EPC193-22v1.2

ISO #####-#:####(X)

ISO TC ###/SC ##/WG #

Date: 2022-11-21

Financial services — Specification of QR-codes for mobile (instant) credit transfers

DIS stage

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

A model manuscript of a draft International Standard (known as "The Rice Model") is available at https://www.iso.org/iso/model_document-rice_model.pdf

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by the Multi-Stakeholder Group on Mobile Initiated SEPA (Instant) Credit Transfers, established by the European Payments Council (see www.epc-cep.eu) and drafted in accordance with the ISO editorial rules. It is based on the document Standardisation of QR-codes for mobile initiated SEPA (instant) credit transfers (EPC024-22v1.0, [2]), published by the EPC. It will submitted to ISO for adoption under the “fast-track procedure” with the intention to assign it to ISO Technical Committee ISO/TC 68, Financial services, Subcommittee SC 9, Information exchange for financial services.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

QR-codes are one of the proximate technologies that may be used for the data exchange between a payer and a payee to enable the initiation of an (instant) credit transfer.

This document specifies the QR-code formats for both a payer-presented and a payee-presented QR-code. They have been defined to support the initiation of (instant) credit transfers by the payer (so-called push payments) for various payment contexts, including person-to-person, person-to-business, business-to-person and business-to-business payments, including public services.

Financial services - Standardisation of QR-codes for (instant) credit transfers

1 Scope

This document provides a specification for QR-codes for mobile (instant) credit transfers (MCTs) whereby the payer uses a mobile device to initiate the payment transaction. The QR-code is used to exchange data between the payer and the payee to enable the initiation of the (instant) credit transfer by the payer.

This document is applicable to both cases where the QR-code is presented by the payee or by the payer.

This document excludes the following from its scope:

— The details of technical requirements and the supporting infrastructure to achieve interoperability amongst mobile (instant) credit transfer (MCT) service providers;

— The detailed implementation specification of the payload included in the QR-code.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18004: 2015, *Information technology -- Automatic identification and data capture techniques - QR-code bar code symbology specification*

ISO/IEC 15417: 2007, *Information technology — Automatic identification and data capture techniques — Code 128 bar code symbology specification*

ISO 12812-1: 2017, *Core banking – Mobile financial services – Part 1: General framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12812 – Part 1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp
— IEC Electropedia: available at https://www.electropedia.org/

3.1
alias
see proxy (ISO 12812-1 [4])

3.2
account servicing payment service provider
ASPSP

PSP providing and maintaining a payment account for a PSU

[SOURCE: ISO 23195: 2021, 3.1.6 [6]]

3.3
business identifier code
means a code as defined by ISO 9362 [3].

3.4
consumer device
an internet capable device used by the consumer (payer) to conduct an (instant) payment.

EXAMPLE: mobile phone, tablet.

3.5
2D barcode
a two-dimensional barcode is a machine-readable optical label that contains digital information.

EXAMPLE: QR-codes, tag barcodes.

3.6
hub
an infrastructure ensuring connectivity between MCT service providers.

3.7
instant
at once, without delay

3.8
instant payment
electronic retail payment solutions available 24/7/365 and resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payer (within seconds of payment initiation).

3.9
MCT payment application
a set of modules (application software) and/or data (application data) needed to provide functionality for an MCT as specified by the MCT service provider in accordance with the rules of the (instant) credit payment scheme.

3.10
MCT service provider
a mobile financial service provider that offers or facilitates a mobile initiated (instant) credit transfer to a payer and /or a payee.

3.11
merchant-presented data
data provided by the merchant's POI to the consumer to enable the initiation of an MCT.

3.12
payee-presented data
data provided by the payee to the payer to enable the initiation of an MCT.

3.13
payee reference party
a person/entity on behalf of or in connection with whom the payee receives a payment.

3.14
payer-presented data
data provided by the payer to the payee to enable the initiation of an MCT.

3.15
payload issuer
the entity responsible for issuing the payload.

3.16
payment account
an account held in the name of one or more PSUs which is used for the execution of payment transactions

3.17
payment account identifier
PA-ID
a unique identifier that is assigned by an ASPSP and references a payment account record hold by a PSU.

EXAMPLE: IBAN, see [4]

3.18
payment initiation service provider
PISP
a third party payment service provider that initiates a payment on behalf of the payer with the payer's ASPSP holding the payment account

3.19
payment institution
an entity authorized to provide payment services under the applicable regulations

3.20
account servicing payment service provider identifier
ASPSP-ID
a unique identifier that is assigned to every payment institution

EXAMPLE: BIC, see [3]

3.21
payment request
a set of rules and technical elements (including messages) that allow a payee to claim an amount of money from a payer for a specific transaction.

3.22
payment service provider
PSP
entity that provides payment services to a payment service user

EXAMPLE: ASPSP, PISP.

3.23
payment service user
PSU
a natural or legal person making use of a payment service in the capacity of payer, payee, or both.

3.24
payment transaction
an act, initiated by the payer or on his/her behalf or by the payee (beneficiary), of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.

3.25
QR-code
Quick-response code (see ISO/IEC 18004).

3.26
token
a surrogate value for PSU identification and/or transaction data; if the token is included in the payee-presented data it might be referred to as a payee token and if the token is included in the payer-presented data it might be referred to as a payer token.

3.27
token service
a system comprised of the key functions that facilitate generation and issuance of tokens and maintain the established mapping of tokens to the related data when requested by the token requestor.

3.28
token service provider
TSP
an entity that provides a token service.

4 Abbreviations

an:	alphanumeric
API:	Application Programme Interface
ASPSP:	Account Servicing Payment Service Provider
ASPSP-ID:	Account Servicing Payment Service Provider Identifier
BIC:	Business Identifier Code
CDUVM:	Consumer Device User Verification Method
CT:	(Instant) Credit Transfer
SCT:	SEPA (Instant) Credit Transfer
IBAN:	International Bank Account Number
IG:	Interoperability Guidance
MCT:	Mobile Initiated (Instant) Credit Transfer
MSCT:	Mobile Initiated SEPA (Instant) Credit Transfer
PA-ID:	Payment Account Identifier
PISP:	Payment Initiation Service Provider
POI:	Point of Interaction
POS:	Point of Sale
PSP:	Payment Service Provider
PSU:	Payment Service User
SEPA:	Single Euro Payments Area
TSP:	Token Service Provider
TTP:	Trusted Third Party

5 Interoperability of MCTs

Mobile initiated (instant) credit transfers (MCTs) are initiated directly (by the payer) or indirectly (by an MCT service provider at the request of the payer) in compliance with the applicable regulations, using a mobile device. MCT solutions are offered by so-called MCT service providers which are service providers that offer or facilitate a payment service to a payer/a payee based on an (instant) CT. As an example, an MCT service provider could be an ASPSP, a PISP or a technical service provider supporting a PSP.

MCTs typically use an MCT payment application or a browser on the payer device to initiate or at least authenticate and authorise the (instant) CT transaction, besides some features of the payer device such as the support of a CDUVM (e.g., a mobile code or biometrics on the mobile device), the mobile device screen to display transaction information, etc. MCTs may involve the provision of a dedicated MCT payment application for download on the payer's or the payee's device or the provision of dedicated software for the payee's (e.g. merchant's) POI.

In this document the following generic 4-corner model is used for the technical interoperability of MCTs. Hereby it is assumed that both payer and payee are customers of different ASPSPs that are (instant) CT scheme participants, while the entities assuming the role of MCT service provider are depicted as separate entities that are different for the payer and the payee. Obviously, if the role of MCT service provider would be assumed by an ASPSP the model below would simplify. Alternatively, multiple PSPs (such as a PISP or a collecting PSP on behalf of the merchant) could be involved between the payer/payee and their respective ASPSP.

NOTE Interoperability models involving a PISP or collecting PSP have for instance been studied in the MSCT IG [1].

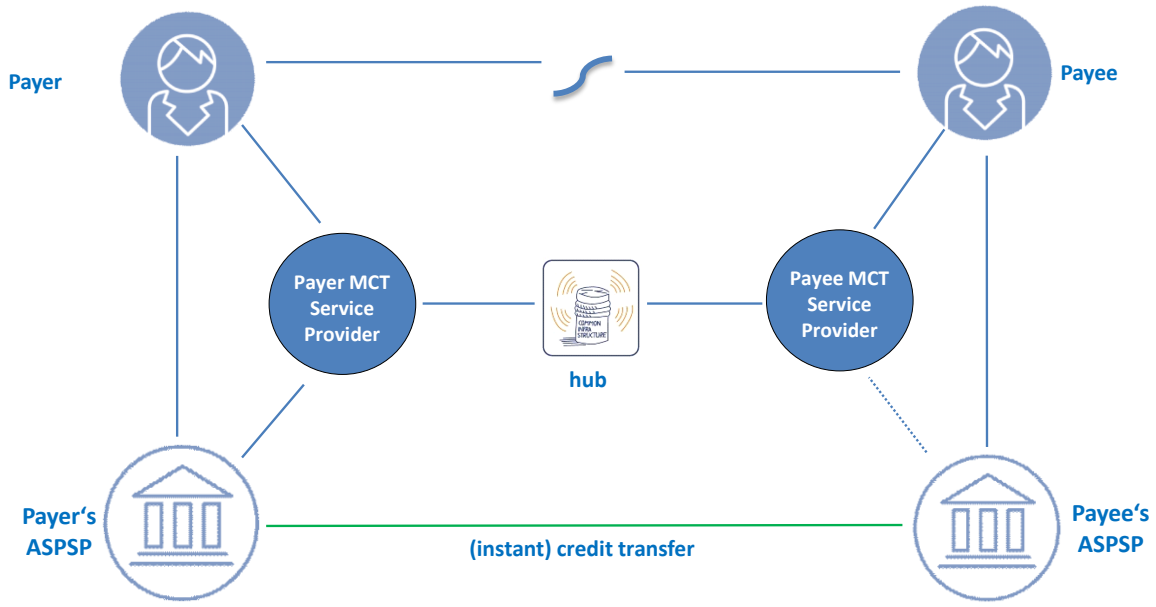


Figure 1 — Generic 4-corner interoperability model for MCTs

As depicted above, the payer's MCT service provider is linked to the payer's ASPSP and the payee's MCT service provider may be linked to the payee's ASPSP (this linkage may include both technical and contractual aspects).

The MCT ecosystem involves some new stakeholders in the payment value chain, including a so-called Token Service Provider (TSP) who is a TTP which is involved if tokens are used in MCTs as surrogate values for MCT related data (including for instance the payee/payer identification data, the payee/payer PA-ID, the ASPSP-ID, transaction amount or merchant transaction identifier). The TSP manages the generation and issuance of tokens, and maintains the established mapping of tokens to the related transaction data. For simplification it is assumed in this document that the role of the TSP is assumed or is under the control of the MCT service provider (and therefore the TSP is not depicted in the figure above).

To achieve interoperability for the generic basic 4-corner model, the concept of a "hub" to interconnect the respective MCT service providers is considered as shown in the figure above. Hereby the term "hub" is used to indicate an "infrastructure" that enables interconnectivity between MCT service providers but it is meant to be agnostic to the way it might be implemented – different implementation models may be possible (centralised or de-centralised (e.g. a direct API)).

EXAMPLE The technical interoperability requirements between MCT service providers involving a "hub" have been analysed and defined in detail in the MSCT IG [1]. Examples of interoperability process flows may also be found in Annex B.

One of the technical interoperability aspects for MCTs is the exchange of (transaction) data between the payer and the payee to enable the initiation of an MCT. The usage of QR-codes for this data exchange will be treated in the next clause.

6 Standardisation of QR-codes for MCTs

6.1 Introduction

This chapter is devoted to MCTs whereby a QR-code (see ISO 18004) is used as proximate technology for the data exchange between the payer and the payee to enable the initiation of an MCT. Hereby two modes may be distinguished:

- *MCTs based on payee-presented data:* in this mode the data presented refers both to payee identification data and transaction data;
- *MCTs based on payer-presented data:* in this mode the data presented refers to payer identification data.

6.2 Minimum data set and QR-code format for payee-presented QR-codes

6.2.1 Introduction

This section considers the exchange of data (payee identification data and transaction data) via a QR-code displayed by the payee (e.g. merchant POI or payee's mobile device) and read by the payer's mobile device. For the purpose of this document, the following three cases with respect to the type of payee-presented data are considered:

- *The payee-presented data includes a "(payee) token"*. In this case, a de-tokenisation process needs to take place such that all the data (payee identification and transaction data) can be derived from the token and provided to the payer via their MCT service provider. This generally requires the support of the payee's MCT service provider (see for example the Information Request/Response messages in Annex B) prior to the initiation of the MCT transaction.
- *The payee-presented data contains a "proxy" for the payee identification data.* In this case the data that is not present in clear but corresponds to the proxy, needs to be provided by the payee's MCT service provider upon request from the payer's MCT service provider prior to the initiation of the MCT transaction.
- *The payee-presented data includes all data in "clear"* (e.g. the payee's name, trade name, the payee's PA-ID, the payee's ASPSP-ID, the transaction amount, the transaction identifier, etc.). This enables the immediate initiation of the MCT transaction.

Next to this data exchanges also an identifier of the payee MCT service provider is needed by the hub for routing purposes for the exchange of messages between the respective MCT service providers.

Note also that in the last two cases described above, appropriate security measures need to be taken to ensure the integrity of the data and the confidentiality as appropriate (see Clause 7 and [7]).

To achieve interoperability within an (instant) MCT scheme or framework, the payee MCT service provider should support at least one of the types while the payer's MCT service provider should be able to support all types as specified by the scheme or framework.

6.2.2 Minimum data sets

The minimum data set to be exchanged between the payee and the payer, will rely on the MCT transaction feature, as described above:

1 If the payee-presented data provided to the payer contains a (payee) token, the minimum data will consist of both routing info and the token as payload. The minimum data will be forwarded in a Transaction Information Request message through the hub from the payer's

MCT service provider to the payee's MCT service provider for de-tokenisation into the transaction data (see Annex B).

2 If the payee-presented data provided to the payer contains only part of the transaction data in clear but contains a proxy for the payee data, the data related to the proxy will need to be provided by the payee's MCT service provider. The minimum data set will consist of both routing info, the proxy and the available transaction data in clear. The proxy will be forwarded in a Transaction Information Request message through the hub from the payer's MCT service provider to the payee's MCT service provider for completion of the transaction data.

3 If the payee-presented data provided to the payer contains all transaction data "in clear", the minimum data set will consist of both routing info and all necessary payload data in clear.

Therefore the minimum data sets for the payee-presented QR-code, covering the three cases described above are as follows:

Table 1 — Payee-presented QR-code

Payee-presented QR-code
Payee-presented QR-code includes a token: [Version]+[Type]+ [Payee MCT Service Provider ID] + [(payee) token]
Payee-presented QR-code contains a proxy for the payee: [Version]+[Type]+ [Payee MCT Service Provider ID] + [proxy] + [a clear-text name/value string]
Payee-presented QR-code includes all transaction data "in clear": [Version]+[Type]+ [Payee MCT Service Provider ID] + [a clear-text name/value string]

Note: A combination of these different formats may appear in a single QR-code to enable the payee (e.g. the merchant) to support multiple MCT schemes through a single QR-code having multiple payloads.

The reader is referred to Clause 6.4 for an explanation of the "Version" and "Type" in the Table above.

6.3 Minimum data set and QR-code format for payer-presented QR-codes

6.3.1 Introduction

To achieve interoperability of MCTs based on payer-presented data, at least payer identification data (which enables the payer's MCT service provider to identify the payer) and an identifier of the payer's MCT service provider are needed.

The payer identification data is defined by the MCT service provider and may take a variety of forms and may be static or dynamic. This payer identification data will need to be transferred as part of the

Payment Request message from the payee to their MCT service provider and further to the payer's MCT service provider to enable the identification of the payer (see Annex B).

In addition, an identifier of the payer's MCT service provider is needed by the payee's MCT service provider and subsequently by the hub to know where to route the Payment Request message.

6.3.2 To achieve interoperability within an (instant) MCT scheme or framework, all payee and payer MCT service providers should support this payer-presented data.Minimum data set

The minimum data set to be exchanged between the payer and the payee included in the payer-presented QR-code contains the (payer) token and may contain additional clear-text (e.g. related to a loyalty scheme).

Therefore the minimum data set for the payer-presented QR-code is as follows:

Table 2 — Payer-presented QR-code

Payer-presented QR-code
[Version]+[Type]+[Payer MCT Service Provider ID]+[(payer) token]+ [a clear-text name/value string]

The reader is referred to section 6.4 for an explanation of the "Version" and "Type" in the Table above.

6.4 Standardised format of QR-codes for MCTs

6.4.1 Introduction

To enable MCT interoperability for the data exchange between the payee and the payer, MCT QR-codes formats need to be standardised based on the minimum data sets defined in the clauses.

The standardised payee-presented QR-codes should be adopted by all MCT service providers and supported by the payer's device in a given MCT interoperability scheme or framework, either in the MCT payment application (direct reading of the QR-code by the MCT payment application) or other appropriate methods to achieve interoperability.

The standardised payer-presented QR-code should be adopted by all MCT service providers and supported by the payee's equipment (e.g. merchant's POI or payee's mobile device) in a given MCT interoperability scheme or framework.

6.4.2 Assumptions for the development of QR-codes for MCTs

For the development of a standardised QR-code for MCTs, based on ISO /IEC 18004, the following four assumptions are followed:

— Mobile wallets will often support multiple payment instruments. The wallet user will often select or set a default payment instrument;
— Payees (e.g. merchants) may often support multiple payment instruments and brands. The payee could set a preferred (prioritised) payment brand for MCTs based on a payee-presented QR-code;
— Need to 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 payer would like to use);
— Need to avoid any special actions from the wallet user at the POI (more in particular in stores - e.g., swiping through a POS-menu to find a specific wallet generates friction).

When following the assumptions above, a QR-code format for MCTs for data exchange between the payee and the payer is hereby defined based on the following preconditions:

— Make a generic routing/payload data-exchange between the payee and the payer;
— Routing goes directly or via (a) hub(s) between MCT service providers;
— Enable to avoid having specific details about payee, payer and transaction in the data exchanged in order to
    - Reduce privacy/security concerns;
    - Reduce maintenance concerns related to QR-code distribution;
    - Increase readability of the QR-code.

6.4.3 QR-codes for MCTs

The QR-codes format for MCTs are URL based with a recognisable structure.

The structure of the QR-code for MCTs is defined as follows:

— A URL based on https:// structure
— First part of the URL: ordinary domain structure
— Second part of the URL: version
— Third part: type (this may refer to the payment context)
— Fourth part: routing information
— Fifth part: payload information[1].

Table 3 — Payee-presented QR-code

HTTPS://<Domain_name>/<Version>/<Type>/<Payee MCT service provider ID>/<Payload>

Table 4 — Payer-presented QR-code

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

[1] The payload is included in the URL as a query string.

The **Domain name** refers to an MCT Interoperability Framework or Scheme.

The **Version** refers to the specification version of the QR-code and allows future updates to the QR-code.

The **Type** refers to

- for payee-presented QR-codes it refers to the different payment contexts (e.g. mobile payment at the POI):
- for payer-presented QR-codes it is for future, e.g. it could enable to add other services[2].

The **MCT service provider identifier** is used in the interoperability space for routing purposes, therefore a standardised coding of this data element is necessary (see Clause 6.5).

The payload is at the discretion of the payload issuer who may be the MCT service provider or a different entity, operating under this MCT service provider. It shall contain the minimum data for the payload as defined in sections 6.2 and 6.3. In addition the payload shall contain the identification of the entity issuing the content of the payload – the so-called payload issuer. Since different payload issuers may operate under the same MCT service provider, this MCT service provider is responsible for the identification of the payload issuers.

6.5 Coding of the QR-code data fields

In view of the interoperability of QR-codes for MCTs, the coding of the different data fields in the QR-code shall be standardised as defined in the sections below. Note that the payload is at the discretion of the payload issuer. The only constraint is that the parameters have to be structured so that the URL in its entirety is a valid URL according to the URL specification

(https://www.w3.org/Addressing/URL/url-spec.txt).

6.5.1 Domain_name

The domain name refers to the interoperability domain for MCT service providers for MCTs and shall refer to an "*MCT Interoperability Framework*" or "an *MCT Scheme* or participant" operated under the MCT Interoperability Framework or scheme. The exact coding of this field needs to be defined by the MCT Interoperability Framework or Scheme, e.g., qr.INTFRM.org.

To provide maximum flexibility and decentralised administration of local apps INTFRM.org should support the main domain (qr.INTFRM.org), subsequent subdomains (xy.INTFRM.org) and local URL (qr.xy.xy). A look-up table service by the MCT Interoperability Framework or Scheme could support the above as well as domestically existing QR-codes of the Interoperability Framework or Scheme members and potential interoperability with other QR-code standards.

6.5.2 Version

A version number shall support further updates to the QR-code.

/1/ refers to the first version.

6.5.3 Type

For payee-presented QR-codes: the type indicates what kind of payment context is expected.

The pre-defined payment context could also determine what kind of query parameters will be allowed in the payload. For example, because of security issues, a QR-code used at the POI would not allow clear-text data.

[2] An example may be a refund.

The following coding shall be applied:

— /m/ mobile payment at the POI

— /e/ e-commerce (and m-commerce) payment

— /i/ invoice payment

— /p/ person-to-person payment

— /w/ opening a URL in a webview (e.g. virtual POI).

For payer-presented QR-codes: the type is reserved for future use.

6.5.4 MCT service provider ID

An identifier needs to be assigned to every MCT service provider for routing purposes. This will require an eligibility checking and registration of the MCT service provider under the "MCT Interoperability Framework or Scheme".

This MCT Interoperability Framework of Scheme is also responsible for the issuance of the MCT service provider ID.

The coding of the MCT service provider ID shall be 3 characters alphanumeric (an).

6.5.5 Payload

The information included in the payload is at the discretion of the payload issuer. Standard URL query parameters should be used to delimit the payload information, such as "?" as starting parameter and "&" as delimiter of information. Annex A provides examples of payloads for the three cases defined in section 6.2.2 for payee-presented QR-codes and for the unique case defined in section 6.3.2 for payer-presented QR-codes are listed.

7 Security aspects of QR-codes and their data

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

In principle, a QR-code code may be static, e.g., payee account data and related payment details for a fixed transaction amount (typical use case is a sticker to initiate a payment) or may be dynamic (i.e. the QR-code is invalid whence used) to initiate/identify a single specific MCT transaction (e.g., at a POI).

Tampering QR-code data may lead to fraudulent transactions or data leakage. Therefore the sensitive payment data in the QR-code should be adequately protected while also the integrity of the data elements in the QR-code should be ensured to avoid any service disruptions. Obviously the integrity of this data, as appropriate, shall be checked before any transaction information is displayed to the payer on their mobile device.

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

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

7.1.1 Payee-presented QR-codes

If proxy or other payload information is present "in clear" in the QR-code, it is strongly recommended to have an adequate integrity protection of these data to avoid manipulations with the intention to initiate fraudulent transactions (e.g., to a fake payee or with a wrong transaction amount).

It should further be noted that in certain countries, there are recommendations to protect the PA-ID outside the space between PSPs. This means that in some countries it is recommended that the PA-ID (e.g. IBAN) is not included "in clear" into the payee-presented QR-code.

In view of the considerations made above, the usage of a dynamic token to represent the payee identification and transaction data, more in particular for C2B payments, is recommended.

In addition, to protect the data contained in the QR-code, the MCT payment application on the payer's mobile device must enforce a properly encrypted and authenticated connection to the payer's MCT service provider.

7.1.2 Payer-presented QR-codes

If the payer-presented QR-code is static (e.g., a static token) it could lead to impersonation attacks and initiation of fraudulent transactions and reputational damage. Therefore, the usage of a dynamic token (i.e. that can only be used once) to represent the payer identification data, more in particular for C2B payments is recommended.

If additional data is present "in clear" in a payer-presented QR-code, it is recommended to have integrity protection of these data to avoid mistakes.

In addition, to protect the data contained in the QR-code, the MCT payment application on the payee's infrastructure (e.g. POI, mobile device) must enforce a properly encrypted and authenticated connection to the payee MCT service provider.

7.1.3 Additional security measures

For both modes, appropriate security measures should also be applied by the entity/application creating the QR-code.

A more detailed risk analysis on payments based on QR-codes with the specification of mitigating security measures is undertaken in [7]. Most of the security requirements and guidelines in this document are also applicable to QR-codes for MCTs such as:

- The MCT payment application should prohibit the screenshot function when displaying the QR-code, or provide corresponding security measures, such as reminding the payer promptly or notifying the server side to invalidate the displayed QR-code when detecting a screenshot attack.
- The payer/payee device shall be able to recognise illegitimate codes, reject them or prompt a warning message (e.g., by the inclusion of a white list into the MCT payment application).

Annex A
(informative)
Examples of payload data in QR-codes for MCTs

A.1 Introduction

In the clauses below, examples of payload data for MCTs based on (instant) CTs within SEPA for payee-presented QR-codes and for payer-presented QR-codes are provided. Standard URL query parameters should be used to delimit the payload information, such as "?" as starting parameter and "&" as delimiter of information. Furthermore, the tables below indicate whether a data element in the payload is mandatory (M) or optional (O), in compliance to Annex 5 in the MSCT IG (see EPC269-19 [1]).

A.2 Payload for payee-presented QR-codes

The table below provides examples of payloads for MCTs based on (instant) CTs within SEPA for payee-presented QR-codes, for each of the three types specified in Table 1.

Table 5 — Payload for payee-presented QR-codes for MCTs within SEPA

Payload for payee-presented QR-codes for MCTs within SEPA			
QR-code content	Attribute	Purpose	Coding
QR-code contains a token	Payload Issuer (M)	Entity responsible for issuing the content of the Payload	3 an
	Token (M)	Token for the payee identification and transaction data	1 to 300 an
QR-code contains a proxy[3]	Payload Issuer (M)	Entity responsible for issuing the content of the Payload	3 an
	Proxy (M)	Proxy for the payee identification data	1 to 70 an
	Proxy (O)	Proxy for the payee reference party identification data	1 to 70 an
	MCC (M for C2B)	Merchant Category Code	4n
	Type of payment instrument (M)	SCT or SCT Inst	3 to 4an
	Purpose of credit transfer (includes e.g. merchant transaction identifier) (O)	Data for reconciliation purposes at payee (e.g., merchant) – is included from initiation through entire transaction payment chain	1 to 4 an

[3] This use case represents an example of usage of a proxy. All data that is not represented by the proxy shall be present "in clear" in the payload.

	Remittance information structured or Remittance information unstructured (O)	Information supplied by the payer in the SCT Inst/ SCT Instruction and transmitted to the payee in order to facilitate the payment reconciliation	1 to 35 an
	Currency (M)		1 to 3 an
	Transaction amount (M)		1 to 12 n
QR-code contains all data "in clear"	Payload Issuer (M)	Entity responsible for issuing the content of the Payload	3 an
	Name payee (account holder) (M)		1 to 70 an
	Trade name merchant (M for C2B and B2B)		1 to 35 an
	Name of payee reference party (O)		1 to 70 an
	Trade name of payee reference party (O)		1 to 35 an
	IBAN payee (M)		1 to 34 an
	MCC (M for C2B)	Merchant Category Code	4 n
	Type of payment instrument (M)	SCT or SCT inst	3 to 4 an
	Purpose of credit transfer (includes e.g. merchant transaction identifier) (O)	Data for reconciliation purposes at payee (e.g., merchant) – is included from initiation through entire transaction payment chain	1 to 4 an
	Remittance information structured or Remittance information unstructured (O)	Information supplied by the payer in the SCT Inst/ SCT Instruction and transmitted to the payee in order to facilitate the payment reconciliation	1 to 35 an
	Currency (M)		1 to 3 an
	Transaction amount (M)		1 to 12 n

A.3 Payload for payer-presented QR-codes

The table below provides an examples of payload for MCTs based on (instant) CTs within SEPA for payer-presented QR-codes, as specified in Table 2.

Table 6 — Payload for payer-presented QR-code for MCTs within SEPA

Payload for payer-presented QR-codes for MCTs within SEPA			
QR-code content	Attribute	Purpose	Coding
QR-code contains a token	Payload issuer (M)	Entity responsible for issuing the content of the Payload	3 an
	Token (M)	Token for the payer identification data	1 to 70 an
	Additional data for value-added services (O)	Clear-text	1 to 70an

Annex B
(informative)
Examples of process flows for interoperability of MCTs based on QR-codes

B.1 Introduction

This annex provides two examples of process flows when QR-codes are used for MCTs:

- The payee-presented QR-code contains a (payee) token;
- The payer-presented QR-code contains a (payer) token.

These two examples are intended to illustrate the process flows between the different actors involved in the payment transaction.

Note that both examples have been illustrated in a C2B payment context (i.e. the payee is a merchant and the payer is a consumer) at a physical POI based on an instant CT.

B.2 Process flow for merchant-presented QR-code containing a token

The detailed process flows between the different actors involved in this MCT transaction are shown in the next figure. Hereby the token contained in the merchant-presented QR-code is sent by the consumer MCT service provider to the merchant MCT service provider (over the hub) in the Transaction Information Request message to obtain the merchant and transaction data to enable the initiation of the MCT. Note that it is hereby assumed that the merchant MCT service provider fulfils the role of Token Service Provider for the merchant. The merchant MCT service provider ID (retrieved from the merchant-presented QR-code and contained in the Transaction Information Request message) is used by the hub to route the Transaction Information Request message to the merchant MCT service provider.

Note that if the merchant-presented QR-code would contain all the merchant-presented data "in clear-text", steps 7 to 10 would be omitted.

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

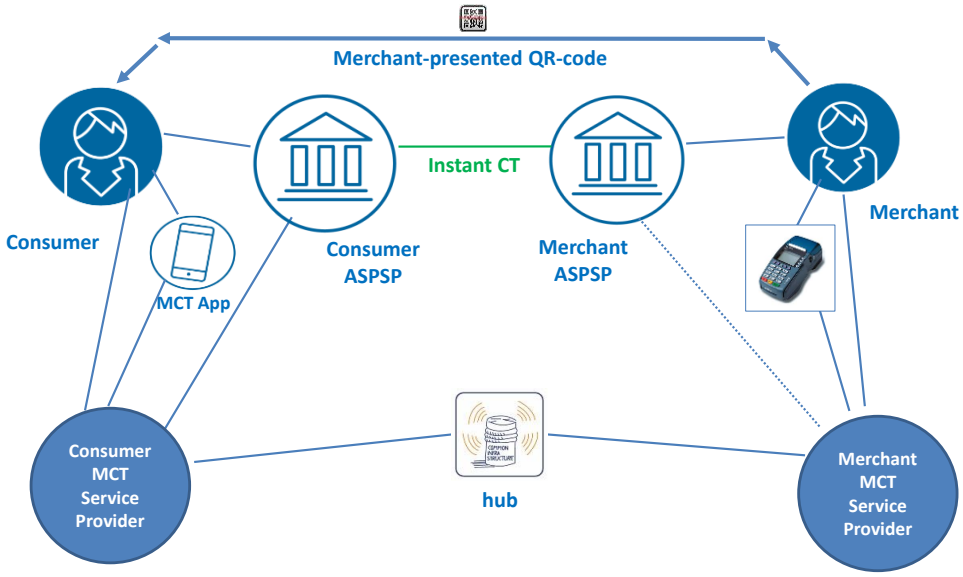
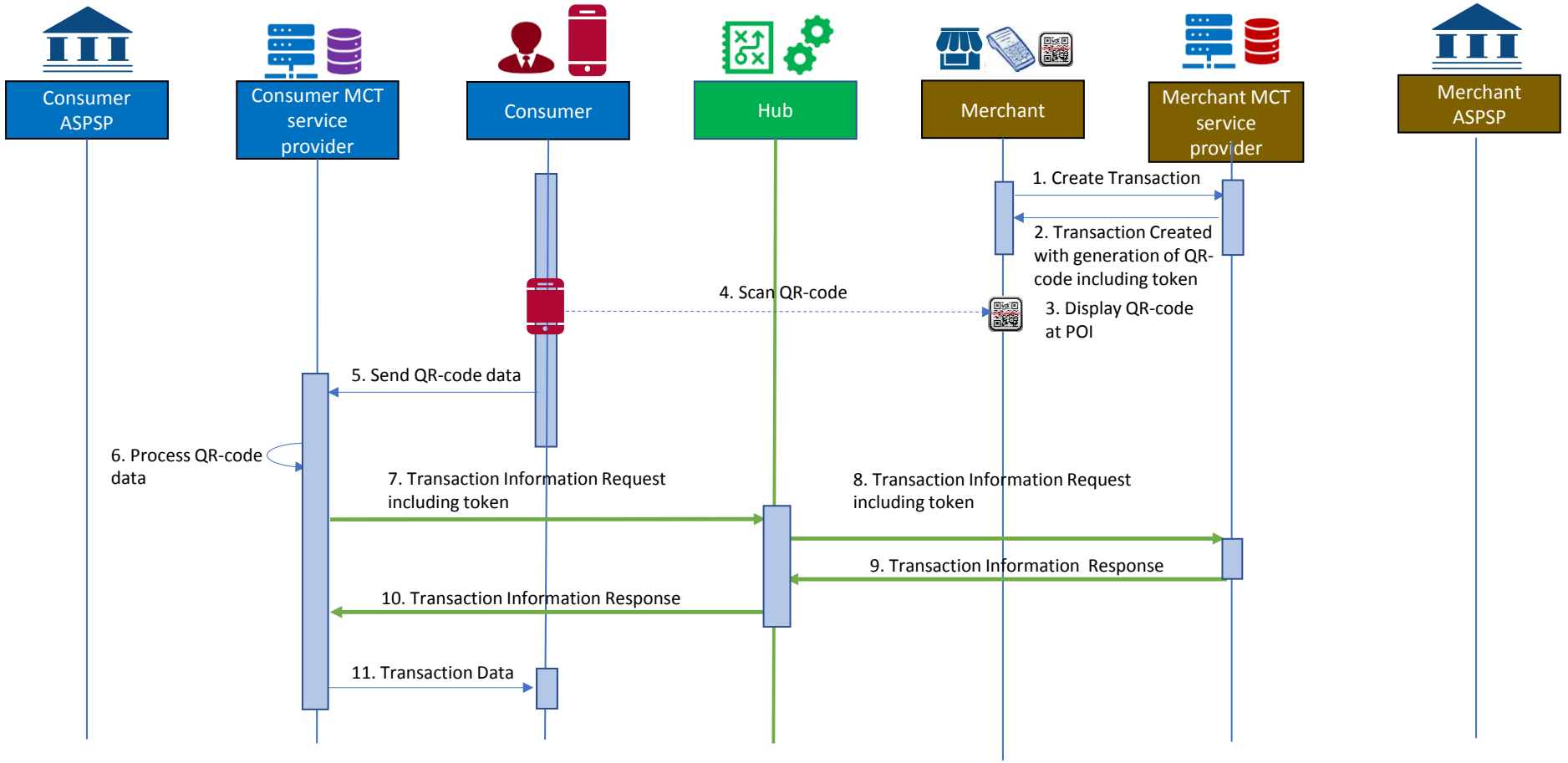


Figure 2 — Actors for MCT with merchant-presented QR-code

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



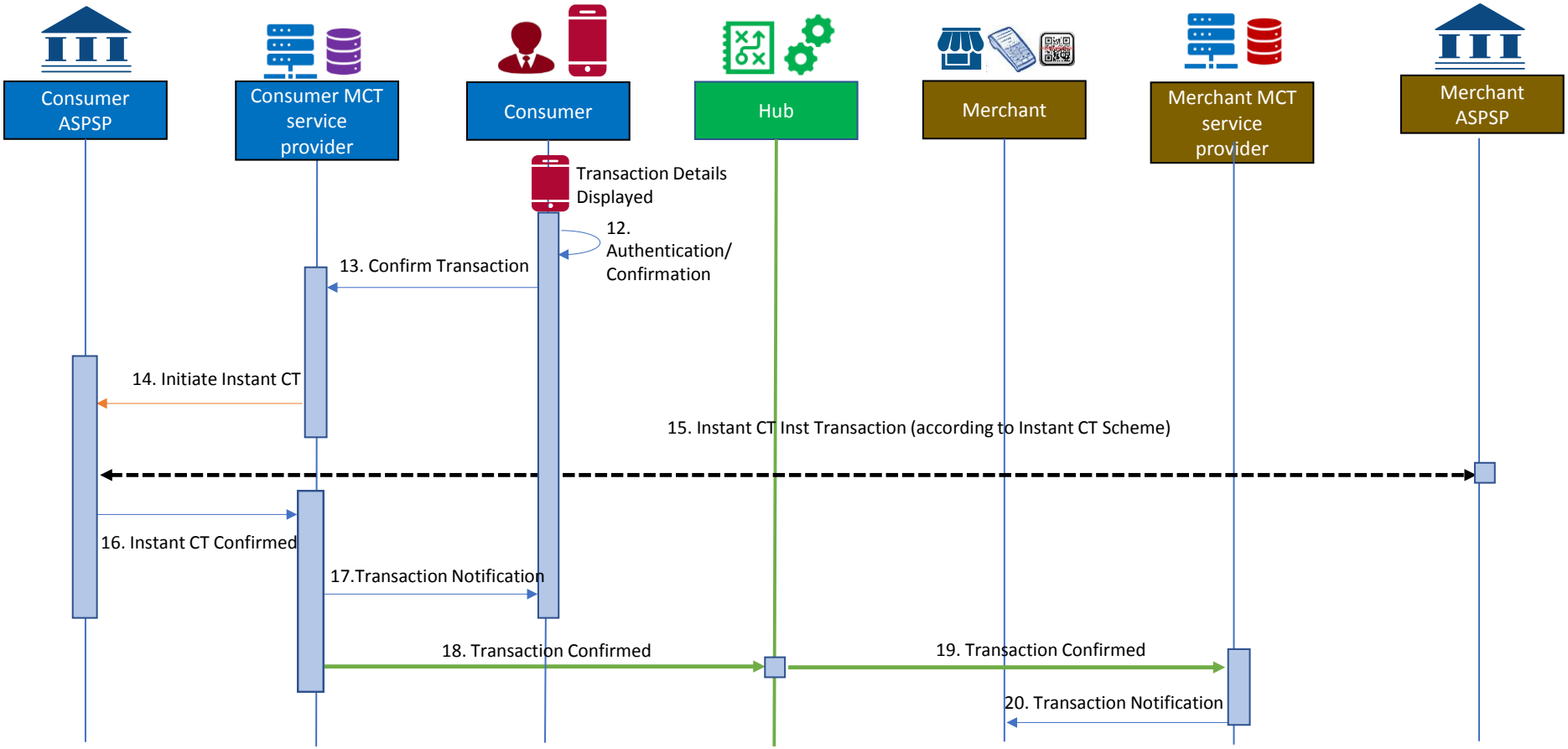


Figure 3 — Process flow – Merchant-presented QR-code with token

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 MCT service provider[4].

Step 2:

The merchant's MCT service provider returns a QR-code including a unique token based on the transaction details (transaction amount, name/trade name merchant, PA-ID merchant, ASPSP-ID, transaction identifier) and their MCT service provider identifier to the merchant.[5]

Step 3:

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

Step 4:

The consumer opens their MCT payment application and scans the QR-code.

Step 5:

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

Step 6:

The consumer's MCT 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 MCT service provider identifier is sent to the hub.

Step 8:

The hub identifies the merchant's MCT service provider and forwards them the Transaction Information request.

Step 9:

The merchant's MCT service provider checks the request, prepares the response and sends the Transaction Information Response to the hub.

[4] Alternatively, the merchant POI infrastructure may generate the QR-code.
[5] As an alternative, the MCT service provider could also return the token to the merchant and their POI generates the QR-code.

Step 10:

The hub forwards the Transaction Information Response to the consumer's MCT service provider.

Step 11:

The consumer's MCT service provider retrieves the transaction details from the Transaction Information Response and sends them to the consumer.

Step 12:

The consumer consents to the transaction based on the details displayed and performs an authentication[6] and confirmation of the transaction.

Step 13:

The confirmation including, where relevant, the authentication response is provided to the consumer's MCT service provider.

Step 14:

The consumer's MCT service provider sends an instant CT Inst instruction to the consumer's ASPSP including the transaction details.

Step 15:

The consumer's ASPSP sends the instant CT transaction to the merchant's ASPSP and the transaction flow is handled according to the underlying instant CT scheme.

Step 16:

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

Step 17:

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

Step 18:

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

[6] The consumer authentication may be performed by the consumer's MCT service provider or by their ASPSP. This may involve additional steps which are not illustrated in this process flow since they do not impact the interoperability. Here it is assumed that the consumer's MCT service provider has received delegation from the consumer's ASPSP for the consumer authentication subject to appropriate agreements.

Step 19:

The hub forwards the transaction notification message to the merchant's MCT service provider.

Step 20:

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

B.3 Process flow for consumer-presented QR-code containing a token

The detailed process flows between the different actors involved in this MCT transaction are shown in the next figure. Hereby the token contained in the consumer-presented QR-code is sent by the merchant MCT service provider to the consumer MCT service provider (over the hub) in the Payment Request message, with the merchant and transaction data, to retrieve the consumer identification data to enable the initiation of the MCT. Note that it is hereby assumed that the consumer MCT service provider fulfils the role of Token Service Provider for the consumer. The consumer MCT service provider ID (retrieved from the consumer-presented QR-code and contained in the Payment Request) is used by the hub to route the Payment Request message to the consumer MCT service provider.

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

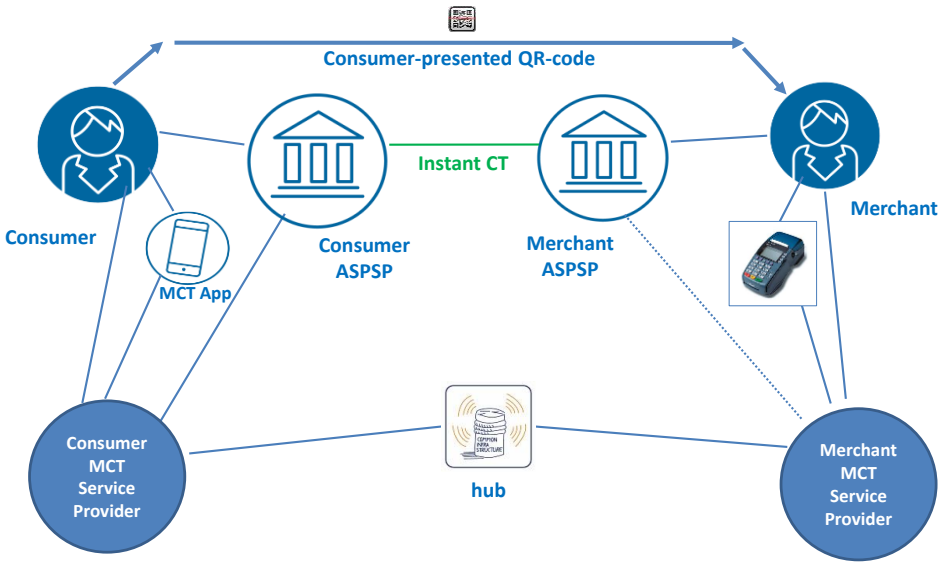
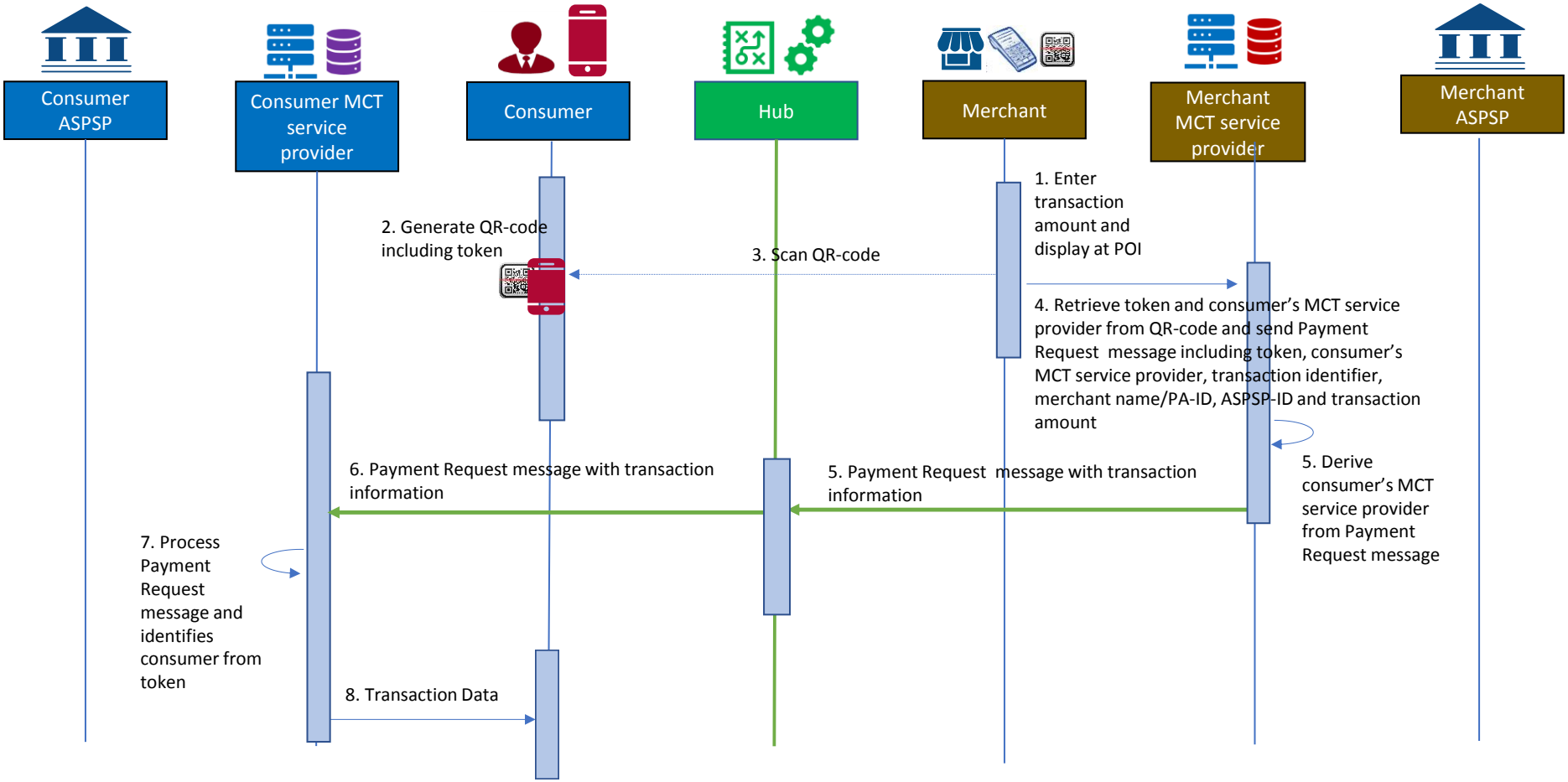


Figure 4 — Actors for MCT with consumer-presented QR-code

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



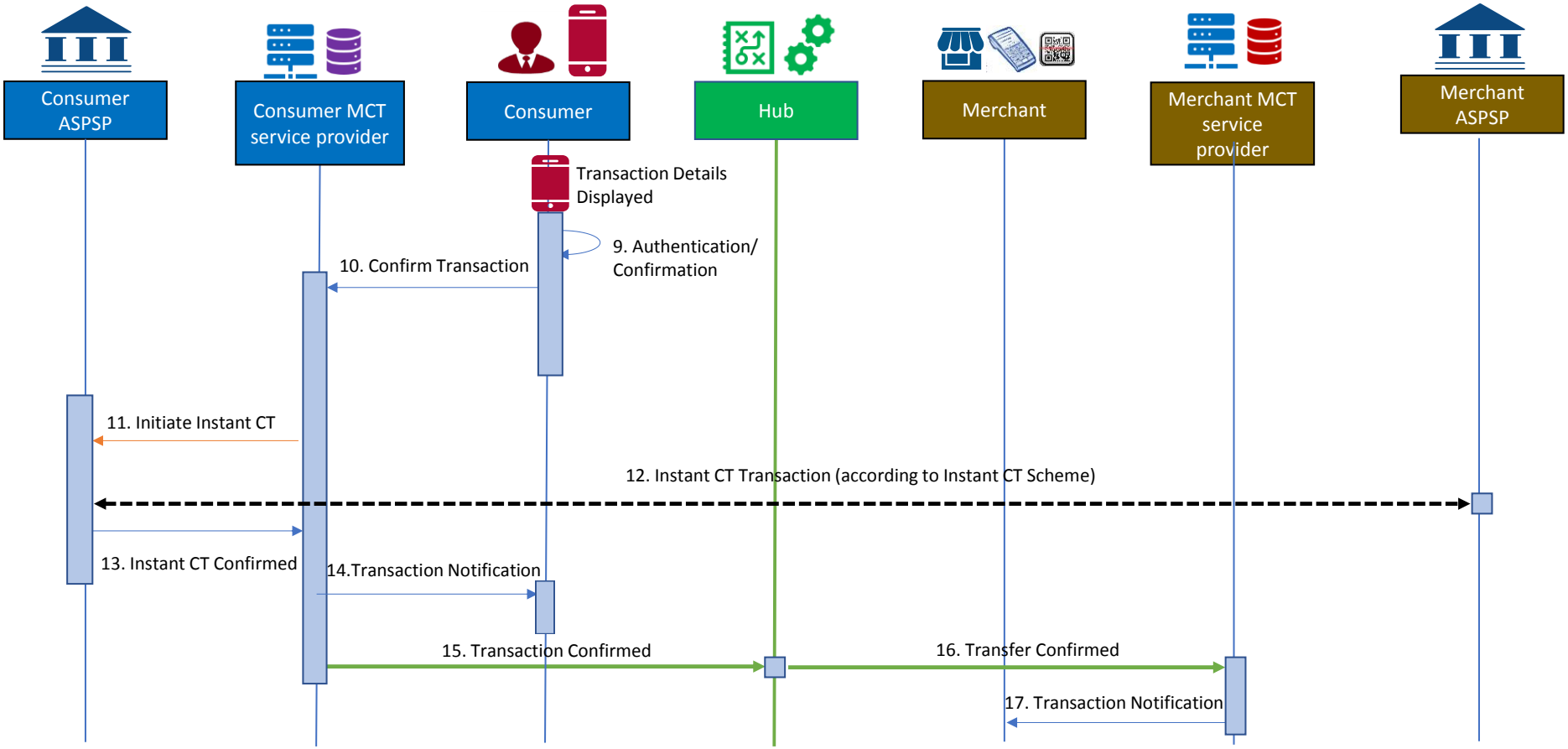


Figure 5 — Process flow - Consumer-presented QR-code with token

In the figure above the following steps are involved:

Step 1:

The merchant enters the transaction amount which is displayed on the POI[7].

Step 2:

- The consumer selects and opens the MCT payment application on their mobile device which possibly involves the entry of a password.
- A QR-code containing a consumer token and their MCT service provider identifier is generated by the MCT payment 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 MCT service provider identifier from the QR-code and sends a Payment Request message to their MCT service provider, including the merchant's name, PA-ID of the merchant[8], the merchant's ASPSP-ID, the merchant transaction identifier, the transaction amount, the consumer's MCT service provider identifier and the consumer token.

Step 5:

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

Step 6:

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

Step 7:

The consumer's MCT service provider checks the Payment Request message, retrieves the transaction data and the consumer's name and possibly their PA-ID and ASPSP-ID from the consumer token.

Step 8:

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

[7] The display of the transaction amount by the POI may happen after step 3, since the consumer identification might have an impact on the final transaction amount (e.g., due to discounts).
[8] Instead of the PA-ID merchant and the merchant ASPSP-ID, a proxy may be used.

Step 9:

The consumer consents to the transaction based on the details displayed and performs an authentication[9].

Step 10:

The confirmation including, where relevant, the authentication response is provided to the consumer's MCT service provider.

Step 11:

The consumer's MCT service provider sends an (instant) CT instruction to the consumer's ASPSP including the transaction details.

Step 12:

The consumer's ASPSP sends the instant CT transaction to the merchant's ASPSP and the transaction flow is handled according to the underlying instant CT scheme.

Step 13:

The consumer's ASPSP sends a confirmation message to the consumer's MCT service provider about the execution of the instant CT Instant transaction.

Step 14:

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

Step 15:

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

Step 16:

The hub forwards the transaction notification message to the merchant's MCT service provider.

Step 17:

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

[9] The consumer authentication may be performed by the consumer's MCT service provider or by their ASPSP. This may involve additional steps which are not illustrated in this process flow since they do not impact the interoperability. Here it is assumed that the consumer's MCT service provider has received delegation from the consumer's ASPSP for the consumer authentication subject to appropriate agreements.

Bibliography

[1] EPC269-19v2.0, *Mobile Initiated SEPA (Instant) Credit Transfer Payments and Technical Interoperability Guidance (*www.epc-cep.eu)

[2] EPC024-22v1.0, *Standardisation of QR-codes for MSCTs* (www.epc-cep.eu)

[3] ISO 9362, *Banking - Banking telecommunication messages - Business identifier code (BIC)*

[4] ISO 12812, *Core banking - Mobile financial services - Parts 1-5*

[5] ISO 13616, *Financial services - International Bank account number (IBAN) - Part 1: Structure of the IBAN*

[6] ISO 23195: *Security objectives of information systems of third-party payment services*

[7] ISO DIS 5201, *Financial services – Code scanning payment security*