

SEPA PAYMENT~~CARDS~~ STANDARDISATION (SPCS) “VOLUME”  
STANDARDS’ REQUIREMENTS

# BOOK 7

PAYMENT~~CARDS~~ PROCESSING FRAMEWORK

*Payments and Cash Withdrawals ~~with Cards~~ in SEPA  
Applicable Standards and Conformance Processes*

© European Payments~~Cards~~ Stakeholders Group AISBL.  
Any and all rights are the exclusive property of  
EUROPEAN CARDS~~PAYMENTS~~ STAKEHOLDERS GROUP AISBL.

Abstract	This document contains the work on SEPA <del>cards—</del> <u>payment</u> standardisation to date
Document Reference	EPSG001-18
Issue	Book 7 – v10.5
Date of Version	27.11.2025
Reason for Issue	Public consultation
Reviewed by	EPSG Board – 25 November 2025
Produced by	EPSG Book 7 Expert Team
Owned and Authorised by	EPSG
Circulation	Public (draft for consultation release)

Change History of Book 7		
7.7.1.0x	2014-2015	Working version 2014-2015
7.7.1.05	11.02.2015 (published 10.03.2015)	Consultation version 2015. First release of Book.
7.7.1.1	08.12.2015	EPC Published version – Volume v7.1
7.7.1.11- 7.7.1.9	16.12.2015	Working Version 2015-2016
8.7.00	01.03.2017	ECSG Published version - Volume v8.0
8.7.40	07.11.2018	Board Approval version for Consultation as 8.5
8.7.50	17.12.2018	Public Consultation Release v8.5
8.8	19.07.2019	Working Version to V9
9.0	15.01.2020	ECSG Published Version - Volume 9.0
9.0	December 2021	Public Consultation Release v9.5
10.0	01.10.2022	ECSG Published Version – Volume 10.0
<a href="#">10.01- 10.12</a>	<a href="#">2023-2025</a>	<a href="#">Working Versions towards v10.5</a>
<a href="#">10.5</a>	<a href="#">27.11.2025</a> <small>(published in December 2025)</small>	<a href="#">Public Consultation Release 10.5</a>

## Table of Contents

<b>1</b>	<b>GENERAL.....</b>	<b>5</b>
1.1	Book 7 - Executive summary .....	5
1.1.1	Purpose of this document.....	5
1.1.2	Structure of this book .....	5
1.2	Description of changes since the last version of Book 7.....	7
<b>2</b>	<b>CARDS FRAMEWORK.....</b>	<b>8</b>
2.1	Cards Processing Framework .....	8
2.1.1	Introduction .....	8
2.1.2	Context and Environment .....	8
2.2	Business Objectives .....	13
2.2.1	Business Principles and Requirements per domain.....	14
2.2.2	Common business principles and requirements to all domains..... <b>Error! Bookmark not defined.</b>	
<b>3</b>	<b>INSTANT CREDIT TRANSFER (ICT) TRANSACTION FRAMEWORK.....</b>	<b>26</b>
3.1	Introduction: various ICT Transaction models .....	26
3.2	Open Banking-based model: PSD2 variant .....	27
3.2.1	Business requirements for the acceptance/merchant domain .....	27
3.2.2	Business requirements for the PISP .....	28
3.2.3	Business requirements for the Customer's ASPSP .....	28
3.3	Open banking-based model: Open banking scheme variant.....	30
3.4	PSP Scheme-based model: single scheme variant .....	31
3.4.1	Business requirements for the Acceptance Domain .....	31
3.4.2	Business requirements for the Acceptor PSP Domain .....	32
3.4.3	Business requirements for the Inter-PSP Domain .....	33
3.4.4	Business requirements for the Customer PSP Domain.....	33
3.5	PSP scheme-based model: Interoperability variant.....	33
<b>4</b>	<b>TABLE OF FIGURES .....</b>	<b>34</b>



## 1 GENERAL

### 1.1 Book 7 - Executive summary

#### 1.1.1 Purpose of this document

This book defines business principles and requirements for market access and participation in card payment domain services, with the main objective of facilitating an open and transparent market.

This objective is expressed depending on the Payment Instrument:

- Payment Card: it is fully achieved with a common processing framework to the various card schemes, compliant to the Article 7 of the IFR (Interchange Fees Regulation) related to the unbundling between scheme and processing levels
- Instant Credit Transfer: The market is still evolving and we have identified the common requirements for payment initiation across both open banking and PSP schemes; these should be defined in more detail in the future according to the status of the evolution. The interoperability variant of the PSP scheme is still in progress.

#### 1.1.2 Migration Roadmap

~~A migration roadmap will be proposed after discussion and alignment with the EPSG and will be defined later.~~

#### ~~1.1.4~~1.1.2 Structure of this book

This book contains ~~two~~three main parts; each part is related to a specific Payment Instrument with its own ecosystem and features

- Section 2: Addressing the Cards Framework, covering the following aspects:
  - i. Description of existing Cards Processing Framework
    - ⊖ Business objectives expected via the production of this Book of the ~~SCS~~SPS Volume
  - ii.
  - iii. Business Principles applying to the different parts of the card payment value chain (e.g., Scheme, Acquirer/processor, Issuer/processor) aiming to achieve the defined business objectives;

~~1. Description of existing Cards Processing Framework~~

~~2. Business objectives expected via the production of this Book of the ~~SCS~~ Volume~~

~~Business Principles applying to the different parts of the card payment value chain (e.g., Scheme, Acquirer/processor, Issuer/processor) aiming to achieve the defined business objectives~~

Section 3: Addressing Instant Credit Transfer Transactions.



## 1.2 **Description of changes since the last version of Book 7**

This version of Book 7 is new from the v10. It includes the following updates:

- A new version of the diagram of the ecosystem (section 2.2 context and environment)
- The addition of the Acceptance Processing
- A figure about the juxtaposition of both environments: SRC (or Click-to-Pay) and card payment (execution) following the last SRC Task Force of the ECSG
- Integration of Business Requirements related to EMV tokens coming from the Tokenisation Annex
- A Requirement about the GDPR compliance for Joint Data Controller between Scheme and the PSP member
- Recommendations from the ERPB on enhanced transparency of beneficiary information for retail payment end-users and compliance with the European Accessibility Act [EAA].
- The inclusion of the first models of Instant Credit Transfer Transactions related to the Open Banking-based (PSD2) and the single scheme variant of PSP-Scheme based

## 2 CARDS ~~PROCESSING~~ FRAMEWORK

### 2.1 Cards Processing Framework

#### 1

#### 1.32.1.1 Introduction

The market model described is the traditional four party ~~card-S~~ scheme, where

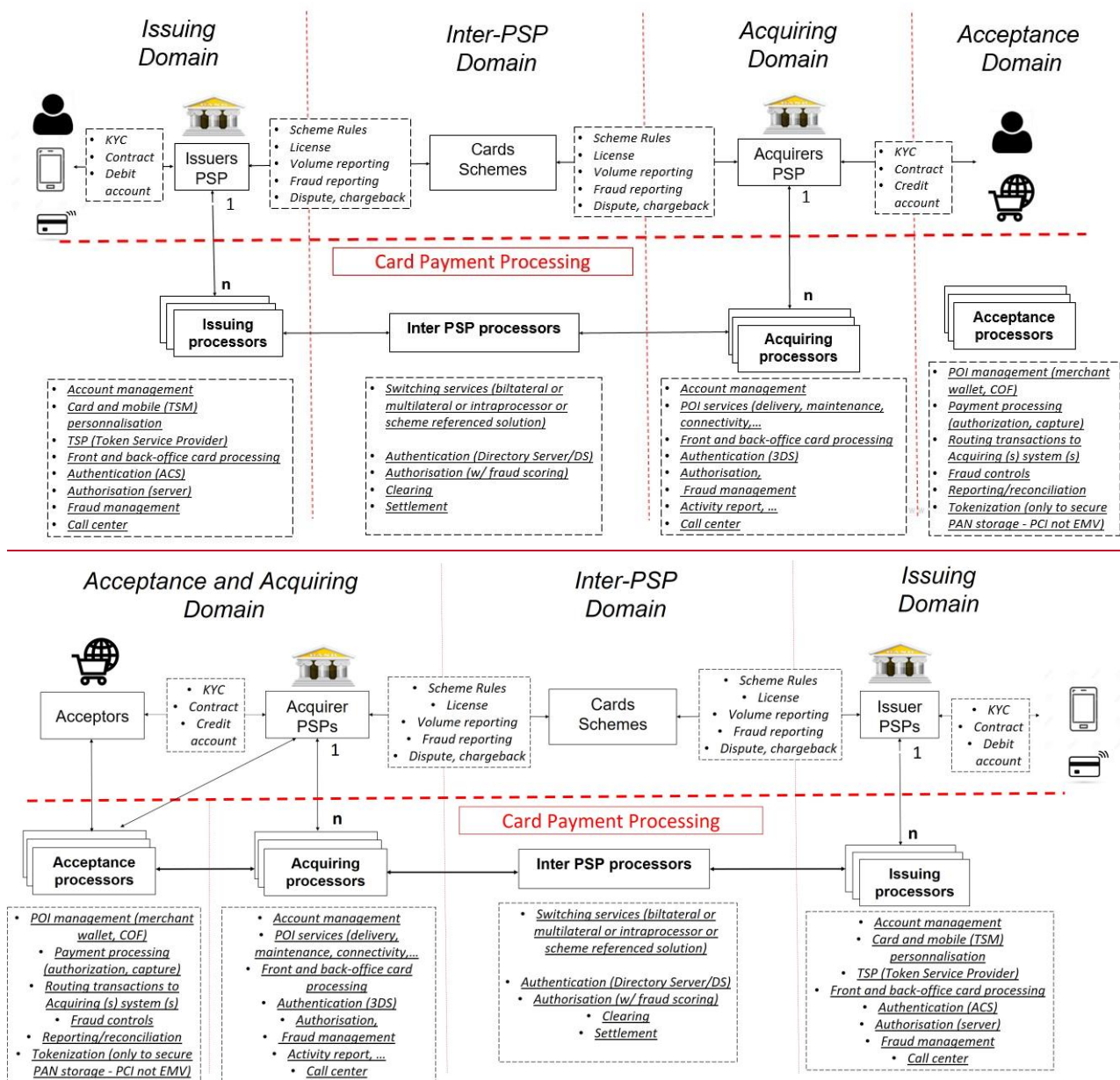
- Acceptor has contractual relationship with Acquirer;
- ~~Cardholder~~Customer has contractual relationship with Issuer;
- Acquirer and Issuer interact for authorisation, clearing and financial settlement of transaction.

The Cards Processing Framework should apply to all SEPA ~~card-scheme~~Schemes, however the three party ~~card-scheme~~Scheme model is not covered in this version.

#### 1.42.1.2 Context and Environment

The diagram below depicts main actors and services of the four party ~~card-scheme~~Scheme.





**Figure 1:** The main actors and services of the four party ~~card-scheme~~ Scheme

In some cases, the Acceptance and the Acquiring Domain are managed by two different actors, while in some other cases the Acquirer will manage all or part of the Acceptance functions. This model applies to card based payment transactions, on ATM, physical POI, remote payment environment (PC, mobile device), in other words any medium that allows the initiation of a Card based transaction.

Service providers may provide one or several services in one or several domains; type of services are defined within contractual agreements between Acceptors / Acquirers / Issuers and their service providers.

#### 1.4.12.1.2.1 Schemes play an important role

~~Card Payment~~ Schemes are key players; they define for each of their ~~card brands~~ Payment Brands the rules (business, functional, security, procedural) governing the use and deployment of the products and services associated with those Payment ~~b~~ Brands and, through oversight requirements, they bear responsibility for operational reliability (business continuity), security levels and commercial accountability (financial liabilities and risks).

Acquirers and Issuers are Scheme Participants. They sign Licence Agreements with the Scheme, follow the Scheme rules and implement the mandatory services, such as Volume reporting, Fraud reporting, Dispute and Chargeback procedures. In most cases, Acquirers and Issuers support several ~~card Payment~~ b Brands potentially from several ~~Card Payment~~ Schemes.

Processors provide services to Scheme Participants for the acquiring of transactions and/or issuing of payment applications for one or several ~~Card~~ Payment Brands for one or several ~~Card Payment~~ Schemes. For the sake of clarity, an Acquirer or an Issuer may be its own processor for some or all services (or may subcontract those services to an external supplier).

#### 1.4.22.1.2.2 ~~Three~~ Four main domains

~~Three~~ Four domains are identified in the cards processing landscape:

- Acceptance domain: service provided to Merchants or Acceptors
- Acquiring domain: services provided to Acquirers and their merchant customers for acceptance of transactions (acquiring domain also covers merchant acceptance)
- Issuing domain: services provided to Issuers and their ~~cardholder~~ Customers for issuance of card payment products
- Inter-PSP domain (also called inter-bank domain): services allowing Acquirer Processors to interact with Issuing Processors for the execution of the transactions

In each domain, the services are quite broad and can be provided by several suppliers. Scheme Participants (e.g., Acquirers, Issuers) may use services from different processors, some being more specialized in some activities. For instance, services related to delivery of POI and services related to provisioning of a payment application on a Secure Element of a mobile device are quite specific, independent and in general provided by different suppliers.

#### 1.4.32.1.2.3 Several solutions possible in the 'inter-PSP' domain

The 'inter-PSP' domain covers the interactions between Acquirer (Processors) and Issuers (Processors) and ensures the full reachability of any issuer by any acquirer for a specific scheme:

- An acquirer must be able to reach any issuer

- An issuer must be reachable by all acquirers.

For the Authorisation, Clearing and Settlement services, several solutions are operational on the market

- Bilateral agreements between one acquirer and one issuer for the use of a specific solution
- Multilateral agreements between several acquirers and several issuers to use a common solution, either based on a common interface standard and several connections between each party or via connection to a central switch
- Intraprocessor solution provided by one processor (acting as acquirer and issuer processor) for its acquirer and issuer customers
- Scheme default solution referenced by Scheme (e.g., central solution, multilateral solution)

The current market situation already illustrates the fact that a Scheme may not impose the sole use of its Scheme default Inter-PSP solution. The different solutions may use different technical standards and implementations provided they are compliant with the Scheme rules, which is also in line with the standardisation and conformance ecosystem defined within the Volume.

#### 1.4.42.1.2.4 Some services are ~~s~~Scheme/~~Payment B~~Brand specific, others are generic

Many services supported by Scheme Participants and/or their Processors are not scheme dependent; the services are generally performed in a similar manner regardless of the scheme. Examples of these services include but are not limited to:

- Acceptor payment, reporting, contracting, invoicing
- POI acceptance (e.g., POI to Acquiring processor protocol, acquiring processing)
- Card processing (e.g., EMV processing)
- Financial part of the authorisation process (rather specific per card product type, e.g., a 'pay before', a 'pay now' or a 'pay later' product, than typically per ~~Payment B~~Brand)

Other services are '~~S~~scheme/~~Payment B~~Brand dependent', mainly for interactions with the Payment Schemes. Examples of such Scheme/~~Payment B~~Brand dependent services usually include but are not limited to:

- Interface with the Scheme default ~~Payment B~~Brand reachability solution (Switch, Clearing & Settlement for interaction between acquirer and issuer, Directory for remote transactions ...) are currently specific per scheme. However, ~~S~~scheme/~~Payment B~~Brand independent Implementation Specifications can already be used provided they take into consideration the scheme governed specific business rules (e.g., real time clearing mandated versus batch clearing).
- Scheme reporting (e.g., volume of transactions, number of cards)

- Fraud reporting (e.g., information on cases of frauds encountered)
- Dispute management, chargeback processes (between Acquirer and Issuer)

Some Scheme rules can be specific per payment scheme, for instance the concept of on-line clearing rather than batch clearing, the support of specific transactions types which are mostly optional.

In the context of emerging products and services, e.g., wallets, mobile payments, it is expected that in the initial phases specific products and services will be developed with non-standard features. These products and services would ideally be aligned to SEPA-wide (scheme independent) standards once the [ESG](#), through its own process, has determined that they are sufficiently mature to be included in the Volume.

#### 1.4.52.1.2.5 *SPS Volume aims to ease deployment of [Payment Brand/Scheme independent standards](#)*

The Standardisation ecosystem is described in Book 5, with some key principles, such as:

- Several Implementation Specifications per domain of value chain (e.g., POI-acquirer part), with some exceptions, e.g., EMV for card-POI part
- Role of Specification Provider highlighted – independently of Scheme related bodies
- Optional Labelling process to demonstrate conformance of the Implementation Standard with the Volume (requirements and governance)
- Schemes to make public the list of Implementation Specifications they support (transparency objective)
- Approval process by Schemes of products certified by Specification Providers

The combination of those principles with the fact that several [card-Payment Sservices](#) are similar for different [Sschemes](#) (same functional and security requirements) will ease the development of [brandPayment Brand/Ss](#)cheme independent Implementation Specifications by Specification Providers which may be independent of Scheme organisations.

### 2.1.2.6 The SRC (Secure Remote Commerce) or Click-to-Pay ecosystem

The juxtaposition of the SRC environment (ie the check-out process) with the current Payment one (ie payment execution process) is as follows:

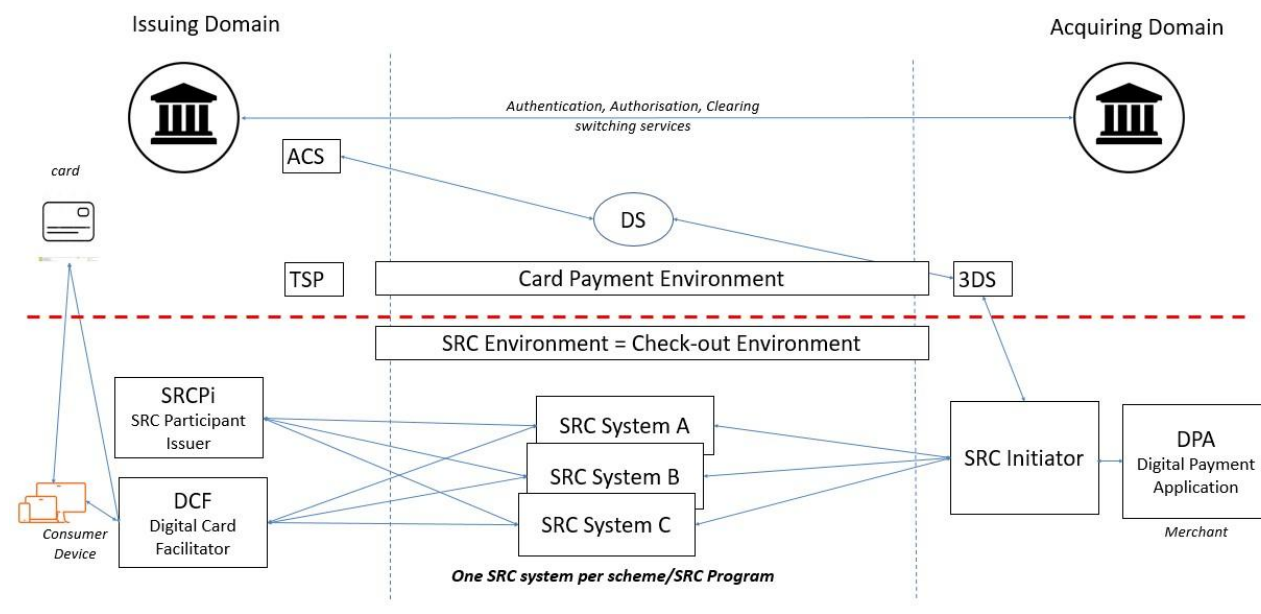


Figure 2: The card payment ecosystem including SRC

## 22.2 Business Objectives

The Standardisation and conformance ecosystem developed by [CSG-EPSG](#) within this [SPS](#) Volume aims to ease the development of 'Payment [b](#)Brand independent' Implementation Specifications (e.g., EMV, POI-acquirer protocol ...) and solutions for the benefit of all stakeholders.

The description of the context and environment highlights some key characteristics of [card](#) [Payment](#) [S](#)ervices:

- Clear separation of roles between the actors : schemes, acquirers, issuers, processors

Several services by different suppliers for one acquirer/issuer illustrate that competition already exists

- Most services are 'Payment [b](#)Brand independent' and instead are specific to the card product type
- Cooperation already exists, as demonstrated by the use of common technical and security standards (e.g., EMV, 3D Secure for remote payment) in a competitive context (e.g., specific scheme rules).

In addition to the books related to requirements (functional, security) and the conformance verification process, this book defines additional business principles and requirements for market access and participation with the main objective of further facilitating an **open and transparent market**, which

- maintains competition
- improves efficiency
- fosters interoperability

and are based on scheme independent standards developed by Specification Providers in cooperation with relevant actors in the cards' payment landscape (e.g., schemes, processors, vendors ...).

Those additional business principles and requirements can be considered as the 'Cards Processing Framework'.

#### **2.12.2.1 Business Principles and Requirements per domain**

In this section, Business Principles and Requirements refer to the business dimensions that apply to the actors of the card payment value chain with the objectives mentioned above.

##### **2.1.12.2.1.1 Schemes**

- Req S1: Schemes shall not discriminate among Acquirers and Issuers for licensing their products provided the parties meet the Scheme requirements to get a Scheme license.
- Req S2: Schemes shall make available without discrimination and at the same time, to their Participants (Acquirer, Issuer) and their Processors, the applicable scheme rules and specific information, (e.g., BIN tables, MIF rules, product rules), allowing them to setup and operate the Scheme related services according to their contractual agreement (License) with the Scheme.
- Req S3: Schemes shall ensure that their Rules are in line with the requirements of the Volume for products or services in a mature stage. If some requirements of the Volume are considered as not aligned with the latest market needs or with emerging solutions that ensure secure services, Schemes shall propose an update of the requirements of the Volume. For emerging solutions<sup>1</sup> (e.g., new wallet solutions) it is expected that a Scheme will define its own specific rules until such solutions are covered by the requirements within the [SCSSPS](#) Volume.

---

<sup>1</sup> Emerging solutions refer to new services not yet described in the [SPES](#) Volume.



Req S4: Schemes shall make publicly available the list of Implementation Specifications they support (e.g., POI application and POI to Acquirer protocol).

Req S5: In order to promote deployment of [Payment Brand](#) independent SEPA Implementation Specifications, Schemes shall not

- Impose their own Implementation Specifications as the only possible solution,
- Refuse Implementation Specifications, which have been proven to be Volume conformant, without objective reasons (e.g., specific functionality within the Scheme rules not supported by this specification),
- Impose amendments to Volume conformant Implementation Specifications.

However, as Solution Providers, Schemes may decide which Implementation Specifications they use and accept for their default scheme processing infrastructure.

Req S6: In line with the requirements outlined within Book 5, Schemes and Approval Bodies shall ensure that certified products or solutions can be submitted for Type Approval, provided that the product has implemented a listed Implementation Specification and it has been certified by an approved certification body.

Req S7: Schemes shall ensure full reachability (of all Issuers by all Acquirers) by identifying the default infrastructure components required to achieve this (e.g., Connectivity for authorisation, clearing, settlement).

Req S8: Schemes shall not provide their Participants more favourable services and terms when these Participants are using default inter-PSP processing infrastructure identified by the Scheme. For instance, ~~card-scheme~~[Schemes](#) shall not discriminate when pricing services or charging fees, between banks and payment institutions who use additional services offered by the said ~~card-scheme~~[Scheme](#) and banks and payment institutions who do not, or only partially do so.

Req S9: Schemes shall not impose a specific solution provider (e.g., processor) on their Participants. Schemes may however define minimum standards to ensure quality and scheme integrity as long as it does not create discriminatory barriers.

Req S10: Schemes shall not bundle the characteristics of their Card Products (defined in Scheme Rules) such that it requires the use of a specific processing infrastructure (e.g., supported card transaction types are independent of inter-PSP infrastructure used). For emerging solutions (e.g., new wallet solutions) to develop and promote the new service, Schemes may allow the development and operation of a dedicated infrastructure until the requirements have been described in the [SPCS](#) Volume; at which point, the principle of free choice of solution provider by Participant as defined above shall apply.

## 2.1.2.2.1.2 Acceptance, Acquiring and relative processing~~Acquirer and acquirer processing~~

The acceptance function can be done by the Acceptor or the Acquirer. The Acceptance processor is subject to the same requirements as the Acquirer for the function they perform.

- Req A1: Acquirers, who are working with several Payment Bbrands, shall not restrict Acceptors from choosing the Payment bbrands they want to accept.
- Req A2: Acquirers shall not prevent Acceptors from choosing their acquirer for each Payment bbrand, so that Acceptors shall be free to choose. However, Acceptors may be subject to risk assessment and certification by the acquirer.
- Req A3: Acquirers shall not discriminate amongst POI vendors or POI and Acceptance host solution providers, chosen by their Acceptors, provided those parties meet the acquirer's technical and security requirements and support the Acquirer's protocol.
- Req A4: Acquirers shall be able to choose which schemes they want to acquire. The scheme shall not discriminate among acquirers in relation to participation in the scheme. However, Acquirers may be subject to risk assessment and certification by the scheme.
- Req A5: Acquirers shall follow Scheme rules as stated in their licence agreement. Acquirers are liable for the compliance of their acquirer processors. Acceptors and all the other relying parties shall collaborate with the Acquirers to make sure that those rules are followed.
- Req A6: Acceptors and Acquirers shall be free to choose the processor(s) of choice for their processing services.
- Req A7: Acquirers ~~s processors~~ shall be free to choose which schemes and which related scheme services they support as per Schemes rules.
- Req A8: As provider of services to Acquirer, Acquirer processors and relying parties of the acceptors shall also follow Scheme rules. Acquirer processors and relying parties of the acceptors shall have the right to obtain scheme specific information to enable them to process scheme transactions (e.g., BIN routing information). Such necessary information could be provided by the Scheme or the Acquirer to the Acquiring processor and to relying parties of the acceptors.
- Req A9: Acquirer processors (and relying parties of the acceptors) are free to define the level of services they offer to acquirers (and their customers, the acceptors), how they implement and operate them, e.g., the interfaces between acquirer and processor.
- Req A10: Acquirer processors shall be free to choose which Inter-PSP Service Providers (Authorisation, Clearing and Settlement) solutions they use to connect to the issuers under a given scheme (with the agreement of their acquirer customers).
- Req A11: Acquirer processors and relying parties of the acceptors may be subject to certification by the Inter-PSP Service Providers to which they connect.



- Req A12: Acquirer / processor and relying parties of the acceptors may be subject to approval by the schemes (e.g., security compliance of HSM, data protection).
- Req A13: Acquirer processors and relying parties of the acceptors shall decide which Implementation Specifications they want to support, e.g., the POI-Acquirer interface, taking into consideration the customers' needs and the standards recognised by the Schemes they support.
- Req A14: Acquirer processors and relying parties of the acceptors may be subject to certification by the Specification Provider of the Implementation Specifications they use.
- Req A15: Acquirer processor may get card transactions from the POI either directly or through one or several levels of acceptance host solutions (or acceptance processor) which connect to the POI.
- Req A16: A POI or a combination of POI and acceptance host solutions (or acceptance processor) should support features which allow the Acceptor to facilitate (e.g., by configuration) the support of new card-Payment Brands and/or new Acquirers/Processors.
- It is expected that the new card-Payment Brands and/or acquirer processors implement the same Implementation Specification as the one already supported on the POI or its acceptance host (or acceptance processor).
- Req A17: POI or combination of POI and acceptance host solutions (or through an acceptance processor) may be subject to certification by the Specification Provider of the Implementation Specifications they use.

### 2.2.1.3 Issuers and issuing processing

- Req I1: Issuers shall be able to choose which schemes they want to issue. The scheme shall not discriminate between issuers in relation to participation in the scheme. However, Issuers may be subject to risk assessment and certification by the Scheme.
- Req I2: Issuers shall follow Scheme rules as stated in their licence agreement.
- Req I3: Issuers shall be free to choose the processor(s) of choice for issuing processing services.
- Req I4: Issuing processors shall be free to choose which schemes and which related scheme services they support as per Schemes rules.
- Req I5: As provider of services to Issuers, Issuing processors shall also follow Scheme rules. Issuer processors shall have the right to obtain scheme specific information to enable them to process scheme transactions (e.g., product specific requirements). Such necessary information could be provided by the Scheme or the Issuer to the Issuing processor.
- Req I6: Issuing processors are free to define the level of services they offer to issuers (and their customers, the cardholder Customers), how they implement and operate them, e.g., the interfaces between issuer and processor.

- Req I7: Issuing processors shall be free to choose which Inter-PSP Service Providers (Authorisation, Clearing and Settlement) solutions can be used to connect acquirers for a given scheme (with the agreement of their issuer customers), provided they shall ensure that they are reachable by any Acquirer processor.
- Req I8: Issuing processors may be subject to certification by the Inter-PSP Service Providers to which they connect.
- Req I9: Issuing processors may be subject to approval by the schemes (e.g., security compliance of HSM, data protection).
- Req I10: Issuing processors shall choose which Implementation Specifications they support, e.g., the Acquirer (processor)-Issuer (processor) interface (aligned with customers' needs and standards recognized by the Schemes supported).

Req I11: Like the PAN-based physical card issuing, the EMV token issuing is the responsibility of the card issuer. The processing can be either in-house or with the use of third party providers. The Token Service Provider (TSP) service is in the issuing domain. See the Tokenisation annex for more details on the functional architecture.

Req I12: Whether choosing an in-house or third party model for the TSP, it is highly important to ensure the integrity of the overall ecosystem in general and of any given Token Programme from a scheme in particular. In order to bridge these two needs, flexibility of choice for the important function of the TSP and preserving the integrity of the system, the following business principle applies: The issuer is free to select one or more approved supplier(s) for the role of Token Service Provider within any single Token Programme. The approval will be performed by a Payment System who has defined the Token Programme and will include a number of Security, Functional and Operational requirements.

Req I13: As for other processing services, these requirements must be based on the principles of:

- Competition
- Transparency
- Non-discrimination
- Efficiency
- Security

Req I14: Issuing processors may be subject to certification by the Specification Provider of the Implementation Specifications they use.

#### 2.1.42.2.1.4 Inter-PSP processing

- Req IP1 Inter-PSP service providers may propose inter-PSP services to acquirers (processors) and issuers (processors) without discrimination between those customers.
- Req IP2 Inter-PSP service providers may choose which schemes' services they process.

- Req IP3 Inter-PSP service providers may decide which level of services they deliver to their customers (e.g., transport of authorisation and/or transport of clearing data and settlement); they shall ensure that those services follow scheme rules.
- Req IP4 Inter-PSP service providers may require issuer and acquirer processors to certify their interfaces and their behaviour (e.g., connection and transaction authorisation and/or clearing files).
- Req IP5 A Processor acting as an acquirer and issuer processor may propose inter-PSP solutions to its acquirer and issuer customers (intra-processor solutions without obligation to open the service to other processors).
- Req IP6 Inter-PSP service providers may be subject to approval by the schemes (e.g., security compliance of HSM, data protection).

#### 2.1.5.2.1.5 Implementation Specifications

Note: The following principles as defined in Book 5 are highlighted here with the objective of fostering the continuation of an open market.

The standardisation and conformance ecosystem described in the [SCSSPS](#) Volume envisage the existence of several Implementation Specifications for each part of the card payment value chain, with some exceptions, such as for the contact card-POI interface (EMV).

Migration/Convergence to a smaller set of Implementation Specifications per domain of the card payment value chain will be market driven.

- Req IS1: The Specification Providers are responsible to develop the Implementation Specifications (e.g., description of functionalities, interfaces, protocols), to ensure Products implementing those Implementation Specifications may be certified, and once certified can be smoothly deployed in the field (e.g., solving potential interoperability issues between parties implementing the same implementation standard).
- Req IS2: Specification Providers shall ensure their Implementation Standard and their Governance is conformant with the requirements of the [SCSSPS](#) Volume.
- Req IS3: Specification Providers shall make the Implementation Specifications available to the Service Providers candidates to implement them, without discrimination and at the same time.
- Req IS4: Specification Providers and Certification Bodies involved in the certification processes shall not discriminate between Service Providers applying for certification.

## **2.2 — Business principles related to the EMV tokens**

~~Card issuers may want to be a Token Service provider (TSP). Alternatively, it may also happen that card issuers want to use third party providers to perform tokenisation services.~~

~~While recognising those cases, it is equally important to ensure the integrity of the overall ecosystem in general and of any given Token Programme in particular.~~

~~In order to bridge these two needs, flexibility of choice for the important function of the TSP and preserving the integrity of the system, the following business principle applies:~~

~~“The issuer is free to select one or more approved supplier(s) for the role of Token Service Provider within any single Token Programme. The approval will be performed by a Payment System who has defined the Token Programme and will include a number of Security, Functional and Operational requirements.~~

~~These requirements must be based on the principles of:~~

- ~~● Competition~~
- ~~● Transparency~~
- ~~● Non-Discrimination~~
- ~~● Efficiency~~
- ~~● Security~~

~~In conformance with these business principles, the TSP (Token Service Provider) is in the Issuing domain.~~

~~Two options of functional architecture are illustrated below:~~

- ~~● Option 1: the TSP is connected behind the CMS (Card Management System) of the Issuer which is in direct relation with the inter-PSP processor~~
- ~~● Option 2: the TSP is directly connected to an Inter-PSP processor (switching)~~

### **2.2.1 — Option 1**

~~Note: This is a logical diagram and does not represent the physical location of a TSP~~

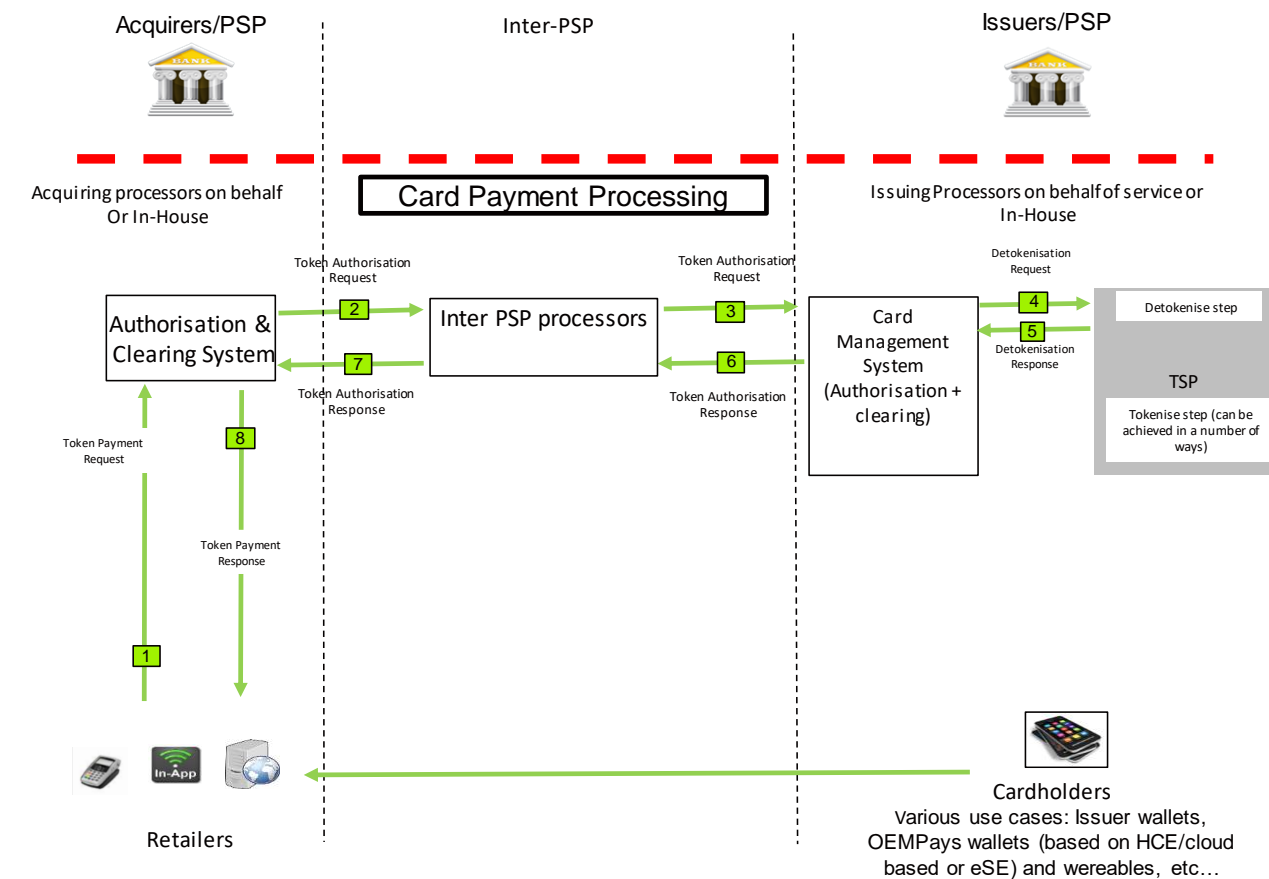


FIGURE 2: OPTION 1: TSP IN THE ISSUING DOMAIN BEHIND THE CMS

The CMS of the Issuer, linked to the Inter PSP processor for the authorisation and clearing flows, sends a detokenisation request to the TSP in order to retrieve the PAN.

Only the EMV token (not the PAN) is transmitted to the acquirer in the token authorisation response.

### 2.2.2 Option 2

Note: This is a logical diagram and does not represent the physical location of a TSP

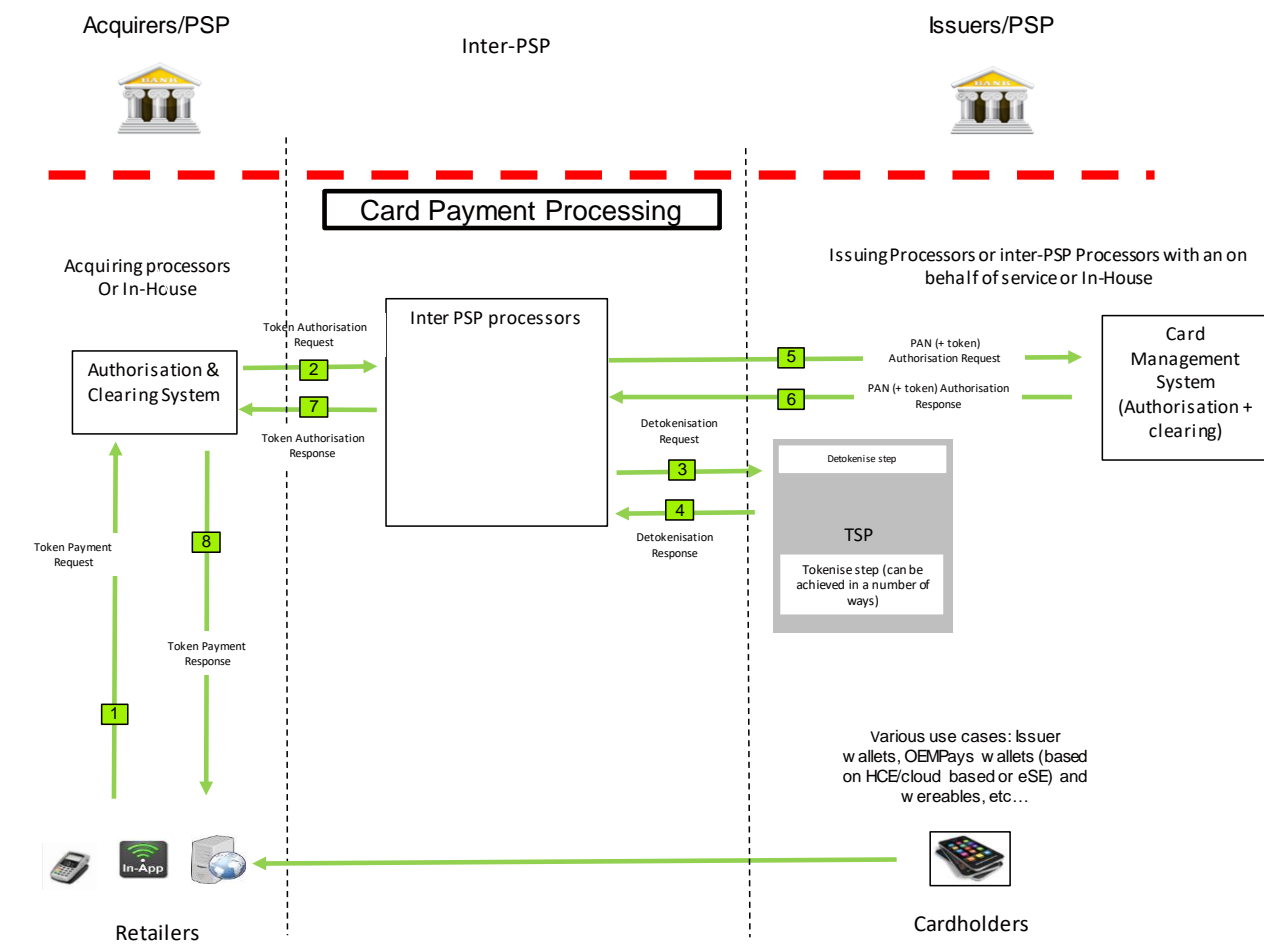


FIGURE 3: OPTION 2: TSP IN THE ISSUING DOMAIN IN FRONT OF THE CMS

In this option, the inter-PSP processor send:

1. To the TSP (always in the issuing domain) a detokenisation request to retrieve the PAN
2. And in a second step to the CMS an authorisation request with the PAN and the token

Only the token is transmitted by the Inter-PSP processor to the acquirer in the token authorisation response.

### 2.2.3 Token Issuance diagram

The previous diagrams only describe the interoperability of token-based payment flows. Token Issuance is outside the functional scope of the Volume. However, for the sake of clarity and completeness, the following diagram illustrates token issuance for any token payment model. This diagram works with both options described above.

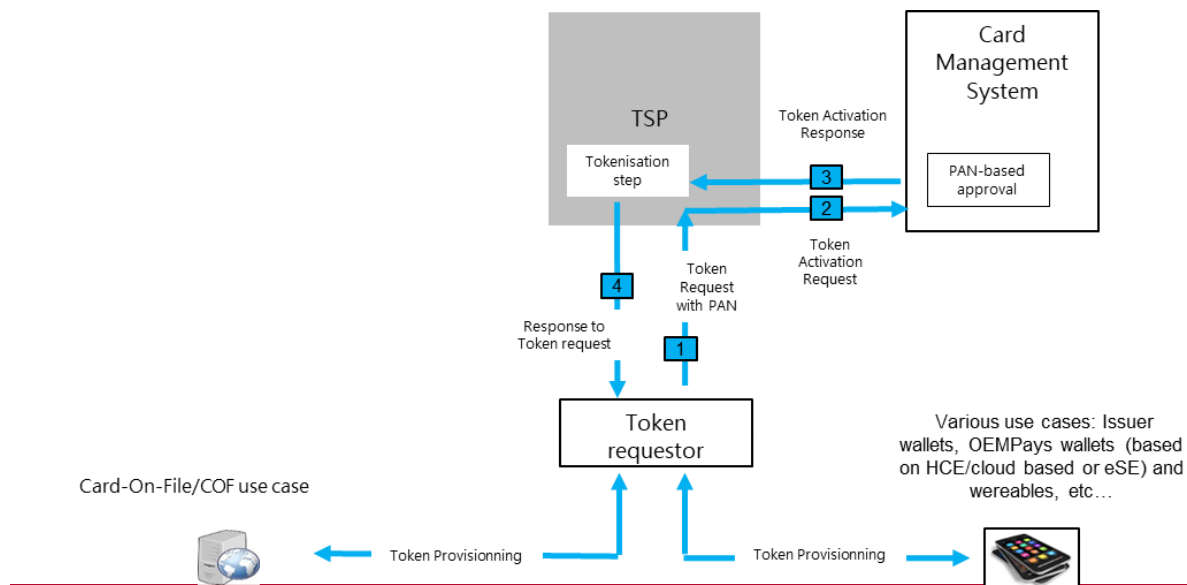


FIGURE 4: DIAGRAM FOR ANY TOKEN PAYMENT MODELS

~~Token provisioning covers both the cardholder use case (i.e. wallets) and the merchant use case (i.e. Card-On-File).~~

## 2.2.2 Common business principles and requirements to all domains

### 2.2.2.1 Obligations related to applicable law, rules and regulations

Card Payment Schemes must ensure their rules are compliant with law, rules and regulations applicable to their activity in the targeted markets, such as for instance the Payment System Directive and the EBA RTS, the Regulation (EU) 2015/751 on interchange fees for card-based payment transactions, GDPR or the European Accessibility Act.

The scheme rules must enforce their Members to also remain compliant with applicable law, rules and regulations.

Schemes and their Members should also follow the applicable recommendations or best practices applicable to their activity, such as for instance the ERPB recommendations on enhanced transparency for beneficiary information for retail payment end-users

### 2.2.2.2 Recommendations on GDPR compliance

The identification of the roles between the data controllers (acquirers, schemes and issuers) and the data processors (see Figure one) is defined by the purpose of processing of each personal data (PAN, PAN Token and PAR).

But as a requirement, any mandatory service in the rulebook of a Scheme means the definition of a joint data controller relationship between the scheme and its member (acquirer and/or issuer).

#### 2.2.2.3 Recommendations from ERPB on enhanced transparency for beneficiary information for retail payment end-users

The Euro Retail Payments Board (ERPB) set up a working group in July 2020, with the participation of relevant stakeholders, to address the need for enhanced transparency for beneficiary information for retail payment end-users i.e. the easy identification, from a consumer's payment account statement or corresponding application, of to whom, where and when the consumer made a payment.

Several recommendations were made, which can be found in document "ERPB work on transparency – Finalisation of the impact assessment, ERPB/2022/009, 17 June 2022", such as (not exhaustive list):

- To ensure that the Payee's commercial trade name is collected at the start of the transaction, retained at all its subsequent stages, and used for the generation of the consumer's payment/card account statement.
- To ensure that the identified datasets, transaction/reservation date and location of the Payee are retained at all stages of the transaction and used for the generation of the consumer's payment/card account statement,

In particular, Card Payment Schemes with their Members are encouraged to follow recommendation 1:

"If possible, adopt a common and co-ordinated approach to make the implementation by your members easier. Consider updating scheme rules or specifications to ensure that the commercial trade name of the payee is kept at all stages and appears on the payer's payment account statement."

#### 2.2.2.4 Recommendation on the European Accessibility Act [EAA]

The directive on the accessibility requirements for products and services, also known as European Accessibility Act that will come in force in June 2025, introduces common requirements related to the accessibility for products and services to fulfil design requirements, for people with disabilities, mainly for mobile and web devices.

All the stakeholders should follow and be responsible for the implementation of the European Accessibility Act.

The directive is available on EUR-Lex.

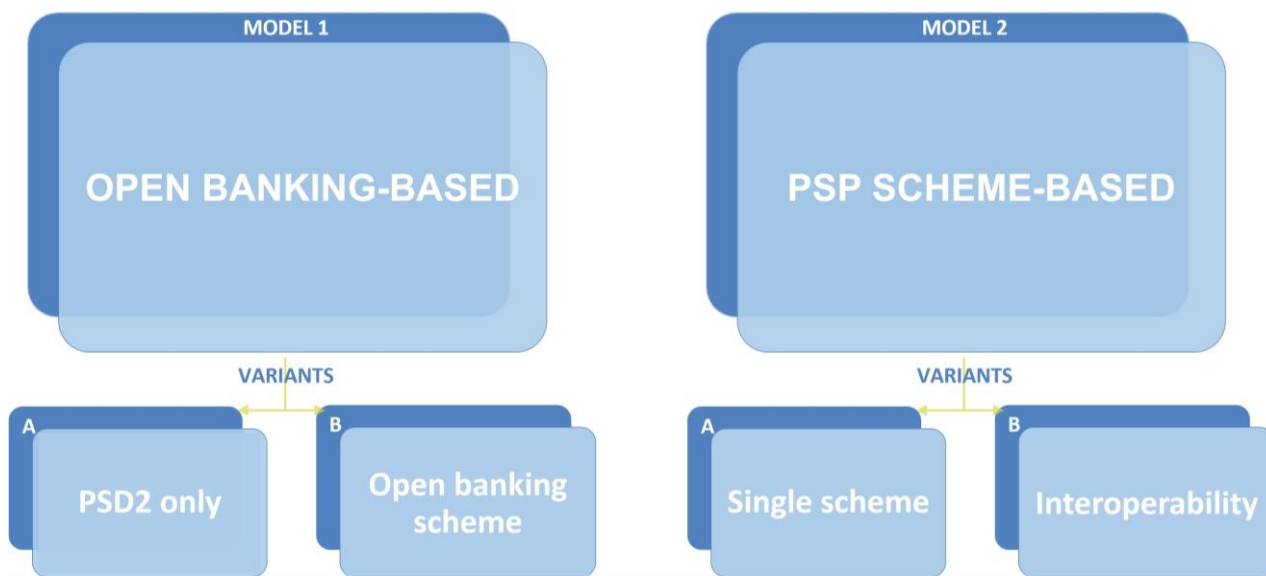




### 3 INSTANT CREDIT TRANSFER (ICT) TRANSACTION FRAMEWORK

#### 3.1 Introduction: various ICT Transaction models

The European market for instant payments (Instant Credit Transfer Transactions) is structured according to various models:



**Figure 3: Models of ICT Transactions in the European market**

Each ICT Transaction model has its own business requirements for the involved players but there is a common feature versus the card framework:

There is no distinction between scheme and processing levels due to the absence of relevant regulation (as outlined in Article 7 of [IFR] regarding the unbundling of these levels).

Two levels are only distinguished: payment initiation (i.e. “the overlay”) and payment execution.

The delivery of each model in the Book 7 will follow these assumptions:

- Limit to existing ICT Transaction models within European market excluding models in progress or those under consideration.
- For the payment execution level, at a first stage, only the models using the existing Execution Scheme will be described. And consequently, the requirements of [EPC SCT Inst] will be referenced without duplicate them in this book.
- Only one type of Payment Service is considered in this first stage: One-off Payment.

## 3.2 Open Banking-based model: PSD2 variant

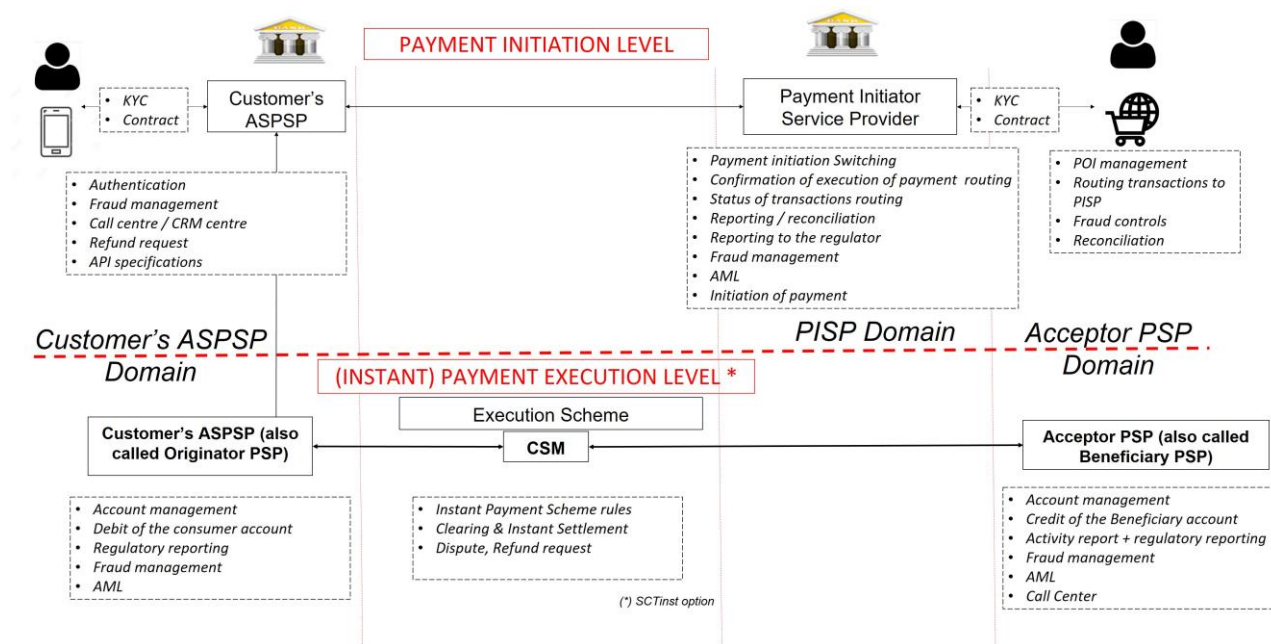


Figure 4: The main actors and services of the Open Banking-based model

### 3.2.1 Business requirements for the acceptance/merchant domain

#### Non discrimination

**Req AD1:** The service will be presented to the Customer, whether by NFC, QR code or other means as determined by the PISP. The acceptor POI will accept any customer who is able to conform to the PISP's interface.

#### Routing transaction to the POI

**Req AD2:** Transactions will be routed to and from the PISP, as agreed between the Acceptor and the PISP, including Payment request (including summary of payment details, payers ASPSP ID), and confirmation of payment initiation and execution.

**Req AD3:** The Acceptor shall not collect any data at the POI with respect to the transaction except as agreed with the PISP.

#### Fraud Controls

**Req AD4:** The Acceptor must exercise fraud controls as appropriate.

### Reconciliation

Reg AD5: The Acceptor **should** reconcile successful transactions processed by the PISP with funds received into the Acceptor's ASPSP account. This requirement may be performed by the PISP on the Acceptor's behalf.

### 3.2.2 Business requirements for the PISP

#### Payment Initiation and confirmation

Reg PI1: The information and conditions under which the PISP undertakes to process the Payment shall be made available to the Customer at the point of initiation, in accordance with national competent authority rules.

Reg PI2: The PISP shall enable initiation of payments by any Customer's **ASPSP** without discrimination.

Reg PI3: The PISP shall provide the Customer's ASPSP all data necessary for initiation of an SCTinst in the payment initiation request.

Reg PI4: The PISP shall notify the Acceptor of the status (i.e. initiated, successful or unsuccessful) of payment execution when this information is available and within the timescale agreed with the Acceptor (noting also that this must align to the timescale for the Customer's ASPSP to report as defined within the EPC SCTinst scheme). As an alternative, where the PISP has an arrangement with the beneficiary ASPSP, they may use information from th**at** ASPSP to provide confirmation of receipt to the Acceptor.

#### Fraud

Reg PI5: The PISP shall provide processes to detect fraud being perpetrated by payers and other parties (including Customers of the Acceptor in the case of Marketplaces), as agreed with the Acceptor.

#### Reconciliation and reporting

Reg PI6: The PISP shall provide sufficient information to the Acceptor to enable the reconciliation of payments processed by the PISP to balances reported by the Acceptor's ASPSP.

### 3.2.3 Business requirements for the Customer's ASPSP

#### Connectivity and Non discrimination towards PISP

**2.2.4** — Reg CA1: Customer's ASPSP must be open to any PISP without any discrimination as long as they follow the integration specifications required by the Customer's ASPSP.

Req CA2: Customer's ASPSP shall be free to decide how the Payment Service Providers will be integrated and must publish interface specifications and provide test environments to the PISP.

Req CA3: Customer's ASPSP should allow the same capabilities of initiation of Instant Payments as proposed from Remote banking services. Customer's ASPSP should allow the Payment Initiation Service Providers to get the same level of status of the transactions as they share with their own customers.

Req CA4: Customer's ASPSP shall be free to propose value added services beyond legal requirements on commercial terms to the PISP under a dedicated contract relationship.

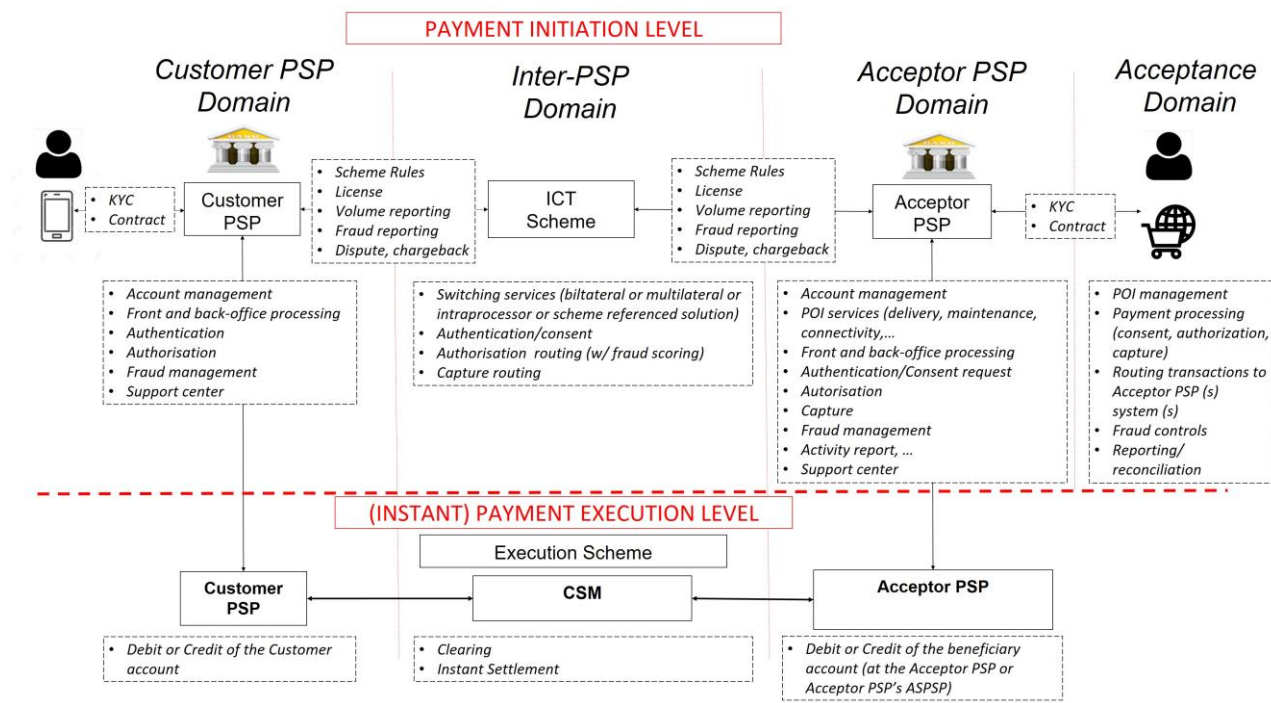
### Authentication

Req CA5: Customer's ASPSP are responsible for the authentication of their own Customers. Under contractual agreement, Customer's ASPSP may delegate the Authentication of their Customers to the PISP.

### **3.3 Open banking-based model: Open banking scheme variant**

This model is not described in this edition, but it may be included in future editions depending on how the market implementations and related standardisation evolve (see section 3.1).

### 3.4 PSP Scheme-based model: single scheme variant



**Figure 5: The main actors and services of the PSP Scheme-based model**

#### 3.4.1 Business requirements for the Acceptance Domain

The acceptance function can be done by the Acceptor or the Acceptor PSP.

Req Ac1: Acceptors and all the other relying parties shall collaborate with the Acceptor PSP to make sure that those rules are followed.

Req Ac2: As provider of services to acceptors, relying parties of the acceptors shall also follow Scheme rules. Relying parties of the Acceptors shall have the right to obtain scheme specific information to enable them to process scheme transactions. Such necessary information could be provided by the Scheme or the Acceptor PSP or the Acceptors to the relying parties of the Acceptors.

Req Ac3: Acceptors and their relying parties may be subject to certification by the ICT Scheme.

Req Ac4: Relying parties of the Acceptors may be subject to approval by the ICT Scheme.

Reg Ac5: Relying parties of the Acceptors shall decide which Implementation Specifications they want to support, taking into consideration the Customers' needs and the standards recognised by the ICT Scheme.

### **3.4.2 Business requirements for the Acceptor PSP Domain**

Reg AP1: Acceptor PSP, who are working with several Payment Brands, shall not restrict Acceptors from choosing the Payment Brands they want to accept.

Reg AP2: Acceptor PSP shall not prevent Acceptors from choosing their Acceptor PSP for each Payment Brand, so that Acceptors shall be free to choose. However, Acceptors may be subject to risk assessment and certification by the Acceptor PSP.

Reg AP3: Acceptor PSP shall not discriminate amongst POI vendors or POI and Acceptance host solution providers, chosen by their Acceptors, provided those parties meet the Acceptor PSP's technical and security requirements and support the Acceptor PSP's protocols specifications.

Reg AP4: Acceptor PSP shall be able to choose which ICT Scheme they want to acquire. The ICT Scheme shall not discriminate among Acceptor PSP in relation to participation in the ICT Scheme. However, Acceptor PSP and their relying parties may be subject to risk assessment and certification by the ICT Scheme.

Reg AP5: Acceptor PSP shall follow ICT Scheme rules as stated in their licence agreement. Acceptor PSP are liable for the compliance of their own relying parties.

Reg AP6: Acceptor PSP shall be free to choose which ICT Scheme and which related scheme services they support as per ICT Scheme rules.

Reg AP7: As provider of services to Acceptor PSP, relying parties of the Acceptor PSP shall also follow ICT Scheme rules. Relying parties of the Acceptor PSP shall have the right to obtain scheme-specific information to enable them to process ICT Scheme transactions. Such necessary information could be provided by the ICT Scheme or the Acceptor PSP to the relying parties of the Acceptor PSP.

Reg AP8: Acceptor PSP and their relying parties may be subject to approval by the ICT Schemes (e.g., security compliance of HSM, data protection).

Reg AP9: Acceptor PSP may get transactions from the POI either directly or through one or several levels of acceptance host solutions (or acceptance processor) which connect to the POI.

Reg AP10: Acceptor PSP shall be free to choose an external ASPSP of their choice for the execution of ICT Transactions.

Reg AP11: The Acceptor PSP or the chosen ASPSP of the Acceptor PSP must be able to execute ICT Transactions with the Execution Scheme.



### **3.4.3 Business requirements for the Inter-PSP Domain**

This domain at the ICT Scheme level covers the main following requirements:

Req IN1: To define and maintain the principal constituent elements of an ICT Scheme: the rulebook, the payment services and use cases, the specifications and the certification policy.

Req IN2: To manage the eligibility criteria and forms of in the ICT Scheme.

Req IN3: To switch all the Transactions from the Acceptor PSP to the Customer PSP which are the consent, authorisation, capture and chargebacks.

Req IN4: To manage the fraud risk on the transactions.

Req IN5: To specify the payment execution method (e.g. SCT Inst or other).

### **3.4.4 Business requirements for the Customer PSP Domain**

Req CU1: To manage the contractual relationships with their Customers (KYC).

Req CU2: To manage the fraud and credit liquidity risk on receipt of an Authentication and Authorisation request from the Acceptance domain.

Req CU3: To process front and back IT systems solutions according to the requirements of the ICT Scheme (Rulebook, certification policy and SLAs).

Req CU4: To order the execution of the settlement from the capture transaction received (i.e. to initiate an ICT Transaction as an Originator PSP, compliant **with** the Execution Scheme).

### **3.5 PSP scheme-based model: Interoperability variant**

This model is not described in this edition, but it may be included in future editions depending on how the market implementations and related standardisation evolve (see section 3.1).

**4** **TABLE OF FIGURES**

<a href="#">Figure 1: The main actors and services of the four party Scheme</a>	9
<a href="#">Figure 2: The card payment ecosystem including SRC</a>	13
<a href="#">Figure 3: Models of ICT Transactions in the European market</a>	26
<a href="#">Figure 4: The main actors and services of the Open Banking-based model</a>	27
<a href="#">Figure 5: The main actors and services of the PSP Scheme-based model</a>	31