
[27]	FIDO Privacy White paper (Jan. 2016)	FIDO Alliance
[28]	FIDO & PSD2 – Meeting the needs for Strong Customer Authentication (2017)	FIDO Alliance
[29]	FIDO Authentication and the General Data Protection Regulation (GDPR) (May 2018)	FIDO Alliance
[30]	FIDO for PSD2- Providing for a satisfactory customer journey (Sept. 2018)	FIDO Alliance
[31]	GPD_SPE_009: TEE System Architecture	GlobalPlatform
[32]	GPD_SPE_042: TEE TUI Extension: Biometrics API	GlobalPlatform
[33]	GPS_GUI_006: End-to-End Simplified Service Management Framework for payment	GlobalPlatform
[34]	GSMA TS.26: NFC Handset Requirements	GSMA
[35]	GSMA TS.27: NFC Handset Test Book	GSMA

[36]	GSMA SGP.21 RSP Architecture	GSMA
[37]	GSMA SGP.22 RSP Technical specification	GSMA
[38]	NFC Functions and Security Certification overview	GSMA
[39]	HCE and Tokenisation for Payment Services - Discussion paper	GSMA / Consult Hyperion
[40]	The Mobile Economy 2018	GSMA
[41]	RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3	IETF
[42]	ISO 9362: Business Identifier Code (BIC)	ISO
[43]	ISO 13616: Financial services - International Bank account number (IBAN) -- Part 1: Structure of the IBAN	ISO
[44]	ISO 20022: Financial Services – Universal Financial Industry Message Scheme	ISO
[45]	ISO 12812: Core banking - Mobile financial services - Parts 1-5	ISO
[46]	ISO/IEC 14443: Identification cards - Contactless integrated circuit(s) cards - Proximity cards – Parts 1-4	ISO
[47]	ISO/IEC 18004: Information technology -- Automatic identification and data capture techniques -- QR-code bar code symbology specification	ISO
[48]	ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems -- Near Field Communication - Interface and Protocol (NFCIP-1)	ISO
[49]	World Telecommunication/ICT Indicators Database 2018 (https://www.itu.int/pub/D-IND-WTID.OL-2018)	ITU
[50]	White Paper - Alternatives for Banks to offer Secure Mobile Payments	Mobey Forum
[51]	Mobile wallet – Parts 1-5	Mobey Forum
[52]	The Host Card Emulation in Payments - Options for Financial Institutions	Mobey Forum
[53]	Biometrics in Payments – Touching convenience	Mobey Forum
[54]	NFC Activity Technical Specification	NFC Forum
[55]	NFC Digital Protocol Technical Specification.	NFC Forum
[56]	NFC Controller Interface (NCI) Specifications	NFC Forum
[57]	NFC Analog Technical Specification	NFC Forum
[58]	Vetting the Security of Mobile Applications, NIST. Draft NIST Special publication 800-163, Revision 1, July 2018	NIST

	(https://csrc.nist.gov/CSRC/media/Publications/sp/800-163/rev-1/error/documents/sp800-163r1-draft.pdf)	
[59]	OMTP Trusted Environment TR0 v1.2 (https://www.gsma.com/newsroom/all-documents/omtp-documents/omtp-documents-1-2-omtp-trusted-environment-omtp-tr0-v1-2/)	OMTP
[60]	OMTP Security Threats on Embedded Consumer Devices v1.1 (https://www.gsma.com/newsroom/all-documents/omtp-documents/omtp-documents-1-1-omtp-security-threats-on-embedded-consumer-devices-v1-1/)	OMTP
[61]	OMTP Advanced Trusted Environment TR1 v1.1 (https://www.gsma.com/newsroom/all-documents/omtp-documents/omtp-documents-1-1-omtp-advanced-trusted-environment-omtp-tr1-v1-1/)	OMTP
[62]	Open Banking Customer Experience Guidelines, version 1.0, September 2018 (https://www.openbanking.org.uk/wp-content/uploads/Customer-Experience-Guidelines.pdf)	Open Banking
[63]	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
[64]	OWASP Code Review Guide, Version 2.0, July 2017 (https://www.owasp.org/images/7/78/OWASP_AlphaRelease_CodeReviewGuide2.0.pdf)	OWASP
[65]	OWASP Mobile Application Security Verification Standard (MASVS), Version 1.1, July 2018 https://github.com/OWASP/owasp-masvs	OWASP
[66]	OWASP Mobile Security Testing Guide (MSTG). Version 1.1, 2018 (https://github.com/OWASP/owasp-mstg)	OWASP
[67]	OWASP Testing Guide. Version 4.0, 2014 (https://www.owasp.org/images/1/19/OTGv4.pdf)	OWASP
[68]	PCI Payment Application Data Security Standard, PA DSS, Version 3.2, May 2016	PCI
[69]	Biometrics in Payment https://www.smartpaymentassociation.com/images/easyblog_articles/_18-05-15_SPA-Biometrics-For-Payments.pdf	Smart Payment Association
[70]	STET PSD2 API V1.4, January 2019	STET

	(https://www.stet.eu/assets/files/PSD2/1-4-1/api-dsp2-stet-v1.4.1.3-part-3-interaction-examples.pdf)	
[71]	Joint Initiative on a PSD2 Compliant XS2A Interface - NextGenPSD2 XS2A Framework Implementation Guidelines (https://www.berlin-group.org/nextgenpsd2-downloads)	The Berlin Group
[72]	Digital Payments Solutions Industry Considerations (http://www.theukcardsassociation.org.uk/wm_documents/Digital%20Wallets%20-%20Industry%20Considerations%20Outline.pdf)	The UK Cards Association
[73]	W3C Web Authentication: An API for accessing Public Key Credentials (https://www.w3.org/TR/webauthn/)	W3C
[74]	W3C Payment Request API (https://www.w3.org/TR/payment-request/)	W3C
[75]	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 [2], [13] and [19].

Term	Definition
Account Servicing Payment Service Provider (ASPSP)	A PSP providing and maintaining a payment account for a payer (see [2]).
Account statement information	The information on the SCT payment (for the data elements to be provided, see [13], [19]) available to the Beneficiary on the basis agreed between the Beneficiary and their Beneficiary 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.[1] (see ISO 12812 – Part 1 [45])
Authentication Application	An application accessed through the mobile device performing the functions related to a user authentication, as dictated by the Authentication Service Provider.
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: - 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 [58]).
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 [2].
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 [45]). In case the user is a cardholder this is also referred to as Consumer Device Cardholder Verification Method (CDCVM – see [6]).
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 [46]).
Credential(s)	Payment account related data that may include a code (e.g., mobile code), provided by the PSP to their customer for authentication purposes.
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 [2]).
Credit Transfer instruction	An instruction given by an Originator to an Originator ASPSP requesting the execution of a credit transfer transaction, comprising such

[1] Note that the PSD2 [2] 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.

	information as is necessary for the execution the credit transfer and is directly or indirectly initiated in accordance with the provisions of [2].
Credit Transfer Transaction	An instruction executed by an Originator ASPSP by forwarding the Transaction to a CSM for forwarding the transaction to the Beneficiary ASPSP.
Customer	A payer or a beneficiary which may be either a consumer or a business (merchant).
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 [2].
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 beneficiary	A means of uniquely identifying the beneficiary 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 [22]).
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(ly)	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 [20]).
Intermediary PSP	A PSP which is neither that of the Originator nor that of the Beneficiary and who participates in the execution of a credit transfer (see section 3.4 in [13]).
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 [43]).
Merchant	A beneficiary 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 Instant or MSCT transaction as specified by the MSCT service provider in accordance with the SEPA SCT Instant or SCT scheme.
MSCT Application user interface	The user interface of a mobile payment application.
MSCT Service Provider	A service provider that offers an MSCT service to a payer and/or beneficiary based on a SCT Instant or SCT payment transaction. This may involve the provision of an 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 an ASPSP, a mobile P2P payment service provider or any party acting as a PISP.

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 [56]) are based on ISO/IEC 18092 [48] but have been extended for harmonisation with EMVCo and interoperability with ISO/IEC 14443 [46].
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 [2]) (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 [2]).
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 [2]).
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 [2].

Payment Service Provider (PSP)	An entity referred to in Article 1(1) of [2] or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33 of [2].
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 [2]).
Payment transaction	An act, initiated by the payer or on his/her behalf or by the payee (beneficiary), of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee (as defined in [2].
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 [4]).
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.).
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 beneficiary to claim an amount of money from a payer for a specific transaction (see [18]).

Request-to-Pay message	Message sent by the Beneficiary to the Payer, directly or through agents. It is used to request the movement of funds from the payer account to the beneficiary account.
Reservation of the Amount	The Originator Bank Instantly, (i) either reserves the amount of the SCT Inst Instruction on the Originator's Payment Account with this information being Instantly accessible to the Originator, (ii) or Immediately debits the amount of the SCT Inst Instruction from the Originator's Payment Account; in both instances the Originator 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 [22]).
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 [3]).
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 Originator, see section 4.4 in [13] and/or section 4.3.2 in [20].
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 [2]).
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 [13]).
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 [19]).
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 [22]).
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 Originator ASPSP and Beneficiary 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 [2]).
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 [2]).
Tokenisation	Process of substituting payment account or transaction related data with a surrogate value, referred to as a token.
Token	Tokens can take on a variety of formats across the payments industry. They generally refer to a surrogate value for payment account 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.
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 [31] 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 [45].

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
EBA	European Banking Authority
EC	European Commission
ECSG	European Cards Stakeholders Group
EIPP	Electronic Invoice Presentment and Payment
EPC	European Payments Council
ERP	Enterprise Resource Planning
ERPB	Euro Retail Payments Board
eSE	Embedded Secure Element
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
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS
HSM	Hardware Security Module
IBAN	International Bank Account Number
ID	Identifier
ICT	Information and Communication Technology
IRP	Initiator Registry Provider
IPR	Intellectual Property Rights
iSE	Integrated Secure Element
ISO	International Organization for Standardization
ISP	Information Service Provider
LCM	Lifecycle Management
MA	Mobile Application
MACP	Mobile Application Cloud Platform
ME	Mobile Equipment
MNO	Mobile Network Operator

MSCT (Instant)	Mobile initiated SCT (or SCT Instant)
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
PISP	Payment Initiation Service Provider
POI	Point of Interaction
POS	Point of Sale
PSD	Payment Services Directive
PSP	Payment Service Provider
QR code	Quick Response code
RBA	Risk-Based Authentication
REE	Rich Execution Environment
RFID	Radio Frequency Identification
RRP	Responder Registry Provider
RSP	Remote SIM Provisioning
RTP	Request-To-Pay
RTS	Regulatory Technical Standard
SCT	SEPA Credit Transfer
SE	Secure Element
SEPA	Single Euro Payments Area
SIM	Subscriber Identity Module
SP	Service Provider
SPL	SEPA Proxy Lookup
SSL	Secure Sockets Layer
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
XML	Extensible Markup Language

Table 3: Abbreviation

1.5 Maintenance Process

The EPC has established a dedicated multi stakeholder group (see Annex 1: Overview regulatory documents) for the development of this document. The present version has been produced following a public consultation. 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 March 2017, the EPC published the last edition of a white paper [16], which provides a high-level description of mobile payments in general covering mobile proximity and mobile remote payments, including those based on SEPA credit transfers.

This new document is intended for readers who require more detail on guidance for mobile initiated SEPA (instant) credit transfers (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.

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/beneficiary acknowledgements and notification messages, it focuses on the technology and security used in the customer-to-ASPSP space, since the SCT Instant and SCT transactions as such have already been specified in the respective rulebooks (see [13] and [19]). It furthermore specifies various security guidelines for MSCTs (e.g. MSCT app, CDUVM, etc.). Finally, the document discusses the main interoperability issues and barriers identified for MSCTs.

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 (e.g., consumer) and beneficiary (e.g., payee, merchant) 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 consumer devices and POIs;
- Wide availability and usability of appropriate POI equipment and consumer 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.

2.3 Scope

The guidance focuses on interoperability between the different stakeholders involved in the MSCT ecosystem. In particular, they address the 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 [19] and [13]) are the underlying SEPA payment instrument[2].

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

A description of MSCT use cases;

- The MSCT transaction aspects outside the interbank space and the impact of new rules and regulations (PSD2 [2] and RTS [3] , GDPR [4]);
- The roles of the main stakeholders in the MSCT ecosystem;
- Lifecycle management aspects for MSCTs;
- Risk and security aspects related to MSCTs;
- Interoperability aspects for MSCTs;
- 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] Note that the use cases and service models introduced in these guidelines may also be applied outside SEPA.

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: Overview regulatory documents).
- Describe how MSCTs can be implemented while maintaining appropriate methodologies for risk management, supporting adaption to prevent fraud.
- Identify barriers to achieving an adequate level of interoperability for MSCTs.
- Strive for a harmonised customer experience across SEPA for MSCTs at the POI.
- Enhance the security and trust in MSCTs.
- Provide guidance for the implementation of MSCTs which is complementary to the SCT and SCT Instant rulebooks (see [19] and [13]) and to the standards developed by standardisation and industry bodies in the MSCT ecosystem (see chapter 16).

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;
- Merchants and merchant organisations;
- Consumers;

- 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 [16]) with a special emphasis on MSCTs.

1. To support the need for SEPA interoperability, the usage of SCT or SCT Instant as specified in the respective rulebooks (see [13] and [19]) is assumed.

2. The service models as described in chapter 4 and infrastructures used for SCT and SCT Instant 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 end-customers (payers and beneficiaries), 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 beneficiaries) payment liabilities should be clear, and in line with applicable regulations (see Annex 1: Overview regulatory documents).

8. PSPs should have the possibility to develop MSCT services on all the common mobile platforms[3] in the market openly.

9. The mobile device interface / wallet provider should enable the MSCT service provider to define the graphical interface to the consumer for its 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 devices[4] and should not be bound to a specific MNO.

[3] Combination of different hardware and software on a mobile device.
[4] 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 device[5].

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: Overview regulatory documents**Error! Reference source not found.**).

[5] subject to appropriate agreements.

4 SCT Instant 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 [19], [20] and [21] and [13] and [14] respectively.

4.2 SCT Instant scheme

An SCT Inst is a payment instrument for the execution of instant credit transfers in euro between customer payment accounts in SEPA. The SCT Inst is executed on behalf of the Originator holding a payment account with an Originator ASPSP in favour of a Beneficiary holding a payment account with a Beneficiary ASPSP.
The execution of an SCT Inst payment involves four main actors:

- **The Originator:** is the customer who initiates directly or indirectly[6] the instant credit transfer by providing the Originator ASPSP with an instruction. The funds for such an SCT Inst are reserved from a specified payment account of which the Originator is account holder.

- **The Originator ASPSP**: is the participant that receives the SCT Inst Instruction from the Originator and acts on the payment instruction by processing instantly the payment to the Beneficiary ASPSP in favour of the Beneficiary's Payment Account according to the information provided in the instruction and in accordance with the provisions of the Scheme. The Originator ASPSP is also obliged to inform immediately the Originator in case the funds have not been made available to the Beneficiary.

- **The Beneficiary ASPSP**: is the participant that receives the SCT Inst transaction from the Originator ASPSP and immediately makes the funds available to the Beneficiary, according to the information provided in the transaction and in accordance with the provisions of the Scheme. The Beneficiary ASPSP is also obliged to send a confirmation message (positive or negative) immediately through the same CSM to the Originator Bank to confirm whether the SCT Inst transaction has been accepted and funds have been made available immediately to the Beneficiary (positive confirmation) or not (negative confirmation).

Note: The Originator ASPSP and Beneficiary ASPSP may be one and the same participant.

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

[6] In compliance with the Payment Services Directive (see [2].

Originator ASPSPs and Beneficiary ASPSPs are responsible for meeting their obligations under the SCT Instant rulebook [19].

The operation of the Scheme also involves other parties indirectly:

- **CSMs**: Such mechanisms could include the services of a Clearing and Settlement provider such as an automated clearing house or other mechanisms such as intrabank 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 Originator and/or Beneficiary ASPSPs, for example in cases where they are not themselves direct participants in a CSM.
- **Payment initiation service providers (PISP):** Originators may make use of a PISP to initiate an instant credit transfer.

An SCT Instant payment under the SCT Instant Scheme consists of the following steps as specified in [19] and illustrated in the figure below.

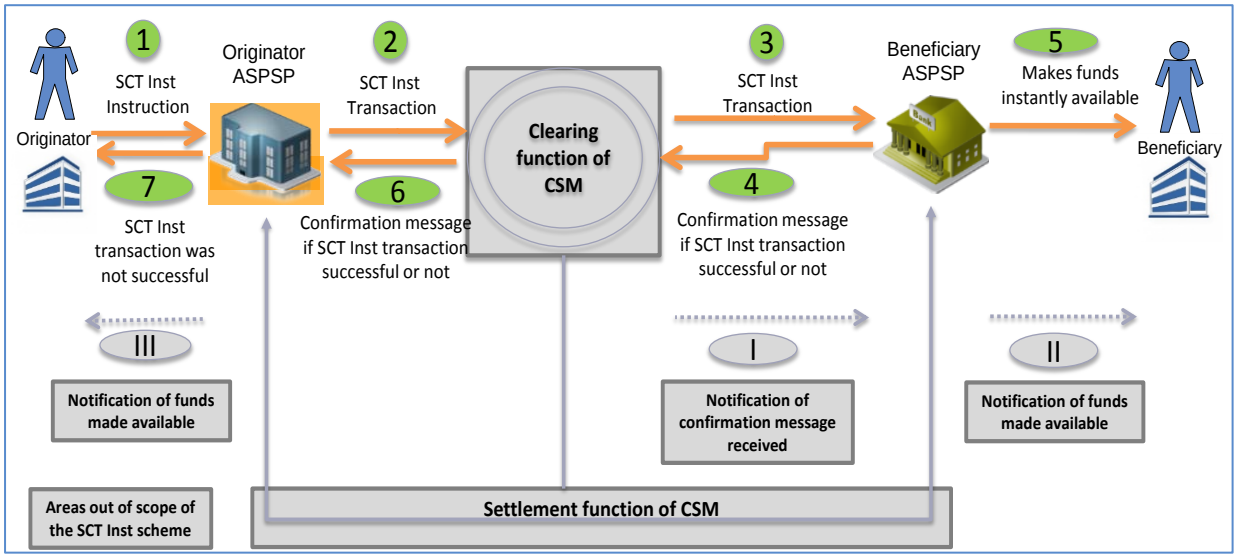


Figure 1: Overview SCT Instant transaction process flow

Note: 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 Originator ASPSP receives an SCT Inst instruction from the Originator[7].
The Originator ASPSP then instantly executes all processing conditions and Funds availability checks. When these validation checks are successful, the Originator ASPSP *instantly* makes a

[7] Directly or indirectly initiated in compliance with the Payment Services Directive 2 (PSD2)

"Reservation of the Amount"[8] on the Originator's payment account with this information *instantly* accessible to the Originator, *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 Originator ASPSP *instantly* sends the SCT Inst transaction message to the CSM of the Originator ASPSP. Via this message, the Originator ASPSP gives the authorisation to the CSM of the Originator 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 Originator ASPSP *instantly* reserves funds from the Originator ASPSP as settlement cover for the SCT Inst transaction. The CSM of the Originator ASPSP *instantly* sends the SCT Inst transaction to the CSM of the Beneficiary ASPSP.

Step 3: the CSM of the Beneficiary ASPSP *instantly* sends the SCT Inst transaction message to the Beneficiary ASPSP.
For the Beneficiary ASPSP, this message under step 3 implies that the Beneficiary ASPSP has *settlement certainty* for this SCT Inst transaction in case the Beneficiary ASPSP accepts the transaction for further processing.
The Beneficiary ASPSP *instantly* verifies if it can apply the SCT Inst transaction to the Beneficiary's payment account and executes various validation checks.

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

[8] See chapter 7 in [20] for the definition of "Reservation of the Amount"

- The CSM of the Beneficiary ASPSP initiates the final settlement processing for this specific SCT Inst Transaction with the CSM of the Originator ASPSP.

Step 5: only when the Beneficiary ASPSP has sent a positive confirmation via the message in step 4 *and* the Beneficiary ASPSP has the *certainty* that the message under step 4 has been *successfully delivered* to the CSM of the Beneficiary ASPSP, it *instantly makes the funds available* to the Beneficiary. The Beneficiary 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 Beneficiary. This action means that the Beneficiary has immediate use of the funds subject to the terms and conditions governing the use of the payment account of the Beneficiary.

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

Step 6: the CSM of the Originator ASPSP Instantly reports to the Originator 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 Originator ASPSP had received via the CSM of the Beneficiary ASPSP.

Step 7: in case the Originator ASPSP receives a negative confirmation about the SCT Inst transaction which indicates that t*he funds have not been made available* to the Beneficiary, the Originator ASPSP is *obliged* to *immediately* inform the Originator. The Originator ASPSP lifts the "Reservation of the Amount" made in step 1.

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

If agreed with the Originator, the Originator ASPSP informs the Originator about the *funds made available* to the Beneficiary. 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 Originator ASPSP and the Beneficiary ASPSP, and as such credited by the CSM to the Beneficiary ASPSP during the settlement process.

For the exception handling related to SCT Instant payments and the *"R-transactions"*, the reader is referred to section 4.3.2 in [20].

4.3 SCT Scheme

A SEPA Credit Transfer is a payment instrument for the execution of credit transfers in euro between customer 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 [13] and illustrated in the figure below.

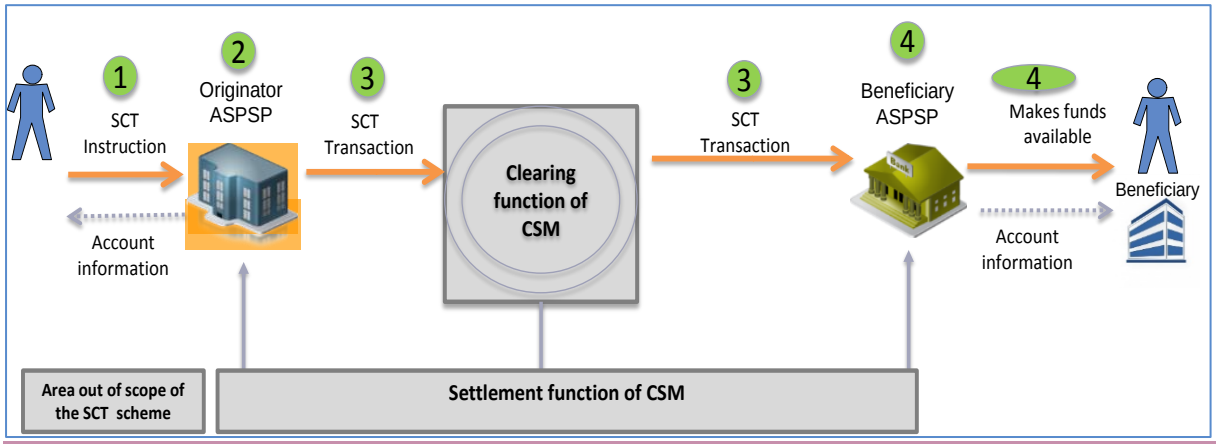


Figure 2: Overview SCT transaction process flow

Note: **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 Originator[9] completes and forwards the Credit Transfer Instruction. The instruction will be submitted by any means agreed between the Originator and the Originator ASPSP. The data elements to be provided are defined in [13].

Step 2: The Originator 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 PSD2[10].

[9] Directly or indirectly initiated in compliance with the Payment Services Directive 2 (PSD2)

[10] The "Requested Execution Date" corresponds with a date requested by an Originator for commencing the execution of the Credit Transfer Instruction. The Originator may choose to request a Requested Execution Date in the future and submit the Credit Transfer Instruction to the Originator ASPSP in accordance with its Terms and Conditions with the Originator 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 Originator ASPSP will debit the account of the Originator[11]. This will be followed by the sending of the Credit Transfer Instruction to ensure receipt by the Beneficiary ASPSP via the selected CSM in accordance with the rules of the Scheme. The data elements to be provided are defined in [13].

Step 4: The Beneficiary ASPSP should credit the account of the Beneficiary in accordance with the provisions of the PSD2 [2]. The Beneficiary ASPSP will make the information on the SCT payment (for the data elements to be provided, see [13]) available to the Beneficiary on the basis agreed between the Beneficiary and their Beneficiary 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 [13] 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 Originator instructs the Originator ASPSP, for the purposes of the Scheme, the Originator ASPSP need only inform the Originator of the reason.

A *"Return"* occurs when a credit transfer is diverted from normal execution after interbank settlement, and is sent by the Beneficiary ASPSP to the Originator 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 Beneficiary 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 Beneficiary's account has already been credited and the Beneficiary wishes to return the funds. Instead, the procedure of initiating a new Credit Transfer applies.

A *"Recall"* occurs when the Originator ASPSP requests to cancel a SEPA Credit Transfer. The Recall procedure must be initiated by the Originator 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 Originator ASPSP, which may do it on behalf of its customer. Further details on the reasons for a Recall may be found in 4.3.2.2 in [13].

A *"Request for Recall by the Originator"* can be initiated by the Originator ASPSP after an Originator has requested the Originator ASPSP to reverse a settled credit transfer for a reason

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

other than duplicate sending, technical problems resulting in erroneous Credit Transfer(s) and a fraudulently originated Credit Transfer.

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 [13].

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

MSCT transactions are SCT Instant or SCT transactions that are initiated by the payer (the originator) using a mobile device. They are based on the existing SCT Instant or SCT rulebooks (see [19] and [13] respectively) in the so-called "interbank 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 Instant or SCT transaction, besides some features of the mobile device such as the support of CDUVM, the mobile device screen to display transaction information, etc. Therefore, this document will mainly focus on the interactions outside the interbank space such as between the mobile device and the POI, between the payer and their MSCT service provider, between the merchant and their MSCT service provider, etc. (see also Figure 1 and Figure 2).

5.3 MSCT Provisioning and life cycle management

For MSCTs, the hosting of a dedicated MSCT application in 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 "main memory", 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.

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 beneficiary related to a SCT Instant or SCT payment transaction. This typically involves the provision of an MSCT application for download on the customer'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 beneficiary's ASPSP (this linkage includes both technical and contractual aspects). Note that a PSP 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 transaction data such as the IBAN, merchant identifier or merchant transaction identifier (see section 10.4). 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.
- The Mobile Wallet Issuer is a service provider that issues mobile wallet functionalities to the customer (consumer or merchant).
- Other relevant new stakeholders include for example:
    - SE providers, if the MSCT 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 suppliers,
    - Mobile equipment manufacturers,
    - 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 [40]). 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[12] with enriched technology and service levels. More in particular in Europe, nowadays, "smart phones" have become ubiquitous[13]. 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 paper 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 presented in chapter 15.

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

Consumers' expectations and demands

- Efficiency: speed of payment initiation, frictionless;
- Convenience and mobility: make cashless payments anywhere, anytime;
- Consistent consumer experience;
- Simplicity for enrolment and to conduct a payment;
- Confidence and trust;
- 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;

[12] The number of active mobile devices and human beings crossed over somewhere around the 7.19 billion mark (see http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html)
[13] See https://www.statista.com/statistics/494554/smartphone-users-in-western-europe/

- Resilience (zero downtime);
- Cost effectiveness;
- Consumer focused: The payment process needs to be a convenient, simple process, 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 immediate release of goods or services to the consumer;
- Desire for cash displacement and in some countries paper cheque displacement;
- Reachability of consumers through any mobile device (interoperability);
- Easy to implement and quick to market;
- Standardisation of reporting from the ASPSP to the merchant to enable transaction and account statement reconciliation.
- 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: Overview regulatory documents).

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 [45]:

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 activation[14] 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;

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;

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

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, t*he 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.

Payment context	Card-based	Account-based (SCT or SCT Instant)
Person-to-Person (P2P)		

• Mobile banking
  ○ Browser
  ○ Dedicated application
• Dedicated P2P application
	• EPC White paper mobile payments (EPC492-09)	• EPC White paper mobile payments (EPC492-09)
		• MSCT IG

Consumer-to-Business (C2B) or Business-to-Business (B2B)		
m-Commerce[15] • Browser-based (on mobile device) • Dedicated MSCT application • App-to-App • In-App	• EPC White paper mobile payments (EPC492-09)	• EPC White paper mobile payments (EPC492-09) • MSCT IG
Proximity payments (physical interaction) • NFC • QR-codes • BLE • …….	• MCP IG (EPC144-17v1.0) • White paper non-NFC mobile SEPA card proximity payments (awaiting publication by the EPC)	• EPC White paper mobile payments (EPC492-09) • MSCT IG

Table 4: Overview mobile payments

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

[15] Currently, e-commerce (purchase via e.g. merchant webpage on PC) whereby the payment is initiated through the payer's mobile device is not considered.

In this chapter, MSCT use cases will be described as they appear in the market today, with a diagram depicting the different actors involved and a description of the different steps 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.

Payment context	Use case description
Person-to-Person (P2P) payments	1. Mobile device – mobile banking via browser – static customer authentication with on-line passcode
	2. Mobile device – MSCT application – proxy – strong customer authentication involving a mobile code
	3. Mobile device – payment request message via messaging application – strong customer authentication involving a fingerprint
	4. Mobile device – using proximity between the 2 parties - QR-code generated by dedicated MSCT application by beneficiary – strong customer authentication involving a facial recognition
Consumer-to-Business (C2B) payments	1. Mobile device - Payment of invoice involving a QR-code – strong customer authentication involving a mobile code
	2. Mobile device – Payment at POI involving merchant-presented QR-code – strong customer authentication via MSCT application involving a mobile code
	3. Mobile device – Payment at POI involving merchant-presented QR-code – MSCT application with strong customer authentication using a dedicated authentication application (decoupled app-to-app) involving a fingerprint
	4. Mobile device – m-commerce – merchant application - PISP with redirection to consumer's ASPSP for strong customer authentication involving a dynamic authenticator
	5. Mobile device - m-commerce - mobile browser - PISP with embedded strong customer authentication involving a dynamic authenticator
	6. Mobile device – transport ticketing – in-app payment – strong customer authentication involving a fingerprint
Business-to-Business	1. Mobile device – Request to pay – strong customer authentication involving a mobile code

Table 5: Overview 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.
- Other biometric methods may be used than those mentioned above, see section 8.2.

A more detailed overview on the characteristics of the MSCT use cases presented in the table above is provided in Annex 2 Overview MSCT use cases.

7.2 Person-to-person (P2P) payments

MSCT use case P2P-1: Mobile device – mobile banking via browser – static customer authentication with on-line passcode

This use case presents an example of user experience whereby the payer uses their mobile device to conduct an MSCT (Instant) from their payment account to the payment account of a beneficiary (payee) using a mobile browser.

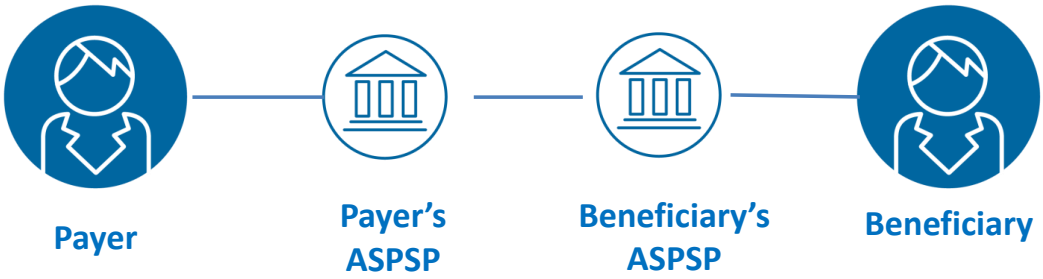


Figure 3: Actors in MSCT use case P2P-1

Payer and beneficiary 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 [2]). Further information on the possible application of exemptions for SCA may be found in section 8.3.

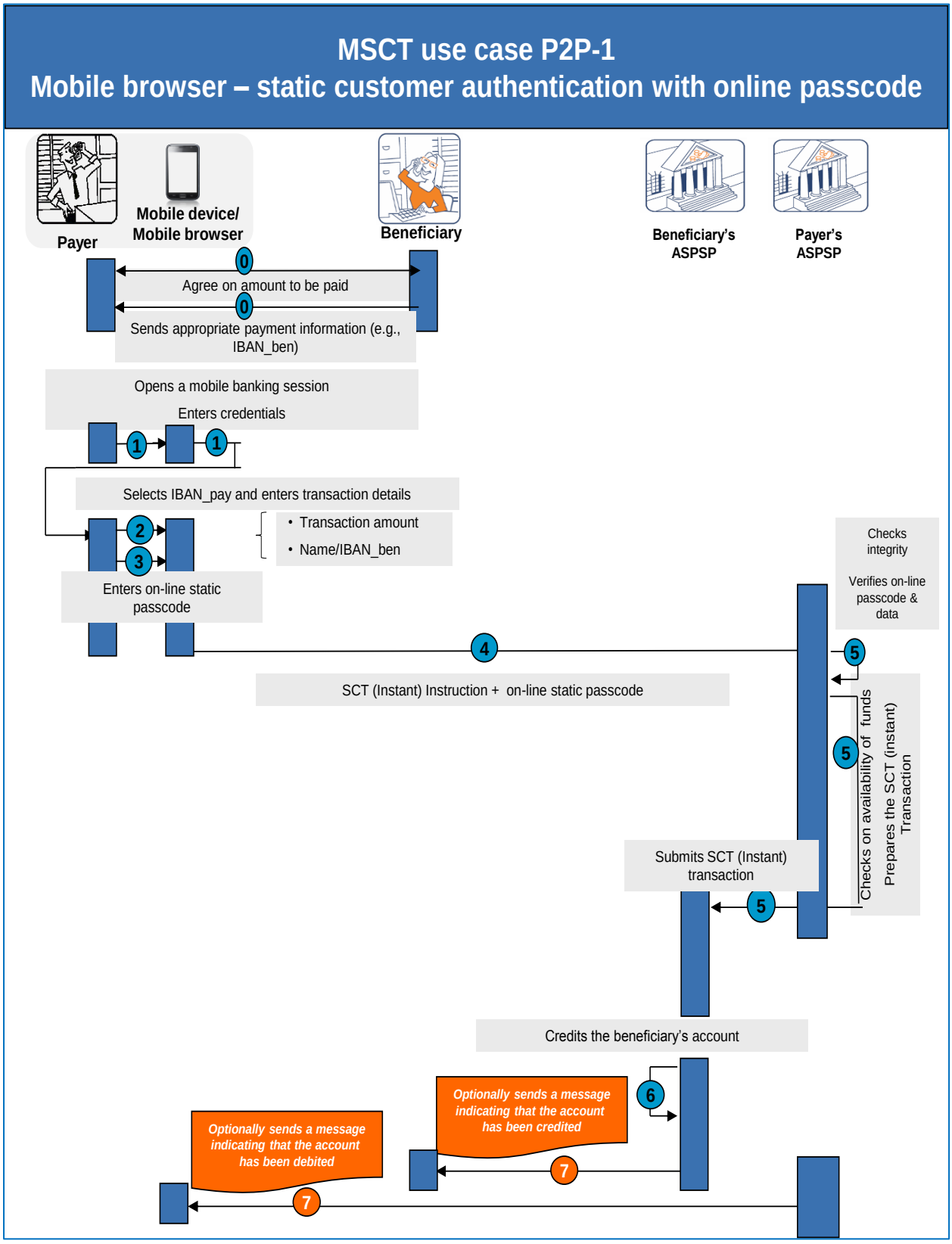


Figure 4: MSCT use case P2P-1

In the figure above, the following steps are illustrated:

Step 0

- The payer and the beneficiary agree upon the amount to be paid to the beneficiary (which is assumed to be low value[16]). Subsequently, the beneficiary 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 user-ID 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_pay) 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 (beneficiary name, IBAN_ben) of the beneficiary's account to be credited; this information can be put in full by the payer or by accessing a pre-registered beneficiary.

and

- Optionally, a value date and remittance data (structured or unstructured).

Step 3

The payer confirms the SCT (Instant) Instruction on the webpage via their mobile device.

Step 4

The SCT (Instant) Instruction including the beneficiary name, the IBAN_ben, 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 (Instant) 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 (Instant) Transaction to the beneficiary's ASPSP.

[16] Exempted from SCA according to Article 16 of the RTS [3].

Step 6

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

Step 7

- The beneficiary is optionally informed by their ASPSP that their account has been credited.
- The payer is optionally informed by their ASPSP that their account has been debited.

Analysis MSCT Use case P2P-1	
Interoperability	• The payer and the beneficiary may have different ASPSPs. • Interoperable in view of SCT and SCT Instant rulebooks.
Challenges	• The beneficiary needs to provide their IBAN to the payer. • Cumbersome for the payer to enter the IBAN of the beneficiary. • 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 information messages in step 7 are not included in the SCT Instant and SCT schemes.

Table 6: Analysis MSCT use case P2P-1

MSCT use case P2P-2: Mobile device – MSCT application – proxy – strong customer authentication 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 (Instant) from their own payment account to the payment account of a beneficiary (payee).

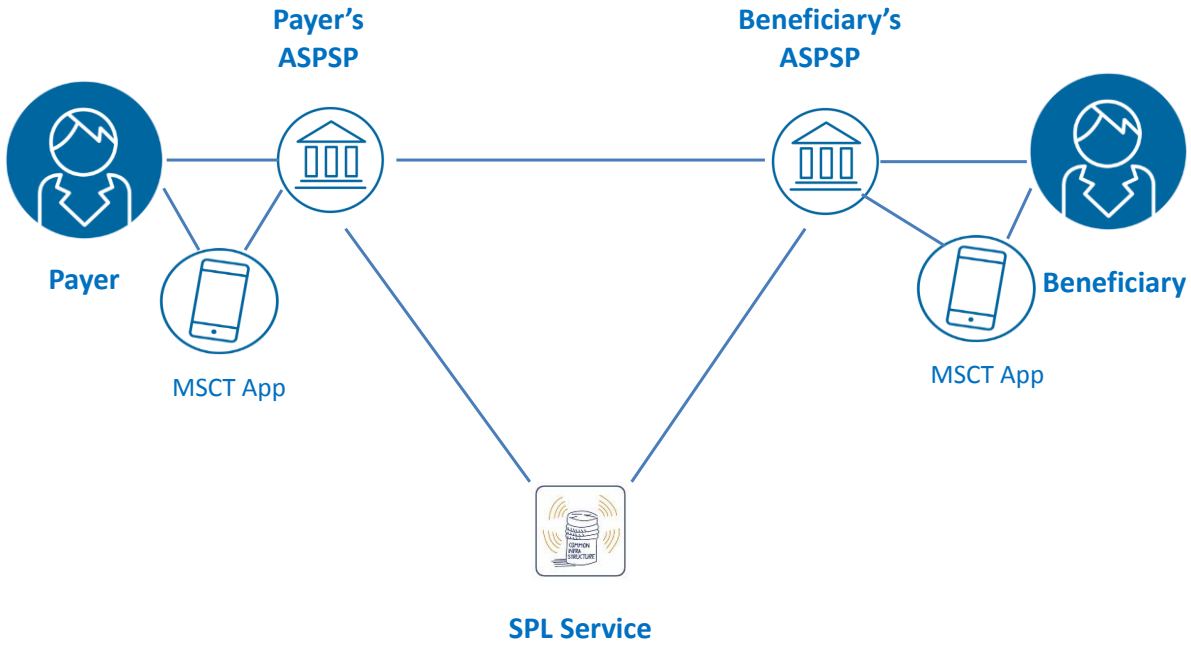


Figure 5: Actors in MSCT use case P2P-2

Payer and beneficiary may, and frequently will, hold their payment accounts with different ASPSPs and have downloaded different MSCT (Instant) applications[17] (so-called mobile P2P applications) from their ASPSP on their mobile device.
A beneficiary proxy (e.g., mobile phone number) will be in place, making the input of the beneficiary details considerably more convenient for the payer. A strong payer authentication (see section 8.3) in accordance to PSD2 [2] is performed, involving the entry of a mobile code by the payer (see section 8.2).
In view of the usage of a proxy, the so-called SEPA Proxy Lookup (SPL) Service is used to link the beneficiary's proxy as to their account details. For more information on the SPL service, the reader is referred to section 15.3.

[17] The MSCT application may also be downloaded from an MSCT service provider. The payer and beneficiary may have different MSCT service providers.

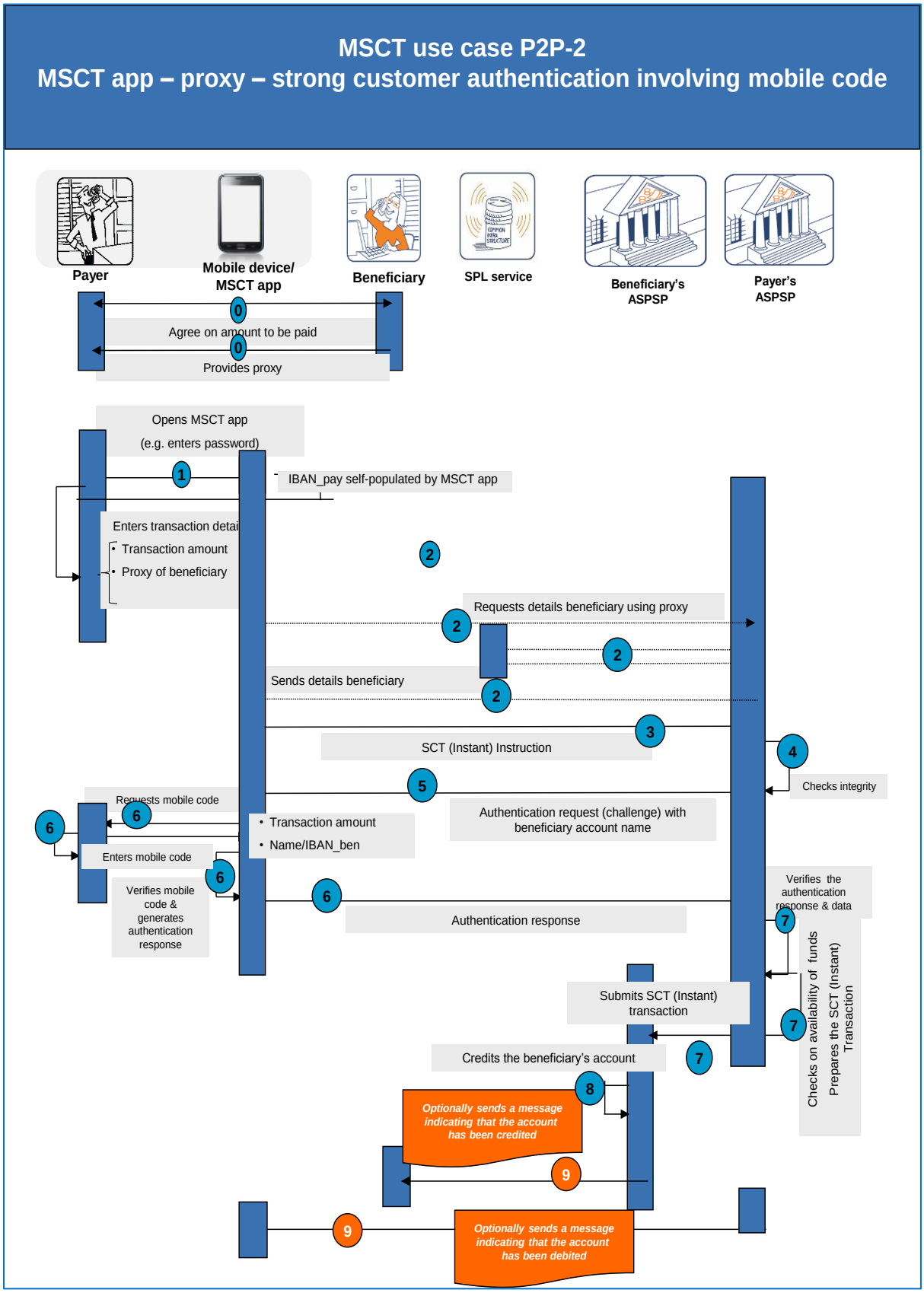


Figure 6: MSCT use case P2P-2

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 (Instant) application[18] from their ASPSP on their mobile device. This MSCT application is typically linked to a specific payer account.
- The beneficiary also needs to be subscribed to the MSCT service and have downloaded a dedicated MSCT (Instant) application from their ASPSP on their mobile device.
- The payer and the beneficiary agree upon the amount to be paid to the beneficiary. The beneficiary provides their proxy (e.g., mobile phone number) to the payer, if not previously known to the payer.
- The payer's ASPSP and beneficiary'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 (Instant) application on their mobile device, which possibly involves the entry of a password.

Step 2

- Once the MSCT (Instant) application is selected, the IBAN_pay is self-populated.
- The payer enters the details of the transaction via their mobile device:
    - The transaction amount,
    - The beneficiary'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 beneficiary.
- The MSCT (Instant) application uses the SPL service to retrieve the beneficiary account data based on the beneficiary's mobile phone number received.

Step 3

The SCT (Instant) Instruction including the beneficiary name, the IBAN_ben and the transaction amount, is transmitted to the payer's ASPSP.

Step 4

The payer's ASPSP checks the integrity of the SCT (Instant) Instruction.

Step 5

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

[18] Typically a mobile P2P application.

Step 6

- The authentication request is handled automatically by the MSCT (Instant) application on the payer's mobile device.
- The beneficiary's name/IBAN_ben 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 (Instant) 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 (Instant) Transaction to the beneficiary's ASPSP.

Step 8

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

Step 9

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

Analysis MSCT Use case P2P-2	
Interoperability	• The payer and beneficiary may have different ASPSPs and different MSCT applications. • The SPL service is needed and both the payer's ASPSP and beneficiary's ASPSP need to be participants in the SPL service (directly or indirectly).
Challenges	• How to handle the cases where the beneficiary's account data could not be retrieved from the SPL service because the beneficiary's ASPSP is not registered in the SPL service. • The information messages in step 9 are not included in the SCT Instant and SCT schemes. • In case of an SCT there is no immediate, irrevocable crediting of the funds. How to inform the beneficiary that the payment has been initiated (after step 8) if we do not have an SCT Instant?

Table 7: Analysis MSCT use case P2P-2

MSCT use case P2P-3: Mobile device – payment request message via messaging application – strong customer authentication involving a fingerprint

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

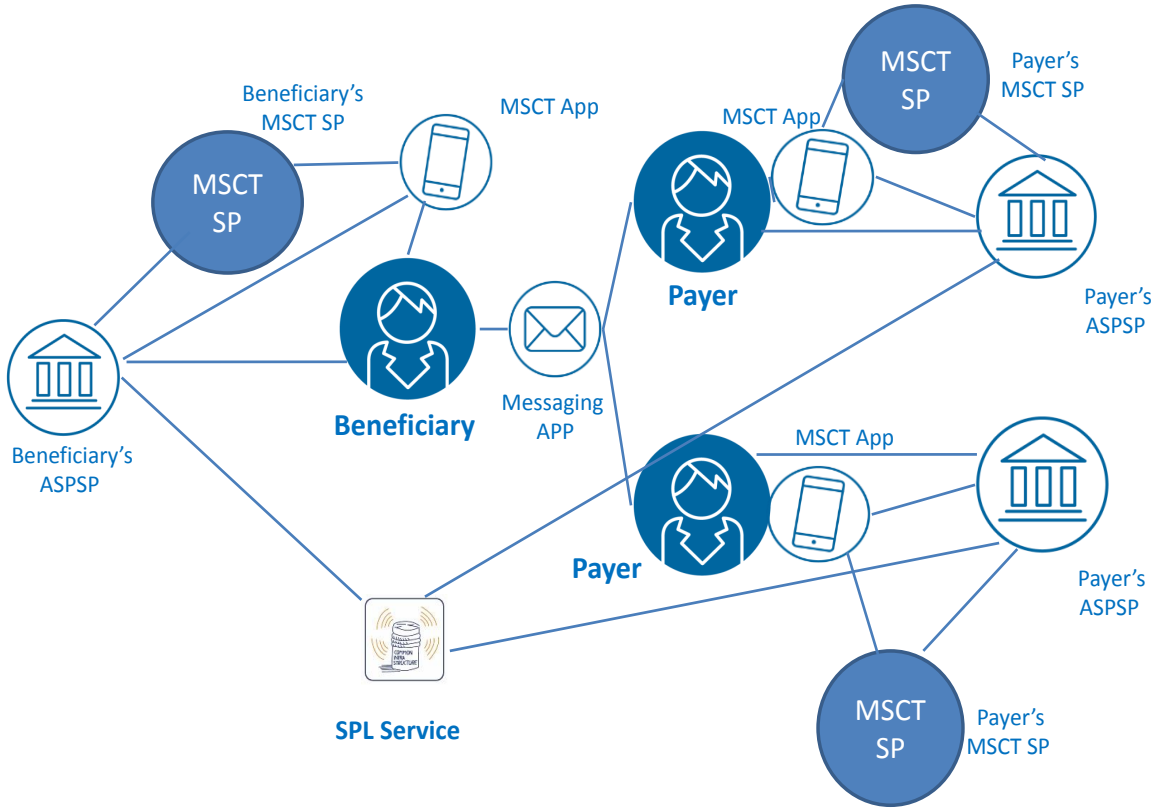


Figure 7: Actors in MSCT use case P2P-3

Payers and beneficiary may, and frequently will, hold their payment accounts with different ASPSPs and have downloaded different MSCT Instant applications from potentially different MSCT service providers. Each ASPSP is a participant in an MSCT Service (not necessarily the same). A strong payer authentication (see section 8.3) in accordance with PSD2 [2] is performed, involving the presentation of a fingerprint[19] by the payer (see section 8.2). In case the MSCT Instant 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.

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

[19] Note that other biometric methods may be used, see section 8.2.

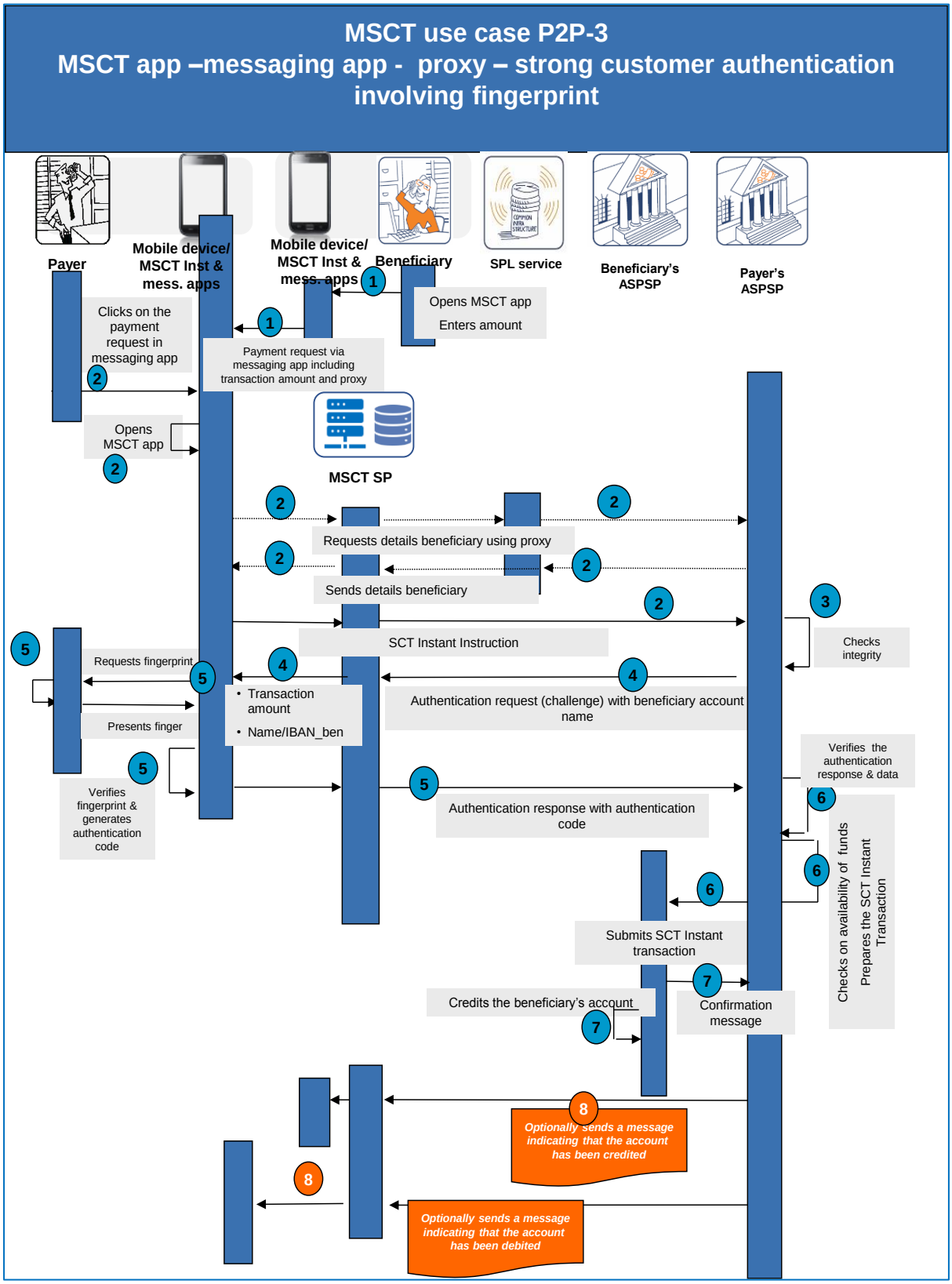


Figure 8: MSCT use case P2P-3

In the figure above, the following steps are illustrated:

Step 0

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

Step 1

- The beneficiary opens their MSCT Instant application on their mobile device and enters the amount to be paid, the split of the amount and a personal message.
- The beneficiary 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 beneficiary.[20]
- The beneficiary can check in their MSCT Instant 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 Instant application of their MSCT service provider. (The selection of the ASPSP has already been done during the registration process).
- The MSCT Instant application uses the SPL service to retrieve the beneficiary account data based on the beneficiary's mobile phone number received.
- The SCT Instant Instruction including the beneficiary name, the IBAN_ben 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 Instant Instruction.

[20] 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 beneficiary's name/IBAN_ben, the transaction amount and a challenge to the MSCT Instant application in the mobile device of the payer via the MSCT service provider.

Step 5

- The authentication request is handled automatically by the MSCT (Instant) application on the payer's mobile device.
- The beneficiary's name/IBAN_ben 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 Instant application[21] 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 Instant Transaction to the beneficiary's ASPSP.

Step 7

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

Step 8

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

[21] In case the MSCT Instant 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.

Analysis MSCT Use case P2P-3	
Interoperability	• All payers and the beneficiary have to be subscribed to the same messaging service provider and use the same messaging application. • All payers and the beneficiary may have different ASPSPs. • All payers and the beneficiary may have different MSCT Service providers and different MSCT applications. • The SPL service is needed and all payer ASPSPs and the beneficiary's ASPSP need to be participants in the SPL service (directly or indirectly).
Challenges	• How to handle the cases where the beneficiary's account data could not be retrieved from the SPL service because the beneficiary's ASPSP is not registered in the SPL network. • Standard for the interface between the messaging application and the MSCT services providers. • The information messages in step 8 are not included in the SCT Instant and SCT schemes. • In case of an SCT there is no immediate, irrevocable crediting of the funds. How to inform the beneficiary that the payment has been initiated (after step 6)?

Table 8: Analysis MSCT use case P2P-3

MSCT use case P2P-4: Mobile device – using proximity between the 2 parties - QR-code generated by dedicated MSCT application by beneficiary – strong customer authentication involving facial recognition

This use cases presents an example of payer experience using their mobile device to pay a beneficiary (e.g. for sharing costs), whereby the details of the beneficiary and the amount to be paid are retrieved from a QR code scanned from the beneficiary's mobile device.

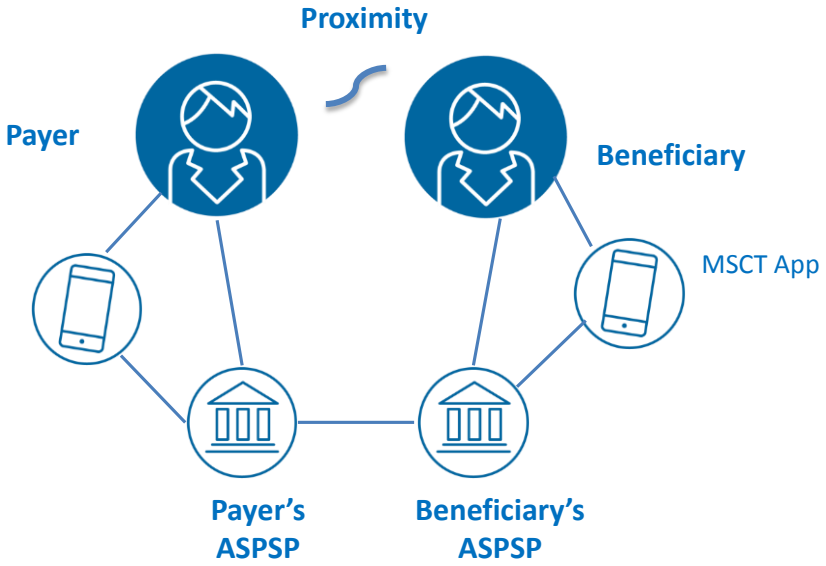


Figure 9: Actors in MSCT use case P2P-4

Payer and beneficiary may, and frequently will, hold their payment accounts with different ASPSPs and have downloaded a dedicated MSCT (Instant) application from their ASPSP[22]. A strong payer authentication (see section 8.3) in accordance with PSD2 [2] is performed, involving a facial recognition[23] of the payer (see section 8.2).

[22] The MSCT application may also be downloaded from an MSCT service provider. The payer and beneficiary may have different MSCT service providers.
[23] Note that other biometric methods may be used, see section 8.2.

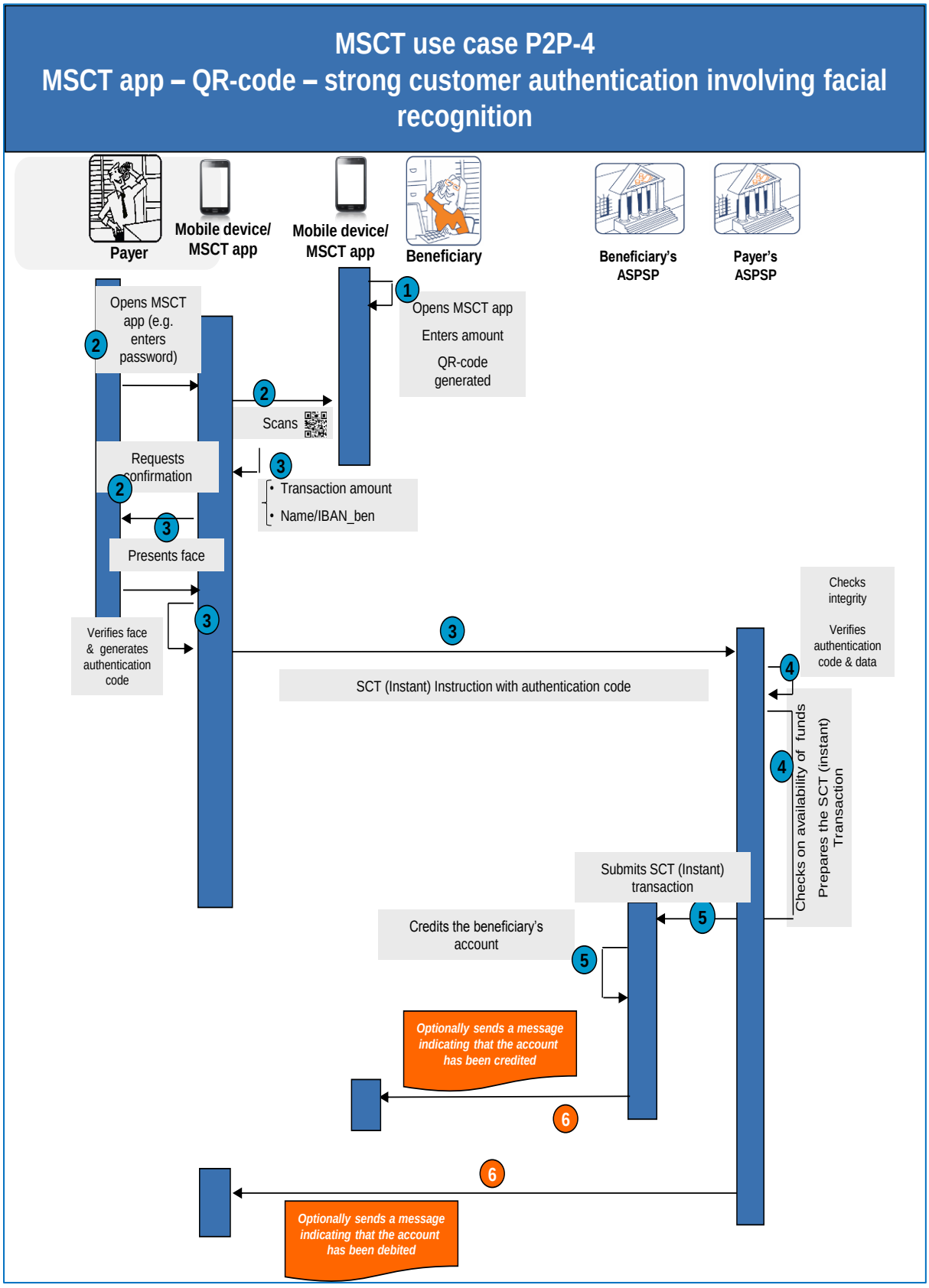


Figure 10: MSCT use case P2P-4

In the figure above, the following steps are illustrated:

Step 0

- The beneficiary needs to be subscribed to the MSCT (Instant) service of their ASPSP and has downloaded an MSCT (Instant) application that is enabled to generate QR- codes.
- The payer needs to be subscribed to the MSCT (Instant) service of their ASPSP and has downloaded an MSCT (Instant) application that is enabled to read QR-codes.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The beneficiary opens their MSCT (Instant) application on their mobile device and enters the amount to be paid.
- The MSCT application on the beneficiary's mobile device generates a QR-code including the beneficiary name, the IBAN_ben, and the amount to be paid.

Step 2

- The payer selects and opens the MSCT (Instant) application on their mobile device, which possibly involves the entry of a password.
- The payers scans the QR-code from the beneficiary's mobile device.
- The MSCT application retrieves the name of the beneficiary, the IBAN_ben, 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 (Instant) application[24] and transmitted with the SCT (Instant) Instruction to the payer's ASPSP.

Step 4

- The payer's ASPSP checks the integrity of the SCT (Instant) 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 (Instant) Transaction to the beneficiary's ASPSP.

[24] 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 Instant, a confirmation message is returned from the beneficiary's ASPSP to the payer's ASPSP (not shown on the figure).
- The beneficiary's ASPSP makes the funds available to the beneficiary.

Step 6

- The beneficiary is optionally informed by their ASPSP that their account has been credited.
- The payer is optionally informed by their ASPSP that their account has been debited.

Analysis MSCT Use case P2P-4	
Interoperability	• The payer and the beneficiary may have different ASPSPs and MSCT (Instant) applications.
Challenges	• Standardisation of a "QR-code", ensuring the correct beneficiary name/IBAN_ben link. • Integrity of the QR-code. • The information messages in step 6 are not included in the SCT Instant and SCT schemes. • In case of an SCT there is no immediate, irrevocable crediting of the funds. How to inform the beneficiary that the payment has been initiated?

Table 9: Analysis MSCT use case P2P-4

7.3 Consumer-to-Business (C2B) payments

MSCT use case C2B-1: Mobile device - Payment of invoice involving a QR-code – strong customer authentication 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 (Instant) from their own payment account to the payment account of a merchant (beneficiary). Hereby a dedicated MSCT (Instant) application on the consumer's mobile device is used, provided by their ASPSP[25].

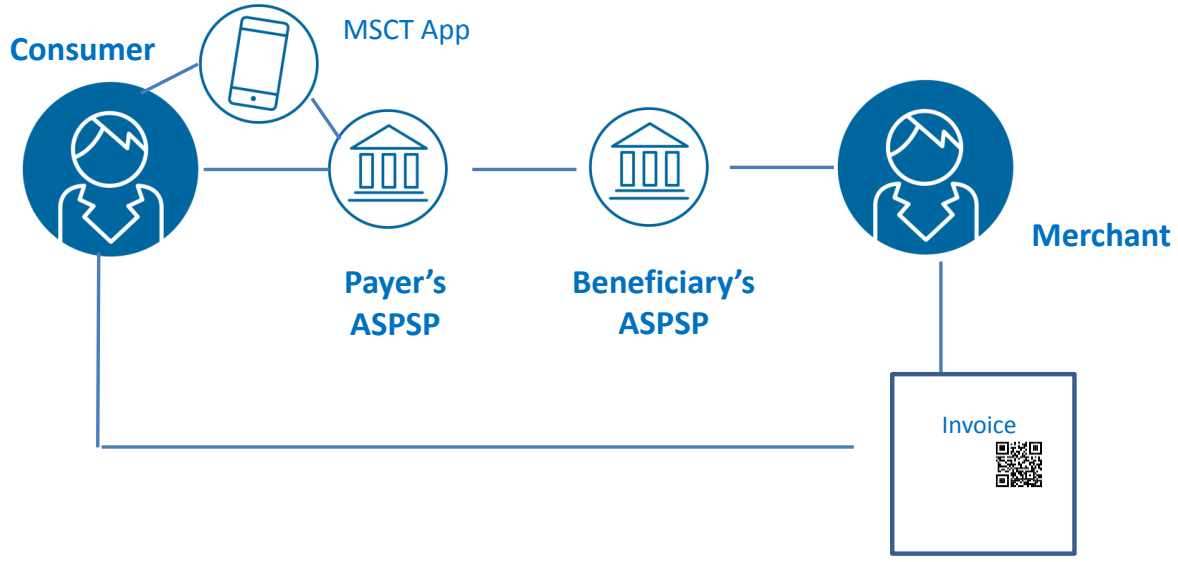


Figure 11: Actors in MSCT use case C2B-1

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 [2] is performed involving a mobile code (see section 8.2).

[25] The MSCT application may also be downloaded from an MSCT service provider.

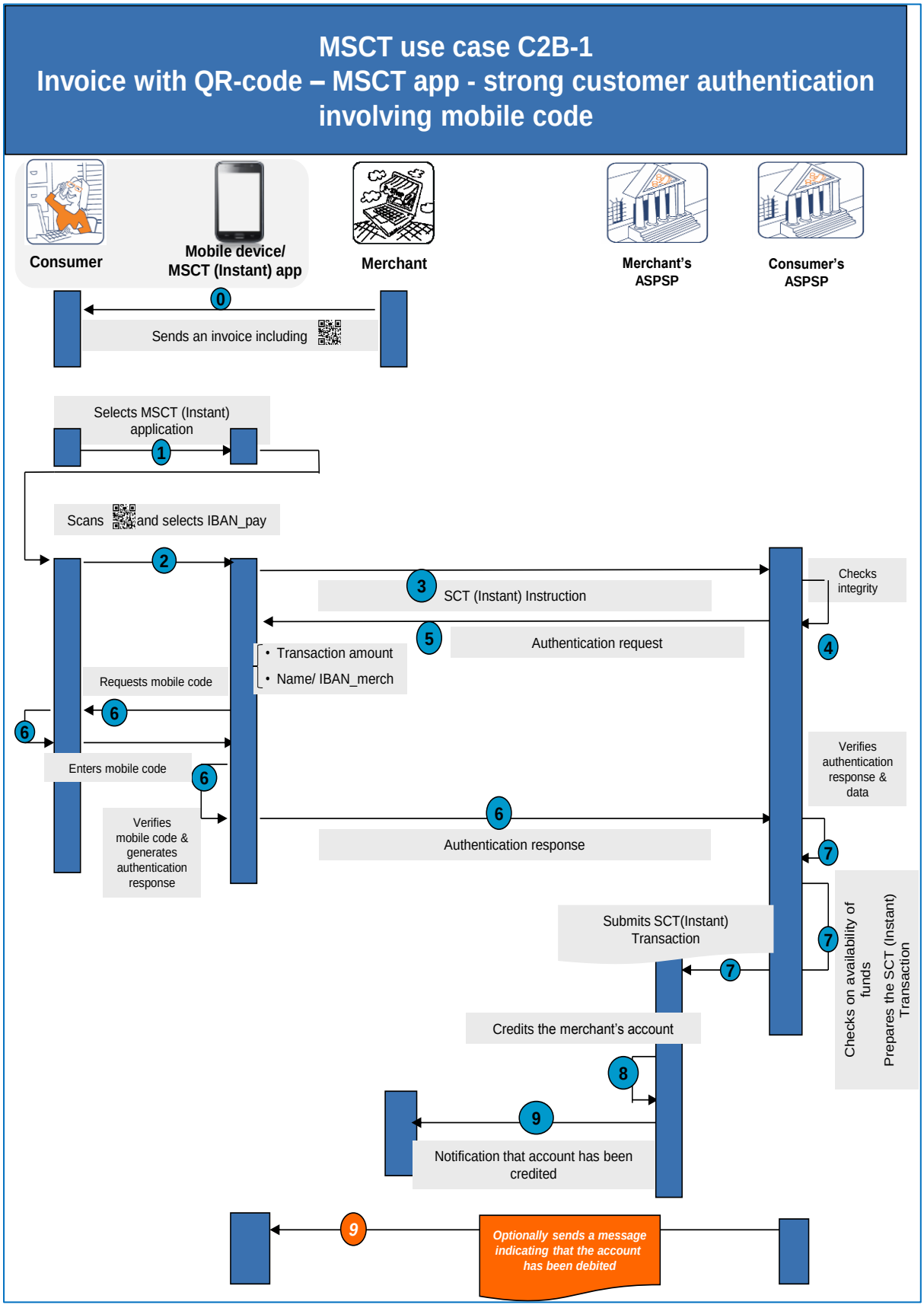


Figure 12: MSCT use case C2B-1

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 (Instant) service with their ASPSP and has downloaded a dedicated MSCT (Instant) application on their mobile device.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The consumer selects and opens the MSCT (Instant) 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_pay 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 (Instant) Instruction is generated by the MSCT (Instant) application.

Step 3

The SCT (Instant) Instruction is transmitted to the consumer's ASPSP.

Step 4

The consumer’s ASPSP checks the integrity of the SCT (Instant) Instruction.

Step 5

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

Step 6

- The authentication request is handled automatically by the MSCT (Instant) application on the consumer’s mobile device.
- The beneficiary'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 (Instant) 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 (Instant) Transaction to the beneficiary's ASPSP.

Step 8

- In case of an SCT Instant, 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 informed by their ASPSP that their account has been credited.
- The consumer is optionally informed by their ASPSP that their account has been debited.

Analysis MSCT Use case C2B-1	
Interoperability	• The consumer and the merchant may have different ASPSPs and MSCT (Instant) applications.
Challenges	• Standardisation of a "QR-code", ensuring the correct beneficiary name/IBAN_merch link. • Integrity of the QR-code. • The information messages in step 9 are not included in the SCT Instant and SCT schemes.

Table 10: Analysis MSCT use case C2B-1

MSCT use case C2B-2: Mobile device – Payment at POI involving merchant-presented QR-code – strong customer authentication via MSCT Instant application involving a mobile code

This use cases 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 Instant service[26]. The consumer has downloaded a dedicated MSCT Instant application from the MSCT service provider on their mobile device. The merchant has downloaded dedicated software on their POI from the MSCT service provider.

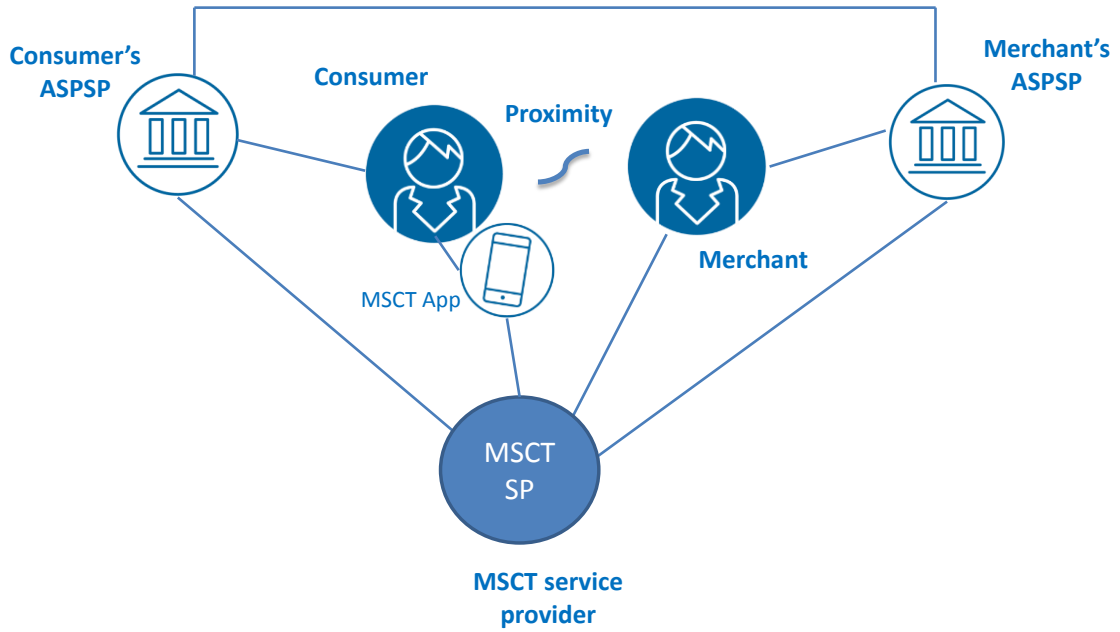


Figure 13: Actors in MSCT use case C2B-2

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

In this payment transaction a strong customer authentication (see section 8.3) in accordance with PSD2 [2] is performed involving a mobile code (see section 8.2), which is handled by the MSCT application. 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.

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

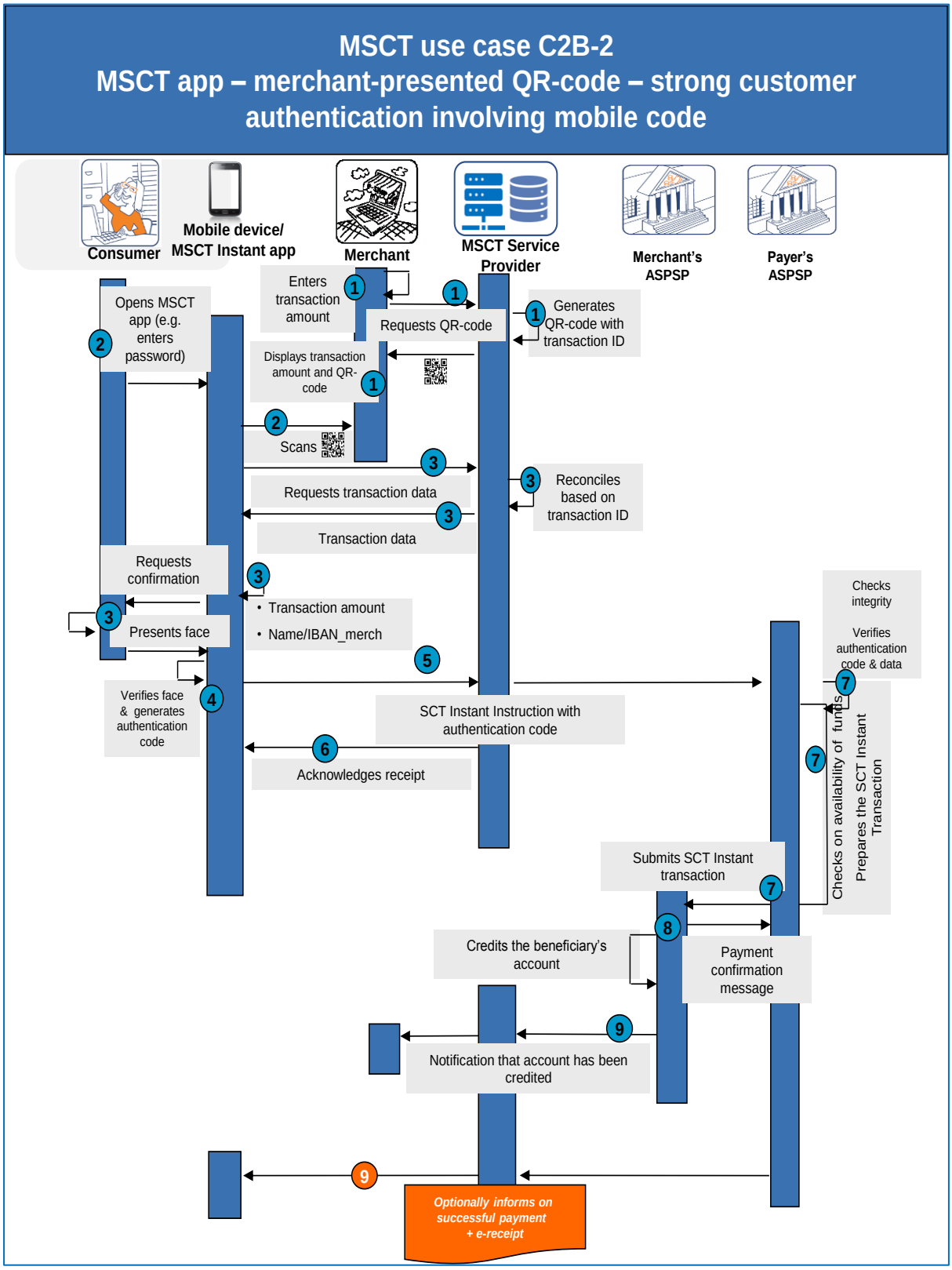


Figure 14: MSCT use case C2B-2

In the figure above, the following steps are illustrated:

Step 0

- The consumer needs to be subscribed to an MSCT Instant service and needs to have downloaded a dedicated MSCT Instant application from the MSCT Instant service provider, linked to a specific payment account of their ASPSP.
- The merchant needs to be subscribed to the same MSCT Instant 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 Instant 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 Instant 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 Instant application, an authentication code is calculated by the MSCT application.

Step 5

The SCT Instant 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 Instant Instruction to the consumer.

Step 7

- The consumer's ASPSP checks the integrity of the SCT Instant 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 Instant Transaction to the beneficiary'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 informed by the MSCT service provider (information provided by the merchant's ASPSP) that their account has been credited.
- The consumer is optionally informed 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.

Note: The MSCT service provider may be replaced by a PISP in which case in step 9, 1st bullet, the information to the MSCT service provider (PISP) is provided by the consumer's ASPSP.

Analysis MSCT Use case C2B-2	
Interoperability	• 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	• Standardisation of a "QR-code", ensuring the correct beneficiary name/IBAN_merch link. • Integrity of the QR-code. • Standardisation of merchant transaction identifier. • The information messages in step 9 are not included in the SCT Instant scheme.

Table 11: Analysis MSCT use case C2B-2

MSCT use case C2B-3: Mobile device – Payment at POI involving merchant-presented QR-code – strong customer authentication 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 Instant 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 application[27] in the consumer's mobile wallet[28].

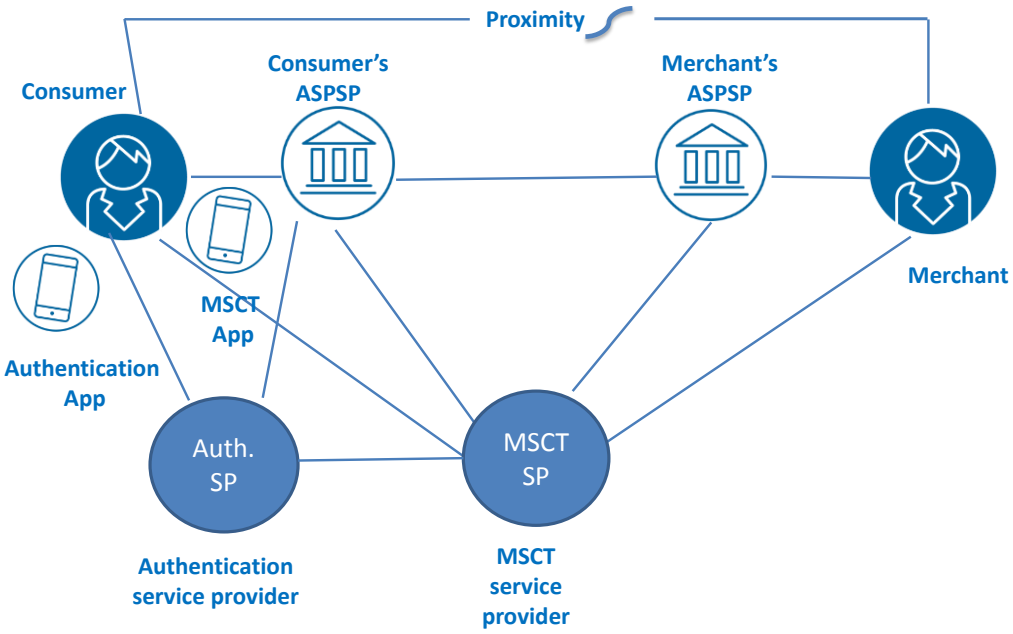


Figure 15: Actors in MSCT use case C2B-3

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. Both ASPSPs are participants in the same MSCT Instant Service[29].
Also, the merchant needs to be subscribed to the MSCT Instant 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 [2] is performed involving a fingerprint[30] (see section 8.2).

[27] An application accessed through the mobile device performing the functions related to a user authentication, as dictated by the Authentication service provider.
[28] 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.
[29] This refers to the current MSCT solutions in the market.
[30] Note that other biometric methods may be used, see section 8.2).

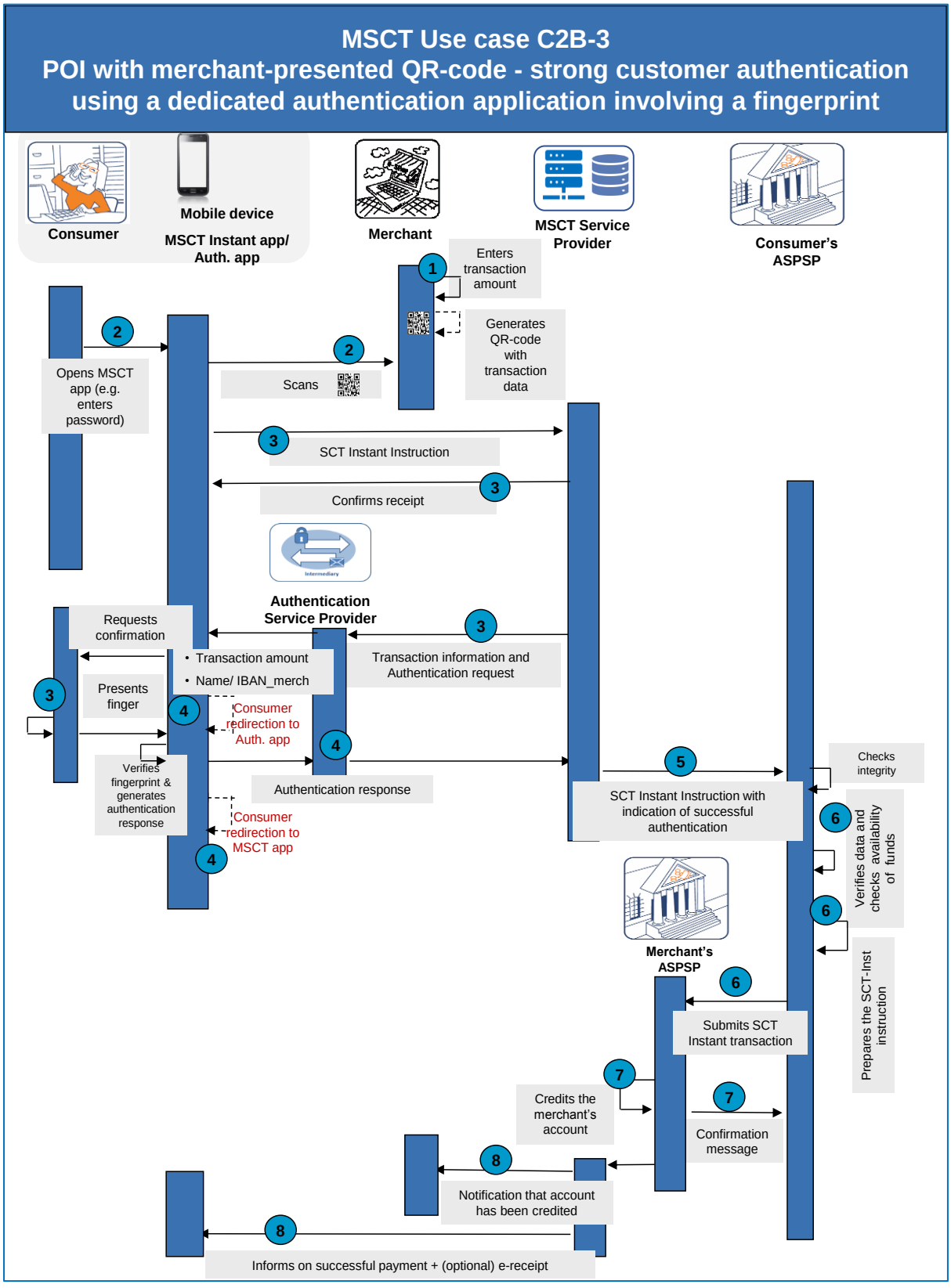


Figure 16: MSCT use case C2B-3

In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, the consumer would need to first subscribe to the MSCT Instant service and download a dedicated MSCT Instant application from the MSCT Instant 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 Instant 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 Instant service, e.g., through their ASPSP or the MSCT Instant service provider directly.
- The MSCT Instant 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 Instant 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 Instant application retrieves the merchant name, IBAN_merch, merchant transaction identifier and the transaction amount from the QR-code and sends an SCT Instant Instruction to the MSCT Instant service provider.
- The consumer is informed about the receipt of the MSCT Instant Instruction by the MSCT Instant 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 MSCT Instant service provider is informed by the Authentication service provider.
- The consumer is redirected to the MSCT Instant application.

Step 5

The SCT Instant 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 Instant Instruction.
- The consumer's ASPSP checks the availability of funds on the consumer's account.
- The consumer's ASPSP prepares and submits the SCT Instant 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 informed by the MSCT service provider (information provided by the merchant's ASPSP) that their account has been credited.
- The consumer is informed 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.

Note: The MSCT service provider may be replaced by a PISP in which case in step 8, 1st bullet, the information to the MSCT service provider (PISP) is provided by the consumer's ASPSP.

Analysis MSCT Use case C2B-3	
Interoperability	• 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	• Standardisation of messages including data elements between MSCT service provider back-ends • Standardisation of a "QR-code", ensuring the correct beneficiary name/IBAN_merch link. • Integrity of the QR-code. • How is the transaction reconciled with the purchase (e.g., purchase identifier)? • The information messages in step 8 are not included in the SCT Instant scheme.

Table 12: Analysis MSCT use case C2B-3

MSCT use case C2B-4: Mobile device – m-commerce – merchant application - PISP with redirection to consumer's ASPSP - strong customer authentication 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 Instant. Therefore the consumer is redirected to the on-line banking system of their ASPSP.

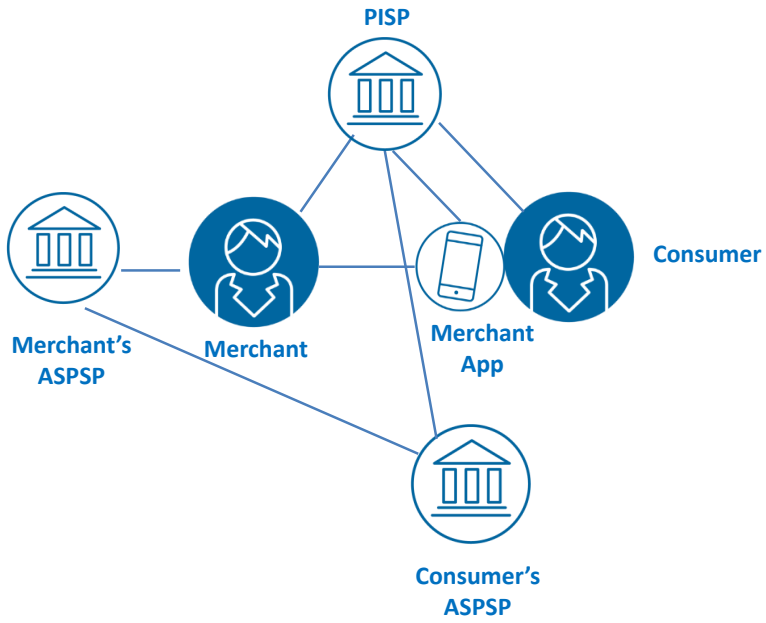


Figure 17: Actors in MSCT use case C2B-4

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's website to their ASPSP's online banking service where a strong customer authentication (see section 8.3) involving a dynamic authenticator (e.g. an OTP - see section 8.2) is performed in accordance to PSD2 [2].

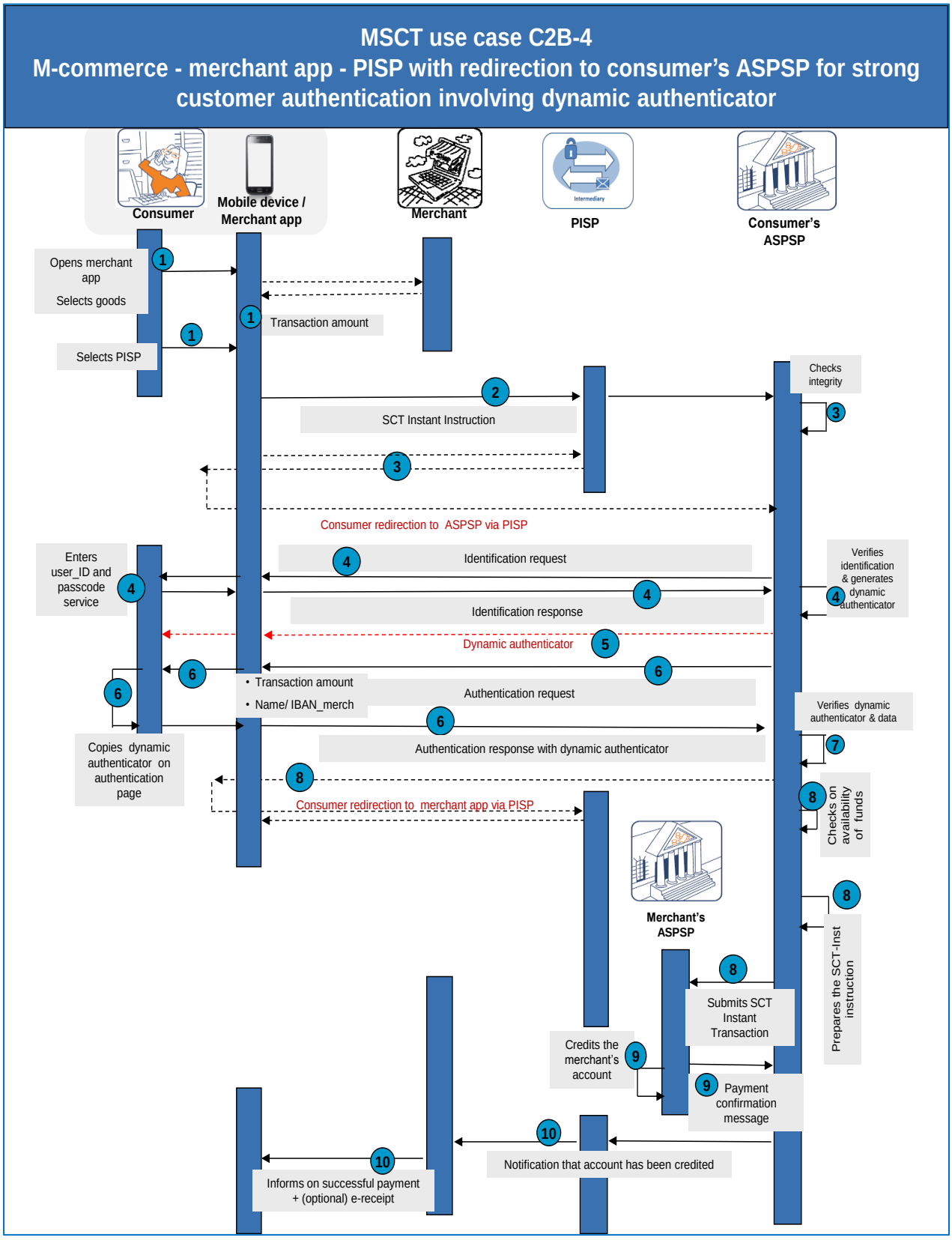


Figure 18: MSCT use case C2B-4

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.
- 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 customer.
- The consumer selects their preferred PISP payment solution in this checkout section.

Step 2

An SCT Instant 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 Instant Instruction.
- The consumer is redirected from the merchant application through the PISP to the on-line banking service of their ASPSP.

Step 4

- The consumer is invited to enter their user-ID 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., using a one-per-transaction number linked to the transaction amount and merchant) to the consumer.

Step 6

The consumer is subsequently requested to enter this dynamic authenticator into a dedicated authentication page to authorise the SCT Instant Instruction.

Step 7

The consumer's ASPSP verifies the dynamic authenticator.

Step 8

- The consumer is redirected 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 Instant 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 informed 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 in their merchant application.

Note: If an SCA is not requested by the ASPSP (see section 8.3), steps 5 through 7 may be omitted.

Analysis MSCT Use case C2B-4	
Interoperability	• The merchant needs to have a contractual relationship with the PISP. • Interoperable due to the underlying SCT Instant scheme • Consumer authenticates in "known" on-line banking environment.
Challenges	• The PISP needs to connect to # ASPSPs. • In view of the lack of an MSCT application and pre-onboarding, the consumer authentication process is less convenient. • The information messages in step 10 are not included in the SCT Instant scheme.

Table 13: Analysis MSCT use case C2B-4

MSCT use case C2B-5: Mobile device – m-commerce – mobile browser – PISP with embedded strong customer authentication 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 Instant is used from the consumer's payment account to the payment account of the merchant (beneficiary) which is initiated using a mobile browser.

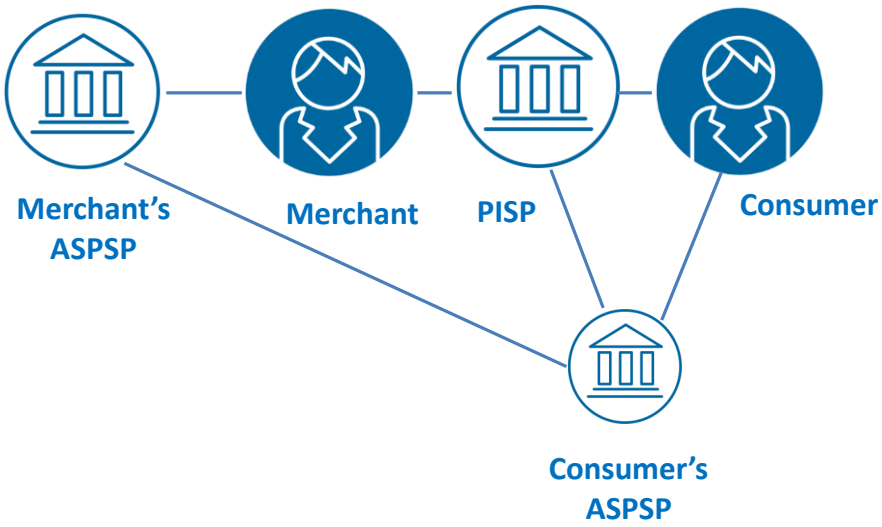


Figure 19: Actors in MSCT use case C2B-5

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 dynamic authenticator (e.g. an OTP - see section 8.2) is performed in accordance with PSD2 [2] via a PISP i-frame on the merchant's website (embedded model). In this case there is a delegated authentication from the consumer's ASPSP to the PISP. Therefore an agreement between the consumer's ASPSP and the PISP is required.

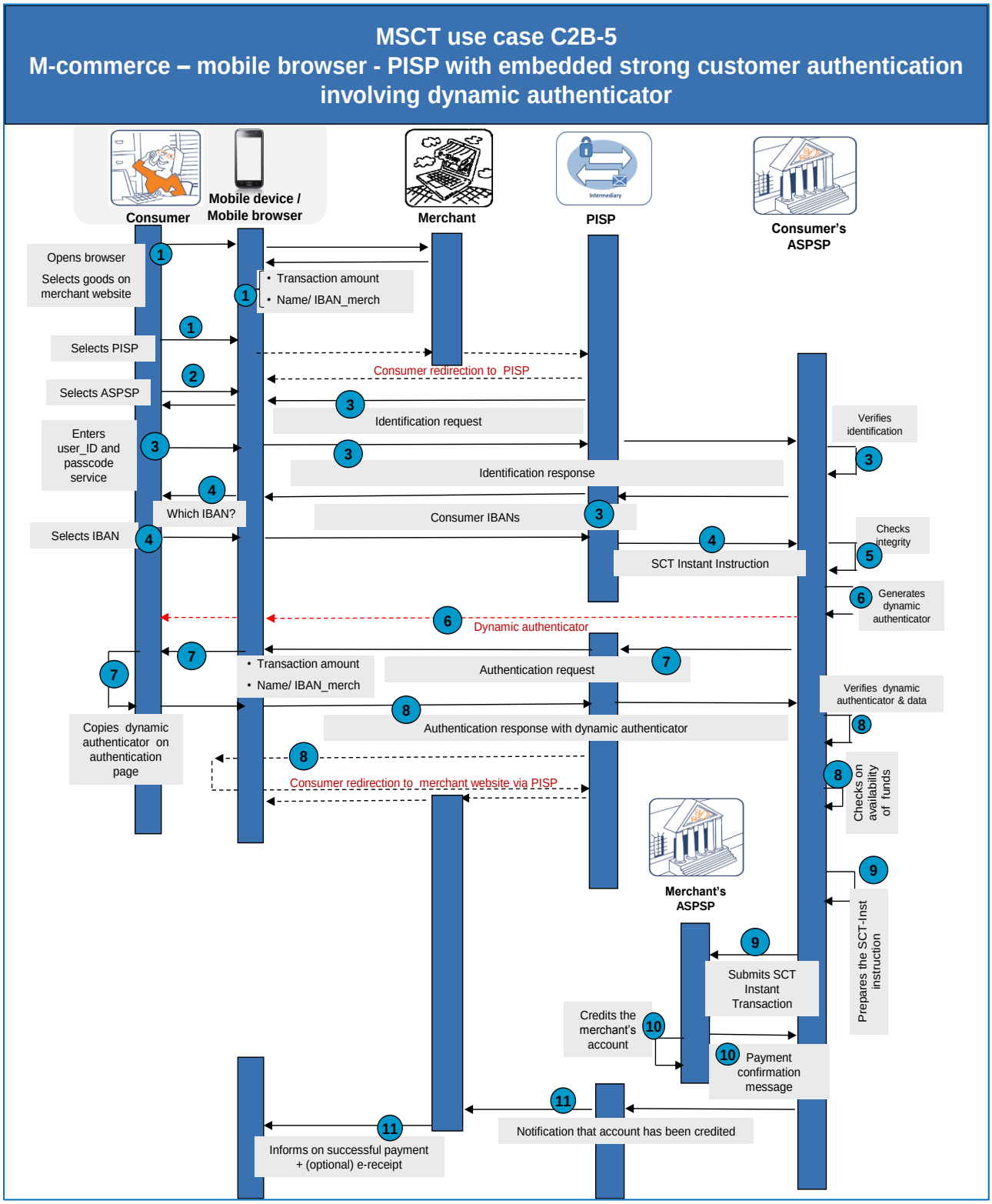


Figure 20: MSCT use case C2B-5

In the figure above, the following steps are illustrated:

Step 0

- The merchant needs to be registered with a PISP.
- The PISP has an agreement with the consumer's ASPSP and has received delegation of authority for customer authentication.
- The consumer is registered with their bank 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 customer.
- 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 user-ID and identification data 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 PISP.[31]

Step 4

- The consumer is invited to select the IBAN they want to use for this purchase on the PISP's iframe.
- An SCT Instant 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 Instant Instruction.

[31] This requires further clarification by the EBA in accordance to document API EG 045-18 – Recommended functionality 2(e) (see https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/api-evaluation-group-recommended-functionalities-psd2rts)

Step 6

The consumer's ASPSP transmits a dynamic authenticator (e.g., using a one-per-transaction number linked to the transaction amount and merchant) 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 Instant 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 informed 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-5	
Interoperability	• The merchant needs to have a contractual relationship with the PISP. • The PISP needs to have an agreement with the consumer's ASPSP (delegation of authority for customer authentication). • Interoperable due to the underlying SCT Instant scheme.
Challenges	• 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. • The information messages in Step 11 are not included in the SCT Instant scheme. • The ASPSP's API needs to make the consumer IBANs available to the PISPs – this issue is awaiting further clarification by the EBA see API EG 045-18, Recommended functionality 2(e).

Table 14: Analysis MSCT use case C2B-5

MSCT use case C2B-6: Mobile device – transport ticketing – in-app payment, strong customer authentication involving fingerprint

This use cases 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.

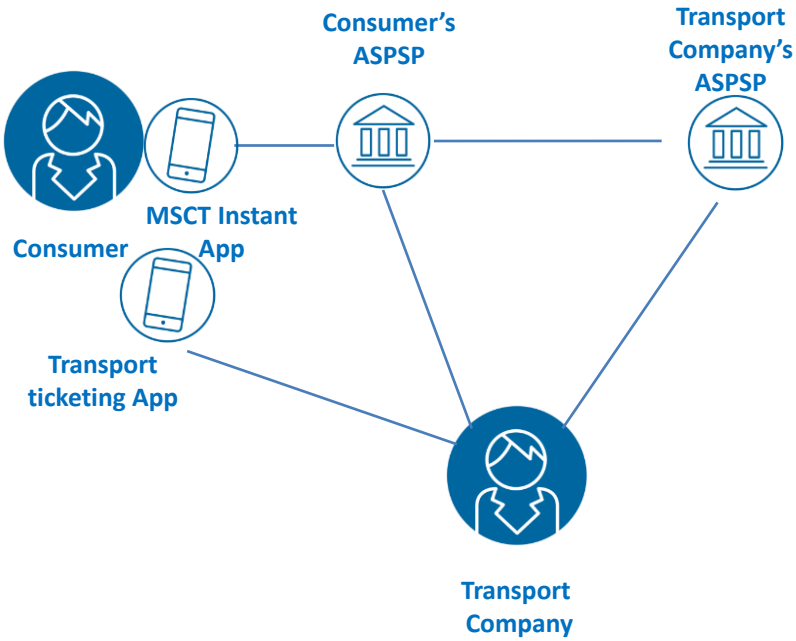


Figure 21: Actors in MSCT use case C2B-6

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 [2] is performed involving a fingerprint[32] (see section 8.2).

[32] Note that other biometric methods may be used, see section 8.2.

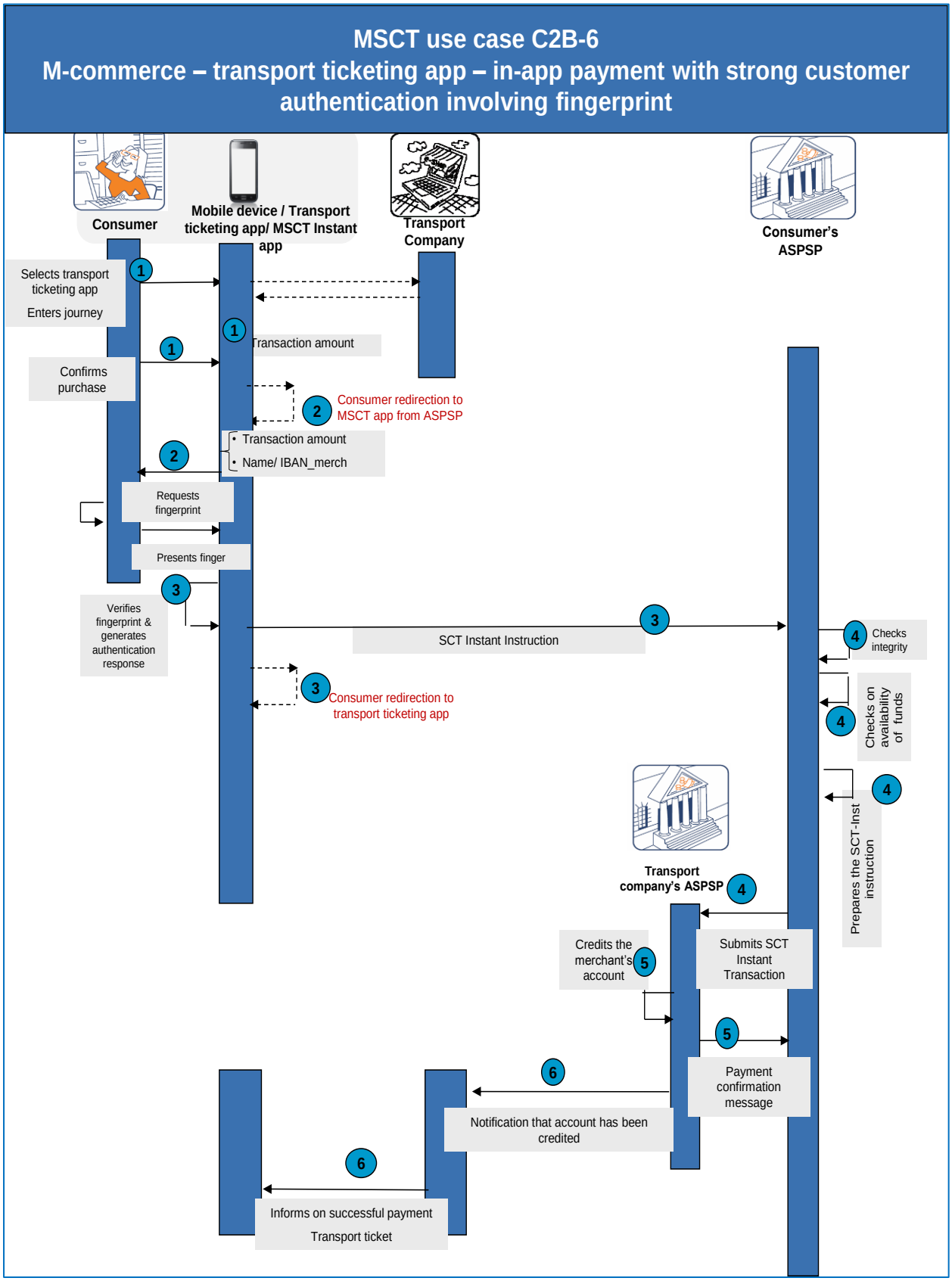


Figure 22: MSCT use case C2B-6

In the figure above, the following steps are illustrated:

Step 0 (Pre-requisite)

- The consumer has downloaded an MSCT Instant 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 Instant 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 Instant 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 Instant 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 SCT Instant Instruction is submitted to the consumer's ASPSP.
- The consumer is informed about the submission of the SCT Instant Instruction and redirected to the transport ticketing application.

Step 4

- The consumer's ASPSP checks the integrity of the SCT Instant Instruction.
- The consumer's ASPSP checks the availability of funds on the consumer's account.
- The consumer's ASPSP prepares and submits the SCT Instant 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 informed by their ASPSP about the successful SCT Instant payment.
- The consumer is informed about the successful payment and receives the electronic transport ticket from the transport company they can store in their mobile wallet.

Analysis MSCT Use case C2B-6	
Interoperability	• 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	• The information messages in step 6 are not included in the SCT Instant scheme.

Table 15: Analysis MSCT use case C2B-6

7.4 Business-to-Business (B2B) payments

MSCT use case B2B-1: Mobile device – Request-to-Pay – strong customer authentication involving a fingerprint

This use case presents an example of user experience whereby a business (payer) is requested via an EIPP service (see [24]) to pay an invoice from a beneficiary. The invoice is paid with an MSCT. The "request-to-pay" message included in the EIPP service contains the elements to initiate a payment to the beneficiary and the transaction amount.

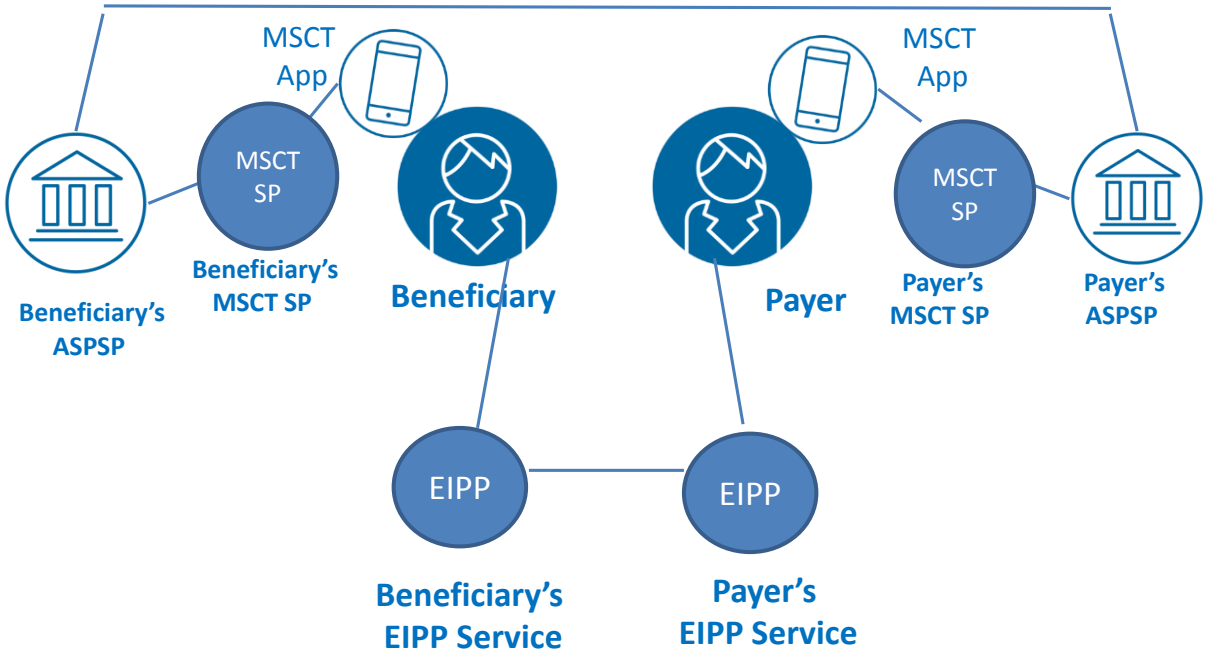


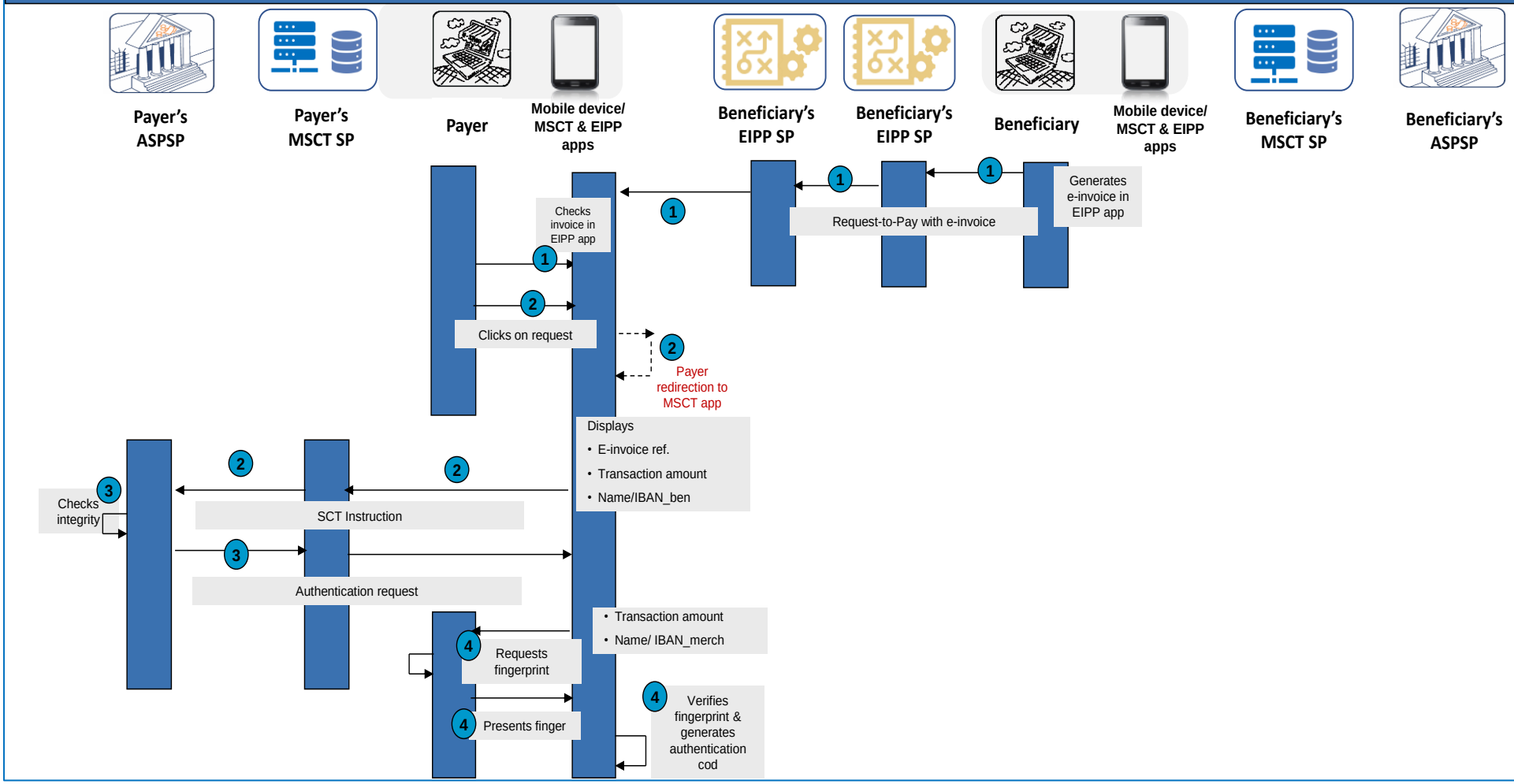
Figure 23: Actors in MSCT use case B2B-1

Payer and beneficiary have subscribed to potentially different EIPP solution providers (see [24]).

Payer and beneficiary 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 [2] is performed, involving the presentation of a fingerprint[33] (see section 8.2) by the payer.

[33] Note that other biometric methods may be used, see section 8.2.

MSCT use case B2B-1
MSCT app – Request-to-Pay – strong customer authentication involving fingerprint (1)



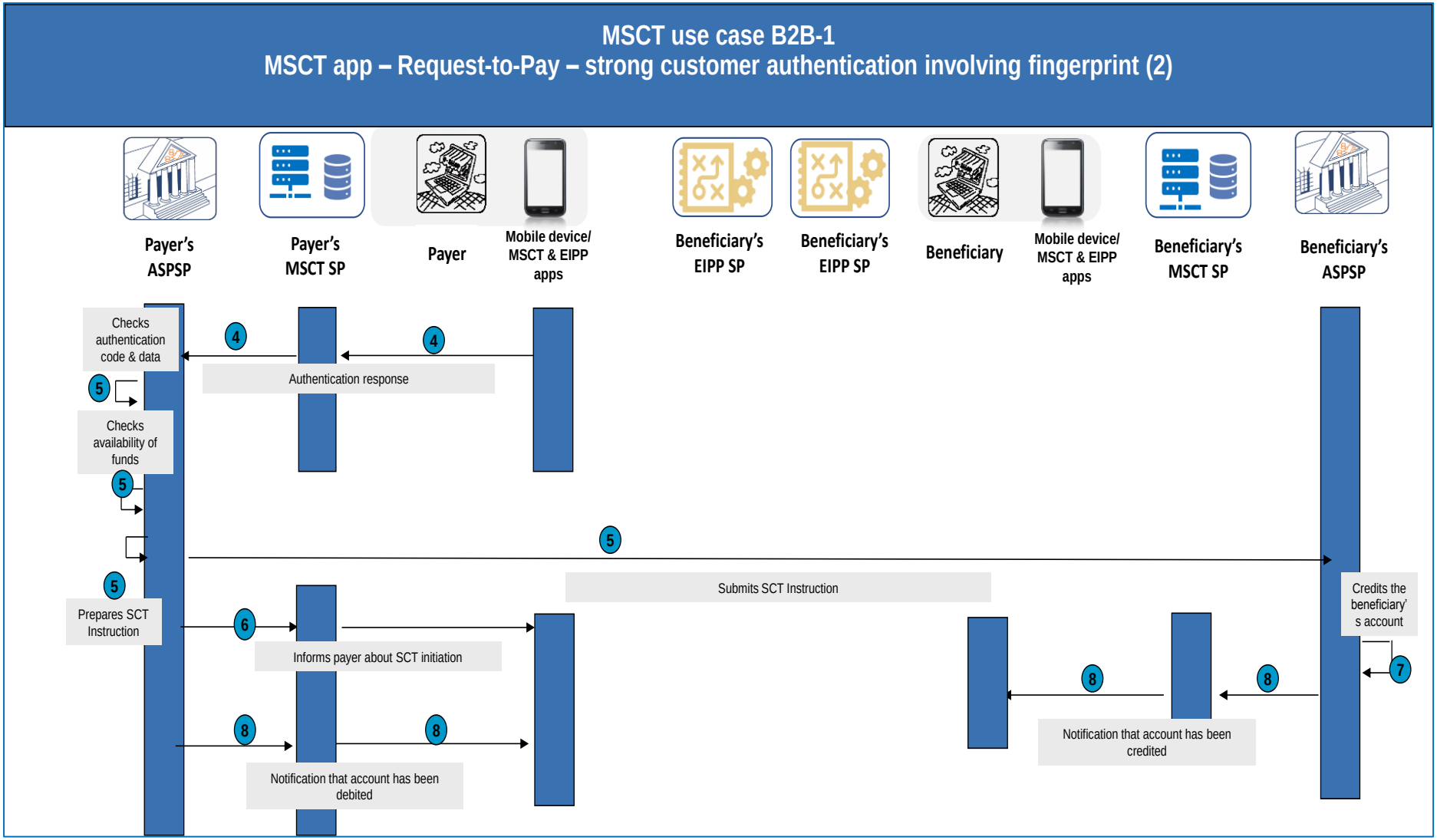


Figure 24: MSCT use case B2B-1

In the figure above, the following steps are illustrated:

Step 0

- As a prerequisite, the payer and the beneficiary 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 beneficiary 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 beneficiary, that delivers to the beneficiary and their EIPP solution provider all the information required to deliver e-invoices and related Request-to-Pay messages from the beneficiary to the payer.
- The payer and the beneficiary 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 beneficiary accounts.
- The ASPSPs of the payer and the beneficiary are participants in the chosen MSCT services.
- As a prerequisite, a mobile internet connection is required during the transaction.

Step 1

- The beneficiary sends a “request-to-pay”, containing an e-invoice as an annex, to their EIPP solution provider.
- The beneficiary’s EIPP solution provider forwards the “request-to-pay” to the payer’s EIPP solution provider.
- The payer’s EIPP solution provider sends the e-invoice and the “request-to-pay” including an e-invoice reference, transaction amount and IBAN_ben, to the payer.
- The payer can check in their EIPP solution provider application the invoice received.

Step 2

- The payer receives the “request-to-pay” 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, beneficiary name and IBAN_ben.
- 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 beneficiary'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 beneficiary'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 beneficiary'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 beneficiary's ASPSP makes the funds available to the beneficiary merchant.

Step 8

- The beneficiary is informed by their MSCT service provider (information provided by the beneficiary's ASPSP) that the funds related to their payment request have been received.
- The payer is informed by 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 Instant. In this case, in step 7 there is a confirmation message sent from the beneficiary'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	• The payer and the beneficiary may have different MSCT service providers and EIPP solution providers. • The payer and the beneficiary may have different ASPSPs.
Challenges	• The information messages in step 8 are not included in the SCT schemes.

Table 16: Analysis MSCT use case B2B-1

7.5 Applicability of MSCTs

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

Payment Context	SCT Instant	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 17: 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 Instant and SCT transactions.

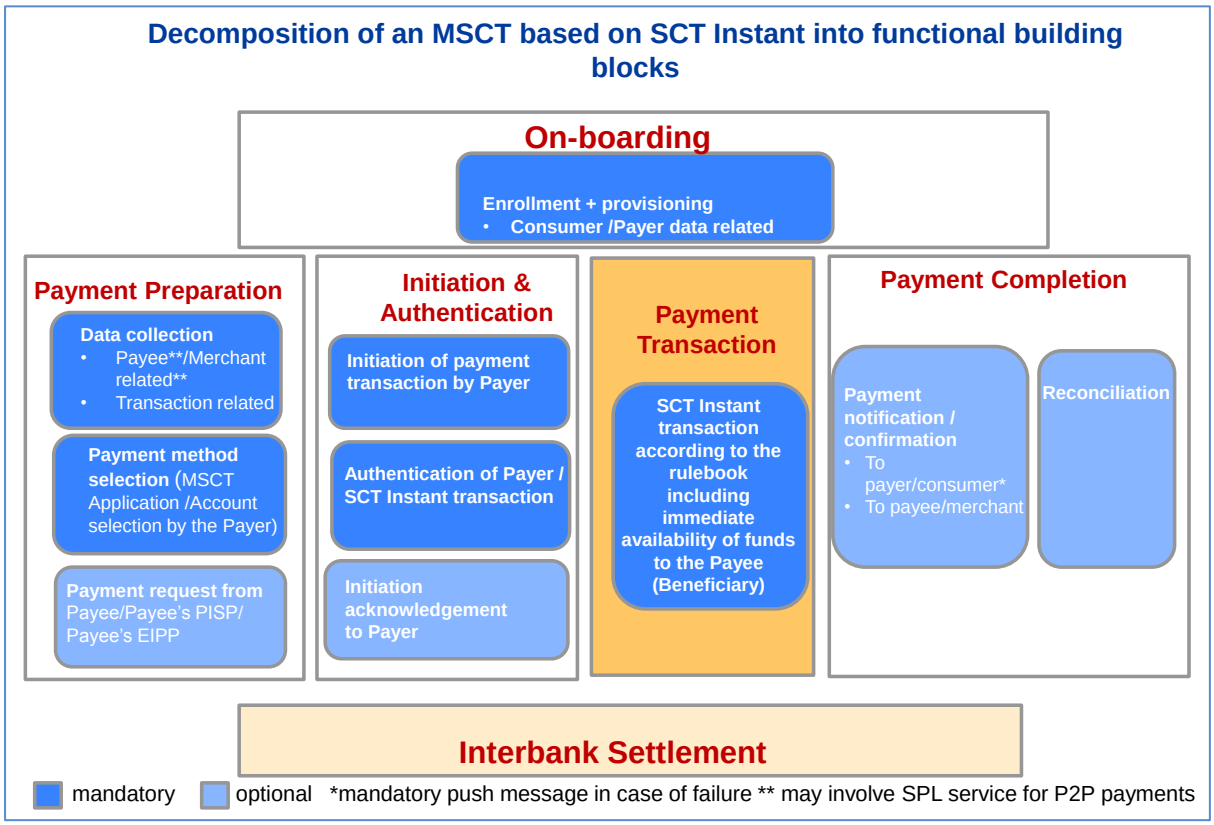


Figure 25: Decomposition of MSCT based on SCT Instant into building blocks

The amber coloured box in the figure is covered by the SCT Instant scheme rulebook [20] and supporting documents (see 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 Instant includes an immediate, irrevocable availability of the funds.

On-boarding refers to the process of registration of a payer (consumer) with an MSCT service provider (including ASPSPs, PISPs) or a merchant.

The optional boxes are features which may or may not be present in the MSCT Instant transaction. This may depend on the payment context.

In case of P2P payments, a mobile phone number of the beneficiary may be used which may require the support by the SPL service[34] (see section 15.3) for the linking with the IBAN_ben.

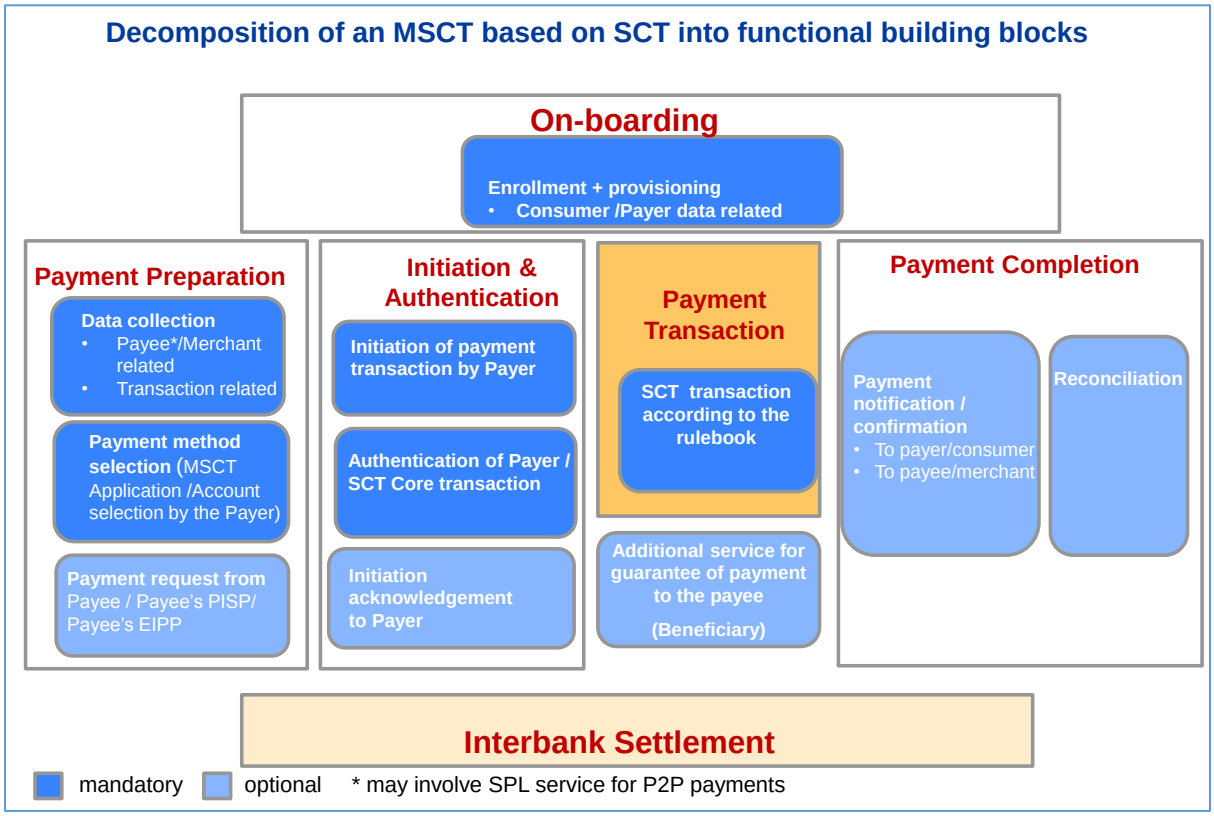


Figure 26: Decomposition of MSCT based on SCT into building blocks

The amber coloured box in the figure is covered by the SCT scheme rulebook [13] and supporting documents (see 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 Instant transaction, the SCT scheme does not include an immediate availability of funds to the beneficiary.

On-boarding refers to the process of registration of a payer (consumer) with an MSCT service provider (including ASPSPs, PISPs) or a merchant.

The optional boxes are features which may or may not be present in the MSCT transaction. This may depend on the payment context.

In case of P2P payments, a proxy (e.g., mobile phone number) of the beneficiary may be used which may require the support by the SPL service (see section 15.3) for the linking with the IBAN_ben.

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

The following section in this chapter will focus on the different aspects of the blocks "Initiation and Authentication" and "Payment Completion", while aspects related to the block "Payment Preparation" are treated in chapter 9.

8.2 Payer authentication

The term payer authentication in an MSCT transaction refers to the methods used for the authentication of the consumer / payer. Certain features of the mobile device such as the keyboard could be used in this process.

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 [2] 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 [3]).

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 [53] and [69])).

Consumer Device User Verification Method

For MSCTs, the payer authentication method used typically involves a Consumer Device User Verification Method[35] (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 code[36]: 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 [53] and [69].

On a mobile device, a distinction may be made between a CDUVM verified by the ASPSP, and a so-called "shared" CDUVM, which is shared amongst different mobile applications accessible via the mobile device. This "shared" CDUVM may be verified by another mobile

[35] 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

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

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 [11]). 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).
For MSCTs, other factors, such as the consumer choice, may influence the usage of a CDUVM.

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 through manual entry by the payer on the mobile device.

- 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 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.

Challenge/response method

In case a dedicated MSCT or an Authentication application[37] is accessible via the mobile device, a dynamic authentication method (e.g., challenge/response method) is initiated by the ASPSP 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.) once during the MSCT transaction process.

In case of an Authentication Application is used, there needs to be a delegation of authority by the Payer's ASPSP to the Authentication Service Provider for the authentication of the payer.

More information on the usage of an Authentication application may be found in [30].

8.3 Strong Customer Authentication (SCA)

PSD2 [2] 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 [2] mandates the usage of strong customer authentication for MSCT transactions, except for the exemptions (Article 98)[38] 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 [3].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.

[37] 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. In such case there needs to be for MSCTs, a delegation of authority by the payer's ASPSP to the Authentication Service Provider for the authentication of the payer.

[38] Since MSCT transactions are electronic remote transactions as connectivity via mobile internet from the payer's mobile device is used to conduct the transaction, the exemption mentioned under Article 11 of the RTS does not apply. This needs to be confirmed through the EBA Q&A tool (see https://eba.europa.eu/single-rule-book-qa).

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 [2]and the RTS [3].

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 (beneficiary) and their account and possibly a time factor.

Moreover, the payer authentication is often a combined method with the transaction authentication for consumer convenience, which implicitly provides consumer 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)[39].

As MSCTs are electronic remote transactions, in view of the fact that connectivity via mobile internet from the payer's mobile device is used to conduct the transaction, Article 97(2) of the PSD2 [2] applies in this context.

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 [3].

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 [3]).

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 [30].

[39] see also requirement 12 in https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/api-evaluation-group-recommended-functionalities-psd2rts

8.5 Transaction risk analysis

Transaction risk analysis refers to the use of statistical models via transaction, location, device and profile data, without active consumer participation, in the decision-making process for strong customer authentication (see also Article 18.3 in [3]) 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, beneficiary/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 [4]).

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 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 Authentication application is present in the mobile device. 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 supported[40] or to add any other risk parameter they seem to be appropriate.

These risk parameters are further described in detail below.

	MSCT data type		
Risk parameters	**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 18: Risk parameters for MSCTs

**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 (see section 15.2) to the MSCT application, if present. The latter needs to be confirmed through the EBA Q&A tool (see https://eba.europa.eu/single-rule-book-qa).

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.

[40] subject to an agreement with the payer's ASPSP in case the MSCT service provider received delegation of authority for strong customer authentication.

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*[41] 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 [2] (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 [3]). Transactions for which the value is greater than the *No-SCA Limit* require the usage of an SCA.

The value of the *No-SCA Limit* is set by the payer's ASPSP and shall be compliant with the dedicated Regulation (see [2] and [3]).

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 [2] 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 [3] 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.

[41] 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.

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 [2] 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 N-SCA Limit* is set and defined by the payer's ASPSP in accordance to Article 16 of the RTS [3] 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

Acknowledgement to payer of receipt of SCT (Instant) Instruction

The MSCT service provider shall inform the payer about the receipt of the SCT (Instant) Instruction including the information specified in Article 46 [Information for the payer and payee (beneficiary) after the initiation of the payment order] and Article 48 [Information for payer after receipt of the payment order] of PSD2 [2]. In case the MSCT service provider is not the payer's ASPSP, the appropriate information shall be provided by the payer's ASPSP to the MSCT service provider.

More in particular, this acknowledgement is convenient for the payer in case of an SCT when there is no immediacy of payment.

In case of a refusal of the SCT (Instant) Instruction, the payer's ASPSP shall provide or make available the notification in an agreed manner with the payer. This notification shall include the information as specified in Article 79 [Refusal of payment orders] of the PSD2 [2].

Acknowledgement to merchant of SCT Initiation by PISP

In case of a request for an MSCT transaction from a merchant through a PISP to the consumer, the merchant needs to be informed about the initiation of the SCT (Instant) transaction. The PISP shall make the information available as specified in Article 46 [Information for the payer and payee (beneficiary) after the initiation of the payment order] of PSD2 [2] to the merchant.

Notification to payee after execution of the MSCT

Immediately after execution of the payment transaction, the payee's PSP shall provide the payee (beneficiary) with the appropriate information about the SCT transaction as specified in Article 49 [Information for the payee after execution] of the PSD2 [2].

Notification to payer after execution of the MSCT

A message may be sent by the MSCT service provider to the payer that their account has been debited. In case the MSCT service provider is different to the payer's ASPSP, the MSCT service provider will need to receive this message from the payer's ASPSP.

The content of this notification message may vary, depending on the payment context.

In case of a successful MSCT Transaction, the notification message should contain at least a proper reference to the SCT Instruction including the transaction date and time, the amount, the rejection reason and a reference of the beneficiary subject to the applicable regulations.

In case of an unsuccessful MSCT Transaction, the notification message should contain at least a proper reference to the SCT Instruction, if possible transaction date and time, the amount. For an SCT Instant transaction, this message is mandatory according to the SCT Instant rulebook (see [19]).

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 record[42] 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:

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

- Transaction Date and Time;
- Transaction Amount;
- Transaction Identifier[43];
- Payer's IBAN
- Payee's identification (e.g., 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.

[43] This is an end-to-end reference which enables the identification of the MSCT transaction by the payer and the beneficiary.

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

9.1 Introduction

In this chapter the security in the 'Customer-to-ASPSP/MSCT Service Provider space/PISP space for MSCTs based on SCT Instant or SCT payments is considered. This includes the communication between the Originator (Payer) and their ASPSP/MSCT service provider/PISP and the communication between the Beneficiary (Payee, Merchant) 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	**Originator impersonation** This occurs when an attacker poses as the Originator when transmitting the SCT (Instant) Instruction to the Originator ASPSP/MSCT Service Provider/PISP. The attacker may pose as a genuine Originator by initiating an SCT (Instant) Instruction to the Originator ASPSP/MSCT service provider/PISP with a valid IBAN.
T2	**Spoofed Originator ASPSP / MSCT service provider/PISP towards Originator** This occurs when an attacker poses as the genuine Originator ASPSP/MSCT Service Provider/PISP towards the Originator in order to • Intercept SCT (instant) Instructions; • Capture sensitive data (e.g. credentials) or other personal data from Originators; • Create fraudulent MSCT related messages[44] or information to the Originator.
T3	**Tampering with SCT (Instant) Instruction messages** 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.
T4	**Tampering with MSCT acknowledgement / confirmation /notification messages (i.e. MSCT related messages)** 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.
T5	**Tampering with Account statement information** The Account statement information may be deliberately and maliciously tampered with while in transfer between the Beneficiary ASPSP and the Beneficiary, or between the Originator ASPSP and the Originator.

[44] For more details on these messages see section 2.6.

T6	**Tampering with R-transaction messages or "Request-to-Pay messages** 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.
T7	**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.
T8	**(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.
T9	**Repudiation by Originator** • An Originator may refute SCT (Instant) Instructions which they have previously initiated; • An Originator may deny receipt of MSCT related messages from the Originator ASPSP/MSCT Service Provider.
T10	**Repudiation by Originator ASPSP/MSCT Service Provider/PISP** • An Originator ASPSP/MSCT Service Provider/PISP may refute the receipt of an SCT (Instant) Instruction; • An Originator ASPSP/MSCT Service Provider/PISP may refute sending/ deny the receipt of MSCT related messages.
T11	**Disclosure of Originator or Beneficiary personal data/sensitive payment data** This occurs when sensitive personal information about the Originator/Beneficiary 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).
T12	**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.
T13	**Spoofed Beneficiary ASPSP/ PISP/MSCT service provider towards Beneficiary** This occurs when an attacker poses as the genuine Beneficiary ASPSP/PISP/MSCT Service Provider towards the Beneficiary in order to • Create fraudulent MSCT related messages or information to the Beneficiary; • Capture sensitive data (e.g. credentials) or other personal data from Beneficiaries.

T14	**Beneficiary impersonation** This occurs when an attacker poses as the Beneficiary when transmitting the transaction data to their MSCT Service Provider, PISP or the Originator. The attacker may pose as a genuine Beneficiary when creating fraudulent QR-codes, "Request-to-Pay" messages, etc.
T15	**Repudiation by Beneficiary** • A Beneficiary may refute "Request-to-Pay" messages which they have previously initiated; • A Beneficiary may deny receipt of MSCT related messages from the Beneficiary ASPSP/MSCT Service Provider/PISP.
T16	**Repudiation by Beneficiary ASPSP/MSCT Service Provider/PISP** • A Beneficiary ASPSP/MSCT Service Provider/PISP may deny the receipt of a "Request-to-Pay" message; • A Beneficiary ASPSP/MSCT Service Provider/PISP may refute the sending/ deny the receipt of MSCT related messages.

Table 19: MSCT threats list in the Customer-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 Originators, Beneficiaries 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 [2] and [4] and used solely for the purposes explicitly allowed by the respective "data subject" (natural person, see [4]).
G-SG2	A secure communication channel between the Originator and the Originator 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 Originator's mobile device.
G-SG3	A secure communication channel between the Beneficiary and the Beneficiary 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 Beneficiary's mobile device.

G-SG4	The Originator ASPSP/MSCT Service Provider/PISP should provide the Originator 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 Beneficiary unless the Originator's ASPSP decides to apply an exemption in accordance to the PSD 2 [2] and RTS [3] (see chapter 8).
G-SG5	All personalised security credentials issued to the Originator should meet the security requirements and be protected according to the requirements specified in the RTS [3].
G-SG6	The Originator ASPSP/MSCT Service Provider/PISP should protect the messages to the Originator in order to ensure the origin and integrity of the message and the confidentiality of sensitive payment data as appropriate. In addition, the Originator ASPSP/MSCT Service Provider/PISP should take measures to ensure the authenticity of the Originator 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 Originators 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 Originators should adequately protect their personal security credentials.
G-SG8	The Beneficiary ASPSP/MSCT Service Provider/PISP should protect the messages to the Beneficiary in order to ensure the origin and integrity of the message, and the confidentiality of sensitive payment data as appropriate. In addition, the Beneficiary ASPSP/MSCT Service Provider/PISP should take measures to ensure the authenticity of the Beneficiary as receiver of the message.
G-SG9	Given the importance of security, entities with direct relationships with Beneficiaries 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 Beneficiaries should adequately protect their personal security credentials. 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).
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 Originator ASPSP/Beneficiary ASPSP/MSCT Service Provider/PISP should implement adequate fraud monitoring systems to detect fraudulent SCT (Instant) transactions/R-transactions and MSCT related messages.

Table 20: Overview security guidelines for MSCTs in the Customer-to-PSP/MSCT service provider space

9.4 4 Overview

The table below shows the relationships between the threats identified (see Table 19) and the security requirements and best practices (see Table 20).

	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 21: Mapping security guidelines on threats for MSCTs

10 Security considerations for the payer-to-beneficiary space

In this chapter different technologies used for the interface between the consumer and the merchant or between two persons 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.

QR-code

A two-dimensional code consists of black 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 [47]. In the context of MSCTs, the QR-code is used as a means of payment initiation, in one of two modes;

- Merchant-presented QR-code - where the code contains data to identify the merchant and transaction

or

- Consumer-presented QR-code – where the code contains data to identify the customer.

In the case of a merchant-presented QR-code, the consumers need to have an MSCT application on their mobile device that has the capability of scanning the QR-code of the merchant and initiating an MSCT transaction.

In the case of a consumer-presented QR-code, the consumer can make purchases using data associated with themselves or their account and previously provisioned to their mobile device. This data may range from cardholder 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 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 merchant at the time of payment to complete the purchase.

This document only contains MSCT use cases with merchant-presented QR-codes as currently present in the market today.

A QR-code may contain both sensitive and non-sensitive payment data that can be used in different phases of the MSCT transaction, like “Request-to-Pay”, merchant transaction identifier, IBAN_ben, etc.

A QR-code code may be static, e.g., merchant 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 SCT (Instant) 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 (e.g., through encryption and digital signature based on public-key cryptography, see [15]).

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.

The integrity of the QR-code should always be checked if security mechanisms have been implemented (e.g. digital signature) and, if possible, the sensitive payment data retrieved could be checked against available data in the backend.

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 implemented[45]. 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.

[45]To 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.

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.

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.

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 [56]) are based on ISO/IEC 18092 [48] but have been extended for harmonisation with EMVCo and interoperability with ISO/IEC 14443 [46] 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 Forum[46] 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 mode[47], 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/beneficiary identification and transaction data.

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 [41]).
- 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 [41]). 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 [15]).
- Consider the use of emerging Web standards to mitigate major security risks such as the OWASP top 10 application security risks[48]. For example:
    - To prevent against scripting attacks by leveraging the specifications of the W3C Web Application Security Working Group[49]. 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 [73]), part of the FIDO2 suite of specifications[50].
    - 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 [74].

Additional guidance may also be found in "Securing the Web," a finding of the W3C Technical Architecture Group see [75].

[46] https://nfc-forum.org/product/nfc-data-exchange-format-ndef-technical-specification/
[47] An example is the Core NFC framework of iOS 11.
[48] See https://www.owasp.org/index.php/Top_10-2017_Top_10
[49] https://www.w3.org/2011/webappsec/
[50] https://fidoalliance.org/fido2/

10.3 Merchant applications

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

10.4 Additional security measures

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 the merchant data (e.g., 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 beneficiary 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 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).

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.

Securing the link payee name / IBAN_payee

For (instant) credit transfers, it is crucial that the link payee (beneficiary) name/IBAN_payee (beneficiary) 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 "Request-to-Pay 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 guidelines for mobile devices

The following security guidelines apply for mobile devices.

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 [59], [60], [61] and the GlobalPlatform documents [31], [32].
MD-SG3	There should be a mechanism to: • 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., • Rooting / jailbreaking a phone • App Downloading from untrusted sources. It is recommended that the MSCT service provider provides information to the customer 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 • Clearer messaging of permissions requested by given MSCT Application • Reduce set of permissions to only the necessary ones.

Table 22: Security guidelines for mobile devices

The following additional 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 consumer device. This detection is limited by the capabilities provided by the device and its operating system.

Device fingerprinting

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

Device binding

Mobile device binding refers a reliable and consistent verification of the mobile device used for MSCTs by registering the mobile device and binding it with a user credential, e.g. as part of the customer on-boarding process. 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 be found in [34] and [38]:

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.

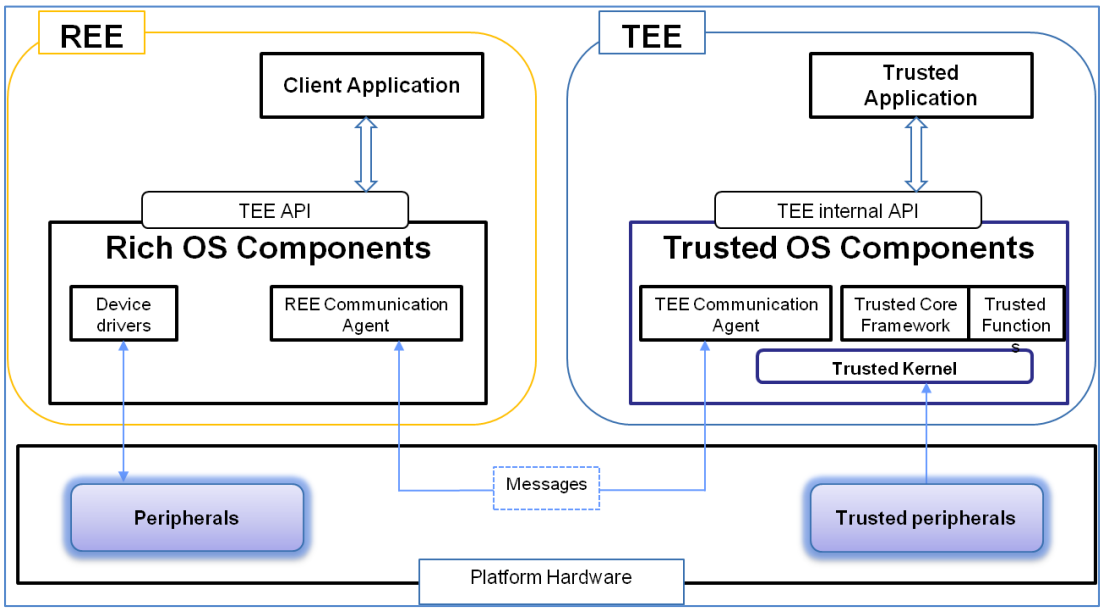


Figure 27: Example of a TEE model

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 [6]) which provides similar guidance in the context of card-based payments.

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 [8], the security of the overall mobile payments solution relies heavily on the effectiveness of the *server-side components and backend system* in handing 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 [65], 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.

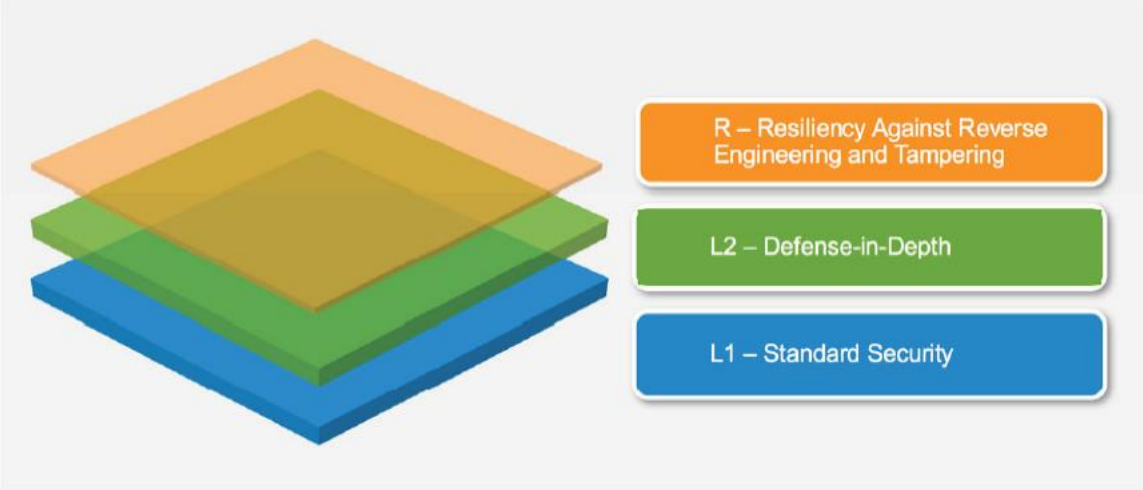


Figure 28: OWASP Security Verification Levels as per MASVS[51, 52]

Considering the context of the MSCT applications, it is appropriate to request at least the security verification level L2 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 [8].

[51] MASVS – Mobile Application Security Verification Standard, see [65].
[52] The figure is courtesy of OWASP

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 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	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. When the application receives or collects data for a payment initiation e.g., Request-to-Pay, QR-code) it could be altered.	This flaw exposes an individual user's data and can lead to account theft. Payment initiation transaction data may be tampered and funds redirected. A “man in the middle” proxy redirect might be in place.
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.	Masquerade as a legitimate payment initiation service provider to facilitate low-amount payments not requiring SCA. A “man in the middle” attack targeting customer credentials.
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	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

	insecure cookie for authentication endpoints; caching sensitive data; HTTP specific security requirements not implemented in full (e.g. refer to [64] for the list of baseline requirements)	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 23: 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 [63], [65] as well as the dedicated sections of the test guides [66] and [67] 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 [66] and [67] 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 [65], 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 [66], 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 [66] 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 [6]) for further security guidance.

13 Security guidelines for CDUVMs

In [11], 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 [11] 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 [11] 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 [11] 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 [12]

14 Guidelines for customer on-boarding by MSCT service providers

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

It is essential for payment services 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 customers. PSPs should furthermore use reliable methods for authenticating the identity and authorisation of established customers seeking to register for new MSCT services.

Customers may be registered for MSCT services by one of the following means:

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

In case of remote electronic registration, appropriate measures should be in place to control the connection such that unknown third parties cannot displace known customers (see also chapter 9).

This explicit registration aims to raise customer 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 customer device.

CoB-GL1	MSCT service providers which are not ASPSPs, should rely on the customer identification and authentication method used by the customer's ASPSP for the on-boarding of the customer for the MSCT service and the linking to the customer's account.

Know Your Customer (KYC) processes used by ASPSPs are set out by national regulatory authorities and are based on robust customer identification and authentication processes applied for the registration of customers. These are particularly important in the cross-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 and the greater difficulty in conducting effective credit checks on potential customers.

In case customers use PKI certificates for their identification when registering for an MSCT service, the customer identification used by the certificate authority should be accepted by the ASPSP and supervised by the financial supervisory authorities. In case eIDAS certificates for customers are used, the mutual recognition for the usage of these certificates is laid down in the eIDAS Regulation, which enhances cross-border trust.

CoB-GL2	Customers should explicitly register for an MSCT service, linked to one or more accounts from their ASPSPs. The guideline remains valid in case of a re-registration process.

CoB-GL3	To ensure that the request was made by the legitimate customer and their registered device, without disrupting the user experience, mobile device binding should be implemented.

This means that the trust of existing mobile devices could be leveraged. As an example a strong device ID could be used. This is a unique tamper resistant identifier that cryptographically binds a specific mobile device to a customer's identity, leveraging PKI capabilities.

CoB-GL4	MSCT service providers should have controls to ensure that credentials as appropriate are distributed to customers in a way that is trustworthy. The level of trust in the customer's identity should be maintained throughout the MSCT service lifecycle.

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

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 PIS service 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 models supported by the PSD2 [2] and the RTS [3], including references to additional information on these models. For the functionalities to be supported by the APIs used by these PISPs, the reader is referred to the document on "Recommended Functionalities (PSD2/RTS)" developed by the API Evaluation Group[53], the EBA Q&A[54] tool and the Opinion document published by the EBA (EBA-Op-2018-04, see Annex 1).

Redirection Model

The redirection model is an approach whereby the payer starts interacting with the MSCT application and is redirected via the same mobile device to either their ASPSP on-line banking website or to an 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 APIs, for example from the Berlin Group (see [71]), Open Banking Implementation Entity (OBIE) (see [62]) and STET (see [70]) support the redirection model.

Decoupled Model

The decoupled model is similar to the redirection approach, but here not the PISP, but the ASPSP request the payer to authenticate via the ASPSP's authentication application. Typically, the SCT transaction would be initiated from a browser or an online banking application on another device (e.g. a wearable not designed to make a payer authentication), while the payer authentication would be executed through a Dedicated Authentication application on the payer's mobile device or a dedicated authentication device.

[53] https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/api-evaluation-group-recommended-functionalities-psd2rts
[54] see https://eba.europa.eu/single-rule-book-qa

Through the decoupled approach, the payer authentication process is fully processed by the payer's ASPSP. The payer in this case, will not leave the PISP interface during the authentication process.

The currently published APIs, for example from the Berlin Group (see [71]), Open Banking Implementation Entity (OBIE) (see [62]) and STET (see [70]) support the decoupled model.

Embedded Model

In the embedded model, the payer authentication is performed using the PISP interface, e.g. on a merchant website. In a first step, the payer is identified via the entry of ASPSP credentials (e.g. identifier and password) which are transmitted to the payer's ASPSP. The strong customer authentication by the payer's ASPSP makes use of the PISP interface for the entry of the Authentication Code by the payer, the Authentication Code is subsequently transmitted by the PISP to the payer's ASPSP for verification.

The currently published APIs, for example from the Berlin Group (see [71]) and STET (see [70]) support the embedded model.

Delegated Model

In the delegated model, the strong customer authentication is performed by the PISP, not the payer's ASPSP. However, this model raises a number of challenges in terms of providing trust to the ASPSP and in terms of liabilities in case of fraudulent payments and is therefore subject to an agreement between the PISP and the payer's ASPSP and an on-boarding of the payer by the PISP.

15.3 SEPA Proxy Lookup Service

The mobile P2P payment services in the market today are mostly domestic solutions that require both payer and beneficiary (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 beneficiary (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 beneficiary. 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 [22]).

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 beneficiary based on their mobile phone number, if the

beneficiary is not registered in their own mobile P2P payment service. As such it enables MSCTs based upon the mobile phone number of the beneficiary, between a payer and beneficiary 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 beneficiary's mobile phone number. Subsequently, the payer's mobile payment service provider can initiate an MSCT to the beneficiary. The EPC has defined an SPL scheme[55] 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 beneficiary 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. The SPL service will transfer the incoming IBAN request to the network of registered mobile P2P payment service providers.

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 will select the most recent entry to be presented to the payer's mobile P2P payment service provider. This means that the SPL service is in fact operating as a routing network (also sometimes referred to as a "switch") and is not a dedicated central IBAN database.

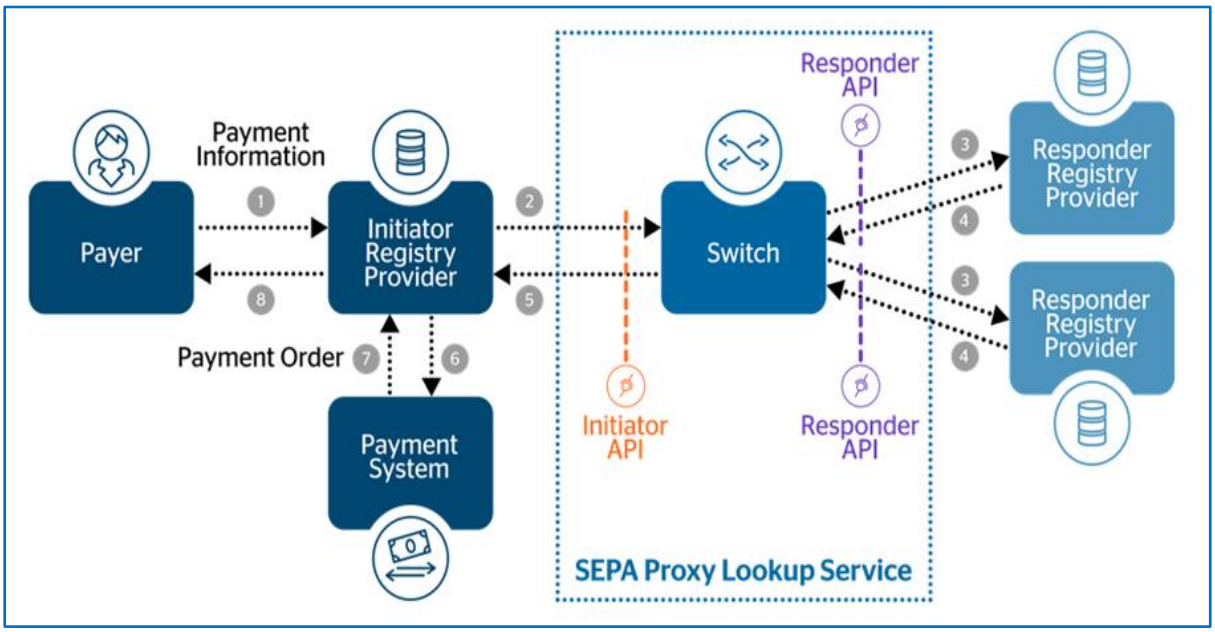


Figure 29: The SEPA Proxy Lookup Service

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

[55] see https://www.europeanpaymentscouncil.eu/what-we-do/other-schemes/sepa-proxy-lookup-scheme

implementation of the APIs to IRPs and RRPs, the implementation of the mapping (mobile number to IBAN). Besides that, the SPL service also contains support functions like reporting, statistics and billing.

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.

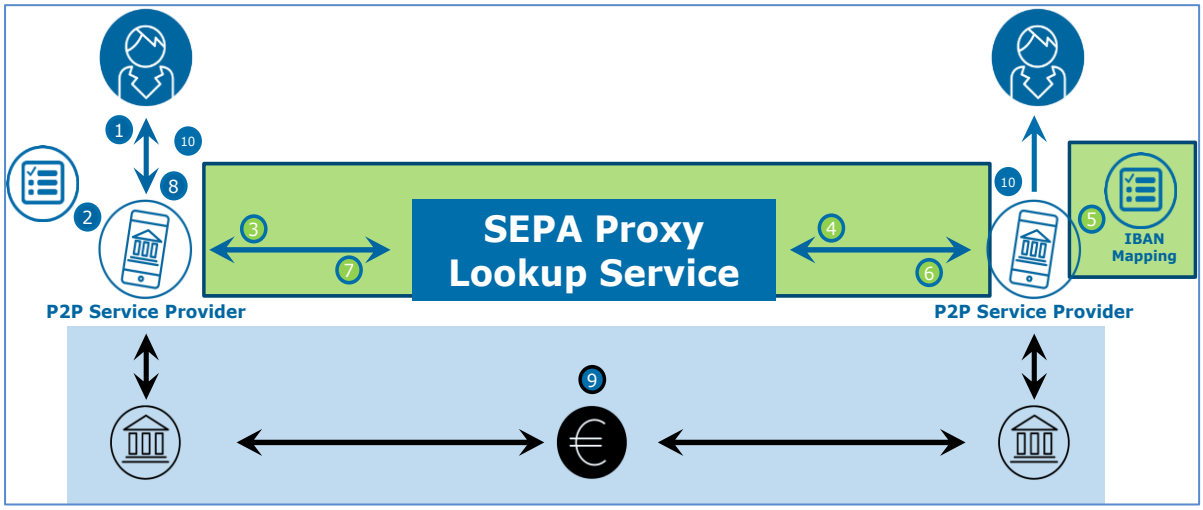


Figure 30: MSCT using the SEPA Proxy Lookup Service

In the figure above, the following steps are illustrated:

Step 0 (prerequisites)
Both the payer's and beneficiary's mobile P2P service providers should be registered participants in the SPL service.

Both the payer and beneficiary 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 service)
The payer opens the mobile application of their mobile P2P service provider to transfer funds to the beneficiary. The mobile P2P application checks the phone book of the payer on their mobile device to retrieve the mobile number of the beneficiary.

Step 2 (outside the SPL service)
Subsequently based on this mobile phone number, the payer's mobile P2P payment service provider checks first if the beneficiary is a known customer in their local directory, in which case the IBAN and name of the beneficiary are retrieved. If not, it checks the phone book of the payer to get the mobile number of the beneficiary.

Step 3
If not present in their local directory, the payer's mobile P2P payment service provider sends a request to the SPL service with the beneficiary's mobile phone number.

Step 4
The SPL service 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 beneficiary's account data based on the SPL scheme rules if multiple replies are received.

Step 8 (outside the SPL service)
The payer's mobile P2P payment service provider requests the payer a strong customer authentication based on the beneficiary account data and transaction amount.

Step 9 (outside the SPL service)
The (instant) credit transfer is initiated by the payer's mobile P2P payment service provider and the funds are transferred towards the beneficiary's ASPSP.

Step 10 (outside the SPL service)
- The beneficiary 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 17) also different mappings could possibly be requested from the SPL service (e.g., beneficiary 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 beneficiary (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 2017[56] as the

[56] see https://www.ecb.europa.eu/paym/retpaym/shared/pdf/8th-ERPB-meeting/EIPP_working_group_report.pdf?522a05eb9fde0192136bc7fdf062ac4f

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 [24]).

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/beneficiary, sent to a debtor/originator. As reflected in the statement published after the ERPB meeting of November 2018[57], the EPC was invited to coordinate the necessary work in this area and as a result, the RTP multi-stakeholder group (RTP MSG, see [18]) was created in the beginning of 2019. The objective of this group is 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 with the option to include them in the SCT and SCT Instant 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 eco-systems 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.

[57] see https://www.ecb.europa.eu/paym/retpaym/shared/pdf/10th-ERPB-meeting/Statement.pdf?32cf8f15483d29182fc1d72f40bbf7b4

16 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 [6] 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 [7] through [12] (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 [13] through [22] (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. Moreover, ETSI has specified the requirements for a "Smart Secure Platform"[58] (see [25]) (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 [27] through [30] (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 [31][31] through [33] (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).

[58] Enabling the provision of value-added services relying on authentication of the user, regardless of the mobile device, communication channel and underlying technology - taking into account the requirements for mobile payments.

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 is involved with mobile payments in ISO TC68 SC9 (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 [50] through [52] (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 [48]) 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 [54] to [57] (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 [63] through [67] (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 [68]) (www.pcisecuritystandards.org).

17 MSCT interoperability aspects

17.1 Introduction

As illustrated in the MSCT use cases (see chapter 7), most implementations for MSCTs in the market today are based on the following model depicted in the figure below, which is also sometimes referred to as a "closed loop" model. This MSCT model is applicable for P2P, C2B (in this case the payer is a consumer and the beneficiary is a merchant) and B2B (instant) credit transfer transactions and typically cover a certain geography (e.g., within (part of) a country).

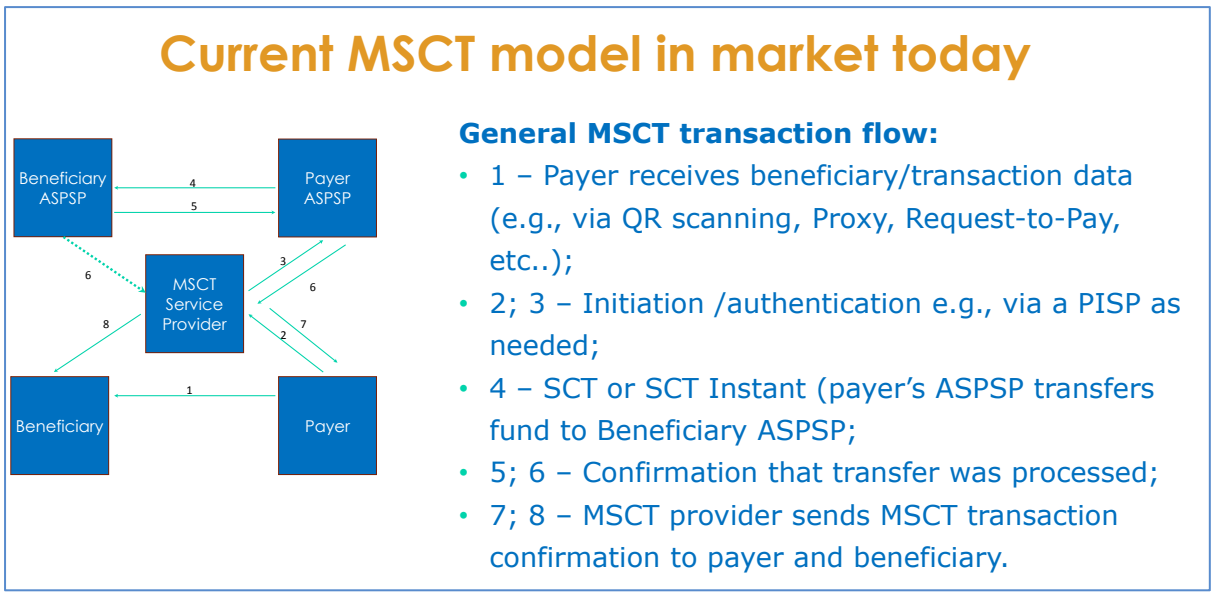


Figure 31: MSCT models in the market today

Notes:

- Steps 4 and 5 in the interbank space are not affected with respect to interoperability of MSCTs;
- The dotted line between the MSCT service provider and the beneficiary ASPSP means that for some MSCT services, this link may be present, in others there is no link.

In order to achieve interoperability, the main issue is how to interconnect these different MSCT services as illustrated in the figure below.

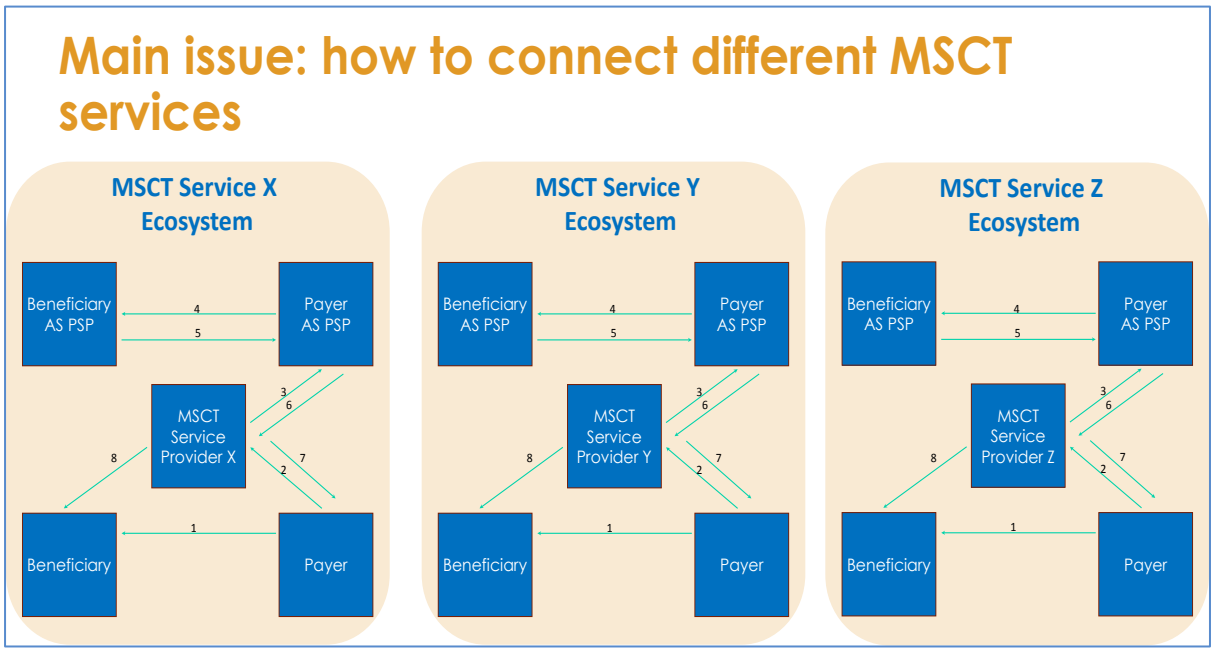


Figure 32: How to interconnect different MSCT services?

Below an analysis is made separately for each type of MSCT transaction.

17.2 Interoperability analysis

In this section a separate analysis will be performed on the main interoperability aspects for each type of MSCT transaction (P2P, C2B and B2B).

Person-to-Person (P2P) MSCTs

For P2P MSCTs, the interoperability between the different P2P MSCT solutions, when a mobile phone as proxy is used for the beneficiary, is ensured by the implementation of the SPL scheme (see section 15.3). Note that today the SPL scheme only covers a mobile phone number as proxy for the beneficiary and only mandates to return the beneficiary's IBAN for the mobile phone number, and not necessarily the beneficiary's name. This may be an issue in case the beneficiary's name is not known by the payer or 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 P2P MSCT payments. In principle this scheme could be considered sufficient from a pure "technical perspective" if the beneficiary is known by the payer, to achieve full interoperability. However, for customer friendliness other types of proxies might need to be covered.

In addition, the following confirmation / notification messages (see section 8.7) have been identified as being key factors for customer adoption:

- Confirmation of receipt from the MSCT service provider to the payer about the receipt of the SCT (Instant) instruction;

- Notification of payment to the beneficiary by the MSCT service provider or beneficiary's ASPSP;

- Notification of payment to the payer by the MSCT service provider or payer's ASPSP.

The customer experience could further be enhanced by the specification of a "request-to-pay" message that a beneficiary could use to request the MSCT payment to the payer and may be sent e.g. by a messaging service (that needs to be linked to an MSCT application) or a QR code (including the beneficiary's account details) that could be scanned by the payer's mobile device from the beneficiary's mobile device.

Customer-to-Business (C2B) MSCTs

As said before, the current market solutions are all based on the model depicted in Figure 31: MSCT models in the market today whereby both the consumer and merchant 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"?

More in particular related to customer adoption, similar confirmation-notification messages as described above in the P2P section would need to be specified. In addition, it is a key issue for merchants to be able to receive reconcile the transaction with the payment.

Business-to-Business (B2B) MSCTs

For B2B, the reconciliation on the beneficiary side appears to be a major issue – more in particular for SCT Instant payments; although it should be recognised that this problem reaches obviously beyond MSCTs. Immediate information on the incoming payments, processed by the beneficiary'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 Instant by corporates. With SCT Instant, the EPC has defined messages from initiator to ASPSP, from ASPSP to ASPSP (pacs.008) and ASPSP to initiator but not from ASPSP to beneficiary. Corporates would like to see an immediate "ASPSP to beneficiary message" in the context of SCT Instant closing the chain of information from initiator to beneficiary.

17.3 Interoperability solutions

Introduction

The different interoperability aspects described in section 17.2 could be represented in a 3-layer approach as shown in the figure below.

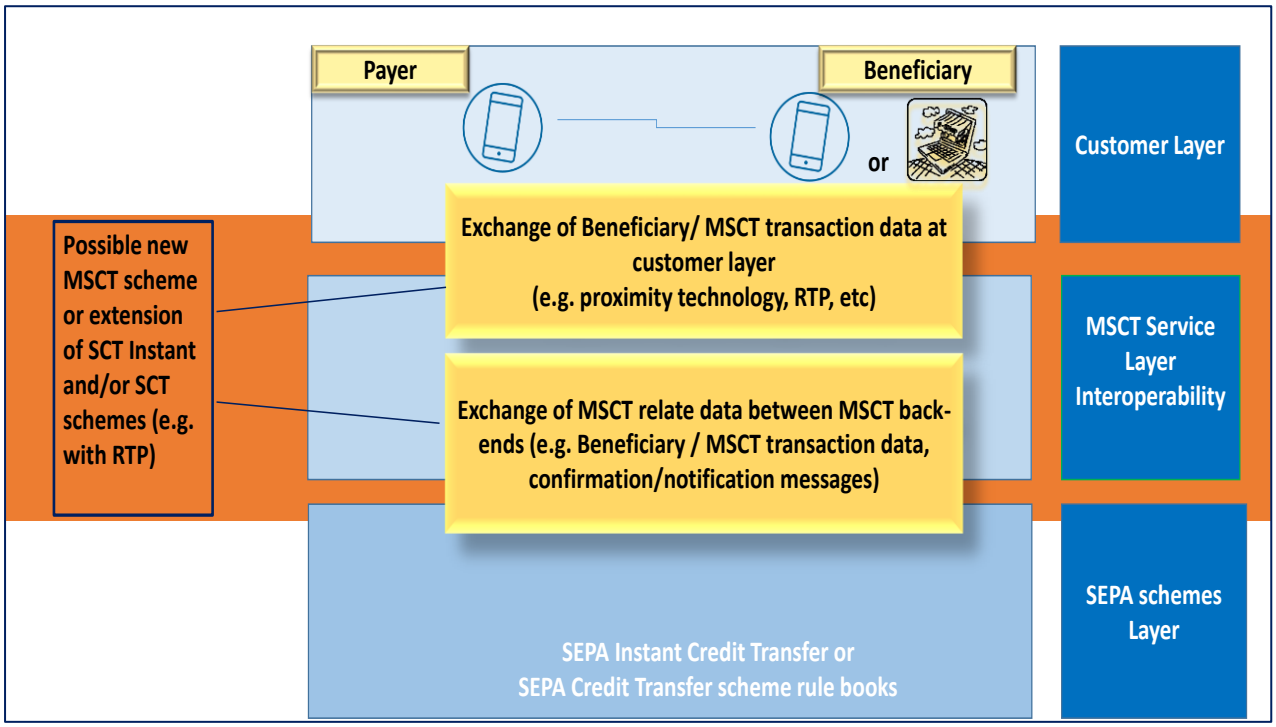


Figure 33: MSCT interoperability layers

In what follows, a high level overview will be provided on potential solutions for this interoperability gaps.

Customer layer

Introduction

It is generally recognised that the customer layer, being it the MSCT application on the payer's mobile device or the MSCT application on the retailer's POI, is in the competitive space of the MSCT service. However, a minimum standardisation would be needed on how the beneficiary/MSCT transaction data are exchanged between the payer and beneficiary.

In case the beneficiary's name, IBAN and transaction amount are known/ entered on the mobile device by the payer, the respective SCT Instant and SCT schemes would ensure interoperability for MSCTs. In all other cases, e.g. if proximity technologies, proxies (e.g. mobile phone number) or tokens are used to make this data available to the payer, interoperability issues arise.

As mentioned before, in case a mobile phone number is used as proxy for the beneficiary, the interoperability for MSCTs could be ensured by the SPL service (see section 15.3) in case the beneficiary's name is known by the payer. In view of the current market situation and the fact that the usage of RTP for MSCTs will be covered by a dedicated RTP MSG (see section 15.4), this document focuses below on the interoperability based on QR-codes at the customer layer.

MSCT QR-code

For the proposed standardisation of a generic MSCT QR-code format, work is still being carried out by the MSG MSCT in coordination with other mobile payment initiatives in the market. The aim is to define a unified QR-code format for MSCTs which can be used in the various payment contexts (e.g., P2P, retail payments, including both in-store (proximity (also including a poster)) and e- or m-commerce). This unified QR-code will be based on a common minimal data set to be exchanged between payer and payee to enable MSCT interoperability across SEPA. This will be published in a separate document.

MSCT service layer

The interoperability solutions at this layer will depend on the beneficiary/MSCT transaction data that has been directly exchanged between the payer and beneficiary at the customer layer.

In case, the full beneficiary/MSCT transaction data is exchanged directly between the beneficiary and the payer, the MSCT transaction can be immediately initiated by the payer while the SCT Instant and SCT scheme rules ensure the interoperability. What needs to be

developed is the infrastructure needed to exchange the notification/acknowledgement messages[59] to the payer and beneficiary (see section 8.7).

A possible option could be the specification of additional requirements for the exchange of these notification messages by the respective ASPSPs to their customers through an extension of the SCT Instant and SCT rulebooks, hereby also taking into account the MSCT service provider as a possible new stakeholder in the MSCT ecosystem[60].

Another option would be the development of a dedicated infrastructure for the exchange of these messages. This could be implemented through a central routing service, for example by a possible extension of the SPL service, or via a more distributed platform (e.g., based on blockchain technology). Hereby the minimum data elements required in the message flows would need to be standardised.

In case only a proxy (typically linking only to beneficiary data) or a token (typically linking to both beneficiary data and MSCT transaction data) is directly exchanged between the beneficiary and the payer, the corresponding beneficiary data and/or MSCT transaction data needs to be retrieved at the appropriate entity (e.g. MSCT service provider, token provider, etc.) before the MSCT transaction can be initiated. Moreover, the beneficiary name and transaction amount need to be displayed to the payer though their mobile device for authentication of the MSCT transaction.

Similar as described above, the infrastructure needed could be implemented through a central routing service or via a more distributed platform. However, in this case, more message flows will need to be specified, while again the minimum data elements for these messages would need to be standardised.

The implementation of a central routing service could be achieved through a distributed infrastructure based on local directories maintained by for example the MSCT service providers or through a central database.

Clearly, a more detailed technical analysis is required on the different available options for the interoperability infrastructure needed which will be undertaken by the multi-stakeholder group over the coming months and will result in a separate deliverable. Next to the technical aspects, also the operating rules, liabilities, adherence to these requirements and governance should be addressed[61]. This could be achieved through the set-up of a dedicated “MSCT scheme” to which the (existing) MSCT providers should participate to ensure interoperability of MSCT services.

[59] Currently the SCT Instant rulebook requires the transmission of the negative confirmation message as notification by the payer’s ASPSP to the payer (see [19]), while the SCT rulebook does not cover any customer notification (see [13]).
[60] In case the MSCT provider is not an ASPSP.
[61] See also the ERPB report Instant Payments at the POI at https://www.ecb.europa.eu/paym/groups/erpb/html/index.en.html

18 Additional challenges and opportunities

By analysing the different MSCT solutions that are currently available in the market, the following challenges in addition to those described in chapter 17 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.

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 the "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 as well as an issue by the ECSG and included in their November 2019 stocktake report to the ERPB[62].

[62] See https://www.ecb.europa.eu/paym/groups/erpb/html/index.en.html

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 on the market today to support competitiveness; examples are an open (but secure) 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 on mobile device usage for payment services initiation is in many countries still low. In absence of an MSCT 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.

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 leave 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.

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 16) 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 recent announcement by ETSI about the finalisation of their specification of requirements for a "Smart Secure Platform" [25] (enabling the provision of value-added services relying on authentication of the user, regardless of the mobile device, communication channel and underlying technology) (see also recommendation F in [23]).

Unclarity in European rules and regulations

There are still unclarities in EU rules and regulations such as the PSD2 [2], the RTS [3] and the GDPR [4], 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), 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).

Customer on-boarding

The trust in MSCTs, more in particular for cross-border payments, strongly relies on the mutual recognition and trust in customer on-boarding procedures and mechanisms. Weak customer on-boarding procedures may lead to customer 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 beneficiary name

It is important for trust and transparency that the commercial brand name of the beneficiary 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 beneficiary.

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. However more transparency to the customer is expected to be ensured by new regulation[63].

[63] 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)

Opportunities

Whilst there are challenges to achieve interoperability for MSCTs as described in chapter 17 and above, the introduction of these solutions also offers a number of opportunities to customers.

For some MSCT payments, the initiation of the payment involves an exchange of data that allows the identification of a known customer 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.

Last but not least, the take-up of MSCTs would enhance the customer choice (both for the consumer and the merchant) with respect to payment instruments available for retail payments.

19 Conclusions

This document provides interoperability guidance for MSCTs. It aims to reflect the current state of play and market situation at the time of specification 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/beneficiary acknowledgements and notification messages, it focuses on the technology and security used in the customer-to-ASPSP space, since the SCT Instant and SCT transactions as such have already been specified in the respective rulebooks (see [13] and [19]). It furthermore specifies various security guidelines for MSCTs (e.g. MSCT app, CDUVM, etc.). Finally, the document identifies the main interoperability issues and barriers detected 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 17).

This includes:

- the standardisation of beneficiary (payee)/transaction data between the payer and the beneficiary e.g. by the specification of an MSCT QR-code, enabling multiple payment contexts;

- the availability of an infrastructure to interconnect the different MSCT providers notably for the support of token/proxy-based MSCTs and MSCT confirmation and notification messages to customers (payers and beneficiaries);

- 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 scheme” to which the (existing) MSCT providers would participate to ensure interoperability of MSCT services.

Regarding the SEPA Proxy Lookup (SPL) scheme (see section 15.3) that has been developed for the support of P2P MSCTs, it should be noted that today it covers a mobile phone number as proxy for the beneficiary and only mandates to return the beneficiary’s IBAN for the mobile phone number. However the beneficiary’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 by the new multi-stakeholder group on this topic [18] will complement the current document and will further contribute to the customer adoption of MSCTs.

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 requirements of a “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 [25] is of utmost importance. The multi-layered functional and security approach taken by ETSI will ensure more flexibility and portability for mobile payment providers.

There is still a dependency of the consumer on the type of mobile device with respect to the choice of MSCT services. Therefore, access to the mobile device contactless interface in order to ensure that the consumer can have a choice amongst payment applications from different mobile payment providers, independently of the mobile device and the operating system used, should be ensured by all handset manufacturers and mobile OS developers (see also [23]).

The impact of the new PSD2 [2] with the RTS [3] and the GDPR [4] on payments and more in particular the unclarity regarding certain provisions as well as their interplay when applied to MSCTs might be a barrier for the quick take-up of MSCTs (see chapter 8).

Although some of the issues mentioned above have already been identified in the ERPB report in 2015 [23], the multi-stakeholder group recognises that the most urgent work needed is a further analysis of the interoperability issues described in chapter 17 and above.

The multi-stakeholder group has organised focused work on these interoperability issues through a dedicated technical expert work-stream. Note that also the ERPB has established a working group for instant payments at POI that further lookinto the major challenges for this type of payments[64].

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.

[64] See https://www.ecb.europa.eu/paym/retpaym/shared/pdf/Mandate_of_the_working_group_on_instant_payments_at_the_POI.pdf

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.

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	http://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]	4th 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')[65]	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

[65] 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/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
[9]	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
[10]	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
[11]	EBA/GL/2018/05 Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2)	https://www.eba.europa.eu/documents/10180/2281937/Guidelines+on+fraud+reporting+under+Article+96%286%29%20PSD2+%28EBA-GL-2018-05%29.pdf/5653b876-90c9-476f-9f44-507f5f3e0a1e
[12]	ESA JC/GL/2017-16/ Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service	https://esas-joint-committee.europa.eu/Publications/Guidelines/Joint%20Guid

	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	elines%20to%20prevent%20terrorist%20financing%20and%20money%20laundering%20in%20electronic%20fund%20transfers%20(JC-GL-2017-16).pdf

Table 24: Overview regulatory documents

Annex 2 Overview MSCT use cases

Below an overview is provided on the characteristics of the MSCT use cases described in chapter 7.

Use case ref.	Mobile Techn.	Payer interface provider (s)	Customer experience	Proxy type	Authentication	Description of the underlying service
P2P1	Mobile browser	ASPSP	Payer uses a mobile browser to access their mobile banking service and sends funds to a beneficiary who holds an account with the same or with a different ASPSP.	IBAN_ben in full or pre-registered	Static UserID + Passcode	The payer accesses their mobile banking environment, authenticates and sends a SCT (Inst) instruction.
P2P2	MSCT app	ASPSP	Payer selects a functionality made available by a previously downloaded MSCT app and sends funds to a beneficiary who holds an account with the same or with a different ASPSP.	Alias (SPL) - mobile phone number	Strong - Mobile code	The MSCT (P2P) app enables the originator to select a beneficiary from the list of contacts and prepares an SCT (Inst) Instruction using the mobile number of the beneficiary as an alias. The MSCT app uses the SPL service to retrieve the beneficiary account data.

	P2P3		MSCT app + messaging app		MSCT service provider + Messaging service provider		Beneficiary selects a functionality made available by a previously downloaded MSCT app, enters the amount that is split amongst # payers and enters personal message. Beneficiary sends a payment request via the messaging app and selects the payers in the address book. The message contains the amount, the personal message and the mobile phone number of the beneficiary. The payers click on the request and open their MSCT app. The MSCT app uses the SPL service to retrieve beneficiary's account and sends funds.		Alias (SPL) - mobile phone number		Strong - Fingerprint	The MSCT (P2P) app enables the originator to split the amount and connect to a messaging service that also holds an address book to select the payers. The MSCT Instant application uses the SPL service to retrieve the beneficiary account
	P2P4		MSCT app + QR-code scanner		ASPSP		The beneficiary selects a functionality made available by the MSCT app and enters the amount to be paid. The MSCT app generates a QR code containing beneficiary name, IBAN and amount. Payer scans the QR-code and		QR-code		Strong - Facial recognition	The beneficiary uses an MSCT app to generate a QR-code containing the transaction details for the payer to scan.

						acquires the beneficiary data and confirms the operation.					
	C2B1		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 beneficiary data, the amount and the invoice nr.		QR-code		Strong - Mobile code	The beneficiary generates a QR-code containing payment details and prints it on an invoice for the payer to scan.
	C2B2		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 beneficiary has downloaded a specific application on the POI. ASPSPs need to be registered with the same MSCT Instant service provider.		QR-code		Strong - Mobile code	The merchant POI can produce a dynamic QR-code containing all data necessary to request an SCT Inst payment.

	C2B3		MSCT app + QR-code scanner + MSCT app 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.		QRCode		Strong - Fingerprint	The user has a separate authentication application on his/her mobile device that has been previously linked to the MSCT Instant application, which allows to perform a digital signature.
	C2B4		Merchant application + PISP service		ASPSP + Merchant + PISP		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 enters user-ID and identification data and dynamic authenticator to confirm the transaction.		Pre-registered consumer IBAN		Strong - UserID + Pasccode and Dynamic authenticator	The merchant app enables in app shopping. An SCT Inst Instruction is forwarded to the consumer's ASPSP through the PISP. The user accesses their mobile banking environment.
	C2B5		Mobile browser		ASPSP + PISP		The consumer is redirected from a merchant website to the mobile banking service of their ASPSP in a way that meets the requirements for re-direction according to PSD2.		IBAN_merch		Strong - Dynamic authenticator	The consumer is redirected with the transaction details including the beneficiary's name, transaction amount and IBAN_merch to their ASPSP portal. The merchant

											webpage embeds an iFrame provided by the PISP.
	C2B6		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		Strong - Fingerprint	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.
	B2B1		eIPP app + MSCT app		ASPSP + MSCT provider + eIPP solution provider		The beneficiary 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_ben. The payer receives the Request-to-Pay in their EIPP app and clicks on the request. This opens the		IBAN_ben		Strong - Fingerprint	The beneficiary 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

							MSCT app that retrieves and displays the invoice information. The payer confirms the transaction.					amount, beneficiary name and IBAN_ben.

Table 25: Overview characteristics MSCT use cases

Annex 3: The multi-stakeholder group

The following organisations have contributed to the development of this document through participation in the multi-stakeholder group Mobile Initiated SEPA (Instant) Credit Transfers (MSCTs):

DNB Bank – representing EPC
Crédit Mutuel - representing EPC
KBC - representing EPC
AIB on behalf of Banking & Payments Federation Ireland (BPFI) - representing EPC
Estonian Banking Association- representing EPC
La Banque Postale - representing EPC
Intesa Sanpaolo on behalf of Italian Banking Association (ABI) – representing EPC
IKEA - representing EuroCommerce
Carrefour - representing EuroCommerce
Total - representing EuroCommerce
Colruyt - representing EuroCommerce
European Consumer Organisation (BEUC)
Gemalto – representing Smart Payment Association
OpenWay
Payconiq
EquensWorldline
UAB „Mobilieji mokėjimai“ (MOQ)
SIA S.p.A.
TAS Group
National Clearing House KIR Poland
European Association of Corporate Treasurers (EACT)
KPN – representing GSMA
Orange - representing GSMA
W3C
Eurosystem – as observer
European Central Bank (ECB) – as observer
European Commission – as observer

Table 26: The multi-stakeholder group

The multi-stakeholder group further wishes to thank to PPRO, HPS and Tink 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