European Payments Council

Technical Interoperability for MSCTs based on payer-presented data

EPC096-20 / 2020 Version 1.0 / Date issued: 8 December 2020

Public

Technical Interoperability for MSCTs based on payer-presented data

European Payments Council

European Payments Council AISBL,
Cours Saint-Michel 30 B-1040 Brussels
T +32 2 733 35 33
Enterprise N°0873.268.927
secretariat@epc-cep.eu

EPC096-20
Version 1.0
8 December 2020

Public

Table of Contents

1. Introduction

The main focus of this document is to analyse in further detail the interoperability aspects related to mobile initiated SEPA (instant) credit transfers (MSCTs) as identified in the *Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance* (MSCTG IG- EPC269-19v1.0).

The document discusses the interconnectivity and related functionality amongst the respective MSCT service providers of the payer and payee for MSCT use cases based on payer-presented data (e.g., through a QR-code). It further specifies the data to be exchanged between the payer and the payee to enable the initiation of such MSCTs. Examples for illustrative purposes of MSCTs use cases based on payer-presented data may be found in the MSCT IG (see the use cases P2P-3 and C2B-4, 5 in chapter 7) while additional examples of MSCT use cases based on consumer-presented data in Consumer-to-Business (C2B) payment contexts may be found in the Annex to this document.

Note also that the MSG MSCT intends, in future work, to analyse MSCTs involving a PISP or a Collecting PSP[1] (CPSP) on behalf of the merchant and their impact on the interoperability of MSCTs.

Throughout the document, the terminology, abbreviations and references specified in the MSCT IG (EPC269-19v1.0) apply. Throughout this document, a "Payment Request" refers to the messages sent by the payee to the their MSCT service provider and from the payee MSCT service provider to the payer MSCT service provider, as appropriate, including all transaction data for presentation to the payer to enable them to initiate a transaction[2].

This document covers Person-to-Person (P2P) and Consumer-to-Business (C2B) payment contexts (see chapter 7 in the MSCT IG). At a later stage, further analysis is required whether the interconnectivity and related functionalities are also sufficient to cover the requirements for Business-to-Business (B2B) payment contexts as well.

Moreover, this document focuses on the usage of QR-codes as proximity technology. Note however, since other proximity technologies such as NFC and BLE are used in the market today for mobile initiated (instant) credit transfers in a uni-directional mode, the analyses made in this document remain valid.

It should be noted that this document only deals with the technical interoperability of MSCTs and the derived requirements for interconnectivity of MSCT service providers. Next to these technical requirements, agreements between the MSCT service providers are needed to cover for operating

[1] A collecting PSP that has a contract with the merchant to collect MSCT transactions on their behalf.

[2] An implementation example is provided by the SEPA Request-to-Pay (RTP) messages (see https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/12th-ERPB-meeting/Report_from_the_RTP_MSG.pdf?efe8385c4196f8094d5b6625f7ffdc79.
It is further to be noted that the interoperability aspects related to the exchange of the so-called SEPA "Request-to-Pay" messages is currently addressed by the EPC through the development of a dedicated interoperable SEPA RTP scheme. Note that other RTP solutions are already present in SEPA today.

rules, liability, recognition label, etc.). These could for instance be covered under a "to be developed" dedicated framework.[3]

Note that this document is now released as a standalone document, but the aim is to integrate it into the next release of the MSCT IG.

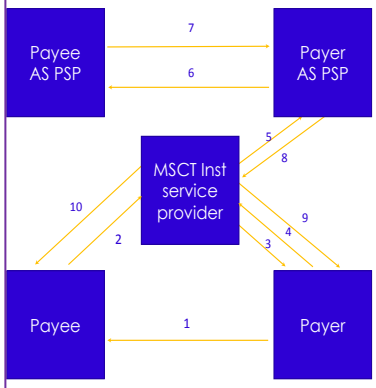
A separate document on the interoperability of MSCTs based on payee-presented data has already been published.

2. MSCT Interoperability Challenges

2.1 MSCT interoperability

Payer and payee are customers of the same MSCT service provider
In the figure below, a generic description is provided of the process flow for an MSCT transaction based on payer-presented data if both the payer and the payee are customers of the *same* MSCT service provider (see section 2 of this document and chapter 7 in the MSCT IG).

Current model in the market for MSCTs based on payer-presented data



General MSCT transaction flow:

- Payee receives payer-presented data (e.g. via QR-code) (1)
- Payee sends payment request message with payer token and transaction data (2 & 3)
- Transaction initiation / authentication (4 & 5)
- SCT or SCT Instant (payer's AS PSP transfers funds to payee's AS PSP) (6);
- Confirmation that transfer was processed (7 & 8);
- MSCT service provider sends transaction notification to payer and payee (9 & 10).

Figure 1: Current MSCT service model in the market for MSCTs with payer-presented data

[3] The need for such a framework has also been identified in the ERPB report Instant Payments at the POI (see https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/12th-ERPB-meeting/Report_from_the_ERPB_WG_on_instant_at_POI.pdf?efe8385c4196f8094d5b6625f7ffdc79) and has been addressed by a new ERPB WG (see https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/Mandate_of_the_working_group_on_instant_payments_at_the_POI.pdf.

Payer and payee are customers of different MSCT service provide

In case the payer and payee are customers of different MSCT service providers, the section 17.2 of the MSCT IG already identifies the high level requirements for interoperability related to the interconnectivity between those providers that are described below.

The challenge is how to interconnect two different MSCT service solutions as depicted in the figure below. In other words, how can the necessary exchange of transaction data between MSCT service providers be ensured such that a payer that is on-boarded with MSCT service provider "X" can make an (instant) SEPA credit transfer to a payee that is on-boarded with MSCT service provider "Y" as shown below.

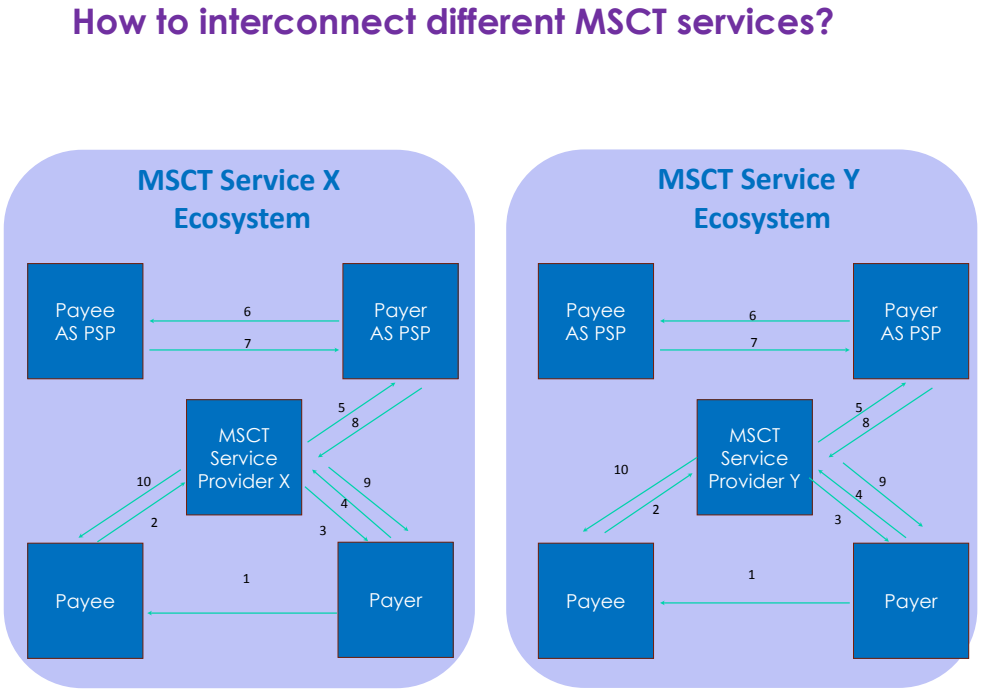


Figure 2: Interconnection of MSCT services based on payer-presented data

The MSCT service provider X is connected to the payer ASPSP. The interconnection needed for the execution of the Instant SCT or SCT transfer between the respective ASPSPs (following the receipt by the payer ASPSP of the SCT Instant or SCT initiation request from the payer and the subsequent authentication of/confirmation by the payer) to ensure interoperability across SEPA, is already covered in the SCT Instant and SCT rulebooks (see EPC004-16 and EPC125-05 respectively).

As a consequence, the MSCT IG (EPC269-19v1.0) has focused for an MSCT transaction on what is referred to in Figures 25 and 26 in chapter 8 of the MSCT IG as *Payment Preparation (or prepayment), Initiation and Authentication* and *Payment Completion* phases related to an Instant SCT or SCT transaction.

It should further be noted that for mobile initiated SCT Instant or SCT transactions as described in the MSCT IG (EPC269-19v1.0 - chapter 8), the strong customer authentication (SCA) of the payer by their ASPSP is in the payer-to-payer ASPSP domain and is as such not impacting the interoperability.

Neither is the interoperability impacted if the payer ASPSP has delegated the strong customer authentication to the payer MSCT service provider or to a so-called authentication service provider.

What is however impacting the interoperability (as stated already in section 17.2 of the MSCT IG) and will be further analysed in this document are the following three issues:

- How is "payer-presented data" made available by/exchanged from the payer to the payee?
- How is "transaction data" made available by the payee to the payer for the strong customer authentication with dynamic linking[4]?
- How are the acknowledgement/notification messages provided by the respective MSCT service providers to the payer and the payee?

These three interoperability aspects will be analysed in more detail below. For each aspect, a reference is included to (a) specific step(s) illustrated in Figure 4 in section 4.2 of this document.

It is further noted that there is also a possible additional requirement to define the technical support needed between MSCT service providers for the implementation of a fee structure. However, this topic will not be further analysed in this document.

2.2 Exchange of payer-presented data

To achieve interoperability of MSCTs based on payer-presented data, at least *payer identification data* (which enables the payer MSCT service provider to identify the payer) and an *identifier of the payer MSCT service provider* are needed in this payer-presented data (see steps 2 and 3 in Figure 4 below).

The *payer identification data* is defined by the payer MSCT service provider and may take a variety of forms and may be static or dynamic. However, this payer identification data has no impact on the interoperability between MSCT services. This payer identification data will need to be transferred as part of the Payment Request message from the payee to their MSCT service provider and further to the payer MSCT service provider, see section 2.3 below.

The *identifier of the payer MSCT service provider* is needed by the payee MSCT service provider and subsequently by the HUB to know where to route the Payment Request message, see sections 2.3 and 4 below.

2.3 Exchange of transaction data

The transaction data (payee data and payment data) needed by the payer for the initiation of the MSCT transaction is to be exchanged between the payee and the payer via their respective MSCT service providers[5] as follows:

[4] Subject to further clarifications to be provided by EBA on the questions 2020_5366 and 2020_5367.

[5] If a bi-directional proximity technology is used between the payer's mobile device and the payee's device, a direct transfer of the transaction data may be possible but will not be further investigated in this document, since the process flows would be similar to MSCT use cases based on payee-presented data (see EPC312-19).

- The transaction data is provided by the payee to their MSCT service provider via a "Payment Request"[6] message. Thereby the payer identification data and the identifier of the payer MSCT service provider will need to be retrieved from the payer-presented data by the payee and included, next to the transaction data, in the Payment Request message. The Payment Request message between the payee and their MSCT service provider should further at least contain a transaction identifier, the name and the IBAN[7] of the payee and the transaction amount (see step 5 in Figure 4 below).
- The Payment Request message is transferred by the payee MSCT service provider via the HUB to the payer MSCT service provider using the identifier of the payer MSCT service provider received (see step 6 in Figure 4 below).
- The payer MSCT service provider identifies the payer and possibly their IBAN from the token included in the Payment Request message and provides the transaction data (at least the transaction amount and the name and the IBAN of the payee) to the payer for authentication purposes (see steps 7 and 8 in Figure 4 below).

2.4 Acknowledgement/notification messages

The MSCT IG has identified the following messages needed (see section 8.7 in EPC269-19v1.0) in that respect:

- Acknowledgement of receipt provided to the payer by their MSCT service provider on the receipt of the SCT (Instant) instruction;
- Notification of payment to the payee by their MSCT service provider;
- Notification of payment to the payer by their MSCT service provider.

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

Since the acknowledgement message is between the payer and their MSCT service provider, this as such is not impacting the interoperability across SEPA and is therefore not further discussed in this document.

However, the notification messages mentioned above, and some messages related to exception handling are impacting the interoperability across SEPA.

Notification of payment to the payee by their MSCT service provider (see step 18 in Figure 4)

- *Successful transaction*
    - SCT Instant: The payee shall be informed by their MSCT service provider about the execution of the payment. This implies that either

[6] In this document, a "Payment Request" refers to a message sent by the payee to its MSCT service provider and from the payee's MSCT service provider to the payer MSCT service provider including all transaction data for presentation to the payer to enable them to initiate a transaction and perform SCA as needed.

[7] This may vary and is implementation dependent, e.g., if the IBAN is already known by the payee's MSCT service provider it may be omitted.

- the payer ASPSP upon receipt of the confirmation message 6 in Figure 1 in the MSCT IG (EPC269-19) needs to inform the payer MSCT service provider, who subsequently needs to inform the payee MSCT service provider (e.g. via the HUB[8])

or

- the payee ASPSP upon receipt of the funds needs to inform the payee MSCT service provider (for specific cases only).

- SCT: The payer ASPSP upon initiation of the SCT informs the MSCT service provider of the payer.
  - The payer MSCT service provider subsequently needs to inform the payee MSCT service provider (e.g. via a HUB) who then informs the payee

  or

  - The payee ASPSP informs the payee (for specific cases only).

  For SCT, also a guarantee of payment[9] could be considered, but falls outside the scope of this dedicated technical interoperability document.[10]

- *Unsuccessful transaction*

  - SCT Instant: The merchant shall be informed by their MSCT service provider about the unsuccessful payment transaction. This implies that either
    - the payer ASPSP upon receipt of the negative confirmation message 6 in Figure 1 in the MSCT IG (EPC269-19) needs to inform the payer MSCT service provider, who subsequently needs to inform the payee MSCT service provider (e.g. via a HUB)

    or

    - the payee ASPSP informs the payee about the unsuccessful payment transaction (for specific cases only).

  - SCT:
    - In case the failure is at the payer ASPSP, the payer ASPSP needs to inform the payer MSCT service provider, who subsequently needs to inform the payee MSCT service provider (e.g. via a HUB);
    - In case the failure is at the payee ASPSP it is an offline process.

Notification of payment to the payer by their MSCT service provider (see step 15 in Figure 2)

- *Successful transaction*

  - SCT Instant: The payer shall be informed by their MSCT service provider about the execution of the payment. This implies that the payer ASPSP upon receipt of the

[8] The usage of the term HUB is meant to be agnostic to the way it might be implemented – different models may be possible, as examples it could be a central infrastructure with a routing service but it could also be implemented via a direct API.

[9] This could potentially be addressed by a dedicated framework.

[10] See for instance https://www.europeanpaymentscouncil.eu/news-insights/news/request-pay-specifications-standardisation-framework. This feature is currently planned to be included in the 2nd release of the SEPA Request-to-Pay Scheme rulebook.

confirmation message 6 in Figure 1 in the MSCT IG (EPC 269-19v1.0) needs to inform the payer MSCT service provider.

- SCT: the payer ASPSP informs the MSCT service provider of the payer about the execution of the payment.

- *Unsuccessful transaction*

  - SCT Instant: The payer shall be informed by their MSCT service provider about the unsuccessful payment transaction. This implies that the payer ASPSP upon receipt of the negative confirmation message 6 in Figure 1 in the MSCT IG (EPC 269-19v1.0) needs to inform the payer MSCT service provider.[11]

  - SCT:
    - In case the failure is at the payer ASPSP, the payer ASPSP needs to inform the payer MSCT service provider, who subsequently needs to inform the payer (not impacting interoperability across SEPA since this is between the payer and their MSCT service provider)

    - In case the failure is at the payee ASPSP it is an offline process.

3. "HUB" interconnectivity

In order to accommodate interoperability, the following requirements need to be implemented by a HUB providing a routing service. Hereby the term HUB is meant to be agnostic to the way it might be implemented – different models may be possible, but it should at least cover a kind of routing service.

In the table below, the required functionalities for the HUB are listed for both the transaction data exchange and the notification messages.

MSCT transaction feature	Requirements on HUB
Payer-presented data	
Transfer of payer *MSCT service provider identifier* to payee MSCT service provider	The payer MSCT service provider identifier is used by the payee MSCT service provider and the HUB for routing purposes and is included in the Payment Request message.
Transfer of payer token to payer MSCT service provider as *payer identification data*	Transfer of the payer token between the respective MSCT service providers – but included in the Payment Request message

[11] This would imply a change request to the SCT Instant rulebook (EPC004-16) where the negative confirmation message 7 is currently sent directly from the payer ASPSP to the payer.

Transfer of CustomerID[12] and IBAN to payer MSCT service provider as *payer identification data*[13]	Transfer of the CustomerID and IBAN between the respective MSCT service providers – but included in the Payment Request message	
Transfer of CustomerID[14] and IBAN-proxy to payer MSCT service provider as *payer identification data*	Transfer of the CustomerID and IBAN-proxy between the respective MSCT service providers – but included in the Payment Request message	
Transaction data		
Transfer of *transaction data* to the payer MSCT service provider	Transfer of Payment Request message between MSCT service providers that includes the transaction data	
Notification messages	**SCT Instant**	**SCT**
Notification to the payee about successful transaction	Notification from payer MSCT service provider to payee MSCT service provider	Notification from payer MSCT service provider to payee MSCT service provider
Notification to payee about unsuccessful transaction	Notification from payer MSCT service provider to payee MSCT service provider	Notification from payer MSCT service provider to payee MSCT service provider in case the failure is at the payer ASPSP
Notification to payer about successful transaction	Not applicable	Not applicable
Notification to payer about unsuccessful transaction	Not applicable	Not applicable

Table 1: Required HUB functionalities for MSCTs based on payer-presented data

4. Process flows for MSCT interoperability

4.1 Introduction

In this section the full process flows between the HUB and respective MSCT service provider back-ends will be illustrated. Note that as defined in the MSCT IG (EPC269-19v1.0), an MSCT service provider could be an ASPSP. This means that in the process flows below, one or both MSCT providers could be one or both of the respective ASPSPs in which case the process flows would simplify.

[12] In the context of this document, a CustomerID is an identification of the payer (consumer), issued by their ASPSP for access to (a) customer facing user interface(s) (e.g. their on-line banking system), as required in the PSD2 API.
[13] In this case additional protection of the data might be required, subject to further clarifications to be provided by the EBA on questions 2020_5476 and 2020_5477.
[14] In this case additional protection of the CustomerID might be required, subject to further clarifications to be provided by the EBA on question 2020_5476.

Only one C2B use case will be illustrated below since for P2P use cases based on payer-presented data, the interoperability challenges and process flows will be similar as the one described for the C2B payment context. Moreover, for the C2B payment contexts, the process flow is illustrated for a purchase in a physical store based on a QR-code presented by the consumer including a token as payer identification data. For e-commerce, other means for providing the consumer identification data will need to be used (e.g. manual entry on a payment page of an e-merchant) but this will not impact the interoperability process flow.

For MSCT use cases based on consumer-presented data whereby there is a need for the merchant to identify the payer, extra steps in the process flow below might be needed to accommodate a de-tokenisation process by the consumer's MSCT service provider via the HUB prior to the sending of a Payment Request message by the merchant.

Note also that the MSG MSCT intends, in future work, to analyse the interoperability of MSCTs whereby a PISP or a Collecting PSP[15] (CPSP) on behalf of the merchant are involved.

MSCT transactions type	Support from the HUB
C2B – consumer-presented QR-code contains a token	• Transfer of Payment Request message (including payer identification data and transaction data) between MSCT service providers (see sections 2.2 and 2.3) • Notification messages (see section 2.4)

Table 2: Mapping of MSCT transaction type onto HUB functionalities

Note that the consumer-presented QR-code may be static or dynamic[16].

In the process flow below, the implicit assumption is made that the MSCT transaction is successful and the first options in section 2.4 are illustrated. The flow for an unsuccessful transaction would need to be analysed separately. Moreover, the process flow is based on an instant SCT transaction (see chapter 4 in the MSCT IG (EPC269-19v1.0)).

The process flow described below does not include potential exchanges needed between MSCT service provider back-ends for the application of a fee structure to support a business model.

In the process flow below, the representation and description of strong customer authentication (SCA) is simplified since the focus is on the interconnectivity between the respective MSCT service providers. More details on SCA are provided in chapter 8 of the MSCT IG and are illustrated in section 2 of this document and in chapter 7 of the MSCT IG.

4.2 C2B with consumer token

In this section the process flow for an in-store payment between a consumer (payer) and merchant (payee) using the HUB is illustrated. In this example, it is assumed that the consumer-presented

[15] A collecting PSP that has a contract with the merchant to collect MSCT transactions on their behalf.
[16] Forthcoming work of the MSG MSCT on the security of QR-codes and their data is planned to be included in a new release of the MSCT IG.

data does not contain the consumer identification "in clear" but that a token[17] is used instead (see section 5). It is hereby assumed that the tokenisation/de-tokenisation process (see sections 5.4 and 10.4 in the MSCT IG (EPC269-19v1.0) is handled by or via the consumer's MSCT service provider. The consumer-presented data includes the identifier of the consumer's MSCT service provider "in clear" so that it can be retrieved by the merchant and provided to their MSCT service provider in the Payment Request message.

Note also that the example illustrates a successful transaction (see section 2.3).

In this example, the following actors and interconnectivity are required as depicted below.

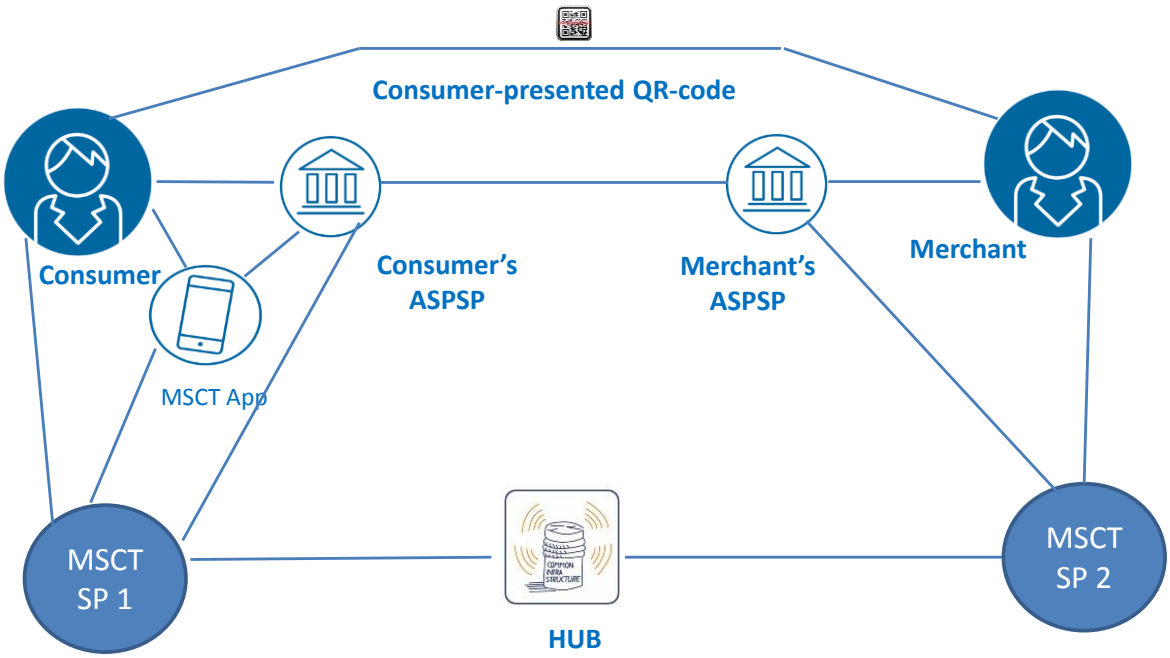
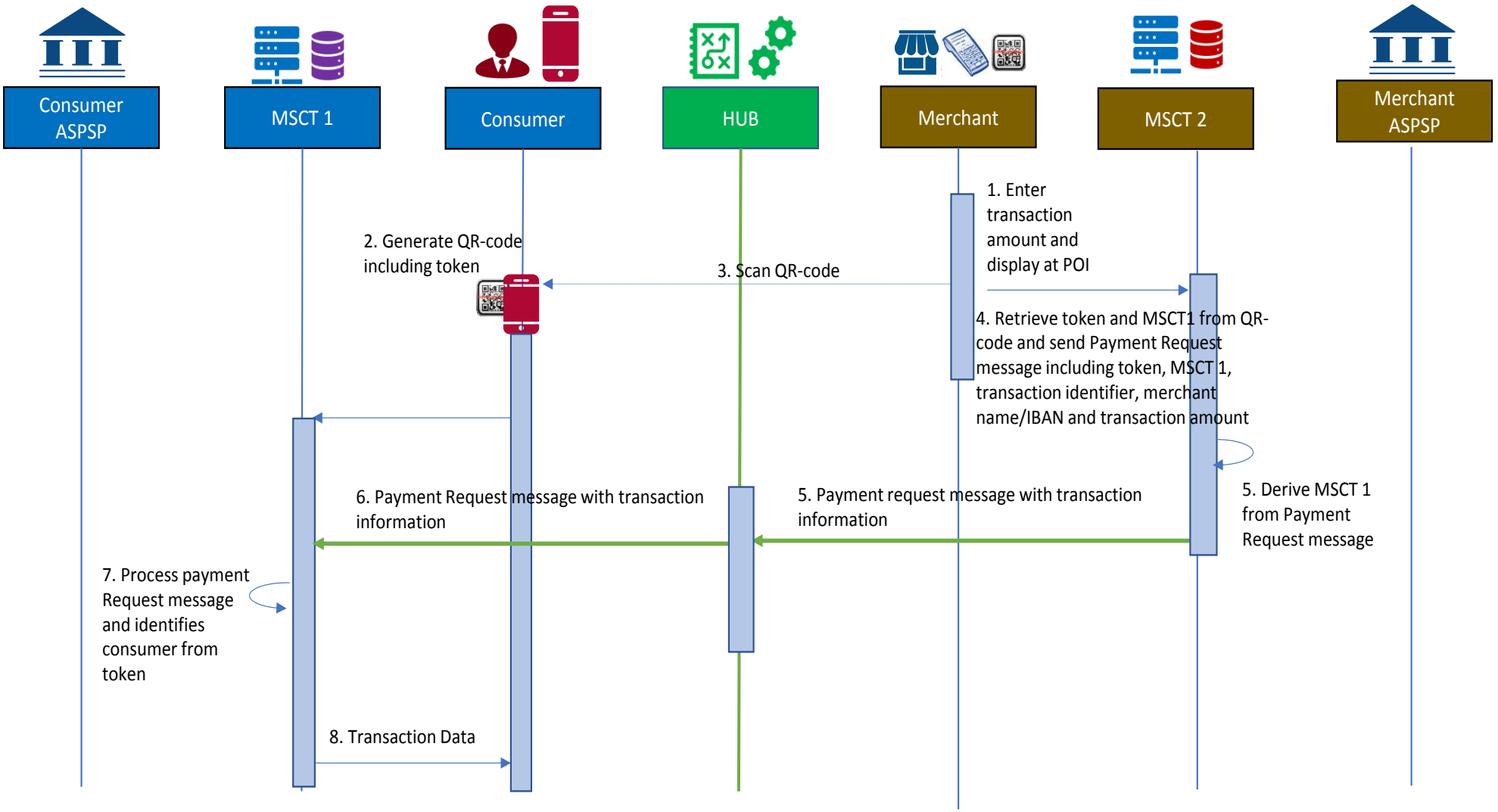


Figure 3: Actors for C2B - with consumer token

The detailed process flows between the different actors involved for this MSCT transaction type are shown in the next figure.

[17] This token may be dynamic or static.


Consumer ASPSP
MSCT 1
Consumer
HUB
Merchant
MSCT 2
Merchant ASPSP
1. Enter transaction amount and display at POI
2. Generate QR-code including token
3. Scan QR-code
4. Retrieve token and MSCT1 from QR-code and send Payment Request message including token, MSCT 1, transaction identifier, merchant name/IBAN and transaction amount
5. Derive MSCT 1 from Payment Request message
5. Payment request message with transaction information
6. Payment Request message with transaction information
7. Process payment Request message and identifies consumer from token
8. Transaction Data

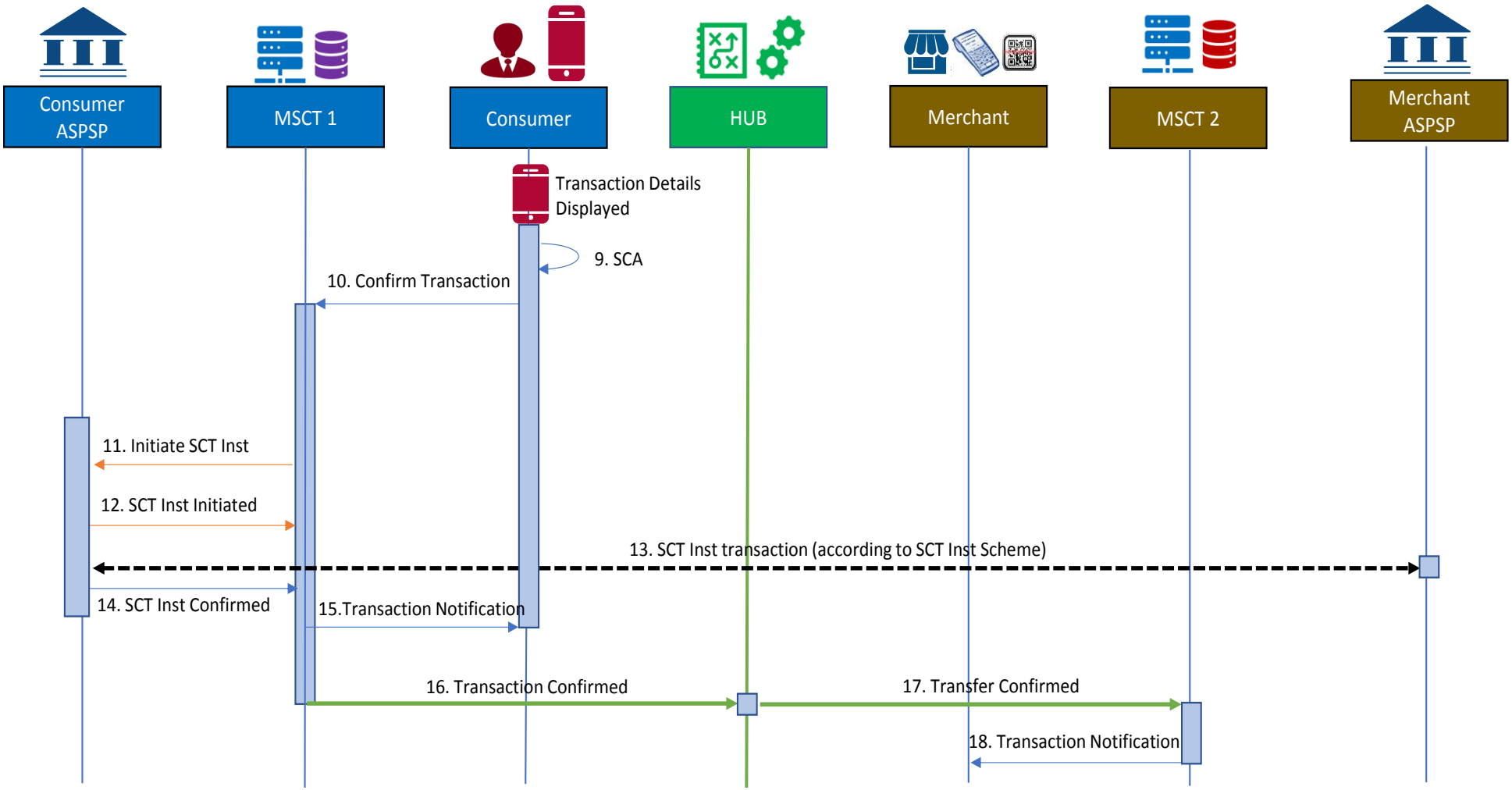


Figure 4: Process flow – C2B – consumer-presented QR-code with token

In the figure above the following steps are involved:

Step 1

- The merchant enters the transaction amount which is displayed on the POI[18].

Step 2

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

Step 3

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

Step 4

The merchant retrieves the consumer's token and the consumer's MSCT service provider identifier from the QR-code and sends a Payment Request message to their MSCT service provider, including the merchant's name, IBAN_merchant[19], merchant transaction identifier, the transaction amount, the consumer's MSCT service provider identifier and the consumer token.

Step 5:

The Payment Request message including the consumer's MSCT service provider identifier is sent to the HUB.

Step 6:

The HUB identifies the consumer's MSCT service provider and forwards them the Payment Request message containing the consumer token and transaction data.

Step 7:

The consumer's MSCT service provider checks the Payment Request message, retrieves the transaction data and the consumer's name and possibly IBAN from the consumer token.

[18] The display of the transaction amount by the POI may happen at a later stage since the payer indemnity might have an impact on the final transaction amount (e.g., discounts). However this could require additional steps to obtain the payer identification from the token received. This would need to be analysed in forthcoming work by the MSG MSCT.

[19] Instead of the IBAN_merchant a proxy may be used.

Step 8:

The consumer's MSCT service provider sends the transaction details to the consumer.

Step 9:

The consumer consents to the transaction based on the details displayed and performs SCA[20].

Step 10:

The confirmation including the authentication response is provided to the consumer's MSCT service provider.

Step 11:

After checking the authentication response, the consumer's MSCT service provider sends an SCT Inst instruction to the consumer's ASPSP including the transaction details.

Step 12:

The consumer's ASPSP sends a message to the consumer's MSCT service provider confirming the initiation of the SCT Inst.

Step 13:

The consumer's ASPSP sends the SCT Inst transaction to the merchant's ASPSP and the transaction flow is handled according to the SCT Inst scheme (see section 4.2 in MSCT IG).

Step 14:

The consumer's ASPSP sends a confirmation message to the consumer's MSCT service provider about the execution of the SCT Inst transaction.

Step 15:

The consumer's MSCT service provider sends a transaction notification message to the consumer.

Step 16:

The consumer's MSCT service provider sends a transaction notification message to the HUB with the merchant's MSCT service provider identifier.

[20] The SCA may be performed by the consumer's MSCT service provider or by their ASPSP. This may involve additional steps which are not illustrated in this process flow since they do not impact the interoperability (see chapter 8 of the MSCT IG (EPC269-19v1.0). Here it is assumed that the consumer's MSCT service provider has received delegation from the consumer's ASPSP for SCA subject to appropriate agreements.

Step 17:

The HUB forwards the transaction notification message to the merchant's MSCT service provider.

Step 18:

The merchant's MSCT service provider sends a transaction notification message to the merchant.

5. Minimum data set for MSCTs based on payer-presented data

To achieve interoperability for MSCTs, an agreement on a minimum data set is required for the data to be exchanged between the payer/consumer and the payee/merchant being it in the payer-presented data or in the Payment Request messages exchanged (see section 8).

The minimum data set to be exchanged between the payer and the payee included in the payer-presented data relies on the type of payer identification data included in the payer-presented data as described in Table 1 in section 2 of this document:

1. If the payer-presented data provided to the payee contains a *(payer) token*, the minimum data will consist of both routing info (i.e. the identifier of the payer MSCT service provider) and the (payer) token as payload. The minimum data will be forwarded in the Payment Request message through the HUB from the payee MSCT service provider to the payer MSCT service provider for de-tokenisation into the payer identification data, together with the other transaction data.

2. If the payer-presented data provided to the payee contains the *CustomerID and IBAN* "in clear" (e.g. in clear in a QR-code) of the payer, the minimum data set will consist of both routing info (i.e. the identifier of the payer MSCT service provider) and the CustomerID and IBAN. The minimum data will be forwarded in the Payment Request message through the HUB from the payee MSCT service provider to the payer MSCT service provider together with the other transaction data.

3. If the payer-presented data provided to the payee contains the *CustomerID* ("in clear") and an *IBAN-proxy* of the payer, the minimum data set will consist of both routing info (i.e. the identifier of the payer MSCT service provider) and the CustomerID and IBAN-proxy. The minimum data will be forwarded in the Payment Request message through the HUB from the payee MSCT service provider to the payer MSCT service provider together with the other transaction data. The IBAN will need to be derived from the IBAN-proxy by the payer MSCT service provider.

The minimum data sets for these 3 cases include:

For case 1 - the payer-presented data includes a token: [Version]+[Type]+[payer MSCT service provider ID]+[(payer) token]
For case 2 – the payer-presented data contains the CustomerID and IBAN "in clear" [Version]+[Type]+[payer MSCT service provider ID]+[CustomerID + IBAN_payer]
For case 3 – the payer-presented data contains the CustomerID "in clear" and a proxy [Version]+[Type]+[payer MSCT service provider ID]+[CustomerID + IBAN-proxy]

Table 3: Minimum data sets for MSCTs based on payer-presented data

Note: There might be a need for the merchant, in C2B payment contexts, to identify the consumer to offer additional services or benefits. For interoperability, the consumer identification means would need to be standardised in future work and could be added to the payload information (see Table 4).

The version refers to the specification version of the format of the proximity technology used (e.g., the QR-code, see section 6).

The type may refer to the cases above and may enable to add other services[21].

The payer MSCT service provider identifier is used in the interoperability space for routing purposes, therefore a standardisation of this data element will be necessary.

The payer identification data (that is part of the payload) needs to be included in the Payment Request message. Therefore, a predefined length and character set need to be specified.

6. Example: Payer-presented QR-code for MSCTs

As an example, to enable MSCT interoperability across SEPA, for the data exchange between the payer and payee for all payment contexts, an MSCT QR-code should be standardised based on the minimum data set defined in section 5 of this document. Note that the proposed QR-code[22] format aims to address both P2P and C2B payment contexts.

[21] An example may be a repayment (transfer back).

[22] Note that in a transition period not all POIs may be able to read QR-codes. For barcodes, the usage of a URL may be impossible in view of its size.

This standardised MSCT QR-code should be adopted by all MSCT service providers and supported by the MSCT apps in the payer's mobile device and the MSCT app on the payee's POI (e.g. POI in case the payee is a merchant)[23].

For the development of a standardised MSCT QR-code the following three principles will be followed:

A. Mobile wallets will often support multiple payment methods. The wallet user will often select and set a default payment method;
B. Avoid any special actions from merchant personnel at POI (e.g. in a store - all extra actions generate friction, such as asking what kind of wallet or what kind of payment instrument the consumer would like to use);
C. Avoid any special actions from the wallet user at POI (more in particular in stores - e.g. swiping through a POS-menu to find your wallet generates friction).

When following the principles above, a payer-generated QR-code format for MSCTs for data exchange between the payer and the payee could be based on the following preconditions:

1. Make a generic routing/payload data-exchange at POI between the payer and the payee;
2. Routing goes directly or via (a) HUB(s) between MSCT service providers;
3. Avoid having specific details about the payer in the data exchange in order to
    a. Reduce privacy/security concerns;
    b. Reduce maintenance concerns related to QR-code distribution;
    c. Increase readability of the QR-code.

QR-code format:

It is suggested that the QR-code should be based on the following format:

- A URL based on https:// structure
- First part of the URL: ordinary domain structure
- Second part of the URL: version
- Third part: type
- Fourth part: routing information
- Fifth part: payload information (in fact payer identification data)

HTTPS://<Domain_name>/<Version>/<Type><Payer MSCT service provider ID/<Payload>

Table 4: Coding of QR-code with payer-presented data

The Domain name refers to a dedicated MSCT interoperability framework (see section 1).

[23] See also the document on a Framework for interoperability of IPs at the POI developed by the dedicated ERPB WG (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/14th-ERPB-meeting/ERPB_working_group_on_instant_at_the_POI_-_Framework_for_interoperability_of_instant_payments_at_the_POI.pdf?db00f43b17d4aeeb4a83ae82187d53c8).

7. Payment Request messages

Any future specification for the Payment Request messages from the payee to their MSCT service provider and between the respective MSCT service providers, through the HUB, will need to take the following minimum data set into account.

From payee to their MSCT service provider

Name:	**Payment Request Presentment by payee to payee MSCT service provider**
Description:	This dataset describes the content of the Payment Request message as presented by the payee to the payee MSCT service provider. Attributes are mandatory unless otherwise indicated.
Attributes contained	• The payer identification data (M) • The transaction amount (M) • The currency (M) • The remittance Information sent by the payee to the payer (O) • The payer MSCT service provider identifier (M) • The Requested Execution Date/Time of the Payment Request (M) • The IBAN of the payee (M) • The name of the payee (M) • The trade name of the payee (M for C2B) • The payee's reference party (O) • The address of the payee (O) • The BIC code of the payee ASPSP (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • The purpose of the Payment Request (O) • The Merchant Category Code (MCC) (M for C2B) • The expiry date of the Payment Request (O) • Type of payment instrument requested by the payee (SCT or SCT Inst) (M) • Flag notification message required (O) • Place holder for charging (O)

Table 5: Dataset for Payment Request Presentment by Payee to Payee MSCT service provider

Between MSCT service providers

Name:	Inter-MSCT service provider Payment Request Presentment
Description:	This dataset describes the content of the Payment Request presentment by the payee MSCT service provider to the payer MSCT service provider via the HUB). Attributes are mandatory unless otherwise indicated.
Attributes contained	• The payer identification data (M) • The transaction amount (M) • The currency (M) • The remittance information (O) • The payer MSCT service provider identifier (M) • The Requested Execution Date/Time of the Payment Request (M) • The IBAN of the payee (M) • The name of the payee (M) • The trade name of the payee (M for C2B) • The payee's reference party (O) • The address of the payee (O) • The BIC code of the payee ASPSP (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • The purpose of the Payment Request (O) • The Merchant Category Code (MCC) (M for C2B) • The expiry date of the Payment Request (O) • Type of payment instrument requested by the payee (SCT or SCT Inst) (M) • Flag notification message required (O) • Additional unique reference provided by the payee MSCT service provider (O) • Place holder for charging (O)

Table 6: Dataset for Payment Request Presentment by the payee MSCT service provider to the payer MSCT service provider

Annex: MSCT use cases based on payer-presented data

A.1 Introduction

Next to the MSCT use cases based on payer-presented data that have been described in chapter 7 of the MSCT IG, this section provides another two examples of such illustrative use cases for SCT Inst in C2B payment contexts. Note that also the description of the Strong Customer Authentication (SCA) in these use cases is illustrative since other methods could be used as described in chapter 8 of the MSCT IG.

For P2P payment contexts, MSCTs based on payer-presented data would involve similar steps as the use cases presented, except that the payer-presented data (e.g. a QR-code) would be transferred to a dedicated app on the payee's mobile device instead of the merchant's POI.

In the examples below it is assumed that both payer and payee have the same MSCT service provider. Interoperability of MSCTs whereby payer and payee have different MSCT service providers are treated in the forthcoming sections in this document.

The MSCT use cases use the concept of a "Payment Request". This refers to dedicated messages sent by the payee to the MSCT service provider and from the MSCT service provider to the payer including all transaction data to enable the payer to initiate a transaction and to perform SCA (as needed (see chapter 8 in the MSCT IG)).

Furthermore, next to the MSCT use cases included in the MSCT IG and in this section, the MSG MSCT has planned further work over the coming months on MSCT use cases involving a PISP or a Collecting PSP (an entity collecting payment transactions on behalf of the merchant).

A.2 Use case C2B-1: Mobile device – Payment at a physical POI involving consumer-presented QR-code – strong customer authentication using a dedicated authentication application involving a fingerprint

This MSCT use case presents an example of consumer experience whereby their mobile device is used to pay in-store by presenting consumer-presented QR-code to 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 device.

The consumer authentication is performed through a dedicated Authentication application[24] in the consumer's mobile device[25].

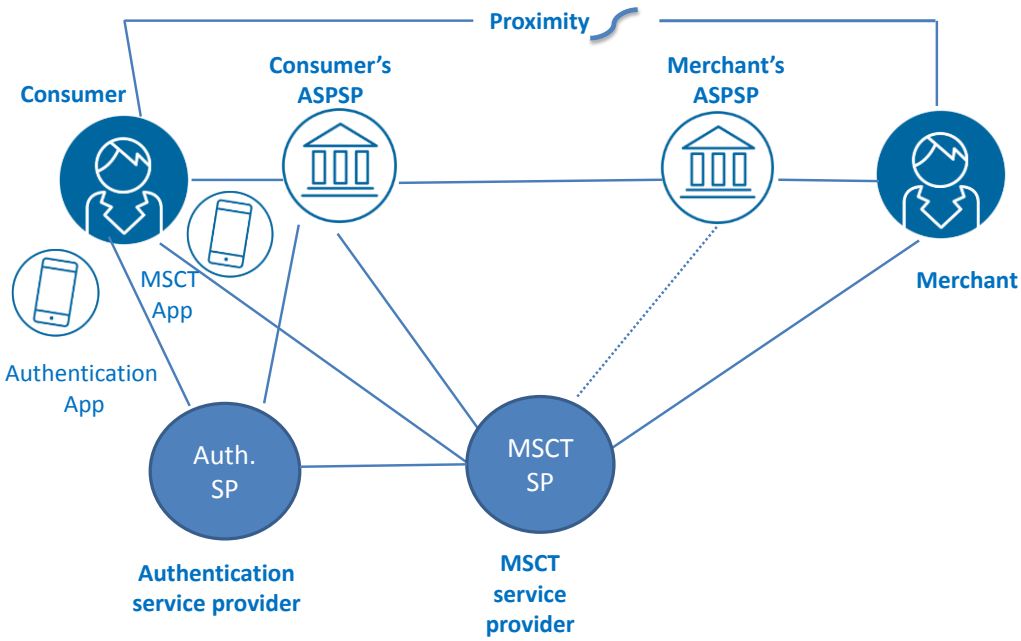


Figure 5: Actors in MSCT Use case C2B-1

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. Both ASPSPs are participants in the same MSCT Instant Service[26].

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 MSCT IG) in accordance with the relevant PSD2 requirements is performed involving a fingerprint[27] (see section 8.2 in MSCT IG). Note that hereby delegation for the consumer authentication needs to be given by the consumer's ASPSP to the Authentication service provider.

[24] An application accessed through the mobile device performing the functions related to a user authentication, as dictated by the Authentication service provider.
[25] In this case there is a delegated authentication from the consumer's ASPSP to the Authentication service provider. Also an agreement between the payer ASPSP and the Authentication service provider is needed.
[26] This refers to the current MSCT solutions in the market.
[27] Note that other biometric methods may be used.

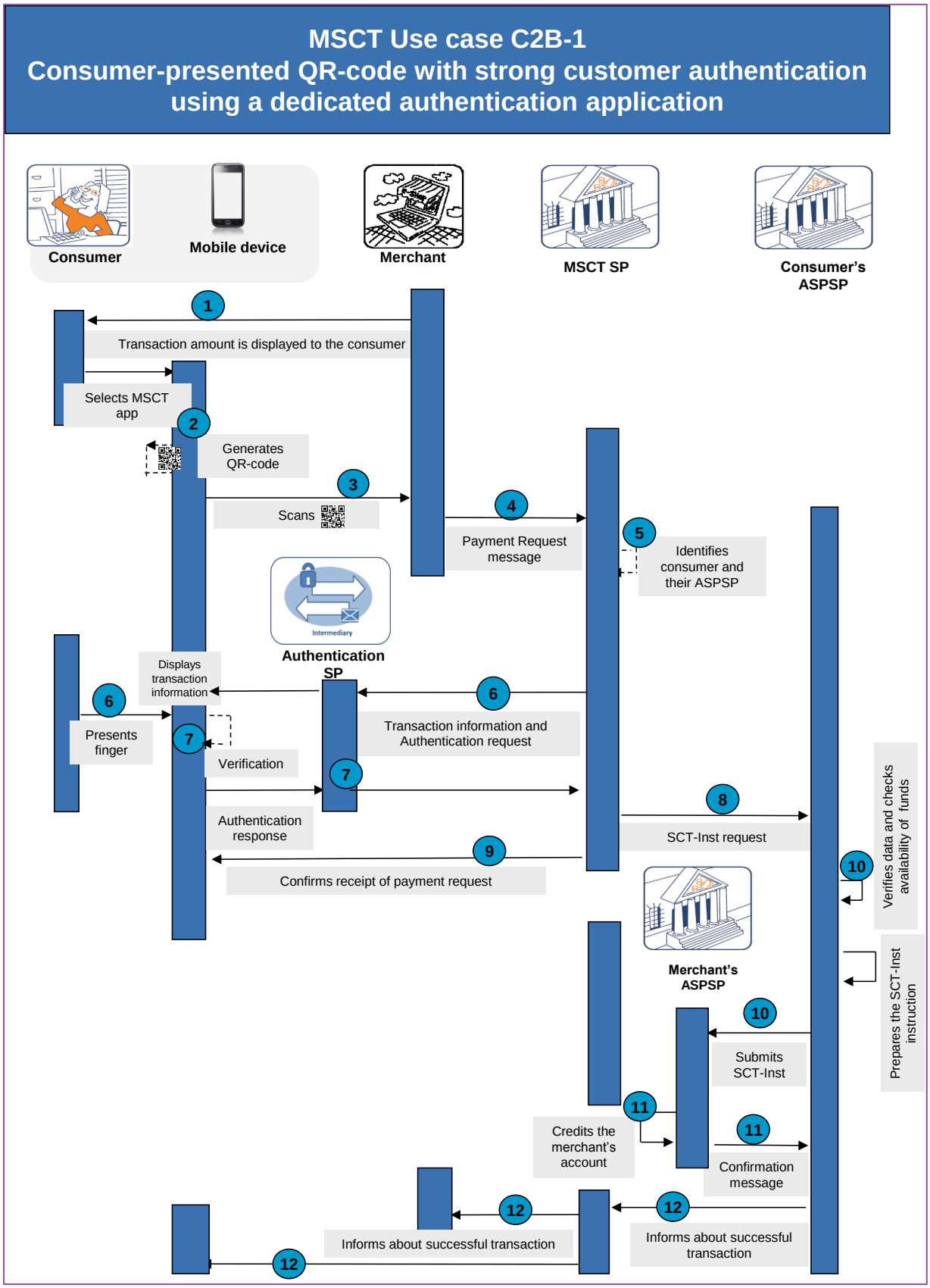


Figure 6: MSCT Use case C2B-1

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 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 delegates the authentication of the consumer to the Authentication service provider.
- The merchant also needs to be subscribed to the MSCT Instant service, e.g., through their ASPSP or the MSCT service provider directly, has downloaded dedicated software and has the appropriate equipment to scan QR-codes in their POI environment.
- The MSCT service provider is linked to the consumer's ASPSP.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The merchant enters the transaction amount which is displayed on the POI[28].

Step 2

- The consumer selects and opens the MSCT Instant application on their mobile device which possibly involves the entry of a password (or other means of authentication).
- A QR-code containing a token for the consumer is generated by the MSCT Instant application on the mobile device.

Step 3

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

Step 4

The merchant retrieves the consumer's token from the QR-code and sends a payment Request message to their MSCT service provider, including the merchant's name, IBAN_merchant[29], merchant transaction identifier, the transaction amount and the consumer token.

[28] The display of the transaction amount by the POI may happen after step 3, since the customer identification might have an impact on the final transaction amount.
[29] Instead of the IBAN_merchant a proxy may be used.

Step 5

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

Step 6

- The MSCT service provider forwards the transaction information to the MSCT Instant app on the consumer's mobile device.
- The consumer is invited to confirm the transaction and is redirected to their Authentication application which displays the merchant name/ IBAN_merchant and the transaction amount.
- The consumer authenticates and confirms the transaction by presenting their finger to the mobile device.

Step 7

Upon successful fingerprint verification by the mobile device, the MSCT service provider is informed by the Authentication service provider.

Step 8

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

Step 9

The MSCT service provider acknowledges successful receipt of the SCT Instant Instruction to the consumer.

Step 10

- 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 11

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

Step 12

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

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

Analysis MSCT Use case C2B-1	
Interoperability	The consumer and the merchant are subscribed to the same MSCT service while the consumer's ASPSP needs be linked to the corresponding MSCT service provider. For a truly "open" approach and a SEPA-wide interoperability, if the MSCT service provider of the consumer is different to the MSCT service provider of the merchant, a framework will need to be specified that interconnects the different MSCT service providers.
Challenges	• Standardisation of messages including data elements between MSCT service provider back-ends. • Standardisation of a "QR-code" and identification of consumers. • Standardisation of the Payment Request messages. • Security of the QR-code/consumer token29F[30]. • Standardisation of interface between MSCT providers and ASPSPs. • How is the transaction reconciled with the purchase (e.g., purchase identifier)? • The information messages in step 12 are not included in the SCT Instant scheme.

Table 7: Analysis MSCT Use case C2B-1

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

[30] The MSG MSCT will address this issue in forthcoming work.

A.3 Use case C2B-2: Mobile device – Payment at a physical POI involving consumer-presented QR-code – strong customer authentication using an MSCT application involving a mobile code

This use case presents an example of consumer experience whereby their mobile device is used to pay in-store by presenting a consumer-presented QR-code to the POI. Hereby a dedicated MSCT 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 the MSCT application in the consumer's mobile wallet.

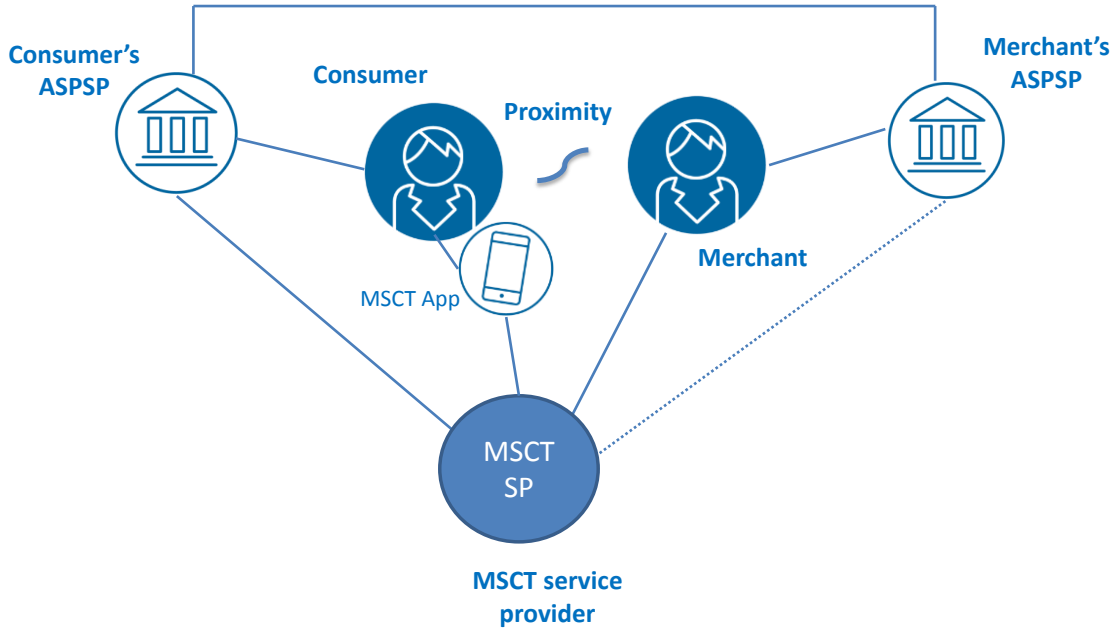


Figure 7: Actors in MSCT Use case C2B-2

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. Both ASPSPs are participants in the same MSCT Instant Service[31].

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 MSCT IG) in accordance with the relevant PSD2 requirements is performed involving a mobile code[32] (see section 8.2 in MSCT IG). Note that hereby delegation for the consumer authentication needs to be given to the MSCT service provider by the consumer's ASPSP.

[31] This refers to the current MSCT solutions in the market.
[32] Note that also biometric methods may be used.

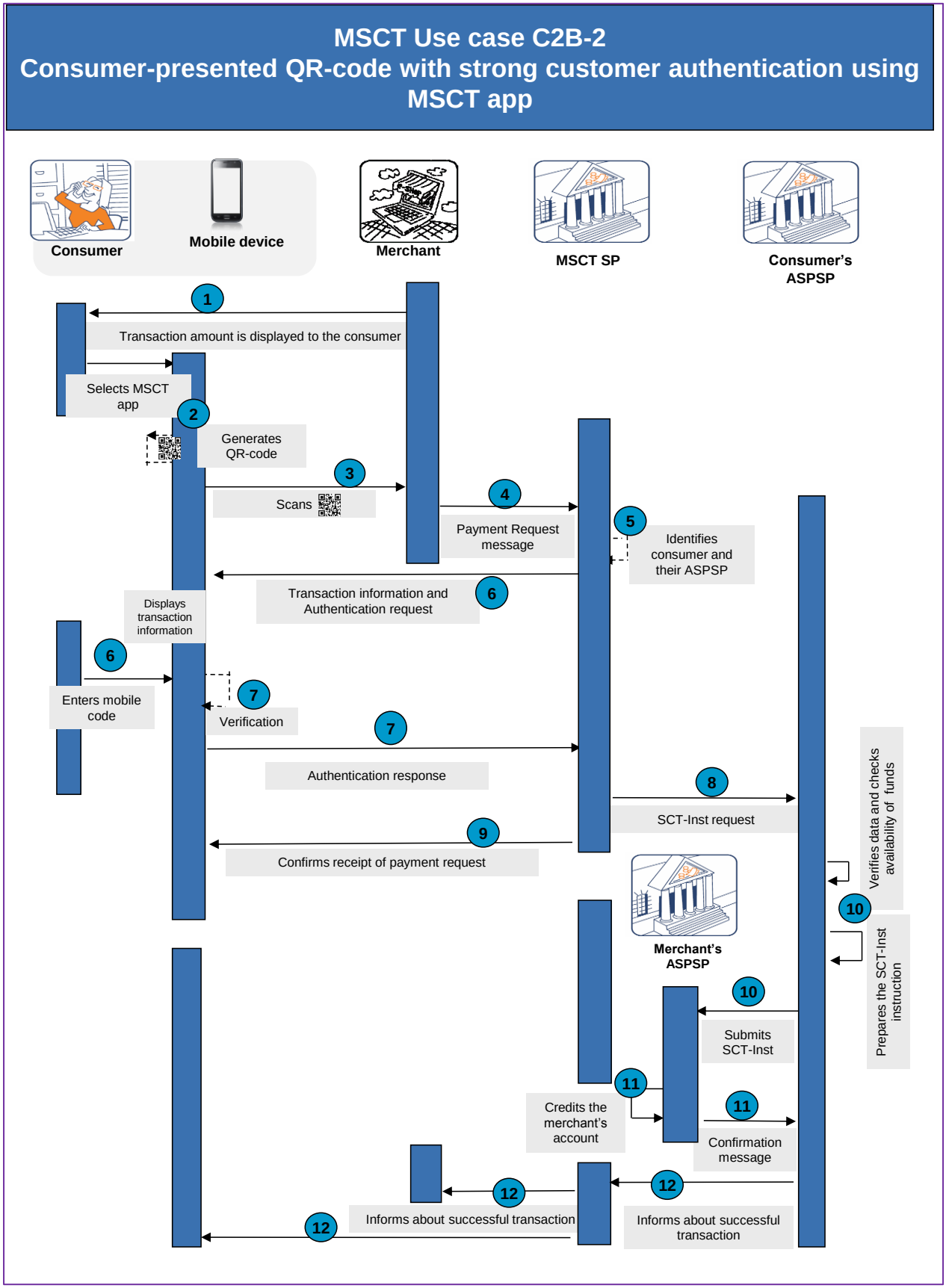


Figure 8: MSCT Use case C2B-2

In the figure above, the following steps are illustrated:

Step 0

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

Step 1

- The merchant enters the transaction amount which is displayed on the POI.[33]

Step 2

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

Step 3

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

Step 4

The merchant retrieves the consumer's token from the QR-code and sends a Payment Request message to their MSCT service provider, including the merchant's name, IBAN_merchant[34], merchant transaction identifier, the transaction amount and the consumer identifier.

Step 5

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

[33] The display of the transaction amount by the POI may happen after step 3, since the customer identification might have an impact on the final transaction amount.
[34] Instead of the IBAN_merchant a proxy may be used.

Step 6

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

Step 7

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

Step 8

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

Step 9

The MSCT service provider acknowledges successful receipt of the SCT Instant Instruction to the consumer.

Step 10

- 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 merchant's ASPSP.

Step 11

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

Step 12

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

Analysis MSCT Use case C2B-2	
Interoperability	The consumer and the merchant are subscribed to the same MSCT service while the consumer's ASPSP needs be linked to the corresponding MSCT service provider. For a truly "open" approach and a SEPA-wide interoperability, if the MSCT service provider of the consumer is different to the MSCT service provider of the merchant, a framework will need to be specified that interconnects the different MSCT service providers.
Challenges	• Standardisation of messages including data elements between MSCT service provider back-ends. • Standardisation of a "QR-code" and identification of consumers. • Standardisation of the Payment Request messages. • Security of the QR-code/consumer token34F[35]. • Standardisation of interface between MSCT providers and ASPSPs • How is the transaction reconciled with the purchase (e.g., purchase identifier)? • The information messages in step 12 are not included in the SCT Instant scheme.

Table 8: Analysis MSCT Use case C2B-2

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

[35] The MSG MSCT will address this issue in forthcoming work.