Framework for interoperability of instant payments at the point of interaction (IPs at the POI)

ERPB Inst@POI 09-20
Version 1.1
7 December 2020

Public

Euro Retail Payments Board (ERPB)

Framework for interoperability of instant payments at the point of interaction

(IPs at POI)

Table of Contents

List of tables

List of figures

1 Executive summary

In March 2020 the ERPB established the ERPB working group on a framework for interoperability of instant payments at the Point-of-Interaction (IPs at the POI) to foster the development of pan-European instant payment services for this use case. As follow-up on the report from the ERPB working group on IPs at the POI in 2019, the new working group's focus was on a subset of the recommendations endorsed by the ERPB at their November 2019 meeting, i.e. those related to the development of a framework to manage the interoperability rules and appropriate governance for solutions enabling instant payments at the POI.

In the context of this document an IP at POI is an instant payment transaction based on a SEPA Instant Credit Transfer (SCT Inst), by a consumer to a merchant at the POI which may be for example a Point-of-Sale (POS) in a store or a payment page on an e-or m-commerce website.

For the development of this document, the ERPB WG leveraged the work undertaken by the Multi-Stakeholder Group for Mobile Initiated SEPA (Instant) Payments (MSG MSCT) and this report refers to the various documents they released on MSCTs.

The present document first provides an overview and taxonomy for IPs at POI. Next, it specifies the technical interoperability requirements based on a generic 4-corner model based on a HUB[1] which are subsequently illustrated in some process flows. This is followed by the specifications of the minimum data sets to be exchanged between the consumer and the merchant, the derived QR-code standards and the minimum data elements for the interoperability messages exchanged over the HUB.

Next some security and trust aspects are included for IPs at the POI. As requested in the mandate, a dedicated chapter defines the "Security requirements for payment service user on-boarding", developed in a Joint Task Force with the MSG MSCT.

[1] An infrastructure ensuring connectivity between IP service providers.

The document defines furthermore the interoperability rules and provides a high level description of a Framework Governance for which more work on further details and its set-up would be required.

In two separate annexes, the document also analyses IP at POI models involving a Payment Initiation Service Provider (PISP) or a Collecting Payment Service Provider (CPSP) as a collecting entity of transactions on behalf of the merchants and their respective impacts on the interoperability of IPs at the POI.

While developing this document, the ERPB WG has identified a number of challenges that would need to be addressed before this interoperability framework for IPs at the POI with an appropriate governance could be established. This includes at least the following topics:

- clarifications to be provided by the EBA Q&A tool on the different questions related to this document and its Annex 1 that have been coordinated with but entered by the MSG MSCT;
- the additional services for instant SCTs that have been included in the Recommendation E in the ERPB Statement of November 2019;
- the development of a recognition label as recommended in the Recommendation A in the ERPB Statement of November 2019.

The ERPB WG wishes to make the following recommendations to the ERPB:

#	Addressee	Rationale	Recommendation	Dead-line
A	MSG MSCT[2]	To address the technical gaps identified during the development of the Interoperability Framework for IPs at the POI	• Analyse interoperability of additional flows and r-messages between the respective IP service providers in case of unsuccessful /failed transactions;	June 2021

[2] Subject to the approval of the Extension of the mandate of the MSG MSCT by the EPC Board in November 2020.

			• Further analyse technical interoperability for models involving a PISP or CPSP; • Analyse impact of replies on EBA Q&A questions[3] posted by the MSG MSCT on technical interoperability of IPs at POI and related security aspects; • Develop use cases for IPs at POI whereby the consumer device has no internet connection at the transaction time (so-called offline use case) and analyse their impact on interoperability. These deliverables[4] should serve as inputs to any further work on an Interoperability framework for IPs at the POI.	
B[5]	Group with multi-stakeholder participation consisting of market participants in card	Need to ensure that the consumer's choice of a given payment instrument to conduct a payment transaction at the POI is respected	Develop standards, business and technical requirements as appropriate, leading to interoperable specifications that ensure consumer selection of preferred payment instrument (card payment or SCT Inst) to conduct a payment transaction at the POI (physical or virtual POI) based on the deliverable ERPB Inst@POI 45-20v1.1.	Nov. 2021

[3] See EBA Q&A 2020_5365-5367, 5476, 5477, 5570-5573, 5587)
[4] In accordance with the scope of the proposed MSG MSCT mandate extension (MSG MSCT 91-20).
[5] This recommendation is also contained in document ERPB Inst@POI 45-20v1.1.

	and SCT Inst payments			
C	Group with multi-stakeholder participation	A dedicated framework is needed to manage the interoperability rules and appropriate governance for IP at POI solutions.	To evaluate the outcome of the following: • The clarifications to be provided by the EBA Q&A tool on the different questions related to this document and its Annex 1 that have been coordinated with but entered by the MSG MSCT; • The additional services for instant SCTs that have been included in the Recommendation E in the ERPB Statement of November 2019; • The development of a recognition label as recommended in the Recommendation A in the ERPB Statement of November 2019; • The deliverables developed per Recommendation A above • The market situation in the light of other on-going initiatives with respect to the establishment of an interoperability framework for IPs at the POI. At the same time the current document would be updated as appropriate. The proposal is that this work is carried out by a group with a similar composition as the present WG,	June 2021 till November 2021

			depending on the outcome of the deliverables mentioned above and the market situation in June 2021.	

Note that for the "Specifications for consumer selection of preferred payment instrument", as requested in the mandate, the ERPB WG has established a Joint Task Force with the European Cards Stakeholders Group (ECSG) and this deliverable is submitted to the ERPB as a separate document (see ERPB Inst@POI 045-20v1.1).

2 Document information

2.1 Structure of the document

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

- Chapter 1 is the executive summary;
- Chapter 2 provides the document information;
- Chapter 3 includes general information on the purpose of the document and the IP at POI ecosystem;
- Chapter 4 describes a set of IP use cases to be covered by the framework;
- Chapter 5 provides the process flows for IPs at POI based on respectively merchant- and consumer-presented data;
- Chapter 6 defines the interoperability requirements for IPs at the POI;
- Chapter 7 gives an overview on the HUB interconnectivity requirements;
- Chapter 8 specifies the data sets, QR-code standards and minimum data elements for the interoperability messages;
- Chapter 9 discusses some security and trust aspects;
- Chapter 10 defines the security requirements for payment service user on-boarding;
- Chapter 11 defines the rules and procedures for the interoperability framework;
- Chapter 12 covers the framework governance aspects;
- Chapter 13 provides the conclusions with recommendations on the way forward;
- Annex 1 analyses PISP-based models;
- Annex 2 analyses models involving a CPSP;
- Annex 3 is the mandate of the ERPB working group on an interoperability framework of IPs at the POI;
- Annex 4 is the list of ERPB working group participants;
- Annex 5 is the list of Joint Task Force ERPB – ECSG participants;
- Annex 6 is the list of Joint Task Force ERPB – MSG MSCT participants.

2.2 References

Throughout this document, the following references are used.

N°	Title	Issued by
[1]	EBA/GL/2019/04: EBA Guidelines on ICT and security risk management	EBA
[2]	PSD2: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC	EC
[3]	Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (also referred to as "RTS")	EC
[4]	General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC	EC
[5]	eIDAS: Regulation (EU) No 910/2014 of the European parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	EC
[6]	European Commission Report on existing remote on-boarding solutions in the banking sector – December 2019	EC
[7]	EPC004-16: SEPA Instant Credit Transfer Scheme Rulebook	EPC
[8]	EPC250-18: The SEPA Proxy Lookup (SPL) Scheme Rulebook	EPC
[9]	EPC269-19v1.0: Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance (MSCT IG)	EPC
[10]	EPC302-19v1.0: 2019 Payment Threats and Fraud Trends Report	EPC
[11]	EPC 312-19v1.0: Technical interoperability of MSCTs based on payee-presented data	EPC
[12]	EPC 014-20: SEPA Request-to-Pay (SRTP) Scheme Rulebook	EPC

[13]	EPC 096-20: Technical interoperability of MSCTs based on payer-presented data	EPC
[14]	RTP MSG 005-19: Request-to-Pay – Specifications for a standardisation framework	EPC
[15]	ERPB Final report of the ERPB working group on Instant Payments at POI	ERPB
[16]	Internal standards on combating money laundering and the financing of terrorism and proliferation – The FATF recommendations	FATF
[17]	ISO 9362: Business Identifier Code (BIC)	ISO
[18]	ISO 12812: Core banking - Mobile financial services - Parts 1-5	ISO
[19]	ISO 13616: Financial services - International Bank account number (IBAN) -- Part 1: Structure of the IBAN	ISO
[20]	ISO 18092: Information technology - Telecommunications and information exchange between systems -- Near Field Communication - Interface and Protocol (NFCIP-1)	ISO
[21]	ISO 20022: Financial Services – Universal Financial Industry Message Scheme	ISO
[22]	ISO/IEC 14443: Identification cards - Contactless integrated circuit(s) cards - Proximity cards – Parts 1-4	ISO
[23]	ISO/IEC 18004: Information technology -- Automatic identification and data capture techniques -- QR-code bar code symbology specification	ISO
[24]	Joint Initiative on a PSD2 Compliant XS2A Interface - NextGenPSD2 XS2A Framework Implementation Guidelines	The Berlin Group
[25]	NFC Controller Interface (NCI) Specifications NFC Forum	NFC Forum

Table 1: Bibliography

2.3 Definitions

Throughout this document, the following terms are used.

Term	Definition
Account Servicing Payment Service Provider (ASPSP)	A PSP providing and maintaining a payment account for a payer (see Article 4 in [2]) or a payee.
Alias	See Proxy
Beneficiary	See Payee.
Bluetooth Low Energy (BLE)	A wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications including beacons. Compared to classic Bluetooth, BLE is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range.
Business Identifier Code (BIC)	An 8 or 11 character ISO code assigned by SWIFT and used to identify a financial institution in financial transactions (see [7] and [17]).
Collecting Payment Service Provider (CPSP)	A payment service provider according to PSD2 that collects the payment transactions on behalf of the merchant (the ultimate beneficiary) and as such is the beneficiary of the 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 [2]).
Consumer Device	An internet capable device used by the consumer to conduct an instant payment. Examples include a mobile device or a personal computer (PC).
Consumer Device UVM (CDUVM)	A user verification method (UVM) entered by or captured from the consumer (user) on the consumer device (e.g. a mobile device).
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 [22]).
(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 [2]).
Credit transfer	A payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the PSP which holds the payer's payment account, based on an instruction given by the payer (see (see Article 4 in [2]).

Credit Transfer instruction	A payment instruction given by an originator to an originator ASPSP requesting the execution of a credit transfer transaction, comprising such information as is necessary for the execution the credit transfer and is directly or indirectly initiated in accordance with the provisions of [2].
Credit Transfer Transaction	An instruction executed by an originator ASPSP by forwarding the transaction to a CSM for forwarding the transaction to the beneficiary ASPSP.
Customer	A payer or a beneficiary which may be either a consumer or a business (merchant).
CustomerID	In the context of this document, an identification of the payer (consumer), issued by their ASPSP for access to (a) customer facing user interface(s) (e.g. their on-line banking system), as required in the PSD2 API.
2D barcode	A two-dimensional barcode is a machine-readable optical label that contains digital information. They are also referred to as matrix barcodes. Examples include QR codes and tag barcodes.
Digital wallet	A service accessed through a consumer device which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications (e.g., value added services such as loyalty, couponing, etc.). A digital wallet is sometimes also referred to as an e-wallet.
Electronic identification	The process of using personal identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.
Electronic identification means	Material and/or immaterial unit containing person identification data and which is used for authentication for an online service.
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.
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 (see Article 4 in [2]).
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.
Instant(ly)	At once, without delay.
Instant Payment	Electronic retail payment solutions available 24/7/365 and resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payer (within seconds of payment initiation) (see [7]).
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 [19]).
Instant Payment (IP) Application	A set of modules (application software) and/or data (application data) needed to provide functionality for an Instant Payment (IP) as specified by the IP service provider in accordance with the SEPA Instant Credit Transfer scheme.
Instant Payment (IP) Service Provider	A service provider that offers or facilitates a payment service to a consumer and/or merchant based on an SCT Instant transaction. This may involve the provision of a dedicated application for download on the consumer's device or the provision of dedicated software for the merchant POI. As an example, an IP 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.
Lock Transaction (LT) Indicator	A parameter that identifies the need for transmission of a Lock Transaction message (see Chapters 6 and 8).
Merchant	A beneficiary within a payment scheme for payment of the goods or services purchased by the consumer. The merchant is a customer of their PSP. A merchant may also be referred to as payee.
Merchant-presented data	Data provided by the merchant's POI to the consumer.
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, wearables, car on-board units.
Mobile Network Operator (MNO)	A mobile phone operator that provides a range of mobile services, potentially including facilitation of NFC services. The MNO ensures connectivity Over the Air (OTA) between the consumer and their PSP using their own or leased network.
Mobile payment service	A payment service made available by software/hardware through a mobile device.
Mobile service	A service such as identification, payment, ticketing, loyalty, etc., made available through a mobile device.

Mobile wallet	A digital wallet accessed through a mobile device. This service may reside on a mobile device owned by the 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).
NFC (Near Field Communication)	A contactless protocol for mobile devices specified by the NFC Forum for multi-market usage. NFC Forum specifications (see [25]) are based on ISO/IEC 18092 [20] but have been extended for harmonisation with EMVCo and interoperability with ISO/IEC 14443 [22].
Originator	See Payer.
Payee	A natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction (see Article 4 in [2]), (examples include merchant, business).
Payer	A natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order (see Article 4 in [2]).
Payment account	An account held in the name of one or more payment service users which is used for the execution of payment transactions (see Article 4 in [2]).
Payment Initiation Service Provider (PISP)	A payment service provider pursuing business activities as referred to in Annex I.7 of [2].
Payment Request	Set of rules and technical elements (including messages) that allow a payee to claim an amount of money from a payer for a specific transaction. As an example see [14] and [12].
Payment Request message	Message sent by the payee to the payer, directly or through agents. It is used to request the movement of funds from the payer account to the beneficiary account.
Payment Service Provider (PSP)	An entity referred to in Article 1(1) of [2] or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33 of [2].
Payment Service User (PSU)	A natural or legal person making use of a payment service in the capacity of payer, payee, or both (see Article 4 in [2]).
Payment scheme	A technical and commercial arrangement (often referred to as the “rules”) between parties in the payment value chain, which provides the

	organisational, legal and operational framework rules necessary to perform a payment transaction.
Payment system	A funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions (see Article 4 in [2]).
Payment transaction	An act, initiated by the payer or on his/her behalf or by the payee (beneficiary), of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee (see Article 4 in [2]).
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (see [4]).
Physical POI	A POI that is a physical device and consists of hardware and software, hosted in acceptance equipment to enable a consumer and/or merchant to perform an MCST. The merchant-controlled POI may be attended or unattended. Examples of POI include Point-of-Sale (POS), vending machine.
Point of Interaction (POI)	The initial point in the merchant's environment (e.g. POS, vending machine, payment page on merchant website, QR-code on a poster, etc.) where data is exchanged with a consumer device (e.g., mobile phone, wearable, etc.) or where consumer data is entered to initiate an instant credit transfer.
Proximity Payment	A payment where the 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 will be referred to as IBAN-proxy in this document.
QR-code	Quick Response-code [23], see also 2D barcode.
Remote POI	The initial point where data enters the merchant's domain for remote transactions. It exists in a variety of technical platforms which enable a 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 consumer device conducted over internet.
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.
Sensitive payment data	Data including personalised security credentials which can be used to carry out fraud (see Article 4 in [2]).
SEPA Instant Credit Transfer	The SEPA Instant Credit Transfer is the payment instrument governed by the rules of the SEPA Instant Credit Transfer Scheme for making instant credit transfer payments in euro throughout the SEPA from payment accounts to other payment accounts (see [7]).
Settlement	An act that discharges obligations with respect to the transfer of Funds between Originator ASPSP and Beneficiary ASPSP.
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).
Strong Customer Authentication (SCA)	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 [2]).
Tokenisation	Process of substituting payment account, PSU identification data or transaction related data with a surrogate value, referred to as a token.
Token	Tokens can take on a variety of formats across the payments industry. They generally refer to a surrogate value for payment account (e.g., the IBAN), PSU identification data (e.g., CustomerID) or transaction related data. Payment Tokens must not have the same value as or conflict with the real payment account related data. If the token is included in the 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.
Token Requestor	An entity requesting a token to the Token Service
Token Service	A system comprised of the key functions that facilitate generation and issuance of tokens and maintain the established mapping of tokens to

	the related data when requested by the token requestor. It may also include the capability to establish the token assurance level to indicate the confidence level of the payment token to the related information binding. The service also provides the capability to support token processing of payment transactions submitted using tokens by de-tokenising the token to obtain the actual related information (see also the definition of Token).
Token Service Provider (TSP)	An entity that provides a Token Service.
Trusted Third Party (TTP)	An entity which facilitates interactions between stakeholders of the ecosystem who all trust this third party (examples are SE provider, common infrastructure manager…).
UICC	Universal Integrated Circuit Card - A generic and well standardised SE owned and issued by the MNOs.
User Verification Method	A method for checking that a consumer is the one claimed (see [18]).

Table 2: Terminology

2.4 Abbreviations

Throughout this document, the following abbreviations.

Abbreviation	Term
ASPSP	Account Servicing PSP
API	Application Programming Interface
BIC	Business Identifier Code
BLE	Bluetooth Low Energy
BoD	Board of Directors
CDUVM	Consumer Device UVM
CPSP	Collecting Payment Service Provider
CSM	Clearing and Settlement Mechanism
2D barcode	Two dimensional barcode
EBA	European Banking Authority
EC	European Commission
ECSG	European Cards Stakeholders Group

EPC	European Payments Council
ERPB	Euro Retail Payments Board
GA	General Assembly
GDPR	General Data Protection Regulation
IBAN	International Bank Account Number
ID	Identifier
IP	Instant Payment
ISO	International Organization for Standardization
LT	Lock Transaction
MNO	Mobile Network Operator
MSCT	Mobile Initiated (Instant) SCT
MSCT IG	Mobile Initiated SEPA (Instant) Credit Transfer Interoperability Guidance
MSG MSCT	Multi-Stakeholder Group for Mobile Initiated (Instant) SCT
NFC	Near-Field Communication
PC	Personal Computer
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
RFID	Radio Frequency Identification
RTP	Request-To-Pay
RTS	Regulatory Technical Standard
SCT Inst	SEPA Instant Credit Transfer
SE	Secure Element
SEPA	Single Euro Payments Area

SP	Service Provider
TSP	Token Service Provider
TTP	Trusted Third Party
UI	User Interface
UICC	Universal Integrated Circuit Card
URL	Uniform Resource Locator
UVM	User Verification Method

Table 3: Abbreviations

3 General

3.1 Purpose of the document

In March 2020 the ERPB established the ERPB working group on a framework for interoperability of instant payments at the Point-of-Interaction (IPs at the POI) to foster the development of pan-European instant payment services for this use case. Hereby an IP at POI is an instant payment transaction based on a SEPA Instant Credit Transfer (SCT Inst, see [7]), by a consumer to a merchant at the POI which may be for example a Point-of-Sale (POS) in a store or a payment page on an e- or m-commerce website.

As follow-up on the report from the ERPB working group on IPs at the POI in 2019 [15], the mandate of the new working group (see Annex 3), set up with the participation of relevant stakeholders (see Annex 4), focuses on a subset of the recommendations endorsed by the ERPB at their November 2019 meeting[6], namely those recommendations related to the development of a framework to manage the interoperability rules and appropriate governance for solutions enabling instant payments at the POI. The working group was also tasked to develop the following deliverables:

- Security requirements for payment service user on-boarding processes to be adopted by instant payment service providers and merchants;
- Appropriate specifications to enable consumer selection of preferred payment instrument to conduct a transaction at the POI.

For the development of these deliverables, the ERPB WG was expected to leverage the work undertaken by the ad-hoc Multi-stakeholder Group for Mobile Initiated SEPA (Instant) Credit Transfers (MSG MSCT).

In addition, considering the evolving market situation, the working group was also requested to review the stocktake of existing and planned end-user solutions for instant payments at the POI carried out by the ERPB working group on instant payments at the POI in 2019. In particular, the

[6] See https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/12th-ERPB-meeting/Statement.pdf?8f5bd56a229964fc0353ee6289a799b6

working group was expected to: i) update the information for the reported solutions and ii) add any relevant solutions that were not reported in the previous stocktake.

While the results of the 2020 stocktake have been shared with the ERPB in July 2020 in the interim report[7] prepared by the WG, the present document intends to cover all other deliverables as requested in the mandate and described above.

3.2 IP at POI ecosystem

3.2.1 Introduction

Instant Payments (IPs) at the POI are initiated directly (by the consumer) or indirectly (by an IP service provider at the request of the consumer) in compliance with the PSD2 (see [7]), using a consumer device. IP at POI solutions are offered by so-called IP service providers which are service providers that offer or facilitate a payment service to a consumer and/or merchant based on an SCT Instant transaction. As an example, an IP 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.

IPs in euro are based on the existing SCT Instant Scheme rulebook [7] in the so-called "interbank space" and are therefore using in that space the existing payment infrastructure. They typically use an IP application or a browser on the consumer device to initiate or at least authenticate and authorise the SCT Instant transaction, besides some features of the consumer device such as the support of CDUVM (e.g., a mobile code or biometrics on the mobile device), the consumer device screen to display transaction information, etc.

The figure below presents a decomposition of an IP at POI into functional building blocks.

[7] See https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/13th-ERPB-meeting/Item_4.4_-_Interim_report_of_the_WG_on_a_framework_for_instant_at_POI.pdf

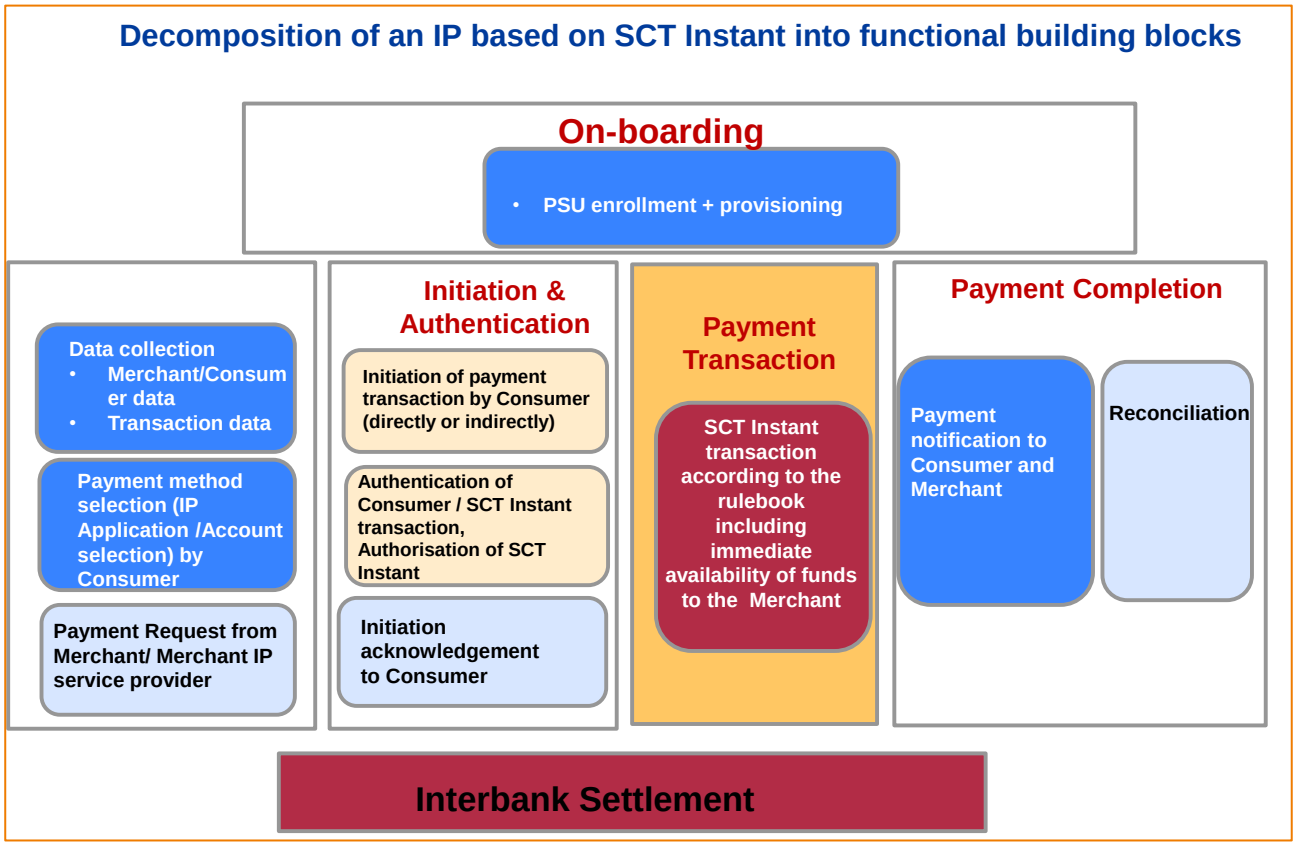


Figure 1: Decomposition of an IP at POI based on SCT Instant into building blocks

Dark blue	Light blue	Dark amber	Light amber

The dark amber coloured box in the figure is covered by the SCT Instant Scheme rulebook [7] and supporting documents[8] which form *the backbone* for the Framework for interoperability of IPs at POI.

The Framework will focus on the *interoperability outside the interbank space* such as between the consumer device and the merchant's POI, between the consumer and their IP service provider(s),

[8] See https://www.europeanpaymentscouncil.eu/what-we-do/sepa-payment-schemes/sepa-instant-credit-transfer/sepa-instant-credit-transfer-rulebook

between the merchant and their IP service provider(s)[9], 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 IP at POI transaction. This may depend on the payment context (e.g. a Payment Request from the merchant / merchant IP service provider for IPs based on consumer-presented data, see chapters [7] and [8]). Since these features are impacting the interoperability of IP at POI services, they will be covered by the Framework.

"On-boarding" (see dark blue box in the On-boarding) refers to the registration process of a consumer with an IP service provider or a merchant (see chapter 10) for a specific IP at POI service, before using the service for actual payment transactions. Since the security of the on-boarding process is a cornerstone for the trust in IP at POI services and for fraud mitigation, specific security requirements are defined under the Framework (see chapter 9).

The light amber boxes refer to functionalities which are not impacting the interoperability if different IP service providers or different IP at POI services for the consumer and the merchant are involved (see also section 5.3).

3.2.2 The IP at POI ecosystem

For the analysis of the interoperability requirements for the Framework for IPs at POI, the following generic 4-corner model will be used. Hereby it is assumed that both consumer and merchant have different ASPSPs that are SCT Inst scheme participants (see section 5.4 in [7]), while the entities assuming the role of IP service provider are depicted as separate entities that are different for the consumer and the merchant. Obviously, if the role of IP service srovider would be assumed by an ASPSP the model below would simplify or, alternatively, if multiple PSPs (such as a PISP licensed under PSD2 or a CPSP) would be involved between the consumer/merchant and their respective ASPSP this model might become more complex (see also Annexes 1 and 2).

[9] In so far that they impact the interoperability of IPs at the POI.

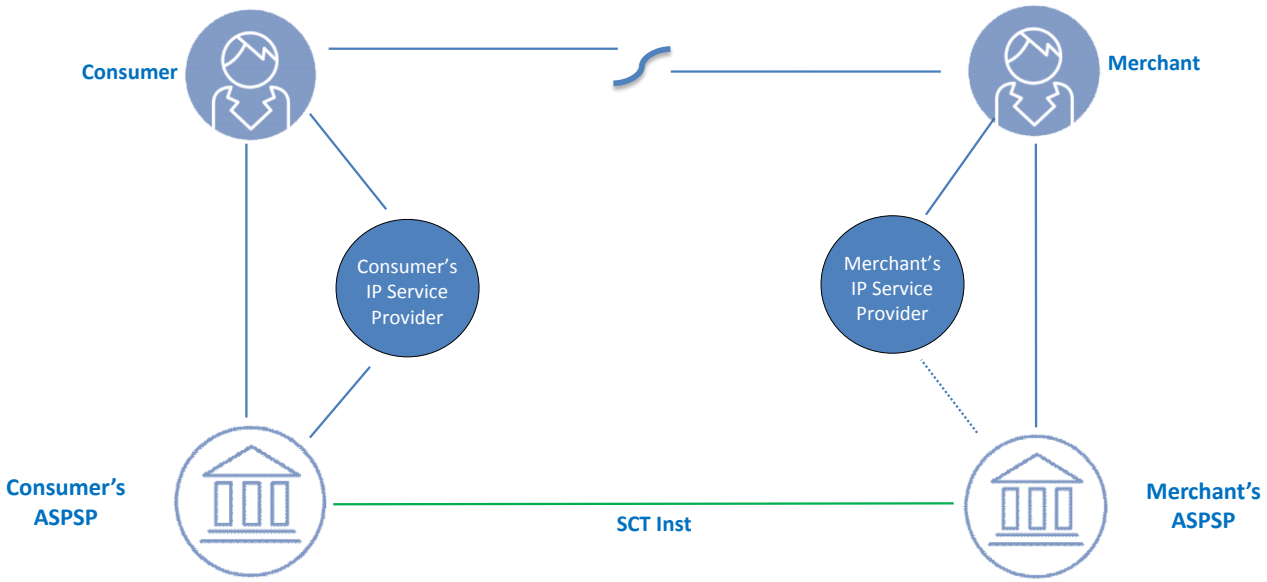


Figure 2: Generic 4-corner model for IPs at POI

IP service providers are service providers that offer or facilitate a payment service to a consumer and/or merchant based on an SCT Instant transaction. The consumer's IP service provider is linked to the consumer's ASPSP and the merchant's IP service provider may be linked to the merchant's ASPSP (this linkage may include both technical[10] and contractual aspects).

The IP at POI ecosystem involves some other new stakeholders in the value chain compared to the ones described in the SCT Instant Scheme rulebook [7] including:

- The Token Service Provider (TSP) who is a TTP involved if tokens are used in IPs as surrogate values for the transaction data (including the merchant/consumer IBAN, merchant/consumer identifier, transaction amount or merchant transaction identifier). The TSP manages the generation and issuance of tokens, and maintains the established mapping of tokens to the related transaction data. For simplification it is assumed in this document that the role of the TSP is assumed or is under the control of the IP service provider (and hence the TSP is not depicted in the figure above)[11].

[10] For the technical aspects see Chapter 5.
[11] The same is valid in case of usage of a proxy. The role of the provider involved is assumed or is under the control of the IP service provider.

- The (Mobile) Wallet Issuer is a service provider that issues (mobile) wallet functionalities to the PSU (consumer or merchant).
- The SE provider, if the IP application is stored in an SE on the mobile device. This is the MNO in case of a UICC, the mobile equipment manufacturer, the IP service provider or a third party in case of an embedded SE, and the SE manufacturer.
- Cloud service providers (which may be the IP service providers themselves or this service may be delegated to a TTP),
- Application developers (IP application, user interface, (mobile) wallet …),
- Operating System suppliers,
- Equipment manufacturers,
- Organisations performing infrastructure certification (e.g., IP applications, POI, mobile devices, etc.)
- Etc.

4 IP at POI use cases

4.1 Overview

This section provides typical examples of use cases for instant payments at the POI. They include wherever possible, cross-references to other documents where detailed descriptions of possible implementations of these use cases are provided as they mostly appear in the market today (where typically both the consumer and the merchant have the same IP service provider). The use cases will be used in forthcoming chapters to derive generic requirements for technical interoperability in case consumer and merchant have different IP service providers. These technical interoperability requirements would need to be adhered to under the Framework.

Use-case identifier	Description	Reference to detailed description of illustration of use case if available

IP-C2B-1: merchant-presented data in physical store	A merchant provides merchant-presented data in a physical store to the consumer (e,g, via a QR-code on the POI) to enable the consumer to initiate an IP transaction using a dedicated IP application on their device for immediate delivery of purchased goods or services.	See C2B-2 and C2B-3 in [9] https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/mobile-initiated-sepa-instant-credit-transfer-interoperability
IP-C2B-2: merchant-presented data on merchant webpage for e-or m-commerce	A merchant provides merchant-presented data to the consumer (e.g., via a QR-code on the webpage) to enable the consumer to initiate an IP transaction using a dedicated IP application on their device for delivery of purchased goods or services.	
IP-C2B-3: consumer-presented data in physical store	A consumer provides consumer-presented data in a physical store to the merchant (e.g., via a QR-code on their device) to enable the merchant to initiate an IP transaction using a Payment Request for immediate delivery of purchased goods or services.	See C2B-1 and C2B-2 in [13] https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/public-consultation-document-technical-interoperability-mscts

IP-C2B-4: consumer-presented data for e- or m-commerce	A consumer provides consumer-presented data on a webpage or merchant app for e- or m-commerce to enable the merchant to initiate an IP transaction using a Payment Request for delivery of purchased goods or services.	See C2B-4 and C2B-5 in [9] https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/mobile-initiated-sepa-instant-credit-transfer-interoperability

Table 4: IP at POI use cases

4.2 Taxonomy of IP at POI use cases

In order to assess the interoperability requirements for IPs at POI for a generic model as introduced in section 3.2.2 and to identify the possible needs for standardisation, this section sets out a possible categorisation based on the characteristics of the above mentioned use cases.

These use cases can be categorised by multiple criteria, depending on the perspectives the analysis is focused on. However, in the context of this document, categorisation will be done in view of the potential impact on the technical interoperability as follows:

- How is transaction data collected in the preparation phase (see Figure 1): merchant- or consumer-presented data?
- In which form is the transaction data exchanged between the consumer and the merchant in the initial step: in “clear” or using a “token”?
- Is all transaction data needed for the initiation of the transaction exchanged in the initial step between the consumer and the merchant?

5 Technical interoperability requirements

5.1 Introduction

The different technical interoperability aspects could be represented in a 3-layer approach as shown in the figure below.

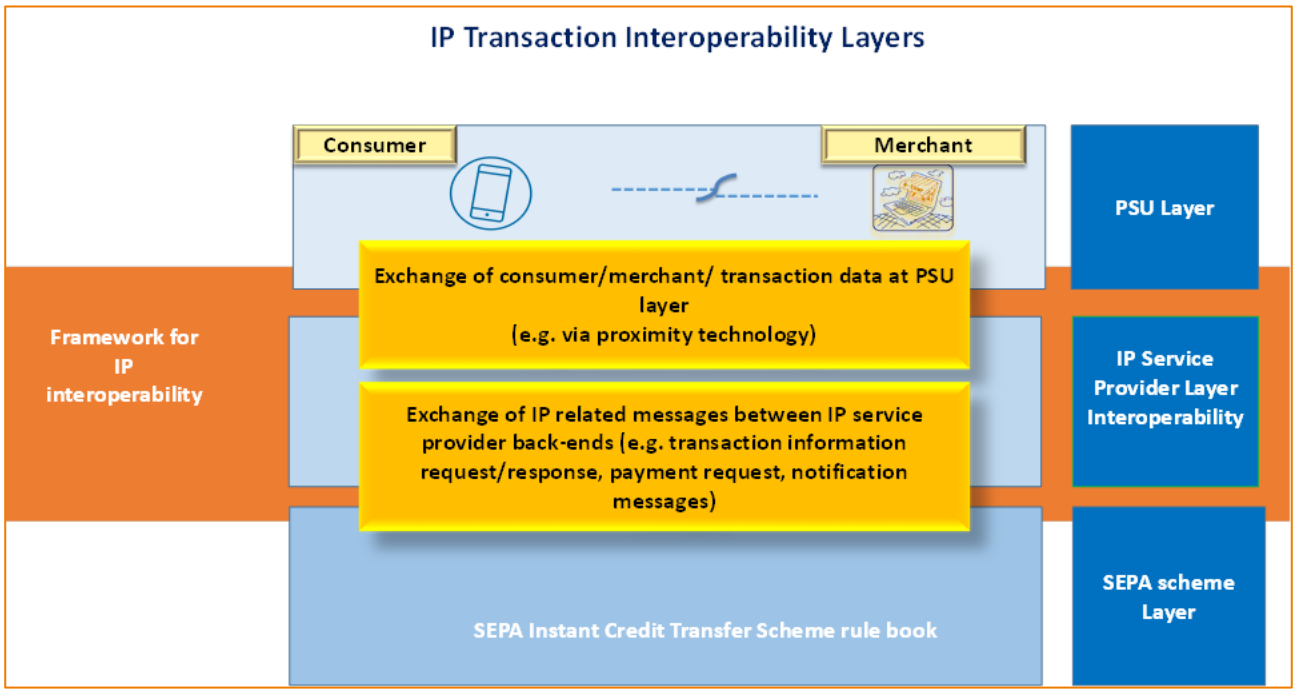


Figure 3: IP transaction interoperability layers

This section will focus on the analysis of the technical interoperability requirements at both the PSU and the IP service provider layers since the technical interoperability in the "interbank space" is already covered in the SCT Instant Scheme rulebook (see [7]).

5.1.1 PSU layer

It is generally recognised that the PSU (consumer/merchant) layer, for instance an IP service application on the consumer's mobile device or the IP application on the merchant's POI, is in the competitive space of the IP service. However, a minimum standardisation would be needed on how the consumer or merchant data and other IP transaction data are exchanged between the consumer and the merchant.

In case for instance a proximity technology between the consumer and the merchant or a payment request message via the IP service providers back-ends would be used for the exchange of the IP transaction data, a standardisation of the message content / data format is needed (e.g., standardisation of a QR-code or standardisation of the data in the payment request messages).

5.1.2 IP service layer

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

In case the full IP transaction data is exchanged directly in clear between the merchant and the consumer, the IP transaction can be immediately initiated while the SCT Instant Scheme rules ensure the interoperability.

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

Also the infrastructure needed to exchange the notification messages[12] to the consumer and merchant (see section 5.4) would need to be developed as well as the standardisation of the minimum data elements required in the message flows between IP service providers (see section 8.3).

[12] Currently the SCT Instant Scheme rulebook only requires the transmission of the negative confirmation message as notification by the consumer's ASPSP to the consumer (see [7]).

In the sections below, a detailed analysis will be made on the technical interoperability requirements for IPs at POI based on respectively merchant- and consumer-presented data, derived from the analysis made for technical interoperability of MSCTs by the MSG MSCT in [11] and [13].

Moreover, as already mentioned in section 3.2.1, the focus for technical interoperability requirements for IPs is on the Payment Preparation and Payment Completion phases related to an SCT Instant as depicted in Figure 1. Indeed, for IPs, the strong customer authentication of the consumer by their ASPSP is in the consumer-to-consumer's ASPSP domain and is as such not impacting the interoperability if different IP service providers for the consumer and the merchant are involved. Neither is the interoperability impacted if the consumer's ASPSP has delegated the strong customer authentication to the consumer's IP service provider or to a so-called authentication service provider.

As mentioned before, what is impacting the interoperability is the following:

- How is the transaction data exchanged between the consumer and the merchant?
- How are the acknowledgement/notification messages provided by the respective IP service providers to the merchant and the consumer?

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

Offline use cases whereby the consumer device has no internet connection and hence direct consumer-to-consumer's ASPSP authentication is impossible, would need to be further analysed at a later stage with respect to their interoperability.

It is further noted that there is also an additional requirement to define the technical means needed between IP service providers for the implementation of an inter-SP fee structure. However, this topic will not be further analysed in this document.

5.2 Interoperability model based on a HUB

To achieve interoperability for the generic basic 4-corner model introduced in Chapter 3, the concept of a HUB is introduced to interconnect the respective IP service providers as shown in the figure below.

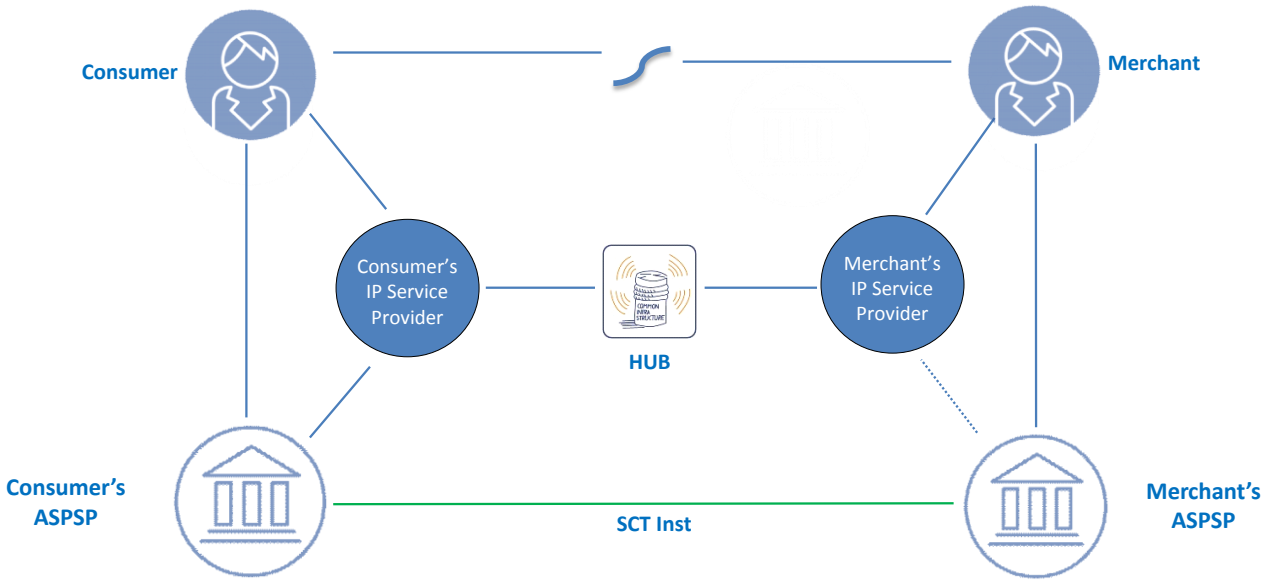


Figure 4: Generic 4-corner interoperability model

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

5.3 Exchange of data at PSU layer

5.3.1 IPs based on merchant-presented data

With respect to the availability of the transaction data (merchant data and payment data) needed by the consumer for the initiation of the IP transaction the following cases need to be considered:

- All transaction data is exchanged between the merchant and the consumer through a proximity technology (QR-code, NFC, BLE, etc.).

In this case a distinction needs to be made whether

- The merchant-presented data includes a "(merchant) 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 consumer via their IP service provider. This generally requires the support of the merchant's IP service provider (see Information Request/Response messages in Figure 6 below) prior to the initiation of the IP transaction.
- The merchant-presented data includes all transaction data in "clear"[13] (e.g. the merchant's name, trade name, IBAN of the merchant's account, transaction amount, etc.). This enables the immediate initiation of the IP transaction.

- Only part of the transaction data is exchanged between the merchant and the consumer through a proximity technology (QR-code, NFC, BLE, etc.) or only part of the transaction data exchanged is in clear (e.g. merchant-presented data contains a proxy). In this case the complete transaction data needs to be provided by the merchant's IP service provider upon request from the consumer's IP service provider (see Information Request/Response messages in Figure 6 below) prior to the initiation of the IP transaction.

5.3.2 IPs based on consumer-presented data

Consumer-presented identification data

To achieve interoperability of IPs based on consumer-presented data, at least consumer identification data (which enables the consumer's IP service provider to identify the consumer) and an identifier of the consumer's IP service provider are needed in this consumer-presented data.

The *consumer identification data* is defined by the IP service provider and may take a variety of forms and may be static or dynamic. However, this consumer identification data has no impact on the interoperability between IP services. This consumer identification data will need to be

[13] Obviously in this case additional measures should be taken to ensure the security of the data exchanged (for some guidance see [9]).

transferred as part of the Payment Request message from the merchant to their IP service provider and further to the consumer's IP service provider to enable the identification of the consumer. For the purpose of this document, the following three cases with respect to the type of consumer identification data are considered:

- The consumer identification data is a (consumer) token;
- The consumer identification data consists of a CustomerID and IBAN;
- The consumer identification data consists of a CustomerID and IBAN-proxy.

In the last two cases however, appropriate security measures need to be taken to ensure the integrity of the data and the confidentiality as appropriate (see chapter [11]).

The *identifier of the consumer's IP service provider* is needed by the merchant's IP service provider and subsequently by the HUB to know where to route the Payment Request message.

Transaction data

The transaction data (merchant data and payment data) needed by the consumer for the initiation of the IP transaction needs to be provided by the merchant to the consumer via their respective IP service providers[14] as follows:

- The transaction data is provided by the merchant to their IP service provider via a "Payment Request"[15] message. Thereby the consumer's identification data and the identifier of the consumer's IP service provider will need to be retrieved from the consumer-presented data

[14] If a bi-directional proximity technology is used between the consumer device and the merchant POI, 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 IPs based on merchant-presented data.
[15] A "Payment Request" refers to messages sent by the merchant to their IP service provider and from the merchant's IP service provider to the consumer's IP service provider including all transaction data for presentation to the consumer to enable them to initiate a transaction and perform SCA as needed. As an example see [14] and [12]. Take text from MSG MSCT
If the merchant's IP service provider is a PISP, the "Payment Request" may end there and result directly in a payment initiation, which however, also carries all transaction data for presentation to the consumer and to perform SCA as needed.

by the merchant and included in the Payment Request message. The Payment Request message between the merchant and their IP service provider should further at least contain a transaction identifier, the name / trade name/ IBAN[16] of the merchant and the transaction amount (see step 5 in the Figure 10 below).

- The Payment Request message is transferred by the merchant's IP service provider via the HUB to the consumer's IP service provider using the identifier of the consumer's IP service provider received (see step 6 in Figure 10 below).
- The consumer's IP service provider identifies the consumer and possibly their IBAN from the token included in the Payment Request message and provides the transaction data (at least the transaction amount and IBAN /name / trade name merchant) to the consumer for authentication purposes (see steps 7 and 8 in Figure 10 below).

5.4 Acknowledgement/notification messages

The following messages have been identified (see section 8.7 in [9]) in that respect:

- Acknowledgement of receipt of the SCT Instant instruction provided to the consumer by their IP service provider;
- Notification of payment to the merchant by their IP service provider;
- Notification of payment to the consumer by their IP service provider.

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

Since the acknowledgement of receipt message is between the consumer and their IP service provider, this as such is not impacting the interoperability of IP at POI services across SEPA.

However, the notification messages mentioned above and some messages related to exception handling are impacting the interoperability of IP at POI services across SEPA.

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

Notification of payment to the merchant by their IP service provider

- *Successful transaction:*

  The merchant shall be informed by their IP service provider about the execution of the payment. This implies that either

  - The consumer's ASPSP upon receipt of the confirmation message 6 in Figure 1 in [7] needs to inform the consumer's IP service provider, who subsequently needs to inform the merchant's IP service provider (e.g. via HUB, see Chapters 6 and 7);

  or

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

- *Unsuccessful transaction:*

  The merchant shall be informed by their IP service provider about the unsuccessful payment transaction. This implies that either

  - The consumer's ASPSP upon receipt of the negative confirmation message 6 in Figure 1 in [7] needs to inform the consumer's IP service provider, who subsequently needs to inform the merchant's IP service provider (e.g. via a HUB, see Chapters 6 and 7);

  or

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

Notification of payment to the consumer by their IP service provider

- *Successful transaction:* The consumer shall be informed by their IP service provider about the execution of the payment. This implies that the consumer's ASPSP upon receipt of the confirmation message (6) in Figure 1 in [7] needs to inform the consumer's IP service provider.

- *Unsuccessful transaction:* The consumer shall be informed by their IP service provider about the unsuccessful payment transaction. This implies that the consumer's ASPSP upon receipt of the negative confirmation message (6) in Figure 1 in [7] needs to inform the consumer's IP service provider.

6 Process flows

In this chapter, the process flows for interoperability for IPs will be shown for some cases listed in the table below. For all cases illustrated a QR-code is used as proximity technology between the consumer and the merchant for the initial exchange of the data.

Nr	IP transactions type	Support from the HUB
1.	**C2B - merchant-presented data contains a token**	Retrieval of the transaction data from the token Conditional transaction lock messages (see below) Notification messages
2.	**C2B - merchant-presented data which contains all transaction data in clear[17]**	Conditional transaction lock messages (see below) Notification messages
3.	**C2B - merchant-presented data which contains only part of the transaction data or only part of the transaction data is in clear[18] (e.g. merchant-presented data contains a proxy**	Retrieval of the complete transaction data Conditional transaction lock messages (see below) Notification messages

[17] Obviously in this case additional measures should be taken to ensure the integrity of the data exchanged (see also Chapter 9).
[18] Obviously in this case additional measures should be taken to ensure the integrity of the data exchanged (see also Chapter 9).

4.	**C2B – consumer-presented data which contains a token**	Transfer of Payment Request messages Notification messages
5.	**C2B – consumer-presented data which contains a CustomerID + IBAN in clear[19]**	Transfer of Payment Request messages Notification messages
6.	**C2B- consumer-presented data which contains a CustomerID[20] + IBAN-proxy**	Transfer of Payment Request messages Notification messages

Table 5: Mapping IP transaction types onto HUB functionalities

Only types 1, 2 and 4 will be illustrated below and the process flows will be described for physical POIs. Note however that the process flows would remain the same if the merchant-presented QR-code is shown on a payment page of an e- or m-merchant (virtual POI).

The process flow for type 3 is similar to the process flow for type 1, whereby the retrieval of the full transaction data needs to be supported by the HUB, based on the data available in the merchant-presented data.

The process flows for types 5 and 6 are identical to the process flow for type 4, except that the detokenization process is not needed and for type 6, the consumer's IBAN needs to be retrieved from their proxy by their IP service provider. However, those are not impacting the interoperability requirements for the HUB.

[19] Obviously in this case additional measures should be taken to ensure the integrity and confidentiality as needed (subject to clarification to be obtained from the EBA Q&A) of the data exchanged (see also Chapter 9).
[20] Obviously in this case additional measures should be taken to ensure the integrity and confidentiality as needed (subject to clarification to be obtained from the EBA Q&A) of the data exchanged (see also Chapter 9).

For IPs with consumer-presented data for e- and m-commerce transactions, the process flows would be similar as for physical POIs, except that the consumer-presented data will need to be transferred to the merchant in a different way (e.g., entered manually by the consumer into the merchant's website or payment page).

Note also that the QR-code may be static or dynamic. In case dynamic QR-codes are used for IPs with merchant-presented QR-codes, a conditional "transaction lock function" is defined as follows. The function consists of conditional lock transaction messages that are sent between the consumer's IP service provider and the merchant's IP service provider via the HUB to prevent that multiple consumers from different IP service providers pay the same transaction after strong customer authentication. The transaction lock function would be 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 LT Indicator. Two consumers could perform SCA on the same transaction. In this case, the consumer (with successful SCA) for which the *lock function sent by their IP service provider reaches as first* the IP service provider of the merchant is the one for which the transaction is locked.

Furthermore it should be noted that in the process flows below, the representation and description of strong customer authentication (SCA) is simplified since the focus of the flows is on the interconnectivity between the respective IP service providers. SCA could for instance be performed by the consumer's IP service provider or by their ASPSP. More details on SCA are provided in section 8.3 in [9] and are illustrated in the chapter 7 in [9] and in section 2 in [13].

In the process flows below, the implicit assumption is made that all IP transactions are successful. The flows for unsuccessful transactions would need to be analysed separately.

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

6.1 Merchant-presented QR-code with token

In this section the process flow for an in-store payment at a physical POI between a consumer and merchant using a HUB is illustrated. In this example, it is assumed that the merchant-presented data contains a token. Note that this token may be dynamic or static. It is hereby assumed that the tokenisation/de-tokenisation of (part of) the transaction data is handled by or via the merchant's IP service provider.

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

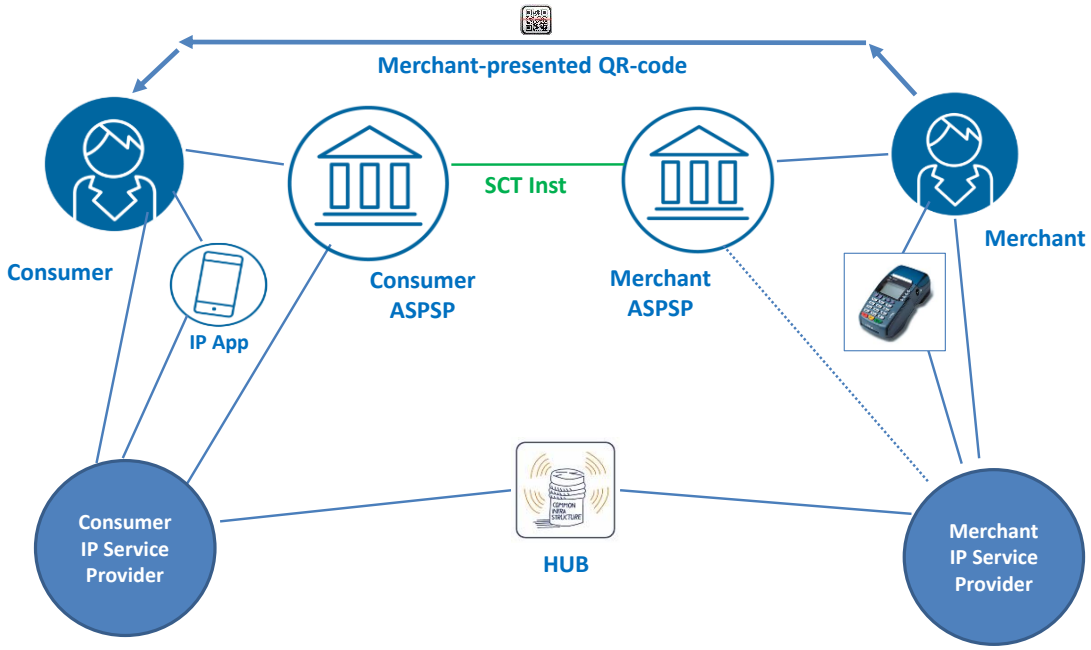
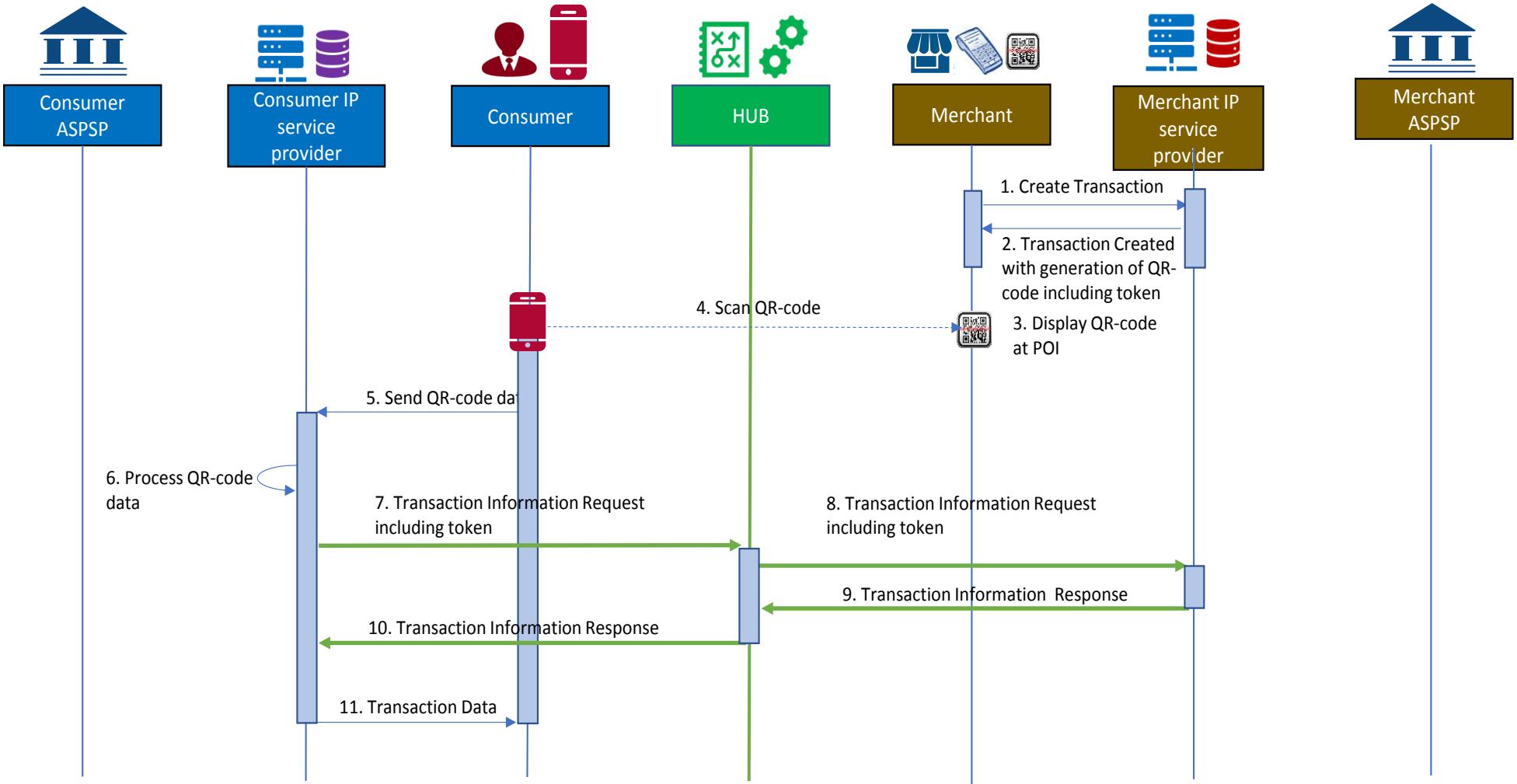


Figure 5: Actors for IP with merchant-presented data

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


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

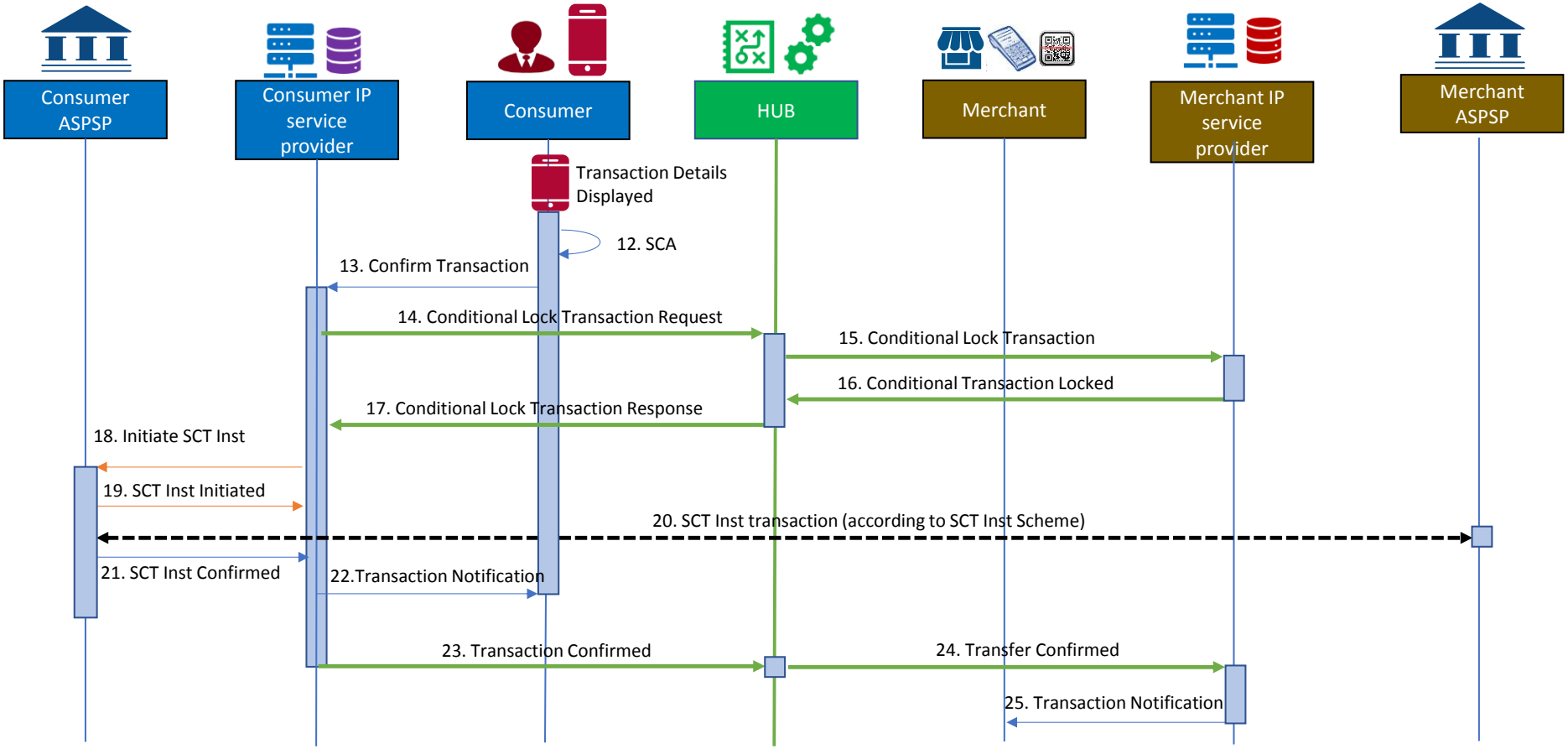


Figure 6: Process flow – C2B – merchant-presented QR-code with token

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 IP service provider[21].

Step 2:

The merchant's IP service provider returns a QR-code including a unique token based on the transaction details (transaction amount, name/trade name merchant, IBAN_merchant, transaction identifier) and their IP service provider identifier to the merchant.22

Step 3:

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

Step 4:

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

Step 5:

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

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

Step 6:

The consumer's IP 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 IP service provider identifier is sent to the HUB.

Step 8:

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

Step 9:

The merchant's IP 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 IP service provider.

Step 11:

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

Step 12:

The consumer consents to the transaction based on the details displayed and performs SCA[23].

[23] The SCA may be performed by the consumer's IP 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

Step 13:

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

Step 14 (conditional)[24]:

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

Step 15 (conditional):

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

Step 16 (conditional):

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

Step 17 (conditional):

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

Step 18:

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

that the consumer's IP service provider has received delegation from the consumer's ASPSP for SCA subject to appropriate agreements.

[24] See Chapter 6. In case the LT Indicator does not require a lock transaction function, steps 14 through 17 will not be present.

Step 19:

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

Step 20:

The consumer's ASPSP sends the SCT Inst transaction to the merchant's ASPSP and the transaction flow is handled according to the SCT Inst scheme (see [7]).

Step 21:

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

Step 22:

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

Step 23:

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

Step 24:

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

Step 25:

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

6.2 Merchant-presented QR-code with all transaction data in clear

In this section the process flow for an in-store payment at a physical POI between a consumer and merchant using a HUB is illustrated. In this example, it is assumed that the merchant-presented data contains all transaction data "in clear".

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

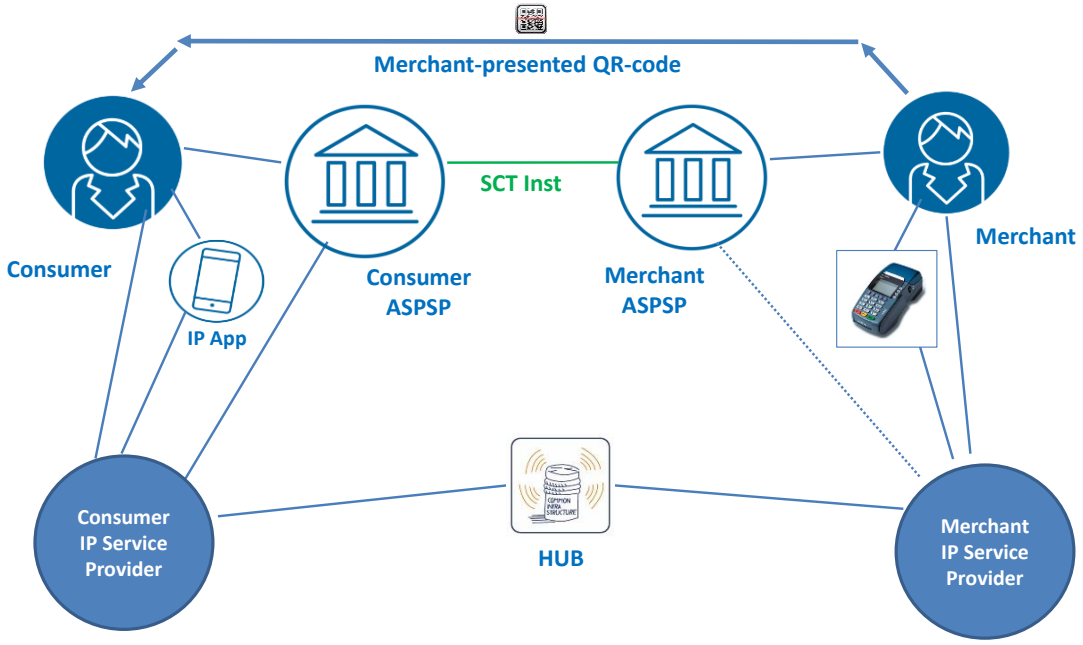
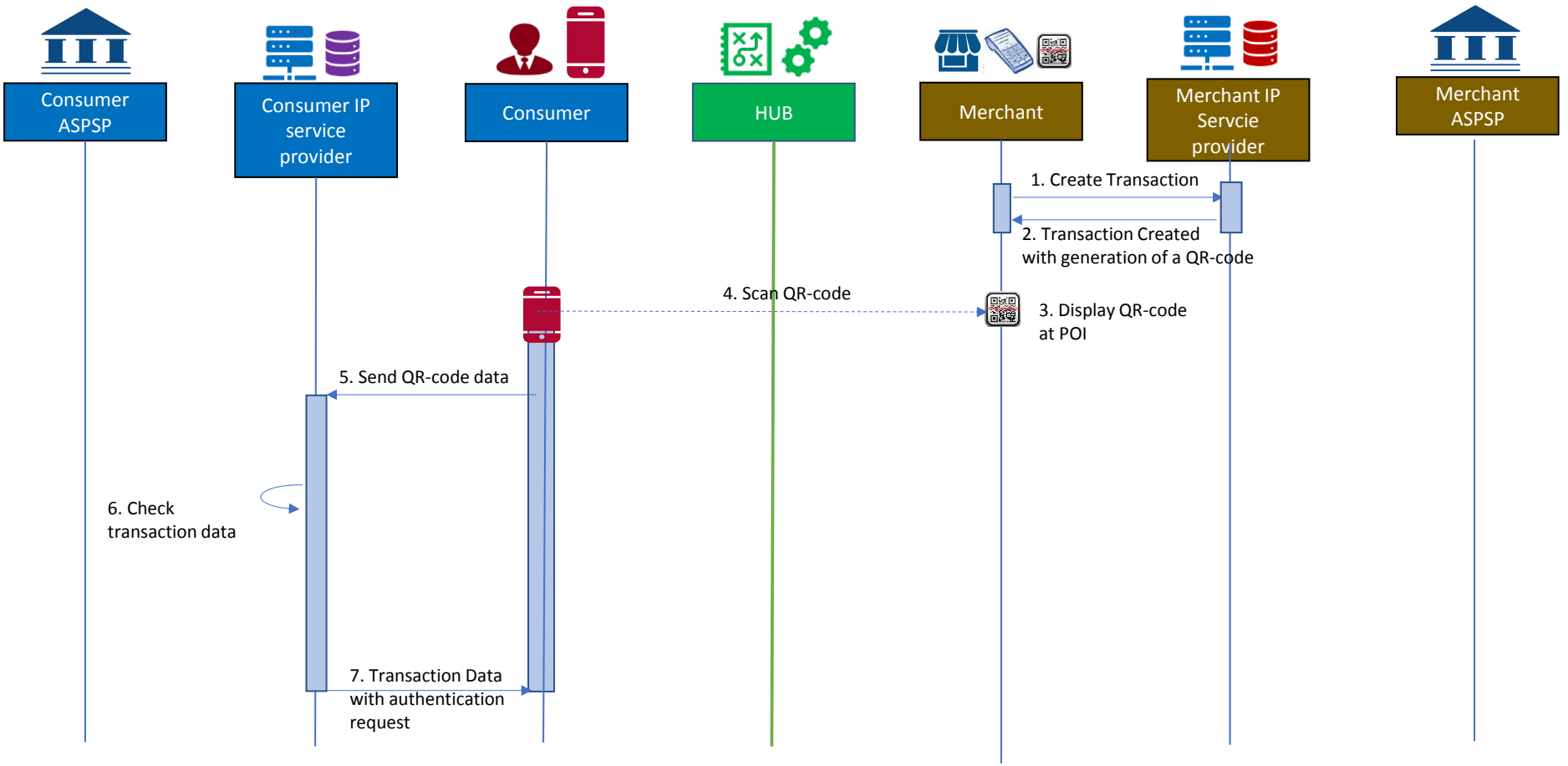


Figure 7: Actors for IP with merchant-presented data

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


Consumer ASPSP
Consumer IP service provider
Consumer
HUB
Merchant
Merchant IP Servcie provider
Merchant ASPSP
1. Create Transaction
2. Transaction Created with generation of a QR-code
3. Display QR-code at POI
4. Scan QR-code
5. Send QR-code data
6. Check transaction data
7. Transaction Data with authentication request

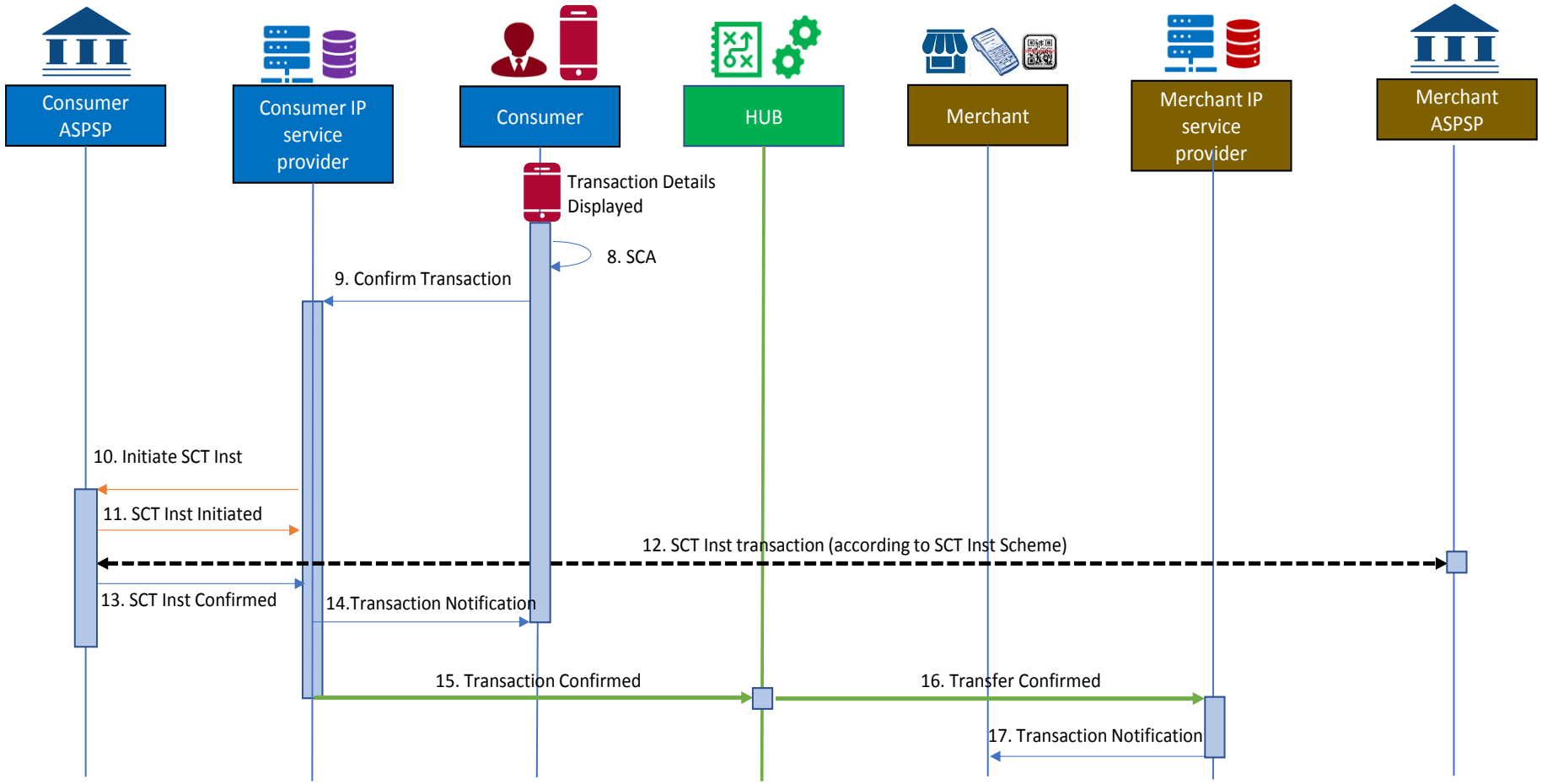


Figure 8: Process flow – C2B – merchant-presented QR-code with all transaction data "in clear"

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 IP service provider[25].

Step 2:

The merchant's IP service provider returns a QR-code based on the transaction details (transaction amount, name/trade name merchant, IBAN_merchant, transaction identifier) and their IP service provider identifier to the merchant.

Step 3:

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

Step 4:

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

Step 5:

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

Step 6:

The consumer's IP service provider checks the transaction data.

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

Step 7:

The IP service provider sends the transaction details to the consumer.

Step 8:

The consumer consents to the transaction based on the details displayed and performs SCA[26].

Step 9:

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

Step 10:

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

Step 11:

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

Step 12:

The consumer's ASPSP sends the SCT Inst transaction to the merchant's ASPSP and the transaction flow is handled according to the SCT Inst scheme (see [7]).

[26] The SCA may be performed by the consumer's IP 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 IP service provider has received delegation from the consumer's ASPSP for SCA subject to appropriate agreements.

Step 13:

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

Step 14:

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

Step 15:

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

Step 16:

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

Step 17:

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

6.3 Consumer-presented QR-code with token

In this section the process flow for an in-store payment at a physical POI between a consumer and merchant using a HUB is illustrated. In this example, it is assumed that the consumer-presented data contains a token. Note that this token may be dynamic or static. It is hereby assumed that the tokenisation/de-tokenisation is handled by or via the consumer's IP service provider. The consumer-presented data also includes the identifier of the consumer's IP service provider "in clear" so that it can be retrieved by the merchant and provided to their IP service provider in the Payment Request message.

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

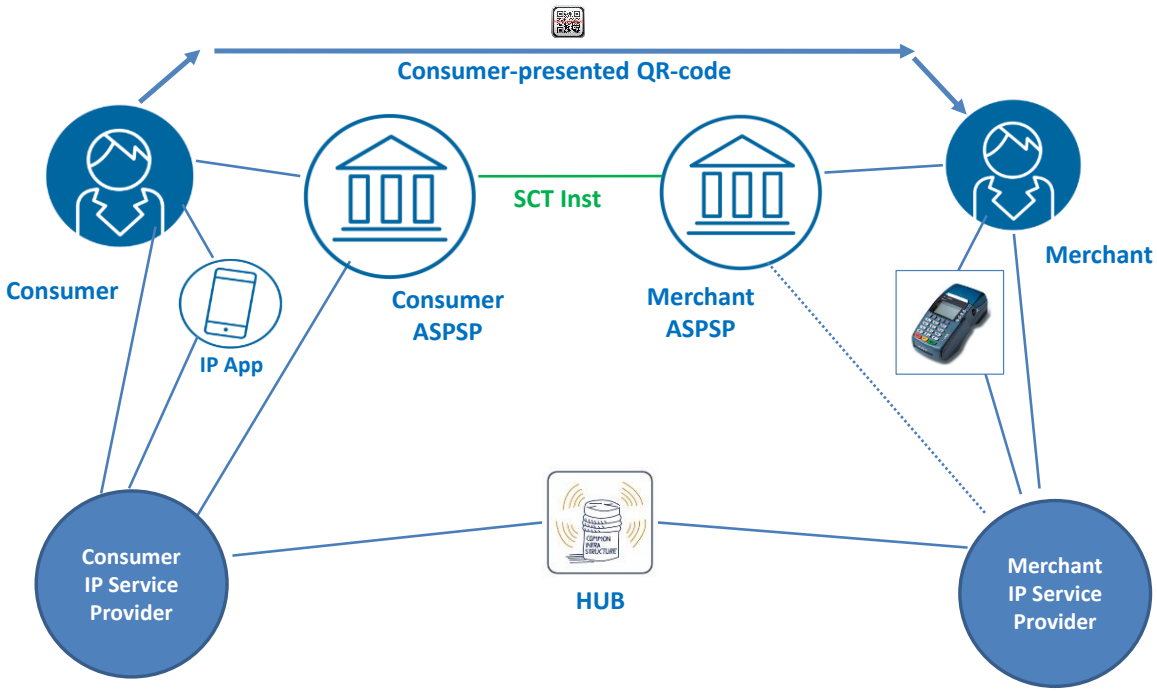
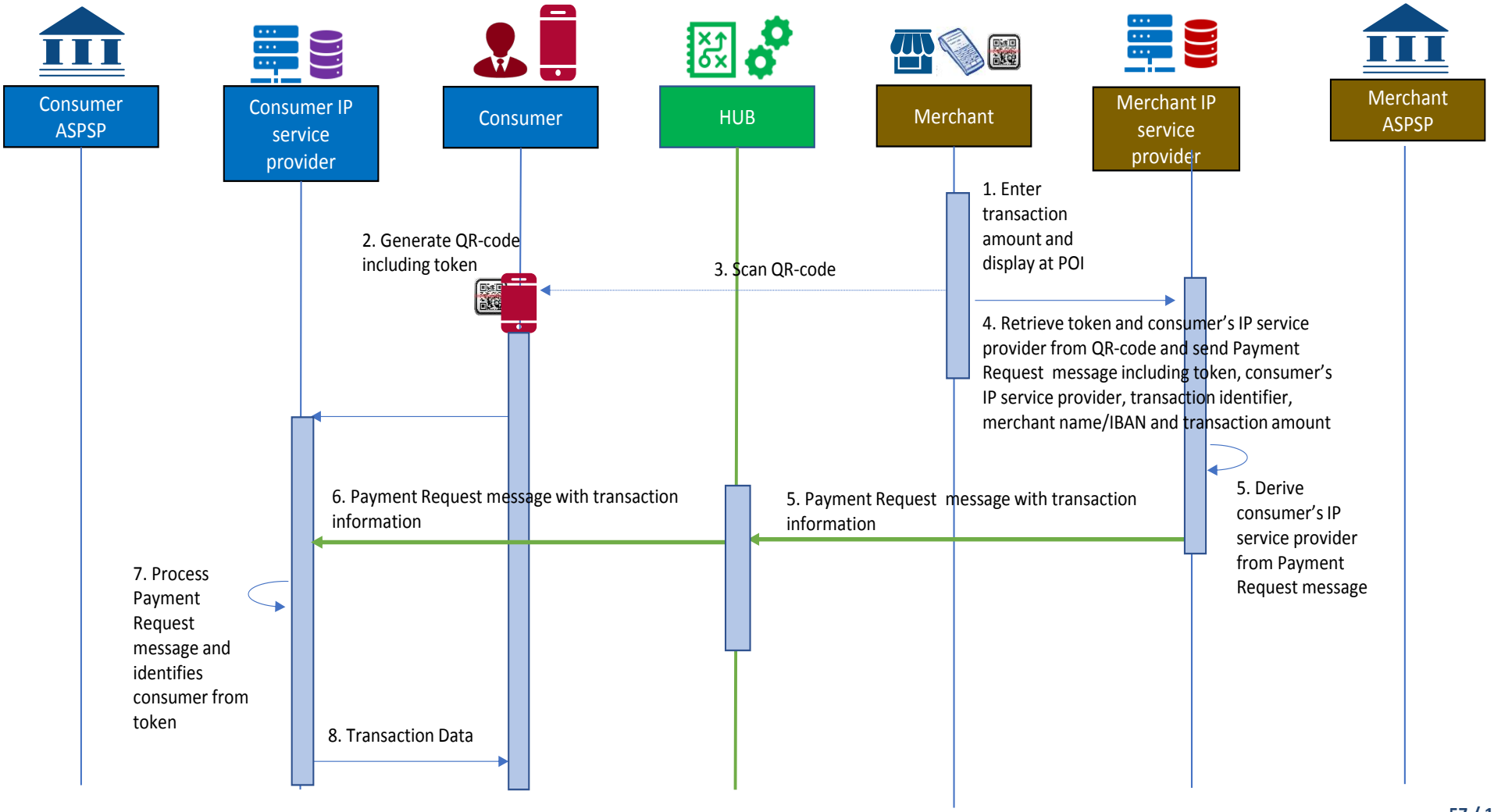


Figure 9: Actors for IP with consumer-presented data

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


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

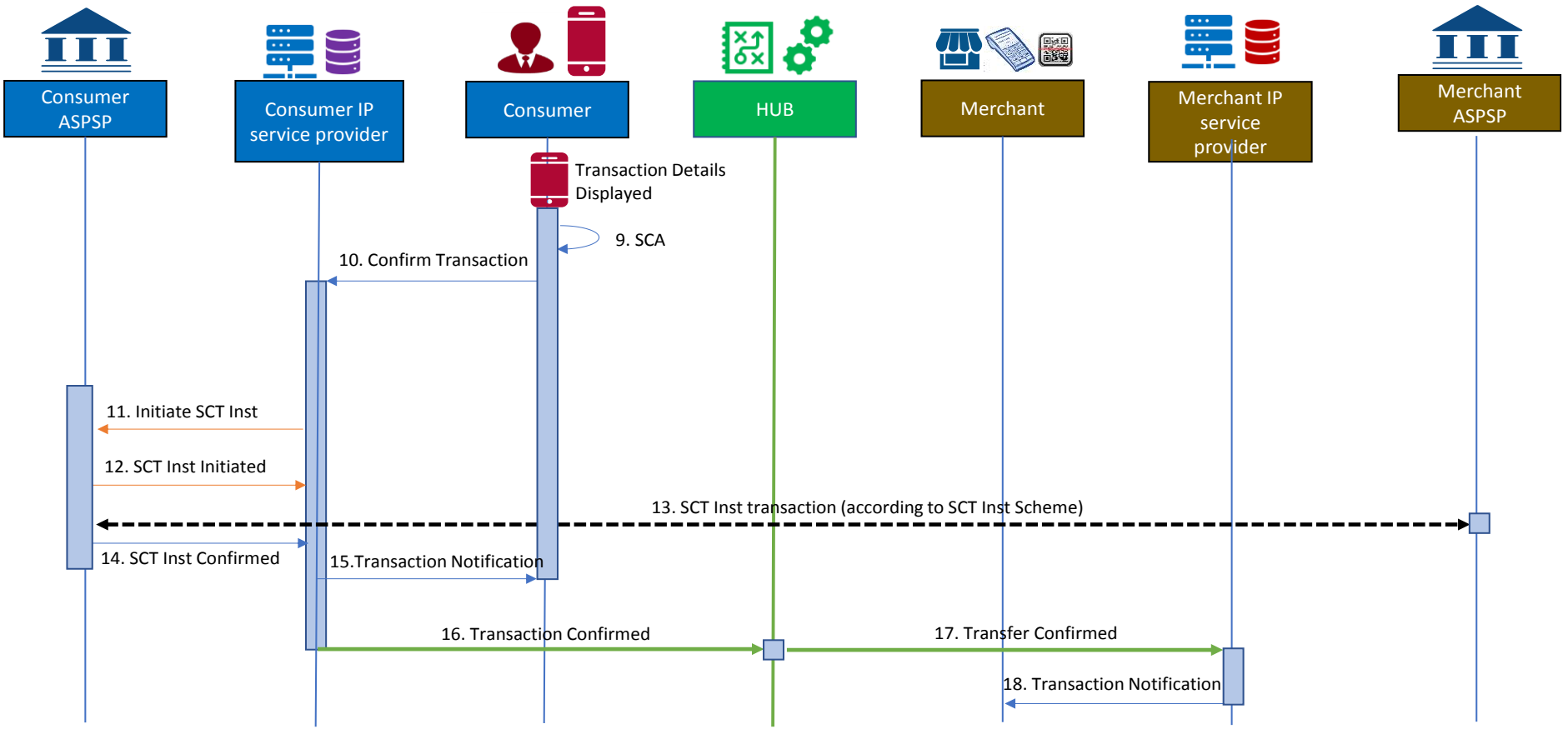


Figure 10: Process flow – C2B – consumer-presented QR-code with token

In the figure above the following steps are involved:

Step 1:

The merchant enters the transaction amount which is displayed on the POI[27].

Step 2

- The consumer selects and opens the IP application on their mobile device which possibly involves the entry of a password.
- A QR-code containing a consumer token and their IP service provider identifier is generated by the IP 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 IP service provider identifier from the QR-code and sends a Payment Request message to their IP service provider, including the merchant's name, IBAN_merchant[28], merchant transaction identifier, the transaction amount, the consumer's IP service provider identifier and the consumer token.

Step 5:

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

[27] The display of the transaction amount by the POI may happen after step 3, since the consumer identification might have an impact on the final transaction amount (e.g., due to discounts).
[28] Instead of the IBAN_merchant a proxy may be used.

Step 6:

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

Step 7:

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

Step 8:

The consumer's IP 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[29].

Step 10:

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

Step 11:

The consumer's IP 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 IP service provider confirming the initiation of the SCT Inst.

[29] The SCA may be performed by the consumer's IP 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 IP service provider has received delegation from the consumer's ASPSP for SCA subject to appropriate agreements.

Step 13:

The consumer's ASPSP sends the SCT Inst transaction to the merchant's ASPSP and the transaction flow is handled according to the SCT Inst scheme (see [7]).

Step 14:

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

Step 15:

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

Step 16:

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

Step 17:

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

Step 18:

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

7 HUB interconnectivity requirements

In order to enable interoperability, the following requirements need to be implemented by a HUB for the generic basic 4-corner model. Hereby the term HUB is meant to be agnostic to the way it might be implemented – logically or physically / centralised or de-centralised (e.g.., a direct standardised API) - different models may be possible which may or may not require a routing service.

In the tables below, the required functionalities for the HUB are listed for both the exchange of IP related data between the consumer and the merchant and the notification messages as analysed above.

IPs at POI based on merchant-presented data	
IP transaction feature	**Functional requirements on HUB**
Exchange of transaction data	
Merchant-presented data includes a token	De-tokenisation into transaction data is needed – Interconnection between consumer's and merchant's IP service providers is required via the HUB
All transaction data is available "in clear" to the consumer (e.g. in clear in QR-code)[30]	Not applicable
Merchant-presented data does not contain all transaction data or only part	Provision of full transaction data is needed – Interconnection between consumer's and merchant's IP service providers is required via the HUB

[30] In this case, another mechanism would need to be implemented to ensure the integrity of the data, see also Chapter 9.

of the transaction data in clear (e.g. contains a proxy)	
Notification messages	
Notification to merchant about successful/unsuccessful transaction	Notification from consumer's IP service provider to merchant's IP service provider
Notification to consumer about successful/unsuccessful transaction	Not applicable

Table 6: Required HUB functionalities for IPs at POI based on merchant-presented data

IPs at POI based on consumer-presented data	
IP transaction feature	**Functional requirements on HUB**
Consumer identification data	
Transfer of consumer's IP service provider identifier to merchant's IP service provider	The consumer's IP service provider identifier is used by the merchant's IP service provider and the HUB for routing purposes.
Transfer of consumer's token to consumer's IP service provider	Transfer of the consumer's token between the respective IP service providers – but included in the Payment Request message
Transfer of CustomerID and IBAN to consumer's IP service provider	Transfer of the CustomerID and IBAN between the respective IP service providers – but included in the Payment Request message

Transfer of CustomerID and IBAN-proxy to consumer's IP service provider	Transfer of the CustomerID and IBAN-proxy between the respective IP service providers – but included in the Payment Request message
Transaction data	
Transfer of transaction data to the consumer's IP service provider	Transfer of Payment Request message between IP service providers that includes the transaction data
Notification messages	
Notification to the merchant about successful/unsuccessful transaction	Notification from consumer's IP service provider to merchant's IP service provider
Notification to consumer about successful/unsuccessful transaction	Not applicable

Table 7: Required HUB functionalities for IPs at POI based on consumer-presented data

8 Minimum data sets and interoperability messages

This chapter specifies the minimum data sets to be exchanged between the consumer and merchant (see section 8.1), the QR-code standards to be used for data exchange between consumer and merchant (see section 8.2) and the minimum data elements to be included in the interoperability messages exchanged over the HUB (see section 8.3).

8.1 Minimum data sets

To achieve interoperability for IPs, an agreement on a minimum data set is required for the data to be exchanged between the consumer and the merchant. Any future specification of the data included in the messages between the respective IP service providers, through the HUB, will need to take this minimum data set into account.

8.1.1 IPs based on merchant-presented data

The minimum data set to be exchanged between the merchant and the consumer, will rely on the IP transaction feature, as described in Table 6 in section 7 in this document:

1. If the merchant-presented data provided to the consumer contains a (merchant) token, the minimum data will consist of both routing info and the token as payload. The minimum data will be forwarded in a Transaction Information Request message through the HUB from the consumer IP service provider to the merchant IP service provider for de-tokenisation into the transaction data.
2. If the merchant-presented data provided to the consumer contains all transaction data “in clear” (e.g. in clear in QR-code), the minimum data set will consist of both routing info and all necessary payload data.
3. If the merchant-presented data provided to the consumer contains only part of the transaction data in clear (e.g., contains a proxy), the transaction data will need to be further completed by the merchant’s IP service provider. The minimum data set will consist of both routing info and the available transaction data (e.g. the proxy). The minimum data will be forwarded in a Transaction Information Request message through the HUB from the

consumer IP service provider to the merchant IP service provider for completion of the transaction data.

The minimum data sets for these 3 cases include:

For case 1 - the merchant-presented data includes a token: [Version]+[Type]+ [Merchant IP Service Provider ID] + [token]
For case 2 - the merchant-presented data includes all transaction data "in clear": [Version]+[Type]+ [Merchant IP Service Provider ID] + [a clear-text name/value string]
For case 3 – the merchant-presented data contains a proxy for the merchant: [Version]+[Type]+ [Merchant IP Service Provider ID] + [proxy] + [a clear-text name/value string]

Table 8: Minimum data sets for IPs based on merchant-presented data

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 Payment Context / Case and the Lock Transaction (LT) Indicator (see Chapter 6).

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

8.1.2 IPs based on consumer-presented data

The minimum data set to be exchanged between the consumer and the merchant included in the consumer-presented data relies on the IP transaction feature, as described in Table 7 in section 7 in this document:

1. If the consumer-presented data provided to the merchant contains a (consumer) token, the minimum data will consist of both routing info and the (consumer) token as payload. The

minimum data will be forwarded in the Payment Request message through the HUB from the merchant's IP service provider to the consumer IP service provider for de-tokenisation into the consumer identification data, together with the other transaction data.

2. If the consumer-presented data provided to the merchant contains the CustomerID[31] and IBAN[32] "in clear" (e.g. in clear in a QR-code), the minimum data set will consist of both routing info and the CustomerID and IBAN. The minimum data will be forwarded in the Payment Request message through the HUB from the merchant's IP service provider to the consumer IP service provider together with the other transaction data.
3. If the consumer-presented data provided to the merchant contains the CustomerID[33] ("in clear") and an IBAN-proxy, the minimum data set will consist of both routing info and the CustomerID and IBAN-proxy. The minimum data will be forwarded in the Payment Request message through the HUB from the merchant's IP service provider to the consumer IP service provider together with the other transaction data. The IBAN will be derived from the IBAN-proxy by the consumer IP service provider.

The minimum data sets for these 3 cases include:

For case 1 - the consumer-presented data includes a token: [Version]+[Type]+[Consumer IP Service Provider ID]+[(consumer's) token]
For case 2 – the consumer-presented data contains the CustomerID and IBAN "in clear" [Version]+[Type]+[Consumer IP Service Provider ID]+[CustomerID + IBAN]
For case 3 – the consumer-presented data contains the CustomerID "in clear" and a proxy [Version]+[Type]+[Consumer IP Service Provider ID]+[CustomerID + IBAN-proxy]

Table 9: Minimum data sets for IPs based on consumer-presented data

[31] Subject to further clarification by EBA that CustomerID is non-sensitive data (see EBA Q&A 2020_5476).
[32] Subject to further clarification by EBA (see EBA Q&A 2020_5477).
[33] Subject to further clarification by EBA that CustomerID is non-sensitive data (see EBA Q&A 2020_5476).

Note: There might be a need for the merchant to identify the consumer to offer additional services or benefits. For interoperability, the consumer identification means would need to be standardised in future work and could be added to the payload information (see section 8.2.3).

The version refers to the specification version of the format of the proximity technology used (e.g., the QR-code, see section 8.2).

The type may refer to the cases above and may enable to add other services[34].

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

The consumer identification data needs to be included in the Payment Request message. Therefore, a predefined length and character set need to be specified.

8.2 IP at POI QR-codes standard

8.2.1 Introduction

To enable IP interoperability across SEPA, for the data exchange between the merchant and consumer, IP QR-codes should be standardised based on the minimum data sets defined in section 8.1 in this document.

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

The standardised consumer-presented QR-codes should be adopted by all IP service providers and supported by the merchant's POI.

[34] An example may be a refund.

8.2.2 Principles for development of IP QR-codes

For the development of a standardised IP QR-code based on ISO /IEC 18004 [23] the following four principles will be followed:

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

When following the principles above, a QR-code format for IPs for data exchange between the merchant and the consumer could be based on the following preconditions:

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

8.2.3 IP QR-codes format

It is suggested that the IP QR-codes are be based on the following format:

- A URL based on https:// structure
- First part of the URL: ordinary domain structure
- Second part of the URL: version

- Third part: type (this may refer to the payment context or the LT indicator)
- Fourth part: routing information
- Fifth part: payload information[35].

HTTPS://<Domain_name>/<Version>/<Type><merchant IP service provider ID/<Payload>

Table 10: Merchant-presented QR-code

HTTPS://<Domain_name>/<Version>/<Type><consumer IP service provider ID/<Payload>

Table 11: Consumer-presented QR-code

The Domain name refers to the IP interoperability framework.

The Version refers to the specification version.

The Type could refer

- for merchant-presented QR-codes to different payment contexts (e.g. physical POI in store or e- and m-commerce) or cases as described in section 8.1.1 and the Lock Transaction Indicator (see Chapter 6);
- for consumer-presented QR-codes to the different cases as described in section 8.1.2 or enable to add other services[36].

The Lock Transaction Indicator is used to inform about the need of the Lock Transaction Function to mitigate the risk about unwanted multiple payments for the same merchant-presented QR-code (see also chapter 6).

8.2.4 Examples of payload content for merchant-presented IP QR-codes

In the table below, the payload data for the three cases defined in section 8.1.1 are listed.

[35] For consumer-presented QR-codes this would be the consumer identification data.
[36] An example may be a refund.

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

Case 3[37] **the merchant-presented transaction data includes a proxy for the merchant**	MCC	Merchant Category Code
	Purpose of credit transfer (includes e.g. merchant transaction identifier)	Data for reconciliation purposes at merchant – is included from initiation through entire transaction payment chain)
	Remittance information structured or Remittance information unstructured	
	Currency	
	Transaction amount	

Table 12: Examples of payload data for merchant-presented IP QR-codes

8.2.5 Examples of payload content for consumer-presented IP QR-codes

In the table below, the proposed payload data for the three cases defined in section 8.1.2 are listed.

Payload Data (Consumer identification data)	
Case 1 **the consumer-presented transaction data includes a token**	Token
Case 2	CustomerID (Consumer)

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

the consumer-presented transaction data includes all consumer identification data "in clear"	IBAN Consumer
Case 3	CustomerID (Consumer)
The consumer-presented transaction data includes a proxy	IBAN-Proxy (for the IBAN Consumer)

Table 13: Examples of payload data for consumer-presented IP QR-codes

8.3 Interoperability messages

This section aims to identify the minimum data elements that need to be included in the various interoperability messages exchanged over the HUB (see chapter 7). Obviously these data sets need to be further validated by appropriate implementations and interoperability testing of IPs at the POI. Additional flows and r-messages might be needed between the respective IP service providers in case of unsuccessful /failed transactions that will need to be further analysed and specified in future work.

8.3.1 Transaction Information Request and Response

This section describes the minimum data elements to be included in the Transaction Information Request and Response messages to be exchanged between the respective IP service providers via the HUB for IPs at POI based on merchant-presented data whereby not all transaction data is provided "in clear". The purpose of these messages is to provide the full transaction data in clear to the Consumer IP service provider to enable the initiation of an IP at POI based on the token or proxy for the merchant, obtained by the Consumer IP service provider from the merchant-presented data (see chapters 5 and 6).

Between IP service providers

Name:	Transaction Information Request
Description:	This dataset describes the content of the Transaction Information Request sent by the consumer IP service provider to the merchant IP service provider via the HUB to obtain the full transaction data based on a proxy, token or part of the transaction data provided in the merchant-presented data. Attributes are mandatory (M) unless otherwise indicated (O).
Attributes contained	• The merchant-proxy, token or part of the transaction data[38] (M) • The consumer IP service provider identifier (M) • The merchant IP service provider identifier (M) • The Identification code of the IP at POI scheme (M) • Additional unique reference provided by the consumer IP service provider (O) • Place holder for charging (O)

Table 14: Dataset for Transaction Information Request by the consumer IP service provider to the merchant IP service provider

Between IP service providers

Name:	Transaction Information Response
Description:	This dataset describes the content of the Transaction Information Response sent by the merchant IP service provider to the consumer IP service provider via the HUB to deliver the full transaction data. Attributes are mandatory (M) unless otherwise indicated (O).
Attributes contained	• The transaction amount (M) • The currency (M) • The remittance Information (O) • The consumer IP service provider identifier (M) • The IBAN of the merchant (M) • The name of the merchant (M) (account holder) • The trade name of the merchant (M) • The merchant's reference party[39] (O) • The address of the merchant (O)

[38] As provided in the merchant-presented data e.g. transaction identifier.
[39] Ultimate party to which an amount of money is due.

Name:	Transaction Information Response
	• The BIC code of the merchant ASPSP (O) • The merchant IP service provider identifier (M) • The Identification code of the IP at POI scheme (M) • The transaction identifier (M) • The Merchant Category Code (MCC) (M) • Type of payment instrument requested by the merchant (SCT Inst) (M) • Flag notification message required (M) • Additional unique reference provided by the consumer IP service provider (O) • Place holder for charging (O)

Table 15: Dataset for Transaction Information Response by the merchant IP service provider to the consumer IP service provider

8.3.2 Lock transaction messages

This section describes the minimum data elements to be included in the Lock Transaction messages exchanged between the respective IP service providers via the HUB for IPs at POI based on merchant-presented data. The purpose of these messages is to prevent that multiple consumers from different IP service providers pay the same transaction. The transaction lock function would be typically required in case the QR-code stays active for a certain time window that would enable multiple scans and related payment (see chapter 6).

Name:	Lock Transaction Request by consumer IP service provider to merchant IP service provider
Description:	This dataset describes the content of the Lock Transaction Information Request sent by the consumer IP service provider to the merchant IP service provider via the HUB to lock the transaction for a specific consumer. Attributes are mandatory (M) unless otherwise indicated (O).
Attributes contained	• The transaction identifier (M) • The transaction amount (M) • The currency (M) • The name of the consumer(M) • The IBAN of the consumer (M) • The name of the merchant name (M)

Name:	Lock Transaction Request by consumer IP service provider to merchant IP service provider
	• The trade name of the merchant (M) • The merchant's reference party (O) • The IBAN of the merchant (M) • The remittance Information (O) • The consumer IP service provider identifier (M) • The merchant IP service provider identifier (M) • The Identification code of the IP at POI scheme (M) • Place holder for charging (O)

Table 16: Dataset for Lock Transaction Request by the consumer IP service provider to the merchant IP service provider

Name:	Lock Transaction Response by merchant IP service provider to consumer IP service provider
Description:	This dataset describes the content of the Lock Transaction Information Response sent by the merchant IP service provider to the consumer IP service provider via the HUB to lock the transaction for a specific consumer. Attributes are mandatory (M) unless otherwise indicated (O).
Attributes contained	• The transaction identifier (M) • The transaction amount (M) • The currency (M) • The name of the consumer (M) • The IBAN of the consumer (M) • The name of the merchant name (M) • The trade name of the merchant (M) • The merchant's reference party (O) • The IBAN of the merchant (M) • The remittance Information (O) • The consumer IP service provider identifier (M) • The merchant IP service provider identifier (M) • The Identification code of the IP at POI scheme (M) • Place holder for charging (O)

Table 17: Dataset for Lock Transaction Response by the merchant IP service provider to the consumer IP service provider

8.3.3 Payment Request Messages

This section addresses the minimum data sets for the Payment Request Messages exchanged in support of IPs at POI from the Merchant to their IP service provider and between the respective IP service providers, through the HUB for IPs based on consumer-presented data (see chapters 5 and 6).

From merchant to merchant IP service provider

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

Table 18: Dataset for Payment Request Message by merchant to merchant IP service provider

Between IP service providers

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

Table 19: Dataset for Payment Request Message by the merchant IP service provider to the consumer IP service provider

8.3.4 Notification Messages

This section describes the minimum data elements to be included in the Notification Messages from the consumer ASPSP to the consumer IP service provider (subsequent to the confirmation message

(6) in Figure 1 in [7]) and from the consumer IP service provider to the merchant IP service provider via the HUB (see chapters 5 and 6). Note that the Notification messages to the consumer and the merchant from their respective IP service providers are not specified in this document since they are not impacting the interoperability of IPs at the POI and are left at the discretion of the respective IP service providers.

From consumer ASPSP to consumer IP service provider

Name:	**Notification about the execution of the IP by the consumer ASPSP to the consumer IP service provider**
Description:	This dataset describes the content of the Notification about the execution of the IP from the consumer ASPSP to the consumer IP service provider via the HUB. Attributes are mandatory (M) unless otherwise indicated (O).
Attributes contained	• Transaction status • The name of the Consumer • The transaction amount (M) • The currency (M) • The remittance Information (O) • The time of execution • The Consumer IP service provider identifier (M) • The IBAN of the Merchant (M) • The name of the Merchant (M) (account holder) • The trade name of the Merchant (M) • The merchant's reference party (O) • The BIC code of the Merchant ASPSP (O) • The Merchant IP service provider identifier (M) • The Identification code of the IP at POI scheme (M) • The transaction identifier (M) • Additional unique reference provided by the Consumer IP service provider (O) • Place holder for charging (O)

Table 20: Dataset for Notification message about the execution of the IP by the consumer ASPS to the consumer IP service provider

Between IP service providers

Name:	Inter IP service provider Notification about the execution of the IP
Description:	This dataset describes the content of the Notification about the execution of the IP from the consumer IP service provider to the merchant IP service provider via the HUB. Attributes are mandatory (M) unless otherwise indicated (O).
Attributes contained	• The name of the Consumer (M) • The transaction amount (M) • The currency (M) • The remittance Information (O) • Transaction status • The time of execution • The Consumer IP service provider identifier (M) • The IBAN of the Merchant (M) • The name of the Merchant (M) (account holder) • The trade name of the Merchant (M) • The merchant's reference party (O) • The BIC code of the Merchant ASPSP (O) • The Merchant IP service provider identifier (M) • The Identification code of the IP at POI scheme (M) • The transaction identifier (M) • Additional unique reference provided by the Consumer IP service provider (O) • Place holder for charging (O)

Table 21: Dataset for Notification message about the execution of the IP by the consumer IP service provider to the merchant IP service provider

9 Security and trust

9.1 Security guidelines for IPs at POI

It is not the purpose of this document to provide detailed specifications related to security and trust. Nevertheless, the framework for interoperability of IPs at the POI shall follow some principles to ensure security and trust.

With respect to the customer authentication for IPs at the POI, the PSD2, RTS and EBA guidelines define the regulatory framework comprehensively. Guidance is also provided in chapter 8 of the MSCT IG [9].

A risk analysis and security measures for the SCT Inst scheme are specified in the Risk Management Annex to the SCT Inst scheme rulebook [7]. Additional guidelines for security aspects related to instant payments initiated through a mobile device have also been specified in the MSCT IG [9] and could be leveraged for IPs at the POI (i.e. also for those IPs initiated via other consumer devices than mobile devices) to achieve and maintain an appropriate level of trust and security in the IP at POI ecosystem.

The MSCT IG [9] covers the following security guidelines:

- Generic security requirements for the customer-to-PSP space[40] (see chapter 9 in [9]) based on a threat analysis. These are covering the communications between the consumer and their MSCT provider and between the merchant and their MSCT provider, which can easily be extended for IPs at the POI;
- Security considerations for the consumer-to merchant space (see chapter 10 in [9]) that includes proximity technologies, web-based payments, merchant applications and some additional security measures in this space;
- Security guidelines for mobile devices (see chapter 11 in [9]);
- Security guidelines for MSCT applications (see chapter 12 in [9]) that could be straightforward extended to IP applications.

[40] Note that the security guidelines related to the inter PSP space are specified in the Risk Management Annex of the SCT Inst scheme rulebook which is applicable to SCT Inst scheme participants.

9.2 Security aspects of QR-codes and their data

9.2.1 Introduction

This section discusses in some more detail the security of the QR-codes defined in Chapter 8. It has been contributed by the MSG MSCT[41] and was subsequently updated by the ERPB WG.

The QR-code shall only contain non-sensitive payment data to be used in the processing of the IP at POI transaction. Nevertheless, tampering of QR-codes may lead to fraudulent transactions or data leakage. Below a brief security analysis is made for the two QR-code formats defined in section 8.2.

For merchant-presented QR-codes, three possible minimum data sets have been identified for the payload in section 8.1.1.

In the case of a merchant-presented QR-code, the consumer needs to have an IP application or another application linked to the IP application on their consumer device that has the capability of scanning the QR-code of the merchant. Typically, from this QR-code the data will be retrieved to enable the initiation of the IP using the IP application.

For consumer-presented QR-codes, three possible minimum data sets have been identified for the payload in section 8.1.2.

In the case of a consumer-presented QR-code, the consumer can make purchases using data associated with themselves or their account and previously provisioned to their consumer device. This data may range from consumer identification data, over an IBAN[42] to a token which are used to calculate a QR-code (static or dynamic). The consumer typically has to select the QR option within their IP application, which will result in the display of the QR-code on the consumer device. The QR-code is scanned by the merchant at the time of payment to complete the purchase.

A QR-code code may be static, e.g., merchant account data and related payment details for a fixed transaction amount (typical use case of a transport ticket) or may be dynamic to initiate/identify a single specific IP at POI transaction.

[41] It is intended to be included in a future release of the MSCT IG (see [9]).
[42] Subject to further clarification by EBA (see EBA Q&A 2020_5477).

Tampering QR-code data may lead to fraudulent transactions or data leakage. Therefore, the processing of QR-code data should be adequately protected. Also the integrity of the data elements in the QR-code should be ensured to avoid any service disruptions.

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

9.2.2 Merchant-presented QR-codes

Proxy and payload information that is present "in clear" in the QR-code needs an integrity protection to avoid manipulations with the intention to initiate fraudulent transactions (e.g. to a fake merchant or with a wrong transaction amount).

Depending on the outcome of EBA Q&A 5477, the IBAN of the merchant, if present "in clear", may also require additional security protection outside the inter-PSP space, e.g. in the QR-code.

It should further be noted that in certain countries (e.g., France, Sweden, …), in view of national regulations, the IBAN needs to be protected outside the inter-PSP space This means that in some countries it is recommended that the IBAN is not included "in clear" into the merchant-presented QR-code.

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

9.2.3 Consumer-presented QR-codes

Any form of a static consumer-presented QR-code, e.g. a static CustomerID and IBAN or a static token) could lead to impersonation attacks and initiation of fraudulent transactions (see for example [10]) and reputational damage. Therefore, preference should be given to dynamic QR-codes on the consumer side, and static ones must be handled with great care.

Customer IDs, IBANs and proxies that are present "in clear" in the QR-code need an integrity protection to avoid mistakes with the initiation of transactions (e.g. using the wrong consumer).

The CustomerID might be a consumer credential (e.g. for access to online banking system). Capture of the CustomerID and IBAN could lead to impersonation attacks and initiation of fraudulent transactions[43] (see for example [10]) and reputational damage while also contaminating other payment instruments such as SDD. Depending on the outcome of EBA Q&A 5476, if the CustomerID is considered to be sensitive payment data, it needs to be properly protected, e.g. encrypted or tokenised to ensure its confidentiality, before it can be used in a QR-code.

Depending on the outcome of EBA Q&A 5477, the IBAN of the consumer may also require additional security protection outside the inter PSP space, e.g. in the QR-code.

It should further be noted that in certain countries (e.g., France, Sweden, …), in view of national regulations, the IBAN needs to be protected outside the inter-PSP space This means that in some countries it is recommended that the IBAN is not included “in clear” into the consume-presented QR-code.

Depending on the outcome of EBA Q&A 2020_5587, the creation of the consumer-presented QR-code could be subject to specific security measures and restricted to some form of supervision or certification of the entity/application creating the QR-code.

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

[43] Although application of SCA in the instant SCT transaction is a mitigating measure.

10 Security requirements for payment service user on-boarding

This chapter specifies Security requirements for payment service user (PSU) on-boarding processes to be adopted by instant payment service providers and merchants and has been developed by a dedicated Joint Task Force ERPB WG / MSG MSCT (see Annex 5). The Joint Task Force leveraged for their development the chapter 14 of the MSCT IG [9].

10.1 Introduction

IP service providers and merchants shall take appropriate measures to identify and register PSUs to whom they deliver their services.

It is essential for payment service providers to check that a particular communication, transaction, or access request is legitimate. Accordingly, IP service providers shall use reliable methods for verifying the identity and authorisation of new PSUs. PSPs should furthermore use reliable methods for authenticating the identity and authorisation of established PSUs seeking to register for new IP services. Also merchants that on-board consumers to facilitate IPs (e.g., by offering a dedicated app or storing consumer data related to IPs) shall use similar reliable methods for this process.

Details on the risks involved with PSU on-boarding, are for example provided in chapter 5 and the overview tables on pages 37-38 in [6] and in section 4.5 in [10].

Furthermore, when implementing secure measures to comply with the requirements specified in this document, proportionality of these measures should be taken into account to achieve the right balance between security and PSU acceptance (see [16]).

10.2 Security requirements

PSUs shall be registered (on-boarded) for IP services by IP service providers or merchants using one of the following means:

- Electronically via a dedicated application (e.g. an on-line banking app or merchant app) or via a website;
- Physical presence.

RQ1	In case of remote electronic registration, appropriate measures shall be in place to control the connection (communication channel) between the IP service provider or the merchant and the PSU such that unknown third parties cannot displace PSUs.

A secure communication channel ensuring integrity and confidentiality as needed between the PSU and their IP service provider or the merchant shall be made available. Examples include a website connection via TLS1.2 or higher (according to the state of the art) or a dedicated app with endpoint security on the PSU's device.

RQ2	IP service providers and merchants[44] who are not ASPSPs, shall rely on the PSU identification and authentication method used by the PSU's ASPSP for the on-boarding of the PSU for the IP service and the linking to the PSU's account.

Electronic identification and "Know Your Customer" (KYC) processes used by ASPSPs are set out by regulatory authorities and are based on robust customer identification and authentication processes applied for the registration of customers[45]. These are particularly important in the cross-border context given the additional difficulties that may arise from doing business electronically with customers across national borders, including the increased risk for identity impersonation (see [6] and [10]) and the greater difficulty in conducting effective credit checks on potential customers.

In case customers use PKI certificates for their electronic identification when registering for an IP service, the PSU identification used by the certificate authority shall be accepted by the ASPSP and supervised by the competent authorities. In case eIDAS electronic identification means for PSUs are used, the mutual recognition for the usage of these means is laid down in the eIDAS Regulation [5], which enhances cross-border trust.

[44] Or a third party acting on behalf of them.
[45] For example, Annexes 2 and 3 in [2] provide insights into the different KYC methods used.

In case a third party is involved e.g., on behalf of a merchant, appropriate agreements shall be in place that cover the security requirements and liabilities.

RQ3	PSUs shall explicitly register for an IP service, linked to one or more payment accounts from their ASPSPs. This requirement remains valid for any re-registration[46] or de-registration process.

This explicit registration aims to raise PSU awareness and stresses the trust factor involved in conducting IPs. This may also involve the download and activation of a dedicated IP application or software on the PSU device.

RQ4a	To ensure that the request was made by the legitimate consumer and their registered device, without disrupting the user experience, consumer device binding shall be implemented by ASPSPs, IP service providers and merchants as appropriate. The procedure implemented shall also cater for loss or renewal of the consumer device.
RQ4b	To ensure that the request was made by the legitimate merchant and their POI, the POI platform used shall be identified and possibly platform binding applied as appropriate[47]. The procedure implemented shall also cater in case of upgrades of the POI platform.

PSU device binding refers to a reliable and consistent verification of the PSU device used for IPs by registering the PSU device and binding it with a PSU credential, e.g. as part of the PSU on-boarding process. This enables to validate this PSU device used in subsequent IP transactions.

[46] As examples, a re-registration process is needed in case of change of payment account or loss of the consumer device.
[47] Depending on the type of POI platform.

For achieving this binding, the trust of existing PSU devices could be leveraged. As an example a strong PSU device ID could be used. This is a unique tamper resistant identifier that cryptographically binds a specific PSU device (e.g. mobile device) to a PSU's identity, leveraging PKI capabilities.

RQ5	IP service providers, if involved, shall implement controls to ensure that credentials as appropriate are distributed to PSUs in a way that is trustworthy. The level of trust in the PSU's identity shall be maintained throughout the IP service lifecycle, including the re-issuance of credentials.

IP service providers shall keep control of addressing information (physical or online) which are used for communication with the PSU. IP service centre staff shall be well informed and educated in the procedures that are used for distributing credentials. All distributions of new credentials or downloading of the IP application shall be logged. IP service providers should consider giving the PSU a notification through a dual communication channel (see [1]).

RQ6	All stored personal data about PSUs and (sensitive) payment data related to IP transactions and related messages IP service providers hold shall be protected in strict accordance with the legal and regulatory requirements (PSD2, GDPR) and used solely for the purposes explicitly allowed by the respective "data subject".

11 Interoperability rules and procedures

11.1 Interoperability principles

The following principles for interoperability of IPs at POI across SEPA shall be supported by IP service providers of consumers and merchants:

Consumer IP service providers:
Consumer IP service providers shall enable their consumers to perform IPs at POI with both consumer- and merchant-presented data modes with their consumer device.
Merchant IP service providers:
Merchant IP service providers shall enable the merchant's POI (physical and/or virtual POIs) to support at least one mode for IPs: either merchant-presented or consumer-presented data.

Table 22: Interoperability principles for IPs at POI

11.2 Recognition Label

There is a need for the development of a recognition label that shows to PSUs that an IP at POI solution may be used for the payment of goods or services with a merchant, hereby ensuring interoperability of IPs at the POI as specified in this Framework.

Since Recommendation A of the ERPB Statement published in November 2019[48] has assigned the development of such a label to the MSG MSCT, the present document will not further elaborate on this topic.

[48] See https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/12th-ERPB-meeting/Statement.pdf?8f5bd56a229964fc0353ee6289a799b6

11.3 Registration of IP service providers

To ensure interoperability between IP service providers, there is a need to register these providers and assign them a unique IP service provider ID that is present in the minimum data sets exchanged between the consumer and the merchant for routing purposes (see Chapter 8) of the interoperability messages used in the process flows for IPs at POI transactions (see Chapter 6). This will need to be dealt with when establishing the Framework for interoperability (see Chapter 12).

11.4 Need for additional IP services

There is need to address additional payment services for IPs at the POI such as a repayment (refund[49]), pre-authorisation and recurring payments to ensure the success of IPs at the POI. Since Recommendation E of the ERPB Statement published in November 2019[50] has recommended the EPC to further analyse these services for the instant SCT scheme by November 2020, the present document will refrain from further elaborating on this topic.

[49] Referred to as "Transfer back" in [7].
[50] See https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/12th-ERPB-meeting/Statement.pdf?8f5bd56a229964fc0353ee6289a799b6

12 Governance

12.1 Introduction

Since a Framework is currently seen as the best way forward to support the interoperability of IPs at the POI, this chapter aims to address at a high-level a possible Framework governance and the different aspects to be covered, which would need to be further detailed before such a governance structure could be established.

The main aim of the Framework governance is to support the development and maintenance of the specifications, rules and procedures and security requirements for interoperability of IPs at POI across SEPA as specified in this Framework document (see Chapters 5, 7, 8, 9, 10 and 11).

Participation to the Framework should be on a voluntary basis and market support should be achieved by ensuring that attractive market opportunities can be enabled through the Framework.

12.2 Framework governance principles

The following principles should be considered when establishing a Framework governance:

- Definition of the scope of activities that the Framework governance can decide on. This scope is reflected by what is in the red box in the figure below.

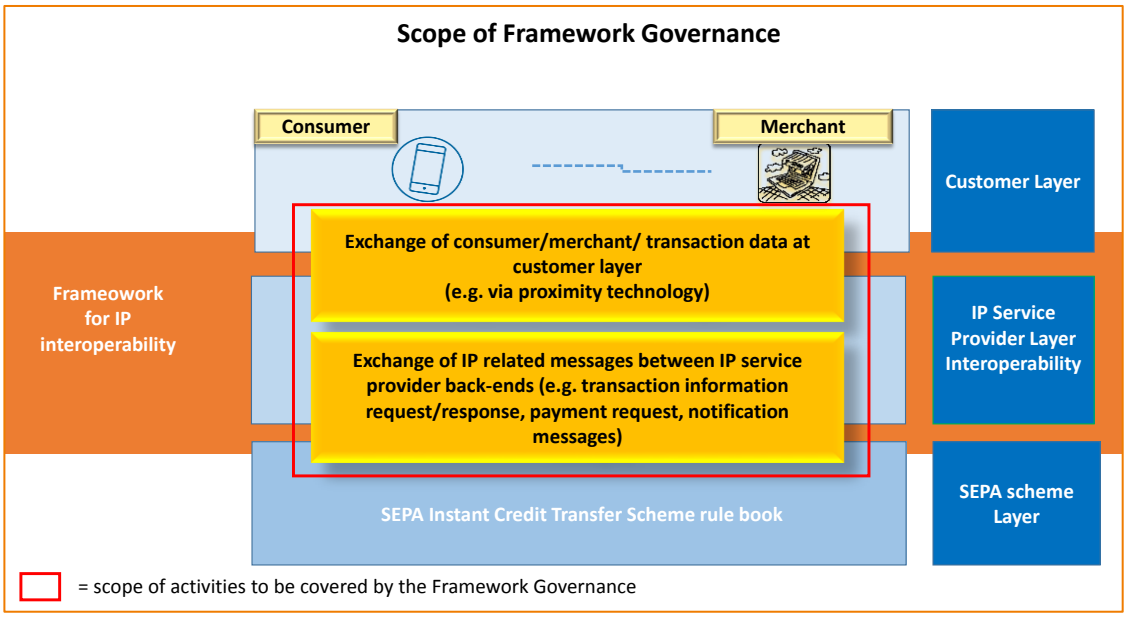


Figure 11: Scope for the governance of the interoperability framework for IPs at the POI

- The Framework will be open to all eligible actors in the ecosystem.
- All members of the Framework Governance Body shall adhere to the specifications set by the Framework as appropriate (see section 12.3).
- Applications and membership are managed by the Board of the Framework Governance Body (see section 12.5).
- Compliance to the Framework specifications will need to be defined by the Framework Governance Body (e.g. self-certification or certification by an external trusted auditor).
- Dedicated Framework Governance Body internal rules need to be developed to govern the funding, intellectual property, compliance and dispute handling, etc. of the Framework.
- The Framework evolution and maintenance process shall be entrusted to the Framework Governance Body.
- The Framework should be promoted throughout the IP at POI value chain, to enable a more harmonised SEPA IP at POI ecosystem.

12.3 Framework adherence

In principle, subject to applicable regulatory requirements, the Framework for interoperability of IPs at POI should be open for adherence to all relevant stakeholders involved in the IP at POI ecosystem, which meet the relevant eligibility requirements (to be defined).

This means that multiple types of adhering entities could implement the interoperability requirements specified in this Framework such as:

- ASPSPs
- IP service providers
- IP at POI solutions
- IP at POI schemes
- Processors
- Retailers (Merchants)

- …….

Adherence to the interoperability framework should be based on a form of certification (e.g. self-certification or certification by an external trusted auditor) and could potentially be linked to the permission for usage of the recognition label (see section 11.2).

12.4 Membership of the Framework Governance Body

In principle, subject to applicable regulatory requirements, Framework participation should be open to all relevant stakeholders involved in the IP at POI ecosystem. This means it should potentially accommodate multiple types of participating entities that could be grouped into "Sectors" such as

- ASPSPs
- IP service providers
- IP at POI solutions
- IP at POI schemes
- Processors
- Retailers (Merchants)
- Consumer organisations
- Vendors (consumer devices, POI, HW, SW)
- ……

Hereby two categories of participation in the Framework could be envisaged:

- A *Full Member* is a participant in the Framework that adheres to the interoperability requirements of the Framework as appropriate. A Full Member is expected to **actively contribute** to the further enhancement of the Framework. Full Members will need to participate through a specific Sector[51] involved in the interoperability framework.
- An *Associate Member* is a participant that adheres to interoperability requirements of the Framework as appropriate. An Associate Member has only a **consulting role** with respect to

[51] Although potentially a member could be involved in several Sectors, they will need to choose their preferred one.

the further development and maintenance of the Framework. Associate Members will need to participate through a specific Sector involved in the interoperability Framework.

- Members (Full and Associate Members) in each Framework Sector can be either individual legal persons or member associations representing (part of) a single Framework Sector. Each of the Framework Sectors will be responsible for organising themselves and developing their own rules of functioning.

12.5 Framework Governance Body

The Framework Governance Body should be composed of representatives of Full Members and Associate Members whereby only Full members are entitled to vote. It should be structured so as to ensure a true and balanced representation of the membership through the different Sectors involved in the Framework.

The main entities of the Framework Governance Body could be a General Assembly and a Board of Directors.

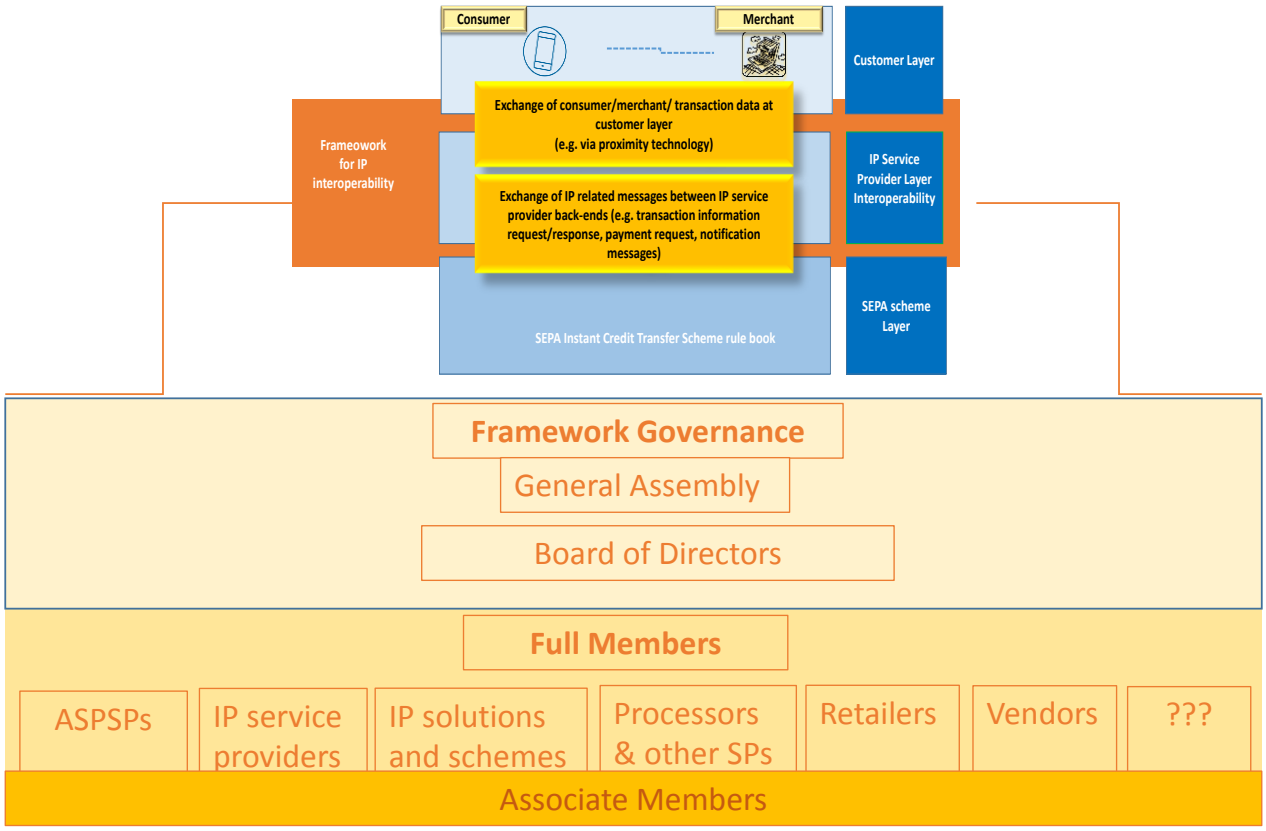


Figure 12: Possible model for Framework Governance

- The Framework General Assembly (GA) should be composed of all Full Members and Associate Members, whereby only Full Members are entitled to vote. It should have the responsibilities as to be defined in the internal rules of the Framework management. It could be supported in its role by the Board of Directors.
- The members of the Framework Governance Body Board of Directors (BoD) should be elected amongst the Full Members by and report to the GA and should represent the various Sectors present within the Framework with a maximum number of seats while having a fair and balanced representation of the Sectors involved in the interoperability framework. The Board should report to the General Assembly and should have all powers necessary to accomplish the purpose of the Framework.
- The Framework Governance should be funded by the different Sectors involved in the interoperability framework. Each Sector should be responsible for organising their representation and funding.
- Decision making processes within the GA and the BoD should ensure that features and any major subsequent changes will be adopted by a large majority of Full Members (e.g. 70 per cent). Decision making powers should be specified in the internal rules at a later stage.
- The Board should be supported by the Sub-Groups, the Task Forces and the Expert Teams that the Board may establish and revoke from time to time.

Framework management internal rules would need to be defined and would need to be transparent to ensure a proper functioning of the Framework. These internal rules should contain clear descriptions of the internal organisation, structure, rules and processes that make up the Framework management. The rules would also need to describe change management and compliance processes and the way the Framework would interact with any potential Framework overseer.

13 Conclusions and way forward

This document is defining the different interoperability requirements (technical and security), interoperability rules and procedures to achieve interoperability of IPs at the POI. It further contains a high level description on different aspects that should be taken into account in a future governance of this interoperability framework.

While developing this document, the ERPB WG has also identified a number of challenges that would need to be addressed before this interoperability framework for IPs at the POI with an appropriate governance could be established. This includes at least the following topics:

- clarifications to be provided by the EBA Q&A tool on the different questions related to this document and its Annex 1 that have been coordinated with but entered by the MSG MSCT;
- the additional services for instant SCTs that have been included in the Recommendation E in the ERPB Statement of November 2019;
- the development of a recognition label as recommended in the Recommendation A in the ERPB Statement of November 2019.

The ERPB WG wishes to make the following recommendations to the ERPB:

#	Addressee	Rationale	Recommendation	Dead-line
A	MSG MSCT[52]	To address the technical gaps identified during the development of the Interoperability Framework for IPs at the POI	• Analyse interoperability of additional flows and r-messages between the respective IP service providers in case of unsuccessful /failed transactions; • Further analyse technical interoperability for models involving a PISP or CPSP; • Analyse impact of replies on EBA Q&A questions[53] posted by the MSG MSCT on technical interoperability of IPs at POI and related security aspects; • Develop use cases for IPs at POI whereby the consumer device has no internet connection at the transaction time (so-called offline use cases) and analyse their impact on interoperability.	June 2021

[52] Subject to the approval of the Extension of the mandate of the MSG MSCT by the EPC Board in November 2020.
[53] See EBA Q&A 2020_5365-5367, 5476, 5477, 5570-5573, 5587)

			These deliverables[54] should serve as inputs to any further work on an Interoperability framework for IPs at the POI	
B[55]	Group with multi-stakeholder participation consisting of market participants in card and SCT Inst payments	Need to ensure that the consumer's choice of a given payment instrument to conduct a payment transaction at the POI is respected	Develop standards, business and technical requirements as appropriate, leading to interoperable specifications that ensure consumer selection of preferred payment instrument (card payment or SCT Inst) to conduct a payment transaction at the POI (physical or virtual POI) based on the deliverable ERPB Inst@POI 45-20v1.1	Nov. 2021

[54] In accordance with the scope of the proposed MSG MSCT mandate extension (MSG MSCT 91-20).
[55] This recommendation is already contained in document ERPB Inst@POI 45-20v1.1.

C	Group with multi-stakeholder participation	A dedicated framework is needed to manage the interoperability rules and appropriate governance for IP at POI solutions.	To evaluate the outcome of the following: • The clarifications to be provided by the EBA Q&A tool on the different questions related to this document and its Annex 1 that have been coordinated with but entered by the MSG MSCT; • The additional services for instant SCTs that have been included in the Recommendation E in the ERPB Statement of November 2019; • The development of a recognition label as recommended in the Recommendation A in the ERPB Statement of November 2019; • The deliverables developed per Recommendation A above • The market situation in the light of other on-going initiatives with respect to the establishment of an interoperability framework for IPs at the POI. At the same time the current document would be updated as appropriate. The proposal is that this work is carried out by a group with a similar composition as the present WG, depending on the outcome of the deliverables mentioned above and the market situation in June 2021.	June 2021 till November 2021

Table 23: Recommendations for interoperability of IPs at POI

Annex 1 – PISP-based models

Payment Initiation Service Providers (PISPs) as specified in the PSD2 and the RTS could be involved to facilitate IP at POI payments. According to Article 94.2 of PSD2 [2], a PISP could be involved between the PSU and their ASPSP *but they shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.*

This annex analyses models for IPs at the POI involving a PISP, impacting the interoperability of IPs at the POI. Hereby, as before in the document, a distinction will be made between IPs based on merchant-presented data and IPs based on consumer-presented data.

1. IPs based on merchant-presented data

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

- *Case 1:* The PISP is the consumer's IP service provider and the consumer has a dedicated IP 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's IP service provider. The consumer has no dedicated IP 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 takes place. On this webpage the consumer confirms or selects a PISP and provides their consumer identification data.

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

Case 1 – PISP is consumer's IP service provider

This model is represented in the figure below.

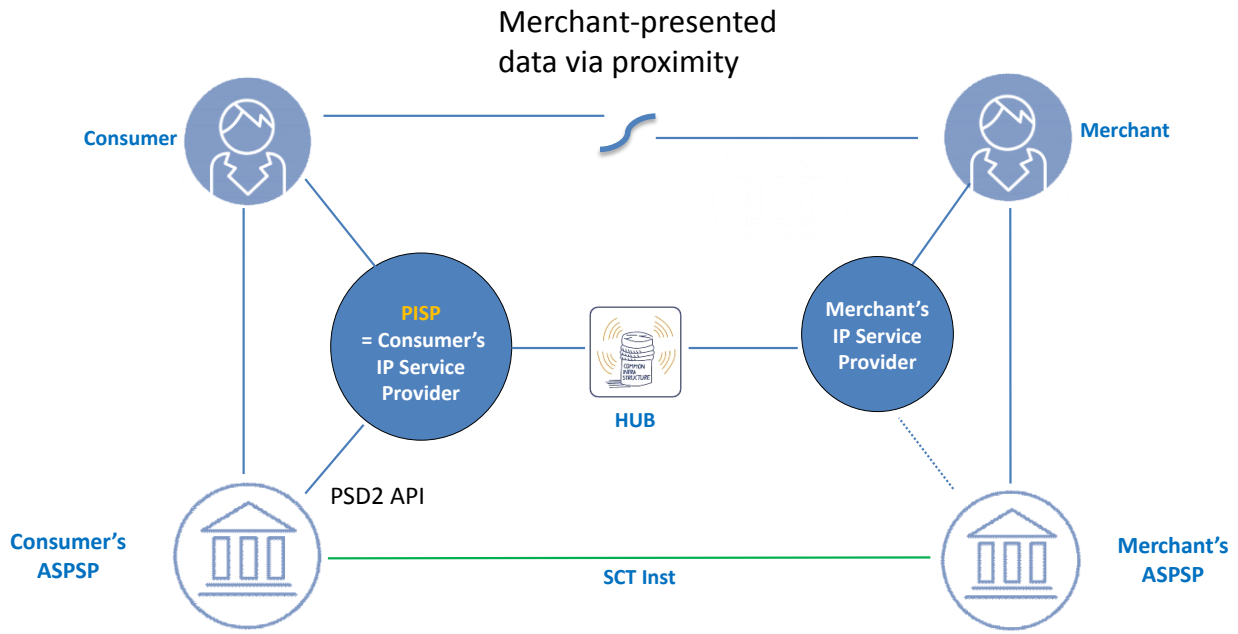


Figure 13: Model for IP based on merchant-presented data whereby PISP is consumer IP service provider

In this model, the consumer has on-boarded with the PISP and downloaded an IP application on their mobile device, hereby providing the necessary consents with respect to the PISP according to PSD2 (Arts. 51 through 58, 64, 66 and 94) and RTS (Art. 30)[56]. The technical interoperability requirements specified in Table 6 apply for the PISP as IP service provider of the consumer. Note also 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 measures (see chapter 10).

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 IP

56

service provider) about the successful/unsuccessful transaction (see Table 6) in support of the notifications to the consumer and the merchant (see section 8.3.4).

Case 2 – PISP is merchant IP service provider

This model is represented in the figure below.

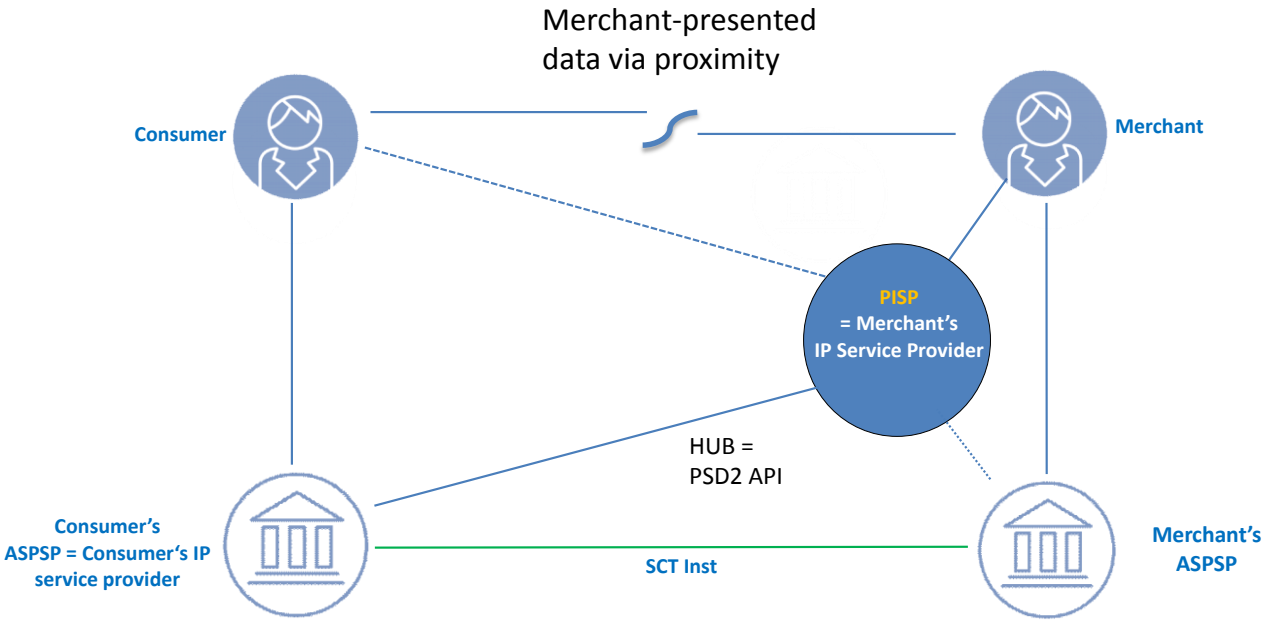


Figure 14: Model for IP based on merchant-presented data whereby PISP is merchant IP service provider

In this model, it is assumed that the consumer's ASPSP is their IP service provider while a PISP is involved on the merchant side as the merchant IP service provider. The merchant-presented data provided to the consumer at the POI (e.g. via a QR-code) is read by a generic QR-code reader on the consumer device and re-directs the consumer to a merchant webpage. To proceed with the payment, the consumer confirms the PISP or is invited to select a PISP hereby giving the appropriate consents to the PISP for the initiation of the IP according to PSD2 (Arts. 44, 45, 64, 66 and 94) and

RTS (Art. 30)[57]. The consumer should subsequently provide their CustomerID and IBAN to the PISP i-frame to enable the PISP the initiation of the IP via the PSD2 API[58].

Since the PISP is the IP service provider of the merchant, the interoperability requirements of Table 7 apply as the transaction data available to the PISP would be the same as in case of an IP based on consumer-presented data. However, the functional requirements for the HUB as listed in Table 7 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 IP service provider) to the PISP (= merchant IP service provider) about the successful/unsuccessful transaction (see Table 7) in support of the notification to the merchant (see section 8.3.4).
- Consumer consents with respect to usage of the PISP (= merchant IP service provider) subject to EBA clarifications ((Arts. 44, 45, 51 through 58, 64, 66 and 94) and RTS (Art. 30)).
- Consumer and merchant experience.

2. IPs based on consumer-presented data

For IPs based on consumer-presented data, a PISP could be involved as an IP service provider to the merchant to facilitate an IP. Hereby there will be a dedicated agreement between the merchant and the PISP.

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

[57] Subject to further clarifications to be provided by the EBA on the following four questions: EBA Q&A 2020_5570 to 5573.
[58] 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.

the merchant IP service provider = PISP for the initiation of the IP. In order to enable the PISP to use the PSD2 API for the communication with the consumer's ASPSP, the CustomerID and IBAN of the consumer should be made available "in clear" to the PISP[59].

One of the main challenges however with the involvement of a PISP on the merchant side is how the consumer can give the appropriate consents for the usage of a PISP according to the PSD2 (Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30)[60].

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

- *Case 1:* A PISP involved on the merchant side for e- and m-commerce;
- *Case 2:* A PISP involved on the merchant side for in-store payments.

Note that for the two cases above, if the PISP is at the same time also the consumer's IP service provider, which means that the consumer has on-boarded with this PISP (see also the first case in section 1 of this Annex), then the model becomes effective a 3-corder model that will not be further discussed in this annex.

An additional case could be considered whereby there is only a PISP involved on the consumer side but this case would need to be further investigated in future work.

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

[59] Note that this is pending clarifications from the EBA on the Q&A 2020_5476 and 2020_5477.
[60] Subject to further clarifications to be provided by the EBA on the following four questions: EBA Q&A 2020_5570 to 5573.

Case 1 – PISP on merchant side for e- or m-commerce

This model is represented in the figure below.

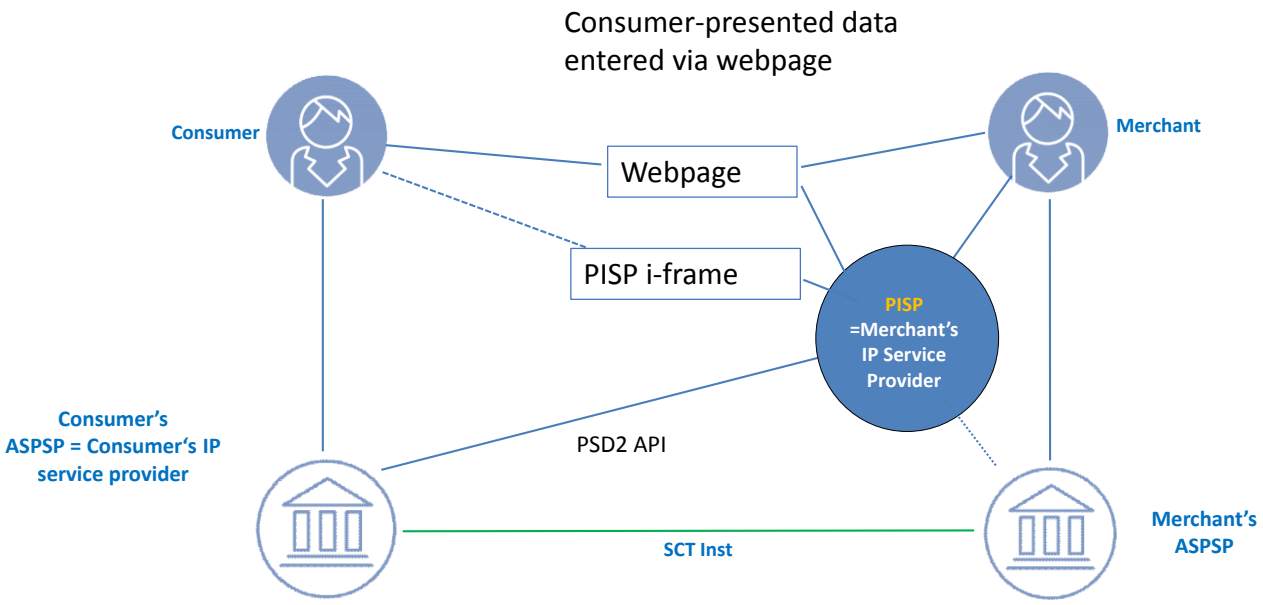


Figure 15: Model for IP based on consumer-presented data whereby PISP is merchant IP service provider / e- and m-commerce

In this model, it is assumed that the consumer's ASPSP is their IP service provider while a PISP is involved on the merchant side as the merchant IP service provider. To proceed with the payment, the consumer is invited to confirm or select a PISP on the merchant's webpage, hereby able to access the appropriate PISP information and giving the appropriate request and consents to the PISP for the initiation of the IP according to PSD2 (Arts. 44, 45, 64, 66 and 94)[61], by providing their CustomerID and IBAN[62] to the PISP i-frame to enable the PISP the initiation of the IP via the PSD2 API to the consumer's ASPSP[63].

[61] Subject to further clarifications to be provided by the EBA on the following four questions: EBA Q&A 2020_5570 to 2020_5573).
[62] Note that this is pending clarifications from the EBA on the Q&A 2020_5476 and 2020_5477.
[63] 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.

Since the PISP is the IP service provider of the merchant, the interoperability requirements of Table 7 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 IP service provider) to the PISP (= merchant IP service provider) about the successful/unsuccessful transaction (see Table 7) in support of the notification to the merchant (see section 8.3.4).
- Protection of CustomerID and IBAN subject to EBA clarifications.
- Consumer consents with respect to usage of the PISP (= merchant IP service provider) subject to EBA clarifications ((Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30)).

Case 2 – PISP on merchant side for in-store

This model is represented in the figure below.

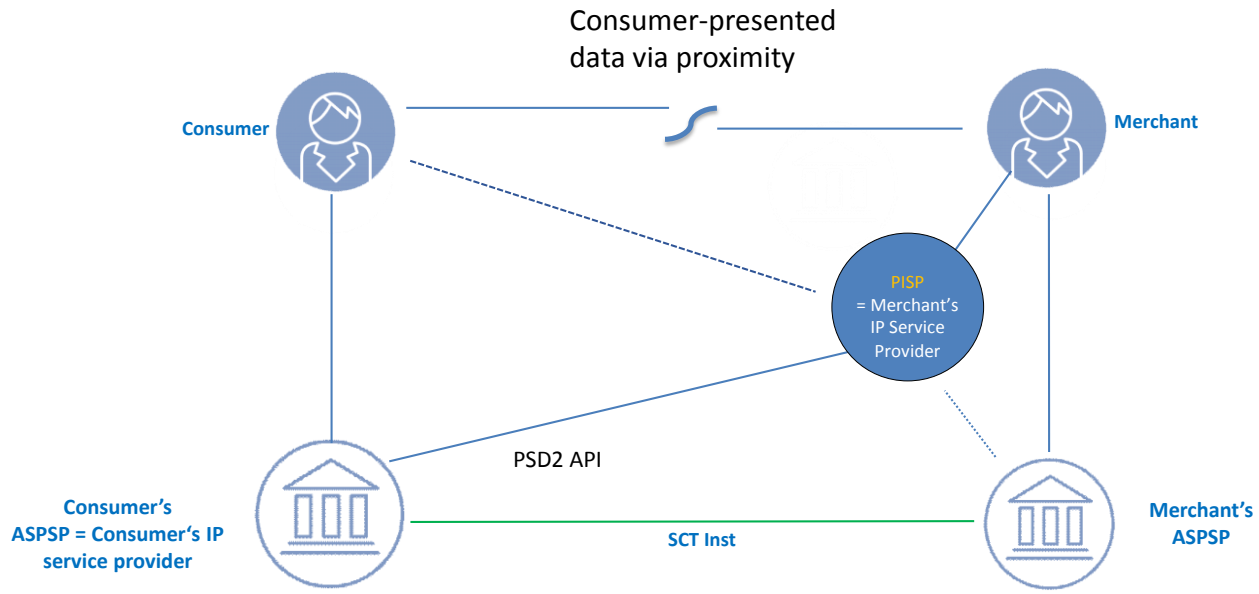


Figure 16: Model for IP based on consumer-presented data whereby PISP is merchant IP service provider / in-store

In this model, it is assumed that the consumer's ASPSP is their IP service provider while a PISP is involved on the merchant side as the merchant IP 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 consents via the merchant on the usage of a PISP for the initiation of the IP according to PSD2 (Arts. 44, 45, 64, 66 and 94)[64]. Moreover, it is hereby assumed that the consumer identification data, i.e. CustomerID and IBAN are provided "in clear"[65] to enable the PISP to use the PSD 2 API for the communication to the consumer's ASPSP.

Since the PISP is the IP service provider of the merchant, the interoperability requirements of Table 7 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 IP service provider) to the PISP (= merchant IP service provider) about the successful/unsuccessful transaction (see Table 7) in support of the notification to the merchant (see section 8.3.4).
- Protection of CustomerID and IBAN subject to EBA clarifications.
- Consumer consent with respect to usage of the PISP subject to EBA clarifications (PSD2 (Arts. 44, 45, 64, 66 and 94) and RTS (Art. 30)).

[64] Subject to further clarifications to be provided by the EBA on the following four questions: EBA Q&A 2020_5570 to 2020_5573).
[65] Note that this is pending clarifications from the EBA on the Q&A 2020_5476 and 2020_5477.

Annex 2 – Models involving a CPSP

This annex analyses models for IPs at POI involving *a Collecting Payment Service Provider* (CPSP) on the merchant side which acts as a collector of payment transactions on behalf of the merchant (the ultimate beneficiary) and their impact on the interoperability of IPs at the POI. This CPSP has their own ASPSP.

The model is represented in the figure below.

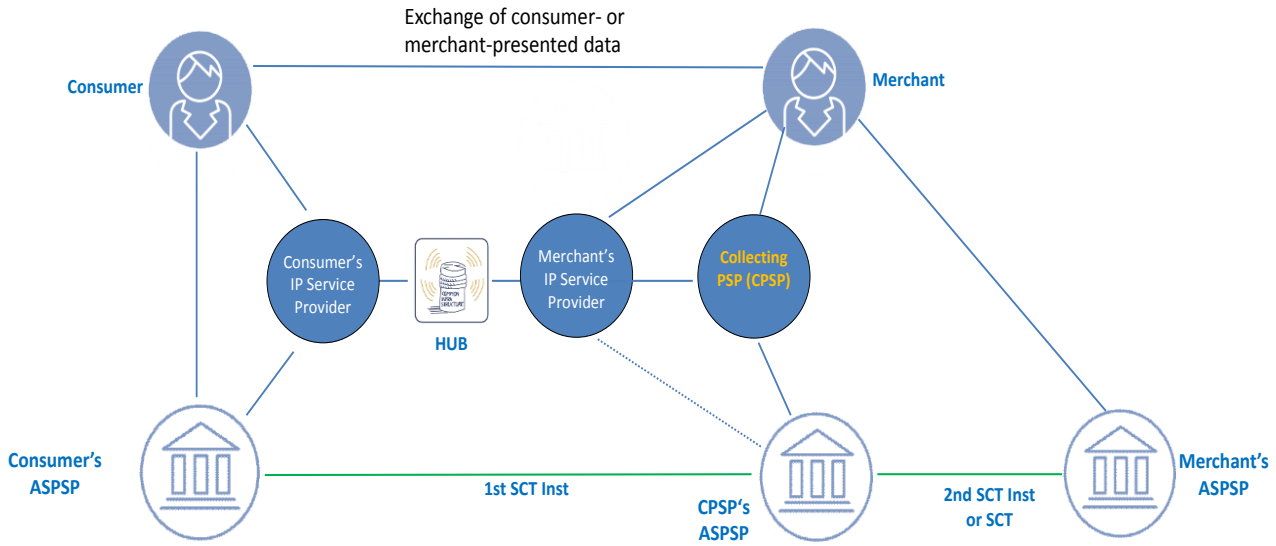


Figure 17: Model involving a CPSP

In this model, the transaction at the POI is an IP from the consumer to the CPSP (as the beneficiary), followed by a second payment, either an SCT Inst or an SCT from the CPSP (the originator) to the merchant. The merchant needs to have contracts with both the CPSP and their ASPSP. After the first SCT Inst payment, which is to be considered as an IP at POI transaction, the merchant shall be informed about the execution by the merchant IP service provider (via the notification message, see section 8.3.4) so that the goods or services can be released. The consumer shall be duly informed

that the IP is conducted to a CPSP which also will impact, if performed, the SCA with dynamic linking. However the consumer shall also be informed that this CPSP is related to the merchant[66] .

From a technical interoperability perspective, the interoperability requirements specified in Table 6, in case of merchant-presented data, and in Table 7, in case of consumer-presented data apply. The subsequent interactions related to the second (instant) credit transfer from the CPSP to the merchant are to follow the respective Instant SCT or SCT scheme rulebooks but fall outside the scope of the ERPB WG since this payment is not an IP at POI transaction.

Furthermore it is to be noted that different implementations may exist, e.g., the IP service provider on the merchant side could be the CPSP IP service provider. The flows of the notification message to the merchant (see section 8.3.4) may depend on the actual implementation model and will need to be further analysed in future work.

[66] This relates to the scope of the ERPB WG on Transparency for retail payments end-users (see https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/13th-ERPB-meeting/Statement_of_13th_ERPB_%20meeting.pdf).

Annex 3 - ERPB WG mandate

EUROPEAN CENTRAL BANK
EUROSYSTEM

ERPB Secretariat

February 2020
ERPB/2020/001

MANDATE OF THE WORKING GROUP
ON A FRAMEWORK FOR INSTANT PAYMENTS AT THE POINT-OF-INTERACTION

Based on Article 8 of the mandate of the Euro Retail Payments Board (ERPB), a working group is set up with the participation of relevant stakeholders to develop principles for an interoperability framework for instant payments at the point-of-interaction (POI), to foster the development of pan-European instant payment services for this use case.

Scope

Following up on the report from the previous ERPB working group on instant payments at the POI, the new working group is expected to focus its work on a subset of the recommendations endorsed by the ERPB at its November 2019 meeting, i.e. those related to the development of a framework to manage the interoperability rules and appropriate governance for solutions enabling instant payments at the POI[1]. It is acknowledged that the European Payments Council (EPC)'s multi-stakeholder group on mobile-initiated SEPA Credit Transfers (MSG MSCT) is expected to carry out follow-up work on technical and other issues that should serve as input for the above mentioned framework[2]. The working group is therefore expected to liaise with the MSG MSCT, in particular regarding these aspects. The working group is furthermore expected to liaise with the European Cards Stakeholders Group regarding issues with an impact on card-based payments[3], with relevant initiatives towards pan-European POI payments on issues of common interest and, where relevant and possible, with the other addressees of the ERPB recommendations related to instant payments at the point-of-interaction[4].

[1] Recommendations A (first point), B and D attached to the ERPB Statement following its November 2019 meeting.

[2] I.e. to develop 1) a pan-European label and its usage for instant payments at the POI solutions and 2) functional and security specifications for interconnectivity of such solutions, including the specification of the minimal data set to be exchanged between consumer and merchant while covering different proximity technologies. See recommendations A (second point) and C attached to the ERPB Statement following its November 2019 meeting.

[3] In particular those related to the consumer's choice of a given payment instrument to conduct a payment transaction

at the POI. See recommendation D attached to the ERPB Statement following its November 2019 meeting.

[4] I.e. recommendations E, F, G, H, I and J attached to the ERPB Statement following its November 2019 meeting.

Deliverables

The working group is expected to deliver principles for a dedicated interoperability framework for instant payments at the POI, covering:

1. Common rules and procedures;
2. Appropriate governance;
3. Security requirements for payment service user onboarding processes to be adopted by instant payment service providers and merchants;
4. Appropriate specifications to enable consumer selection of preferred payment instrument to conduct a transaction at the POI.

Considering the evolving market situation, the working group is also expected to review the stocktake of existing and planned end-user solutions for instant payments at the POI carried out by the ERPB working group on instant payments at the POI. In particular, the working group is expected to: i) update the information for the reported solutions and ii) add any relevant solutions that were not reported in the previous stocktake. The outcome of this reviewed stocktake should be taken into account, where relevant, in the work on the other deliverables.

Time horizon

The working group will be established by the end of February 2020 and shall deliver, by June 2020, an interim report covering the updated stocktake, the principles for a dedicated interoperability framework related to common rules and procedures and appropriate governance, as well as a status update on the other deliverables. The ERPB shall confirm the next steps on the basis of this interim report. The working group shall then complete its deliverables by November 2020.

Participants and chairmanship

The working group shall include relevant stakeholders, including representatives of ERPB member and guest associations. Other relevant stakeholders may also be invited to join as relevant third parties. One representative of the ECB and a limited number of representatives of euro area NCBs are invited to join the working group as active participants. A representative of the EU Commission will be invited as observer. The working group will be co-chaired by EuroCommerce (demand side) and European Payments Council (supply side). The Secretariat will be provided by the European Payments Council.

Members representing their associations and the co-chairs will be appointed by the ERPB Chair based on suggestions from their respective associations. Other participants – after expressing interest to the ERPB secretariat – may be invited by the ERPB Chair to join the group based on consultation with the members of the ERPB.

Rules of procedure

The mandate of the ERPB defines a broad set of rules for the procedures of its working groups: the working group takes positions on a ¾ majority basis; dissenting opinions are mentioned in any relevant documents prepared by the working group. The members of the group decide on how to organise timing and rules of meetings and communication via written procedure, as well as on the need and format of any interim working documentation produced. Costs related to the operation, meetings, chairmanship and secretariat are carried by the members of the group themselves.

Annex 4 - ERPB WG composition

Name	Surname	Nominating Institution
Co-Chairs		
Dag-Inge	Flatraaker	EPC
Michel	Van Mello	EuroCommerce
ERPB Stakeholders		
Jean	Allix	BEUC
Massimo	Battistella	EACT
Gerhard	Huemer	SMEs United
Pascal *alternate:* Alexandre	Spittler Leclerc	EuroCommerce
Matthias *alternate:* Michael	Lange Knetsch	EPC
Rita *alternate:* Anni	Camporeale Mykkänen	EBF
Didier	Darmouni	EACB
Ignacio *alternate:* Robert	Mascarell Renskers	ESBG
Ruth *alternate:* Dimitrios	Mitchell Markakis	EMA
Regis	Massicard	EPIF
Guest organisation		
Ralf *alternates:* Jörn-Jakob Fanny Carlos	Ohlhausen Röber Rodriguez Blanco	ETPPA ETPPA ETPPA ETPPA
NCBs		
Alexandra	Madeline	France
David	Ballaschk	Germany
Rauno	Veske	Estonia
Rui	Pimentel	Portugal
Marían Ángeles	Moreno Cordero	Spain
ECB		
Mirjam	Plooij	ECB
Observer		
Roxane	Romme	

Katarzyna *alternate:* Nicolò	Kobylinska–Hilliard Brignoli	European Commission
Secretariat		
Marijke	De Soete	EPC

Table 24: Composition ERPB WG

Annex 5 – Joint Task Force ERPB WG / MSG MSCT composition

Name	Surname	Nominating Institution
Co-Chairs		
Pascal	Spittler	EuroCommerce (MSG MSCT)
Dag-Inge	Flatraaker	EPC (ERPB WG)
ERPB WG members		
Jean	Allix	BEUC
Ruth	Mitchell	EMA
Emiliano	Anzellotti	EBF (ABI Lab)
MSG MSCT members		
Axel	Schaefer	EuroCommerce (Ikea)
Philippe	Evenot	EPC (La Banque Postale)
Andrea	Cogerino	EPC (ABI- Intesa)
Arie	Schilp	EPC (Rabobank)
Guido	Hogen	Smart Payment Association (Thales)
Andrew *alternate:* Dmitry	Pankratov Yatskaer	OpenWay
Ralf	Ohlhausen	ETPPA (PPRO and Tink)
Magnus *alternate:* Harri	Lageson Giotakis	getswish
Secretariat		
Marijke	De Soete	EPC

Table 25: Composition Joint Task Force ERPB WG/MSG MSCT