European Payments Council

Technical Interoperability of MSCTs based on payee-presented data

EPC312-19 / Version 1.0 / Date issued: 28 May 2020

Public

Technical Interoperability of MSCTs based on payee-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

EPC312-19
Version 1.0
28 May 2020

Public

Table of Contents

1 Introduction

The aim of this document is to analyse in further detail the interoperability aspects related to MSCTs as identified in the Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance (MSG IG - EPC269-19v1.0). More in particular, this document will focus on the interconnectivity and related functionality amongst MSCT service providers for MSCT use cases based on payee-presented data (e.g., through a QR-code) and on the data to be exchanged between the payee and the payer to enable the initiation of such MSCTs.

Throughout the document, the terminology, abbreviations and references specified in the MSCT IG (EPC269-19v1.0) apply. 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.

This document focuses on 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.

With respect to these payments, currently only MSCT use cases based on **payee-presented data** (e.g. payee-presented data via a QR-code, BLE, etc.) will be covered, since those cover most of the MSCT use cases in the market in SEPA today. In a forthcoming document, the interconnectivity between MSCT service providers for MSCT use cases based on payer-presented data will also be analysed.

Moreover, the document focuses on the usage of QR-codes as proximity technology. Note however, since other proximity technologies such as NFC and BLE are currently 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 further be noted that this document focuses only on 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 rules, liability, recognition label, etc.). These could for instance be covered under a "to be developed" dedicated framework.[1]

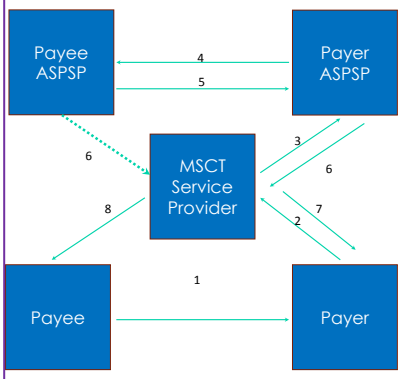
[1] The need for such a framework has also been identified in the ERPB report Instant payments at the POI (see https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/12th-ERPB-meeting/Report_from_the_ERPB_WG_on_instant_at_POI.pdf?efe8385c4196f8094d5b6625f7ffdc79) and will be addressed in a new ERPB WG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

2 MSCT Interoperability Challenges

2.1 MSCT interoperability

In the MSCT IG a description is provided of the process flow for an MSCT transaction if both the payer and payee are customers of the same MSCT provider as depicted below (see section 17.1 in EPC269-19v1.0).

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



General MSCT transaction flow:

- 1 – Payer receives transaction data (e.g., via QR scanning, Proxy, Payment Request, etc.);
- 2; 3 – Initiation /authentication e.g., via a PISP as needed;
- 4 – SCT or SCT Instant (payer's ASPSP transfers fund to Payee's ASPSP;
- 5; 6 – Confirmation that transfer was processed;
- 7; 8 – MSCT service provider sends MSCT transaction notification to payer and payee.

Figure 1: Current MSCT service model in the market for MSCTs based on payee-presented data

In section 17.2 in the same document, also the requirements have been identified with respect to the interconnection between the MSCT service providers. This is to ensure the necessary exchange of transaction data between MSCT service providers such that a payer that is on-boarded with MSCT service "X" can make a (instant) SEPA credit transfer to a payee that is on-boarded in MSCT service "Y" as shown in the figure 2 below.

How to interconnect different MSCT services?

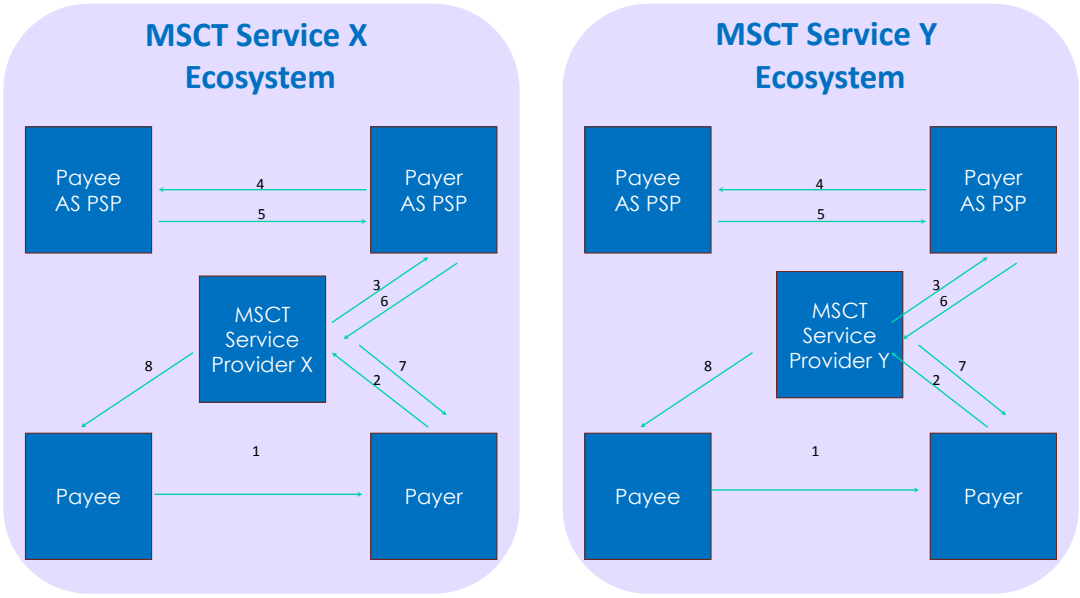


Figure 2: Interconnection of MSCT services

The MSCT service provider X is already connected to the payer's ASPSP. The interconnection needed during the execution of the Instant SCT or SCT transfer (this means after the transaction has been sent by the payer's ASPSP following the receipt 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 (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 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, the strong customer authentication of the payer by their ASPSP is in the payer-to-payer's ASPSP domain and is as such not impacting the interoperability. Neither is the interoperability impacted if the payer's ASPSP has delegated the strong customer authentication to the payer's MSCT service provider or to a so-called authentication service provider.

For MSCTs whereby a PISP is involved which is different to the MSCT service provider, the functionality needed to enable the requirements identified in this document for interconnectivity amongst MSCT service providers should be ensured. However these functionalities will not be discussed in further detail in this document.

What is however impacting the interoperability is the following:

- How is the transaction data, if not known by the payer, made available by/exchanged from the payee to the payer?

- How are the acknowledgement/notification messages provided by the respective MSCT service providers to the payee and the payer?

Both of these interoperability aspects will be analysed in more detail below.

It is further noted that there is also an 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 transaction data

With respect to the availability of the transaction data (payee's data and payment data) needed by the payer for the initiation of the MSCT transaction the following distinctions need to be made:

- *Part of the payee data is not known by the payer and a proxy is used* instead (e.g., a mobile phone number is used as a proxy instead of an IBAN): in this case, the MSCT service provider of the payer needs to be able to retrieve the payee's IBAN/name from the proxy used. This generally requires the support of the payee's MSCT service provider and/or ASPSP.

- *Transaction data is exchanged between the payee and the payer through* a proximity technology (QR-code, NFC, BLE, etc…).

  In this case a distinction needs to be made whether

  - All transaction data, not known by the payer beforehand, is exchanged using a "token": in this case, a de-tokenisation process needs to take place such that the transaction data can be derived from the token and provided to the payer via their MSCT service provider to enable the initiation of the payment. This generally requires the support of the payee's MSCT service provider.

  - All transaction data, not known by the payer beforehand, is exchanged in "clear" [2] (e.g. the payee's name, IBAN of the payee's account, transaction amount, etc. are included in the QR-code): in this case all necessary transaction data is directly available to the payer and enables initiating the payment.

  - The data exchanged between the payee and the payer does not contain all transaction data. In this case the complete transaction data is provided to the payer's MSCT service provider in the Response to the "Transaction Information Request", sent by the payer's MSCT service provider to the payee's MSCT service provider (see sections 4.4 and 4.5). The subsequent provision of the complete data to the payer by their MSCT service provider enables initiating the payment.

[2] Obviously in this case additional measures should be taken to ensure the security of the data exchanged (for some guidance see the MSCT IG).

2.3 Acknowledgement/notification messages

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

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

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.

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

- *Successful transaction*

- SCT Instant: The payee shall be informed by their MSCT service provider about the execution of the payment. This implies that either
  - The payer's ASPSP upon receipt of the confirmation message 6 in Figure 1 in the MSCT IG (EPC269-19v1.0) needs to inform the payer's MSCT service provider, who subsequently needs to inform the payee's MSCT service provider (e.g. via HUB[3], see section 3);

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

- SCT: The payer's ASPSP upon initiation of the SCT informs the MSCT service provider of the payer.
  - The payer's MSCT service provider subsequently needs to inform the payee's MSCT service provider (e.g. via a HUB, see section 3) who then informs the payee;

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

[3] The usage of the term HUB is meant to be agnostic to the way it might be implemented – different models may be possible, but it should cover a routing service.

For SCT, also a guarantee of payment[4] could be considered, but falls outside the scope of this dedicated technical interoperability document[5].

- *Unsuccessful transaction*

  - SCT Instant: The payee shall be informed by their MSCT service provider about the unsuccessful payment transaction. This implies that either
    - The payer's ASPSP upon receipt of the negative confirmation message 6 in Figure 1 in the MSCT IG (EPC269-19) needs to inform the payer's MSCT service provider, who subsequently needs to inform the payee's MSCT service provider (e.g. via a HUB, see section 3);

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

  - SCT:
    - In case the failure is at the payer's ASPSP, the payer's ASPSP needs to inform the payer's MSCT service provider, who subsequently needs to inform the payee's MSCT service provider (e.g. via a HUB, see section 3);
    - In case the failure is at the payee's ASPSP it is an offline process.

Notification of payment to the payer by their MSCT service provider

- *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's ASPSP upon receipt of the confirmation message 6 in Figure 1 in the MSCT IG (EPC269-19v1.0) needs to inform the payer's MSCT service provider.

  - SCT: the payer's 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's ASPSP upon receipt of the negative confirmation message 6 in Figure 1 in the MSCT IG (EPC269-19v1.0) needs to inform the payer's MSCT service provider[6]
  - SCT:
    - In case the failure is at the payer's ASPSP, the payer's ASPSP needs to inform the payer's MSCT service provider, who subsequently needs to inform the payer (not

[4] This could potentially be addressed by a dedicated framework.
[5] Note that this is planned to be addressed in phase 2 of the SEPA RTP scheme under development.
[6] This would imply a change request to the SCT Instant rulebook where the negative confirmation message 7 is currently sent directly from the payer's ASPSP to the payer.

impacting interoperability across SEPA since this is between the payer and their MSCT service provider);

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

3 "HUB" interconnectivity

In order to accommodate interoperability, the following requirements need to be implemented by a HUB. Hereby the term HUB is meant to be agnostic to the way it might be implemented – logically[7] or physically - 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 exchange of transaction data between the payee and the payer and the notification messages as analysed above.

[7] As an example, direct connection amongst MSCT service providers through a dedicated API.

MSCT transaction feature	Requirements on HUB	
Exchange of transaction data exchange Payment Preparation phase (see Figure 26 in MSCT IG)		
All transaction data is available "in clear" to the payer (e.g. in clear in QR-code or known to the payer) [8]	Not applicable	
Payer uses a proxy for the payee	Translation of proxy into payee's name and IBAN – interconnection between payer's and payee's MSCT service providers is required via the HUB	
Payee-presented transaction data includes a token It is hereby assumed that the tokenisation/de-tokenisation is handled by or via the payee's MSCT service provider.	De-tokenisation into transaction data is needed – interconnection between payer's and payee's MSCT service providers is required via the HUB	
Payee-presented transaction data is incomplete (e.g. contains part of the transaction data "in clear")	Completion of the transaction data is needed by the payee's MSCT service provider - interconnection between payer's and payee's MSCT service providers is required via the HUB	
Notification messages Payment Completion phase, (see Figure 26 in MSCT IG)	**SCT Instant**	**SCT**
Notification to payee about successful transaction	Notification from payer's MSCT service provider to payee's MSCT service provider	Notification from payer's MSCT service provider to payee's MSCT service provider
Notification to payee about unsuccessful transaction	Notification from payer's MSCT service provider to payee's MSCT service provider	Notification from payer's MSCT service provider to payee's MSCT service provider in case the failure is at the payer's 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 payee-presented data

[8] In this case, another mechanism would need to be implemented to ensure the integrity of the data (see MSCT IG).

4 Process flows for MSCT interoperability

4.1 Introduction

In this section the full process flows between the HUB and the respective MSCT service provider back-ends will be illustrated. Note that as defined in the MSCT IG an MSCT service provider could be an ASPSP, a mobile P2P service provider (for P2P payment contexts) or any party acting as a PISP. This means that in the process flows below, one or both MSCT providers could be one or both of the respective ASPSPs in which case the process flows would simplify.

Four cases will be considered as listed in the table below.

MSCT transactions type	Support from the HUB
P2P – the payer uses a proxy for the payee	Retrieval of the payee data from the proxy[9] Notification messages (see section 2.2)[10]
P2P – IBAN payee and name payee is known by the payer	Not applicable
C2B - merchant-presented QR-code contains a token	Retrieval of the transaction data from the token Conditional transaction lock messages (see below) Notification messages (see section 2.2)
C2B - merchant-presented QR-code which contains all transaction data in clear[11]	Conditional transaction lock messages (see below) Notification messages (see section 2.2)

Table 2: Mapping MSCT transaction types onto HUB functionalities

For the C2B payment contexts, the process flows are illustrated for physical POIs. Note however that the process flows would remain the same if the QR-code is shown on a payment page of an e-merchant.

The QR-code may be static or dynamic. In case dynamic QR-codes are used, a conditional transaction lock function is defined as follows. The function consists of conditional lock transaction messages that are sent between the payer's MSCT service provider and the merchant's MSCT service provider via the HUB to prevent that multiple payers from different MSCT service providers pay the same transaction after strong customer authentication (SCA - see chapter 8 in the MSCT IG). The transaction lock function is required in case the QR-code stays active for a certain time window that would enable multiple scans and related payments and its need is specified in the dedicated Lock Transaction Indicator (LT Indicator as defined in section 5 in this

[9] As an example, this functionality is already covered by the SEPA Proxy Lookup (SPL) Scheme defined by the EPC (see https://www.europeanpaymentscouncil.eu/what-we-do/other-schemes/sepa-proxy-lookup-scheme).

[10] The functionality to cover for these notification messages could be considered by the SPL scheme as a possible service extension for P2P payments.

[11] Obviously in this case additional measures should be taken to ensure the security of the data exchanged (for some guidance see MSCT IG).

document). If two payers would perform SCA on the same transaction, the payer with successful SCA for which the lock function sent by their MSCT service provider reaches as first the MSCT service provider of the payee is the one for which the transaction is locked.

For P2P transactions whereby the payee presents a QR-code on their mobile device to the payer and for C2B transactions involving QR-codes on invoices, the process flow will be similar as for C2B transactions with merchant-presented QR-codes.

Note also that in the process flows below, the representation and description of strong customer authentication (SCA) is simplified since the focus is on the interconnectivity between the respective MSCT service providers. More details on SCA are provided in section 8.3 and are illustrated in the MSCT use cases in chapter 7 in the MSCT IG.

In the process flows below, the implicit assumption is made that all MSCT transactions are successful. The flows for unsuccessful transactions would need to be analysed separately. Moreover, all process flows are based on instant SCT transactions (see chapter 4 in the MSCT IG).

Furthermore, the process flows do not include potential exchanges needed between MSCT service provider back-ends for applicable remuneration to support a business model.

4.2 P2P with proxy

The process flow below illustrates the usage of the HUB in the case the payer uses a proxy for the payee.

In this MSCT transaction type, the following actors and interconnectivity are required as depicted below.

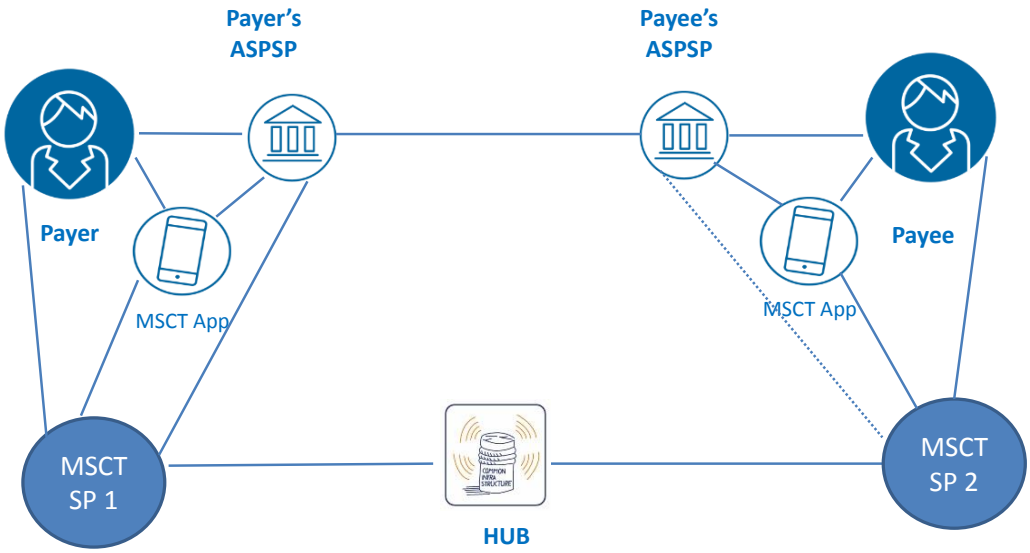
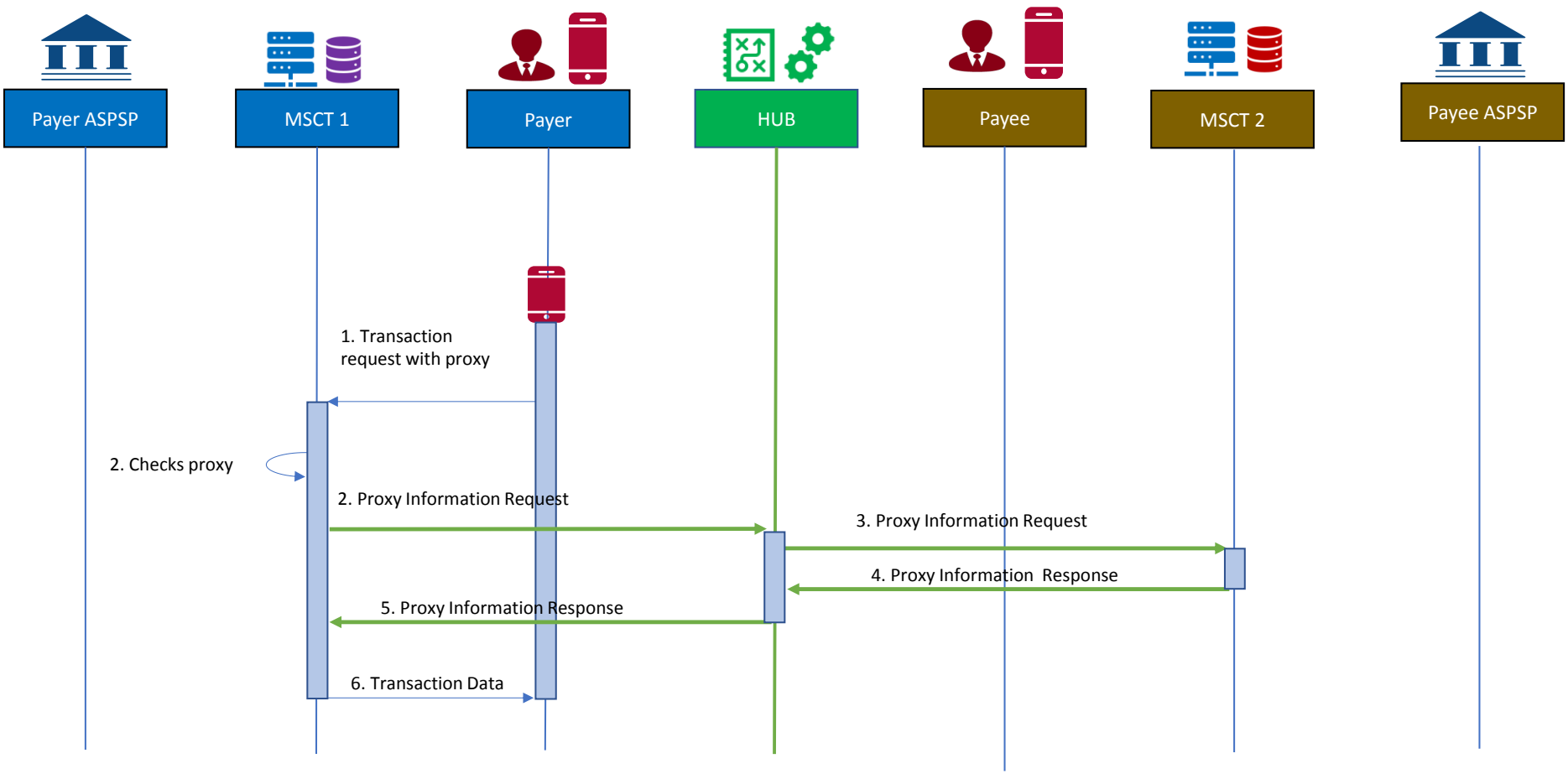


Figure 3: Actors for P2P – with proxy

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


Payer ASPSP
MSCT 1
Payer
HUB
Payee
MSCT 2
Payee ASPSP
1. Transaction request with proxy
2. Checks proxy
2. Proxy Information Request
3. Proxy Information Request
4. Proxy Information Response
5. Proxy Information Response
6. Transaction Data

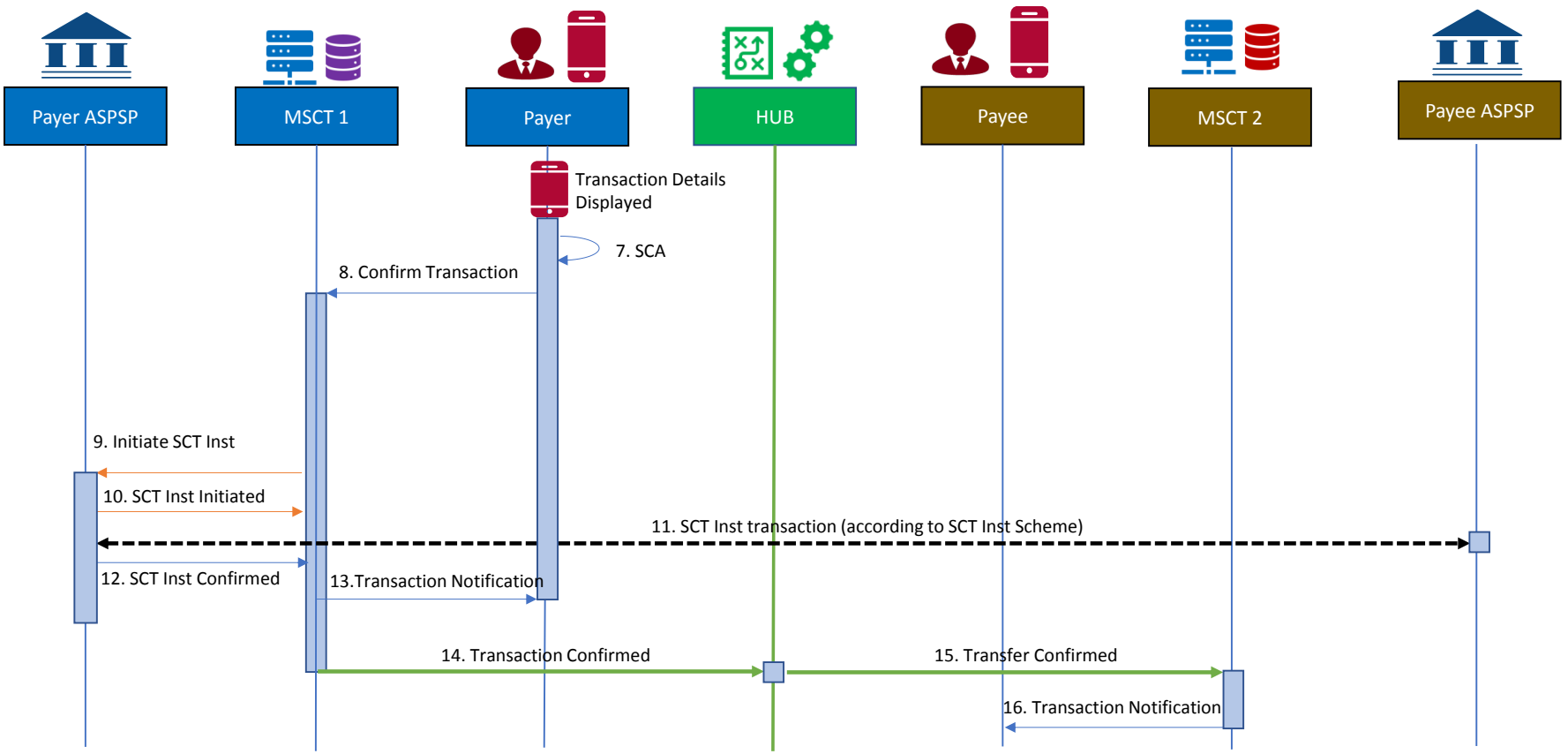


Figure 4: Process flow – P2P – with proxy

In the figure above the following steps are involved:

Step 1:
The payer initiates a new transaction in their MSCT application including the transaction amount and a proxy of the payee which is provided to their MSCT service provider.

Step 2:
The MSCT service provider checks the transaction request received and retrieves the proxy. Next the proxy received is checked in their own directory

- If the IBAN/name of the payee can be retrieved, they are provided to the MSCT app of the payer;
- If the proxy is not available in their own directory, a Proxy Information Request including the proxy is forwarded by the payers' MSCT service provider to the HUB.[12] Note that this is the case illustrated in the figure above.

Step 3:
The HUB forwards the Proxy Information Request to the payee's MSCT service provider.

Step 4:
The payee's MSCT service provider checks the Proxy Information Request, prepares the Proxy Information Response including the IBAN/name of the payee and sends the Proxy Information Response to the HUB.

Step 5:
The HUB forwards the Proxy Information Response to the payer's MSCT service provider.

Step 6:
The payer's MSCT service provider retrieves the payee's details from the Proxy Information Response and provides them to the payer with a request for an SCA.

Step 7:
The payer performs an SCA on the transaction details displayed (see chapter 8 of the MSCT IG).

[12] It is assumed, in case the HUB is provided by the SPL service that both the payer's and the payee's MSCT service providers are registered as IRP and RRP respectively into the SPL scheme (see SPL scheme rulebook, https://www.europeanpaymentscouncil.eu/document-library/rulebooks/sepa-proxy-lookup-spl-scheme-rulebook)

Step 8:
The confirmation including the authentication response is provided to the payer's MSCT service provider.[13]

Step 9:
The payer's MSCT service provider sends an SCT Inst instruction to the payer's ASPSP including the transaction details.

Step 10:
The payer's ASPSP sends a message to the payer's MSCT service provider confirming the initiation of the SCT Inst transaction.

Step 11:
The payer's ASPSP sends the SCT Inst transaction to the payee's ASPSP and the transaction flow is handled according to the SCT Inst scheme (see section 4.2 in MSCT IG).

Step 12:
The payer's ASPSP sends a confirmation message to the payer's MSCT service provider about the execution of the SCT Inst transaction.

Step 13:
The payer's MSCT service provider sends a transaction notification message to the payer.

Step 14:
The payer's MSCT service provider sends a transaction notification message to the HUB.

Step 15:
The HUB forwards the transaction notification message to the payee's MSCT service provider.

Step 16:
The payee's MSCT service provider sends a transaction notification message to the payee.

[13] This description assumes that the payer's MSCT service provider has received delegation from the payer's ASPSP for SCA. Otherwise additional steps are needed for the SCA as described in chapter 7 in the MSCT IG.

4.3 P2P without proxy

The process flow below illustrates that the usage of the HUB is not needed in the case the payer knows the payee name and IBAN, in other words, in case no proxy is used.

In this MSCT transaction type the following actors and interconnectivity are required as depicted below.

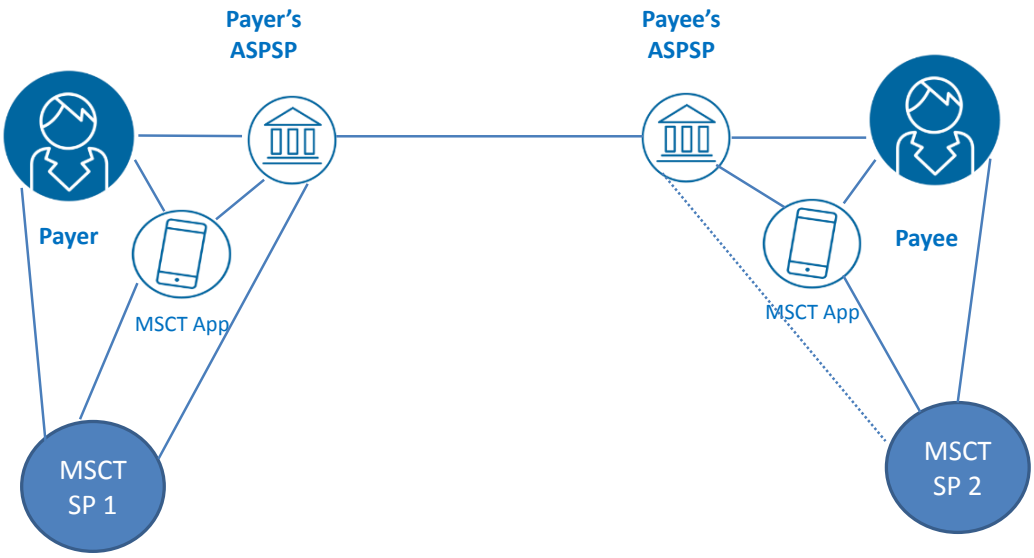
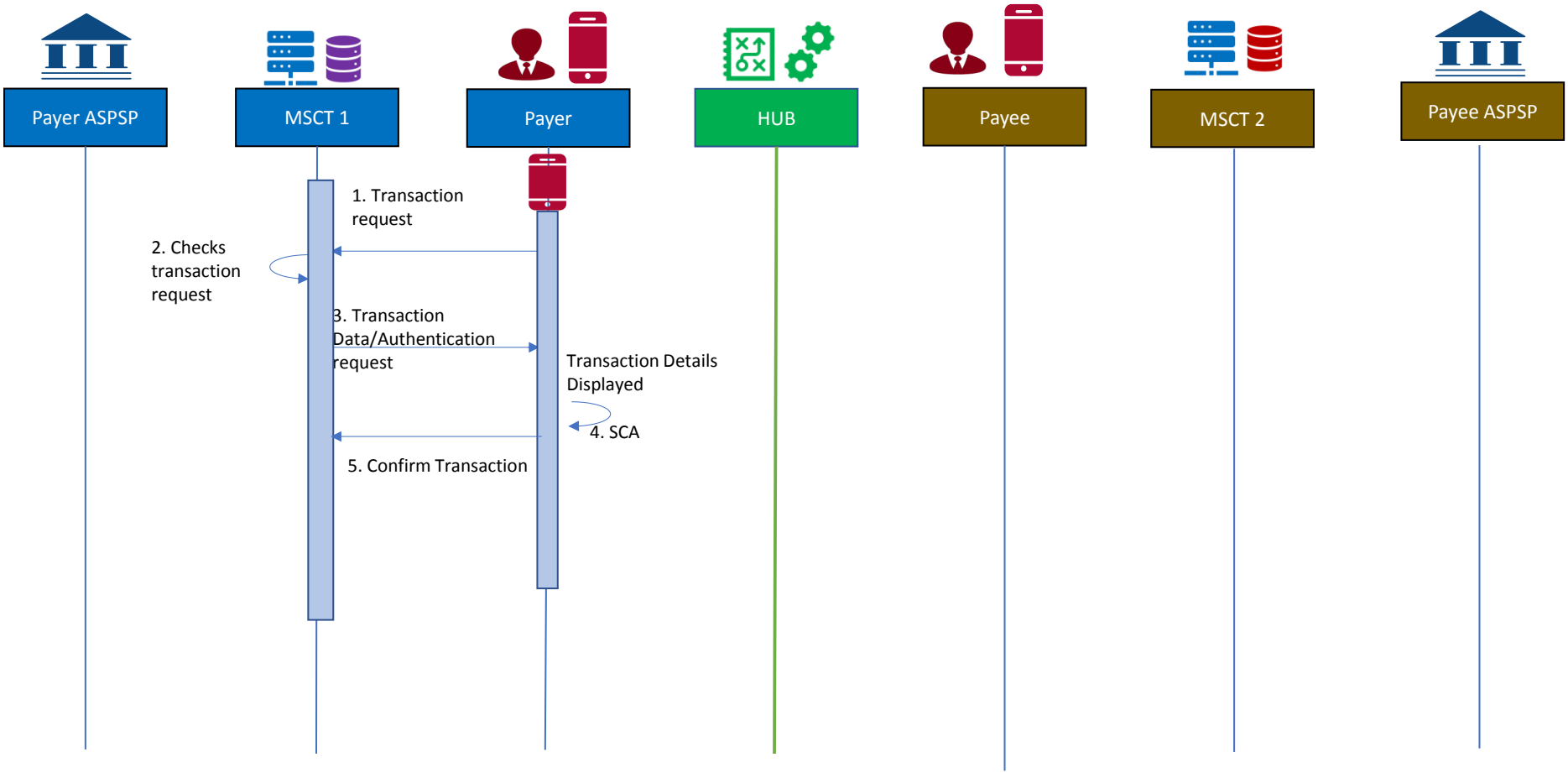


Figure 5: Actors for P2P – without proxy

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


Payer ASPSP
MSCT 1
Payer
HUB
Payee
MSCT 2
Payee ASPSP
1. Transaction request
2. Checks transaction request
3. Transaction Data/Authentication request
Transaction Details Displayed
4. SCA
5. Confirm Transaction

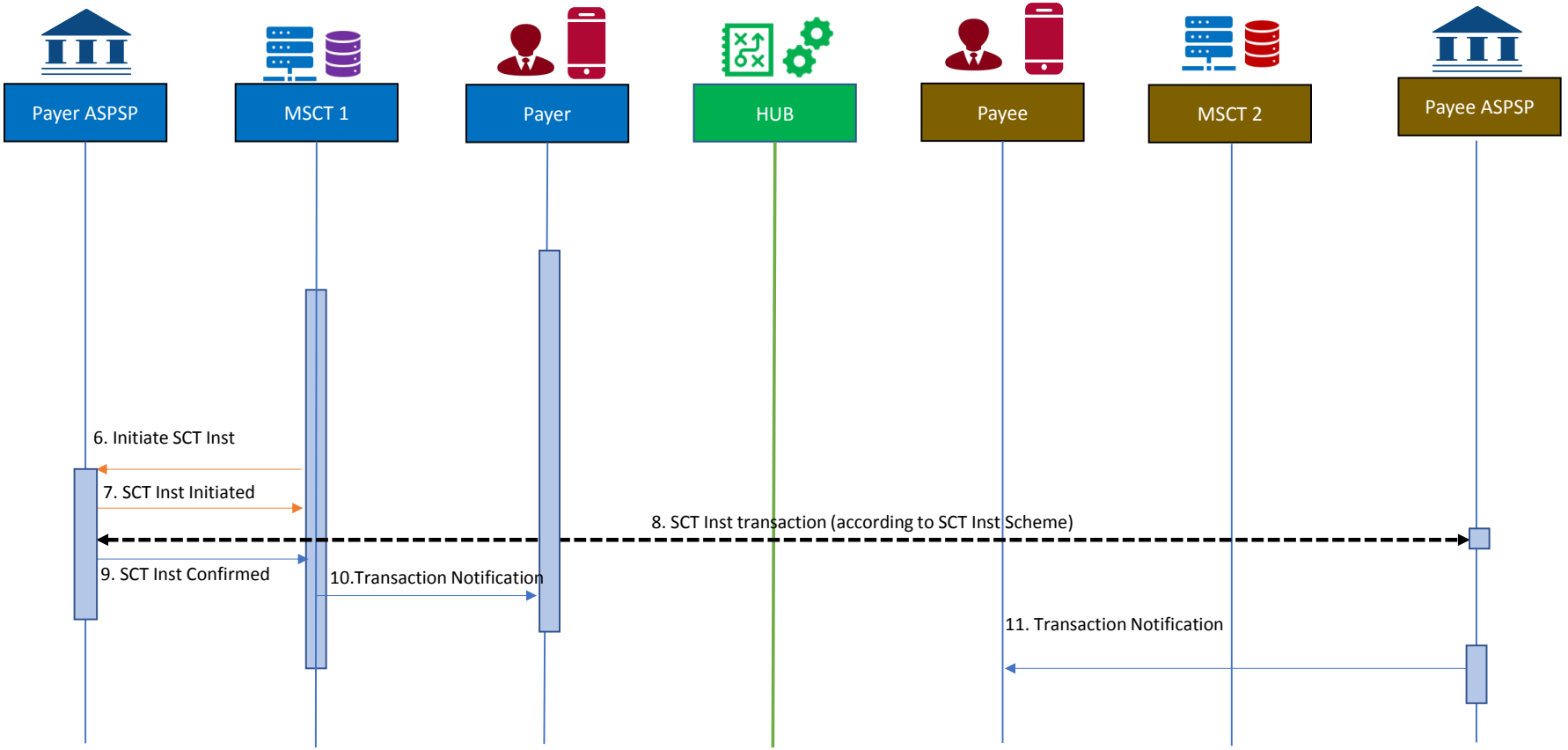


Figure 6: Process flow – P2P – without proxy

In the figure above the following steps are involved:

Step 1:
The payer initiates a new transaction in their MSCT application including the transaction amount and payee details which is provided to their MSCT service provider.

Step 2:
The MSCT service provider checks the transaction initiation request received.

Step 3:
The payer's MSCT service provider sends an SCA request based on the transaction details to the payer.

Step 4:
The payer performs an SCA on the transaction details displayed.

Step 5:
The confirmation including the authentication response is provided to the payer's MSCT service provider.[14]

Step 6:
The payer's MSCT service provider sends an SCT Inst instruction to the payer's ASPSP including the transaction details.

Step 7:
The payer's ASPSP sends a message to the payer's MSCT service provider confirming the initiation of the SCT Inst.

Step 8:
The payer's ASPSP sends the SCT Inst transaction to the payee's ASPSP and the transaction flow is handled according to the SCT Inst scheme (see section 4.2 in MSCT IG).

Step 9:
The payer's ASPSP sends a confirmation message to the payer's MSCT service provider about the execution of the SCT Inst transaction.

Step 10:
The payer's MSCT service provider sends a transaction notification message to the payer.

Step 11:
The payee's ASPSP sends a transaction notification message to the payee.

[14] This description assumes that the payer's MSCT service provider has received delegation from the payer's ASPSP for SCA. Otherwise additional steps are needed for the SCA as described in chapter 7 in the MSCT IG.

4.4 C2B with token

The process flow below illustrates the usage of the HUB in case the merchant-presented data does not contain the necessary transaction data "in clear" and a token is used instead. This may be a dynamic or a static token. It is hereby assumed that the tokenisation/de-tokenisation of (part of) the transaction data is handled by or via the merchant's MSCT service provider.

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

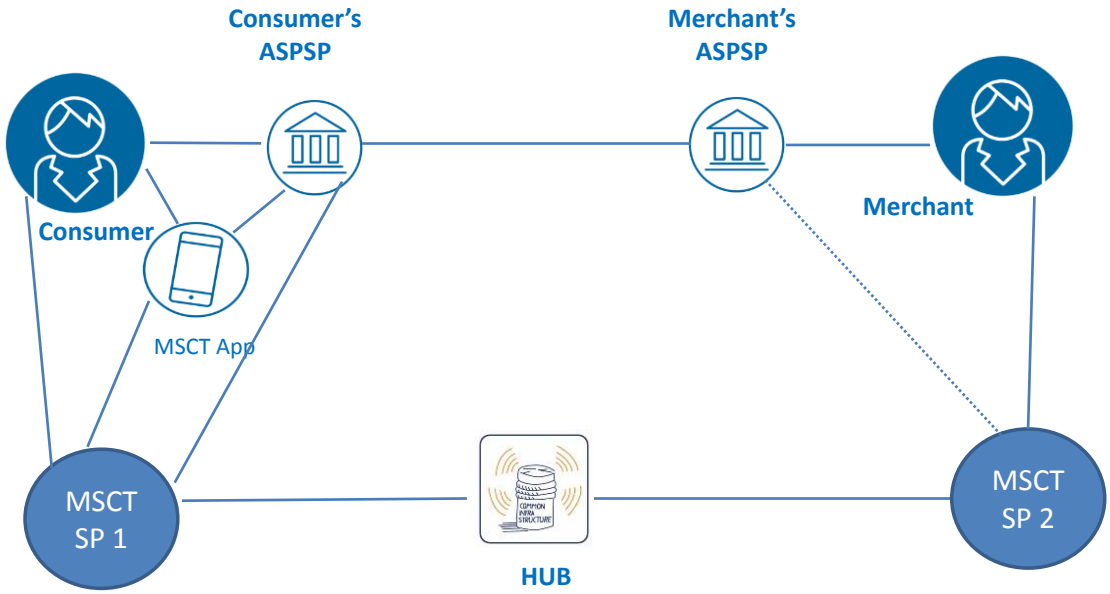
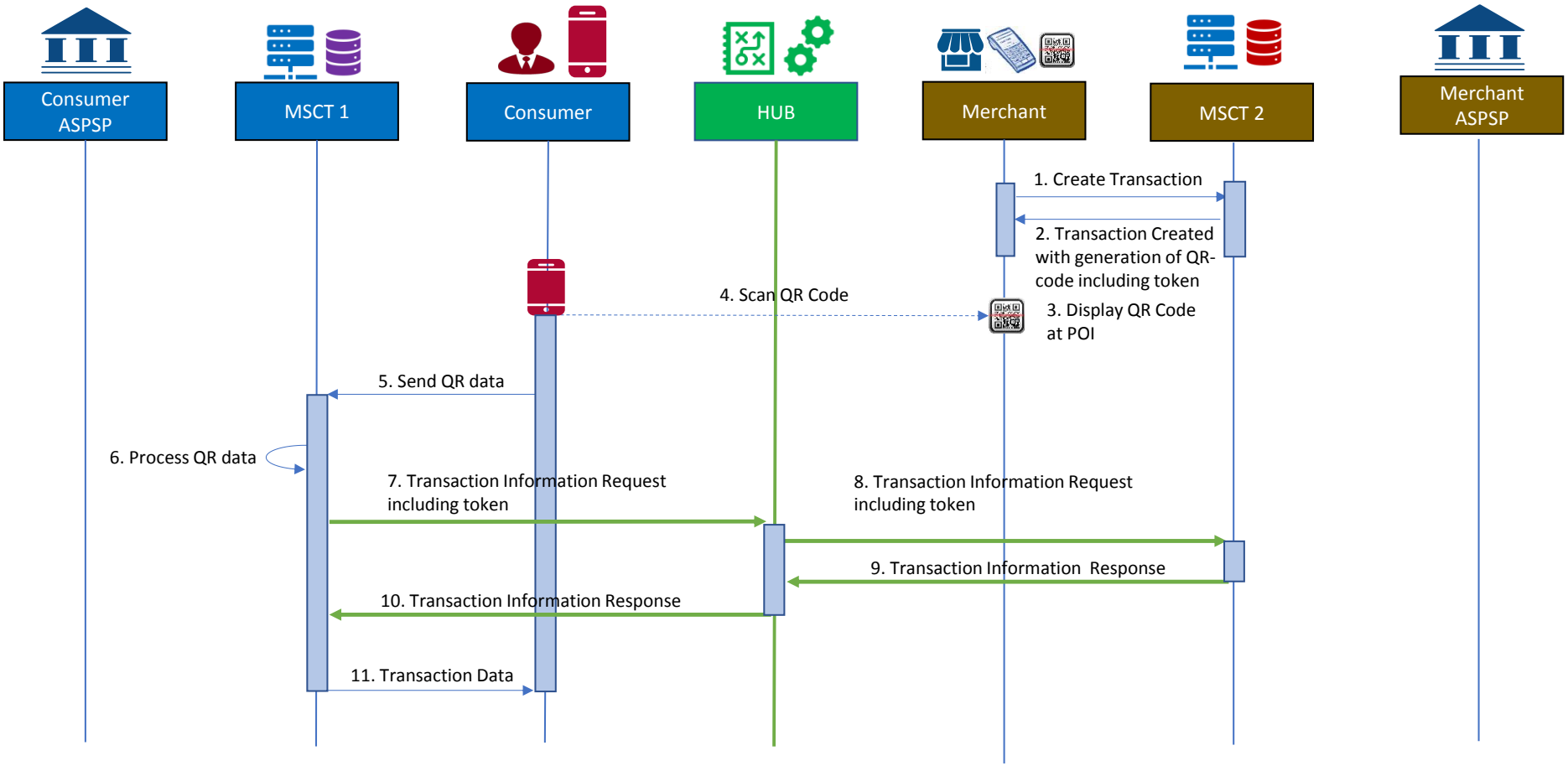


Figure 7: Actors for C2B - with token

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


Consumer ASPSP
MSCT 1
Consumer
HUB
Merchant
MSCT 2
Merchant ASPSP
1. Create Transaction
2. Transaction Created with generation of QR-code including token
3. Display QR Code at POI
4. Scan QR Code
5. Send QR data
6. Process QR data
7. Transaction Information Request including token
8. Transaction Information Request including token
9. Transaction Information Response
10. Transaction Information Response
11. Transaction Data

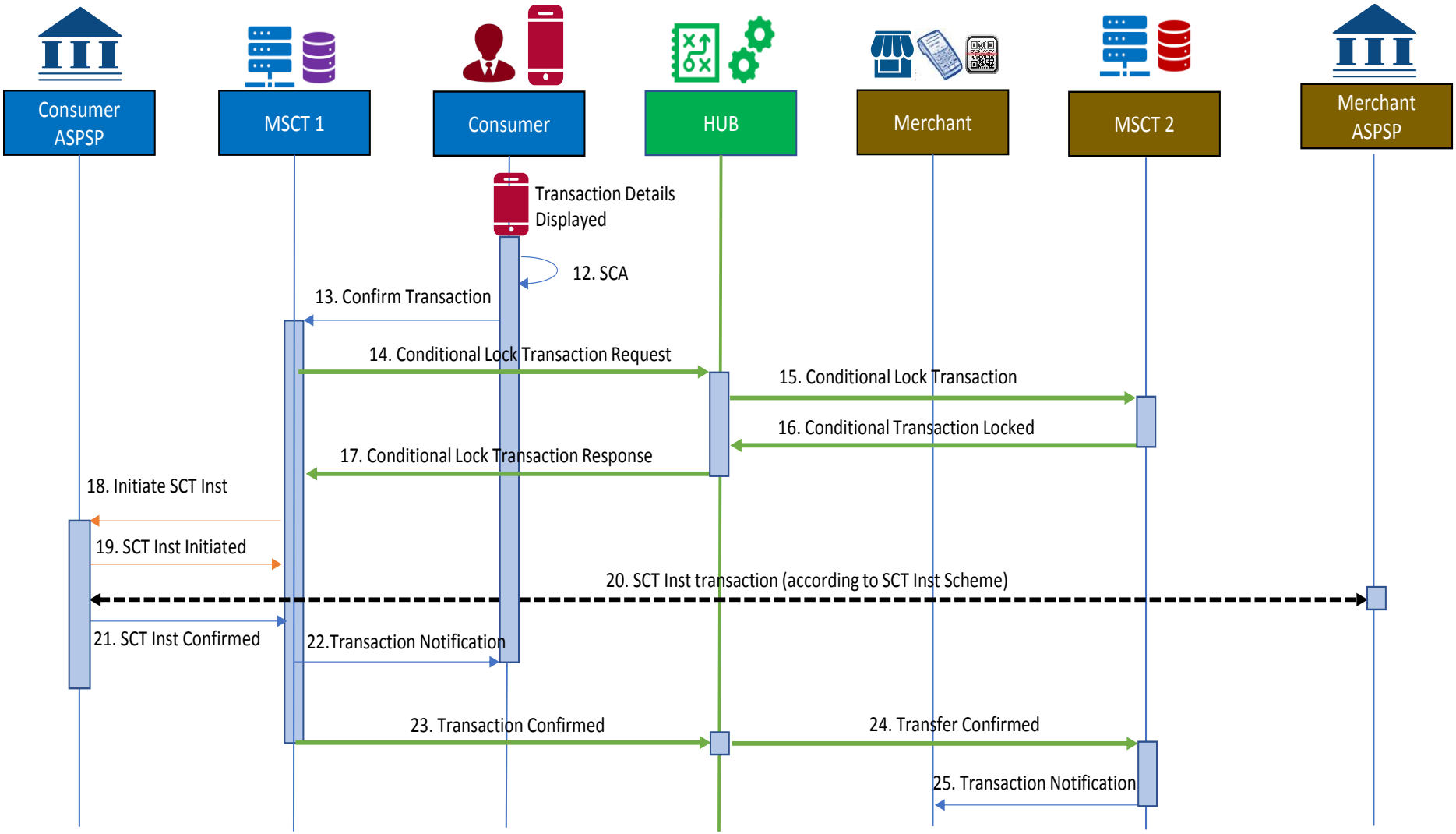


Figure 8: Process flow – C2B – merchant-presented QR-code with token

In the figure above the following steps are involved:

Step 1:
The merchant creates a new transaction and provides a new transaction request with the transaction details, including the transaction amount to their MSCT service provider.

Step 2:
The merchant's MSCT service provider returns a QR-code including a dedicated token based on the transaction details (transaction amount, IBAN_merchant, transaction identifier) and their MSCT service provider identifier to the merchant.[15]

Step 3:
The merchant POI displays the transaction amount with the QR-code.

Step 4:
The consumer opens their MSCT application and scans the QR-code.

Step 5:
The data, including the token and MSCT service provider identifier is retrieved from the QR-code and provided to the consumer's MSCT service provider.

Step 6:
The consumer's MSCT service provider checks the QR-code data and prepares a Transaction Information Request including the token.

Step 7:
The Transaction Information Request including the merchant's MSCT service provider identifier is sent to the HUB.

Step 8:
The HUB identifies the merchant's MSCT service provider and forwards them the Transaction Information request.

Step 9:
The merchant's MSCT service provider checks the request, prepares the response and sends the Transaction Information Response to the HUB.

Step 10:
The HUB forwards the Transaction Information Response to the consumer's MSCT service provider.

Step 11:
The consumer's MSCT service provider retrieves the transaction details from the Transaction Information Response and sends them to the consumer with a request for an SCA.

[15] As an alternative, the MSCT service provider could also return the token to the merchant and their POI generates the QR-code.

Step 12:
The consumer performs an SCA on the transaction details displayed.

Step 13:
The confirmation including the authentication response is provided to the consumer's MSCT service provider.[16]

Step 14 (conditional)[17]:
The consumer's MSCT service provider sends a Lock Transaction Request to the HUB including the merchant's MSCT service provider identifier.

Step 15(conditional):
The HUB forwards a "Lock Transaction" to the merchant's MSCT service provider.

Step 16 (conditional):
The merchant's MSCT service provider sends a "Transaction Locked" to the HUB.

Step 17 (conditional):
The HUB forwards the Lock Transaction Response to the consumer's MSCT service provider.

Step 18:
The consumer's MSCT service provider sends an SCT Inst instruction to the consumer's ASPSP including the transaction details.

Step 19:
The consumer's ASPSP sends a message to the consumer's MSCT service provider confirming the initiation of the SCT Inst.

Step 20:
The consumer's ASPSP sends the SCT Inst transaction to the merchant's ASPSP and the transaction flow is handled according to the SCT Inst scheme (see section 4.2 in MSCT IG).

Step 21:
The consumer's ASPSP sends a confirmation message to the consumer's MSCT service provider about the execution of the SCT Inst transaction.

Step 22:
The consumer's MSCT service provider sends a transaction notification message to the consumer.

[16] This description assumes that the consumer's MSCT service provider has received delegation from the consumer's ASPSP for SCA. Otherwise additional steps are needed for the SCA as described in chapter 7 in the MSCT IG.
[17] See sections 4.1 and 5. In case the LT Indicator does not require a lock transaction function, steps 14 through 17 will not be present.

Step 23:
The consumer's MSCT service provider sends a transaction notification message to the HUB with the merchant's MSCT service provider identifier.

Step 24:
The HUB forwards the transaction notification message to the merchant's MSCT service provider.

Step 25:
The merchant's MSCT service provider sends a transaction notification message to the merchant.

4.5 C2B without token

The process flow below illustrates the usage of the HUB in the case the merchant-presented data does contain all the necessary transaction data "in clear". This will typically occur for a QR-code on an invoice as illustrated below.

In this MSCT transaction type the following actors and interconnectivity are required as depicted below.

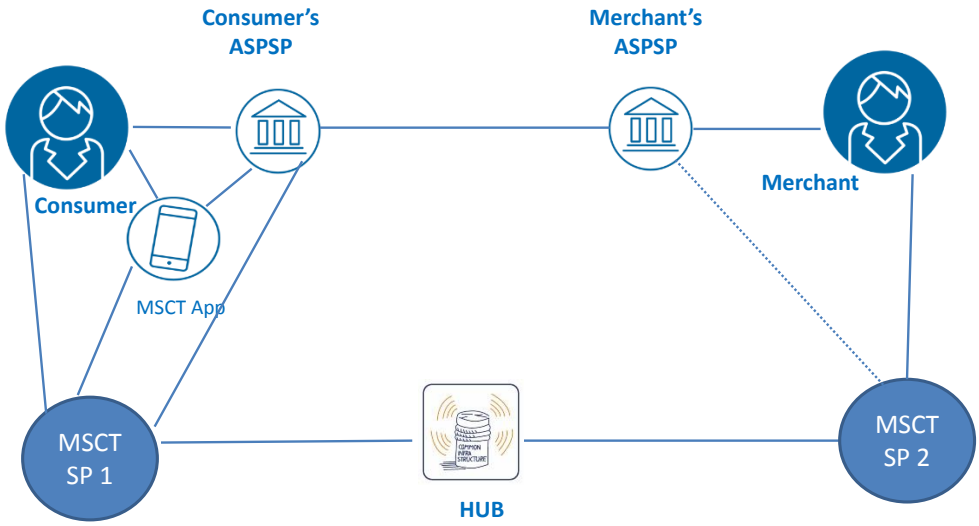
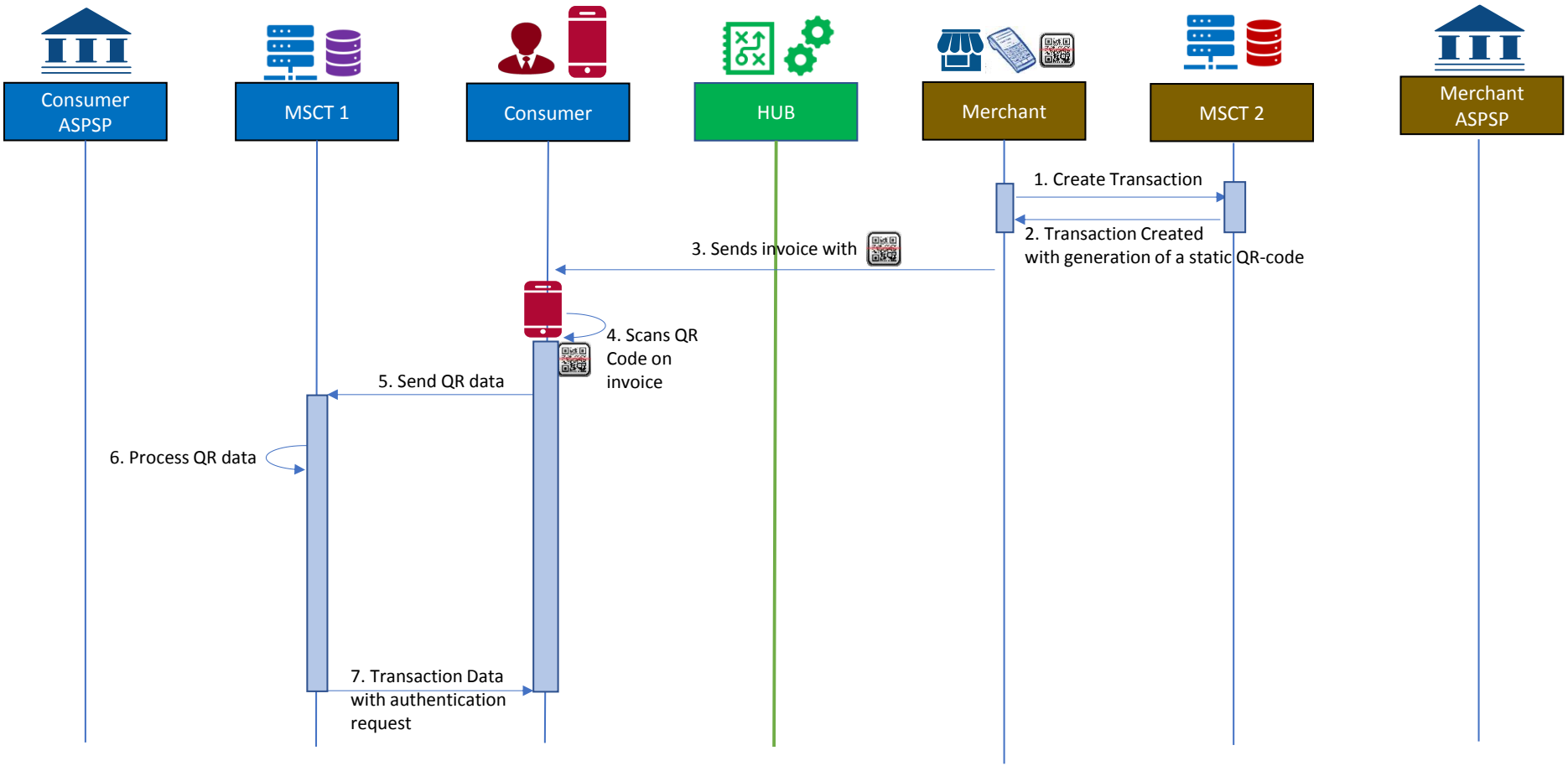


Figure 9: Actors for C2B – without token

The detailed process flows between the different actors involved for this MSCT transaction type are shown in the next figure. In case of an invoice, the LT indicator in the QR-code will not require a lock function and therefore the related messages are not shown in the process flow below.


Consumer ASPSP
MSCT 1
Consumer
HUB
Merchant
MSCT 2
Merchant ASPSP
1. Create Transaction
2. Transaction Created with generation of a static QR-code
3. Sends invoice with
4. Scans QR Code on invoice
5. Send QR data
6. Process QR data
7. Transaction Data with authentication request

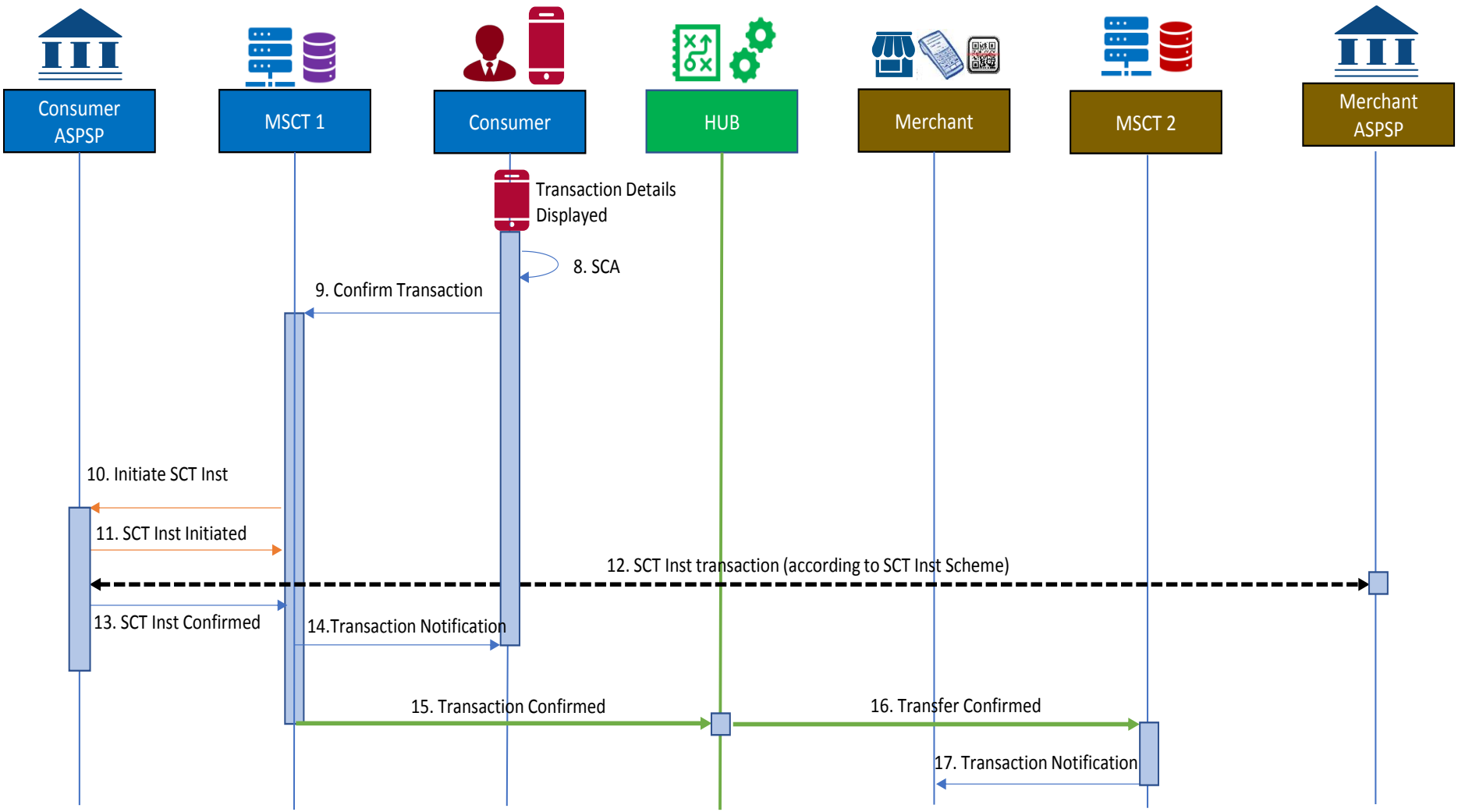


Figure 10: Process flow – C2B – merchant-presented QR-code with full transaction data

In the figure above the following steps are involved:

Step 1:
The merchant creates a new transaction and provides a new transaction request with the transaction details, including the transaction amount to their MSCT service provider.

Step 2:
The merchant's MSCT service provider returns a QR-code based on the transaction details (transaction amount, IBAN_merchant, transaction identifier) and an MSCT service provider identifier to the merchant.[18]

Step 3:
The merchant prepares the invoice, displaying the QR-code and provides the invoice to the consumer.

Step 4:
The consumer opens their MSCT application and scans the QR-code from the invoice.

Step 5:
The transaction data and merchant's MSCT service provider identifier are retrieved from the QR-code and provided to the consumer's MSCT service provider.

Step 6:
The MSCT service provider checks the QR-code data.

Step 7:
The MSCT service provider sends an authentication request to the consumer.

Step 8:
The consumer performs an SCA on the transaction details displayed.

Step 9:
The confirmation including the authentication response is provided to the consumer's MSCT service provider.[19]

Step 10:
The consumer's MSCT service provider sends an SCT Inst instruction to the consumer's ASPSP including the transaction details.

[18] As an alternative, the MSCT service provider could also return the transaction identifier to the merchant and their POI generates the QR-code.
[19] This description assumes that the consumer's MSCT service provider has received delegation from the consumer's ASPSP for SCA. Otherwise additional steps are needed for the SCA as described in chapter 7 in the MSCT IG.

Step 11:
The consumer's ASPSP sends a message to the consumer's MSCT service provider confirming the initiation of the SCT Inst.

Step 12:
The consumer's ASPSP sends the SCT Inst transaction to the merchant's ASPSP and the transaction flow is handled according to the SCT Inst scheme (see section 4.2 in MSCT IG).

Step 13:
The consumer's ASPSP sends a confirmation message to the consumer's MSCT service provider about the execution of the SCT Inst transaction.

Step 14:
The consumer's MSCT service provider sends a transaction notification message to the consumer.

Step 15:
The consumer's MSCT service provider sends a transaction notification message to the HUB with the merchant's MSCT service provider identifier.

Step 16:
The HUB forwards the transaction notification message to the merchant's MSCT service provider.

Step 17:
The merchant's MSCT service provider sends a transaction notification message to the merchant.

5 Minimum Data Set for MSCTs

To achieve interoperability for MSCTs, an agreement on a minimum data set is required for the data to be exchanged between the payer/consumer and payee/merchant. Any future specification of the data needed for the messages between the respective MSCT service providers, through the HUB, will need to take this minimum data set into account.

The minimum data set to be exchanged between the payee and the payer, will rely on the MSCT transaction feature, such as described in Table 1 in section 3 in this document:

1. If the transaction data is available "in clear" to the payer (e.g. in clear in QR-code or known to the payer), the minimum data set will consist of both routing info and necessary payload data.

2. If the payer uses a proxy for the payee, the minimum data will consist of both routing info and necessary payload data, including the proxy. The translation of the proxy into the payee's name and IBAN will be done through the interconnection between the payer's and payee's MSCT service providers through the HUB.

3. If the payee-presented transaction data includes a token, the minimum data will consist of both routing info and a token as payload. The translation of the token into the transaction data will be done through the interconnection between the payer's and payee's MSCT service providers through the HUB.

The proposed minimum data sets for these 3 cases will include:

For case 1 above: *transaction data is available "in clear" to the payer:* [Version]+[Type]+ [Routing info] + [a clear-text name/value string]
For case 2 above: *the payer uses a proxy for the payee:* [Version]+[Type]+ [Routing info] + [proxy] + [a clear-text name/value string]
For case 3 above: *the payee-presented transaction data includes a token:* [Version]+[Type]+ [Routing info] + token]

Table 3: Minimum data sets for MSCTs

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

The type may refer to the Payment Context and the Lock Transaction (LT) Indicator.

As an example, the routing info and payload data for MSCTs based on payee-presented QR-codes are described in the section below.

6 Example: Payee-presented QR-code for MSCTs

To enable MSCT interoperability across SEPA, for the data exchange between the payee and payer for all payment contexts, an MSCT QR-code should be standardised based on the minimum data set defined in section 5 of this document.

This standardised MSCT QR-code should be adopted by all MSCT service providers and supported by the MSCT apps in the payer's mobile device, either in the MSCT app (direct reading of the QR-code by the MSCT app) or via a link between the MSCT app and the QR-reader on the mobile device to achieve interoperability across SEPA.

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

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

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

1. Make a generic routing/payload data-exchange at POI between the payee and the payer;
2. Routing goes directly or via (a) HUB(s) between MSCT service providers;
3. Avoid having specific details about merchant and transaction in the data exchange[20] in order to
    a. Reduce privacy/security concerns;
    b. Reduce maintenance concerns related to QR-code distribution;
    c. Increase readability of the QR-code.

[20] A typical exception would be QR-codes on invoices.

Type

The type contains the Payment Context and the Lock Transaction Indicator.

The Payment Context should enable to differentiate between the three cases mentioned under section 5 above.

As an example, the Payment Context could read as follows:

- /m/ merchant POI (physical POI in-store);
- /e/ merchant POI (e-or m-commerce);
- /i/ invoice payment;
- /p/ P2P payment.

The Lock Transaction Indicator is used to inform about the need of the Lock Transaction Function to mitigate the risk about unwanted multiple payments for the same QR-code (see also section 4.1 in this document).

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.

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

Table 4: Coding of QR-code

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

Content in payload related to the Payment Contexts:

The different payment contexts could require different payload requirements. As examples,

- POI situations should avoid having clear-text information (such as IBAN_merchant) in the QR-code.
- For Invoice-payments, the QR-code could include clear-text information that is visual anyway on the invoices.

In the table below, the proposed payload data for the three use cases defined in section 4 in this document are listed.

Payload Data		
Case 1 *transaction data is available "in clear" to the payer*	Name payee (account holder)	
	Trade name	
	IBAN payee	
	MCC	Merchant Category Code
	Purpose of credit transfer (includes e.g. merchant transaction identifier)	Data for reconciliation purposes at payee – is included from initiation through entire transaction payment chain
	Remittance information structured or Remittance information unstructured	
	Currency	
	Transaction amount	
Case 2 *the payer uses a proxy for the payee*	Proxy	
	MCC	Merchant Category Code
	Purpose of credit transfer (includes e.g. merchant transaction identifier)	Data for reconciliation purposes at payee – is included from initiation through entire transaction payment chain)
	Remittance information structured or Remittance information unstructured	
	Currency	
	Transaction amount	
Case 3 *the payee-presented transaction data includes a token*	Token	

Table 5: Payload data