European Payments Council

Mobile Initiated SEPA (Instant) Credit Transfer Payments and Technical Interoperability Guidance (MSCT IG)

EPC269-19 / Version 2.9.9/ Date issued: 21 May 2024

Table of Contents

Executive Summary

Mobile devices have achieved full market penetration and rich service levels making the mobile channel ideal for leveraging and promoting the use of SEPA payment schemes.

This document provides guidance for Mobile Initiated SEPA (Instant) Credit Transfers (MSCTs) payments and proposes an approach for their technical interoperability, being brand and implementation model agnostic.

Cross-industry cooperation on specifications, guidelines and best practices has been identified as a critical success factor in this area. Therefore, the EPC has coordinated since 2018 a multi-stakeholder group covering the various sectors involved in the MSCT ecosystem to address the interoperability issues. The group developed the *MSCT Interoperability Guidance* (MSCT IG) that was first published in 2019, followed by a second version in February 2022 (EPC269-19v2.0). The present document is a new version of the MSCT IG, with a focus on most relevant use cases and the technical interoperability. It furthermore aligns with the last version of the EPC document *Standardisation of QR-codes for MSCTs*, developed by the MSG MSCT and published in January 2023 which, at the time of publication of this Guidance, has been revised and submitted by the EPC to CEN to become a European standard.

The document aims through the description of some illustrative MSCT use cases to provide an insight into the main issues related to the initiation of (instant) SEPA credit transfers for different payment contexts such as consumer-to-business (retail payments including both in-store and m-commerce payments).. Next to the MSCT transaction aspects it focuses on the technology used in the customer-to-ASPSP space, since the SCT Inst and SCT transactions as such have already been specified in the respective scheme rulebooks (see [16] and [20]).The document analyses in detail the technical interoperability of MSCTs based on payee- or payer-presented data and specifies the technical interoperability requirements between MSCT service providers, for successful and unsuccessful transactions, which are also depicted in some illustrative process flows using a so-called "HUB" between the payer's and payee's MSCT service providers. It defines the minimum data to be exchanged between the payer and payee to enable the initiation of an MSCT and specifies for this a payee- and payer-presented QR-code for MSCTs, while ensuring alignment with [32]. It further specifies the minimum data sets for all interoperability messages between the respective MSCT service providers of the payer and the payee. Additional interoperability models including a Payment Initiation Service Provider (PISP) or a Collecting PSP (on behalf of the merchant) are also included. Finally, the document identifies the main interoperability challenges and opportunities for MSCTs.

Note that subjects such as business cases and revenue models for the MSCT value chain belong to the commercial space and therefore are not addressed in this document.

While producing this document, the multi-stakeholder group has noticed a number of "major challenges and opportunities" that will need to be properly addressed to achieve full interoperability of MSCT transactions (see Chapter 14).

These include:

- The availability of a technical infrastructure to interconnect the different MSCT service providers notably for the support of token/proxy-based MSCTs and MSCT confirmation and notification messages to PSUs (payers and payees);

- The development of an implementation specification for the MSCT QR-codes specified in this document and the subsequent adoption by the market;

- Next to the technical aspects, also the operating rules, liabilities, adherence to these requirements and governance should be addressed. This could be achieved through the set-up of a dedicated "MSCT interoperability framework or MSCT scheme" to which the MSCT service providers (existing and new one) should participate to ensure interoperability of MSCT services;

"Request-to-Pay" services could enhance the customer experience for MSCTs for all payment contexts. The work on the SRTP scheme [26] complements the current document and will further contribute to the consumer adoption of MSCTs.

Other challenges for MSCT services include:

- Complexity and security of the different mobile platforms;

- The co-existence of multiple proximity technologies, possibly linked to different payment instruments at the POI (see Chapter 24);

- Uncertainties regarding European rules and regulations (e.g.; PSD2 [5], RTS [6] and GDPR [7]), also related to their interplay with respect to MSCTs[1] (see also Chapters 7, 8 and 22).

The multi-stakeholder group has organised focused work on the technical interoperability issues through various technical expert work-streams. The work on instant payments at POI has also been conducted under the ERPB (see [38] and [40]) that has leveraged the documents developed by the MSG MSCT.

By developing this interoperability guidance, the multi-stakeholder group aimed to contribute to a competitive MSCT market, by providing the different stakeholders an insight into the different service and technical aspects involved. The document could serve as a reference basis for making certain implementation choices.

1 Document Information

1.1 Structure of the document

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

- Chapter 1 includes the document information.
- Chapter 2 provides the vision on Mobile Initiated SEPA (Instant) Credit Transfers (MSCTs), including SCT Inst, as well as the scope and the objectives of this document;
- Chapter 3 defines the high-level principles;
- Chapter 4 introduces the definition of MSCT modes and the relevant stakeholders
- Chapter 5 provides an overview of MSCT transaction aspects
- Chapter 6 introduces some examples of illustrative MSCT use cases
- Chapter 7 describes proximity technologies used by MSCTs
- Chapter 8 includes a high level analysis of technical interoperability aspects;
- Chapter 9 discusses the technical interoperability of MSCTs based on payee-presented data;
- Chapter 10 discusses the technical interoperability of MSCTs based on payee-presented data;
- Chapter 11 provides an overview on the MSCT interoperability messages;

[1] See EBA Q&A 2020_5247, 5365-5367, 5476, 5477, 5570-5573, 5587 and 2021_6298.

- Chapter 12 discusses new MSCT interoperability models;
- Chapter 13 provides an overview of additional challenges and opportunities;
- Chapter 14 includes the conclusions;
- Annex 2 includes an overview on errors cases;
- Annex 3 specifies the minimum data sets for MSCT interoperability messages;
- Annex 4 gives an overview of the different organisations and companies involved in the multi-stakeholder group that developed this document.

1.2 References

This section lists the references mentioned in this document. Square brackets throughout this document are used to refer to documents in this list.

[1]	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 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN)	EC
[2]	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") (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN)	EC
[3]	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 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN)	EC
[4]	EPC125-05 2019: SEPA Credit Transfer Scheme Rulebook (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2020-04/EPC125-05%202019%20SCT%20Rulebook%20version%201.1.pdf)	EPC
[5]	EPC115-06: SEPA Credit Transfer Scheme Interbank Implementation Guidelines (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2018-11/EPC115-06%20SCT%20Interbank%20IG%202019%20V1.0.pdf)	EPC
[6]	EPC342-08: Guidelines on algorithms usage and key management	EPC

	(https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2021-03/EPC342-08%20v10.0%20Guidelines%20on%20Cryptographic%20Algorithms%20Usage%20and%20Key%20Management_0.pdf)	
[7]	EPC492-09: White paper Mobile Payments (https://www.europeanpaymentscouncil.eu/sites/default/files/KB/files/EPC492-09%20v5.0%20White%20Paper%20Mobile%20Payments%20-%20edition%202017.pdf)	EPC
[8]	EPC004-16: SEPA Instant Credit Transfer Scheme Rulebook (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2020-10/EPC004-16%202019%20SCT%20Instant%20Rulebook%20v1.2_0.pdf)	EPC
[9]	EPC122-16: SEPA Instant Credit Transfer Scheme Interbank Implementation Guidelines (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2018-11/EPC122-16%20SCT%20Inst%20Interbank%20IG%202019%20V1.0_1.pdf)	EPC
[10]	EPC014-20: SEPA RTP Scheme Rulebook (https://www.europeanpaymentscouncil.eu/document-library/rulebooks/sepa-request-pay-scheme-rulebook-version-v30)	EPC
[11]	EPC212-21 - ERPB/2021/017: Standardisation and governance of QR-codes for Instant Payments at the Point of Interaction (IPs at the POI) (https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/standardisation-and-governance-qr-codes-instant-payments-point)	EPC/ERPB
[12]	EPC024-22: Standardisation of QR-codes for MSCTs (https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2023-01/EPC024-22v2.0%20Standardisation%20of%20QR-codes%20for%20MSCTs.pdf)	EPC
[13]	EPC287-22: Interoperability of MSCTs based on NFC or BLE (https://www.europeanpaymentscouncil.eu/document-library/other/final-document-interoperability-mscts-based-nfc-or-ble)	EPC
[14]	ERPB/2019/012: Final report of the ERPB Working Group on Instant Payments at POI (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/12th-ERPB-	ERPB

	meeting/Report from the ERPB WG on instant at POI.pdf?efe8385c4196f8094d5b6625f7ffdc79)	
[15]	ERPB/2020/026: Framework for interoperability of instant payments at the point of interaction (IPs at the POI) (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/14th-ERPB-meeting/ERPB_working_group_on_instant_at_the_POI_-_Framework_for_interoperability_of_instant_payments_at_the_POI.pdf?db00f43b17d4aeeb4a83ae82187d53c8)	ERPB
[16]	ERPB/2020/027: Specifications to enable consumer selection of preferred payment instrument (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/14th-ERPB-meeting/ERPB_working_group_on_instant_at_the_POI_-_Specifications_for_payment_instrument_selection.pdf?db00f43b17d4aeeb4a83ae82187d53c8)	ERPB
[17]	ERPB/2021/005: Report of the Next Phase of the ERPB Working Group on a Single Euro Payments Area (SEPA) Application Programming Interface (API) Access Scheme (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/15th-ERPB-meeting/Report_from_the_ERPB_working_group_on_a_SEPA_API_Access_Scheme.pdf?52770756a713895bdc4fd072873346be)	
[18]	ERPB/2021/006: Report from the ERPB working group on transparency for retail payment end-users (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/15th-ERPB-meeting/Final_report_of_the_ERPB_working_group_on_transparency_for_retail_payments_end_-_users.pdf?e53826e577a16eced647ffe382578861)A	ERPB
[19]	ERPB/2021/018: Business requirements - Consumer selection of preferred payment instrument (https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/16th-ERPB-meeting/Business_requirements_for_consumer_selection_of_preferred_payment_instrument.pdf)	ERPB
[20]	GPD_SPE_009: TEE System Architecture (https://globalplatform.org/wp-content/uploads/2017/01/GPD_TEE_SystemArch_v1.2_PublicRelease.pdf)	GlobalPlatform

[21]	GPC_FST_142: GlobalPlatform Technology – VPP - Concepts and interfaces v1.0.1 https://globalplatform.org/specs-library/globalplatform-technology-virtual-primary-platform-v1-0-1/	GlobalPlatform
[22]	ISO 13616: Financial services - International Bank account number (IBAN) -- Part 1: Structure of the IBAN (https://www.iso.org/standard/81090.html)	ISO
[23]	ISO/IEC 14443: Identification cards - Contactless integrated circuit(s) cards - Proximity cards – Parts 1-4 (https://www.iso.org)	ISO
[24]	ISO/IEC 18004: Information technology -- Automatic identification and data capture techniques -- QR-code bar code symbology specification (https://www.iso.org/standard/43655.html)	ISO
[25]	ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems -- Near Field Communication - Interface and Protocol (NFCIP-1) (https://www.iso.org/standard/38578.html)	ISO
[26]	World Telecommunication/ICT Indicators Database 2018 (https://www.itu.int/pub/D-IND-WTID.OL-2018)	ITU
[27]	NFC Controller Interface (NCI) Specifications (https://nfc-forum.org/product/nfc-controller-interface-nci-technical-specification-2-1/#:~:text=The%20NCI%20specification%20defines%20a,the%20device's%20main%20application%20processor.&text=The%20new%20version%20also%20includes,communicate%20with%20NFC%20Forum%20tags)	NFC Forum
[28]	NFC Analog Technical Specification (https://nfc-forum.org/product/analog-technical-specification-version-2-1/)	NFC Forum
[29]	Vetting the Security of Mobile Applications, NIST. Draft NIST Special publication 800-163, Revision 1, July 2018 (https://csrc.nist.gov/CSRC/media/Publications/sp/800-163/rev-1/error/documents/sp800-163r1-draft.pdf)	NIST
[30]	IPR (Instant Payments Regulation): Regulation (EU) 2024/886 of the European Parliament and of the Council amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro	

Table 1: Bibliography

1.3 Definitions

Throughout this document, the following terms are used. Their definitions are based on [5], [16] and [20].

Term	Definition
Account Servicing Payment Service Provider (ASPSP)	A PSP providing and maintaining a payment account for a payer (see [5]).
Account statement information	The information on the SCT payment (for the data elements to be provided, see [16], [20]) available to the Payee on the basis agreed between the Payee and their Payee ASPSP. This may include a paper account statement, an online account statement or a machine-readable statement.
Alias	See Proxy.
Authentication	The provision of assurance that a claimed characteristic of an entity is correct. The provision of assurance may be given by verifying an identity of a natural or legal person, device or process.[2] (see ISO 12812 – Part 1 [78]).
Authentication Application	An application accessed through the mobile device performing the functions related to a user authentication, as dictated by the Authentication Service Provider.
Authentication Service Provider	A service provider offering a customer authentication service typically in the context of this document, involving an Authentication Application accessed via the mobile device of the customer.
Authenticator	A security factor used in an authentication method such as: - Something you know, such as a password, PIN or passphrase - Something you have, such as a token device or smart card - Something you are, such as a biometric.
Beneficiary	See Payee.
Bluetooth Low Energy (BLE)	A wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications including beacons. Compared to classic Bluetooth, BLE is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range.
Business Identifier Code (BIC)	An 8 or 11 character ISO code assigned by SWIFT and used to identify a financial institution (see [94]).
Collecting Payment Service Provider (CPSP)	A payment service provider according to PSD2 [5] that collects the payment transactions on behalf of the merchant (the ultimate beneficiary) and as such is the beneficiary of the IP 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 [5]).

[2] Note that the PSD2 [5] uses a more restrictive definition: "authentication" means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials.

Consumer device	An internet capable device used by the consumer (payer) to authenticate and/or to conduct a payment. Examples include a mobile device or a personal computer (PC).
Consumer-presented data	Data provided by the consumer at the merchant's POI.
Contactless Technology	A radio frequency technology operating at very short ranges so that the user has to perform a voluntary gesture in order that a communication is initiated between two devices by approaching them. It is a mobile payment acceptance technology at a POI device which is based on ISO/IEC 14443 (see [79]).
(Personalised Security) Credential(s)	Personalised feature(s) provided by the payment service provider to a payment service user for the purposes of authentication (see Article 4 in [5].
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 [5]).
Credit Transfer instruction	An instruction given by a payer to a payer 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 [5].
Credit Transfer Transaction	An instruction executed by a payer ASPSP by forwarding the Transaction to a CSM for forwarding the transaction to the payee ASPSP.
Customer	A payer or a payee which may be either a consumer or a business (merchant).
CustomerID	An identification of the payer, 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.
Dynamic authentication	An authentication method that uses cryptography or other techniques to create a one-per-transaction random authenticator (a so-called "dynamic authenticator").

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.
Facial recognition	A technology capable of identifying or verifying a person from a digital image or a video frame from a video source. It is one of the CDUVM methods used for mobile payments.
Fingerprint	An impression left by the friction ridges of a human finger. It is one of the CDUVM methods used for mobile payments.
Funds	Cash, scriptural money or electronic money as defined in Article 4 in [5].
Host Card Emulation (HCE)	A technology that enables mobile devices to emulate a contactless card. HCE does not require the local usage of an SE on the mobile device for storage of sensitive data such as credentials, cryptographic keys, etc.
HUB	An infrastructure ensuring connectivity between IP 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 IP service providers through a dedicated API.
Identification of payee	A means of uniquely identifying the payee and their underlying account. Examples are the usage of IBAN, an alias, card number, dedicated, identifier, dedicated credentials, …
Immediate(ly)	Synonym for Instant(ly).
In-app payment	These are payments made directly from within a mobile application (e.g., a merchant app). The payment process is completed from within the app to enhance the consumer experience.
Instant(ly)	At once, without delay.
Instant Payment (IP)	Electronic retail payment solutions available 24/7/365 and resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payer (within seconds of payment initiation). This is irrespective of the underlying payment instrument used (credit transfer, direct debit or payment card) and of the underlying clearing and settlement arrangements that make this possible (see [21]).

Intermediary PSP	A PSP which is neither that of the Payer nor that of the Payee and who participates in the execution of a credit transfer (see section 3.4 in [16]).
International Bank Account Number (IBAN)	An internationally agreed system of identifying bank accounts across national borders to facilitate the communication and processing of cross border transactions (see ISO 13616 [76]).
Merchant	A beneficiary within a mobile payment scheme for payment of the goods or services purchased by the consumer. The merchant is a customer of their PSP. A merchant may also be referred to as a payee.
Merchant-presented data	Data provided by the merchant's POI to the consumer.
Mobile code	An authentication credential used for user verification and entered by the consumer via the keyboard of the mobile device.
Mobile device	Personal device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth, etc. Examples of mobile devices include mobile phones, smart phones, tablets and wearables.
Mobile equipment	The mobile phone without the UICC (also referred to as mobile handset).
Mobile Network Operator (MNO)	A mobile phone operator that provides a range of mobile services, potentially including facilitation of NFC services. The MNO ensures connectivity 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 consumer (i.e. the holder of the wallet) or may be remotely hosted on a secured server (or a combination thereof) or on a merchant website. Typically, the so-called mobile wallet issuer provides the wallet functionalities but the usage of the mobile wallet is under the control of the consumer.
Mobile wallet issuer	The service provider that issues mobile wallet functionalities to the customer (consumer or merchant).
MSCT Application	A set of modules (application software) and/or data (application data) needed to provide functionality for an MSCT Inst or MSCT transaction as specified by the MSCT service provider in accordance with the SEPA SCT Inst or SCT scheme.
MSCT Application user interface	The user interface of a mobile payment application.
MSCT Service Provider	A service provider that offers or facilitates an MSCT service to a payer and/or payee based on a SCT Inst or SCT payment

	transaction. This may involve the provision of a dedicated MSCT application for download on the customer's mobile device or the provision of dedicated software for the merchant POI. As an example, an MSCT service provider could be a PSP (e.g., an ASPSP or any party acting as a PISP under PSD2) or a technical service provider supporting a PSP.
Mutual Authentication	This refers to two parties authenticating each other at the same time using an authentication protocol (also referred to as two-way authentication).
NFC (Near Field Communication)	A contactless protocol for mobile devices specified by the NFC Forum for multi-market usage. NFC Forum specifications (see [92]) are based on ISO/IEC 18092 [82] but have been extended for harmonisation with EMVCo and interoperability with ISO/IEC 14443 [79].
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 [5]) (examples include merchant, business).
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 [5]).
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 [5]).
Payment Application Selection User Interface	The mobile phone user interface (component) enabling the consumer to Access the MSCT application User Interface on the mobile phone Select the preferred payment application.
Payment Initiation Service Provider (PISP)	A payment service provider pursuing business activities as referred to in Annex I of [5].
Payment Request	A message sent by the payee to their MSCT service provider and from the payee's MSCT service provider to the payer MSCT service provider including all transaction data. This data may be used by the payer's MSCT service provider for presentation to the payer to enable them to perform SCA and confirm the transaction as needed using their mobile device

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 Service Provider (PSP)	An entity referred to in Article 1(1) of [5] or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33 of [5].
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 [5]).
Payment system	A funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions (as defined in [5]).
Payment transaction	An act, initiated by the payer or on his/her behalf or by the payee (payee), of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee (as defined in [5]).
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 [7]).
Physical POI	A POI that is a physical device and consists of hardware and software, hosted in acceptance equipment to enable a consumer and/or merchant to perform an MCST. The merchant-controlled POI may be attended or unattended. Examples of POI include POS, vending machine.
Point of Interaction (POI)	"Point of Interaction", the initial point in the merchant's environment where data is exchanged with a consumer device (e.g., mobile phone, wearable, etc.) or consumer data is entered (e.g. physical POI, remote POI) or a QR-code on a poster, to initiate an SCT Inst or SCT.
Proximity Payment	A payment where the consumer and the merchant (and/or their equipment) are in the same location and where the communication between the mobile device and the Point of Interaction device takes place through a proximity technology (e.g., NFC, 2D barcodes, BLE, ultrasonic, etc.).
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 may be referred to as IBAN-proxy.
QR-code	Quick-Response code [81], see also 2D barcode.

Remote POI	The initial point where card data enters the merchant's domain for remote transactions. It exists in a variety of technical platforms which enable a cardholder (consumer) and/or a merchant to generate a remote payment (e.g. a payment page accessed via a merchant website or via a mobile app).
Remote transaction	In the context of this document, a transaction using a mobile device conducted over mobile internet.
SEPA Request-to-Pay	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 specified in the SRTP scheme (see [26]).
Risk-based Authentication	The use of statistical models via transaction, location, device and profile data to make a customer authentication decision without active customer participation in the decision-making process (see also Article 18.3 in [6] and [84].
R-transaction	A transaction to reverse an initial SEPA (Instant) Credit Transfer and the subsequent messages. This refers to the exceptional processes flows, including Rejects, Return, Recalls and Request for Recall by the Payer, see section 4.4 in [16] and/or section 4.3.2 in [21].
Secured Server	A web server with secure remote access that enables the secure storage and processing of payment related data.
Secure Element (SE)	A tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g., key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. There are different form factors of SE including Universal Integrated Circuit Card (UICC), embedded SE (including eUICC and iSE) and microSD. Both the UICC and microSD are removable.
Secure Element (SE) Provider	A TTP which owns the original access rights to the SE. Typical examples are MNOs and mobile device manufacturers.
Sensitive payment data	Data including personalised security credentials which can be used to carry out fraud (see [5]).
SEPA Credit Transfer	The SEPA Credit Transfer is the payment instrument governed by the rules of the SEPA Credit Transfer Scheme for making credit transfer payments in euro throughout the SEPA from bank accounts to other bank accounts (see [16]).
SEPA Instant Credit Transfer	The SEPA Instant Credit Transfer is the payment instrument governed by the rules of the SEPA Instant Credit Transfer Scheme for making instant credit transfer payments in euro throughout the SEPA from bank accounts to other bank accounts (see [20]).
SEPA Request-to-Pay message	Message sent by the Payee to the Payer according to the SRTP scheme, directly or through agents. It is used to request the

	movement of funds from the payer account to the payee account (see [26]).
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).
Settlement	An act that discharges obligations with respect to the transfer of Funds between Payer ASPSP and Payee ASPSP.
Strong customer authentication	An authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data (see Article 4 in [5]).
Third Party	This is an entity in the ecosystem that is different from an MNO or an MSCT service provider.
Third Party Payment Service Provider (TPP)	A third party that offers payment services which are different to the Account Servicing PSP (ASPSP) such as a Payment Initiation Service Provider (PISP), Account Information Service Providers (AISP) and Trusted Party Payment Instrument Issuer (TPII) (see [5]).
Token	Tokens can take on a variety of formats across the payments industry. They generally refer to a surrogate value for payment account, PSU identification data or transaction related data (e.g., the IBAN for SCT (Instant) payments). Payment Tokens must not have the same value as or conflict with the real payment account related data. If the token is included in the merchant-presented data it might be referred to as a merchant token; if the token is included in the consumer-presented data it might be referred to as a consumer token.
Tokenisation	Process of substituting payment account or transaction related data with a surrogate value, referred to as a 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 payer account related data when requested by the token requestor. It may also include the capability to establish the token assurance level to indicate the confidence level of the payment token to the payer account related data / payer / merchant / device / environment binding. The service also provides the capability to support token processing of payment transactions submitted using tokens by de-tokenising the token to obtain the actual account related data.

Token Service Provider (TSP)	An entity that provides a Token Service.
Trusted Execution Environment (TEE)	A separate execution environment (as defined by Global Platform, see [61] that runs alongside, but isolated from the main operating system. A TEE has security capabilities and meets certain security-related requirements: it protects TEE assets from general software attacks, defines rigid safeguards as to data and functions that a program can access, and resists a set of defined threats.
Trusted Third Party (TTP)	An entity which facilitates interactions between stakeholders of the ecosystem who all trust this third party (examples are SE provider, common infrastructure manager…).
User Interface (UI)	An application or part of an application enabling the user interactions, as permitted by the application issuer. It allows to provide information to the consumer (such as payment amount) and enables the consumer to interact in order to change preferences, perform queries, enter credentials, etc.
Universal Integrated Circuit Card (UICC)	A generic and well standardised SE owned and issued by the MNOs.
Ultrasonic	Sound waves with frequencies higher than the upper audible limit of human hearing.
Uniform Resource Identifier (URI)	A unique sequence of characters that identifies a logical or physical resource used by web technologies.
User Verification Method	A method for checking that a consumer is the one claimed (see [78].

Table 2: Terminology

1.4 Abbreviations

Abbreviation	Term
an	alphanumeric
ASPSP	Account Servicing PSP
API	Application Programming Interface
B2B	Business-to-Business
B2C	Business-to-Consumer
BIC	Business Identifier Code
BLE	Bluetooth Low Energy
C2B	Consumer-to-Business
CEN	European Committee for Standardisation
CPSP	Collecting Payment Service Provider
CSM	Clearing and Settlement Mechanism
2D barcode	Two dimensional barcode
DSS	Data Security Standards
EBA	European Banking Authority
EC	European Commission
EPSG	European Payments Stakeholders Group
EPC	European Payments Council
ERP	Enterprise Resource Planning
ERPB	Euro Retail Payments Board
ETPPA	European Third Party Providers Association
FIDO Alliance	Fast IDentity Online Alliance
GDPR	General Data Protection Regulation
GSMA	The GSM Association
HCE	Host Card Emulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS
IBAN	International Bank Account Number
ID	Identifier
ICT	Information and Communication Technology
IP	Instant Payment
IPR	Intellectual Property Rights
iSE	Integrated Secure Element
ISO	International Organization for Standardization
LCM	Lifecycle Management
MA	Mobile Application
ME	Mobile Equipment
MNO	Mobile Network Operator
MSCT (Instant)	Mobile initiated SCT (or SCT Inst)

MSCT IG	Mobile Initiated SEPA (Instant) Credit Transfer Payments and Technical Interoperability Guidance
MSG MSCT	Multi-Stakeholder Group for Mobile Initiated (Instant) SCT
n	numeric
NFC	Near-Field Communication
OEM	Original Equipment Manufacturer
OS	Operating System
OTP	One-Time-Password
P2P	Person-to-Person
PCB	Printed Circuit Board
PCI	Payment Card Industry
PID	Person Identification Data
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
REE	Rich Execution Environment
RFID	Radio Frequency Identification
ROM	Read Only Memory
RTP	Request-To-Pay
RTS	Regulatory Technical Standard
SCT	SEPA Credit Transfer
SCT Inst	SEPA Instant Credit Transfer
SDD	SEPA Direct Debit
SE	Secure Element
SEPA	Single Euro Payments Area
SIM	Subscriber Identity Module
SP	Service Provider
SPA	Smart Payment Association
SPAA	SEPA Payment Account Access
SRTP	SEPA Request-To-Pay
TC	Technical Committee
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TP	Third Party
TPP	Third Party Payment Service Provider
TSP	Token Service Provider
TTP	Trusted Third Party
UI	User Interface
UICC	Universal Integrated Circuit Card

URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UVM	User Verification Method
VPP	Virtual Primary Platform
XML	Extensible Markup Language

Table 3: Abbreviation

2 General

2.1 Introduction

In November 2019, the first edition of this document (v1.0), developed by the multi-stakeholder group for mobile initiated SEPA (instant) credit transfers (MSG MSCT) was published on the EPC website, following a public consultation. In view of the rapidly changing market and evolving technology, the multi-stakeholder group developed a new release (v2.0) of this guidance document which was published in February 2022.

The version 2.0 was intended for readers who require a comprehensive detailed (technical) guidance on MSCTs. The document included many updates to the first edition and integrates the various MSCT related documents that have subsequently been developed by the MSG MSCT and which have previously been published as separate documents on the EPC website.
Following the extension of its mandate, approved by the EPC Board in May 2023, the MSG MSCT has developed this document as version 3.0 of the MSCT interoperability guidance. This version is intended to provide a perspective focused on the MSCT *technical interoperability* aspects, resulting from a consultation with major stakeholders involved in providing instant-payments-based mobile payments solutions, rolled-out in the 2nd half of 2023. The MSG MSCT has also taken into consideration the complex regulatory landscape, with several EU legislative acts undergoing, in various stages the adoption process, which are expected to deeply impact the market in the coming years.
As a result, the presentation of the potential use-cases was narrowed-down to a limited number of illustrative cases, aimed at demonstrating the feasibility of the interoperability as it has been elaborated since the first version of this guidance. In addition, some subjects present in the first two versions have been removed from this last version, such as security considerations which will be maintained and further developed by other workstreams, and presentations of underlying payment schemes and supporting services, which have their own roadmap, governance and release lifecycle.
It is important to note that the standardisation of QR-codes for interoperable SCT Inst based payments is ongoing and, at the time of releasing this version, it is in the final stage of approval by the European Committee for Standardization (CEN).

Starting with general description of MSCT, this version further covers transaction aspects, and focuses on the technology used in the customer-to-ASPSP space, since the SCT Inst and SCT transactions as such have already been specified in the respective scheme rulebooks (see [16] and [20]). The document analyses in detail the technical interoperability of MSCTs based on payee- or payer-presented data and specifies the technical interoperability requirements between MSCT service providers, for successful, unsuccessful transactions and rejects, which are also depicted in some illustrative process flows using a so-called “HUB” between the payer’s and payee’s MSCT service providers. It defines the minimum data to be exchanged between the payer and payee to enable the initiation of an MSCT and specifies for this a payee- and payer-presented QR-code for MSCTs, while ensuring alignment with the EPC specifications for QR-codes (see [12]).).

Therefore the interoperability approach as presented in this document relies on two technical pillars:

- The availability and acceptance of the QR-codes standardisation proposed by the EPC, with its options.

- The HUB interconnecting MSCT service providers which, among other functions, should ensure translation between the data formats using these options.

It further specifies the minimum data sets for all interoperability messages between the respective MSCT service providers of the payer and the payee. Additional interoperability models including a Payment Initiation Service Provider (PISP) or a Collecting PSP (on behalf of the merchant) are also included. This guidance document concludes with a discussion on the main interoperability challenges but also opportunities for MSCTs.

This document endeavours to reflect the current state of play and market situation for MSCTs at the time of publication while being brand and implementation model agnostic. On the other hand, it needs to be recognised that the MSCT ecosystem is rapidly evolving and expanding. To date most of the solutions are "closed-loop" solutions, not interoperable between each other. Market adoption of “interoperable” MSCTs constitutes a key assumption for the further evolution and expansion of the ecosystem.

2.2 Vision

This document has been written by the multi-stakeholder group with the following vision:

“To ensure over time, across SEPA, a secure, convenient, consistent, efficient and trusted payment experience for the payer and payee for mobile initiated SEPA (instant) credit transfers, based on commonly accepted and standardised payment technologies.”

This vision is based on the following guiding principles:

- Technical interoperability of MSCTs across SEPA (based on common technical, functional and security standards and an appropriate certification and evaluation framework) both for PSU mobile devices and POIs;
- Full reachability for SCT Inst amongst PSPs;
- Wide availability and usability of appropriate POI equipment and mobile devices;
- Appropriate security and privacy measures to build and maintain trust in the MSCT ecosystem.

The aim is to lead to an enhanced payment experience – e.g., easy P2P payments, faster check out, user-friendliness, a better integration of value-added services with payment – and to cost-effectiveness for society.

This guidance aims to contribute to the creation of the necessary environment so that service providers, vendors and other stakeholders involved in the MSCT ecosystem can deliver secure, efficient and user-friendly MSCT solutions, in an integrated market.

The document contributes to the development of this integrated market for payments in Euro through the development and promotion of standards and guidelines.

This document focuses on the technical interoperability aspects of MSCTs. In the last chapter some non-technical challenges identified with respect to MSCT interoperability are briefly discussed.

2.3 Scope

The guidance focuses on interoperability between the different stakeholders involved in the MSCT ecosystem. In particular, they address the technical interoperability aspects related to the MSCT transaction across SEPA.

The document covers MSCTs, whereby an Instant SEPA Credit Transfer (SCT Inst) or a SEPA Credit Transfer (SCT) as specified in the respective rulebooks (see [20] and [16]) are the underlying SEPA payment instrument.

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

- A description of some illustrative MSCT use cases;
- The MSCT transaction aspects outside the inter-PSP space;
- The roles of the main stakeholders in the MSCT ecosystem;
- Technical interoperability aspects for MSCTs (including messages, etc.);
- The main challenges and barriers to interoperability within the MSCT ecosystem.

Finally, it is important to note that the document only addresses the aspects of MSCTs, which reside in the interoperability space of the stakeholders in the MSCT value chain. As such, the specification of business cases and a detailed analysis of the MSCT value chain fall outside the scope of the document.

2.4 Objectives

The purpose of this document is to provide interoperability guidance for MSCTs. In order to achieve this the document will

- Provide guidance so that all deployed operational and transactional processes directly related to MSCTs can be implemented
- Identify barriers to achieving an adequate level of technical interoperability for MSCTs.
- Strive for a harmonised customer experience across SEPA for MSCTs at the POI.

- Provide guidance for the implementation of MSCTs which is complementary to the SCT and SCT Inst rulebooks (see [20] and [16]).

2.5 Audience

The document is primarily intended for the payment industry. It aims to propose to the industry an option on how to achieve interoperability in the development of MSCT solutions.. It could further be used as a reference by the payment industry to achieve a cohesive payment user experience.

It aims to provide information to stakeholders involved in implementations and deployment of MSCTs, including:

- Payment Service Providers;
- MSCT service providers;
- Other service providers such as Mobile Network Operators (MNO), Tokenisation Providers, etc.;
- Equipment manufacturers;
- Merchants and merchant organisations;
- Consumers and their associations;
- MSCT application developers;
- Regulators;
- Standardisation and industry bodies.

3 High-level principles

The following high-level principles have been followed for the specification of this guidance.

1. To support the need for SEPA interoperability, the usage of SCT Inst or SCT as specified in the respective rulebooks (see [16] and [20]) is assumed.

2. The infrastructures used for SCT Inst and SCT payments should be leveraged as much as appropriate.

3.

4. Creating ease, convenience and trust for PSUs (payers and payees), using a mobile device to initiate an MSCT, is regarded as critical for the further development within this area.

5. Payers shall be able to make MSCTs throughout SEPA, regardless of the original country where the MSCT service was subscribed to and / or provided (issued).

6. A consumer using a specific MSCT service should have a similar experience at the POI throughout SEPA. However, this experience may slightly differ depending on the existing infrastructure or other relevant environmental conditions (e.g., influenced by the risk management or POI environment).

7. PSPs should have the possibility to develop MSCT services on all the common mobile platforms[3] in the market openly[4].

8. The mobile device interface / wallet provider should enable the MSCT service provider to define the graphical interface to the PSU for their MSCT service, including brands and logos, MSCT solution brands, payment type, etc. as appropriate.

9. Payers should have the possibility for their MSCT services to switch mobile devices[5] and should not be bound to a specific MNO.

10. Payers should be able to use all the MSCT services offered by multiple MSCT service providers using their mobile device[6].

11. Payers should be able to select the relevant MSCT service on their mobile device to be used for a particular MSCT transaction.

[3] Combination of different hardware and software on a mobile device.
[4] See Chapter 24
[5] From different providers (including MNOs, handset manufacturers, OS providers, etc.) subject to appropriate agreements.

[6] subject to appropriate agreements and risk management considerations.

4 Mobile initiated SEPA (Instant) Credit Transfers

4.1 Introduction

This chapter aims to provide a high-level overview about MSCTs, including both the MSCT transaction and the provisioning and life cycle management.

4.2 MSCT Transaction

4.2.1 Introduction

MSCT transactions are SCT Inst or SCT transactions that are initiated by the payer using a mobile device. They are based on the existing SCT Inst or SCT rulebooks (see [20] and [16] respectively) in the so-called "inter-PSP space" and are therefore using in that space the existing payment infrastructure. They typically use a mobile MSCT application or mobile browser on the payer's mobile device to initiate the SCT Inst or SCT transaction. Therefore, this document will mainly focus on the interactions outside the inter-PSP space such as between the mobile device and the POI, between the payer and payee, between the payer/payee and their MSCT service provider and between MSCT service providers (see also Figure 1 and Figure 2).

4.2.2 MSCT modes

For MSCTs, basically two modes[7] can be distinguished depending on how the data that enables the initiation of the payment is transferred between the payer and the payee:

- MSCTs based on payee-presented data: in this mode the data, i.e. the payee identification and, as needed, transaction data is provided by the payee to the payer and is either
  - presented by the payee and read by the payer's mobile device (e.g. via proximity technology);
  - already shared by the payee with the payer beforehand (e.g. in P2P payment contexts);

- MSCTs based on payer-presented data: in this mode the data, i.e. the payer identification is provided by the payer to the payee and is either
  - presented by the payer and read by the payee's device via a proximity technology (e.g. physical POI or mobile device);
  - entered by the payer into the payee's POI (e.g. webpage of self-check-out);
  - already shared by the payer with the payee beforehand (e.g. entered by the payer during the on-boarding process and subsequently stored into a merchant app on the payer's mobile device).

A. MSCTs based on payee-presented data

Currently, there is a wider market adoption of MSCTs based on payee-presented data for all payment contexts; it is the most important mode used for P2P payments and for C2B payments at a physical POI, while for payments at a virtual POI there appears to be geographical differences.

[7] Note that when a proximity technology would be is used in a bi-directional way between the payer and payee, MSCT transaction data could be exchanged in the two directions

Moreover, payee-presented QR-codes seem to be the most important proximity technology adopted by the market for C2B payments, except NFC. The payee-presented mode also facilitates the usage of MSCTs for paying invoices through the usage of a payee-presented QR-code.

From a payer perspective, the usage of an MSCT app on their mobile device that supports payee-presented data allows them to pay for all payment contexts (P2P, C2B and B2B), which leads to a consistent payment experience, enhanced trust and no need to share payer identification data with the payee. Moreover, it enables an easier risk management for the payer's MSCT service provider.

B. MSCTs based on payer-presented data

For C2B payment contexts, this mode enables merchants to issue a merchant app to their customers. It also gives them the opportunity to offer value-added services such as loyalty, couponing, etc. More in particular, large merchants appear to be interested in this mode in view of the consistent consumer experience for payments at a physical POI, being it account- or card-based.

However, this mode also comes with a number of challenges. Currently many POI terminals are not equipped yet for payer-presented mode (e.g. missing a QR-code reader). Moreover, there are some security concerns related to the generation of the payer-presented QR-code, e.g., if generated outside the control of the payer's MSCT service provider (see Chapter 810).

4.3 MSCT Provisioning and life cycle management

For MSCTs, the hosting of a dedicated MSCT application on the mobile device may be required. An MSCT application may be supported by complementary applications residing on the mobile device's "Read-Only Memory (ROM)", which are known as the MSCT application user interface and which are dedicated to interacting with the user. The MSCT service provider is responsible for this application, its security characteristics and the secure communication with the MSCT application.

Also a separate dedicated authentication application hosted on the payer's mobile device may be involved to conduct an MSCT.

If no MSCT application is present, the mobile device may be used to store static data/credentials for MSCTs (e.g., in a mobile wallet). If there are security requirements for these data (integrity and/or confidentiality), the data needs to be stored in a trusted environment with appropriate access control.

4.4 Relevant stakeholders in the MSCT ecosystems

MSCTs involve some new stakeholders in the value chain compared to (instant) SEPA credit transfers.

The following entities, in addition to the ones described in SCT and SCT Inst rulebooks may be involved:

- **The MSCT service provider** that offers an MSCT service to a payer and/or payee related to a SCT Inst or SCT payment transaction. This typically involves the provision of an MSCT application for download on the PSU's mobile device or the provision of dedicated software

for the merchant POI. Examples include a mobile P2P payment service provider or a PISP. The MSCT service provider is linked to the payer's ASPSP and may be linked to the payee's ASPSP (this linkage includes both technical and contractual aspects). Note that an ASPSP may assume the role of an MSCT service provider.

- **The Token Service Provider (TSP)** is a TTP who is involved if tokens are used in MSCTs as surrogate values for the payer identification data (for a payer-presented token) or for payee identification data or transaction data such as transaction amount or transaction identifier (for payee-presented tokens) (see section 10.4 and Chapters 17 to 19). The TSP manages the generation and issuance of tokens, and maintains the established mapping of tokens to the related data when requested by the token requestor. The TSP also provides the capability to support token processing of MSCT transactions submitted using tokens by de-tokenising the token to obtain the transaction related data. In the document it is assumed that the role of TSP is covered by the MSCT service provider or is at least under the control of the MSCT service provider.
- **The Mobile Wallet Issuer** is a service provider that issues mobile wallet functionalities to the PSU (consumer or merchant).
- **Other relevant new stakeholders** include for example:
    - Secure Element (SE) providers, if the MSCT application /Authentication application is stored in an SE on the mobile device. This is the MNO in case of a UICC, the mobile equipment manufacturer, the MSCT service provider or a third party in case of an embedded SE, and the SE manufacturer.
    - Cloud service providers (which may be the MSCT service providers themselves or this service may be delegated to a TTP),
    - Application developers (MSCT application, user interface, mobile wallet …),
    - Mobile Operating System (OS) suppliers,
    - Mobile equipment manufacturers,
    - Security technology developers,
    - Mobile Network Operators (MNOs),
    - Organisations performing infrastructure certification (e.g., MSCT applications, POI, mobile devices, etc.).

At this stage, with the large number of stakeholders involved, alignment around key aspects of the ecosystem is crucial to move from fragmentation to harmonisation and to enable the development of SEPA-wide service offerings.

5 MSCT transaction aspects

In the following figure, the decomposition of an MSCT into building blocks are illustrated, both for SCT Inst and SCT transactions.

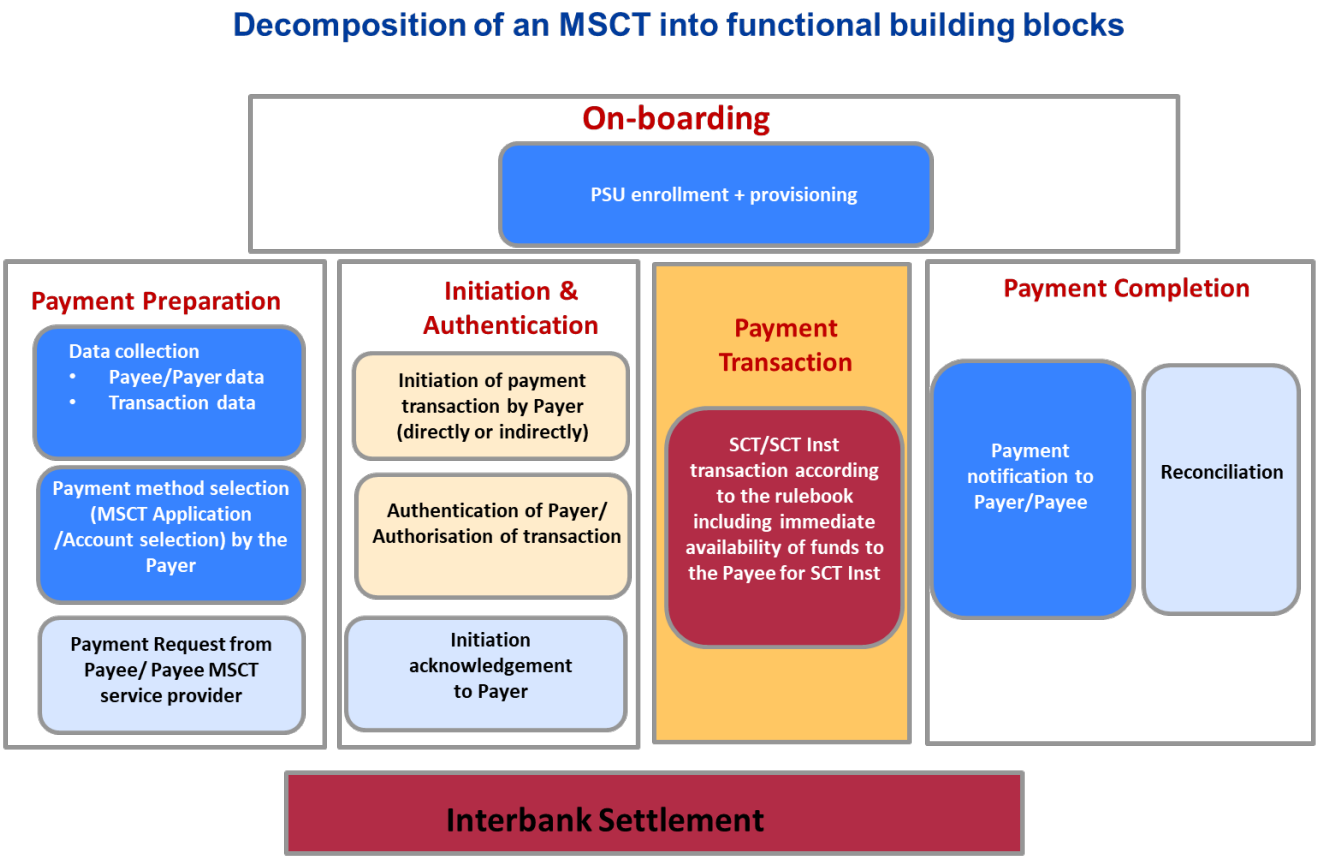


Figure 1: Decomposition of an MSCT into building blocks

Dark blue	Light blue	Dark amber	Light amber

The dark amber box in the above is covered by the SCT Inst and CST scheme rulebooks and implementation guidelines (See [4], [5], [8], and [9]) and falls outside the scope of the MSCT IG. However, they form the basis on which this document is built. The immediacy of payment offered by SCT Inst includes an immediate, irrevocable availability of the funds.

This document focuses on the technical interoperability outside the inter-PSP space such as between the payer mobile device and the payee equipment (e.g. POI, mobile device), between the payer and their MSCT service provider(s), between the payee and their MSCT service provider(s)[8] , etc. (see dark blue boxes in the Payment Preparation and Payment Completion phases).

The light blue boxes in the figure are features which may or may not be present in an MSCT based on SCT or SCT Inst. This may depend on the payment context (e.g., a Payment Request from the

[8] In so far that they impact the interoperability of MSCTs.

merchant / merchant MSCT provider for C2B payments based on consumer-presented data). Since these features are impacting the interoperability of MSCTs, they will be covered in this document.

"On-boarding" (see dark blue box) refers to the registration process of a PSU with an MSCT service provider or a merchant for a specific MSCT service, before using the service for actual payment transactions. Since the security of the on-boarding process is a specific domain that exceeds the scope of this version of the IG, the related requirements are not covered by this guidance document.

The light amber boxes refer to functionalities which are not impacting the interoperability if different MSCT service providers or different MSCT services for the payer and the payee are involved.

In case of P2P payments, a mobile phone number of the payee may be used which may require the support by a "lookup" service for linking the mobile phone number with the IBAN of the payee.

The following sections in this chapter will focus on the different aspects of the "Payment Completion" block in the figure above, while aspects related to the block "Payment Preparation" are treated in Chapters 9 and 10.
The following acknowledgements/notifications messages can be identified as regards the "Payment Completion":

- Acknowledgement of receipt to the payer by their MSCT service provider of the instruction for MSCTs based on SCT involving payee-presented data;
- Acknowledgement of receipt to the payee by their MSCT service provider of the payment request for MSCTs based on SCT involving payee-presented data;
- Notification of reject/successful/unsuccessful transaction to the payee by their MSCT service provider;
- Notification of reject/successful/unsuccessful transaction to the payer by their MSCT service provider or by their ASPSP.

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

All these technical interoperability messages will be analysed in detail in Chapters 9 and 10 in this document.

6 MSCT illustrative use cases

6.1 Introduction

This chapter provides an overview on a selection of illustrative MSCT use cases, covering the two MSCT modes – based on payer-presented and payee-presented data, as well as remote payments (e-commerce or m-commerce).
In the v2.0 of this document more use-cases were included and a follow-up stock-taking exercise identified even more use-cases, covering various SCA methods and all proximity technologies. In this version a limited number was retained, aiming essentially at demonstrating the feasibility of the interoperability vision elaborated further down in other sections of this IG.

Three use-cases will be therefore developed below:

A. C2B-A - merchant presented: Payment at a physical POI with merchant-presented QR-code and SCA on a MSCT application using a mobile code
B. C2B-B - consumer presented: Payment at a physical POI with consumer-presented QR-code and SCA on a dedicated authentication application
C. C2B-C - m-commerce/e-commerce: Payment involving a PISP with redirection to consumer ASPSP for SCA

These use-cases will be described with a diagram depicting the different actors involved[9] and with a decomposition into the different steps of the MSCT transaction which are also shown in a figure. Each MSCT use case is followed by a short evaluation on the interoperability aspects and a short list of the main challenges.

6.2 C2B-A - merchant presented: Payment at a physical POI with merchant-presented QR-code and SCA on a MSCT application using a mobile code

This use cases presents an example of consumer experience whereby their mobile device is used to pay in-store by reading a merchant-presented QR-code on the POI. Hereby both the consumer and merchant are subscribed to the different MSCT Inst services. The consumer has downloaded a dedicated MSCT Inst application from their MSCT service provider on their mobile device. The merchant has downloaded dedicated software on their POI from their MSCT service provider.

[9] In the actors' diagram the dotted lines represent exchanges of data or payment messages and solid lines represent contractual relationships

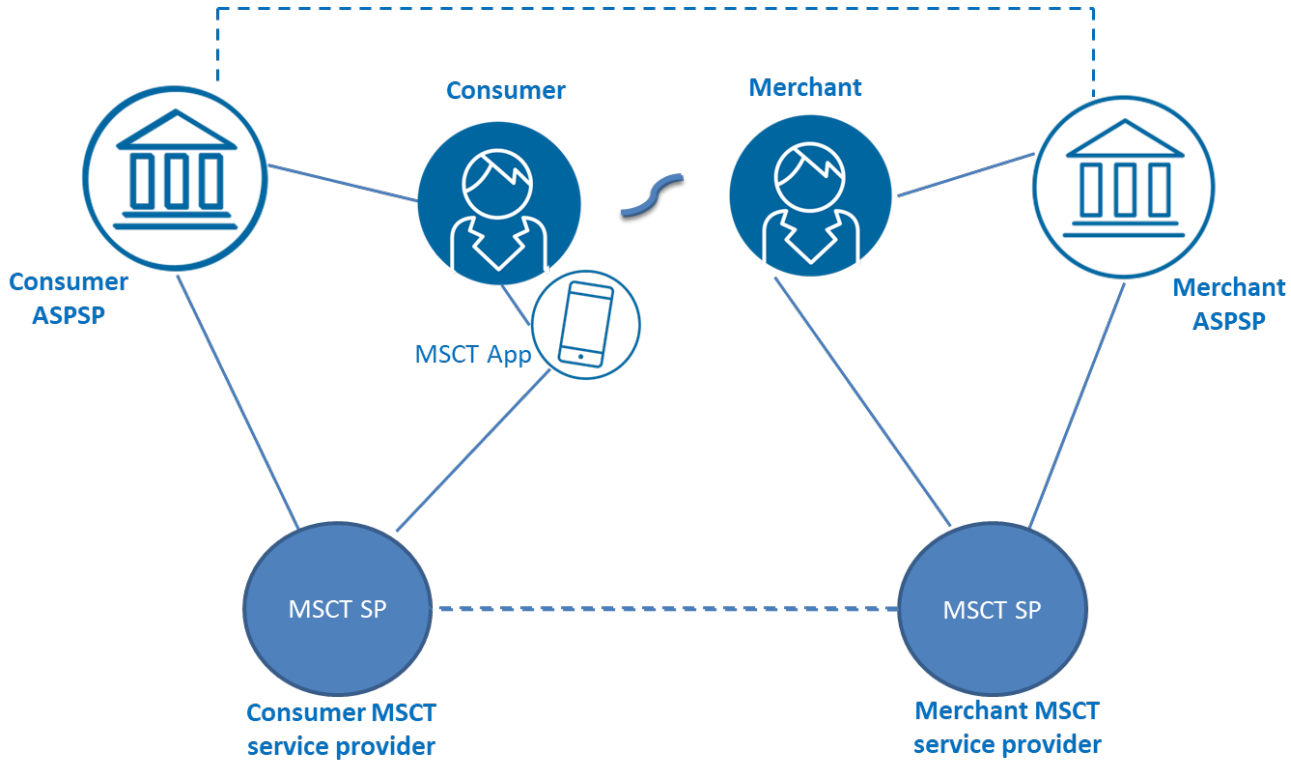


Figure 2: Actors in MSCT use case C2B-A

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. Each ASPSP needs to be in contractual relationship respectively with the consumer and merchant MSCT Inst service provider.

In this payment transaction a strong customer authentication (SCA) in accordance with PSD2 is performed involving a mobile code and the calculation of an authentication code by the MSCT application using a dedicated key. Since the MSCT application is provided to the consumer by an MSCT service provider instead of the consumer's ASPSP, a delegation for payer authentication from the consumer's ASPSP to their MSCT service provider is required. However, this requires an agreement between the consumer's ASPSP and the consumer's MSCT service provider.

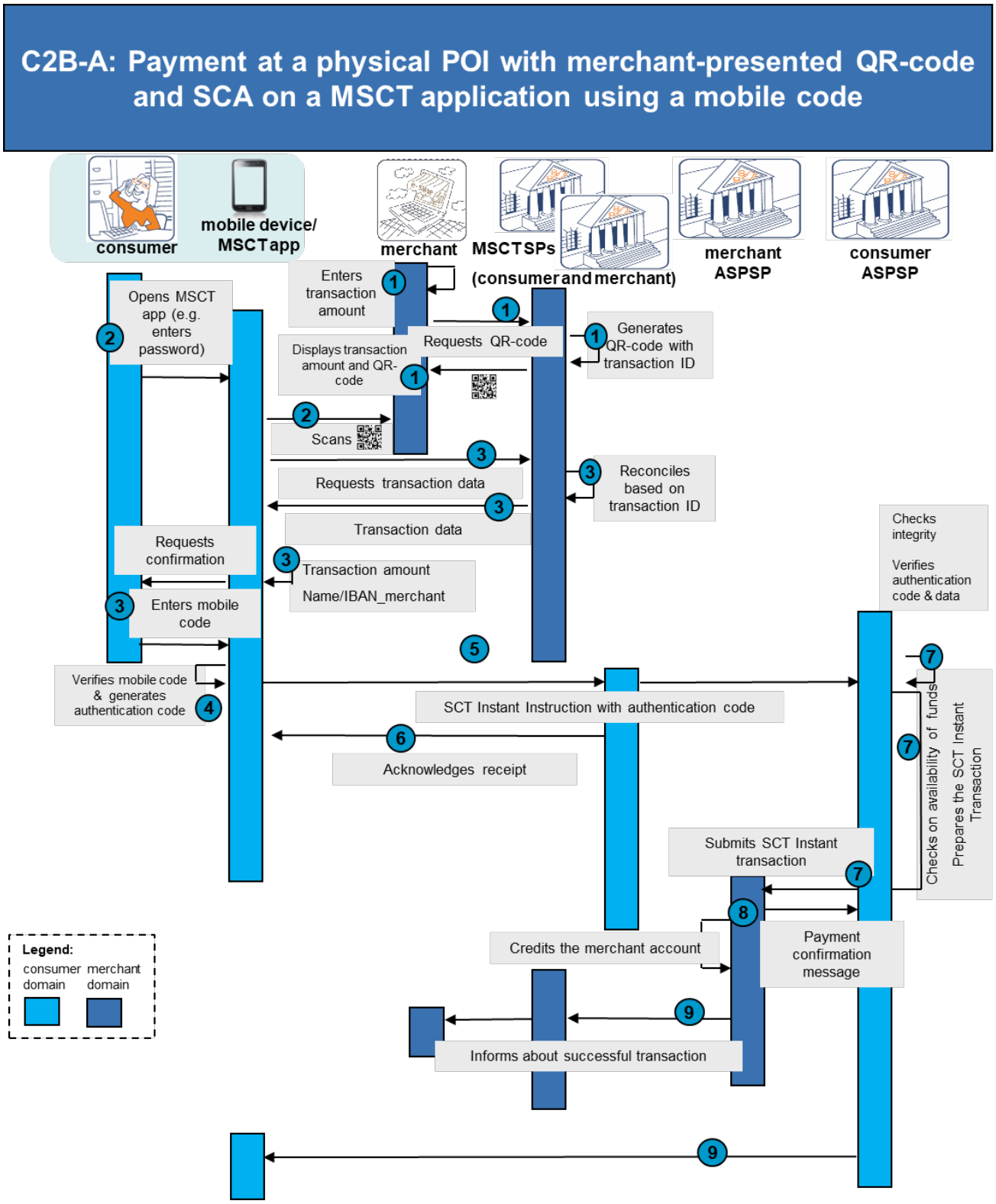


Figure 3: MSCT use case C2B-A

In the figure above, the following steps are illustrated:

Step 0

- The consumer needs to be subscribed to an MSCT Inst service and needs to have downloaded a dedicated MSCT Inst application from the MSCT Inst service provider, linked to a specific payment account of their ASPSP.
- The merchant needs to be subscribed to an MSCT Inst service with a specific account from their ASPSP and have downloaded dedicated software on their POI.
- The two MSCT service providers need to be linked to respectively the consumer ASPSP and merchant ASPSP.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The merchant enters the transaction amount on the POI.
- The POI provides the transaction amount to its MSCT service provider. For simplification, in the figure the two MSCT service provider are grouped and the details of the data flows between them are not presented
- The merchant MSCT service provider generates a QR-code, including the merchant transaction payload.
- The transaction amount is displayed on the merchant's POI with the QR-code, which includes the merchant transaction identifier.

Step 2

- The consumer selects and opens the MSCT Inst application on their mobile device which possibly requires the entry of a password.
- A message is displayed on the mobile device inviting the consumer to scan the QR-code from the POI.

Step 3

- The mobile device retrieves the transaction data from the QR-code and transmits the information to the merchant MSCT service provider.
- The merchant MSCT service provider reconciles this with the information received from the POI.
- The MSCT Inst application pops-up a window with the transaction details including the merchant name/IBAN_merchant and transaction amount.
- The consumer authenticates and confirms the transaction by entering a mobile code on the mobile device.

Step 4

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

Step 5

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

Step 6

The consumer MSCT service provider acknowledges successful receipt of the SCT Inst instruction to the consumer.

Step 7

- The consumer's ASPSP checks the integrity of the SCT Inst instruction and verifies the authentication code.
- The consumer's ASPSP checks the availability of funds on the payer's account,
- The consumer's ASPSP prepares and submits the SCT Inst transaction to the payee's ASPSP.

Step 8

- According to the IPR ([113]), a confirmation message is returned from the merchant's ASPSP to the consumer's ASPSP.
- The merchant's ASPSP makes the funds available to the merchant.

Step 9

- The merchant is notified by its MSCT service provider (information provided by the consumer's ASPSP) that their account has been credited.
- According to the IPR ([113]), the consumer is notified by its ASPSP that the payment has been successfully executed.

Analysis MSCT Use case C2B-A	
Interoperability	• The consumer's ASPSP and the merchant's ASPSP need to have contractual agreements with their respective MSCT services. • For a SEPA-wide interoperability, a framework needs to be specified that interconnects the two MSCT service providers. More details about the technical interoperability functions that this framework would need to implement are presented in Section 10.
Challenges	• Standardisation of a "QR-code", ensuring the correct payee name/IBAN_merchant link. • Integrity of the QR-code. • Standardisation of merchant transaction identifier.

	The notification message from the merchant ASPSP to the consumer ASPSP (step 8) and from the consumer ASPSP to the consumer (step 9) are mandated by the art 5 a) point 4. c) of the IPR.

Table 4: Analysis MSCT use case C2B-A

Notes:

- The standardisation of the QR-code for payee-presented data and related security aspects are addressed in [12].
- The minimum data elements in the notification messages are specified in Annex 5.

6.3 C2B-B - consumer presented: Payment at a physical POI with consumer-presented QR-code and SCA on a dedicated authentication application

This MSCT use case presents an example of consumer experience whereby their mobile device is used to pay in-store by presenting consumer-presented QR-code to the POI. Hereby a dedicated MSCT Inst application on the mobile device of the consumer is used that they have downloaded from an MSCT service provider into their mobile device.

The consumer authentication is performed through a dedicated Authentication application in the consumer's mobile device[10].

[10] In this case there is a delegated authentication from the consumer's ASPSP to the Authentication service provider which is subject to an agreement between the two entities.

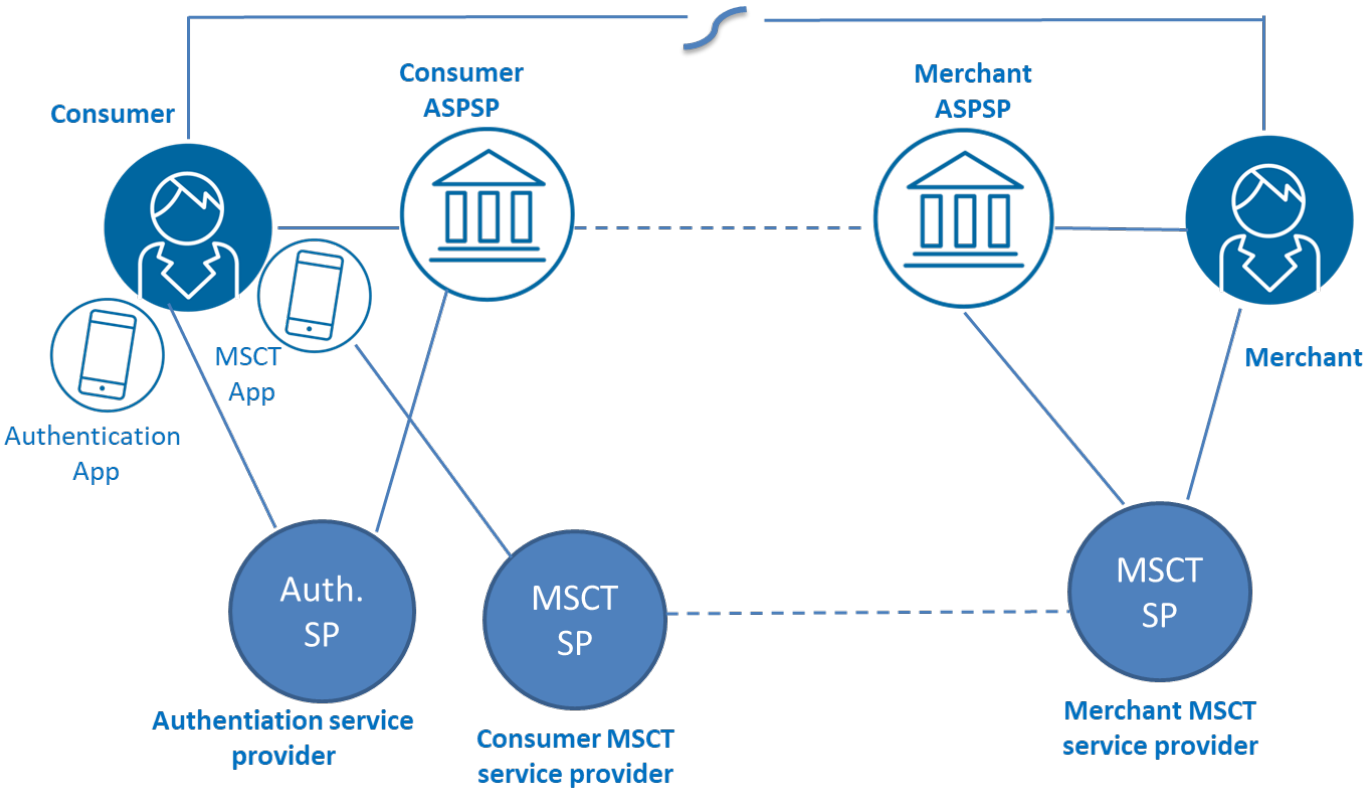


Figure 4: Actors in MSCT Use case C2B-B

Consumer and merchant, may, and frequently will, hold their payment accounts with different ASPSPs. Both ASPSPs are participants different MSCT Inst Services.

Also, the merchant needs to be subscribed to an MSCT Inst service and have downloaded dedicated software on their POI.

In this payment transaction a strong customer authentication in accordance with the relevant PSD2 requirements is performed by a dedicated authentication application. Note that hereby delegation for the consumer authentication needs to be given by the consumer's ASPSP to the Authentication service provider.

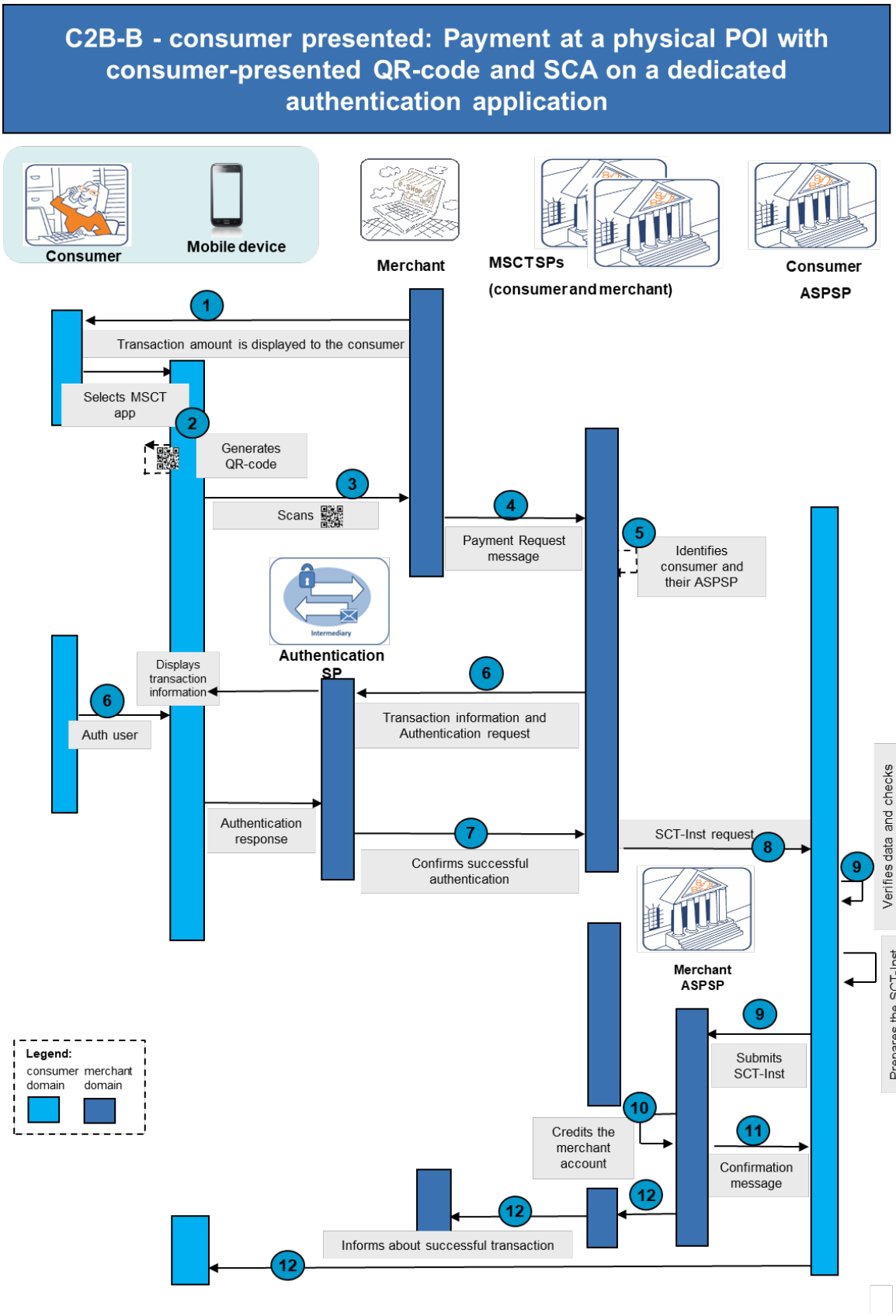


Figure 5: MSCT Use case C2B-B

In the figure above, the following steps are illustrated:

Step 0

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

Step 1

The merchant enters the transaction amount which is displayed on the POI[11].

Step 2

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

Step 3

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

Step 4

The merchant retrieves the consumer's token from the QR-code and sends a payment Request message to their MSCT service provider, including the merchant's name, IBAN_merchant[12], merchant transaction identifier, the transaction amount and the consumer token.

Step 5

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

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

Step 6

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

Step 7

- Upon successful verification, the MSCT service provider is informed by the Authentication service provider.

Step 8

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

Step 9

- The consumer's ASPSP checks the integrity of the SCT Inst instruction.
- The consumer's ASPSP checks the availability of funds on the consumer's account.
- The consumer's ASPSP prepares and submits the SCT Inst transaction to the merchant's ASPSP.

Step 10

The merchant's ASPSP makes the funds available to the merchant.

Step 11

According to the IPR ([113]), a confirmation message is returned from the merchant's ASPSP to the consumer's ASPSP.

Step 12

- The merchant is notified by the MSCT service provider (information provided by the consumer's ASPSP) that their account has been credited.
- According to the IPR ([113]), the consumer is notified by its ASPSP that the payment has been successfully executed.

Analysis MSCT Use case C2B-B	
Interoperability	• The consumer's ASPSP and the merchant's ASPSP need to have contractual agreements with their respective MSCT services. •

	• In a more general approach and a SEPA-wide interoperability, as illustrated above, if the MSCT service provider of the consumer is different from the MSCT service provider of the merchant, a framework needs to be specified that interconnects the two MSCT service providers. More details about the technical interoperability functions that this framework would need to implement are presented in Section 10.
Challenges	• Standardisation of a "QR-code", ensuring the correct payee name/IBAN_merchant link. • Integrity of the QR-code. • Standardisation of merchant transaction identifier. • Standardisation of the reconciliation between the payment transaction and the purchase. • The notification message from the merchant ASPSP to the consumer ASPSP (step 11) and from the consumer ASPSP to the consumer (step 12) are mandated by the art 5a point 4. c) of the IPR ([113]).

Table 5: Analysis MSCT Use case C2B-C

Notes:

- The standardisation of the QR-code for payer-presented data and security related aspects are addressed in EPC024-22.
- The interoperability of MSCTs based on payer-presented data whereby different MSCT service providers are involved for the consumer and merchant is addressed in Section 11.
- The minimum data elements in the payment request and notification messages are defined in Annex 5.

6.4 C2B-C - m-commerce/e-commerce: Payment involving a PISP with redirection to consumer ASPSP for SCA

This use case presents an example of consumer experience whereby a merchant application on their mobile device is used to purchase goods and subsequently pay with an MSCT Inst. For this case it is assumed that the consumer is redirected to the mobile banking app of their ASPSP.

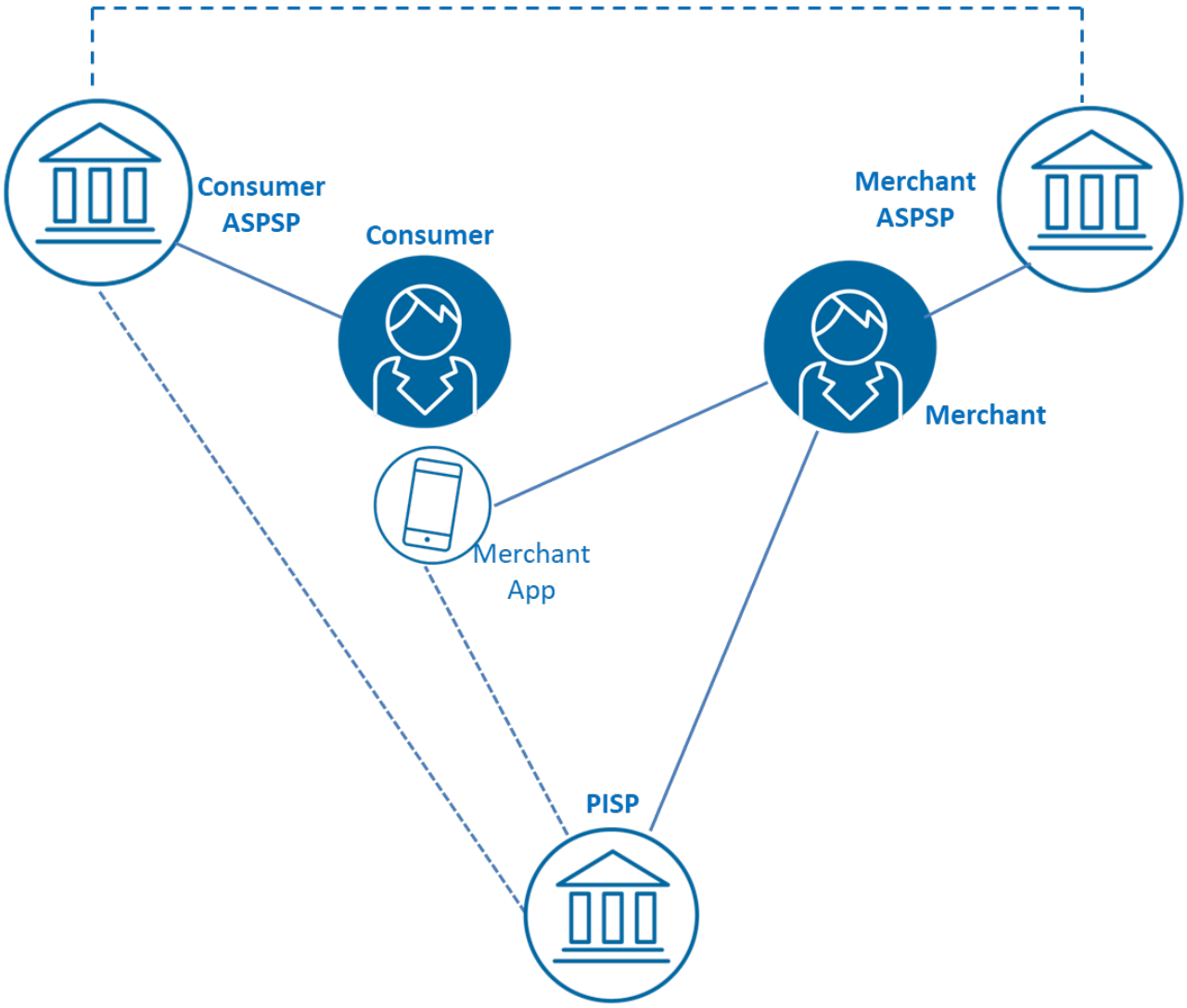


Figure 6: Actors in MSCT use case C2B-C

Consumer and merchant may, and frequently will, hold their payment accounts with different ASPSPs. The consumer have on-boarded with a merchant including their bank account and have downloaded a merchant application on their mobile device. It is assumed that the merchant has a contract with a PISP (= merchant MSCT service provider) that supports the PSD2 API, has downloaded dedicated software on their POI and agreed to make the required PISP information available to the consumer according to the PSD2 Arts. 44 and 45[13].

Furthermore, the consumer is redirected from the merchant application through the PISP to their ASPSP's mobile banking service where a strong customer authentication (see section 8.3 in the MSCT IG) is performed in accordance to PSD2.

[13] See also the EBA answer to Q&A 2020_5573.

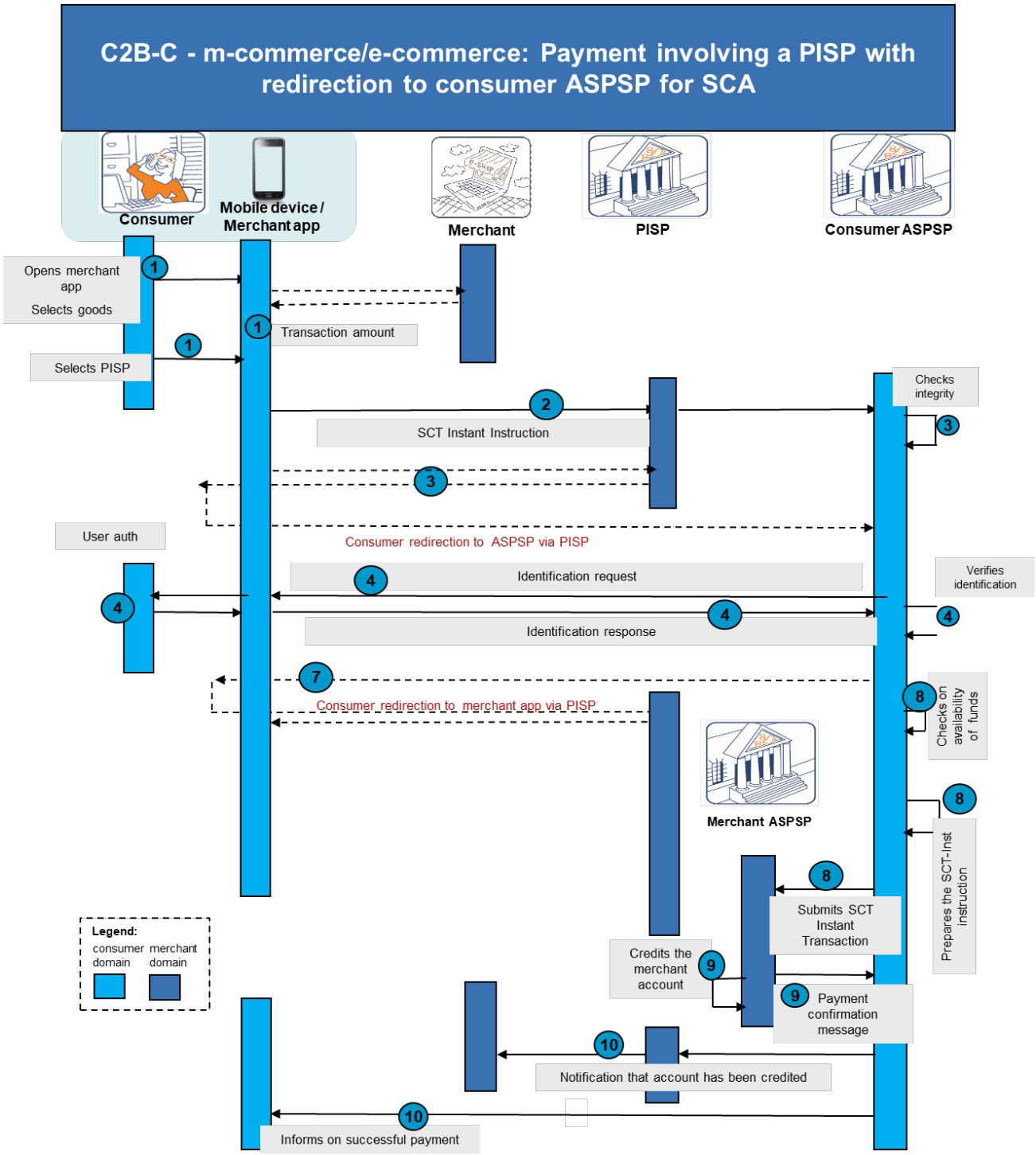


Figure 7: MSCT use case C2B-C

In the figure above, the following steps are illustrated:

Step 0
The merchant needs to have either a contract with a PISP or with a dedicated payment account at a collecting PSP (CPSP) e.g. the merchant's ASPSP.
The PISP has a communication channel to the consumer's ASPSP for PSD2 API (Access to account).
The consumer has downloaded a merchant application on their mobile device and has on-boarded with their account details. The consumer has also downloaded a mobile banking app.
As a prerequisite, a mobile internet connection is required during the purchase.

Step 1
The consumer selects and opens the merchant application, subsequently navigates and selects the goods or services they want to buy. After having accepted the general purchase conditions, they are invited to confirm the purchase.
The checkout section of the merchant application displays the transaction details including the transaction amount and the payment options to the consumer.
The consumer selects their preferred PISP payment solution in this checkout section[14].

Step 2
The PISP initiates an SCT Inst transaction including the transaction amount, the merchant's name, IBAN_merchant and merchant transaction identifier with the consumer's ASPSP.

Step 3
The consumer's ASPSP checks the integrity of the SCT Inst instruction.
The consumer is redirected from the merchant application through the PISP to the mobile banking app of their ASPSP.

Step 4
The transaction details including the transaction amount and merchant name/IBAN_merchant are displayed to the consumer.
The consumer is invited to authenticate and authorise the execution of the payment in accordance with the security policy of their ASPSP.

Step 7
The consumer is redirected back, based on previously received referral information by their ASPSP, via the PISP to the merchant application.

Step 8
The consumer's ASPSP checks the availability of funds on the consumer's account.
The consumer's ASPSP prepares and submits the SCT Inst transaction to the merchant's ASPSP.

Step 9
According to the IPR ([113]), a confirmation message is returned from the merchant's ASPSP to the consumer's ASPSP.
The merchant's ASPSP makes the funds available to the merchant.

Step 10
The merchant is notified by the PISP (information provided by the consumer's ASPSP) that their account has been credited.

[14] Hereby it is assumed that the consumer has been duly informed about the PISP in accordance to PSD2 Arts. 44 and 45.

According to the IPR ([113]), the consumer is notified by its ASPSP that the payment has been successfully executed.

Analysis MSCT Use case C2B-C	
Interoperability	The merchant needs to have a contractual relationship with the PISP. Interoperable due to the underlying SCT Inst scheme Consumer authenticates in "known" on-line banking environment.
Challenges	The PISP needs to connect to # ASPSPs. In view of the lack of an MSCT application and prior on-boarding, the consumer authentication depends on the consumer's ASPSP process. The notification message from the merchant ASPSP to the consumer ASPSP (step 9) and from the consumer ASPSP to the consumer (step 10) are mandated by the art 5a point 4. c) of the IPR.

Table 6: Analysis MSCT use case C2B-C

Notes:
The interoperability of MSCTs involving a PISP is analysed in Section 12.2.
The minimum data elements in the notification messages are defined in Annex 3.

7 Usage of proximity technologies for MSCTs

In this chapter different proximity technologies for the exchange of data between the payer and the payee are outlined. Although various proximity technologies have entered the market over the past years to conduct mobile payments, the most widely used technologies appear to be QR-codes, NFC and BLE. It is noticed that other new technologies such as ultrasonic, BLE beacons, etc., are emerging but the payment market adoption is still in its early days. They have been therefore not further considered by the MSG MSCT and the EPC.

7.1 QR-codes

A two-dimensional code consists of modules arranged in a square pattern on a white background. A Quick Response (QR) code is an example of a 2D code as specified in ISO/IEC 18004 [81]. In the context of MSCTs, the QR-code is used as a means of payment initiation, in one of two modes:

- Payee-presented QR-code - where the code contains data to identify the payee and transaction data;

or

- Payer-presented QR-code – where the code contains data to identify the payer.

In the case of a payee-presented QR-code, the payer needs to have an MSCT application that has the capability of scanning the QR-code of the payee. Typically, from this QR-code the data will be retrieved to enable the initiation of the MSCT using the MSCT application.

In the case of a payer-presented QR-code, the payer can make purchases using data associated with themselves or their account and previously provisioned to their mobile device. This data may range from payer identification data, over credentials to a token which are used to calculate a QR-code (static or dynamic). The consumer typically has to select the QR-code option within their MSCT application, which will result in the display of the QR-code on the mobile device. The QR-code is scanned by the payee at the time of payment to complete the purchase.

The MSG MSCT has developed specifications for QR-codes covering both payee-presented and payer-presented modes. The last version of these specifications was published in January 2023 (see [32]). At the time of writing of this document these specifications are being updated in view of submitting them to CEN, the European standardisation body, to become an European standard.

7.2 NFC and BLE

NFC (Near Field Communication) is a contactless protocol for mobile devices specified by the NFC Forum for multi-market usage and by EMVCo for mobile card payment applications. NFC Forum specifications (see [92]) are based on ISO/IEC 18092 (see [82]) but have been extended for harmonisation with EMVCo and interoperability with ISO/IEC 14443 [79].

Bluetooth is an industry standard according to IEEE 802.15.1 for bidirectional data transmission between devices over relatively short distances using radio technology.

Bluetooth Low Energy (BLE), is a radio technology with which devices in an environment up to about 10 meters can be networked. Compared to "classic" Bluetooth, BLE offers significantly shorter connection times.

The MSG MSCT has developed a guidance document dedicated to the use of NFC and BLE for MSCT payments. It includes detailed descriptions of possible use-cases using these technologies, technical details, security aspects and challenges to be addressed. This document was published in June 2023 (see [34]).

8 Overview of MSCT interoperability aspects

8.1 Introduction

As observed in the majority of the implementations of the MSCTs in the market today, being based on payee- or payer-presented data, the same MSCT service provider, both on the payer and payee side is involved. They are sometimes referred to as a “closed loop” models, whereby both the payer and the payee are customers of the same MSCT service provider. These MSCT models are applicable for P2P, C2B (in this case the payer is a consumer and the payee is a merchant) and B2B (instant) payment contexts and typically cover a certain geography (e.g., within (part of) a country).

8.1.1 Current model for MSCTs based on payee-presented data

In the figure below, the model is depicted for MSCTs based on payee-presented data that are currently in the market, whereby both the payer and payee are customers of the same MSCT service provider.

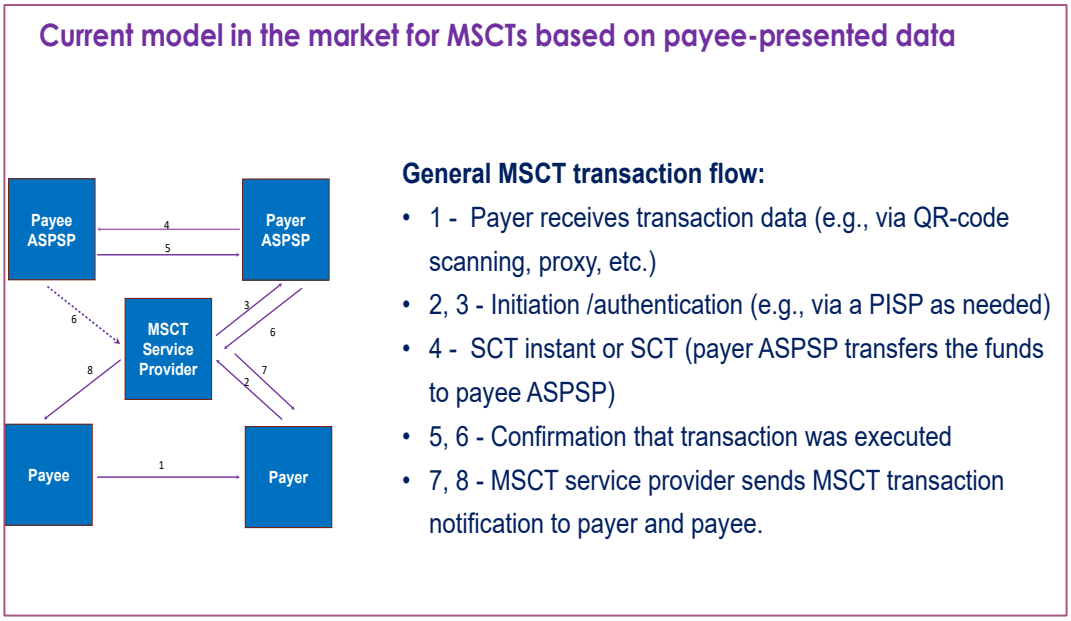


Figure 8: Model for MSCTs based on payee-presented data

Note: The dotted line between the MSCT service provider and the payee ASPSP means that for some MSCT services, this link may be present, in others there is no link.

In order to achieve interoperability for MSCTs, the main issue is how to interconnect these different (closed loop) MSCT services as illustrated in the figure below.

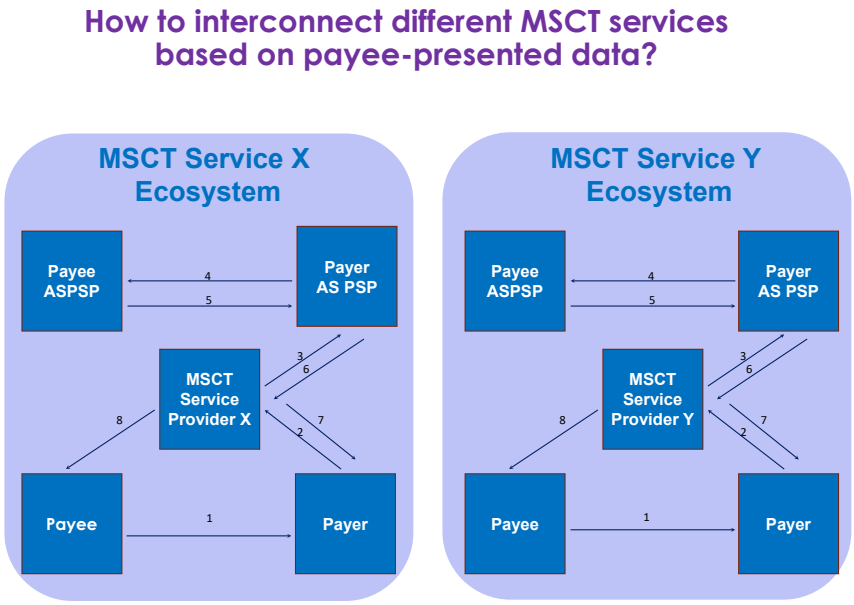


Figure 9: How to interconnect different MSCT services based on payee-presented data?

8.1.2 Current model for MSCTs based on payer-presented data

In the figure below, the model is depicted for MSCTs based on payer-presented data that are currently in the market, whereby both the payer and payee are customers of the same MSCT service provider.

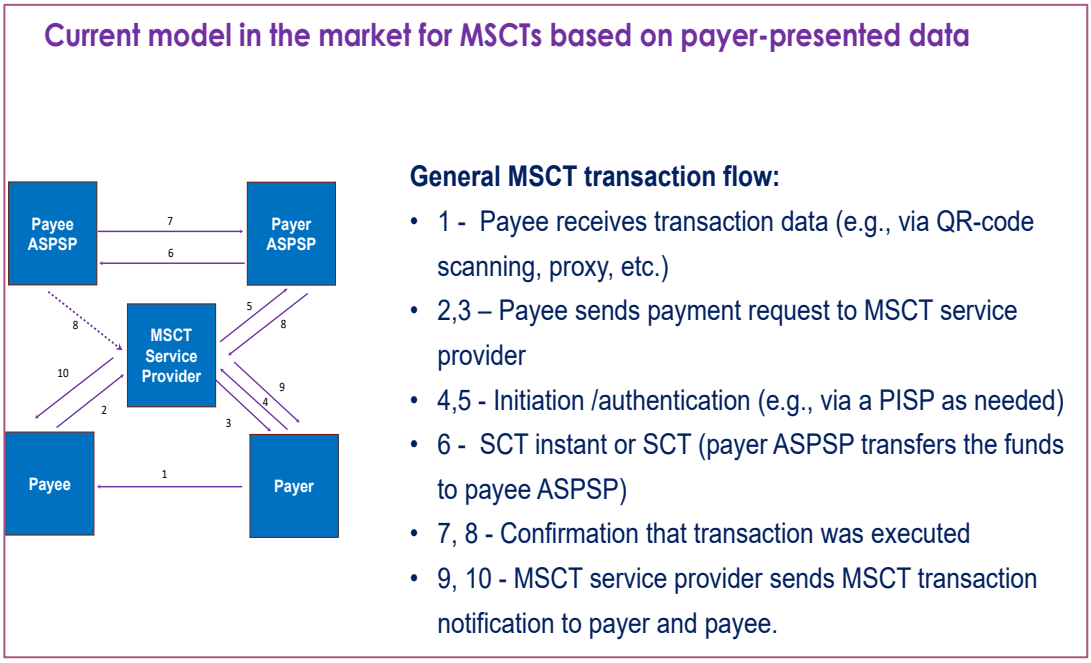


Figure 10: Model for MSCTs based on payer-presented data

Note: The dotted line between the MSCT service provider and the payee ASPSP means that for some MSCT services, this link may be present, in others there is no link.

In order to achieve interoperability for MSCTs, the main issue is how to interconnect these different (closed loop) MSCT services as illustrated in the figure below.

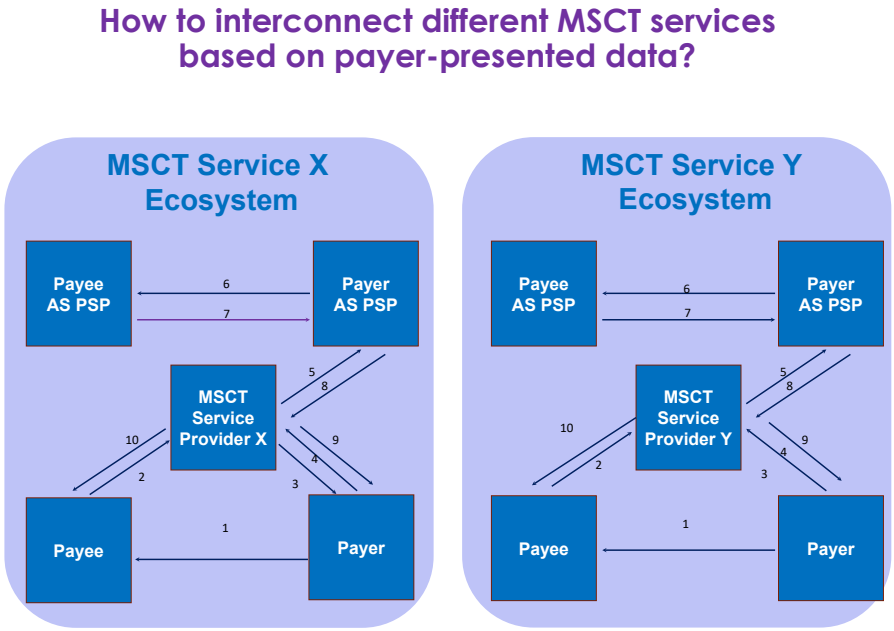


Figure 11: How to interconnect different MSCT services based on payer-presented data?

8.2 MSCT interoperability analysis

In this section a brief analysis will be performed on the main interoperability aspects for MSCTs. For both models, the MSCT service provider X is already connected to the payer's ASPSP. The interconnection between the Payer's ASPSP and Payee's ASPSP needed during the execution of the Instant SCT or SCT transfer[15], to ensure interoperability across SEPA, is already covered in the SCT Inst and SCT rulebooks (See [4] and [8] respectively)).

As a consequence, this document will focus for an MSCT transaction on what is referred to in **Figure 3** as *Payment Preparation (or prepayment), Initiation and Authentication* and *Payment Completion* phases related to an Instant SCT or SCT transaction.

8.2.1 Person-to-Person (P2P) MSCTs

P2P payments are mostly based on payee-presented data. For these MSCTs, the interoperability between the different P2P MSCT solutions, when a proxy is used for the payee such as a mobile phone number or e-mail address, the interoperability should be ensured by the implementation of proxy-lookup services. These services should ensure the return of the payee's IBAN for the proxy.

The implementation and success of such services is crucial for ensuring a SEPA-wide interoperability for these P2P MSCT payments.

[15] This means after the transaction has been sent by the payer's ASPSP following the receipt of the SCT Inst or SCT initiation request and the subsequent authentication of/confirmation by the payer.

For P2Ps based on payer-presented data, a payment request message from the payee will be involved – a further analysis is conducted in Chapter10.

8.2.2 Customer-to-Business (C2B) MSCTs

As said before, most current market solutions are all based on the models depicted in whereby both the payer and the payee have on-boarded (registered) with the same MSCT service provider.

To achieve technical SEPA-wide interoperability, by connecting multiple existing MSCT solutions, two main areas would need to be addressed:

- How to "standardise" the transfer of merchant/transaction data to the consumer – ideally, independently of the technology, while ensuring the security of the link merchant name – IBAN_merchant?

- How to interconnect the MSCT service provider back-end systems so that when a consumer that is on-boarded with MSCT service "X" can make a purchase with a merchant that takes part in MSCT service "Y"?

8.2.3 Business-to-Business (B2B) MSCTs

For B2B, the reconciliation on the payee side appears to be a major issue – more in particular for SCT Inst payments; although it should be recognised that this problem reaches obviously beyond MSCTs. Immediate information on the incoming payments, processed by the payee's ASPSP (individual transaction, push) or on request by the corporate (individual transaction, pull) are strongly demanded features in view of the usability of SCT Inst by corporates. With SCT Inst, the EPC has defined messages from initiator to ASPSP, from ASPSP to ASPSP (pacs.008) and ASPSP to initiator but not from ASPSP to payee. Corporates would like to see an immediate "ASPSP to payee message" in the context of SCT Inst closing the chain of information from initiator to payee.

In addition, for all payment contexts described, and as already mentioned in section 8.7, the following *acknowledgement and notification messages* have been identified as being key factors for market adoption:

- Acknowledgement of receipt to the payer by their MSCT service provider of the instruction for an MSCT based on SCT involving payee-presented data;
- Acknowledgement of receipt to the payee by their MSCT service provider of the payment request message for MSCTs based on SCT involving payer-presented data
- Notification of reject/successful/unsuccessful transaction to the payee by their MSCT service provider;
- Notification of reject/successful/unsuccessful transaction to the payer by their MSCT service provider or their ASPSP.

The interoperability aspects related to these messages will be further analysed in the Chapters 9 and 10.

8.3 MSCT interoperability layers

8.3.1 Introduction

The different technical interoperability aspects described in the previous sections could be represented in a 3-layer approach as shown in the figure below. Since the interoperability in the inter-PSP space is already covered in the respective scheme rulebooks, this document will focus on the interoperability aspects related to MSCTs in the PSU and MSCT service provider layers as depicted in the figure below.

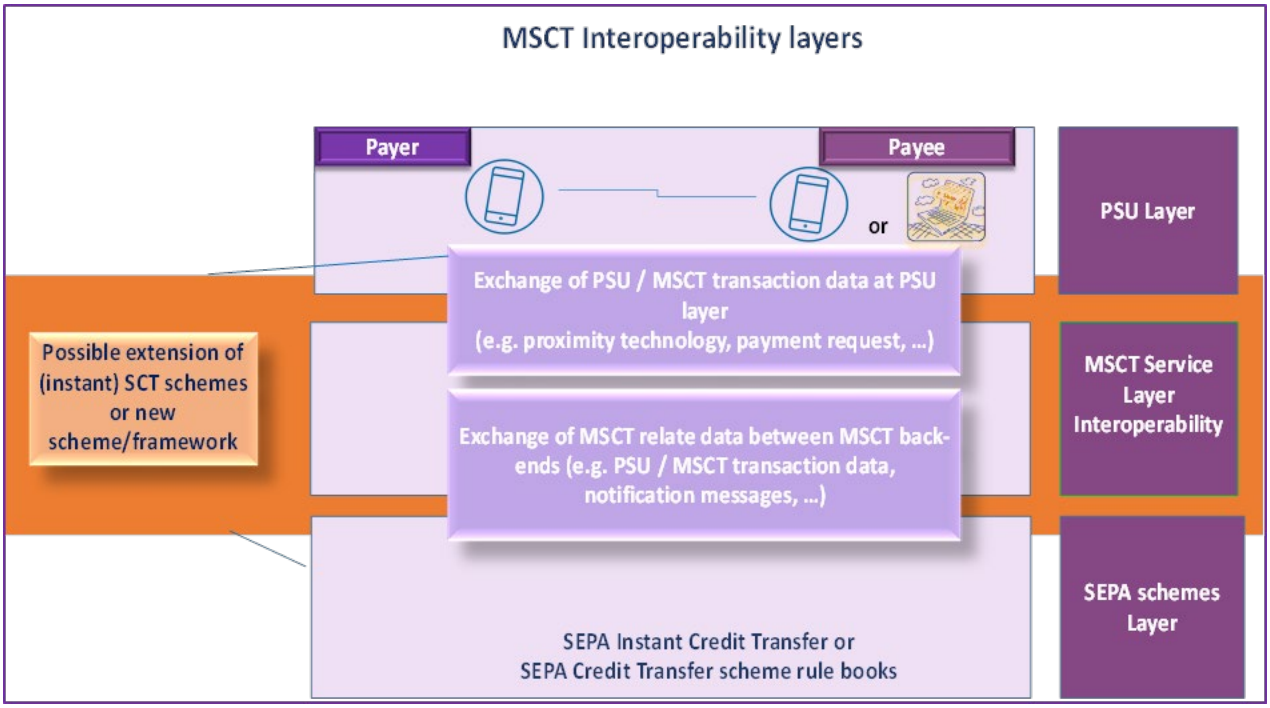


Figure 12: MSCT interoperability layers

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

8.3.2 PSU layer

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

In case the payee's name, IBAN and transaction amount are known/ entered on the mobile device by the payer, the respective SCT Inst and SCT schemes would ensure interoperability for MSCTs. In all other cases, e.g. if proximity technologies, payment request messages, proxies or tokens are used to exchange this data, interoperability issues arise. Those issues will be further analysed in Chapters 18 and 19.

8.3.3 MSCT service layer

The interoperability solutions at this layer will depend on the type of PSU/transaction data that has been exchanged between the payer and payee at the PSU layer.

In case, the full PSU/transaction data needed for the initiation of an SCT Inst or SCT is exchanged directly in clear between the payee and the payer, the MSCT transaction can be immediately initiated by the payer while the SCT Inst and SCT scheme rules ensure the interoperability.

In case the transaction data exchanged contains a token or proxy, the corresponding transaction data in clear-text needs to be retrieved via the appropriate entity (e.g. payer's or payee's MSCT service provider) before the MSCT transaction can be initiated. Moreover, the appropriate transaction data including the payee name / trade name / IBAN and transaction amount need to be displayed to the consumer for authentication of the MSCT transaction. This means that dedicated messages will need to be exchanged between the MSCT service provider back-ends to cover for these functionalities.

Also the infrastructure needed to exchange the notification messages[16] to the payer and payee (see sections 5.2 and 8.2) would need to be developed as well as the standardisation of the minimum data elements required in the message flows between MSCT service providers (see Chapter 11).

8.4 MSCT interoperability model based on a HUB

To achieve MSCT interoperability for a generic basic 4-corner model, the concept of a HUB is introduced in this document to interconnect the respective MSCT service providers as shown in the figure below.

[16]Currently the SCT Inst Scheme rulebook only requires the transmission of the negative confirmation message as notification by the payer's ASPSP to the payer (see [20]). The IPR ([113]) mandates the notification from the payee's ASPSP to the payer's ASPSP (art. 5.a) 4.c.) and from the payer's ASPSP to the payer and where applicable, to the PISP art. 5.a) 4.e).

Hereby it is assumed that both payer and payee have different ASPSPs that are SCT Inst or SCT scheme participants according to the rulebooks of these schemes, while the entities assuming the role of MSCT service provider are depicted as separate entities that are different for the payer and the payee.

The term HUB is used to indicate an "infrastructure" that enables interconnectivity between the respective 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)).

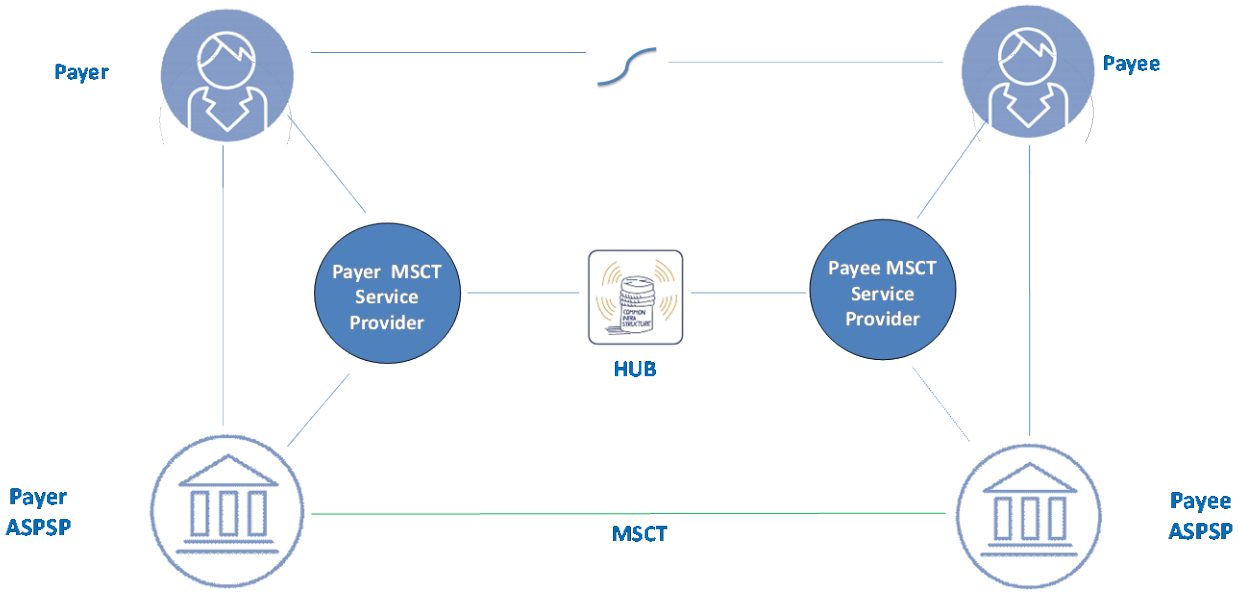


Figure 13: Generic 4-corner MSCT interoperability model

Obviously, if the role of MSCT service provider would be assumed by an ASPSP the model below would simplify. Alternatively, if multiple PSPs (such as a PISP licensed under PSD2 or a Collecting PSP on behalf of the merchant (CPSP)) would be involved between the PSU and their MSCT service provider / ASPSP, this model might become more complex.

Note: The payer's MSCT service provider is linked to the payer's ASPSP and the payee's MSCT service provider may[17] be linked to the payee's ASPSP (this linkage may include both technical and contractual aspects).

The forthcoming chapters specify the requirements on the HUB to achieve interoperability of MSCTs, respectively for MSCTs based on payee-presented data (Chapter 9) and payer-presented data (Chapter 10). The models involving a PISP or CPSP are analysed in Chapter 12.

[17] represented by a dotted line.

9 Technical interoperability of MSCTs based on payee-presented data

9.1 Introduction

This chapter analyses in more detail the interoperability of MSCTs based on payee-presented data. As mentioned before it focuses on the interoperability of MSCTs at the PSU layer and the MSCT service (provider) layer. Hereby two main functionalities will be covered:

- The exchange of the transaction data that enables the initiation of the MSCT;
- The acknowledgement/notification messages sent to the payer and payee after a successful/unsuccessful transaction or a reject.

Next to the specification of the MSCT interoperability requirements for the HUB, based on the generic 4-corner model, illustration of transaction process flows involving the HUB for successful transactions, rejects and unsuccessful transactions are included.

The chapter further defines the minimum data set to be exchanged between payee and payer for this type of MSCTs and specifies a payee-presented QR-code for MSCTs, followed by some examples of payload data for this QR-code.

9.2 Exchange of MSCT data

With respect to the availability of the transaction data (payee data and payment data) needed by the payer for the initiation of the MSCT transaction the following cases need to be considered:

- *Part of the payee data is not known by the payer and a proxy is used* instead (e.g., for P2P payment, a mobile phone number is used as a proxy instead of an IBAN): in this case, the MSCT service provider of the payer needs to be able to retrieve the payee's IBAN/name from the proxy used. This generally requires the support of the payee's MSCT service provider and/or ASPSP.

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

  Hereby the following distinctions need to be made:
  - The payee-presented data includes a "token": in this case, a de-tokenisation process needs to take place such that the transaction data can be derived from the token and provided to the payer via their MSCT service provider. This generally requires the support of the payee's MSCT service provider (see *Transaction information request*/*Transaction information response* messages in section below) prior to the initiation of the MSCT transaction.
  - Only part of the transaction data is exchanged between the payee and the payer through a proximity technology or only part of the transaction data exchanged is in clear (e.g., the payee-presented data contains a proxy). In this case the complete transaction data needs to be provided by the payee's MSCT service provider upon request from the payer's MSCT service provider (see *Transaction information*

request/Transaction information response messages in section 18.5 below) prior to the initiation of the MSCT transaction.

- The payee-presented data includes all transaction data in "clear" (e.g. the payee's name, trade name, IBAN of the payee, transaction amount, transaction identifier, etc.). This enables the immediate initiation of the MSCT transaction.

Next to these 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.

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

From the analysis made above, requirements can be derived for the HUB to support the transaction data exchange needed for the interoperability of MSCTs based on payee-presented data. The table below list the required functionalities for the HUB for this exchange of transaction data

MSCT transaction feature	Requirements on HUB
Exchange of transaction data Payment Preparation phase (see Figure 3)	**MSCTs based on SCT Inst or on SCT**
Payee-presented transaction data includes a token (It is hereby assumed that the tokenisation/de-tokenisation is handled by or via the payee's MSCT service provider)	De-tokenisation into transaction data is needed *Transaction information request* and *Transaction information response* messages between MSCT service providers
Payee-presented transaction data is incomplete, i.e. a proxy is used for the payee identification data	Translation of proxy into payee's name and IBAN *Transaction information request* and *Transaction Information response* messages between MSCT service providers
All transaction data is available "in clear" to the payer (e.g. in clear in QR-code or known to the payer) [18]	Not applicable

Table 7: Required HUB functionalities for exchange of transaction data for MSCTs based on payee-presented data

9.3 Acknowledgement/notification messages

The following messages have already been identified in sections 5.2 and 8.2 in this respect:

[18] In this case, another mechanism would need to be implemented to ensure the integrity of the data.

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

Note: The acknowledgement of receipt of the SCT Inst instruction to the payer is not considered in view of the immediacy of the MSCT transaction.

9.3.1 Acknowledgement of receipt of MSCT instruction based on SCT to the payer

For MSCTs that are based on SCT[19], where there is no immediacy of payment, it might be useful for the payer to receive a confirmation that the MSCT instruction has been well-received by their MSCT service provider. However, since this acknowledgement message is not impacting the interoperability of MSCTs because it is in the payer-to-payer ASPSP space, it will not be further discussed in this document.

9.3.2 Notifications of successful MSCT transactions

This section describes the *notification of successful transaction* messages that need to be supported to duly inform the payee and the payer for MSCTs based on payee-presented data.

A. MSCTs based on SCT Inst

Notification to payee

For all payment contexts, the *notification to the payee* about a *successful MSCT transaction based on SCT Inst* (i.e. after the receipt of the confirmation by the payer's ASPSP from its CSM as indicated in the SCT Inst transaction process flow in the SCT Inst rulebook) requires the following messages to be supported:

Notification to payee **Successful transactions for MSCTs based on SCT Inst with payee-presented data**
1. *Notification of successful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification successful transaction* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification successful transaction* by the payee MSCT service provider to the payee. Or *Notification of successful transaction* by the payee ASPSP to the payee (for specific cases only).

[19] For MSCTs based on SCT Inst, this acknowledgement is not needed in view of the immediacy of the payment.

Table 8: Overview of messages for notification to payee of successful MSCTs based on SCT Inst with payee-presented data

Notification to payer

For all payment contexts, the *notification to the payer* about a *successful MSCT transaction based on SCT Inst* (i.e. after the receipt of the confirmation 6 by the payer's ASPSP in Figure 1) requires the following messages to be supported:

Notification to payer **Successful transactions for MSCTs based on SCT Inst with payee-presented data**
1. *Notification of successful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of successful transaction* by the payer MSCT service provider to the payer. Or Notification by the payer ASPSP to the payer, as stipulated by the art. 5 of the IPR (see [113]).

Table 9: Overview of messages for notification to payer of successful MSCTs based on SCT Inst with payee-presented data

B. MSCTs based on SCT

Notification to payee

For all payment contexts, the *notification to the payee* about a *successful initiation* of an *MSCT transaction based on SCT* (i.e. after the transfer of the SCT transaction message by the payer's ASPSP to the payee's ASPSP as indicated in the SCT transaction process flow in the SCT rulebook) requires the following messages to be supported:

Notification to payee **Successful transaction initiation for MSCTs based on SCT with payee-presented data**
1. *Notification of successful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification successful transaction* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification successful transaction* by the payee MSCT service provider to the payee. Or *Notification of successful transaction* by the payee ASPSP to the payee (for specific cases only).

Table 10: Overview of messages for notification to payee of successful MSCTs based on SCT with payee-presented data

Notification to payer

For all payment contexts, the *notification to the payer* about a *successful MSCT transaction based on SCT* (i.e. after the receipt of the confirmation 6 by the payer's ASPSP in Figure 2) requires the following messages to be supported:

Notification to payer **Successful transactions for MSCTs based on SCT Inst with payee-presented data**
1. *Notification of successful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of successful transaction* by the payer MSCT service provider to the payer. Or Notification by the payer ASPSP to the payer, as stipulated by the art. 5 of the IPR (see [113]).

Table 11: Overview of messages for notification to payer of successful MSCTs based on SCT with payee-presented data

For MSCTs based on SCT, also a guarantee of payment[20] could be considered, but falls outside the scope of this document.

From the analysis made above, requirements can be derived for the HUB to support the notification of successful transactions needed for the interoperability of MSCTs based on payee-presented data. The table below list the required functionalities for the HUB for this.

MSCT transaction feature	**Requirements on HUB**	
Notification messages Payment Completion phase, (see Figure 3)	**SCT Inst**	**SCT**
Notification to payee about successful transaction	Notification from payer's MSCT service provider to payee's MSCT service provider	Notification from payer's MSCT service provider to payee's MSCT service provider

[20] This could potentially be addressed by a dedicated MSCT interoperability framework.

Notification to payer about successful transaction	Not applicable	Not applicable

Table 12: Required HUB functionalities for notification of successful transactions for MSCTs based on payee-presented data

9.3.3 Notifications of unsuccessful transactions and rejects for MSCTs

A. MSCTs based on SCT Inst

For MSCTs with payee-presented data based on SCT Inst, the following categories for rejects and unsuccessful transactions could be distinguished.

Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payee-presented data	
Cat 1	Reject by the payer MSCT service provider (before initiation to payer ASPSP)
Cat 2	Reject by payer ASPSP before execution of the SCT Inst (i.e. before sending the SCT Inst transaction by the payer ASPSP to its CSM)
Cat 3	Unsuccessful transaction - receipt by the payer ASPSP of negative confirmation message from its CSM.

Table 13: Overview of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data

Annex 2 provides an overview on MSCT related errors based on payee-presented data with a mapping on the three categories mentioned above.

The messages in the inter-PSP space related to these *rejects* and *unsuccessful transactions* have been specified in the SCT Inst scheme rulebook [8] and the SCT Instant interbank implementation guidelines [9].

Notification to payee

For all payment contexts, the *notification to the payee* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payee **Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payee-presented data**	
Cat 1	1. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 2. *Notification of reject* by the payee MSCT service provider to the payee.

Cat 2	1. *Notification of reject* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification of reject* by the payee MSCT service provider to the payee.
Cat 3	1. *Notification of unsuccessful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification unsuccessful transaction* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification unsuccessful transaction* by the payee MSCT service provider to the payee. Or *Notification of unsuccessful transaction* by the payee ASPSP to the payee (for specific cases only).

Table 14: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data

***Notification to payer**

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payer **Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payee-presented data**	
Cat 1	*Notification of reject* by the payer MSCT service provider to the payer.
Cat 2	1. *Notification of reject* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of reject* by the payer MSCT service provider to the payer.
Cat 3	1. *Notification of unsuccessful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of unsuccessful transaction* by the payer MSCT service provider to the payer.

Table 15: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data

B. MSCTs based on SCT

For MSCTs with payee-presented data based on SCT, the following categories for rejects and unsuccessful transactions could be distinguished.

Rejects and unsuccessful transactions for MSCTs based on SCT with payee-presented data	
Cat 1	Reject by the payer MSCT service provider (before initiation to payer ASPSP)
Cat 2	Reject by payer ASPSP before execution of the SCT (i.e. before sending the SCT transaction by the payer ASPSP to its CSM)
Cat 3	Unsuccessful transaction - receipt by the payer ASPSP of a "Reject" or "Return" message[21] (see DS-03 in the SCT scheme rulebook)

Table 16: Overview of rejects and unsuccessful MSCTs based on SCT with payee-presented data

Note: For MSCTs based on SCT transactions, the notification messages for unsuccessful transactions after the receipt of a "Return" may only be sent up to three days after the settlement date (Cat 3 in the table above).

Annex 2 provides an overview on errors with MSCTs based on payee-presented data with a mapping on the three categories mentioned above.

The messages in the inter-PSP space related to these *rejects and returns* have been specified in the SCT scheme rule book [4] and the SCT interbank implementation guidelines [5].

Notification to payee

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payee Rejects and unsuccessful transactions for MSCTs based on SCT with payee-presented data	
Cat 1	1. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 2. *Notification of reject* by the payee MSCT service provider to the payee.
Cat 2	1. *Notification of reject* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification of reject* by the payee MSCT service provider to the payee.
Cat 3	1. *Notification of unsuccessful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification unsuccessful transaction* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification unsuccessful transaction* by the payee MSCT service provider to the payee.

[21] Note that a "Return" may be up to three days after the settlement date.

	Or *Notification of unsuccessful transaction* by the payee ASPSP to the payee (for specific cases only).

Table 17: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT with payee-presented data

Notification to payer

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payer **Rejects and unsuccessful transactions for MSCTs based on SCT with payee-presented data**	
Cat 1	*Notification of reject* by the payer MSCT service provider to the payer.
Cat 2	1. *Notification of reject* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of reject* by the payer MSCT service provider to the payer.
Cat 3	1. *Notification of unsuccessful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of unsuccessful transaction* by the payer MSCT service provider to the payer.

Table 18: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payee-presented data

From the analysis made above, requirements can be derived for the HUB to support the notification of unsuccessful transactions and rejects needed for the interoperability of MSCTs based on payee-presented data. The table below list the required functionalities for the HUB for this.

MSCT transaction feature	Requirements on HUB
Notification messages	**MSCTs based on payee-presented data**
	SCT Inst or SCT
Notification of reject to payee (Table 21 and Table 24: Cat 1 and 2)	*Notification of reject* message by payer MSCT service provider to payee MSCT service provider
Notification of unsuccessful transaction to payee (Table 21 and Table 24: Cat 3)	*Notification of unsuccessful transaction* message by payer MSCT service provider to payee MSCT service provider
Notification of reject to payer (Table 22 and Table 25: Cat 1 and 2)	Not applicable
Notification of unsuccessful transaction to payer	Not applicable

(Table 22 and Table 25: Cat 3)	

Table 19: Required HUB functionalities for unsuccessful transactions and rejects for MSCTs based on payee-presented data

9.4 Interoperability process flows for MSCTs based on payee-presented data

9.4.1 Introduction

In this section the full process flows between the HUB and respective MSCT service provider back-ends for a few examples will be described. These examples are provided for illustrative purposes only. Note that as mentioned before, an MSCT service provider could be an ASPSP. This means that in the process flows below, one or both MSCT providers could be one or both of the respective ASPSPs in which case the process flows would simplify.

Two illustrative cases will be considered as listed in the table below.

MSCT transactions	Support from the HUB[22]	Reference
C2B – successful MSCT based on SCT Inst Merchant-presented QR-code contains a token	• Retrieval of the transaction data from the token (see section 9.2) • Conditional transaction lock messages (see below) • Notification of successful transaction (see section 9.3)	Section 9.4.2
C2B - reject by the payer's (consumer) ASPSP for MSCT based on SCT Inst Merchant-presented QR-code including a token (Table 20: Cat 1)	• Retrieval of the transaction data from the token (see section 9.2) • Notification of reject (see section9.3)	Section 9.4.3

Table 20: Illustrative process flows for interoperability of MSCT transactions based on payee-presented data with mapping onto HUB functionalities

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

A *conditional transaction lock function* is defined as follows. The function consists of conditional lock transaction messages that are sent between the consumer's MSCT service provider and the merchant's MSCT service provider via the HUB to prevent that multiple consumers from different MSCT service providers pay the same transaction after strong customer authentication (see section

[22] Depicted by the green arrows in the illustrative process flows below.

8.3). The transaction lock function is required in case the QR-code stays active for a certain time window that would enable multiple scans and related payments and its need is specified in the dedicated Lock Transaction Indicator (LT Indicator as defined in section 18.6 in this document). If two consumers would perform SCA on the same transaction, the consumer with successful SCA for which the lock function sent by their MSCT service provider reaches as first the MSCT service provider of the merchant is the one for which the transaction is locked.

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

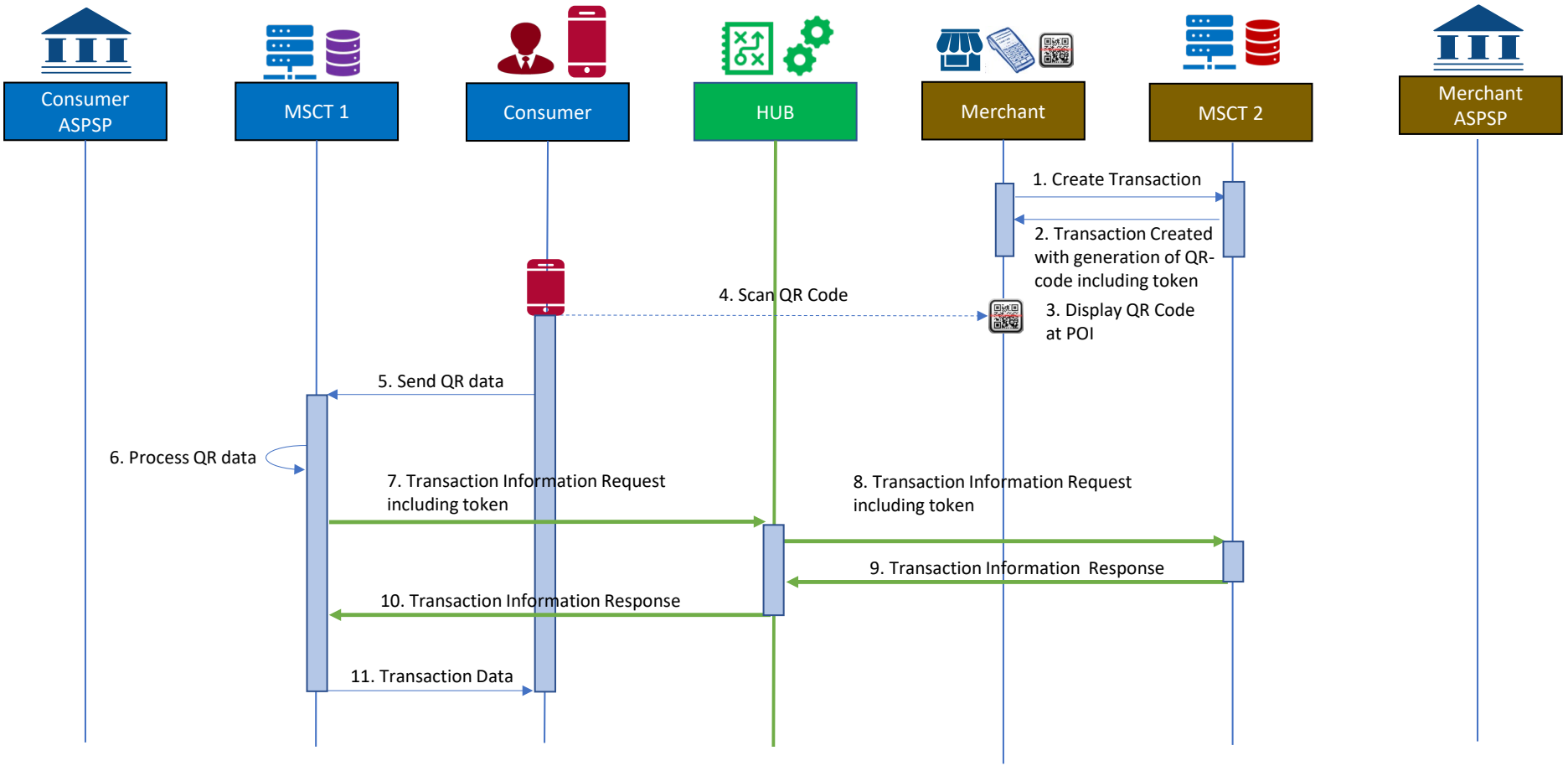
Note also that in the process flows below, the representation and description of strong customer authentication (SCA) is simplified since the focus is on the interconnectivity between the respective MSCT service providers.

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

9.4.2 Successful MSCT - C2B based on SCT Inst with merchant-presented QR-code containing a token

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

In this case the actors and process steps are depicted in Section 6 (use case C2B-A).
The detailed process flows between the different actors involved for this MSCT transaction type are shown in the next figure.


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

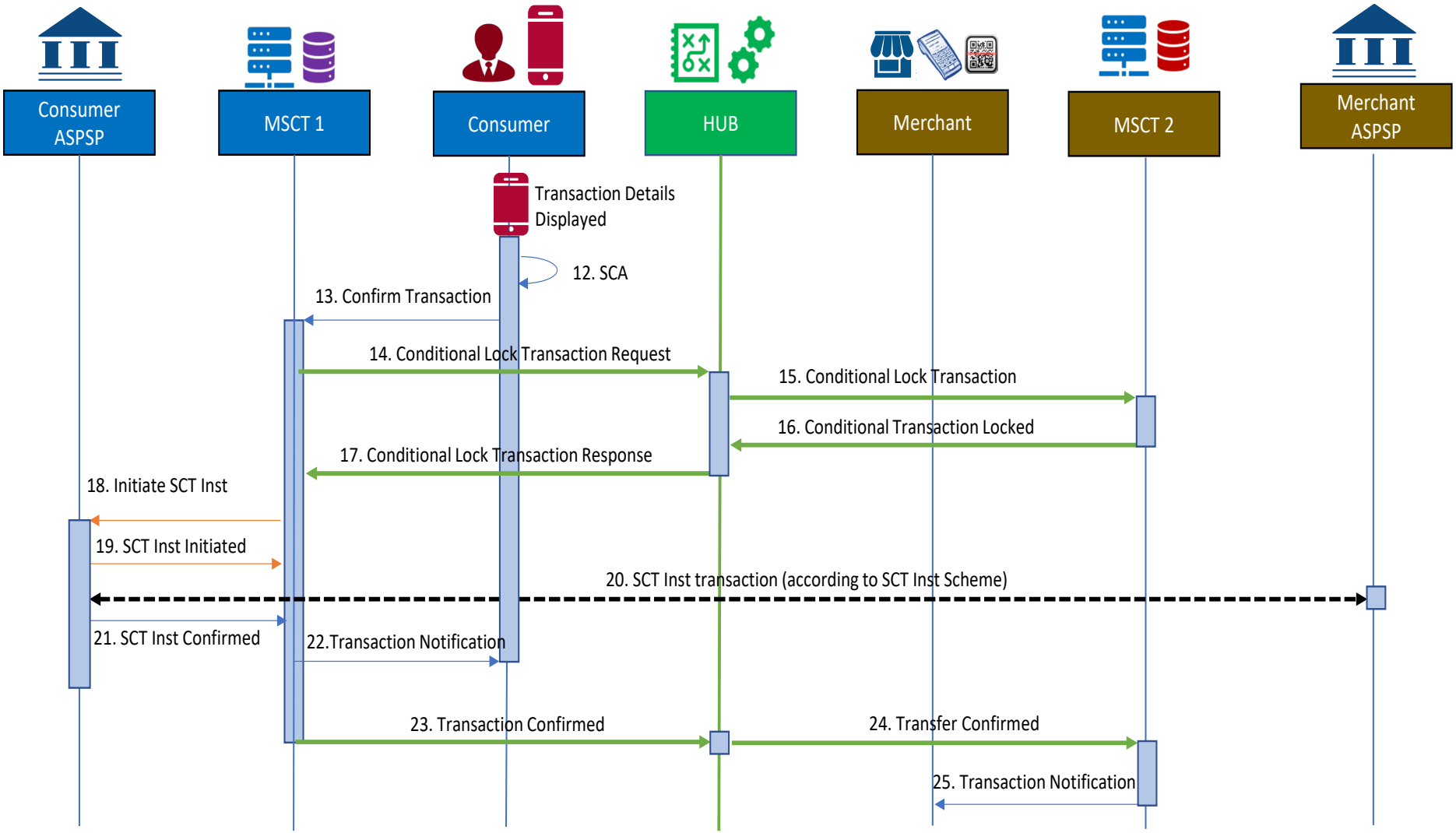


Figure 14: Process flow – C2B – merchant-presented QR-code with token

In the figure above the following steps are involved:

Step 1:

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

Step 2:

The merchant's MSCT service provider returns a QR-code including a dedicated token based on the transaction details (transaction amount, IBAN_merchant, transaction identifier) and their MSCT service provider identifier to the merchant.[23]

Step 3:

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

Step 4:

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

Step 5:

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

Step 6:

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

Step 7:

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

Step 8:

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

Step 9:

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

Step 10:

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

Step 11:

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

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

Step 12:

The consumer performs an SCA on the transaction details displayed.

Step 13:

The confirmation including the authentication response is provided to the consumer's MSCT service provider.[24]

Step 14 (conditional)[25]:

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.

Step 22:

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

Step 23:

[24] This description assumes that the consumer's MSCT service provider has received delegation from the consumer's ASPSP for SCA. Otherwise additional steps are needed for the SCA as described in Chapter 7.
[25] See sections 18.5.1 and 18.6. In case the LT Indicator does not require a lock transaction function, steps 14 through 17 will not be present.

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.

9.4.3 Reject by the payer's ASPSP – C2B based on SCT Inst with merchant-presented QR-code containing a token

The process flow below illustrates the usage of the HUB in the case of a reject by the consumer's (payer) ASPSP for an MSCT based on merchant-presented data using a QR-code including a token. It is hereby assumed that the tokenisation/de-tokenisation of (part of) the transaction data is handled by or via the merchant MSCT service provider. In this illustration it is assumed that the consumer's ASPSP rejects the MSCT (e.g. due to insufficient funds on the payment account or authentication issues).

In this MSCT transaction type, the actors and process steps are depicted in Section 6 – use case C2B-A.

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

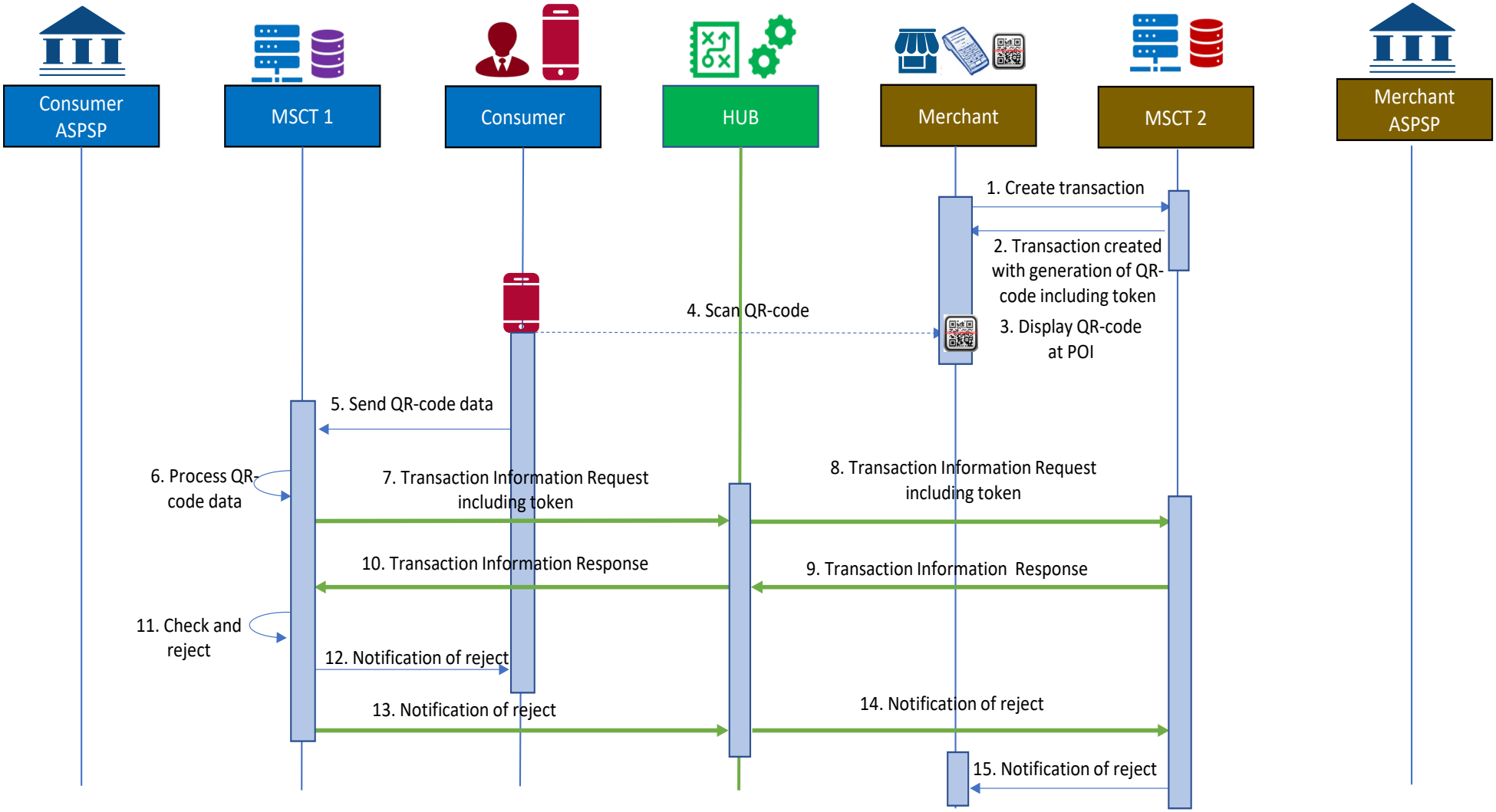


Figure 15: Process flow – C2B – Reject by consumer MSCT service provider for MSCT based on merchant-presented QR-code with token

In the figure above the following steps are involved:

Step 1:

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

Step 2:

The merchant MSCT service provider returns a QR-code including a dedicated token based on the transaction details (transaction amount, IBAN_merchant, name/trade name merchant, transaction identifier) and their MSCT service provider identifier to the merchant.[26]

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 merchant MSCT service provider identifier, is retrieved from the QR-code and provided to the consumer MSCT service provider.

Step 6:

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

Step 7:

The Transaction Information Request including the merchant MSCT service provider identifier is sent to the HUB.

Step 8:

The HUB identifies the merchant MSCT service provider and forwards them the Transaction Information request.

Step 9:

The merchant MSCT service provider checks the request, prepares the response and sends a Transaction Information Response to the HUB.

Step 10:

The HUB forwards the Transaction Information Response to the consumer MSCT service provider.

Step 11:

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

The consumer MSCT service provider retrieves the transaction details from the Transaction Information Response and notices that the information is “invalid” or “incomplete” so that they cannot proceed with the transaction.

Step 12:

The consumer MSCT service provider sends a notification of reject to the consumer.

Step 13:

The consumer MSCT service provider sends a notification of reject to the HUB to the HUB with the merchant MSCT service provider identifier.

Step 14:

The HUB forwards the notification of reject to the merchants MSCT service provider.

Step 15:

The merchant MSCT service provider sends the notification of reject to the merchant.

9.5 Minimum data set for MSCTs based on payee-presented data

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

The minimum data set to be exchanged between the payee and the payer, will rely on the MSCT transaction feature, such as described in Table 14 in section 18.2 in this document:

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

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

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

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

For case 1 above: *the payee-presented transaction data includes a token:* [Version]+[Type]+ [Payee MSCT Service Provider ID] + [token]

For case 2 above: *the payer uses a proxy for the payee:* [Version]+[Type]+ [Payee MSCT Service Provider ID] + [proxy] + [a clear-text name/value string] For case 3 above: *transaction data is available "in clear" to the payer:* [Version]+[Type]+ [Payee MSCT Service Provider ID] + [a clear-text name/value string]

Table 21: Minimum data sets for MSCTs based on payee-presented data

The MSCT interoperability framework and the HUB (its core technical component) should ensure the translation between these dataset formats, so that a consumers using a MSCT service provider participating in this framework can pay to any merchant using a MSCT service provider supporting any of these option.

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

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

The payee MSCT service provider ID is provided for routing purposes.

10 Technical interoperability of MSCTs based on payer-presented data

10.1 Introduction

This chapter analyses in more detail the interoperability of MSCTs based on payer-presented data. As mentioned before it focuses on the interoperability of MSCT at the PSU layer and the MSCT service (provider) layer. Hereby two main functionalities will be covered:

- The exchange of the payer identification and transaction data that enables the initiation of the MSCT;
- The acknowledgement/notification messages sent to the payer and payee after a successful/unsuccessful transaction or a reject.

Next to the specification of the MSCT interoperability requirements for the HUB, based on the generic 4-corner model, illustration of transaction process flows involving the HUB for successful transactions, rejects and unsuccessful transactions are included.

The chapter further defines the minimum data set to be exchanged between payer and payee for this type of MSCTs and specifies a payer-presented QR-code for MSCTs.

10.2 Exchange of MSCT data

For MSCTs based on payer-presented data, both the payer identification data and transaction data need to be exchanged to enable the initiation of an MSCT.

A. Exchange of payer-presented data

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

The *payer identification data* is defined by the payer MSCT service provider, 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 MSCT service provider and further to the payer MSCT service provider, see section 19.2.2 below.

The *identifier of the payer MSCT service provider* is needed by the payee MSCT service provider and subsequently by the HUB to know where to route the Payment Request message, see section 19.2.2 below.

B. Exchange of transaction data

The transaction data (payee data and payment data) needed by the payer for the initiation of the MSCT transaction is to be exchanged between the payee and the payer via their respective MSCT service providers[27] as follows:

- The transaction data is provided by the payee to their MSCT service provider via a Payment Request message. Thereby the payer identification data and the identifier of the payer MSCT service provider will need to be retrieved from the payer-presented data by the payee and included, next to the transaction data, in the Payment Request message. The Payment Request message between the payee and their MSCT service provider should further at least contain a transaction identifier, the name and the IBAN[28] of the payee and the transaction amount.
- The Payment Request message is transferred by the payee MSCT service provider via the HUB to the payer MSCT service provider using the identifier of the payer MSCT service provider received.
- The payer MSCT service provider identifies the payer and possibly their IBAN from the payer identification data included in the Payment Request message and provides the transaction data (at least the transaction amount and the name/trade name and the IBAN of the payee) to the payer for authentication purposes.

From the analysis made above, requirements can be derived for the HUB to support the payer identification and transaction data exchange needed for the interoperability of MSCTs based on payer-presented data. The table below list the required functionalities for the HUB for this exchange of transaction data

MSCT transaction feature	Requirements on HUB

[27] If a bi-directional proximity technology is used between the payer's mobile device and the payee's device, a direct transfer of the transaction data may be possible but will not be further investigated in this document, since the process flows would be similar to MSCT use cases based on payee-presented data (see Chapter 18).
[28] This may vary and is implementation dependent, e.g., if the IBAN is already known by the payee's MSCT service provider it may be omitted.

Exchange of data Payment Preparation phase (see Figure 3)	MSCTs based on SCT Inst or on SCT
Payer-presented data	
Transfer of payer *MSCT service provider identifier* to payee MSCT service provider	The payer MSCT service provider identifier is used by the payee MSCT service provider and the HUB for routing purposes and is included in the Payment Request message.
Transfer of payer token to payer MSCT service provider as *payer identification data*	Transfer of the payer token between the respective MSCT service providers – but included in the Payment Request message
Transaction data	
Transfer of *transaction data* to the payer MSCT service provider	Transfer of Payment Request message between MSCT service providers that includes the transaction data

Table 22: Required HUB functionalities for exchange of payer identification and transaction data for MSCTs based on payer-presented data

10.3 Acknowledgement/notification messages

The following messages have already been identified in sections 8.7 and 17.2 in this respect:

- Acknowledgement of receipt of the payment request message for MSCTs based on SCT to the payee by their MSCT service provider;
- Notification of payment to the payee by their MSCT service provider;
- Notification of payment to the payer by their MSCT service provider.

Note: The acknowledgement of receipt of the Payment Request message for MSCTs based on SCT Inst to the payee is not considered in view of the immediacy of the MSCT transaction.

10.3.1 Acknowledgement of receipt of payment request message for MSCTs based on SCT to the payee

For MSCTs that are based on SCT[29], where there is no immediacy of payment, it might be useful for the payee to receive a confirmation that the payment request message has been well-received by the payer's MSCT service provider. The acknowledgement of receipt needs to be supported by the HUB to support the interoperability of MSCTs.

Acknowledgement of receipt of payment request to payee

MSCTs based on SCT with payer-presented data

[29] For MSCTs based on SCT Inst, this acknowledgement is not needed in view of the immediacy of the payment.

1. *Acknowledgement of receipt of payment request* by the payer ASPSP to the payer MSCT service provider. 2. *Acknowledgement of receipt of payment request* by the payer MSCT service provider to the payee MSCT service provider. 3. *Acknowledgement of receipt of payment request* by the payee MSCT service provider to the payee.

Table 23: Overview of messages for acknowledgement of receipt of payment request to payee for MSCTs based on SCT with payer-presented data

10.3.2 Notifications of successful MSCT transactions

This section describes the *notification of successful transaction* messages that need to be supported to duly inform the payee and the payer for MSCTs based on payer-presented data.

A. MSCTs based on SCT Inst

Notification to payee

For all payment contexts, the *notification to the payee* about a *successful MSCT transaction based on SCT Inst* (i.e. after the receipt of the confirmation 6 by the payer's ASPSP in Figure 1) requires the following messages to be supported:

Notification to payee **Successful transactions for MSCTs based on SCT Inst with payer-presented data**
1. *Notification of successful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification successful transaction* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification successful transaction* by the payee MSCT service provider to the payee. Or *Notification of successful transaction* by the payee ASPSP to the payee (for specific cases only).

Table 24: Overview of messages for notification to payee of successful MSCTs based on SCT Inst with payer-presented data

Notification to payer

For all payment contexts, the *notification to the payer* about a *successful MSCT transaction based on SCT Inst* (i.e. after the receipt of the confirmation 6 by the payer's ASPSP in Figure 1) requires the following messages to be supported:

Notification to payer

Successful transactions for MSCTs based on SCT Inst with payer-presented data
1. *Notification of successful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of successful transaction* by the payer MSCT service provider to the payer.

Table 25: Overview of messages for notification to payer of successful MSCTs based on SCT Inst with payer-presented data

B. MSCTs based on SCT

Notification to payee

For all payment contexts, the *notification to the payee* about a *successful initiation* of an *MSCT transaction based on SCT* (i.e. after the transfer of the SCT transaction by the payer's ASPSP to its CSM) requires the following messages to be supported:

Notification to payee Successful transaction initiation for MSCTs based on SCT with payer-presented data
1. *Notification of successful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification successful transaction* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification successful transaction* by the payee MSCT service provider to the payee. Or *Notification of successful transaction* by the payee ASPSP to the payee (for specific cases only).

Table 26: Overview of messages for notification to payee of successful MSCTs based on SCT with payer-presented data

Notification to payer

For all payment contexts, the *notification to the payer* about a *successful MSCT transaction based on SCT* (i.e. after the receipt of the confirmation by the payer's ASPSP from its CSM) requires the following messages to be supported:

Notification to payer Successful transactions for MSCTs based on SCT Inst with payer-presented data

1. *Notification of successful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of successful transaction* by the payer MSCT service provider to the payer.

Table 27: Overview of messages for notification to payer of successful MSCTs based on SCT with payer-presented data

For MSCTs based on SCT, also a guarantee of payment[30] could be considered, but falls outside the scope of this document[31].

From the analysis made above, requirements can be derived for the HUB to support the notification of successful transactions needed for the interoperability of MSCTs based on payer-presented data. The table below list the required functionalities for the HUB for this.

MSCT transaction feature	Requirements on HUB	
Notification messages Payment Completion phase, (see Figure 3)	**SCT Inst**	**SCT**
Notification to payee about successful transaction	Notification from payer's MSCT service provider to payee's MSCT service provider	Notification from payer's MSCT service provider to payee's MSCT service provider
Notification to payer about successful transaction	Not applicable	Not applicable

Table 28: Required HUB functionalities for notification of successful transactions for MSCTs based on payer-presented data

10.3.3 Notifications of unsuccessful transactions and rejects for MSCTs

A. MSCTs based on SCT Inst

For MSCTs with payer-presented data based on SCT Inst, the following categories for rejects and unsuccessful transactions could be distinguished.

Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payer-presented data	
Cat 1	Reject by the payee MSCT service provider (before the sending of the Payment Request message to the payer MSCT service provider)

[30] This could potentially be addressed by a dedicated MSCT interoperability framework.
[31] Note that this is planned to be addressed in phase 2 of the SEPA RTP scheme under development.

Cat 2	Reject by the payer MSCT service provider (before initiation to the payer ASPSP)
Cat 3	Reject by the payer ASPSP before execution of the SCT Inst (i.e. before sending the SCT transaction by the payer ASPSP to its CSM)
Cat 4	Unsuccessful transaction - receipt by the payer ASPSP of negative confirmation message from its CSM

Table 29: Overview of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data

Annex 2 provides an overview on errors with MSCTs based on payer-presented data with a mapping on the four categories mentioned above.

The messages in the inter-PSP space related to these *rejects* and *unsuccessful transactions* have been specified in the SCT Inst scheme rule book [8] and the SCT Inst Implementation Guidelines[9].

Notification to payee

For all payment contexts, the *notification to the payee* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payee **Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payer-presented data**	
Cat 1	*Notification of reject* by the payee MSCT service provider to the payee.
Cat 2	1. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 2. *Notification of reject* by the payee MSCT service provider to the payee.
Cat 3	1. *Notification of reject* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification of reject* by the payee MSCT service provider to the payee.
Cat 4[32]	1. *Notification of unsuccessful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of unsuccessful transaction* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification of unsuccessful transaction* by the payee MSCT service provider to the payee.

[32] As already specified in EPC096-20v1.0

	Or *Notification of unsuccessful transaction* by the payee ASPSP to the payee (for specific cases only).

Table 30: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data

Notification to payer

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payer **Rejects and unsuccessful transactions for MSCTs based on SCT Inst with payer-presented data**	
Cat 1	1. *Notification of reject* from the payee MSCT service provider to the payee. 2. *Notification of reject* from the payee to the payer about the reject for C2B and B2B payment contexts (e.g. via display on the POI).
Cat 2	*Notification of reject* by the payer MSCT service provider to the payer. Or (for C2B or B2B payment contexts only[33]) 1. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 2. *Notification of reject* by the payee MSCT service provider to the payee. 3. *Notification of reject* from the payee to the payer (e.g. via display on the POI).
Cat 3	1. *Notification of reject* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of reject* by the payer MSCT service provider to the payer. Or (for C2B or B2B payment contexts only) 1. *Notification of reject* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification of reject* by the payee MSCT service provider to the payee. 4. *Notification of reject* from the payee to the payer (e.g. via the POI).
Cat 4[34]	1. *Notification of unsuccessful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of unsuccessful transaction* by the payer MSCT service provider to the payer. Or (for C2B or B2B payment contexts only) 1. Notification *of unsuccessful transaction* by the payer ASPSP to the payer MSCT service provider.

[33] This will typically be used for off-line MSCT use cases whereby the payer's device has no mobile network connectivity.
[34] As already specified in EPC096-20v1.0.

	2. Notification *of unsuccessful transaction* by the payer MSCT service provider to the payee MSCT service provider. 3. Notification *of unsuccessful transaction* by the payee MSCT service provider to the payee. 4. Notification *of unsuccessful transaction* from the payee to the payer (e.g. via the POI).

Table 31: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data

B. MSCTs based on SCT

For MSCTs with payer-presented data based on SCT, the following categories for rejects and unsuccessful transactions could be distinguished.

Rejects and unsuccessful transactions for MSCTs based on SCT with payer-presented data	
Cat 1	Reject by the payee MSCT service provider (before the sending of the Payment Request message to the payer MSCT service provider)
Cat 2	Reject by the payer MSCT service provider (before initiation to the payer ASPSP)
Cat 3	Reject by the payer ASPSP before execution of the SCT (i.e. before sending the SCT transaction by the payer ASPSP to its CSM
Cat 4	Unsuccessful transaction - receipt by the payer ASPSP of a "Reject" or "Return" message[35] (see DS-03 in the SCT scheme rulebook)

Table 32: Overview of rejects and unsuccessful MSCTs based on SCT with payer-presented data

Note: For MSCTs based on SCT transactions, the notification messages for unsuccessful transactions after the receipt of a "Return" may only be sent up to three days after the settlement date (Cat 4 in the table above).

Annex 2 provides an overview on errors with MSCTs based on payer-presented data with a mapping on the four categories mentioned above.

The messages in the inter-PSP space related to these *rejects and returns* have been specified in the SCT Scheme rule book [4] and the SCT Interbank implementation guidelines[5].

Notification to payee

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

[35] Note that a "Return" may be up to three days after the settlement date.

Notification to payee Rejects and unsuccessful transactions for MSCTs based on SCT with payer-presented data	
Cat 1	*Notification of reject* by the payee MSCT service provider to the payee.
Cat 2	1. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 2. *Notification of reject* by the payee MSCT service provider to the payee.
Cat 3	1. *Notification of reject* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification of reject* by the payee MSCT service provider to the payee.
Cat 4	1. *Notification of unsuccessful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of unsuccessful transaction* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification of unsuccessful transaction* by the payee MSCT service provider to the payee. Or *Notification of unsuccessful transaction* by the payee ASPSP to the payee (for specific cases only).

Table 33: Overview of messages for notification to payee of rejects and unsuccessful MSCTs based on SCT with payer-presented data

Notification to payer

For all payment contexts, the *notification to the payer* about a *reject* or an *unsuccessful MSCT transaction* requires the following messages to be supported:

Notification to payer Rejects and unsuccessful transactions for MSCTs based on SCT with payer-presented data	
Cat 1	1. *Notification of reject* from the payee MSCT service provider to the payee. 2. *Notification of reject* from the payee to the payer about the reject for C2B and B2B payment contexts (e.g. via display on the POI).
Cat 2	*Notification of reject* by the payer MSCT service provider to the payer. Or (for C2B or B2B payment contexts only[36])

[36] This will typically be used for off-line MSCT use cases whereby the payer's device has no mobile network connectivity.

	1. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 2. *Notification of reject* by the payee MSCT service provider to the payee. 3. *Notification of reject* from the payee to the payer (e.g. via display on the POI).
Cat 3	1. *Notification of reject* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of reject* by the payer MSCT service provider to the payer. Or (for C2B or B2B payment contexts only) 1. *Notification of reject* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of reject* by the payer MSCT service provider to the payee MSCT service provider. 3. *Notification of reject* by the payee MSCT service provider to the payee. 4. *Notification of reject* from the payee to the payer (e.g. via the POI).
Cat 4	1. *Notification of unsuccessful transaction* by the payer ASPSP to the payer MSCT service provider. 2. *Notification of unsuccessful transaction* by the payer MSCT service provider to the payer. Or (for C2B or B2B payment contexts only) 1. Notification *of unsuccessful transaction* by the payer ASPSP to the payer MSCT service provider. 2. Notification *of unsuccessful transaction* by the payer MSCT service provider to the payee MSCT service provider. 3. Notification *of unsuccessful transaction* by the payee MSCT service provider to the payee. 4. Notification *of unsuccessful transaction* from the payee to the payer (e.g. via the POI).

Table 34: Overview of messages for notification to payer of rejects and unsuccessful MSCTs based on SCT Inst with payer-presented data

From the analysis made above, requirements can be derived for the HUB to support the notification of unsuccessful transactions and rejects needed for the interoperability of MSCTs based on payer-presented data. The table below list the required functionalities for the HUB for this.

MSCT transaction feature	Requirements on HUB
Notification messages	**MSCTs based on payer-presented data**
	SCT Inst or SCT
Notification of reject to payee (Table 37 and Table 40: Cat 1)	Not applicable
Notification of reject to payee (Table 37 and Table 40: Cat 2 and 3)	Notification of reject message by payer MSCT service provider to payee MSCT service provider
Notification of unsuccessful transaction to payee (Table 37 and Table 40: Cat 4)	Notification of unsuccessful transaction by payer MSCT service provider to payee MSCT service provider
Notification of reject to payer (Table 38 and Table 41: Cat 1)	Not applicable

Notification of reject to payer (Table 38 and Table 41: Cat 2)	Notification of reject message by payee MSCT service provider to payer MSCT service provider
Notification of reject to payer (Table 38 and Table 41: Cat 3 for C2B and B2B payment contexts only)	Notification of reject message by payer MSCT service provider to payee MSCT service provider
Notification of unsuccessful transaction to payer (Table 38 and Table 41: Cat 4 for C2B and B2B payment contexts only)	Notification of unsuccessful transaction by payer MSCT service provider to payee MSCT service provider

Table 35: Required HUB functionalities for unsuccessful transactions and rejects for MSCTs based on payer-presented data

10.4 Interoperability process flows for MSCTs based on payer-presented data

10.4.1 Introduction

In this section the full process flows between the HUB and respective MSCT service provider back-ends for two examples will be described. These examples are provided for illustrative purposes only. Note that as mentioned before, an MSCT service provider could be an ASPSP. This means that in the process flows below, one or both MSCT providers could be one or both of the respective ASPSPs in which case the process flows would simplify.

Two illustrative cases will be considered as listed in the table below.

MSCT transactions	Support from the HUB[37]	Reference
C2B – successful transaction based on SCT Inst Consumer-presented QR-code contains a token	• Payment request messages (see section 10.2) • Notification of successful transaction (see section 10.3)	Section 10.4.2
C2B - reject by the payer (consumer) ASPSP service provider for MSCT based on SCT Inst Consumer-presented QR-code including a token (Table 36: Cat 3)	• Retrieval of the payee data from the proxy (see section 10.2) • Notification of reject (see section 10.3)	Section 10.4.3

Table 36: Illustrative process flows for interoperability of MSCT transactions based on payer-presented data with mapping onto HUB functionalities

[37] Depicted by the green arrows in the illustrative process flows below.

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

The QR-code may be static or dynamic. In case dynamic QR-codes are used, a *conditional transaction lock function* is defined as follows. The function consists of conditional lock transaction messages that are sent between the consumer's MSCT service provider and the merchant's MSCT service provider via the HUB to prevent that multiple consumers from different MSCT service providers pay the same transaction after strong customer authentication (see section 8.3). The transaction lock function is required in case the QR-code stays active for a certain time window that would enable multiple scans and related payments and its need is specified in the dedicated Lock Transaction Indicator (LT Indicator as defined in section 18.6 in this document). If two consumers would perform SCA on the same transaction, the consumer with successful SCA for which the lock function sent by their MSCT service provider reaches as first the MSCT service provider of the merchant is the one for which the transaction is locked.

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

Note also that in the process flows below, the representation and description of strong customer authentication (SCA) is simplified since the focus is on the interconnectivity between the respective MSCT service providers.

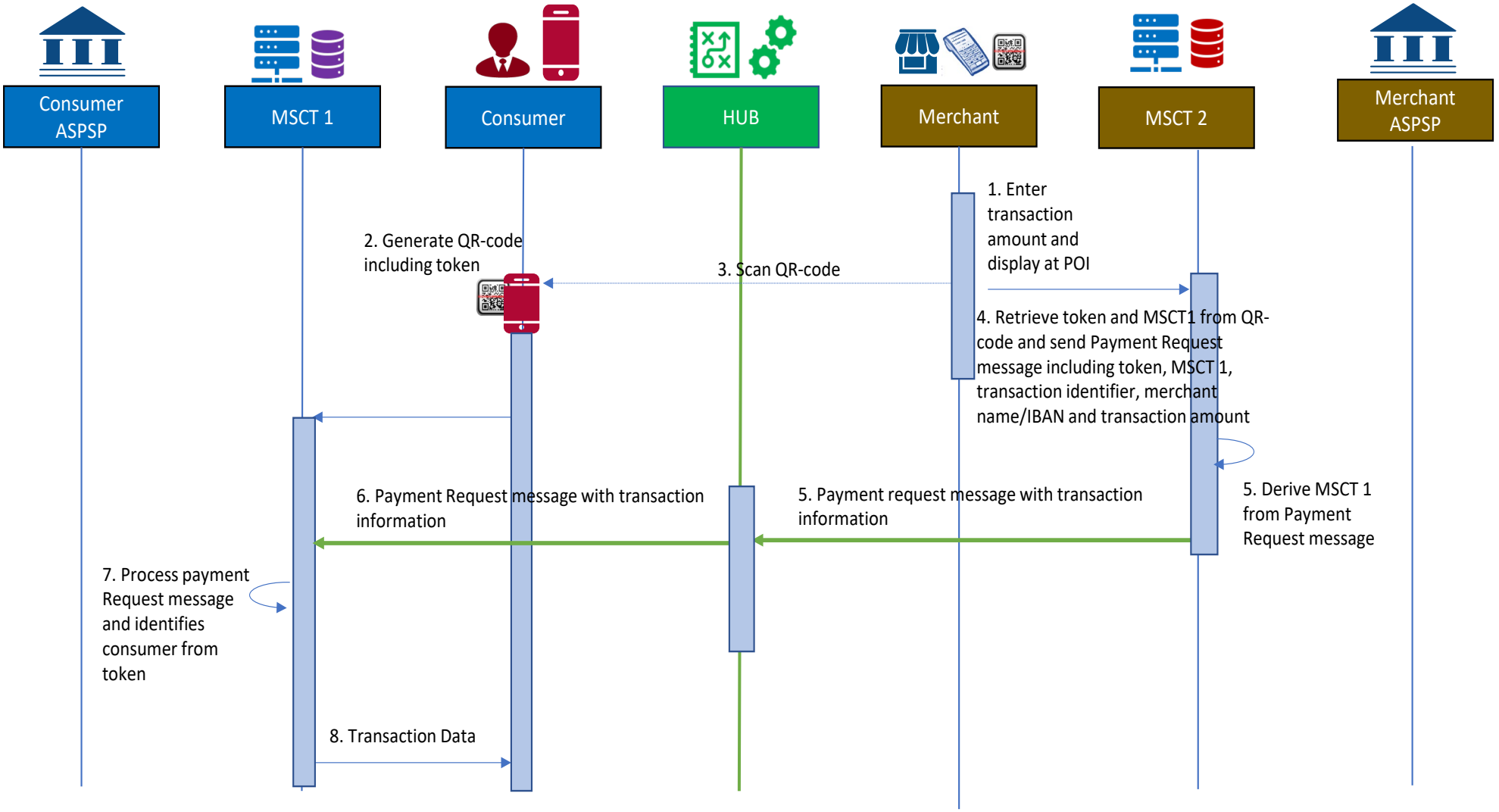
Furthermore, the process flows do not include potential exchanges needed between MSCT service provider back-ends for applicable remuneration to support a business model.

10.4.2 Successful MSCT – C2B based on SCT Inst with consumer-presented QR-code containing a token

In this section the process flow for a successful in-store payment between a consumer (payer) and merchant (payee) using the HUB is illustrated. In this example, it is assumed that the consumer-presented data does not contain the consumer identification "in clear" but that a token is used instead (see section 19.2). It is hereby assumed that the tokenisation/de-tokenisation process is handled by or via the consumer's MSCT service provider. The consumer-presented data includes the identifier of the consumer's MSCT service provider "in clear" so that it can be retrieved by the merchant and provided to their MSCT service provider in the payment request message.

In this example, the actors, interconnectivity and process steps are depicted in Section 6 – use-case C2B-B.

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


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

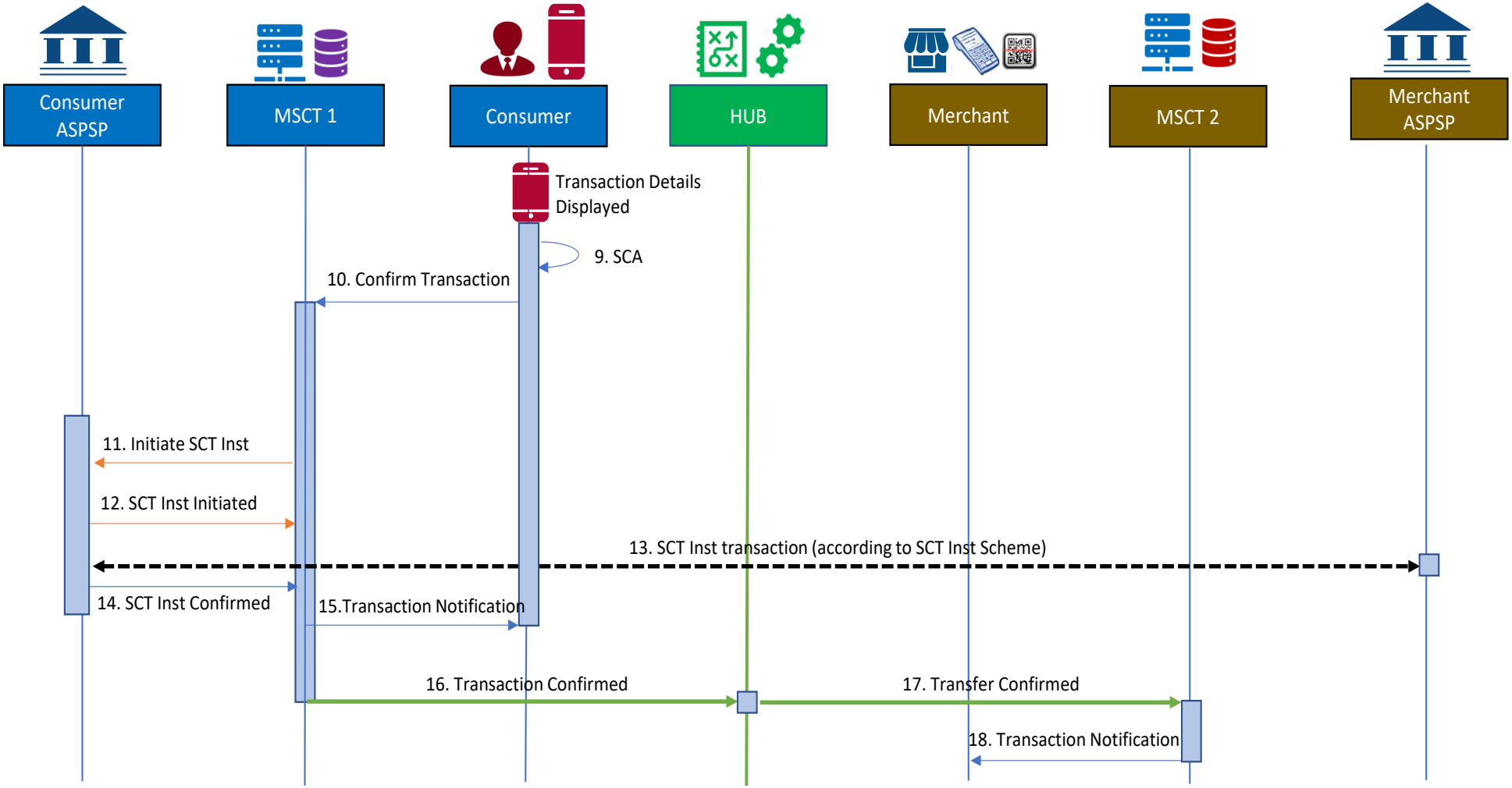


Figure 16: Process flow – C2B – consumer-presented QR-code

In the figure above the following steps are involved:

Step 1

- The merchant enters the transaction amount which is displayed on the POI[38].

Step 2

- The consumer selects and opens the MSCT Inst 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 Inst 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[39], merchant transaction identifier, the transaction amount, the consumer's MSCT service provider identifier and the consumer token.

Step 5:

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

Step 6:

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

Step 7:

The consumer MSCT service provider checks the Payment Request message and retrieves the transaction data and the consumer identification data from the 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[40].

[38] The display of the transaction amount by the POI may happen at a later stage since the payer indemnity might have an impact on the final transaction amount (e.g., discounts). However this could require additional steps to obtain the payer identification from the token received. This would need to be analysed in forthcoming work by the MSG MSCT.
[39] Instead of the IBAN_merchant a proxy may be used.
[40] 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 10:

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

Step 11:

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

Step 12:

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

Step 13:

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

Step 14:

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

Step 15:

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

Step 16:

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

Step 17:

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

Step 18:

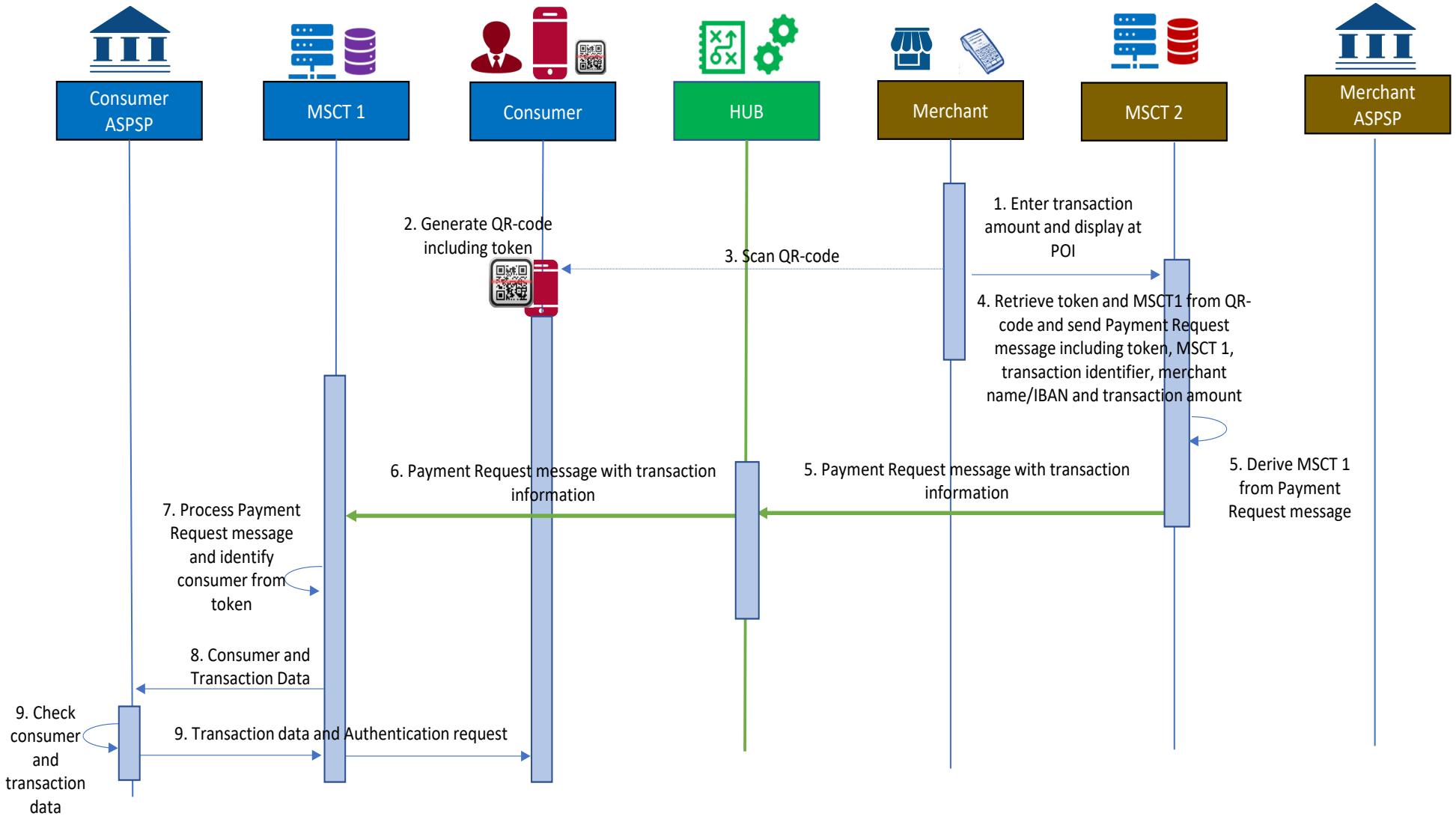
The merchant's MSCT service provider sends a transaction notification message to the merchant.

10.4.3 Reject by payer ASPSP service provider – C2B based on SCT Inst with consumer-presented QR-code containing a token

The process flow below illustrates the usage of the HUB in the case of a reject by the consumer (payer) ASPSP for an MSCT based on consumer-presented data using a QR-code including a token. This may be a dynamic or a static token. It is hereby assumed that the tokenisation/de-tokenisation of (part of) the transaction data is handled by or via the consumer MSCT service provider. In this illustration it is assumed that the payer ASPSP rejects the MSCT after an unsuccessful SCA.

In this example, the actors, interconnectivity and process steps are depicted in Section 6 – use-case C2B-C.

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


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

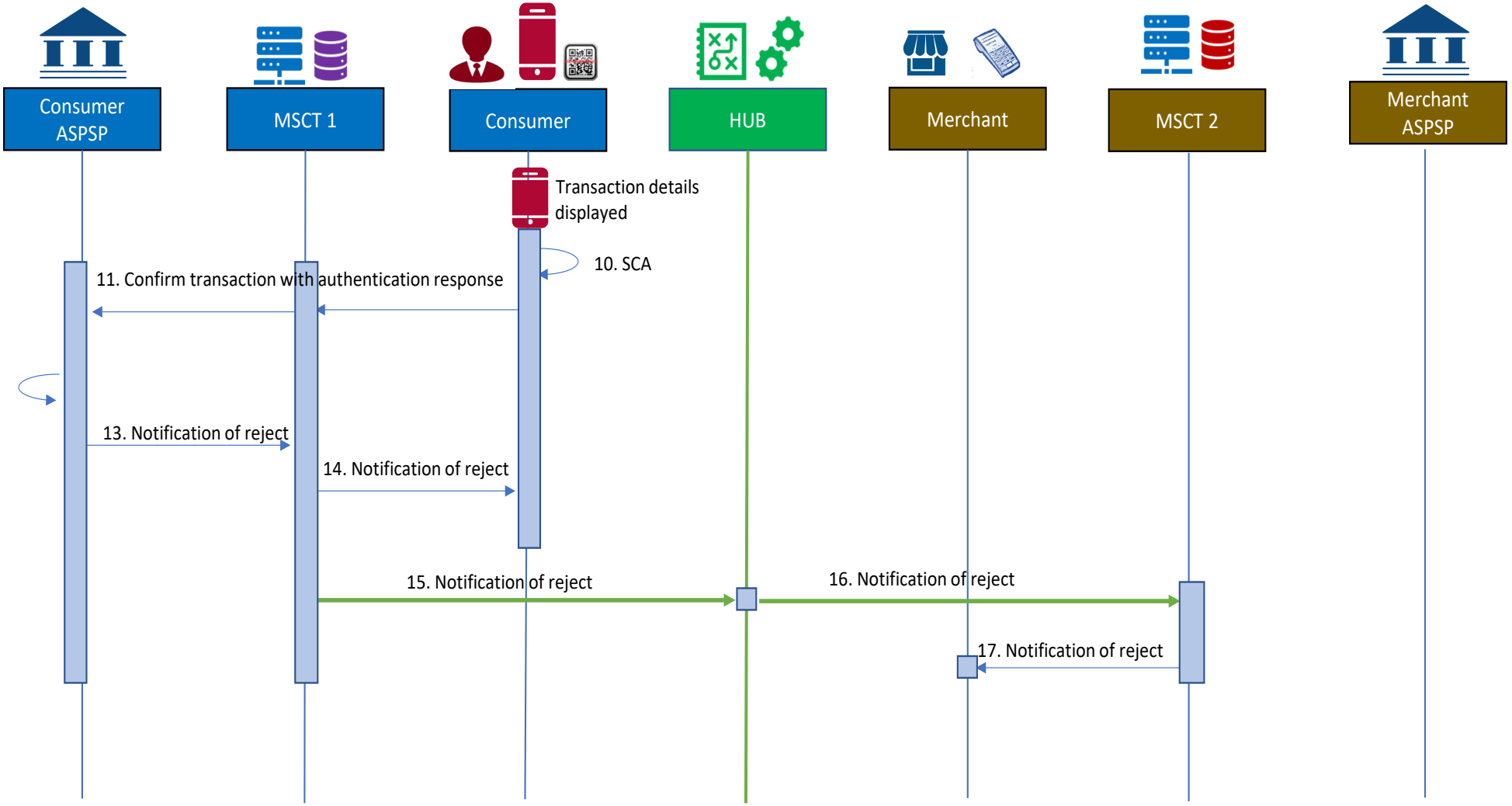


Figure 17: Process flow – C2B – Reject by consumer ASPSP for MSCT based on consumer-presented QR-code

In the figure above the following steps are involved:

Step 1

The merchant enters the transaction amount which is displayed on the POI[41].

Step 2

- The consumer selects and opens the MSCT Inst 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 Inst application on the mobile device.

Step 3

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

Step 4

The merchant retrieves the consumer token and the consumer MSCT service provider identifier from the QR-code and sends a Payment Request message to their MSCT service provider, including the merchant name/trade name, IBAN_merchant18F42, merchant transaction identifier, the transaction amount, the consumer MSCT service provider identifier and the consumer token.

Step 5:

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

Step 6:

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

Step 7:

The consumer MSCT service provider checks the Payment Request message and retrieves the transaction data and the consumer identification data from the token.

Step 8:

The consumer MSCT service provider sends the consumer and transaction details to the consumer ASPSP.

Step 9:

- The consumer ASPSP checks the consumer and transaction details
- The consumer ASPSP sends the transaction details with an authentication request to the consumer via the consumer MSCT service provider.

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

Step 10:

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

Step 11:

The confirmation including the authentication response is provided to the consumer ASPSP via the consumer MSCT service provider.

Step 12:

The consumer ASPSP checks the authentication response which is incorrect and rejects the transaction[43].

Step 13:

The consumer ASPSP sends a notification of reject to the consumer MSCT service provider.

Step 14:

The consumer MSCT service provider sends a notification of reject to the consumer.

Step 15:

The consumer MSCT service provider sends a notification of reject to the HUB with the merchant MSCT service provider identifier.

Step 16:

The HUB forwards the notification of reject to the merchant MSCT service provider.

Step 17:

The merchant MSCT service provider sends the notification of reject to the merchant.

10.5 Minimum data set for MSCTs based on payer-presented data

To achieve interoperability for MSCTs, an agreement on a minimum data set is required for the data to be exchanged between the payer/consumer and payee/merchant, being it in the payer-presented data or in the payment request messages exchanged (see section 19.2).

In the previous version 1.14 of this document and in the report ERPB/2020/026 [40], originally three cases were distinguished with respect to the payer identification data. In view of the answers received from the EBA on Q&A 2020_5476[44] and Q&A 2021_6298[45], the options containing the CustomerID in "clear" do not seem to be allowed[46]. Therefore, this document and [31] consider only one case, namely the payer identification data is a (payer) token. But

[44] https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5476
[45] See https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6298.
[46] 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.

the minimum data set could also include an additional clear-text value string to support value-added services (e.g. loyalty).

The minimum data set to be exchanged (see also Table 29 in section 19.2) between the payee and the payer consists of both routing info (i.e. the identifier of the payer MSCT service provider) and the (payer) token as payload. The minimum data will be forwarded in the Payment Request message through the HUB from the payee MSCT service provider to the payer MSCT service provider for de-tokenisation into the payer identification data, together with the other transaction data.

The minimum data set is as follows:

The payer-presented data includes a token:
[Version]+[Type]+[payer MSCT service provider ID]+[(payer) token]+[a clear-text name/value string]

Table 37: Minimum data set for MSCTs based on payer-presented data

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

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

The type may refer to the cases above and may enable to add other services[47].

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

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

11 MSCT interoperability messages

11.1 Introduction

Through the analysis of the technical interoperability of MSCTs, either based on payee- or on payer-presented data, made in the Chapters 18 and 19 in this document, a number of MSCT interoperability messages have been specified to be supported by the MSCT service providers and the HUB. Note that the messages in the inter-PSP space for SCT Inst and SCT have already been specified in the respective scheme rulebooks (see [20] and [16] respectively) and implementation guidelines (see [21] and [17] respectively).

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

This chapter provides an overview of these MSCT interoperability messages for which the minimum data sets are defined in Annex 3 to this document.

11.2 Overview MSCT interoperability messages

This section provides an overview of all the MSCT interoperability messages identified in the Chapters 18 and 19 in this document.

Since several errors (e.g. execution errors, failures in notification messages, etc.) may occur during the exchange of messages between the respective MSCT service providers (see also Annex 3), there is also a need to define a so-called *"Inquiry request message"* and an *"Inquiry response message"* between the respective MSCT service providers of the payer and the payee. Also for these messages the minimum data elements are defined in Annex 3.

11.2.1 MSCTs based on payee-presented data

The following messages that need to be supported by the HUB have been identified in this document for MSCTs based on payee-presented data.

Message type	Description
Transaction information request	Message sent by the payer MSCT service to the payee MSCT service provider to request (missing) transaction data.
Transaction information response	Message sent by the payee MSCT service to the payer MSCT service provider to provide (missing) transaction data.
Lock transaction request	Message sent by the payer MSCT service to the payee MSCT service provider to request the locking of a transaction for a given payer.
Lock transaction response	Message sent by the payee MSCT service to the payer MSCT service provider to confirm the locking of a transaction for a given payer.
Notification of reject	• Notification to the payer about the reject of the MSCT. This involves the payer, the payer MSCT service provider and may involve the payer ASPSP. • Notification to the payee about the reject of the MSCT. This involves the payee, the payer MSCT service provider, the HUB and the payee MSCT service provider and may involve the payer ASPSP.
Notification of successful / unsuccessful transaction	• Notification to the payer about the successful/unsuccessful execution of the MSCT. This involves the payer, the payer ASPSP and the payer MSCT service provider. • Notification to the payee about the successful/unsuccessful execution of the MSCT. This involves the payee, the payer ASPSP, the payer MSCT service provider, the HUB and the payee MSCT service provider.

Inquiry request message	Message exchanged between MSCT service providers to request a special investigation concerning a specific MSCT
Inquiry response message	Message exchanged between MSCT service providers to reply to an inquiry request message concerning a specific MSCT

Table 38: Overview messages for MSCTs based on payee-presented data

Notes: The following messages will not be covered in this document since they are not impacting the interoperability of MSCTs based on payee-presented data.

- MSCT initiation request message from the payer to the payer MSCT service provider and from the payer MSCT service provider to the payer ASPSP;
- Acknowledgement of receipt of the MSCT instruction based on SCT from the payer ASPSP to the payer MSCT service provider and from the payer MSCT service provider to the payer.

However, the data sets of the MSCT initiation request messages should be aligned with the data sets of the initiation messages DS-01 defined in the SCT Inst and SCT scheme rulebooks ([20] and [16]).

11.2.2 MSCTs based on payer-presented data

The following messages that need to be supported by the HUB have been identified in the document for MSCTs based on payer-presented data.

Message type	Description
Payment request message	Message sent by the payee via their MSCT service provider and the HUB to the payer MSCT service provider.
Confirmation of receipt of payment request message (for MSCTs based on SCT)	Confirmation to the payee about the receipt of the payment request message. This involves the payee, the payer MSCT service provider, the HUB, the payee MSCT service provider and the payee.
Notification of reject message	• Notification to the payer about the reject of the MSCT. This involves the payer, the payer MSCT service provider and may involve the payer ASPSP, the HUB, the payee MSCT service provider and the payee. • Notification to the payee about the reject of the MSCT. This involves the payee, the payee MSCT service provider and may involve the HUB, the payer MSCT service provider and the payer ASPSP.
Notification of successful / unsuccessful transaction	• Notification to the payer about the successful/unsuccessful execution of the MSCT. This involves the payer, the payer ASPSP, the payer MSCT service provider and may involve the HUB and the payee MSCT service provider.

	• Notification to the payee about the successful/unsuccessful execution of the MSCT. This involves the payee, the payer ASPSP, the payer MSCT service provider, the HUB and the payee MSCT service provider.
Inquiry request message	Message exchanged between MSCT service providers to request a special investigation concerning a specific MSCT
Inquiry response message	Message exchanged between MSCT service providers to reply to an inquiry request message concerning a specific MSCT

Table 39: Overview messages for MSCTs based on payer-presented data

Note: The MSCT initiation message from the payer MSCT service provider to the payer ASPSP will not be covered in this document since it is not impacting the interoperability of MSCTs based on payer-presented data. However, it should be aligned with the data sets of the instruction message DS-01 defined in the SCT Inst and SCT scheme rulebooks ([20] and [16]).

11.3 Entities involved in MSCT interoperability messages

The table below presents a mapping of the various MSCT interoperability messages defined in this chapter versus the entities involved in sending/receiving these messages. Hereby the abrreviations for the messages are used between the respective entities as they are defined in Annex 3 to this document.

Message type	Entities involved in the exchange of the MSCT interoperability message									
	Payer/ Payer MSCT service provider		Payer MSCT service provider/ Payer ASPSP		Payer MSCT service provider/HUB		Payee MSCT service provider/HUB		Payee/Payee MSCT service provider	
	Payee-presented data	Payer-presented data	Payee-presented data	Payer-presented dat	Payee-presented data	Payer-presented data	Payee-presented data	Payer-presented data	Payee-presented data	Payer-presented data
Transaction information request					TIRQ		TIRQ			
Transaction information response					TIRP		TIRP			
Lock Transaction Request					LTRQ		LTRQ			
Lock Transaction Response					LTRP		LTRP			
Payment Request message						PR2		PR2		PR1
Confirmation of receipt payment request message						CRPR1		CRPR1		CRPR2
Notification of reject message	NR1	NR1	NR3	NR3	NR2	NR2	NR2	NR2	NR4	NR4
Notification of successful/ unsuccessful transaction message	NT3	NT3	NT1	NT1	NT2	NT2	NT2	NT2	NT4	NT4
Inquiry request message					IRQ	IRQ	IRQ	IRQ		
Inquiry response message					IRP	IRP	IRP	IRP		

Table 40: Overview MSCT interoperability messages and entities involved

12 New MSCT interoperability models

12.1 Introduction

This section studies models involving a Payment Initiation Service Provider (PISP) or a Collecting PSP (CPSP). Next to a brief description of the most important models identified, a brief analysis is made of how the interoperability requirements that have been specified in this document are impacted.

12.2 Models involving a PISP

PISPs as specified in the PSD2 [5] and the RTS [6] could be involved to facilitate MSCTs.

This section analyses models for MSCTs involving a PISP, impacting the interoperability. Hereby the focus will be on C2B payment contexts and a distinction will be made between MSCTs based on merchant-presented data and MSCTs based on consumer-presented data. Although the MSCT transaction in the figures below is depicted as an SCT Inst, the analyses made below remain valid if the MSCT is based on SCT. Likewise, the analyses also remain valid for other payment contexts, although for P2P payments, a PISP will only be involved on the payer side.

12.2.1 MSCTs based on merchant-presented data

Two different cases could be distinguished concerning the involvement of a PISP:

- *Case 1*: The PISP is the consumer MSCT service provider and the consumer has a dedicated MSCT application on their consumer device to initiate the payment after receiving the merchant-presented data from the POI;

- *Case 2*: The PISP is the merchant MSCT service provider. The consumer has no dedicated MSCT application on their device but the merchant-presented data is read by a generic application (e.g. a QR-code reader) on the consumer device and a redirection to a merchant website or merchant app takes place. On this webpage/ merchant app the consumer confirms or selects a PISP and provides their consumer identification data.

Below a brief analysis will be made for both cases and their impact on the technical interoperability requirements.

Case 1 – PISP is consumer MSCT service provider

This model is represented in the figure below.

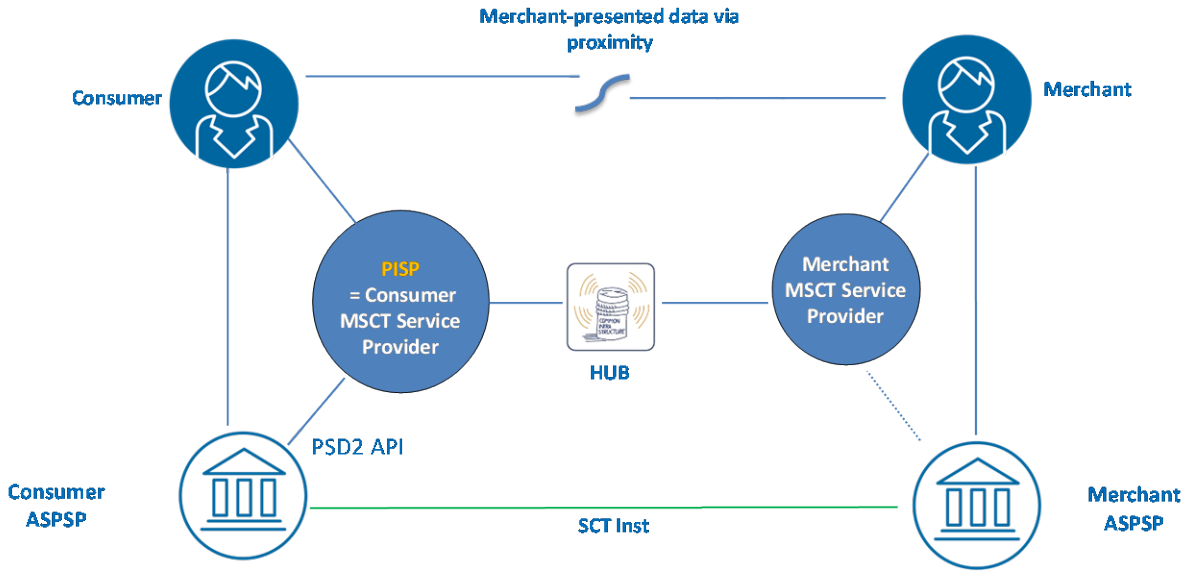


Figure 18: Model for MSCTs based on merchant-presented data whereby PISP is consumer MSCT service provider

In this model, the consumer has on-boarded with the PISP and downloaded an MSCT application on their mobile device, hereby providing the necessary consent with respect to the PISP according to PSD2 (Arts. 51 through 58, 64, 66 and 94) and RTS (Art. 30)[48]. The technical interoperability requirements specified in Chapter 18 apply for the PISP as MSCT service provider of the consumer. Also note that to enable the PISP to use the PSD2 API for the communication with the consumer ASPSP, the consumer should have registered their CustomerID and IBAN during the on-boarding process with the PISP, hereby meeting the appropriate security guidelines (see Chapter 15).

Case 2 – PISP is merchant MSCT service provider

This model is represented in the figure below.

[48] Further clarifications have also been provided in the EBA answers to questions: EBA Q&A 2020_5570 and 2020_5573.

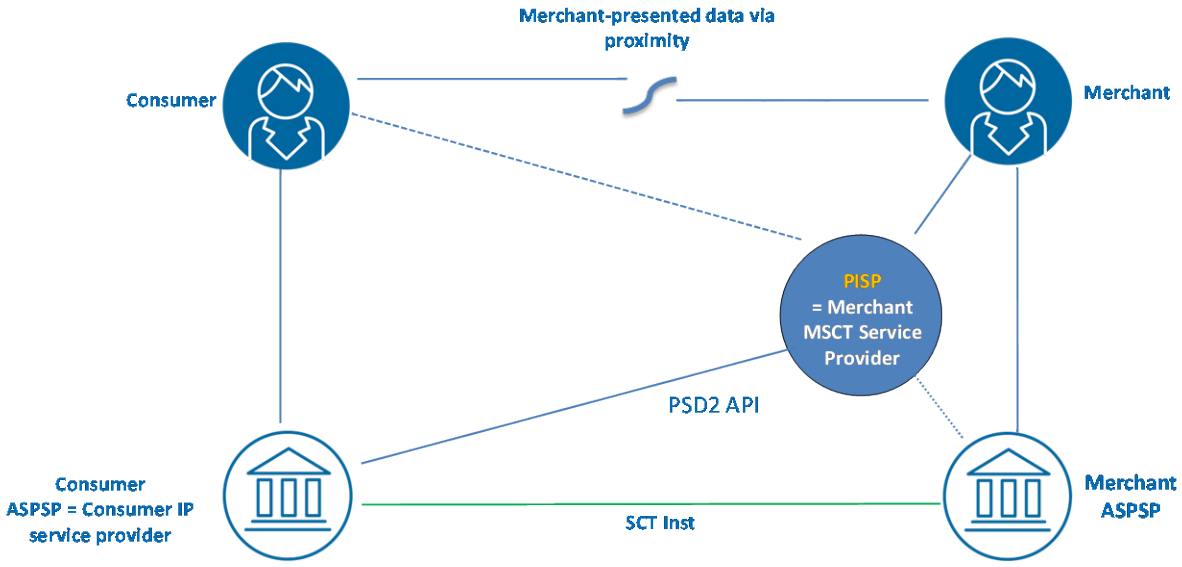


Figure 19: Model for MSCT based on merchant-presented data whereby PISP is merchant MSCT service provider

In this model, it is assumed that the consumer ASPSP is their MSCT service provider while a PISP is involved on the merchant side as the merchant MSCT service provider. The merchant-presented data are provided to the consumer at the POI (e.g. via a QR-code read by a "generic QR-code reader" on the consumer device) and re-directs the consumer to a merchant webpage/ merchant application[49]. To proceed with the payment, the consumer confirms the PISP or is invited to select a PISP hereby giving the appropriate consent to the PISP for the initiation of the MSCT according to PSD2 (Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30)[50]. The consumer should subsequently provide their CustomerID and IBAN to the PISP to enable the PISP to initiate the MSCT via the PSD2 API[51].

Since the PISP is the MSCT service provider of the merchant, the interoperability requirements described in Chapter 10 apply as the transaction data available to the PISP would be the same as in the case of an MSCT based on consumer-presented data. However, the functional requirements for the HUB as listed in this chapter with respect to the transfer of the Payment Request messages could be covered by the PSD2 API; this model is in fact reduced to a 3-corner model.

12.2.2 MSCTs based on consumer-presented data

Two different main cases could be distinguished concerning the involvement of a PISP:

- *Case 1:* The PISP is the consumer MSCT service provider and the consumer has a dedicated MSCT application on their consumer device. The consumer-presented data includes the identifier to route the Payment Request message via the HUB to the PISP (see Chapter 10).

[49] Care should be taken concerning the security of the information included in the QR-code for the redirect (e.g. to avoid man-in-the middle attacks).
[50] Further clarifications have also been provided in the EBA answers to questions: EBA Q&A 2020_5570 and 2020_5573.
[51] Alternative methods exist such as enabling the consumer to select their ASPSP and being redirected towards an ASPSP hosted webpage to enter their identification data.

Case 2: The PISP is also the merchant MSCT service provider. Hereby a dedicated agreement will be needed between the merchant and the PISP.

Both cases will now be further analysed below.

Case 1 – PISP is consumer MSCT service provider

This model is represented in the figure below.

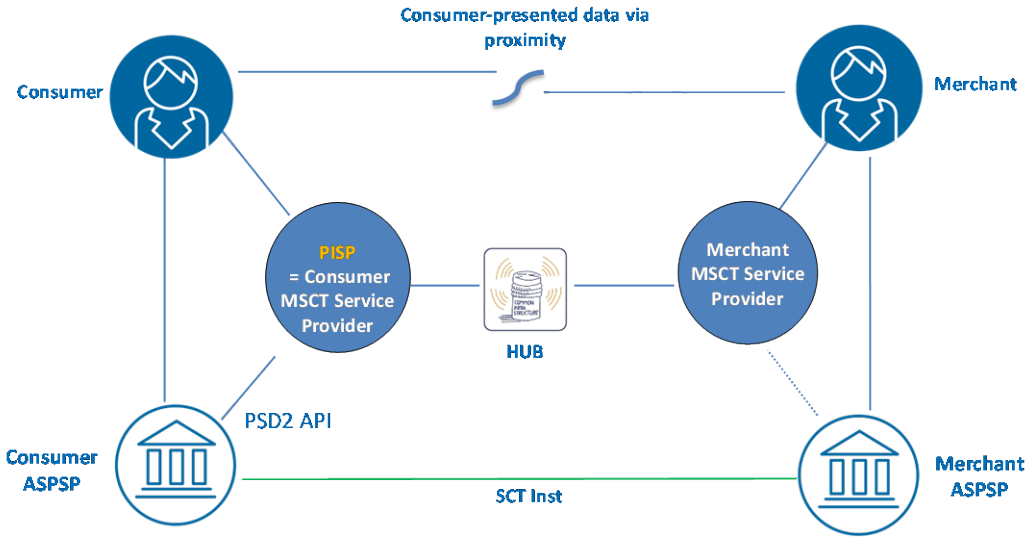


Figure 20: Model for MSCTs based on consumer-presented data whereby PISP is consumer MSCT service provider

In this model, the consumer has on-boarded with the PISP and downloaded an MSCT application on their mobile device, hereby providing the necessary consent with respect to the PISP according to PSD2 (Arts. 51 through 58, 64, 66 and 94) and RTS (Art. 30)[52]. The technical interoperability requirements specified in Chapter 10 apply for the PISP as MSCT service provider of the consumer. Also note that to enable the PISP to use the PSD2 API for the communication with the consumer ASPSP, the consumer should have registered their CustomerID and IBAN during the on-boarding process with the PISP, hereby meeting the appropriate security guidelines (see Chapter 15).

Challenge: Complementing the usage of the PSD2 API, an additional feature (beyond PSD2 and RTS) should be supported, namely the notification from the consumer ASPSP to the PISP (= consumer MSCT service provider) about the successful/unsuccessful transaction or reject in support of the notifications to the consumer and the merchant (see section 10.3).

Note: This model remains valid for e- and m- commerce if the consumer data is entered on a merchant webpage / merchant app whereby the consumer selects or confirms the PISP.

[52] Further clarifications have also been provided in the EBA answers to questions EBA Q&A 2020_5570 and 2020_5573.

Case 2 – PISP is merchant MSCT service provider

Typically, the consumer-presented data is provided by the consumer to the merchant POI and forwarded together with the transaction data (transaction amount, name/IBAN merchant, etc.) to the merchant MSCT service provider = PISP for the initiation of the MSCT. In order to enable the PISP to use the PSD2 API for the communication with the consumer ASPSP, the CustomerID and IBAN of the consumer should be made available "in clear" to the PISP[53].

One of the main challenges however with the involvement of a PISP on the merchant side is how the consumer can give the appropriate consent for the usage of a PISP in accordance with the PSD2 (Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30)[54].

In what follows, two different sub-cases could be distinguished concerning the involvement of a PISP as merchant MSCT service provider:

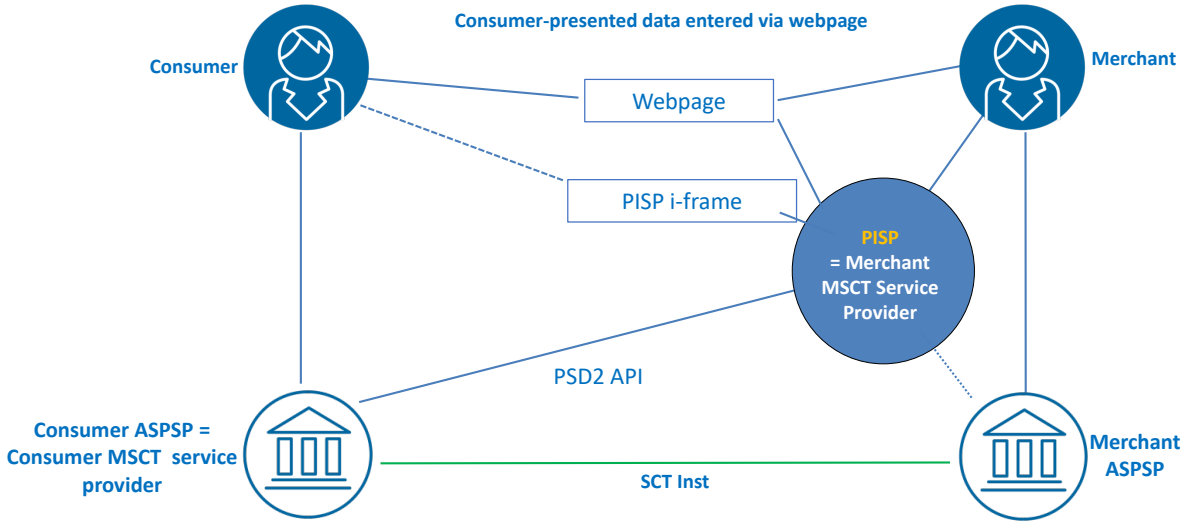
- *Subcase 2.1:* A PISP involved on the merchant side for e- and m-commerce;
- *Subcase 2.2:* A PISP involved on the merchant side for in-store payments.

Note that for the two subcases above, if the PISP is at the same time also the consumer MSCT service provider, which means that the consumer has on-boarded with this PISP (see also the case 1 in this section), then the model becomes effectively a 3-corner model that will not be further discussed in this document.

Below a brief analysis will be made of each of the two subcases distinguished above and their impact on the technical interoperability requirements. Also, the challenges for these two subcases will be identified.

Subcase 2.1 – PISP on merchant side for e- or m-commerce

This model is represented in the figure below.



[53] Further clarifications have also been provided in the EBA answers to questions EBA Q&A 2020_5570 and 2020_5573.

[54] Further clarifications have also been provided in the EBA answers to questions EBA Q&A 2020_5570 and 2020_5573.

Figure 21: Model for MSCT based on consumer-presented data whereby PISP is merchant MSCT service provider / e- and m-commerce

In this model, it is assumed that the consumer ASPSP is their MSCT service provider while a PISP is involved on the merchant side as the merchant MSCT service provider. To proceed with the payment, the consumer is invited to confirm or select a PISP on the merchant webpage / merchant app, whereby they are able to access the appropriate PISP information. They subsequently give the appropriate request and consent to the PISP for the initiation of the MSCT according to PSD2 (Arts. 44, 45, 64, 66 and 94)[55], by providing their CustomerID and IBAN to the PISP to enable the PISP the initiation of the MSCT via the PSD2 API to the consumer ASPSP.

Since the PISP is the MSCT service provider of the merchant, the interoperability requirements specified in Chapter 10 apply. However, the functional requirements for the HUB with respect to the transfer of the Payment Request messages could be covered by the PSD2 API; this model is in fact reduced to a 3-corner model.

Subcase 2.2 – PISP on merchant side for in-store

This model is represented in the figure below.

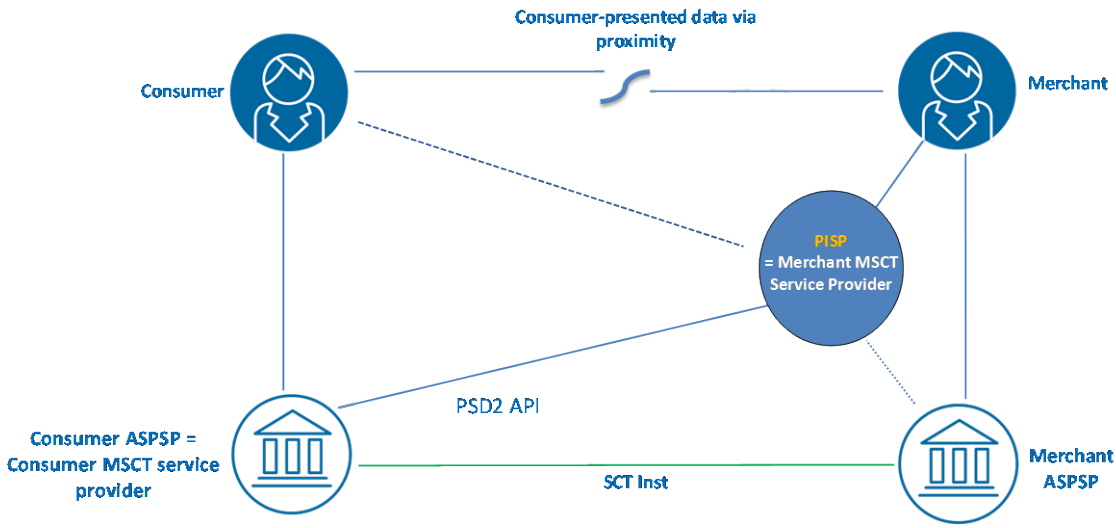


Figure 22: Model for MSCT based on consumer-presented data whereby PISP is merchant MSCT service provider / in-store

In this model, it is assumed that the consumer ASPSP is their MSCT service provider while a PISP is involved on the merchant side as the merchant MSCT service provider. To proceed with the payment, the consumer provides their consumer-presented data to the merchant, e.g. via a QR-code. The consumer should also provide the appropriate consent via the

[55] Further clarifications have also been provided in the EBA answer to question EBA Q&A 2020_5573.

merchant on the usage of a PISP for the initiation of the MSCT according to PSD2 (Arts. 44, 45, 64, 66 and 94)[56]. Moreover, it is hereby assumed that the consumer identification data, i.e. CustomerID and IBAN are provided "in clear" to enable the PISP to use the PSD2 API for the communication with the consumer ASPSP.

Since the PISP is the MSCT service provider of the merchant, the interoperability requirements specified in Chapter 10 apply. However, the functional requirements for the HUB with respect to the transfer of the Payment Request messages could be covered by the PSD2 API; this model is in fact reduced to a 3-corner model.

Challenges:

- Complementing the usage of the PSD2 API, an additional feature (beyond PSD2 and RTS) should be supported, namely the notification from the consumer ASPSP (= consumer MSCT service provider) to the PISP (= merchant MSCT service provider) about the successful/unsuccessful transaction or reject in support of the notification to the merchant (see section 19.3).
- Protection of CustomerID and IBAN subject to EBA clarifications[57].
- Consumer consent with respect to usage of the PISP subject to EBA clarifications ((Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30))[58].

13 Challenges and opportunities

By analysing the different MSCT solutions that are currently available in the market, the following challenges in addition to the technical interoperability requirements specified in Chapters 17 to 22 were identified. Here a special focus was given to both consumer and merchant experience. These challenges would need to be sufficiently addressed for a SEPA-wide take-up of MSCTs.

13.1 Challenges

Proximity technologies

In various countries, the proximity solutions described in this document have been introduced by the local MSCT service providers and the retailers to be able to reach their customers. However, because of the lack of standardisation, these solution are not interoperable. This means that consumers who would like to purchase across a range of merchants or cross-border may need to download many different MSCT applications on their mobile device in view of their "closed-loop" implementations.

The usage of these proximity technologies also come for the retailers with a cost for the adaptation of their POI terminal. Here a distinction is to be noted between the adoption of

[56] Further clarifications have also been provided in the EBA answers to questions EBA Q&A 2020_5570 and 2020_5573.
[57] See also the EBA answers to questions EBA Q&A 2020_5476 and 2020_5477.
[58] Further clarifications have also been provided in the EBA answers to questions EBA Q&A 2020_5570 and 2020_5573.

BLE technology at POIs that may require a hardware change versus the adoption of QR-codes which may require only a software update.

BLE is a potential alternative to NFC for electronic payments with mobile devices at the POI. Both transmission methods work bidirectional and have a sufficiently fast transmission rate.

BLE transmissions can be made secure against unauthorised intrusion if they are operated as a connection with multi-level dynamic key allocation. Static key assignment limits security. When the key is transmitted, exactly this part of the communication is particularly at risk, since only the successful exchange of the key protects a BLE connection.

In analogy to NFC technology, the usage of the BLE technology for making proximity payments requires that the Bluetooth functionality on the consumer's mobile device is switched on, which should be handled by the MSCT app.

Finally, there is a lack of standardisation for the adoption of BLE technology for MSCTs (e.g. common specification for radio range on POI, transaction processing) and "common" customer experience guidelines.

Another challenge may appear when the POI supports multiple proximity technologies. In such an environment, the consumer's mobile device may perform a transaction over an unintended interface.

Mobile competitive landscape

Currently it is unclear what will be the prevailing mobile proximity payment technology in the future, which results into difficult decisions with respect to investments to be made. It is precisely the competition between the different technologies that leads to a fragmented market.

However, there is a strong demand for more openness of the (new) solutions which are entering or are on the market today to support competitiveness; examples are an open and free access to the mobile device capabilities (including the NFC antenna, any component being it the SE or HCE).

It has to be noted that numerous mobile offerings are gaining consumer attention, interest and preference. Nevertheless, consumer awareness of mobile device usage for payment services initiation is in some countries still low. In the absence of an MSCT interoperability framework or scheme, the will from MSCT service providers to conquer the consumer preference, leads into a movement towards the use of "closed loop" solutions, which hinders widespread use and pan-European interoperability of MSCT services, leading to market fragmentation and PSU dissatisfaction.

Complexity and security of mobile devices

A mobile device is a complex piece of equipment with many different components, including the baseband, operating system, firmware, software, multiple external interfaces (including

the NFC controller), possibly a Trusted Execution Environment (TEE) and one or multiple Secure Elements (SEs). Moreover, the production of these components involves different manufacturers before integration in the mobile device. This means that functional and security standards should be ensured throughout the whole production cycle. Also the presence of different software on the mobile device, developed by diverse vendors or service providers, poses a significant challenge to the integrity of the mobile device ecosystem. The versatility of the mobile devices leaves stakeholders in the ecosystem (including MSCT providers, merchants, other service providers, …) with major challenges with respect to the development of strategies / road maps with a viable business case and market reach.

For MSCT service providers there is a strong dependency on the handset manufacturers and mobile OS providers, which is a highly competitive space with little cooperation on standardisation. Therefore they face a huge complexity with different solutions for each handset and/or mobile OS. This means that they need to develop their applications for a large number of different mobile platforms (combinations of different hardware and software) in view of the current platform incompatibilities. This obviously comes with a cost impact and may in some cases also lead to consumer confusion. The fact that there are multiple solutions on the market which are different - read not compatible - makes it challenging for the supply side. Moreover, once the devices are in usage by the consumer, there are a number of additional challenges which remain to be addressed; security and privacy are the most relevant ones.

Several organisations (see Chapter 23) have already developed specifications and standards for securing the mobile contactless payment environment. Furthermore, they have also created some testing and certification activities in accordance with those standards and specifications.

In this context it is also important to mention the development of the specifications by ETSI of the “Smart Secure Platform” (SSP) that addresses some of the concerns raised above (see Chapter 12). However, availability and market adoption of this new platform is still to be achieved.

Lack of clarity of European rules and regulations

There is still lack of clarity regarding EU rules and regulations such as the PSD2 [5], the RTS [6] and the GDPR [7], also related to their interplay, that might have an impact on the take-up of MSCTs in view of different interpretations with respect to strong customer authentication with dynamic linking and the applicability of the exemptions (see Chapter 8), consumer consent (see Chapters 7 and 22), the involvement of a PISP, or the transfer and processing of sensitive payment data (e.g. related to risk-based authentication - see section 8.5)[59]. At the time of publication of this document, additional clarifications are expected by the upcoming adoption of the PSD3 and PSR, revising the PSD2.

PSU on-boarding

[59] See EBA Q&A 2020_5365-5367, 5476, 5477, 5570-5573, 5587 and 2021_6298.

The trust in MSCTs, more in particular for cross-border payments, strongly relies on the mutual recognition and trust in PSU on-boarding procedures and mechanisms. Weak customer on-boarding procedures may lead to PSU impersonation and fraudulent transactions. More in particular, related to mobile initiated instant SCTs this is perceived as an important risk to be adequately addressed (see Chapter 15).

Recognition of payee name

It is important for trust and transparency that the commercial brand name of the payee is provided to the payer's MSCT provider so that it can be properly used in any communication (MSCT app, bank account statements, ...) towards the payer. It might also facilitate every further communication between the payer and the payee.

In this context, the work done by the ERPB WG on Transparency for retail payments end-users should be mentioned [20].

Currency conversion

SCTs have to be denominated in Euros. For retail payments, if the consumer and/ or the merchant are located in non-Euro countries and only their non-Euro account is linked to the MSCT service with their respective ASPSPs, MSCT transactions may be more cumbersome and additional costs may be involved in view of the currency conversion. Transparency to the customer is expected by regulation[60].

13.2 Opportunities

Whilst there are challenges to achieve interoperability for MSCTs as described in Chapter 17 to 22 and above, the introduction of these solutions also offers a number of opportunities to PSUs. More in particular, the immediate availability of funds for MSCTs based on SCT Instant is an attractive feature for the payee. For P2P payments, it is attractive for the payer that they can initiate an MSCT anywhere and anytime. Moreover, the migration of the SCT (instant) schemes to the new version of ISO 20022 payment messages would enable a richer and consistent information exchange between the payee and the payer, and as such provide more transparency to the payer for MSCTs.

For some MSCT payments, the initiation of the payment involves an exchange of data that allows the identification of a known consumer with the merchant's backend system, allowing reconciliation with a merchant's loyalty program or other additional services. The consumer identification can be used for instance to trigger the collection or redemption of loyalty points in combination with the payment transaction. This may provide value added benefits for a retailer and their customer base.

Depending on market demand, mobile payments based on SCT (Instant) could support more use cases and features, including new ones, subject to appropriate business cases.

[60] See Regulation (EU) 2019/518 of the European Parliament and of the Council of 19 March 2019 amending Regulation (EC) No 924/2009 as regards certain charges on cross-border payments in the Union and currency conversion charges (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2019:091:TOC)

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

14 Conclusions

This document provides interoperability guidance for MSCTs. It aims to reflect the current state of play and market situation at the time of writing while being brand and implementation model agnostic. On the other hand, it needs to be recognised that the MSCT ecosystem is rapidly evolving and expanding. To date most of the solutions are "closed-loop" solutions, not interoperable between each other. Market adoption of “interoperable” MSCTs constitutes a key assumption for the further evolution and expansion of the ecosystem.

The document aims through the description of some illustrative MSCT use cases to provide an insight into the main issues related to the initiation of (instant) SEPA credit transfers for different payment contexts. Hereby MSCT use cases whereby payer and payee are customers of different MSCT service providers are involved for the payer and the payee have been considered. Furthermore, MSCT transaction aspects such as payer/payee acknowledgements and notification messages, have been specified The document analyses in detail the technical interoperability of MSCTs based on payee- or payer-presented data and specifies the technical interoperability requirements between MSCT service providers, for successful, and rejects, which are also depicted in some illustrative process flows using a so-called “HUB” between the payer’s and payee’s MSCT service providers. It defines the minimum data to be exchanged between the payer and payee to enable the initiation of an MSCT and specifies for this a payee- and payer-presented QR-code for MSCTs, while ensuring alignment with the document on Standardisation of QR-codes for MSCTs (see[12]). It further specifies the minimum data sets for all interoperability messages between the respective MSCT service providers of the payer and the payee. Additional interoperability models including a Payment Initiation Service Provider (PISP) or a Collecting PSP (on behalf of the merchant) are also included. Finally, the document identifies the main interoperability challenges but also opportunities for MSCTs.

Note that subjects such as business cases and revenue models for the MSCT value chain belong to the commercial space and therefore are not addressed in this document.

While producing this document, the multi-stakeholder group has noticed a number of “challenges and barriers” that will need to be properly addressed to achieve full interoperability of MSCT transactions (see Chapter 24).

This includes:

- The availability of a technical infrastructure to interconnect the different MSCT service providers notably for the support of token/proxy-based MSCTs and MSCT confirmation and notification messages to PSUs (payers and payees);

- The development of an implementation specification for the MSCT QR-codes specified in this document and the subsequent adoption by the market;

- Next to the technical aspects, also the operating rules, liabilities, adherence to these requirements and governance should be addressed. This could be achieved through the set-up of a dedicated "MSCT interoperability framework or MSCT scheme" to which the MSCT service providers (existing and new ones) should participate to ensure interoperability of MSCT services;

Related to the challenges listed above the following should be noted:

- A report on an interoperability framework for instant payments at the POI has been developed by the dedicated ERPB working group (see [40]).

- The MSG MSCT has developed a document on the *Standardisation and governance of QR-codes for Instant Payments at the Point of Interaction* (IPS at the POI, see [31]).

"Request-to-Pay" services could enhance the PSU experience for MSCTs for all payment contexts. The SRTP scheme [26] complements the current document and will further contribute to the customer adoption of MSCTs.

Also the work done in the ERPB WG on SEPA API access scheme [42] and the SPAA scheme [ref] complements the current document for MSCTs involving a PISP.

Another challenge for MSCT service providers remains the support of the different mobile platforms. Mobile devices have different operating systems with different execution environments which directly impacts the "secure" communication between different components in the device. Therefore the development of the "Smart Secure Platform" (enabling the provision of value-added services relying on authentication of the user, regardless of the mobile device, communication channel and underlying technology) by ETSI is of utmost importance. The multi-layered functional and security approach taken by ETSI will ensure, subject to sufficient market take-up, more flexibility and portability for mobile payment providers.

There is still a dependency for the consumer on the type of mobile device with respect to the choice of MSCT services. Therefore access to all resources needed on the mobile device, in order to ensure that the consumer can have a choice amongst payment applications from different mobile payment providers (e.g. the mobile device contactless interface), independently of the mobile device and the operating system used, should be ensured by all handset manufacturers and mobile OS developers[61].

[61] The proposal for a Regulation on contestable and fair markets in the digital sector ("Digital Markets Act") under development by the EU co-legislators, might address also this issue.

The impact of the PSD2 [5] with the RTS [6] and the GDPR [7] on payments and more in particular the uncertainty regarding some provisions as well as their interplay when applied to MSCTs might be a barrier for the quick take-up of MSCTs[62] (see Chapters 6, 5 and 12). However it is expected that the adoption of the IPR and the upcoming adoption of the PSR and PSD3 contributes to the overcoming of these barriers.

By developing this guidance the multi-stakeholder group aimed to contribute to a competitive MSCT market, by providing the different stakeholders an insight into the different service, technical and security aspects involved. The document could serve as a reference basis for making certain implementation choices.

In light of major new trends, and the rapidly changing market, the multi-stakeholder group recommends for the present document to be regularly updated in order to reflect the state of play related to MSCTs and to keep it aligned with the various documents referenced.

The MSCG MSCT has further developed the specifications for QR-codes for MSCTs (covering all payment contexts) and the EPC submitted it to CEN – the the European standardisation body, to become an European standard. Also the usage of other proximity technologies than QR-codes for MSCTs, such as NFC and BLE (see Chapter 7.2), have been investigated and a related document was published in June 2023.

[62] See EBA Q&A 2020_5247, 5365-5367, 5476, 5477, 5570-5573, 5587 and 2021_6298.

Annex 1: Overview of MSCT related error cases

This annex provides an overview on the main errors for MSCTs based on respectively payee- and payer-presented data.

A1.1 MSCTs based on payee-presented data

The table below identifes the different errors which may occur with MSCTs based on payee-presented data for SCT Inst or SCT. For the relevant cases, a mapping is made to the different categories identified in Table 20 and Table 23 in this document.

Error cases for MSCTs based on payee-presented data					
#	Issue description	Mapping on Table 20 and Table 23			Inquiry – Table 49
		Cat 1 - Reject by payer MSCT SP	Cat 2 - Reject by payer ASPSP	Cat 3 – Unsuccessful transaction	
Communication errors between the parties					
1	TLS mutual authentication issues	X	X	X	X
2	Incorrect message syntax	X	X	X	X
3	No server response, timeouts, etc.	X	X	X	X
4	Communication interruptions/failures	X	X	X	X
Issues with the payer MSCT app					
5	MSCT app not recognised by payer MSCT service provider server	X			
6	Payer device not properly personalised (e.g., missing credentials)	X			
QR-code scanning issues					
7	Incorrect QR-code (syntax issue, invalid checksum/signature, etc.)				
8	QR-code impossible to read/partially read				
Payer authentication failure					
9	Incorrect user verification (mobile code, biometrics) by mobile device	X	X		
10	Blocked payer mobile device due to too many consecutive user verification errors	X	X		
11	Incorrect authentication code	X	X		
Dynamic linking errors					
12	Payee data received in authentication request does not match payee data received in payment initiation request	X	X		
13	Dynamic linking verification failure	X	X		
Issues with tokens/proxies					
14	Payee token/proxy not found or invalid	X			X
Payer ASPSP verification issues (other than failed SCA)					

15	Sanction screening / AML/ Fraud controls by payer ASPSP		X		
16	Invalid payer IBAN		X		
17	Insufficient funds		X		
18	Spending limits reached or other risk assessment errors		X		
SCT Inst /SCT execution errors					
19	Sanction screening / AML/ Fraud controls by payee ASPSP			X	
20	Invalid payee IBAN			X	
21	Other SCT Inst /SCT processing issue			X	X
Notification errors					
22	Failure to notify the payee of the correct SCT Inst / SCT execution				X
23	Failure to notify the payee of issues/errors prior to SCT Inst / SCT execution				X
24	Failure to notify the payee of issues/errors with the SCT Inst / SCT execution				X
25	Failure to notify the payer of the correct SCT Inst / SCT execution				X
26	Failure to notify the payer of issues/errors prior to SCT Inst / SCT execution				X
27	Failure to notify the payer of issues/errors with the SCT Inst / SCT execution				X

Table 41: Overview on errors for MSCTs based on payee-presented data

A1.2 MSCTs based on payer-presented data

The table below identifies the different errors which may occur with MSCTs based on payer-presented data for SCT Inst or SCT. For the relevant cases, a mapping is made to the different categories identified in Table 36 and Table 39 in this document.

Error cases for MSCTs based on payer-presented data						
#	Issue description	Mapping on Table 36 and Table 39				Inquiry Table 50
		Cat 1 - Reject by payee MSCT SP	Cat 2 - Reject by payer MSCT SP	Cat 3 - Reject by payer ASPSP	Cat 4 - Unsuccessful transaction	
Communication errors between the parties						
1	TLS mutual authentication issues	X	X	X	X	X
2	Incorrect message syntax	X	X	X	X	X
3	No server response, timeouts, etc.	X	X	X	X	X
4	Communication interruptions/failures	X	X	X	X	X
Issues with the payer MSCT app						
5	MSCT app not recognised by payer MSCT service provider server		X			

6	Payer device not properly personalised (e.g., missing credentials, invalid payer token)		X			
QR-code scanning issues						
7	Incorrect QR-code (syntax issue, invalid checksum/signature, etc.)	X				
8	QR-code impossible to read/partially read	X				
Payer authentication failure						
9	Incorrect user verification (mobile code, biometrics) by mobile device		X	X		
10	Blocked payer mobile device due to too many consecutive user verification errors		X	X		
11	Incorrect authentication code		X	X		
Dynamic linking errors						
12	Payee data received in authentication request does not match payee data received in payment initiation request		X	X		
13	Dynamic linking verification failure		X	X		
Issues with tokens/proxies						
14	Payer token/proxy not found or invalid		X	X		X
Payer ASPSP verification issues (other than failed SCA)						
15	Sanction screening / AML/ Fraud controls by payer ASPSP			X		
16	Invalid payer IBAN			X		
17	Insufficient funds			X		
18	Spending limits reached or other risk assessment errors			X		
SCT Inst /SCT execution errors						
19	Sanction screening / AML/ Fraud controls by payee ASPSP				X	
20	Invalid Payee IBAN				X	
21	Other SCT Inst /SCT processing issue				X	X
Notification errors						
22	Failure to notify the payee of the correct SCT Inst / SCT execution					X
23	Failure to notify the payee of issues/errors prior to SCT Inst / SCT execution					X
24	Failure to notify the payee of issues/errors with the SCT Inst / SCT execution					X
25	Failure to notify the payer of the correct SCT Inst / SCT execution					X

26	Failure to notify the payer of issues/errors prior to SCT Inst / SCT execution					X
27	Failure to notify the payer of issues/errors with the SCT Inst / SCT execution					X

Table 42: Overview on errors for MSCTs based on payer-presented data

Annex 2: Minimum data sets for MSCT interoperability messages

A2.1 Introduction

This section specifies the minimum data sets for the MSCT interoperability messages listed in Chapter 21. The messages cover both MSCTs based on SCT Inst or SCT. For each type identified in these tables, an overview table with the messages involved is provided, followed by tables detailing the minimum data set for each message, with an indication for each data element whether it is mandatory (M), optional (O) or conditional (C)[63].

A2.2 Transaction Information messages

This section provides the *Transaction Information messages* for MSCTs based on SCT Inst or SCT using payee-presented data as defined in Chapter 18. The minimum data elements to be included in these messages are specified below.

Transaction information messages	
TIRQ	Transaction Information request message by payer MSCT service provider to payee MSCT service provider
TIRP	Transaction Information response message by payee MSCT service provider to payer MSCT service provider

Table 43: Overview transaction information messages

Transaction information request

[63] This means that it is dependent on certain conditions, e.g., if it the MSCT is successful, unsuccessful or a reject.

TIRQ	Inter-MSCT service provider transaction information request by payer MSCT service provider to payee MSCT service provider
Description	This dataset describes the content of the transaction information request by the payer MSCT service provider to the payee MSCT service provider via the HUB.
Attributes contained	• The payee proxy or token (M) • The payer MSCT service provider identifier (M) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • The expiry date of the Transaction information request (O) • Type of payment instrument (SCT or SCT Inst) (O) • Date and Time stamp (M)

Table 44: Dataset for transaction information request

Transaction information response

TIRP	Inter-MSCT service provider transaction information response by payee MSCT service provider to payer MSCT service provider
Description	This dataset describes the content of the transaction information response by the payee MSCT service provider to the payer MSCT service provider via the HUB.
Attributes contained	• The payee proxy or token (M) • The name / trade name of the payee (M) • The name / trade name of the payee reference party (O) • The IBAN of the payee (C)

TIRP	Inter-MSCT service provider transaction information response by payee MSCT service provider to payer MSCT service provider
	• The transaction amount (C) • The currency (C) • The Merchant Category Code (C) • The payer MSCT service provider identifier (M) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (O) • Place holder for charging (O) • Date and Time stamp (M)

Table 45: Dataset for transaction information response

A2.3 Lock Transaction messages

This section provides the *Conditional Lock Transaction messages* for MSCTs, based on SCT Inst or SCT, using payee-presented data. These conditional messages may be used to lock a specific MSCT transaction for a given payer in C2B payment contexts as defined in Chapter 18. The minimum data elements to be included in these messages are specified below.

Lock transaction messages	
LTRQ	Lock transaction request message by payer MSCT service provider to payee MSCT service provider
LTRP	Lock transaction response message by payee MSCT service provider to payer MSCT service provider

Table 46: Overview lock transaction messages

Lock transaction request

LTRQ	Inter MSCT service provider lock transaction request by payer MSCT service provider to payee MSCT service provider
Description	This dataset describes the content of the lock transaction request by the payer MSCT service provider to the payee MSCT service provider via the HUB.
Attributes contained	• The payer name/trade name (M) • The transaction amount (M) • The currency (M) • The payer MSCT service provider identifier (M) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (M) • Date and Time stamp (M)

Table 47: Dataset for lock transaction request message

Lock transaction response

LTRP	Inter-MSCT service provider lock transaction response by payee MSCT service provider to payer MSCT service provider
Description	This dataset describes the content of the lock transaction response by the payee MSCT service provider to the payer MSCT service provider via the HUB.
Attributes contained	• Lock transaction status (M) • Date and Time stamp (M) • A copy of the mandatory minimum data elements in LTRQ to which is being responded (M)

Table 48: Dataset for lock transaction response message

A2.4 Payment Request

This section provides an overview on the different messages for the *Payment Request* for MSCTs, based on SCT Inst or SCT, using payer-presented data as defined in Chapter 19. The minimum data elements to be included in these messages are specified below.

Payment Request messages	
PR1	Payment request message by payee to payee MSCT service provider
PR2	Payment request message by payee MSCT service provider to payer MSCT service provider
CRPR1	Confirmation of receipt of payment request message by payer MSCT service provider to payee MSCT service provider
CRPR2	Confirmation of receipt of payment request message by payee MSCT service provider to payee

Table 49: Overview of payment request messages

Payment request messages

From payee to their MSCT service provider

PR1	Payment request message by payee to payee MSCT service provider
Description	This dataset describes the content of the Payment Request message as presented by the payee to the payee MSCT service provider.
Attributes contained	• The payer identification data (M) • The transaction amount (M) • The currency (M) • The remittance Information sent by the payee to the payer (O) • The payer MSCT service provider identifier (M) • The Requested Execution Date/Time of the Payment Request (M)

PR1	Payment request message by payee to payee MSCT service provider
	• The IBAN of the payee (M) • The name of the payee (M) • The trade name of the payee (M for C2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The address of the payee (O) • The BIC code of the payee ASPSP (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • The purpose of the Payment Request (O) • The Merchant Category Code (MCC) (M for C2B) • The expiry date of the Payment Request (O) • Type of payment instrument requested by the payee (SCT or SCT Inst) (M) • Flag notification message required (O) • Place holder for charging (O)

Table 50: Dataset for payment request message by the payee to the payee MSCT service provider

Between MSCT service providers

PR2	Inter-MSCT service provider payment request message by payee MSCT service provider to payer MSCT service provider
Description	This dataset describes the content of the Payment Request presentment by the payee MSCT service provider to the payer MSCT service provider via the HUB.

PR2	Inter-MSCT service provider payment request message by payee MSCT service provider to payer MSCT service provider
Attributes contained	• The payer identification data (M) • The transaction amount (M) • The currency (M) • The remittance information (O) • The payer MSCT service provider identifier (M) • The Requested Execution Date/Time of the Payment Request (M) • The IBAN of the payee (M) • The name of the payee (M) • The trade name of the payee (M for C2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The address of the payee (O) • The BIC code of the payee ASPSP (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • The purpose of the Payment Request (O) • The Merchant Category Code (MCC) (M for C2B) • The expiry date of the Payment Request (O) • Type of payment instrument requested by the payee (SCT or SCT Inst) (M) • Flag notification message required (O)

PR2	Inter-MSCT service provider payment request message by payee MSCT service provider to payer MSCT service provider
	• Additional unique reference provided by the payee MSCT service provider (O) • Type of payment instrument (SCT or SCT Inst) (M) • Place holder for charging (O)

Table 51: Dataset for payment request message by the payee MSCT service provider to the payer MSCT service provider

Confirmations of receipt of payment request

Between MSCT service providers

CRPR1	Inter-MSCT service provider confirmation of receipt of payment request by payer MSCT service provider to payee MSCT service provider
Description	This dataset describes the content of the confirmation of receipt of a Payment Request message by the payer MSCT service provider to the payee MSCT service provider via the HUB.
Attributes contained	• Confirmation of receipt (M) • Date and Time stamp (M) • A copy of the mandatory minimum data elements in PR2 which is being confirmed (M)

Table 52: Dataset for confirmation of receipt of payment request by the payer MSCT service provider to the payee MSCT service provider

From payee MSCT service provider to payee

CRPR2	Confirmation of receipt of payment request by payee MSCT service provider to payee
Description	This dataset describes the content of the confirmation of receipt of a payment request message by the payee MSCT service provider to the payee.
Attributes contained	• Confirmation of receipt (M) • Date and Time Stamp (M) • A copy of the mandatory minimum data elements in PR2 which is being confirmed (M)

Table 53: Dataset for confirmation of receipt of payment request by the MSCT service provider to the payee

A2.5 Notification of Reject messages

This section provides an overview on the different messages for the *Notification of Reject* for MSCTs based on SCT Inst or SCT, using payer- or payee-presented data as defined in Chapter 18 and Chapter 19. The minimum data elements to be included in these messages are specified below.

Notification of reject messages	
NR1	Notification of reject message by payer ASPSP to payer MSCT service provider
NR2	Notification of reject message by payer MSCT service provider to payee MSCT service provider
NR3	Notification of reject message by payer MSCT service provider to payer
NR4	Notification of reject message by payee MSCT service provider to payee

Table 54: Overview of notification of reject messages

From payer ASPSP to payer MSCT service provider

NR1	Notification of reject by payer ASPSP to payer MSCT service provider
Description	This dataset describes the content of the notification of reject message from the payer ASPSP to the payer MSCT service provider.
Attributes contained	• Type of reject (M) • The BIC code of the payer ASPSP (M) • The name of the payer (M) • The transaction amount (M) • The currency (M) • The remittance Information (O)

NR1	Notification of reject by payer ASPSP to payer MSCT service provider
	• The payer MSCT service provider identifier (M) • The IBAN of the payee (M) • The name of the payee (M) • The trade name of the payee (M for C2B and B2B) • The payee reference party (O) • The trade name of the payee reference party (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Reason code for reject (M) • Type of payment instrument (SCT or SCT Inst) (M) • Date and Time stamp (M)

Table 55: Dataset for notification of reject message by the payer ASPSP to the payer MSCT service provider

Between MSCT service providers

NR2	Inter-MSCT service provider notification of reject by payer MSCT service provider to payee MSCT service provider
Description	This dataset describes the content of the notification of reject by the payer MSCT service provider to the payee MSCT service provider via the HUB.
Attributes contained	• Type of reject (M) • The name of the payer (M) • The transaction amount (M) • The currency (M) • The remittance Information (O)

NR2	Inter-MSCT service provider notification of reject by payer MSCT service provider to payee MSCT service provider
	• The payer MSCT service provider identifier (M) • The IBAN of the payee (M) • The name of the payee (M) • The trade name of the payee (M for C2B and B2B) • The payee reference party (O) • The trade name of the payee reference party (O) • The BIC code of the payer ASPSP (O) • The BIC code of the payee ASPSP (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Reason code for reject (M) • Additional unique reference provided by the payer MSCT service provider (O) • Type of payment instrument (SCT or SCT Inst) (M) • Date and Time stamp (M) • Place holder for charging (O)

Table 56: Dataset for notification of reject message by the payer MSCT service provider to the payee MSCT service provider

Between payer MSCT service provider and payer

NR3	Notification of reject by payer MSCT service provider to payer
Description	This dataset describes the content of the notification of reject from the payer MSCT service provider to the payer.

NR3	Notification of reject by payer MSCT service provider to payer
Attributes contained	• Type of reject (M) • The transaction amount (M) • The currency (M) • The IBAN of the payer (O) • The remittance Information (O) • The name of the payee (M) • The trade name of the payee (M for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (O) • Reason code for reject (M) • Date and Time stamp (M)

Table 57: Dataset for notification of reject message by the payer MSCT service provider to the payer

Between payee MSCT service provider and payee

NR4	Notification of reject by payee MSCT service provider to payee
Description	This dataset describes the content of the notification of reject by the payee MSCT service provider to the payee.
Attributes contained	• Type of reject (O) • The name of the payer (M) • The transaction amount (M) • The currency (M)

NR4	Notification of reject by payee MSCT service provider to payee
	• The remittance Information (O) • The name of the payee (O) • The IBAN of the payee (O) • The trade name of the payee (O for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (O) • Date and Time stamp (M)

Table 58: Dataset for notification of reject message by the payee MSCT service provider to the payee

A2.6 Notification of Successful/Unsuccessful Transaction messages

This section provides an overview on the different messages for the *Notification of Successful / Unsuccessful transaction* for MSCTs, based on SCT Inst or SCT, using payer- or payer-presented data as defined in Chapter 18 and Chapter 19. The minimum data elements to be included in these notification messages are specified below.

Notification of successful / unsuccessful transaction messages	
NT1	Notification of successful / unsuccessful transaction message by payer ASPSP to payer MSCT service provider
NT2	Notification of successful /unsuccessful transaction message by payer MSCT service provider to payee MSCT service provider
NT3	Notification of successful /unsuccessful transaction message by payer MSCT service provider to payer

NT4	Notification of successful /unsuccessful transaction message by payee MSCT service provider to payee

Table 59: Overview of notification of successful / unsuccessful transaction messages

From payer ASPSP to payer MSCT service provider

NT1	**Notification of successful / unsuccessful transaction by payer ASPSP to payer MSCT service provider**
Description	This dataset describes the content of the notification of successful / unsuccessful transaction by the payer ASPSP to the payer MSCT service provider.
Attributes contained	• The BIC code of the payer ASPSP (M) • Transaction status (M) • The name of the payer (M) • The transaction amount (M) • The currency (M) • The remittance information (O) • The Payer MSCT service provider identifier (M) • The IBAN of the payee (M) • The name of the payee (M) (account holder) • The trade name of the payee (M for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The payee MSCT service provider identifier (M) • The Identification code of the MSCT scheme (M) • The transaction identifier (M)

NT1	Notification of successful / unsuccessful transaction by payer ASPSP to payer MSCT service provider
	• Reason code for unsuccessful transaction (C) • Identification of party not accepting the transaction (C) • Additional unique reference provided by the payer MSCT service provider (O) • Type of payment instrument (SCT or SCT Inst) • The settlement date of the transaction (C) • Date and Time stamp (M) • Place holder for charging (O)

Table 60: Dataset for notification of successful / unsuccessful transaction message by the payer ASPSP to the payer MSCT service provider

Between MSCT service providers

NT2	Inter-MSCT service provider notification of successful / unsuccessful transaction between payer MSCT service provider and payee MSCT service provider
Description	This dataset describes the content of the notification of successful / unsuccessful transaction by the payer MSCT service provider to the payee MSCT service provider via the HUB.
Attributes contained	• Transaction status (M) • The name of the payer (M) • The transaction amount (M) • The currency (M) • The remittance information (O) • The payer MSCT service provider identifier (M)

NT2	Inter-MSCT service provider notification of successful / unsuccessful transaction between payer MSCT service provider and payee MSCT service provider
	• The IBAN of the payee (M) • The name of the payee (M) (account holder) • The trade name of the payee (M for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Reason code for unsuccessful transaction (C) • Identification of party not accepting the transaction (C) • Additional unique reference provided by the Payer MSCT service provider (O) • Type of payment instrument (SCT or SCT Inst) • The settlement date of the transaction (C) • Date and Time stamp (M) • Place holder for charging (O)

Table 61: Dataset for notification of unsuccessful transaction message by the payer MSCT service provider to the payee MSCT service provider

Between payer MSCT service provider and payer

NT3	Notification of successful / unsuccessful transaction by payer MSCT service provider to payer
Description	This dataset describes the content of the notification of successful / unsuccessful transaction by the payer MSCT service provider to the payee MSCT service provider.
Attributes contained	• Transaction status (M) • The transaction amount (M) • The currency (M) • The remittance Information (O) • The payer MSCT service provider identifier (M) • The IBAN of the payer (O) • The name of the payee (M) • The trade name of the payee (M for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (O) • Reason code for unsuccessful transaction (M) • The settlement date of the transaction (C) • Date and Time stamp (M)

Table 62: Dataset for notification of successful / unsuccessful transaction message by the payer MSCT service provider to the payer

Between payee MSCT service provider and payee

NT4	Notification of successful / unsuccessful transaction by payee MSCT service provider to payee
Description	This dataset describes the content of the notification of successful / unsuccessful transaction by the payee MSCT service provider to the payee.
Attributes contained	• Transaction status (M) • The name of the payer (M) • The transaction amount (M) • The currency (M) • The remittance Information (O) • The name of the payee (O) • The IBAN of the payee (M) • The trade name of the payee (O for C2B and B2B) • The name of the payee reference party (O) • The trade name of the payee reference party (O) • The payee MSCT service provider identifier (O) • The transaction identifier (M) • Type of payment instrument (SCT or SCT Inst) (O) • The settlement date of the transaction (C) • Date and Time stamp (M)

Table 63: Dataset for notification of unsuccessful transaction message by the payee MSCT service provider to the payee

A2.7 Inquiry messages

This section provides an overview on the different messages for the *Inquiry messages* between MSCT service providers for MSCTs, based on SCT Inst or SCT, using payer- or payer-presented data as defined in Chapter 21. The minimum data elements to be included in these notification messages are specified below.

Inquiry messages	
IRQ	Inquiry request message between MSCT service providers
IRP	Inquiry response message between MSCT service providers

Table 64: Overview inquiry messages for MSCTs

Inquiry request message

IRQ	Inter-MSCT service provider inquiry request message
Description	This dataset describes the content of the inquiry request message exchanged between the payer and the payee MSCT service providers via the HUB.
Attributes contained	• Check status request (M) • The payer MSCT service provider identifier (M) • The payee MSCT service provider identifier (M) • The identification code of the MSCT scheme (M) • The transaction identifier (M) • Date and Time stamp (M)

Table 65: Dataset for inquiry request message between MSCT service providers

Inquiry response message

IRP	Inter-MSCT service provider inquiry response message
Description	This dataset describes the content of the inquiry response message exchanged between the payer and the payee MSCT service providers via the HUB.
Attributes contained	• Check status response information (M) • Date and Time stamp (M)

IRP	Inter-MSCT service provider inquiry response message
	• A copy of the mandatory date elements of IRQ to which is responded (M)

Table 66: Dataset for inquiry response message between MSCT service providers

Notes:

- The different status to be reflected in the data field Check status response would need to be defined under an MSCT interoperability framework.
- The reply to an Inquiry request may be a re-sending of a previous message instead of an Inquiry response message.

Annex 3: The multi-stakeholder group

The following organisations have contributed to the development of this 3rd release of the MSCT IG through participation in the Multi-Stakeholder Group Mobile Initiated SEPA (Instant) Credit Transfers (MSG MSCT) Plenary or one of its work-streams:

ABI, representing EPC
BEUC - European Consumer Organisation
Blue Code, representing EMPSA
BP
Circle K
Crédit Agricole, representing EPC
Crédit Mutuel, representing EPC
DNB Bank, representing EPC
EACT - European Association of Corporate Treasurers
EMVCo
EPI
ETPPA, representing EPC
Fiserv
Getswish
H&M, representing EuroCommerce
Ikea, representing EuroCommerce
Mastercard
Millenium BCP, representing EPC
Monei
National Clearing House KIR
Nexi Payments
OpenWay
Orange, representing GSMA
Payconiq
Rabobank, representing EPC
TAS Group
Thales, representing Smart Payment Association
Idemia, representing Smart Payment Association
W3C
nexo
VippsMobilepay
Eurosystem and the ECB as observer
European Commission as observer

Table 67: The multi-stakeholder group MSCT

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 Intellectual Property right.