European Payments Council

Standardisation of QR-codes for Mobile Initiated SEPA (Instant) Credit Transfers

EPC024-22 Version 2.0 / Date issued:10 January 2023

Public

Table of Contents

List of tables

List of figures

Executive Summary

The ERPB invited the EPC in their Statement (ERPB/2021/012), published in June 2021, to coordinate further work on the standardisation and governance of QR-codes for Instant Payments at the Point of Interaction (IPs at the POI), beyond what had already been set out in the report of the ERPB working group on an *Interoperability Framework for IPs at the POI* of November 2020 (see ERPB/2020/026 [14]), hereby involving relevant stakeholders and standardisation bodies. Hereby an IP at POI is an instant payment transaction based on a SEPA Instant Credit Transfer (SCT Inst)[1], by a consumer to a merchant at the POI which may be for example a Point-of-Sale (POS) in a store or a payment page on an e-or m-commerce website.

Subsequently, the EPC requested the Multi-stakeholder Group on Mobile Initiated SEPA (Instant) Credit Transfers (MSG MSCT – see Annex 3) to execute this work. The MSG MSCT developed a dedicated document, including a few recommendations on the next steps towards interoperability of QR-codes, which was endorsed by the ERPB in their meeting on 25 November 2021 (see EPC212-21 [12] and [15]). For the development of this document on the *Standardisation and governance of QR-codes for IPs at the POI*, the MSG MSCT leveraged next to ERPB/2020/026 (see [14]), their work undertaken over the past months which is reflected in the MSCT IG (EPC269-19 [9]), but took also into account the recently received answers from the EBA on Q&A 2020_5476, 2020_5477, and 2021_6298 regarding the content of the QR-code.

The present document developed by the MSG MSCT addresses Recommendation A (see [15]) and builds further on the document mentioned above. It generalises the QR-code standard for IPs at the POI to all types of MSCTs, covering all payment contexts P2P, C2B, B2B and B2C, while addressing both SCT instant and SCT payments. In addition, the document contains a section devoted to the security of the data contained in the QR-codes which is based on Chapter 10 of the MSCT IG [9].

By developing this document, the MSG MSCT aims at contributing to the interoperability of MSCTs and the further market take-up of this means of payment.

In order to help developing a successful MSCT ecosystem that provides value for all, it is very important to gather industry opinion and market feedback regarding this QR-code standard for MSCTs. Therefore an 8-week public consultation was held before this final version of the document was developed. Furthermore, a general version of this document on the *Specification of QR-codes for mobile (instant) credit transfers* (EPC193-22) has been submitted for international standardisation to ISO TC 68 SC 9 - Financial services – Information exchange for financial services, through a so-called fast track procedure.

[1] Note however that the content of this document remains valid for any (instant) account-based payment.

1 Document information

1.1 Structure of the document

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

Executive Summary;
Chapter 1 includes the document information;
Chapter 2 provides an introduction to the document;
Chapter 3 briefly discusses the interoperability model for MSCTs;
Chapter 4 specifies the standard for QR-code formats for MSCTs;
Chapter 5 discusses the security aspects of QR-codes for MSCTs;
Chapter 6 provides the conclusions;
Annex 1 contains some examples of MSCT interoperability process flows for illustrative purposes;
Annex 2 describes the interoperability with some other QR-code initiatives for mobile payments;
Annex 3 lists the participants to the MSG MSCT Plenary;
Annex 4 lists the participants to the work-stream on technical interoperability of QR-codes.

1.2 References

N°	Title	Issued by
[1]	EBA/GL/2019/04: EBA Guidelines on ICT and security risk management	EBA
[2]	PSD2: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC	EC
[3]	Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (also referred to as "RTS")	EC
[4]	General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC	EC
[5]	eIDAS: Regulation (EU) No 910/2014 of the European parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	EC
[6]	EPC125-05: SEPA Credit Transfer Scheme Rulebook	EPC

[7]	EPC069-12v2.1: Quick Response Code - Guidelines to enable data capture for the initiation of a SEPA credit transfer	EPC
[8]	EPC004-16: SEPA Instant Credit Transfer Scheme Rulebook	EPC
[9]	EPC269-19v2.0 (2nd release): Mobile Initiated SEPA (Instant) Credit Transfer Payments and Technical Interoperability Guidance (MSCT IG)	EPC
[10]	EPC193-21v1.0: 2021 Payment Threats and Fraud Trends Report	EPC
[11]	EPC014-20: SEPA Request-to-Pay (SRTP) Scheme Rulebook	EPC
[12]	EPC212-21v1.1: Standardisation and governance of QR-codes for IPs at the POI (= ERPB/2021/017)	EPC
[13]	EC193-22v1.1: Specification of QR-codes for mobile (instant) credit transfers (in ISO format)	EPC
[14]	ERPB/2020/026: ERPB Final report on an Interoperability Framework for Instant Payments at the POI (IPs at the POI)	ERPB
[15]	ERPB/2021/028: Statement following the sixteenth meeting of the ERPB held on 25 November 2021	ERPB
[16]	ISO 12812: Core banking - Mobile financial services - Parts 1-5	ISO
[17]	ISO 13616: Financial services - International Bank account number (IBAN) -- Part 1: Structure of the IBAN	ISO
[18]	ISO 18092: Information technology - Telecommunications and information exchange between systems -- Near Field Communication - Interface and Protocol (NFCIP-1)	ISO
[19]	ISO 20022: Financial Services – Universal Financial Industry Message Scheme	ISO
[20]	ISO TC 68 / SC 2 WD 5201 : Financial services – Code scanning payment security – under development	ISO
[21]	ISO/IEC 18004: Information technology -- Automatic identification and data capture techniques -- QR-code bar code symbology specification	ISO
[22]	ISO/IEC 14443: Identification cards - Contactless integrated circuit(s) cards - Proximity cards – Parts 1-4	ISO
[23]	ISO/IEC 15417: Information technology — Automatic identification and data capture techniques — Code 128 bar code symbology specification	ISO
[24]	NFC Controller Interface (NCI) Specifications NFC Forum	NFC Forum

Table 1: Bibliography

1.3 Terminology

Term	Definition
Account Servicing Payment Service Provider (ASPSP)	A PSP providing and maintaining a payment account for a payer (see Article 4 in [2]) or a payee.
Alias	See Proxy
Beneficiary	See Payee.
Bluetooth Low Energy (BLE)	A wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications including beacons. Compared to classic Bluetooth, BLE is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range.
Collecting Payment Service Provider (CPSP)	A payment service provider according to PSD2 that collects the payment transactions on behalf of the merchant (the ultimate beneficiary) and as such is the beneficiary of the MSCT at POI transaction.
Consumer	A natural person who, in payment service contracts covered by the PSD2, is acting for purposes other than his or her trade, business or profession (see Article 4 in [2]).
Consumer Device	An internet capable device used by the consumer (payer) to conduct an (instant) payment. Examples include a mobile device or a personal computer (PC).
Consumer Device UVM (CDUVM)	A user verification method (UVM) entered by or captured from the consumer (payer) on the consumer device (e.g. a mobile device).
Consumer-presented data	Data provided by the consumer to the merchant's POI to enable the initiation of an MSCT.
Credit transfer	A payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the PSP which holds the payer's payment account, based on an instruction given by the payer (see (see Article 4 in [2]).
Credit Transfer instruction	A payment instruction given by an originator to an originator ASPSP requesting the execution of a credit transfer transaction, comprising such information as is necessary for the execution the credit transfer and is directly or indirectly initiated in accordance with the provisions of [2].
Credit Transfer Transaction	An instruction executed by an originator ASPSP by forwarding the transaction to a CSM for forwarding the transaction to the beneficiary ASPSP.
Customer	A payer or a payee (beneficiary) which may be either a consumer or a business (merchant).

CustomerID	In the context of this document, an identification of the payer (consumer), issued by their ASPSP for access to (a) customer facing user interface(s) (e.g. their on-line banking system), as required in the PSD2 API.
2D barcode	A two-dimensional barcode is a machine-readable optical label that contains digital information. They are also referred to as matrix barcodes. Examples include QR codes and tag barcodes.
Digital wallet	A service accessed through a consumer device which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications (e.g., value added services such as loyalty, couponing, etc.). A digital wallet is sometimes also referred to as an e-wallet.
Electronic identification	The process of using personal identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.
EMVCo	An LLC formed in 1999 by Europay International, MasterCard International and Visa International to enhance the EMV Integrated Circuit Card Specifications for Payments Systems. It manages, maintains, and enhances the EMV specifications jointly owned by the payment systems. It currently consists of American Express, Discover, JCB, MasterCard, Union Pay and VISA.
Funds	Cash, scriptural money or electronic money as defined in (see Article 4 in [2]).
HUB	An infrastructure ensuring connectivity between MSCT service providers. The term HUB is meant to be agnostic to the way it might be implemented – logically or physically - different models may be possible, but it should at least cover (a kind of) routing service. As an example, this could be a direct connection amongst MSCTP service providers through a dedicated API.
Instant(ly)	At once, without delay.
Instant Payment	Electronic retail payment solutions available 24/7/365 and resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee’s account with confirmation to the payer (within seconds of payment initiation) (see [8]).
International Bank Account Number (IBAN)	An internationally agreed system of identifying bank accounts across national borders to facilitate the communication and processing of cross border transactions (see [17]).
MSCT Payment (MSCT) Application	A set of modules (application software) and/or data (application data) needed to provide functionality for a Mobile initiated (instant) SEPA Credit Transfer (MSCT) as specified by the MSCT service provider in accordance with the SEPA (Instant) Credit Transfer scheme.

MSCT Service Provider	A service provider that offers or facilitates an MSCT service to a payer and/or payee based on an SCT Instant or SCT payment transaction. This may involve the provision of a dedicated MSCT application for download on the payer's or payee's device or the provision of dedicated software for the merchant POI. As an example, an MSCT service provider could be a PSP (e.g. an ASPSP or any party acting as a PISP under PSD2) or a technical service provider supporting a PSP.
Merchant	A beneficiary within a payment scheme for payment of the goods or services purchased by the consumer. The merchant is a customer of their PSP. A merchant may also be referred to as payee.
Merchant-presented data	Data provided by the merchant's POI to the consumer to enable the initiation of an MSCT.
Mobile code	An authentication credential used for user verification and entered by the consumer (payer) via the keyboard of the mobile device.
Mobile device	Personal device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth, etc. Examples of mobile devices include mobile phones, smart phones, tablets, wearables, car on-board units.
Mobile Network Operator (MNO)	A mobile phone operator that provides a range of mobile services, potentially including facilitation of NFC services. The MNO ensures connectivity Over the Air (OTA) between the consumer and their PSP using their own or leased network.
Mobile payment service	A payment service made available by software/hardware through a mobile device.
Mobile service	A service such as identification, payment, ticketing, loyalty, etc., made available through a mobile device.
Mobile wallet	A digital wallet accessed through a mobile device. This service may reside on a mobile device owned by the payer (i.e. the holder of the wallet) or may be remotely hosted on a secured server (or a combination thereof) or on a merchant website. Typically, the so-called mobile wallet issuer provides the wallet functionalities but the usage of the mobile wallet is under the control of the payer.
NFC (Near Field Communication)	A contactless protocol for mobile devices specified by the NFC Forum for multi-market usage. NFC Forum specifications (see [24]) are based on ISO/IEC 18092 [18] but have been extended for harmonisation with EMVCo and interoperability with ISO/IEC 14443 [22] .
Originator	See Payer.
Payee	A natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction (see Article 4 in [2]), (examples include merchant, business).

Payee-presented data	Data provided by the payee to the payer to enable the initiation of an MSCT.
Payee Reference Party	A person/entity on behalf of or in connection with whom the payee receives a payment.
Payer	A natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order (see Article 4 in [2]).
Payer-presented data	Data provided by the payer to the payee to enable the initiation of an MSCT.
Payload Issuer	The entity responsible for issuing the payload. This may be the MSCT service provider or a different entity (e.g., an acquirer), operating under this MSCT service provider.
Payment account	An account held in the name of one or more payment service users which is used for the execution of payment transactions (see Article 4 in [2]).
Payment Initiation Service Provider (PISP)	A payment service provider pursuing business activities as referred to in Annex I.7 of [2].
Payment Request	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. As an example, see [11].
Payment Request message	Message sent by the payee to the payer, directly or through agents. It is used to request the movement of funds from the payer account to the beneficiary account.
Payment Service Provider (PSP)	An entity referred to in Article 1(1) of [2] or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33 of [2].
Payment Service User (PSU)	A natural or legal person making use of a payment service in the capacity of payer, payee, or both (see Article 4 in [2]).
Payment scheme	A technical and commercial arrangement (often referred to as the “rules”) between parties in the payment value chain, which provides the organisational, legal and operational framework rules necessary to perform a payment transaction.

Payment system	A funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions (see Article 4 in [2]).
Payment transaction	An act, initiated by the payer or on his/her behalf or by the payee (beneficiary), of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee (see Article 4 in [2]).
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (see [4]).
Physical POI	A POI that is a physical device and consists of hardware and software, hosted in acceptance equipment to enable a consumer and/or merchant to perform an MCST. The merchant-controlled POI may be attended or unattended. Examples of POI include Point-of-Sale (POS), vending machine.
Point of Interaction (POI)	The initial point in the merchant's environment (e.g. POS, vending machine, payment page on merchant website, QR-code on a poster, etc.) where data is exchanged with a consumer device (e.g., mobile phone, wearable, etc.) or where consumer data is entered to initiate an instant credit transfer.
Proximity Payment	A payment where the payer and the payee (and/or their equipment) are in the same location and where the communication between the payer's device and the payee device/infrastructure takes place through a proximity technology (e.g., NFC, 2D barcodes, BLE, ultrasonic, etc.).
Proxy	Data required in order to retrieve a payment account identifier (e.g., mobile phone number, e-mail address, etc.). This is sometimes referred to as an "alias". As an example, a proxy could be used to replace an IBAN which will be referred to as IBAN-proxy in this document.
QR-code	Quick Response-code [21], see also 2D barcode.
SEPA Credit Transfer	The SEPA Credit Transfer is the payment instrument governed by the rules of the SEPA Credit Transfer Scheme for making credit transfer payments in euro throughout the SEPA from payment accounts to other payment accounts (see [8]).
SEPA Instant Credit Transfer	The SEPA Instant Credit Transfer is the payment instrument governed by the rules of the SEPA Instant Credit Transfer Scheme for making instant credit transfer payments in euro throughout the SEPA from payment accounts to other payment accounts (see [8]).

Single Euro Payments Area (SEPA)	The countries and territories which are part of the jurisdictional scope of the SEPA payment schemes (see https://www.europeanpaymentscouncil.eu/document-library/other/epc-list-sepa-scheme-countries).
Tokenisation	Process of substituting payment account, PSU identification data or transaction related data with a surrogate value, referred to as a token.
Token	Tokens can take on a variety of formats across the payments industry. They generally refer to a surrogate value for PSU identification and/or transaction data Payment Tokens must not have the same value as or conflict with the real payment account related data. If the token is included in the payee presented data it might be referred to as a payee token; if the token is included in the payer-presented data it might be referred to as a payer token.
Token Requestor	An entity requesting a token to the Token Service
Token Service	A system comprised of the key functions that facilitate generation and issuance of tokens and maintain the established mapping of tokens to the related data when requested by the token requestor. It may also include the capability to establish the token assurance level to indicate the confidence level of the payment token to the related information binding. The service also provides the capability to support token processing of payment transactions submitted using tokens by de-tokenising the token to obtain the actual related information (see also the definition of Token).
Token Service Provider (TSP)	An entity that provides a Token Service.
Trusted Third Party (TTP)	An entity which facilitates interactions between stakeholders of the ecosystem who all trust this third party (examples are SE provider, common infrastructure manager…).

Table 2: Terminology

1.4 Abbreviations

Abbreviation	Term
an	alphanumeric
ASPSP	Account Servicing PSP
API	Application Programming Interface
B2B	Business-to-Business
BLE	Bluetooth Low Energy
C2B	Consumer-to-Business
CDUVM	Consumer Device UVM

CEN	European Committee for Standardisation
CPSP	Collecting Payment Service Provider
CSM	Clearing and Settlement Mechanism
2D barcode	Two dimensional barcode
EBA	European Banking Authority
EC	European Commission
ECSG	European Cards Stakeholders Group
EPC	European Payments Council
EPI	European Payments Initiative
ERPB	Euro Retail Payments Board
GDPR	General Data Protection Regulation
IBAN	International Bank Account Number
ID	Identifier
IP	Instant Payment
ISO	International Organization for Standardization
MNO	Mobile Network Operator
MSCT	Mobile Initiated (Instant) SCT
MSCT IG	Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance
MSG MSCT	Multi-Stakeholder Group for Mobile Initiated (Instant) SCT
n	numeric
NFC	Near-Field Communication
P2P	Person-to-Person
PISP	Payment Initiation Service Provider
POI	Point of Interaction
POS	Point of Sale
PSD	Payment Services Directive
PSP	Payment Service Provider
PSU	Payment Service User
QR-code	Quick Response-code
RTS	Regulatory Technical Standard
SC	Sub-Committee

SCT Inst	SEPA Instant Credit Transfer
SEPA	Single Euro Payments Area
SP	Service Provider
TC	Technical Committee
TSP	Token Service Provider
TTP	Trusted Third Party
URL	Uniform Resource Locator
UVM	User Verification Method

Table 3: Abbreviations

2 Introduction

This document has been developed by the Multi-stakeholder Group on Mobile Initiated SEPA (Instant) Credit Transfers (MSG MSCT) to address Recommendation A included in the ERPB Statement published in November 2021 (see [15]).

For the development of this document the MSG MSCT leveraged the document on *Standardisation and governance of QR-codes for IPs at the POI* (EPC212-21v1.1, see [12]) and the work undertaken over the past months which is reflected in the *MSCT Payments and Interoperability Guidance* (MSCT IG - EPC269-19 [9]), while taking into account the recently received answers from the EBA on Q&A 2020_5476[2], 2020_5477[3] and 2021_6298[4] regarding the content of the QR-code.

The MSG MSCT (see Annex 3) has extended their work-stream on technical interoperability of MSCTs to conduct the work on the QR-codes with additional members from relevant stakeholders and (industry) standardisation bodies. The composition of this extended work-stream may be found in Annex 4.

The EPC developed in 2012 a document *QR-code - Guidelines to enable data capture for the initiation of a SEPA credit transfer* [7], whereby all data elements reside in clear text in the QR-code. In 2018, the MSG MSCT originally based their specification of a QR-code for MSCTs on a similar format as defined in [7]. However, through the public consultation on the first draft edition of the MSCT IG [9], the market rejected this approach and requested the specification of a URL-based QR-code to offer maximum flexibility. The URL-based QR-code was also adopted in the document QR-codes for IPs at the POI, developed by the dedicated ERPB working group in 2021 [12]. The present document generalises the QR-code standard for IPs at the POI (see Chapter 4 in [12]) to all types of MSCTs, i.e. all payment contexts P2P, C2B, B2B and B2B while addressing both SCT instant and SCT payments. In addition, the document contains a section devoted to the security of the data contained in the QR-codes which is based on Chapter 10 of the MSCT IG [9].

The document also provides a suggestion for further international standardisation of the QR-code and briefly describes in Annex 2 the interoperability of the QR-code standard specified in this document with, amongst possible others, the QR-codes defined by Alipay, EMPSA, EMVCo and EPI.

In order to help developing a successful MSCT ecosystem that provides value for all, it is very important to gather industry opinion and market feedback regarding this QR-code standard for MSCTs. Therefore an 8-week public consultation was held before this final version of the document was developed. The document will also be fully integrated into the third release of the MSCT IG (EPC269-19, [9]).

Furthermore, a general version of this document on the *Specification of QR-codes for mobile (instant) credit transfers* (EPC193-22) has been submitted for international standardisation to ISO TC 68 SC 9 - Financial services – Information exchange for financial services, through a so-called fast track procedure.

[2] See https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5476.

[3] See https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5477.

[4] See https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6298.

3 Interoperability of MSCTs

MSCTs are initiated directly (by the payer) or indirectly (by an MSCT service provider at the request of the payer) in compliance with the PSD2 (see [8]), using a mobile device. MSCT solutions are offered by so-called MSCT service providers which are service providers that offer or facilitate a payment service to a payer/payee based on an SCT Instant or an SCT transaction. As an example, an MSCT service provider could be a PSP (e.g. an ASPSP or any party acting as a PISP under PSD2) or a technical service provider supporting a PSP.

MSCTs in Euro are based on the existing SCT Instant scheme or SCT Scheme rulebooks (see [8] and [6] resp.) in the so-called "inter-PSP space" and are therefore using in that space the existing payment infrastructure. They typically use an MSCT application or a browser on the consumer (payer) device to initiate or at least authenticate and authorise the SCT (Instant) transaction, besides some features of the payer device such as the support of CDUVM (e.g., a mobile code or biometrics on the mobile device), the mobile device screen to display transaction information, etc.

For the analysis of the technical interoperability of MSCTs, the following generic 4-corner model was used in the MSCT IG [9]. Hereby it is assumed that both payer and payee have different ASPSPs that are SCT Inst or SCT scheme participants (see Chapter 4 in [9]), while the entities assuming the role of MSCT service provider are depicted as separate entities that are different for the payer and the payee. Obviously, if the role of MSCT service provider would be assumed by an ASPSP the model below would simplify. Alternatively, multiple PSPs (such as a PISP licensed under PSD2 or a CPSP) could be involved between the payer/payee and their respective ASPSP; this models have been studied in Chapter 20 in the MSCT IG [9].

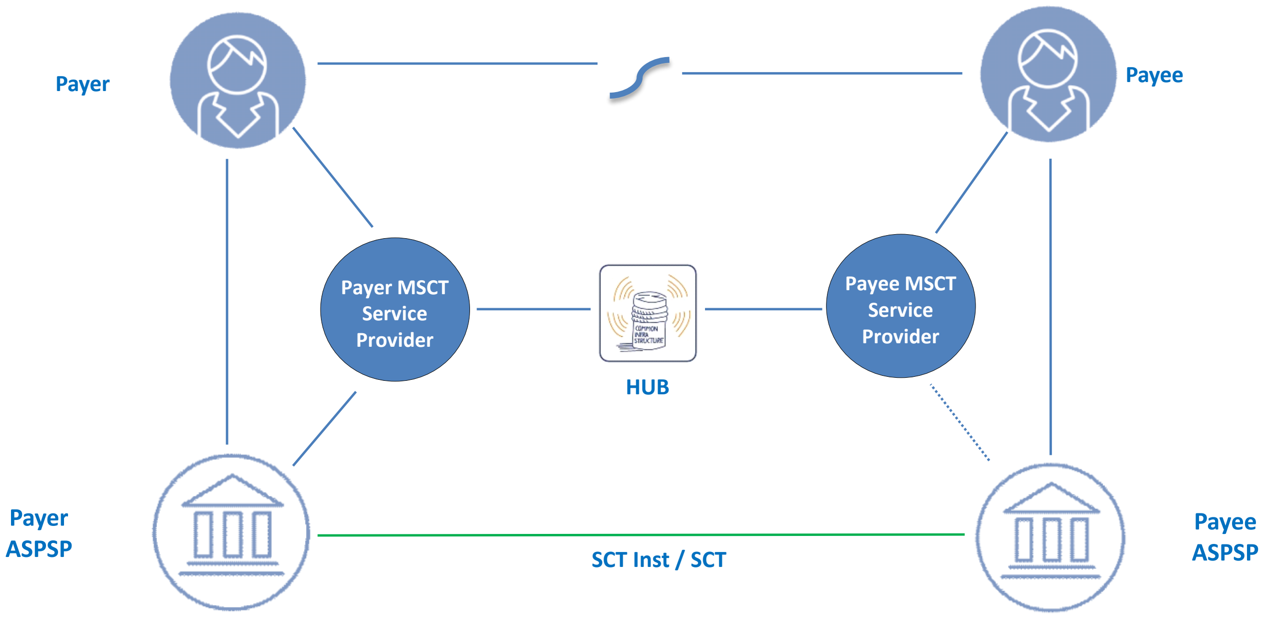


Figure 1: Generic 4-corner interoperability model for MSCTs

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

The MSCT ecosystem involves some other new stakeholders in the value chain compared to the ones described in the SCT Inst or SCT scheme rulebooks (see [8] and [6] resp.) including a so-called Token Service Provider (TSP) who is a TTP involved if tokens are used in MSCTs as surrogate values for the transaction data (including the payee/payer IBAN, payee/payer identifier, 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 MSCT service provider (and hence the TSP is not depicted in the figure above)[5].

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

The technical interoperability requirements between MSCT service providers have been analysed and defined in detail in Chapters 16 through 20 in the MSCT IG [9]. One of the interoperability aspects is the exchange of (transaction) data between the payer and the payee to enable the initiation of an MSCT. The usage of QR-codes for this data exchange will be treated in the next chapter.

[5] The same is valid in case of usage of a proxy. The role of the provider involved is assumed or is under the control of the IP service provider.

4 Standard for QR-codes for MSCTs

4.1 Introduction

This chapter is devoted to MSCTs whereby a QR-code (see ISO 18004, [21]) is used as proximity technology for the data exchange between the payer and the payee to enable the initiation of an MSCT. Hereby, as defined in the MSCT IG [9], two modes may be distinguished:

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

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

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 MSCT service provider. This generally requires the support of the payee's MSCT service provider (see Information Request/Response messages in Figure 4 in Annex 1) prior to the initiation of the MSCT transaction.
- The payee-presented data contains a "proxy" for the payee identification data. In this case the data that is not in clear, but corresponds to the proxy, needs to be provided by the payee's MSCT service provider upon request from the payer's MSCT service provider (see Information Request/Response messages in Figure 4 in Annex 1) prior to the initiation of the MSCT transaction.
- The payee-presented data includes all data in "clear" (e.g. the payee's name, trade name, IBAN of the payee's account, transaction amount, etc.). This enables the immediate initiation of the MSCT transaction.

Next to this data exchanges also an *identifier of the payee MSCT service provider* is needed for routing purposes by the HUB for the exchange of messages between the respective MSCT service providers. For interoperability, the payee MSCT service providers should support at least one of the options specified above while the payer's MSCT service provider should be able to support all types. Further interoperability requirements are specified in the MSCT IG [9].

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 Chapter 5).

Minimum data sets

The minimum data set to be exchanged between the payee and the payer, will rely on the MSCT 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 MSCT service provider to the payee's MSCT service provider for de-tokenisation into the transaction data (see Annex 1).
2 If the payee-presented data provided to the payer contains only part of the transaction data in clear (e.g., contains a proxy), the transaction data will need to be further completed by the payee's MSCT service provider. The minimum data set will consist of both routing info and the available transaction data (e.g. the proxy). The minimum data will be forwarded in a Transaction Information Request message through the HUB from the payer's MSCT service provider to the payee's MSCT service provider for completion of the transaction data.
3 If the payee-presented data provided to the payer contains all transaction data "in clear" (e.g. in clear in QR-code), the minimum data set will consist of both routing info and all necessary payload data.

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

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

Table 4: Minimum data sets for MSCTs based on payee-presented QR-code

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 MSCT schemes through a single QR-code having multiple payloads.

The reader is referred to section 4.4 for an explanation of the "Version" and "Type" in the Table above.

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

Introduction

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

The *payer identification data* is defined by the MSCT service provider and may take a variety of forms and may be static or dynamic. However, this payer identification data has no impact on the interoperability between MSCT services. This payer identification data will need to be transferred as part of the Payment Request message from the payee to their MSCT service provider and further to the payer's MSCT service provider to enable the identification of the payer (see Figure 6 in Annex 1).

In the ERPB report ERPB/2020/026 [14], originally three cases were distinguished with respect to the consumer (payer) identification data. In view of the answer received from the EBA on Q&A 2020_5476[6] and 2021_6298[7] the options containing the CustomerID in "clear" are not allowed[8] Therefore, this document considers only one case, namely the payer identification data is a (payer) token. But the minimum data set could also include an additional clear-text value string to support value-added services (e.g. loyalty).

An *identifier of the payer's MSCT service provider* is needed by the payee's MSCT service provider and subsequently by the HUB to know where to route the Payment Request message.

Minimum data set

The minimum data set to be exchanged between the payer and the payee included in the payer-presented QR-code is as follows:

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

Table 5: Minimum data sets for MSCTs based on payer-presented QR-code

The reader is referred to section 4.4 for an explanation of the "Version" and "Type" in the Table above.

[6] See https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5476.

[7] See https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6298.

[8] ETPPA tabled a dissenting opinion on the impact of the EBA answer. In their view the EBA answer does not allow the removal of these options, because a) any non-PSP – including payers themselves – should still be allowed to provide the CustomerID in clear-text, b) PIS@POS could not work without, because PSD2 APIs require the CustomerID in clear-text as well, and c) tokenisation can never be mandated, because the introduction of a tokeniser brings an unnecessary gatekeeper into the process, which adds cost, complexity and competition issues.

4.4 Standardised format of QR-codes for MSCTs

Introduction

To enable MSCT interoperability across SEPA, for the data exchange between the payee and the payer, MSCT QR-codes formats have been standardised in the MSCT IG [9] and in EPC212-21v1.1 [12] based on the minimum data sets defined in the previous section.

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

The standardised payer-presented QR-codes should be adopted by all MSCT service providers and supported by the payee's equipment (e.g. merchant's POI or payee's mobile device).

Assumptions for the development of QR-codes for MSCTs

For the development of a standardised QR-code for MSCTs, based on ISO /IEC 18004 [21], the following four assumptions have been 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 MSCTs 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 MSCTs for data exchange between the payee and the payer has been 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 MSCT 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.

QR-codes for MSCTs

The QR-codes format for MSCTs have been specified in the MSCT IG [9] and in EPC212-21 v1.1 [12] and are URL based with a recognisable structure.

The structure of the QR-code for MSCTs has been 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[9]

/HTTPS://<Domain name>/<Version>/<Type>/<Payee MSCT service provider ID>/<Payload>

Table 6: Payee-presented QR-code

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

Table 7: Payer-presented QR-code

The **Domain name** refers to an MSCT 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[10].

The **MSCT service provider identifier i**s used in the interoperability space for routing purposes, therefore a standardised coding of this data element is necessary (see section 4.5).

The Payload is at the discretion of the Payload issuer who may be the MSCT service provider or a different entity, operating under this MSCT service provider. It shall contain the minimum data for the Payload as defined in sections 4.2 and 4.3. 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 MSCT service provider, this MSCT service provider is responsible for the identification of the Payload issuers.

4.5 Coding of the QR-code data fields

In view of the interoperability of QR-codes for MSCTs, 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

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

[10] An example may be a refund.

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).

Domain_name

The domain name refers to the interoperability domain for MSCT service providers for MSCTs and shall refer to an "*MSCT interoperability framework*" or "an MSCT scheme or participant" operated under the MSCT interoperability framework. The exact coding of this field needs to be defined by an MSCT Interoperability Framework, once established, 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 MSCT Interoperability Framework could support the above as well as domestically existing QR-codes of the Interoperability Framework members and potential interoperability with other QR-code standards.

Version

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

/1/ refers to the first version.

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.

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.

MSCT service provider ID

An identifier needs to be assigned to every MSCT service provider for routing purposes. This will require an eligibility checking and registration of the MSCT service provider under a so-called "MSCT interoperability framework".

The "to be defined" MSCT Interoperability Framework will be responsible for the issuance of the MCT service provider ID.

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

Payload

In the tables below, the Payload data for the three cases defined in section 4.2.2 for payee-presented QR-codes and for the unique case defined in section 4.3.2 for payer-presented QR-codes are listed. Standard URL query parameters should be used to delimit the payload information, such as "?" as starting parameter and "&" as delimiter of information.[11] Furthermore, the tables indicate whether a data element in the Payload is mandatory (M) or optional (O), in compliance to Annex 5 of the MSCT IG [9].

Payload for payee-presented QR-codes for MSCTs			
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[12]	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
	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

[11] Further implementation guidelines on the coding of the information included in the Payload will be covered under a to be defined "Interoperability Framework for MSCTs".

[12] 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.

	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

Table 8: Coding of payload data for payee-presented QR-codes for MSCTs

Payload for payer-presented QR-codes for MSCTs			
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

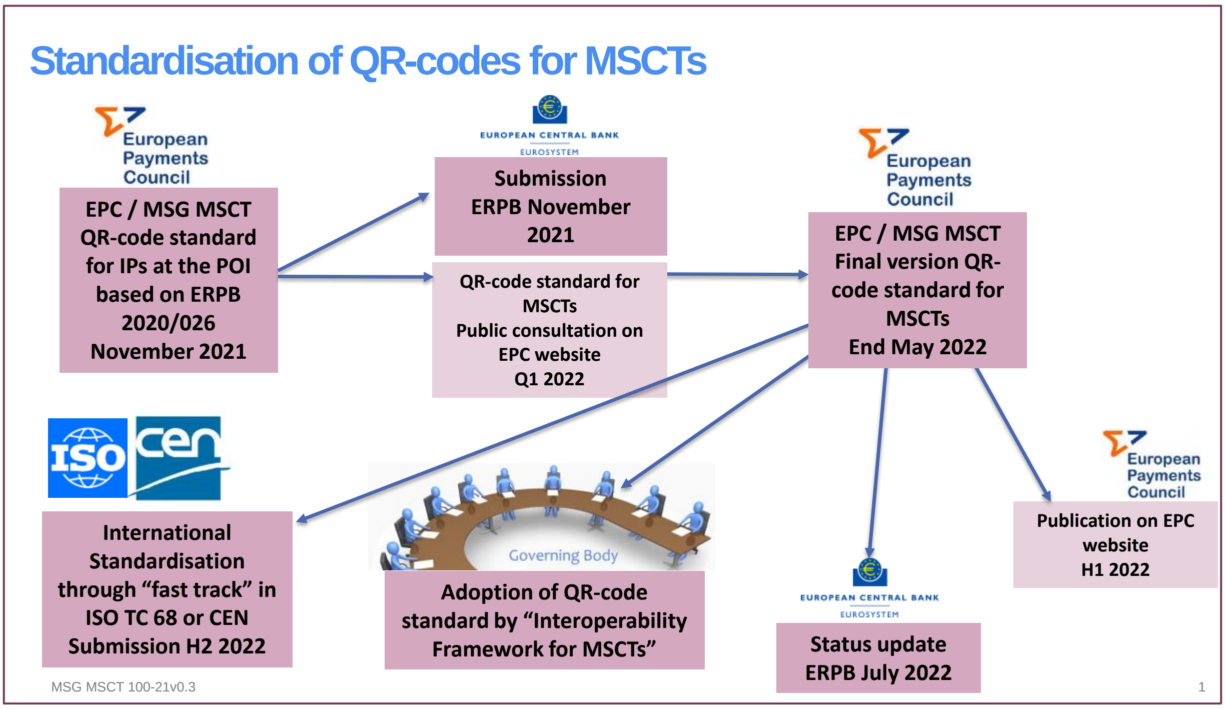
Table 9: Coding of payload data for payer-presented QR-codes for MSCTs

4.6 International standardisation of QR-codes for MSCTs

It would be beneficial in view of a wide usage and market adoption of QR-codes for (instant) credit transfers, if a generic version of this document becomes an International Standard, through the submission to an International Standards Body such as ISO TC 68 – Financial services or CEN.

Both standardisation organisations have a so-called "fast track procedure" which enables a quicker standardisation process. Note also that ISO TC 68 / SC 2 is already developing a standard on *"Code-scanning payment security"* [20] which includes the usage of QR-codes for payments and has currently established a study group in SC 8 on "*Digital wallet identification*".

An overview of the different milestones in the proposed process for the standardisation of QR-codes for MSCTs is shown in the figure below.



Standardisation of QR-codes for MSCTs

EPC / MSG MSCT QR-code standard for IPs at the POI based on ERPB 2020/026 November 2021

Submission ERPB November 2021

QR-code standard for MSCTs Public consultation on EPC website Q1 2022

EPC / MSG MSCT Final version QR-code standard for MSCTs End May 2022

International Standardisation through "fast track" in ISO TC 68 or CEN Submission H2 2022

Adoption of QR-code standard by "Interoperability Framework for MSCTs"

Status update ERPB July 2022

Publication on EPC website H1 2022

MSG MSCT 100-21v0.3

1

Figure 2: Standardisation process for QR-codes for MSCTs

5 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 MSCT 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 MSCT 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 MSCTs.

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).

Based on Art. 4(32) of PSD2 [2], "*the IBAN is not considered to be sensitive payment data and can therefore be included in clear-text in a payee-presented QR-code for the initiation of a transaction at the POI. However, since its disclosure may be used to carry out fraud, it will be for PSPs to assess the risks arising from transmitting the IBAN in clear-text between the POI and the payer's mobile device. Subsequently, PSPs should decide whether it is necessary to implement corresponding security measures to mitigate these risks*"[13].

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

[13] See the EBA answer to question EBA Q&A 2020_5477.

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 MSCT application on the payer's mobile device must enforce a properly encrypted and authenticated connection to the payer's MSCT service provider (as already specified in the MSCT IG - Chapter 9, [9]).

Payer-presented QR-codes

If Customer IDs, IBANs and proxies would be present "in clear" in a payer-presented QR-code, it is recommended to have integrity protection of these data to avoid mistakes with the initiation of transactions (e.g. using the wrong payer).

Moreover, the CustomerID might be a payer credential (e.g. for access to the online banking system). The capture of the CustomerID and IBAN could lead to impersonation attacks and initiation of fraudulent transactions (see for example [10], [20]) and reputational damage while also contaminating other payment instruments such as SDD. Based on the EBA answer to EBA Q&A 5476 that states *"the Customer ID cannot be included in a clear-text in a payer-presented QR-code for the initiation of credit transfers at the point of interaction without any security measures (e.g. encryption, tokenisation, transport layer security) ensuring its confidentiality during the QR-code life-cycle*", and the further clarification given on the generation of the QR-codes in EBA Q&A 2021_6298, the MSG MSCT concluded that CustomerID in "clear" is not allowed in the payer-presented QR-code.

Based on Art. 4(32) of PSD2 [2], the IBAN is not considered to be sensitive payment data and can therefore be included in clear-text in a payer-presented QR-code for the initiation of a transaction at the POI. However, since its disclosure may be used to carry out fraud, it will be for PSPs to assess the risks arising from transmitting the IBAN in clear-text free text between the POI and the payer's mobile device. Subsequently, PSPs should decide whether it is necessary to implement corresponding security measures to mitigate these risks[14].

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

If the payer-presented QR-code is static (e.g., a static token) the same risk as described above applies, namely it could lead to impersonation attacks and initiation of fraudulent transactions (see for example [10], [20]) and reputational damage.

[14] See also the EBA answer to question EBA Q&A 2020_5477.

In view of the considerations made above, 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.

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

For both modes, appropriate security measures should 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 currently being undertaken within ISO TC 68 / SC 2 for the development of a dedicated standard on *Code scanning payment security* [20]. Most of the security requirements and guidelines in this standard under development are also applicable to QR-codes for MSCT such as:

- The MSCT app 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 MSCT app).

6 Conclusions

This document specifies a QR-code standard for MSCTs[15], hereby covering two modes: payee-presented QR-codes and payer-presented QR-codes, to contribute to the interoperability of such means of payments. The standard is based on ERPB 2021/017 [12] and the MSCT IG [9] and takes into account the EBA answers on Q&A 2020_5476[16] , 2020_5477[17] and 2021_6298[18].

The document also contains a dedicated chapter on some security aspects related to the data contained in QR-codes used to initiate MSCTs.

Note that it is proposed that the governance aspects related to the usage of QR-codes should become part of the overall Governance of an "Interoperability Framework for MSCTs". The latter also involves the establishment of a directory for the registration of the MSCT service providers and the issuance of MSCT service provider identifiers.

In order to help developing a successful MSCT ecosystem that provides value for all, it is very important to gather industry opinion and market feedback regarding this QR-code standard for MSCTs. Therefore an 8-week public consultation was held before this final version of the document was developed. Furthermore, a general version of this document on the *Specification of QR-codes for mobile (instant) credit transfers* (EPC193-22) has been submitted for international standardisation to ISO TC 68 SC 9 - Financial services – Information exchange for financial services, through a so-called fast track procedure.

[15] Note however that the content of this document remains valid for any (instant) account-based payment.

[16] See https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5476.

[17] See https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5477.

[18] See https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6298.

Annex 1: Examples of interoperability process flows

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

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

which have been described in detail in the MSCT IG [9] and in the report ERPB/2020/026 [14].

These two examples are intended to illustrate the process flows between the different actors involved in the payment transaction. Examples covering some other cases with respect to the QR-code content specified in Chapter 4 may be found in the report ERPB/2020/026 [14].

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 SCT Inst.

Further examples of process flows for MSCTs may be found in the MSCT IG [9].

A1.1 Process flow for merchant-presented QR-code containing a token

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

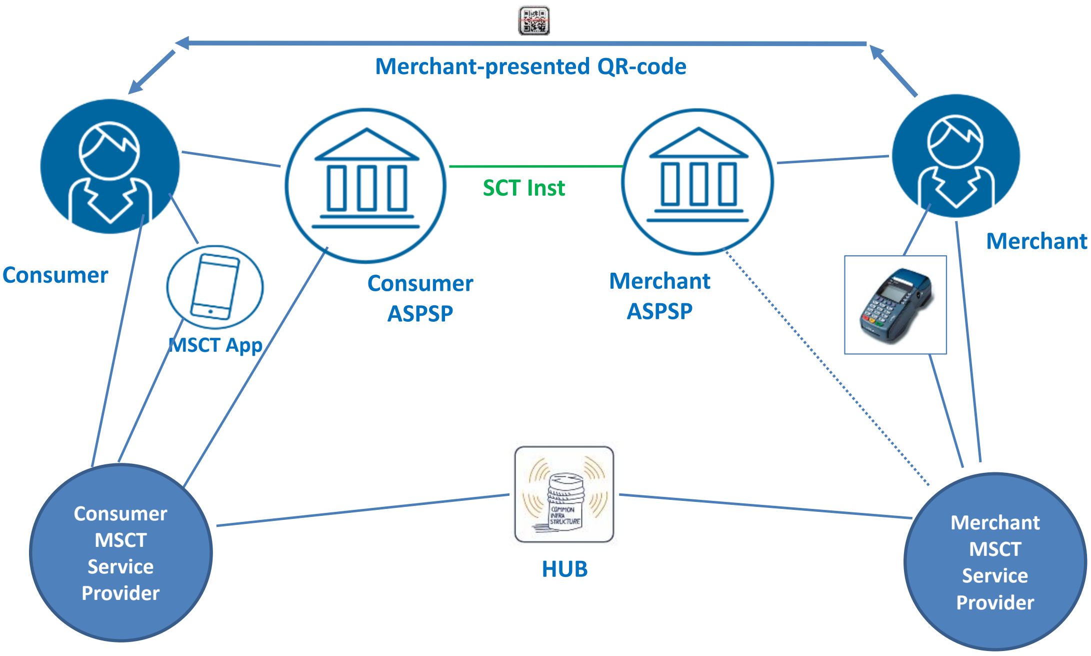
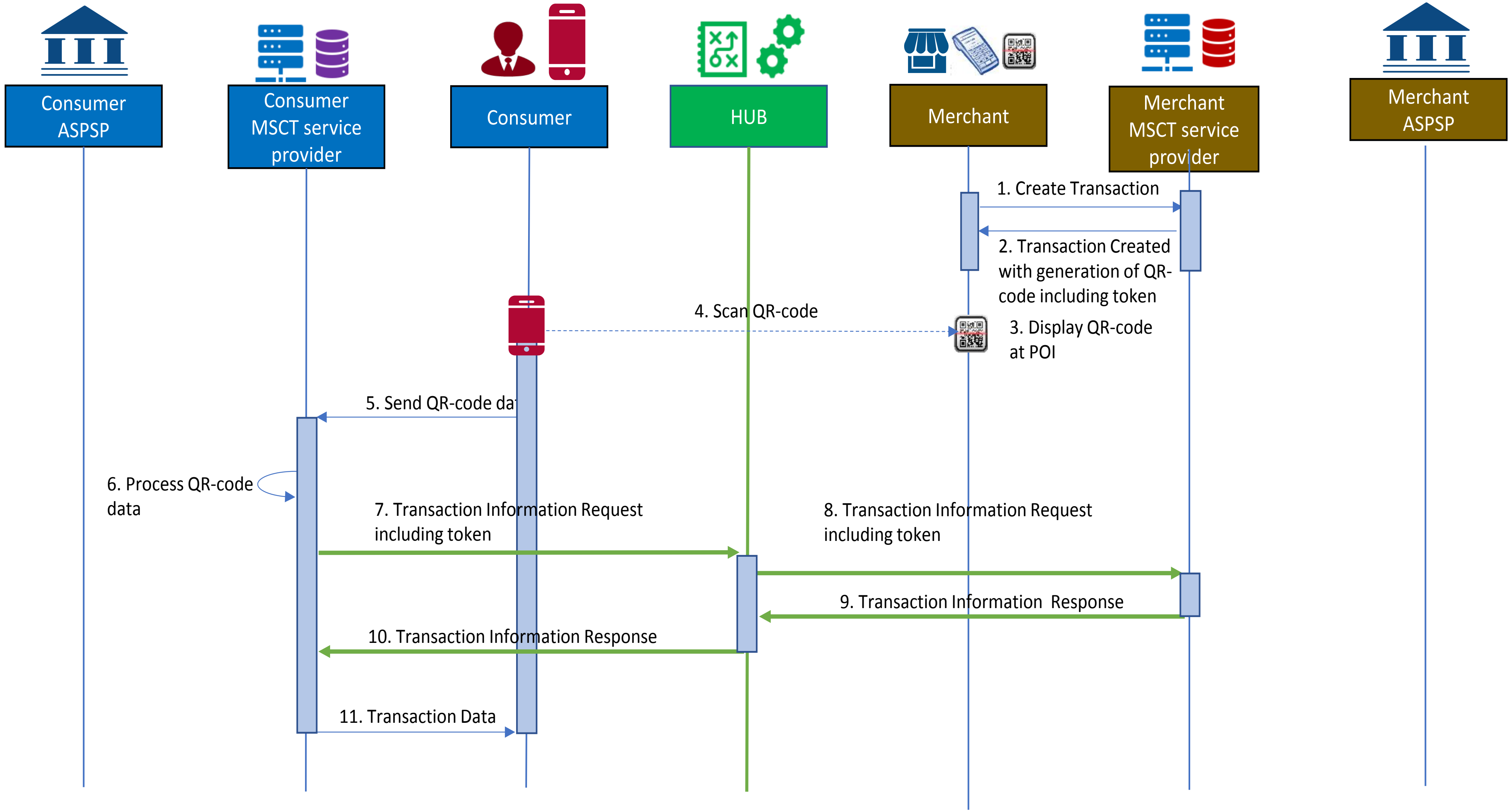

Merchant-presented QR-code
Consumer
MSCT App
Consumer ASPSP
SCT Inst
Merchant ASPSP
Merchant
HUB
COMMON INFRA STRUCTURE
Consumer MSCT Service Provider
Merchant MSCT Service Provider

Figure 3: Actors for MSCT with merchant-presented QR-code

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


Consumer ASPSP
Consumer MSCT service provider
Consumer
HUB
Merchant
Merchant MSCT service provider
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-code da
6. Process QR-code data
7. Transaction Information Request including token
8. Transaction Information Request including token
9. Transaction Information Response
10. Transaction Information Response
11. Transaction Data

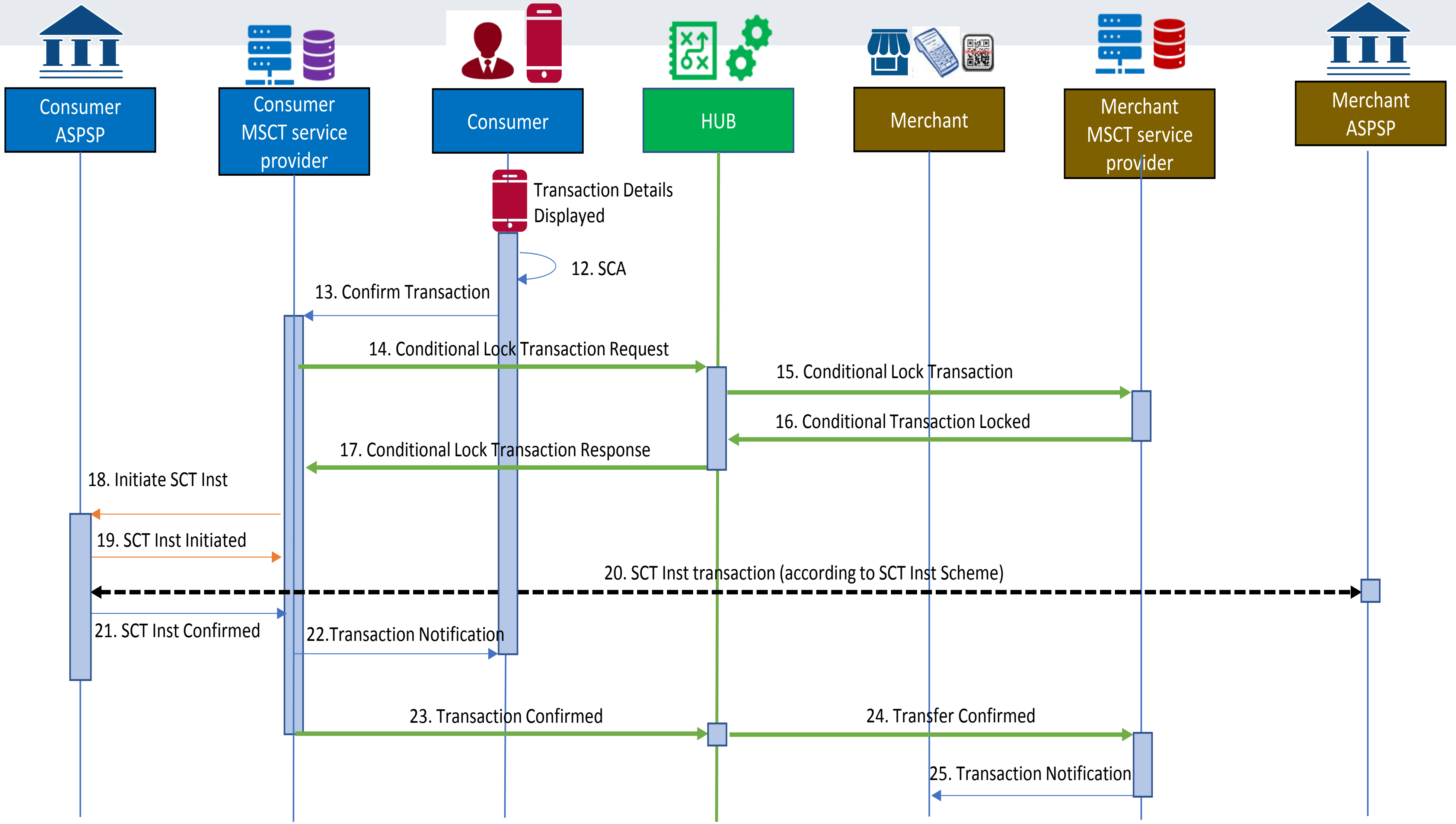

Consumer ASPSP
Consumer MSCT service provider
Consumer
HUB
Merchant
Merchant MSCT service provider
Merchant ASPSP
Transaction Details Displayed
12. SCA
13. Confirm Transaction
14. Conditional Lock Transaction Request
15. Conditional Lock Transaction
16. Conditional Transaction Locked
17. Conditional Lock Transaction Response
18. Initiate SCT Inst
19. SCT Inst Initiated
20. SCT Inst transaction (according to SCT Inst Scheme)
21. SCT Inst Confirmed
22.Transaction Notification
23. Transaction Confirmed
24. Transfer Confirmed
25. Transaction Notification

Figure 4: 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 MSCT service provider[19].

Step 2:

The merchant's MSCT service provider returns a QR-code including a unique token based on the transaction details (transaction amount, name/trade name merchant, IBAN_merchant, transaction identifier) and their MSCT service provider identifier to the merchant.[20]

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.

[19] Alternatively, the merchant POI infrastructure may generate the QR-code.

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

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.

Step 12:

The consumer consents to the transaction based on the details displayed and performs SCA[21].

Step 13:

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

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

Step 14 (conditional)[22]:

The consumer's MSCT service provider sends a Lock Transaction Request to the HUB including the merchant's MSCT service provider identifier.

Step 15 (conditional):

The HUB forwards a "Lock Transaction" to the merchant's MSCT service provider.

Step 16 (conditional):

The merchant's MSCT service provider sends a "Transaction Locked" to the HUB.

Step 17 (conditional):

The HUB forwards the Lock Transaction Response to the consumer's MSCT service provider.

Step 18:

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

Step 19:

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

Step 20:

The consumer's ASPSP sends the SCT Inst transaction to the merchant's ASPSP and the transaction flow is handled according to the SCT Inst scheme.

Step 21:

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

[22] In case the LT Indicator does not require a lock transaction function, steps 14 through 17 will not be present (see Chapter 6 in the MSCT IG [9]).

Step 22:

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

Step 23:

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

Step 24:

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

Step 25:

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

A1.2 Process flow for consumer-presented QR-code containing a token

The detailed process flows between the different actors involved in this MSCT transaction are shown in the next figure. Hereby the token contained in the consumer-presented QR-code is sent by the merchant MSCT service provider to the consumer MSCT 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 MSCT. Note that it is hereby assumed that the consumer MSCT service provider fulfils the role of Token Service Provider for the consumer. The consumer MSCT 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 MSCT service provider.

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

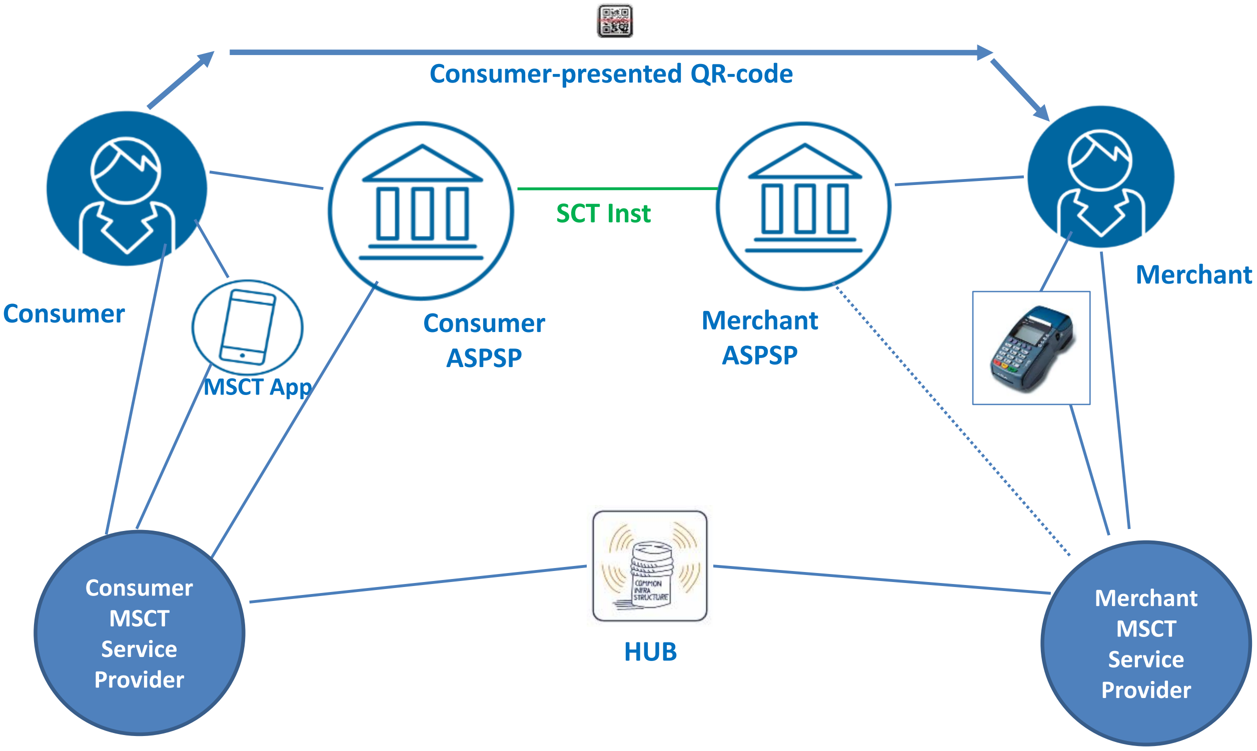
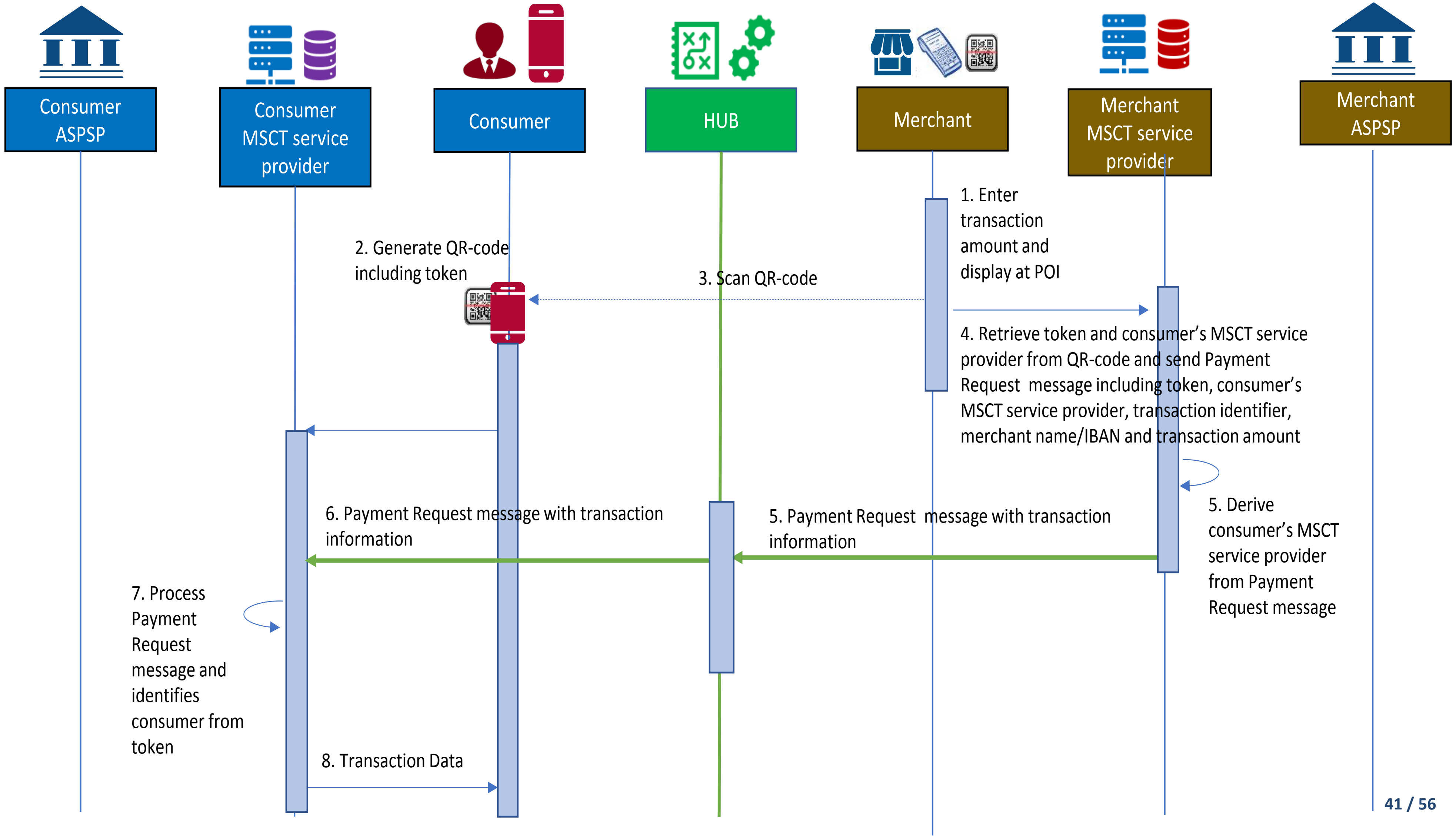

Consumer-presented QR-code
SCT Inst
Consumer
MSCT App
Consumer ASPSP
Merchant ASPSP
Merchant
HUB
Consumer MSCT Service Provider
Merchant MSCT Service Provider

Figure 5: Actors for MSCT with consumer-presented QR-code

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



Consumer ASPSP

Consumer MSCT service provider

Consumer

HUB

Merchant

Merchant MSCT service provider

Merchant ASPSP

1. Enter transaction amount and display at POI

2. Generate QR-code including token

3. Scan QR-code

4. Retrieve token and consumer's MSCT service provider from QR-code and send Payment Request message including token, consumer's MSCT service provider, transaction identifier, merchant name/IBAN and transaction amount

5. Derive consumer's MSCT service provider from Payment Request message

5. Payment Request message with transaction information

6. Payment Request message with transaction information

7. Process Payment Request message and identifies consumer from token

8. Transaction Data

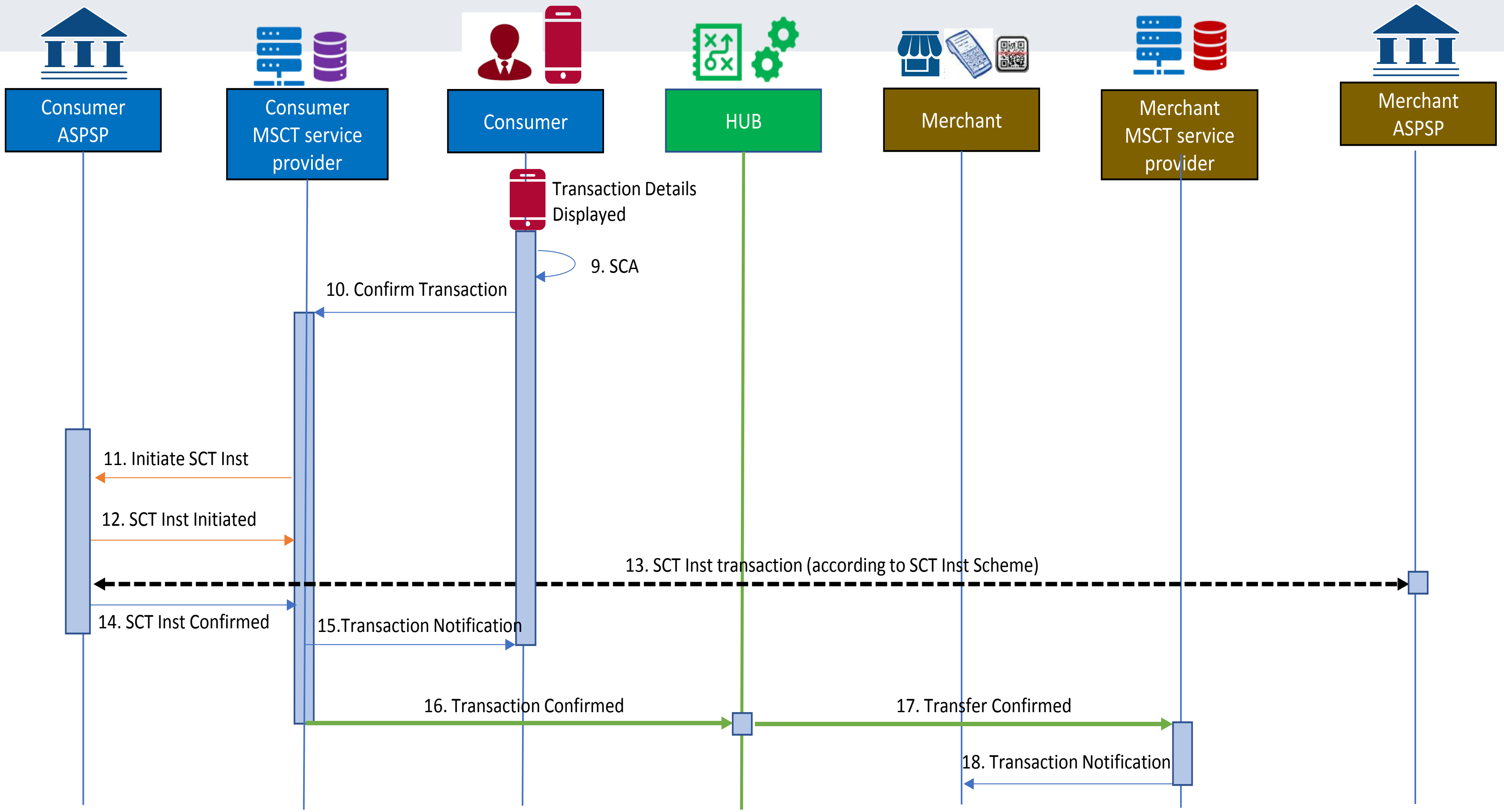

Consumer ASPSP
Consumer MSCT service provider
Consumer
HUB
Merchant
Merchant MSCT service provider
Merchant ASPSP
Transaction Details Displayed
9. SCA
10. Confirm Transaction
11. Initiate SCT Inst
12. SCT Inst Initiated
13. SCT Inst transaction (according to SCT Inst Scheme)
14. SCT Inst Confirmed
15.Transaction Notification
16. Transaction Confirmed
17. Transfer Confirmed
18. Transaction Notification

Figure 6: 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[23].

Step 2:

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

Step 3:

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

Step 4:

The merchant retrieves the consumer's token and the consumer's MSCT service provider identifier from the QR-code and sends a Payment Request message to their MSCT service provider, including the merchant's name, IBAN_merchant[24], merchant transaction identifier, the transaction amount, the consumer's MSCT service provider identifier and the consumer token.

Step 5:

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

Step 6:

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

[23] 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).

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

Step 7:

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

Step 8:

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

Step 9:

The consumer consents to the transaction based on the details displayed and performs SCA[25].

Step 10:

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

Step 11:

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

Step 12:

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

Step 13:

The consumer's ASPSP sends the SCT Inst transaction to the merchant's ASPSP and the transaction flow is handled according to the SCT Inst scheme.

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

Step 14:

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

Step 15:

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

Step 16:

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

Step 17:

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

Step 18:

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

Annex 2: Interoperability with other QR-code initiatives for mobile payments

A2.1 EMPSA

EMPSA's goal is to create interoperability between already established, currently only locally or regionally operating European mobile payment solutions, similar to the roaming model of the MNO providers, without affecting their already established domestic environment. Customers should be enabled to pay with their familiar mobile payment solution (contained e.g. in a wallet) within other payment solutions throughout Europe.

In addition, EMPSA also wants to create compatibility with other payment systems that are not members, so that merchants at the POI can offer their customers a wide variety of payment methods via a uniform infrastructure. For this purpose, EMPSA defined a very flexible code format for merchant-presented data, called the UMAMI code (Universal Mobile Alliance Message Interoperability).

The merchant-presented UMAMI QR-code has the following structure:

```
/https://hostname/version/usecase/routing/?query=...
 <--(sub)domain--> <--    operation     --> <- payload ->
```

Table 10: UMAMI merchant-presented QR-code

The structure of the code only has to correspond to the general specifications for URLs and certain parameters such as version, use case, routing and payload have to be found in a predefined position within the URL. The domain or the payload itself can largely be designed freely by the issuer of the QR code.

The structure of the URL is largely identical to the specifications developed in this document (section 4.5) and in the MSCT IG [9]. In addition, the UMAMI specifications provide the possibility of including information required for SCT Inst within the Payload. "Extended parameters" are already prepared in order to be able to map information such as amount, payee, IBAN, etc.

In this way, merchants who have concluded an acceptance contract with an EMPSA partner and offer merchant-presented data should be enabled to display a uniform QR-code that can also support instant payments such as SCT Inst.

A2.2 Alipay

Alipay and their partners, including acquiring partners and mobile payment partners, are using so-called “CGCP (Contactless Gateway Code Protocol) code” for cross-border payments. A similar code format is also used for domestic payments in China, with some variations regarding the length and the payload part of the code. In Alipay’s portfolio of code-scanning payment products, the following products are designed for in-store payment scenarios:

A2.2.1 User-presented code[26]*:*

Code Issuer ID	Consumer Identification Number

Table 11: Alipay consumer-presented code

Code Issuer ID is an indicator of the code issuer, i.e. Alipay or their mobile payment partners. Consumer Identification Number is generated by the Code Issuer, and randomised for single usage.

All the characters are numeric. The length of the code varies from 17 to 32 digits. Codes with the length ranging from 25 to 32 digits are reserved for future use.

The code is symbolised into one-dimensional Code 128 (as in ISO/IEC 15417 [23]) as well as two-dimensional QR code (as in ISO/IEC 18004 [21]), to suit different merchant devices.

Due to hardware constraints and legacy reasons, many Chinese merchants acquired by Alipay can only read one-dimensional Code 128 no longer than 24 digits. Therefore, the Consumer-presented QR-code as in Table 7 is not recognisable for these merchants. The other way around, the EU merchants which adopt the Consumer-presented QR-code as in Table 7 do not have hardware constraints to support the Alipay user-presented code as in Table 11.

A2.2.2 Merchant-presented code, including Order code and Entry/Store code:

HTTPS://<DOMAIN_NAME>/<optional fields>/	<PAYLOAD to identify an order>

Table 12: Alipay merchant-presented code: order code

HTTPS://<DOMAIN_NAME>/<optional fields>/	<PAYLOAD to identify a merchant>

Table 13: Alipay merchant-presented code: entry/store code

<DOMAIN_NAME> is an indicator of the code issuer, i.e. Alipay or their acquiring partners. <PAYLOAD> is generated by the code issuer. <optional fields> in between are reserved for future use. The code is symbolised into two-dimensional QR code (as in ISO/IEC 18004 [21]).

The Alipay merchant-presented code as in Table 12 and Table 13 adopt similar format with the Merchant-presented QR-code as in Table 6. These codes are read by the consumer payment apps, and the users who have subscribed to the code-scanning payment services usually do not have hardware constraints to support such code format. If the code contains

[26] User refers here to the consumer.

enough information to be distinguishable from other URL-based QR codes, and a so-called “bridge” would be implemented between the HUB of the Interoperability Framework of IPs at the POI and the Alipay backend, interoperability between these two kinds of merchant-presented codes could be achieved.

A2.3 EMVCo

EMVCo develops and maintains the EMV® QR-Code Specifications that include the Merchant-Presented Specification (MPM) and the Consumer-Presented Specification (CPM). The definition and clarity provided by the EMV® QR Code™ Specifications enable merchants to accept QR-code payment solutions from various providers in a standardised manner, using a single QR-code.

The following tables illustrates different implementation choices to support payload for merchant-presented QR-codes for MSCTs. Note: a “default” / “dummy: value of “0” for unused mandatory data fields defined in the EMV specifications is included; another clearly defined default value may be used.

Data Object	ID		Format	Value
Payload Format Indicator	"00"		n	"01"
Merchant Account Information	"26"		ans	As defined by MSCT
	Globally Unique ID	“00”	ans	As defined for MSCT provider, for instance, “com.provider.msct”
	Payload Issuer	“01”	an	
	Token	“02”	an	
Merchant Category Code	“52”		n	“0”
Transaction Currency	“53”		n	“0”
Transaction Amount	“54”		ans	“0”
Country Code	“58”		ans	“0”
Merchant Name	“59”		ans	“0”
Merchant City	“60”		ans	“0”
Cyclic Redundancy Check (CRC)	“63”		ans	“####”

Table 14: EMVCo mapping of Payload of MSCT QR-code containing a token

Data Object	ID		Format	Value
Payload Format Indicator	“00”		n	“01”
Merchant Account Information	“27”		ans	As defined by MSCT
	Globally Unique ID	“00”	ans	As defined for MSCT provider, for instance, “com.provider.msct”
	Payload Issuer	“01”	an	
	Proxy Payee	“03”	an	
	Proxy Payee Reference Party	“09”	an	
	Remittance information structured or Remittance information unstructured	“04”	an	
	Type of payment instrument	“07”	an	SCT or SCT Inst
Merchant Category Code	“52”		n	
Transaction Currency	“53”		n	
Transaction Amount	“54”		ans	
Merchant Name	“59”		ans	As defined for Name payee (account holder)
Additional Data Field Template	“62”		s	
	Purpose of Transaction	“08”	ans	As defined for Purpose of credit transfer (includes e.g. merchant transaction identifier)
Country Code	“58”		ans	“0”

Merchant Name	“59”	ans	“0”
Merchant City	“60”	ans	“0”
Cyclic Redundancy Check (CRC)	“63”	ans	“####”

Table 15: EMVCo mapping of Payload of MSCT QR-code containing a proxy

Data Object	ID		Format	Value
Payload Format Indicator	“00”		n	“01”
Merchant Account Information	“28”		ans	As defined by MSCT
	Globally Unique ID	“00”	ans	As defined for MSCT provider, for instance, “com.provider.msct”
	Payload Issuer	“01”	an	
	Remittance information structured or Remittance information unstructured	“04”	an	
	Trade name	“05”	an	
	IBAN Payee	“06”	an	
	Type of payment instrument	“07”	an	SCT or SCT inst
	Name of Payee reference party	“08”	an	
Merchant Category Code	"52"		n	
Transaction Currency	"53"		n	
Transaction Amount	"54"		ans	
Additional Data Field Template	“62”		s	

	Purpose of Transaction	“08”	ans	As defined for Purpose of credit transfer (includes e.g. merchant transaction identifier)
Country Code	"58"		ans	"0"
Merchant Name	"59"		ans	"0"
Merchant City	"60"		ans	"0"
Cyclic Redundancy Check (CRC)	"63"		ans	"####"

Table 16: EMVCo mapping of Payload of MSCT QR-code containing all data “in clear”

Data Object	ID		Format	Value
Payload Format Indicator	“00”		n	“01”
Merchant Account Information	“26”		ans	As defined by MSCT
	Globally Unique ID	“00”	ans	As defined for MSCT provider, for instance, “com.provider.msct”
	URL	“10”	Ans	As defined by MSCT for accessing provider
Merchant Category Code	“52”		n	“0”
Transaction Currency	“53”		n	“0”
Transaction Amount	“54”		ans	“0”
Country Code	“58”		ans	“0”
Merchant Name	“59”		ans	“0”
Merchant City	“60”		ans	“0”
Cyclic Redundancy Check (CRC)	“63”		ans	“####”

Table 17: EMVCo mapping of URL for retrieving payload from server

The mapping shown in the tables above could potentially be used in the future if EMVCo QR-code based card payments would be supported by merchants throughout SEPA and there is a business incentive to combine multiple mobile payment solutions (e.g., MSCTs at the POI and card-based payments) in a single (EMVCo) QR-code.

A2.4 EPI

The European Payments Initiative (EPI) is currently specifying a solution for card and account-based payments. They consider the usage of QR-codes, for C2B and P2P payments both in payee-presented and payer-presented modes, which are URL based. However, currently, there is no further information available on the format and the coding of these QR-codes.

Annex 3: List of participants to MSG MSCT Plenary

The following organisations have contributed to the development of this document through their participation in the Plenary of the multi-stakeholder group Mobile initiated SEPA (instant) Credit Transfers (MSG MSCT).

AIB on behalf of Banking & Payments Federation Ireland (BPFI) - representing EPC
Bankin’ - representing European Third Party Providers Association (ETPPA)
BEUC - European Consumer Organisation
BlueCode
BP
Carrefour - representing EuroCommerce
Circle K
Colruyt - representing EuroCommerce
Crédit Agricole - representing EPC
Crédit Mutuel - representing EPC
DnB Bank – representing EPC
EACT - European Association of Corporate Treasurers
Estonian Banking Association- representing EPC
EMPSA - European Mobile Payment Systems Association
Fiserv
Getswish
Huawei
Idemia - representing Smart Payment Association
IKEA - representing EuroCommerce
Intesa Sanpaolo on behalf of Italian Banking Association (ABI) – representing EPC
La Banque Postale - representing EPC
Mastercard
Millennium bcp – representing EPC
Monei
National Clearing House KIR
Nexi Payments

nexo
OpenWay
Orange - representing GSMA
Payconiq
PPRO - representing European Third Party Providers Association (ETPPA)
Rabo bank - representing EPC
TAS Group
Thales – representing Smart Payment Association
Tink – representing European Third Party Providers Association (ETPPA)
Vipps
Visa
W3C
Eurosystem – as observer
European Central Bank (ECB) – as observer
European Commission – as observer

Table 18: The MSG MSCT Plenary

Annex 4: List of participants MSG MSCT Work-Stream technical interoperability of QR-codes

The following organisations have contributed to the development of this document through their participation in Work-Stream technical interoperability of QR-codes of the multi-stakeholder group Mobile initiated SEPA (instant) Credit Transfers (MSG MSCT).

BP
BEUC - European Consumer Organisation
BlueCode
CEN
Crédit Mutuel - representing EPC
DnB Bank – representing EPC
EMPSA - European Mobile Payment Systems Association
ETTPA - European Third Party Providers Association
EMVCo
EPI – European Payments Initiative
Getswish
Idemia - representing Smart Payment Association
IKEA - representing EuroCommerce
Mastercard
Monei
Nexi Payments
nexo
OpenWay
PPRO - representing European Third Party Providers Association (ETPPA)
Thales – representing Smart Payment Association
Tink – representing European Third Party Providers Association (ETPPA)
Vipps
Visa

Table 19: The MSG MSCT Work-Stream technical interoperability of QR-codes

The multi-stakeholder group further wishes to thank Alipay for their contributions delivered as input to this document.

The multi-stakeholder group wishes to inform that this document is provided "as is" without warranty of any kind, whether expressed or implied, including, but not limited to, the warranties of merchantability and fitness for a particular purpose. Any warranty of non-infringement is expressly disclaimed. Any use of this document shall be made entirely at the user’s own risk, and neither the multi-stakeholder group nor any of its members shall have any liability whatsoever to any implementer for any damages of any nature whatsoever, directly or indirectly, arising from the use of this document, nor shall the multi-stakeholder group or any of its members have any responsibility for identifying any IPR.