

SEPA PAYMENTS STANDARDISATION VOLUME

Version v11.0



EPSCG

European
Payments
Stakeholders
Group

SEPA PAYMENTS STANDARDISATION (SPS) “VOLUME”**STANDARDS’ REQUIREMENTS**

Book 1

GENERAL PRINCIPLES AND DEFINITIONS*Payments and Cash Withdrawals in SEPA**Applicable Standards and Conformance Processes*

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

Abstract	This document contains the work on SEPA payment standardisation to date
Document Reference	EPSG035-26
Issue	Book 1 – v11.0
Date of Version	25.09.2026
Reason for Issue	Publication
Reviewed by	15 th EPSG Board
Produced by	EPSG Secretariat – Volume Sub-Group and EPSG Expert Teams
Owned and Authorised by	EPSG
Circulation	Public

*The EPSG's Payments Standardisation Volume is dedicated to the memory and legacy of **Jeremy Massey** and **Patrice Hertzog**, whose commitment, leadership and vision have left a lasting mark on our community.*

Jeremy Massey, in his roles as Co-Chair of the informal CSG first, becoming Vice Chair of the registered association ECSG when it was established, exemplified dedication, professionalism and a spirit of collaboration that inspired all those who had the privilege to work with him. Patrice Hertzog, through his skilful guidance as Chair of the ECSG, provided steady leadership and invaluable insight, strengthening both the work and the cohesion of the group.

Beyond their institutional responsibilities, both Jeremy and Patrice are remembered for their generosity, integrity and the meaningful personal connections they fostered. Their contributions continue to resonate in the progress achieved and in the values upheld by this community.

This dedication stands as a tribute to their enduring impact and as a sign of our deep gratitude.

Version number	Dated	Reason for revision
Change history of the Volume		
3.0	05.12.2008	Resolution covering the Volume approved at 17.12.2008 Plenary and announcing some editorial changes in the upcoming months
3.5	31.07.2009	Version for public consultation
4.0	30.11.2009	Version for the EPC Plenary
4.5	03.05.2010	Version for public consultation
5.0	15.12.2010	Version produced and reviewed by the CSG as well as approved by the EPC Plenary
5.5	01.06.2011	Version for public consultation
6.0	14.12.2011	Interim version (see Ch. 5 and 6) produced and reviewed by the CSG as well as approved by the EPC Plenary
7.0	12.12.2013 (published 07.01.2014)	EPC Published version – Volume v7.0
7.0.5	11.02.2015 (published 10.03.2015)	Consultation version 2015
7.1	08.12.2015	EPC Published version – Volume v7.1
Bulletin 001	29.02.2016	Bulleting describing the guidelines for using the Data Element provided by EMVCo for meeting the 9 June 2016 [IFR] deadline
7.5	11.05.2016	Working Version 2015-2016 for approval by the ECSG Board after the public consultation
8.0	01.03.2017	ECSG Published version - Volume v8.0
8.5	17.12.2018	Consultation December 2018-March 2019
9.0	15.01.2020	ECSG Published version - Volume v9.0
9.5	23.11.2021 (published in December 2021)	Consultation version December 2021-March 2022

Version number	Dated	Reason for revision
10.0	01.10.2022	ECSG Published version - Volume v10.0
10.5	27.11.2025 (published in December 2025)	Consultation version December 2025-March 2026
11.0	25.09.2026	EPSG Published version - Volume v11.0

Version number	Dated	Reason for revision
Change history of Book 1		
6.1.0.x	2012-2013	Working version of Book 1
7.1.1.0x	2014-2015	Working version 2014-2015
7.1.2.11-7.1.2.99	16.12.2015	Working Version 2015-2016
7.1.2.5-7.1.2.9	21.11.2016	Working Version 2015-2016 for approval by the ECSG Board after the public consultation
8.1.00	01.03.2017	ECSG Published version - Volume v8.0
8.1.40	22.11.2018	Board Approval version for Consultation as 8.5
8.1.50	17.12.2018	Public Consultation Release v8.5
8.5.4	31.07.2019	Working Version to v9
9.0	15.01.2020	ECSG Published Version – Volume 9.0
9.01-9.12	2020-2021	Working Versions towards v9.5
9.12	15.12.2021	Public Consultation Release v9.5
10.0	01.10.2022	ECSG Published version - Volume v10.0
10.01-10.43	2023-2025	Working Versions towards v10.5

Version number	Dated	Reason for revision
10.5.01	26.05.2026 (sent to the Board for approval on 27.05.2026)	Version validated by the Volume-Subgroup for legal review
10.5.02	31.08.2026	Legal review
10.5.03	03.09.2026	VOLSG Sanity Check
10.5.04	24.09.2026	Board approval for publication

Table of Contents

1	GENERAL	8
	Terms of Use	8
1.1	Executive summary	9
1.1.1	Goal and Addressees.....	9
1.1.2	Volume	9
1.1.3	Payment Services	9
1.1.4	Security	10
1.2	Volume Conformance via Labelling	10
1.3	Volume Maintenance principles	11
1.4	Description of changes since the last version of Book 1	14
1.5	Volume Compliance with European Regulations and Directives	15
1.5.1	Volume impact	15
1.5.2	Work in progress.....	16
1.5.3	High-Level Summary of PSD2-related content	16
1.5.3.1	Merchant Initiated Transactions (MITs)	17
1.6	Tokenisation.....	18
1.7	Secure Remote Commerce (SRC).....	18
1.7.1	SRC summary presentation.....	18
1.7.2	SRC inclusion in the Volume	19
1.8	Instant Credit Transfer (ICT).....	19
1.9	Overview of Payment Applications.....	26
2	THE SPS VOLUME AND ITS BOOKS.....	28
2.1	Introduction to the “SEPA Payments Standardisation Volume”	28
2.2	Scope and Objectives of EPSG Work on Payments Standardisation	29
2.2.1	Scope	29
2.2.2	Objectives.....	29
2.2.3	Impact on the Different Stakeholders	30
2.2.4	Implementation of the Volume and Monitoring	30
2.2.5	Implementation Specifications	30
2.3	Maintenance of the Books.....	30

2.3.1	The Volume, a Set of Books	30
2.3.2	Maintenance cycles.....	31
2.3.3	Intellectual Property Rights	31
3	REFERENCES, ABBREVIATIONS AND DEFINITIONS.....	33
3.1	References	33
3.2	Abbreviations	38
3.3	Definitions	41
4	FIGURES	86

1 GENERAL**Terms of Use**

The European Payments Stakeholders Group (EPSG) AISBL, an industry association actively working on payments standardisation in the Single Euro Payments Area (SEPA), publishes the SEPA Payments Standardisation Volume (“the Volume”), formerly “SEPA Cards Standardisation (SCS) Volume”.

BY CONSULTING OR BY USING THE VOLUME YOU AGREE ON YOUR BEHALF AND ON BEHALF OF EACH ENTITY AND PERSON ON BEHALF OF WHOM YOU ACT TO BE LEGALLY BOUND BY THE TERMS OF USE DETAILED BELOW.

Whilst the EPSG has used its best endeavours to make sure that the information, data, documentation and other materials contained in the Volume are accurate and complete, and whilst the Volume aims to be in accordance with the relevant applicable laws, regulations and directives, the EPSG does not accept any liability for any error, omission or non-conformance, and your use of the Volume and the information, data and other materials contained therein is at your own risk. The Volume and the information, data and other materials contained therein are provided to you “as is” without warranty of any kind, and are not intended to provide, and do not constitute regulatory or legal advice to any individual or entity. It remains your sole responsibility to ensure that your activities related to Payment Services and the use of the Volume and the information, data and other materials contained therein are fully compliant to the relevant applicable laws, regulations and directives in force. You are urged to consult with your own advisors before taking any action based on the Volume.

To the fullest extent permitted by Law, neither EPSG nor its Auxiliaries within the meaning of Book 6 of the Belgian Civil Code (defined as employees, officers, directors, agents, representatives, subcontractors, suppliers or any other entity person engaged, whether or not under authority), nor any other party involved in creating, producing or delivering the Volume, will be liable for any damages whatsoever (including, without limitation, incidental, consequential, indirect or punitive damages, lost profits, or damages resulting from lost data or business interruption) resulting from your use of or inability to use the Volume and the information, data and other materials contained therein, whether based on warranty, contract, tort, or any other legal theory. The exclusion of liability of Auxiliaries is stipulated for the benefit of each of EPSG’s Auxiliaries, who shall be entitled to it invoke in own name and against any party.

You agree to defend, indemnify and hold harmless the EPSG and its members, from and against any and all claims, actions or demands, including costs and attorney’s fees, arising from or in connection with your use of the Volume. The EPSG shall provide notice to you promptly of any such claim, suit or proceeding and shall provide you with reasonable assistance, at your expense, in defending any such claim, suit or proceeding.

The terms of this disclaimer are subject to Belgian law. In case of a dispute only the Brussels courts have jurisdiction.

1.1 Executive summary

1.1.1 Goal and Addressees

This document (The "Volume") is ultimately designed for the benefit of Payment Service Users in Europe (such as customers and acceptors), *enabling them to use Payment Devices (such as cards and mobile phones) to make and receive payments and cash withdrawals throughout SEPA with the same ease and convenience as they do in their home country*. This concept was defined as "SEPA for Cards" by the European public authorities. The Volume is aimed at the entire payment industry active in Europe and provides common standardisation requirements, which need to be adopted with a high priority in order to achieve the aforementioned goal. The Volume also represents the best efforts made by the EPSG in understanding requirements that are part of European regulatory universe, such as the Interchange Fee Regulation [IFR], the European Accessibility Act [EAA], the PSD 2[PSD2] (as modified by Commission delegated regulation 2022/2360 of 3 August 2022), the Commission delegated regulation (2018/389) of 27 November 2017 [RTS SCA/CSC], as well as the General Data Protection Regulation [GDPR].

1.1.2 Volume

The Volume does not address existing practices, processes or standards, but focuses on the objectives and the path for market developments. It is structured as a set of Books, each describing an important aspect. This can be from a standardisation, security or conformance perspective. The Volume is exclusively owned by the European Payments Stakeholders Group (EPSG) which is composed of market representatives from the five main payment-related sectors: Payment Service Providers (gathered in the European Payments Council, "EPC"), Processors, Retailers (acceptors), Schemes and Vendors.

The Volume requirements are not formally imposed on market stakeholders, however its rules are defined by market experts. The ECB and the European Commission provide guidance and actively contribute to this work.

1.1.3 Payment Services

The Volume describes functional requirements applicable to transactions initiated using any Payment Solution — whether at a physical Point of Interaction (traditionally 'local' or 'present') or remotely (traditionally 'not present') — regardless of the underlying Payment Instrument. These transactions result in the provision of the relevant Payment Services to the Customer and Acceptor, as specified in the Volume.

1.1.4 Security

Trust in a payment instrument is largely dependent on the security of all transaction components. Due to the permanently morphing nature of fraud attacks, requirements on the security level are continuously evolving. However, the core security requirements should be common throughout the whole SEPA area. Harmonised security requirements are essential for maximising the security of, and trust in payments, achieving an effective SEPA for all actors and ensuring maximum customer protection and user convenience. This is, however, not the sole responsibility of the EPSG. The relevant regulatory authorities also have a role in that domain.

1.2 Volume Conformance via Labelling

The level of market implementation of the Volume requirements by specification providers is reported to the Euro Retail Payments Board (ERPB) on an annual basis. Further information about the process of verifying Volume conformance, known as labelling, can be found on the EPSG website¹, as well as Book 5 (Conformance Verification Processes) of the Volume.

The Volume conformance process (labelling via the EPSG) became operational in 2017. As a general rule, if an organisation wishes certain products and solutions to be conformant to the Volume, they will need to apply all requirements for those products and solutions defined within the Books. In this case, all newly approved products and solutions shall comply with the requirements of the latest published Volume release, relevant for the functions, services and options being implemented by the products and solutions, within a ***maximum of three years after publication***.

The long-term vision is that all approved Card-based or Instant Credit Transfer-based payment products and solutions for transactions initiated in the SEPA area will in future be compliant with the requirements described in the Volume.

Functional requirements of the Volume may be waived for people with disability, in order to provide them with equal access to payment services. Schemes, Issuers, Acquirers and Terminal Vendors should consider the usability for the visually impaired as well as the provisions set forward in the 'European Accessibility Act' [EAA] when designing Payment Solutions. This is especially important for local transactions.²

Implementation monitoring - Without prejudice to any EU Regulation provisions on implementation deadlines, migration dates and overall deadlines are also included in the Volume as agreed by the different EPSG Sectors. In order to make sure that the market evolves in due time,

¹ <https://www.e-csg.eu/labelling-process-description>

² To assist visually impaired customers, where pin pads are available the "5" key may have a raised dot on it, in accordance with the recommendation in ISO-9564. Furthermore, the vendor should consider providing:

- Raised marks on the function keys, to allow identification without being able to read it.
- A beep when a button is pressed.
- The text in a colour contrasting to the background colour.
- Text to speech functions to allow the terminal to read out the display texts.

in the expected direction and at a normal speed, a monitoring of the implementations is organised and conformance results are made public on the internet.

1.3 Volume Maintenance principles

1. A full version of the Volume with all its Books is planned to be published based on a 3 year cycle.
2. In the meantime, individual Books may be updated to reflect either urgent amendments or changes in legislation, technology and the evolving landscape. Such individual updates are published as Bulletins which will be incorporated in the following full version of the Volume.
3. In all cases except updates due to regulatory changes, a formal public consultation process will be undertaken.

Version 7.0. of the Volume was published in January 2014 as a stable release ready for market implementation. It was however restricted in scope to “Face-to-Face” card transactions.

Version 7.1. of the Volume was published in December 2015 to include card services for Card Not Present [Remote] payments and included conformance to the new card interchange regulation.

Version 8.0 of the Volume was published in March 2017, including i.a., alignments with the Interchange Fee Regulation and the updated Payment Services Directive. This version included **Bulletin 001**, published on 29 February 2016 in order to provide guidelines on how to use the Data Element provided by EMVCo to ease compliance with the Interchange Fee Regulation whose deadline is 9 June 2016.

Version 8.5 of the Volume was published in December 2018 to address regulatory and innovative aspects as well as perform updates as part of the standard Volume cycle.

Version 9.0 of the Volume was published in January 2020.

Bulletin on MIT, published on 25 October 2021 to reflect within the Volume Version 9.0 the requirements for Merchant Initiated Transactions clarified by the European Commission in early 2020 as part of the deployment of the PSD2 regulatory standards of Strong Customer Authentication.

Version 9.5 of the Volume was published in December 2021 to integrate innovative aspects in parallel with general updates as per the usual Volume cycle.

Version 10.0 of the Volume was published in October 2022.

Version 10.5 of the Volume was published in December 2025 to integrate Instant Credit Transfer (ICT) Transactions alongside general updates as per the usual Volume cycle.

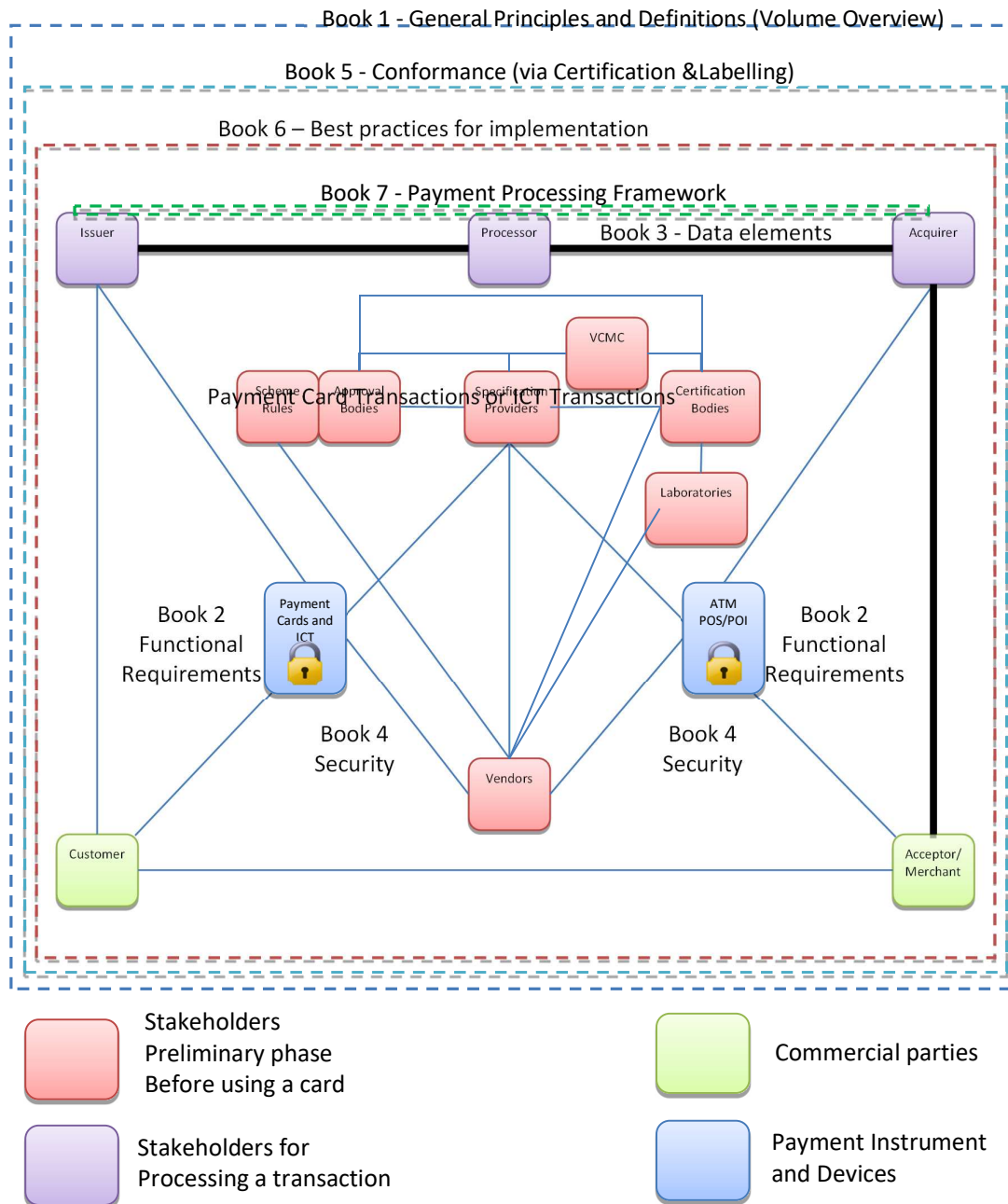


FIGURE 1: VOLUME OVERVIEW

As illustrated in the drawing above, it is currently composed of

Book 1 - ***General Principles and Definitions***

Book 2 - ***Functional Requirements***

Book 3 - ***Data Elements***

Book 4 - ***Security***

Book 5 - ***Conformance Verification Process***

Book 6 - ***Best Practices for Implementation***

Book 7 - ***Payment Processing Framework***

Annex - ***Tokenisation for SEPA Payments***

1.4 Description of changes since the last version of Book 1

This version of Book 1 includes the following updates:

- The section on terms of use has been revised as to reflect the exclusion of any liability of auxiliaries within the meaning of Book VI of the new Belgian Civil code.
- The section on compliance has been revised to reflect the applicable European regulatory framework.
- Instant payments (Instant Credit Transfer Transactions) have been introduced within the scope of the Volume.
- Definitions have been reviewed, completed and aligned both with regulations and with updates made in other Books of the Volume.
- Additional information has been introduced regarding the EPSG initiative on Tokenisation.
- The EMVCo specifications on Secure Remote Commerce (SRC) have been incorporated into the Volume.
- General editorial adjustments have been applied to ensure consistency and improved readability.

1.5 Volume Compliance with European Regulations and Directives

The Volume aims to be compliant with relevant regulations and directives in force at the time of its publication. In the event that inconsistencies are identified, the text of the relevant regulatory documents shall prevail. It remains the responsibility of stakeholders to ensure that their activities related to Payment Services are fully compliant to those regulations. This version of the Volume has been drafted with particular attention given to [PSD2] and the [GDPR], - and their implementation issues that need to be resolved in a harmonised way across SEPA.

There is no doubt that PSD2 and the subsequent Regulatory Technical Standards [RTS SCA/CSC] are strategic milestones for the payments industry. The EPSG has analysed the impact of the [PSD2] and [RTS SCA/CSC] on the EPSG SEPA Payments Standardisation “Volume” and the outcome of that effort is contained in the present version.

Apart from defining requirements, the EPSG, as an industry multi-sector body, may also play a de-facto role in generating awareness, consistency, visibility and comprehension of the different [PSD2]/[RTS SCA/CSC] aspects that are related to payments. It should be noted, however, that the EPSG plays no role in compliance. Conformance with the Volume requirements continues to be of a voluntary nature and based on a self-declaration (see detailed process in the EPSG web-site section “Labelling”).

1.5.1 Volume impact

Compared to the magnitude and paradigm-shifting dimension of the [PSD2]/[RTS SCA/CSC], the impact on the SPS Volume may seem limited. This is due to the following factors:

- The EPSG remit, within this version of the Volume, is limited to Card Transactions and Instant Credit Transfer Transactions, while the [PSD2] has a much wider scope, including all types of electronic payments.
- The EPSG caters for standardization needs, with a particular focus on security and interoperability at the point of interaction between payer and payee. Many aspects of the [PSD2]/[RTS SCA/CSC] are primarily concerned on the interaction between the Issuer (ASPSP) and his Customer (the payer); hence, most of these topics, albeit interesting for the whole industry and although they may benefit from some standardization, are deemed to be out of the scope of the EPSG.
- Some aspects that may indeed be in scope of the EPSG work, were considered too early to be standardised. Future versions of The Volume will re-evaluate these aspects accordingly.

The EPSG acknowledges the importance of ensuring compliance with the mandatory provisions of applicable rules and regulations related to the processing of personal data, notably the 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 ('GDPR').

It remains the responsibility of each stakeholder to ensure that its activities are fully compliant with GDPR. Each stakeholder is responsible for identifying its controller or processor role under the GDPR, understanding which personal data it processes, ensuring the appropriate legal basis for the processing of personal data, including the data subject's consent if required, and implementing all relevant obligations applicable to them under the GDPR, and to demonstrate accountability.

The EPSG is also aware of the adoption of Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data ('Data Act'). The Data Act does not explicitly cover payments. Therefore the Volume does not introduce specific requirements related to the Data Act. However, stakeholders are expected to take this regulation into account when implementing the Volume requirements. As with other applicable legislation, compliance with the Data Act remains the responsibility of each stakeholder. It is up to each party to assess the relevance and applicability of the Data Act to its activities and to ensure that appropriate measures are taken to meet the obligations set out therein.

It is also up to each stakeholder to assess the impact of and comply with Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, in force since January 17th, 2025 [DORA], and with Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets of 31 May, 2023, fully in force since end 2024.

1.5.2 Work in progress

The EBA (European Banking Authority) has a Q&A Tool mechanism through which guidance on the open questions will gradually be made public. Some of the questions and answers may be such that the EPSG needs to work and incorporate the clarifications into the EPSG Volume.

1.5.3 High-Level Summary of PSD2-related content

- Book 1:
 - In addition to this section, some definitions have been completed/enhanced/aligned in view of [PSD2]/[RTS SCA/CSC], such as e.g.: "Contactless", "Credentials", "Instalment" and "Recurring" payments
- Book 2 (Functional Requirements) includes a few impacts such as:
 - Recommendation of EMV 3DS authentication supporting [PSD2]/[RTS SCA/CSC] provisions and notably the regulatory exemptions

- Clarifications on some card-not-present and cardholder-not-present transactions such as instalment and recurrent payments
- Need for a new decline reason “SCA Required”
- Need for quality and certain characteristics in field “Card Acceptor Name and Location”
- Update of requirement T77 in relation to [RTS SCA/CSC] Article 11
- Requirement T28 in relation to [RTS SCA/CSC] Article 12
- Book 4 (Security Requirements) makes numerous references to [PSD2]/[RTS SCA/CSC], whether as requirements or merely as references aiming to increase awareness of certain provisions.
- Book 6 (Implementation Guidelines) was updated to include guidance on exemptions to the requirement to perform Strong Customer Authentication (SCA), specifically for
 - Low value contactless transactions,
 - Unattended terminals used for transport fares and parking fees.
- There is currently no impact identified – or that is stable enough, having achieved a sufficient degree of common interpretation - to be included in Books 3, 5 and 7.

1.5.3.1 Merchant Initiated Transactions (MITs)

- **MIT:**

MITs are excluded from the scope of the RTS SCA. This is essentially because the Payer is no longer “in session” with the Merchant (payee) at the time of a MIT.

MIT Authorisation messages must be properly flagged as such. How this is achieved is implementation-specific.

MIT must not be used for Card On File transactions if the Customer is triggering the Payment. MITs are not preceded by a specific action of the Payer, except for the establishment of the MIT Mandate.

For wider context and details, see EBA Q&A tool, answers 2018_4031, 2018_4404, and 2018_4131.

- **MIT Mandate:**

The MIT Mandate can be established in various forms, electronic or not; if the Mandate is set up electronically, SCA is required.

This SCA can be achieved through different flows depending on the use case, in particular it could include the Card Data of the Card to be used for the MIT.

Normally the SCA is part of a standard flow where an Authentication is followed by an Authorisation. Otherwise, if an Authorisation is not yet necessary at the time of setting up the mandate, then the SCA may be achieved e.g. through a zero-amount Balance Enquiry flow.

Note that a unique reference to this mandate must be included in any subsequent MITs related to this same mandate. This reference may be implementation specific, for example a “Trace Id” could be used.

1.6 Tokenisation

Tokenisation, described in detail in an appendix document to the Volume called the *Annex - Tokenisation for SEPA Payments*, has been playing a critical role in the task of enhancing the security of payments. A specific Tokenisation business requirement has also been added to Book 7.

1.7 Secure Remote Commerce (SRC)

1.7.1 SRC summary presentation

SRC are an EMVCo set of specifications to enable a streamlined processing of e- and m-commerce transactions based on Card Payment technology and infrastructure. SRC aims to deliver the same experience as EMV chip and contactless in a remote environment globally.

SRC is based on the principle of the interconnection of the issuing and acceptance platforms through an SRC system acting as an orchestrator of services. The transmission of payment data from the issuing domain to the acceptance one is thus preferred rather than:

- The consumer (repetitive) manual entry of these data in the acceptance domain.
- The Card On File experience by minimising the local storage of static Payment Data.

This principle has the potential to reduce friction of the transactions, resulting in fewer shopping cart abandonments. A recognisable trigger (SRC visual identification) is provided and implemented in the UI.

The integration of the various industrial platforms to the SRC System is enabled by the delivery of standardised APIs and SDKs.

SRC defines a specific ecosystem with the involved players or participants:

- The SRC System.
- The SRC Participating Issuer (SRCPI).
- The Digital Card Facilitator (DCF).
- The Digital Payment Application (DPA).
- The SRC Initiator (SRCI).

The SRC specifications offer the flexibility to support different checkout experiences, in particular multiple SRC Participant roles may be assumed by a single entity.

In addition to the standard SRC Checkout, alternative Acceptor-driven checkout experiences are considered, such as:

- Merchant orchestrated: A purchase experience which is fully integrated within the Acceptors' current checkout, allowing them to control the user experience and manage recognition of Customers.
- Merchant digital Card-On-File checkout: A purchase experience allowing the Customer to designate a digital card enrolled with an SRC System, which becomes their default digital card stored by this specific Acceptor.

1.7.2 SRC inclusion in the Volume

The scope of SRC is mainly the checkout payment process and the selection of the Card by the Cardholder. Compared to classic EMVCo transactions, no change in the Card payment process following the checkout was identified.

The scope of the Volume being only the payment process, the impacts of SRC are low as it is shown in this figure

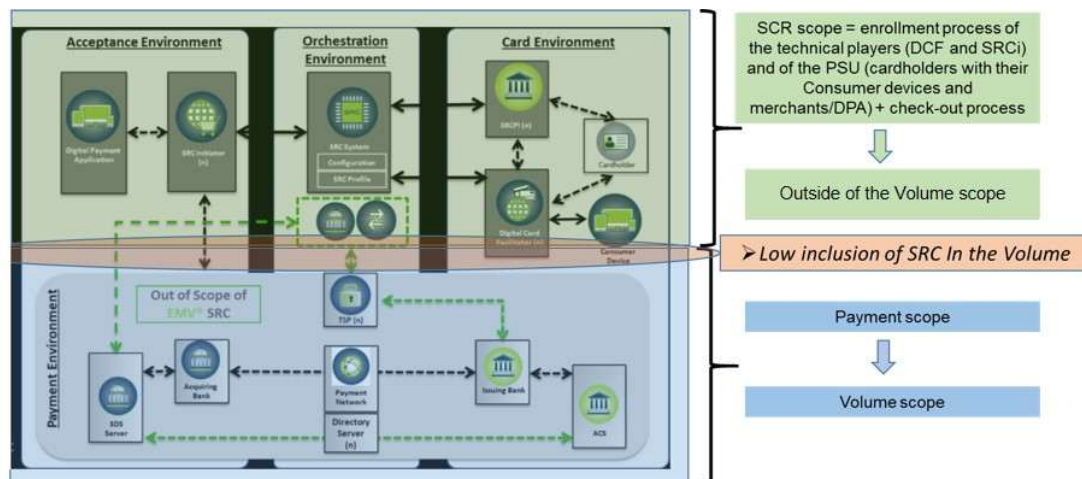


FIGURE 2: VOLUME AND SRC INTEGRATION

1.8 Instant Credit Transfer (ICT)

Instant Credit Transfer (ICT) in this document corresponds exclusively to the Consumer-to-Business (C2B) domain. It is assumed that ICT Transactions may be executed either under the governance of an ICT Scheme or based on published "Open Banking" standards and regulation.

The following diagram introduces the models of ICT Transactions identified by the EPSG within the scope of this Volume, with a primary focus on “*Model 1 Open Banking-based – PSD2 Only variant*” for One-off Payment. Further elaboration and coverage are foreseen in future versions of the Volume.

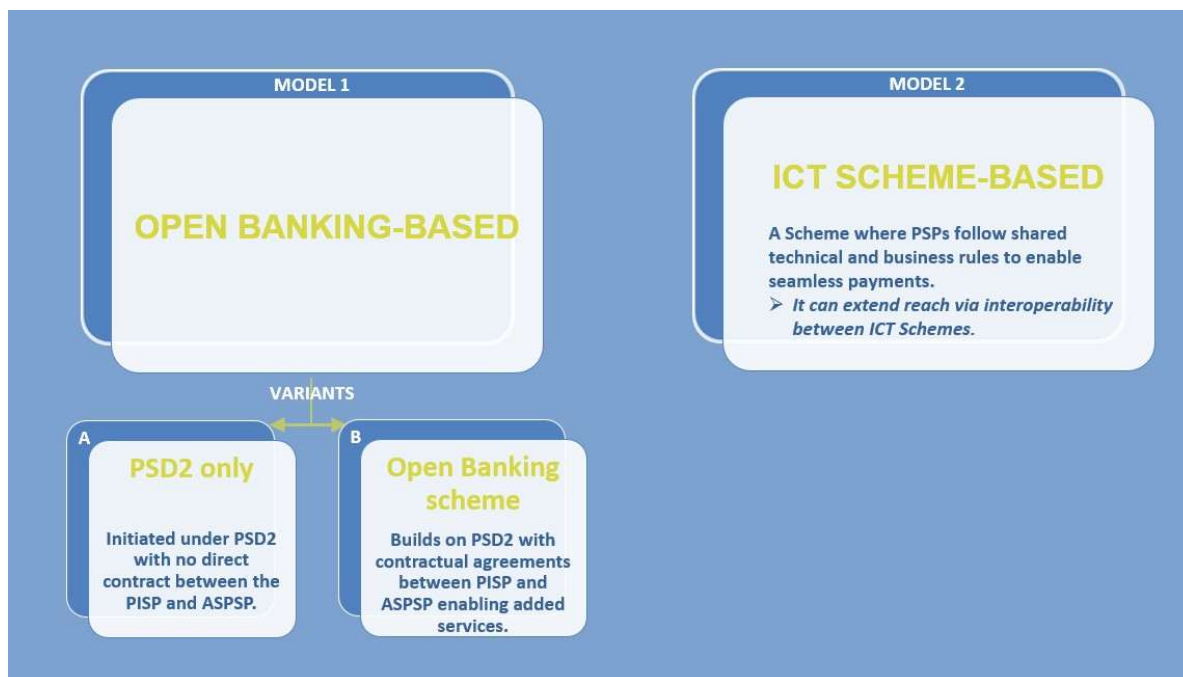


FIGURE 3: ICT TRANSACTION MODELS IN THE CONSUMER-TO-BUSINESS DOMAIN

For the purpose of this version of the Volume, ICT Transactions have at least the following three characteristics:

- The Payment Account of the Customer/Payer is immediately debited.
- The Payment Account of the Acceptor/Payee or the related receiving account is immediately credited within a tolerance of a few seconds, and the funds are immediately available.
- The service providing ICT is continuously available (24/7).

This means that, in this version of the Volume, the EPSG focuses exclusively on ICT Transactions that involve immediate settlement between bank accounts, while acknowledging that some market solutions may appear instant to end users (e.g. via fund blocking) but are in fact based on deferred settlement.

The settlement between bank accounts may also be called the “execution” or “payment execution” of the ICT Transaction. The steps that are performed to initiate the settlement may be referred to as “initiation” or “payment initiation” of the ICT Transaction.

The roles of the actors involved in an ICT Transaction

Several implementations and flows are possible for performing an ICT Transaction. However, in this document, it was decided to focus on an Open Banking-based model implemented via PSD2 (Model 1-A), where five roles/actors supporting the different communication interfaces and protocols for the execution of the ICT Transaction can be identified:

- **Customer/Payer**, equipped with an ICT Payment Instrument provided by the Customer's Account Servicing Payment Service Provider (ASPSP).

Note: In the context of Open Banking, the Customer's ASPSP may provide a dedicated interface (typically an API according to PSD2) to initiate the transfer of funds, but they do not necessarily issue a personalised device (e.g. a Payment Application) to the Customer used to initiate ICT Transactions.

- **Acceptor/Payee**, the final beneficiary of the ICT Transaction, and a customer of the Acceptor PSP.

- **Customer's ASPSP**, the Account Servicing Payment Service Provider of the Customer.

- **Payment Initiation Service Provider (PISP)**, a Third-Party Payment Service Provider with a direct contractual arrangement with the Acceptor but not with the Customer's ASPSP.

- **Acceptor PSP**, the Payment Service Provider of the Acceptor.

The ICT Transaction settlement system in the interbank domain is out of scope.

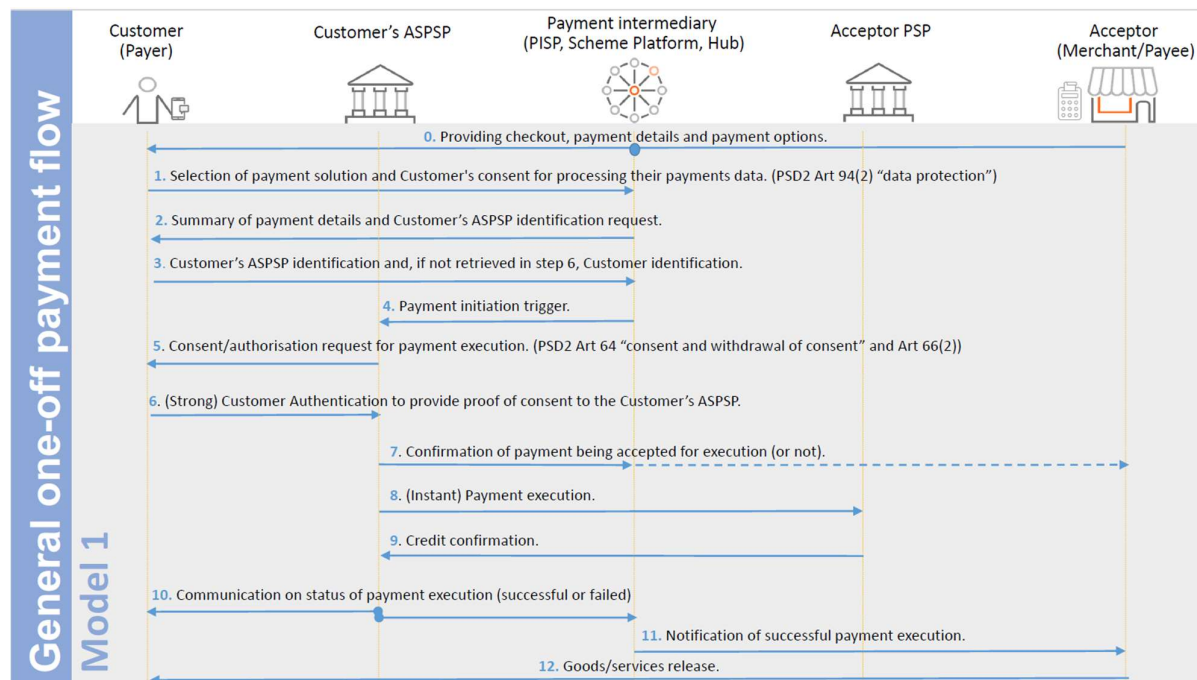


FIGURE 4: LOCAL AND REMOTE ICT TRANSACTION – GENERAL ONE-OFF PAYMENT FLOW (MODEL 1)

In this document, it is assumed that the Customer's ASPSP might offer different interfaces for access to designated ICT accounts:

- One direct interface when the Customer initiates an ICT Transaction from their own ICT Payment Application, resident in one or more form factor(s), including the secure element of a Mobile Device, a Physical Card, a wearable, as well as any secure enclave in a personal computer.
- A dedicated interface (typically an API according to PSD2) when access to the ICT account is requested by a Third-Party Payment Service Provider (TPP PISP – Payment Initiation Service Provider according to PSD2).

The initiation of a Local ICT Transaction may be based on various Acceptance Technologies:

- **QR Code**

In order to optimise the user experience and interoperability, a QR Code standard may be selected and recommended by the EPSG in due course.

The standard should support:

- both Consumer-presented and Merchant-presented modes,
- ability to provide inside one QR Code instance information for multiple Payment Brands, and, in the case of Merchant-presented QR Code, PISP connection (URL) information needed for the Open Banking flow in **FIGURE 5: OPEN BANKING-BASED ICT TRANSACTION – MERCHANT-PRESENTED QR CODE** to be extracted by the built-in camera app of the Customer's Mobile Device.

Such selection of a standard is not yet possible at this stage given that several initiatives are still emerging and interacting, with QR Codes that are still evolving and whose practical implementation (data fields, registration of identifiers) is not fully defined or in the process of being standardised.

For this Volume version, QR Codes are only considered for ICT Transactions and not for Card Transactions.

- **Merchant-presented QR Code**

The initiation of an ICT Transaction based on a Merchant-presented QR Code requires the use of a Mobile Device, where the QR Code is captured by the Mobile Device camera. The QR Code may have been generated dynamically (containing transaction-specific information) or may be static (e.g. decal display on an unattended POI).

FIGURE 5 below, illustrates an ICT Transaction flow for a One-off Payment for Merchant-presented QR Code.

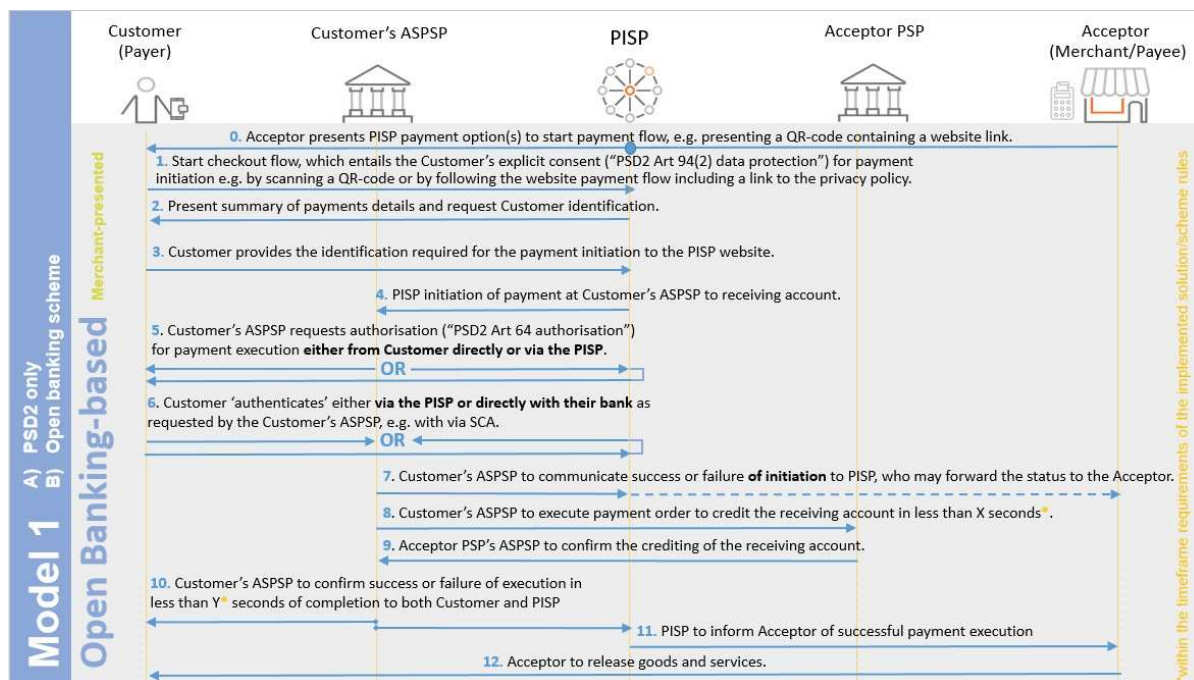


FIGURE 5: OPEN BANKING-BASED ICT TRANSACTION – MERCHANT-PRESENTED QR CODE

○ Consumer-presented QR Code

The initiation of an ICT Transaction based on a Consumer-presented QR Code requires the use of a QR Code scanner at the POI.

While QR Code generation and presentation from part of the Customer can be performed in several ways, the majority of market use cases are based on Mobile Device.

The flow of an ICT Transaction for a One-off Payment using Consumer-presented acceptance is provided in **FIGURE 6**.

In principle, it is possible to perform Customer authentication shown in steps 5 and 6 in **FIGURE 6** not only via the PISP but also via the Acceptor's POI. To this extent, an interface would have been established between PISP and Acceptor's POI to collect the Customer data needed for authentication (e.g. an Online Personal Code and an OTP).

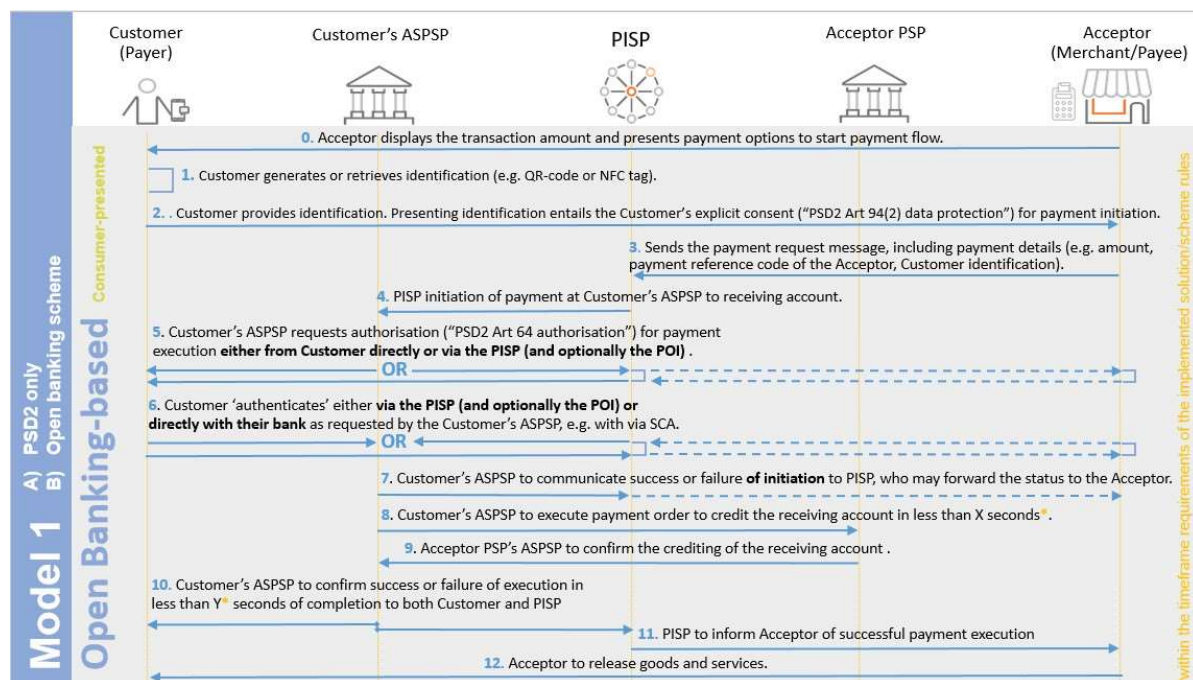


FIGURE 6: OPEN BANKING-BASED ICT TRANSACTION – CONSUMER-PRESENTED QR CODE

- **Mobile Contactless - with Mobile Contactless ICT Payment Application**

The initiation of an ICT Transaction using an NFC interface utilises the same RF communication channel available for a contactless Card Transaction, including Application Selection via Proximity Payment System Environment and assignment of an associated kernel on the POI. The subsequent ICT Transaction flow is specific to the Mobile Contactless ICT Payment Application on the Consumer Device and the POI contactless kernel.

An illustrative example of a One-off Payment transaction based on Mobile Contactless with Mobile Contactless ICT Payment Application issued by the Customer's ASPSP (referred to as Bank app in step 3.) is provided in **FIGURE 7**. This requires that the Bank app issued by the Customer's ASPSP supports providing an e-signed/authorised payment request as shown in step 3 in **FIGURE 7**.

In principle, it is possible to perform an ICT Transaction on Mobile Contactless without the Customer's ASPSP and the Mobile Contactless ICT Payment Application supporting an e-signed/authorised payment request. Customer authentication could alternatively be performed as shown in **FIGURE 5** and **FIGURE 6**. However, this way of performing Customer authentication for Mobile Contactless with Mobile ICT Payment Application is out of scope for this version of the Volume since it requires an internet connection of the Consumer Device during the ICT Transaction.

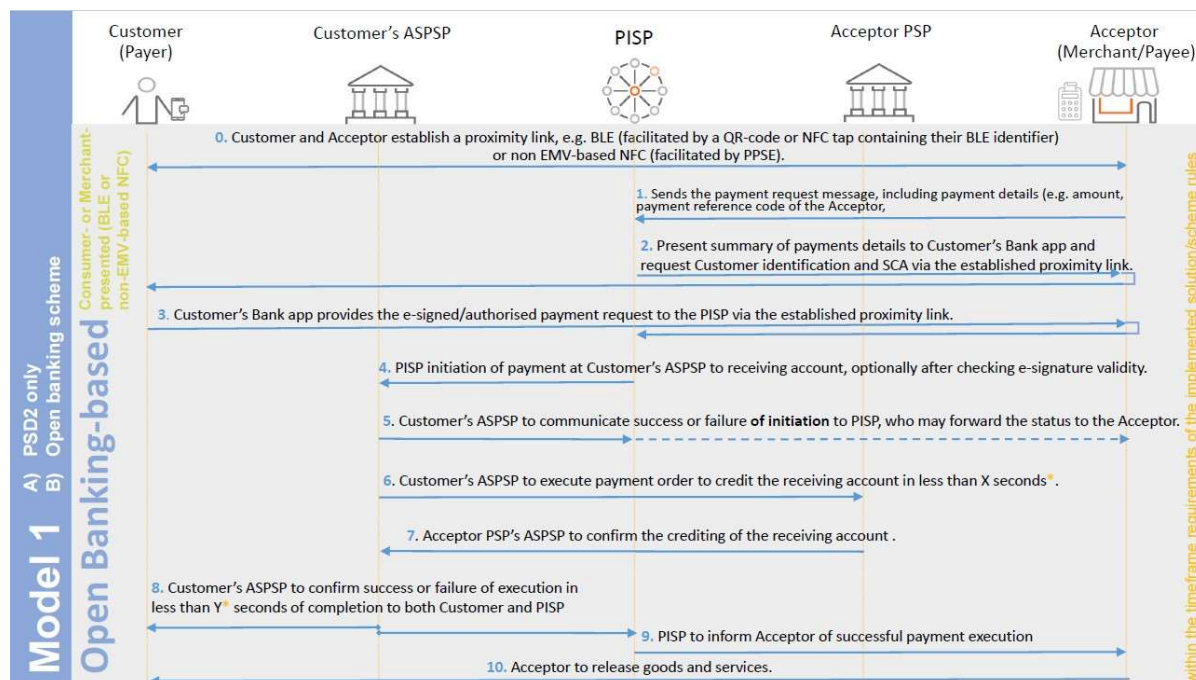


FIGURE 7: OPEN BANKING-BASED ICT TRANSACTION – MOBILE CONTACTLESS WITH MOBILE CONTACTLESS ICT APPLICATION

- Chip with Contact, Chip Contactless or Mobile Contactless - with EMV Card Payment Application**

EMV Card Payment Applications may also be used for ICT Transactions, e.g. by representing the customer's payment account (IBAN) as a tokenised PAN. Such ICT Transactions follow the POI EMV "Chip with Contact" and/or "Chip/Mobile Contactless" technology rails, rules and requirements for Application Selection and Payment Services that are configured for this particular ICT Payment Solution. The POI is to be configured to connect to the PISP (an Acquirer may be in the role of the PISP or Payment Intermediary).

An example of the ICT Transaction flow for a One-off Payment using EMV Contactless Acceptance Technologies is shown in **FIGURE 8:**

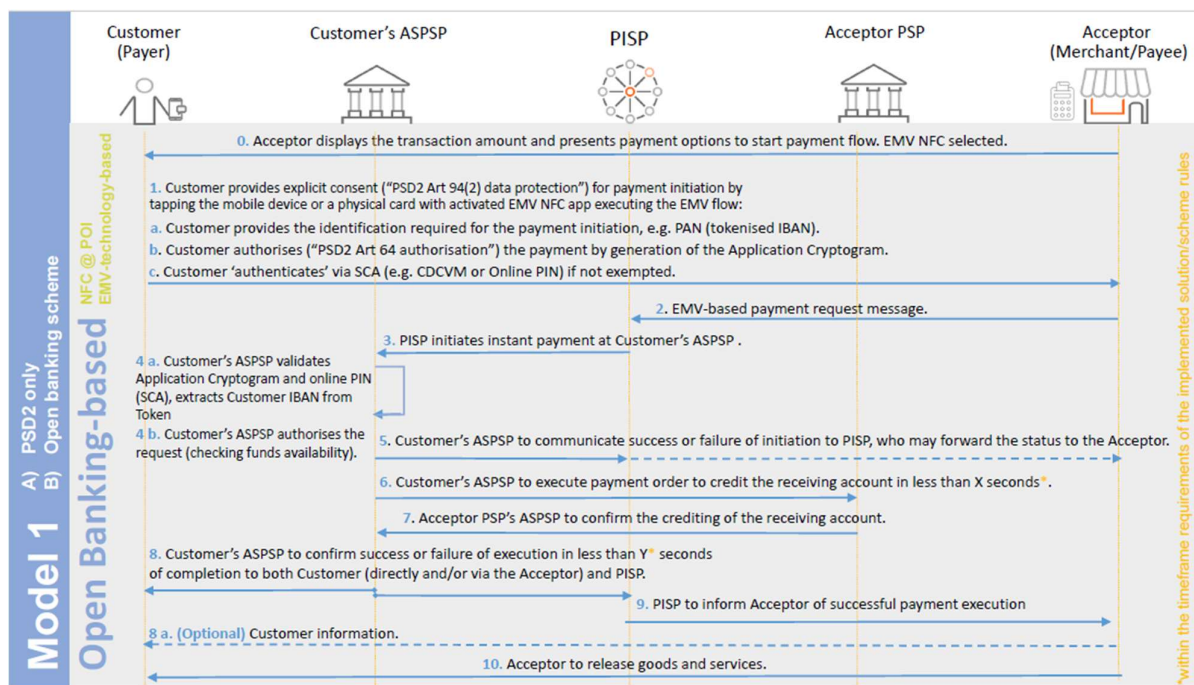


FIGURE 8: OPEN BANKING-BASED ICT TRANSACTION – CONTACT AND CONTACTLESS WITH EMV CARD PAYMENT APPLICATION

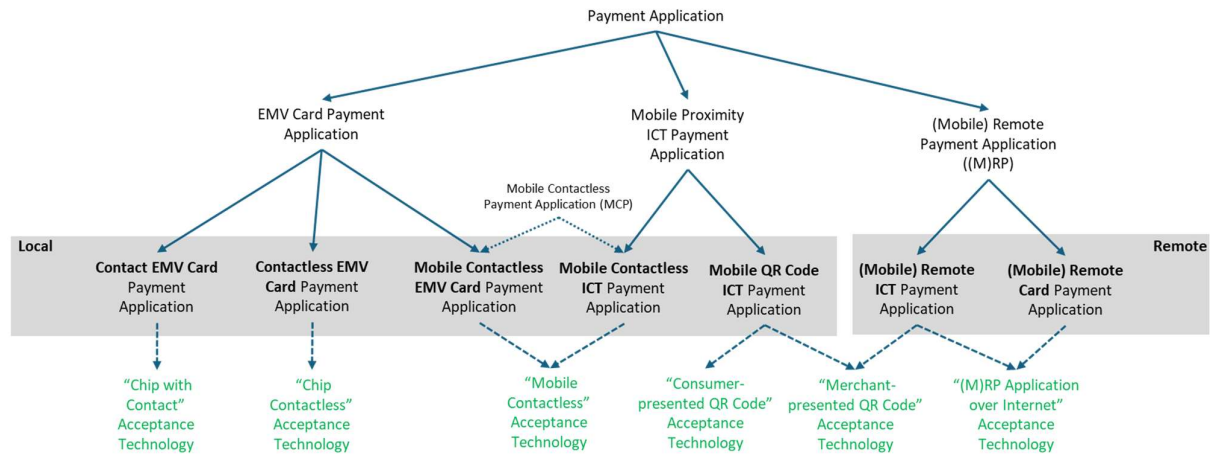
- **Other Acceptance Technologies**
(e.g., BLE, NFC Tags or other communication protocols) are out of scope of this version of the Volume.

ICT Transactions processed as shown in **FIGURE 5**, **FIGURE 6** and **FIGURE 7** are referred to as conventional ICT Transactions to distinguish them from ICT Transactions processed based on EMV technology as shown in **FIGURE 8**.

1.9 Overview of Payment Applications

While Payment Applications are not necessary to perform ICT Transactions, and Remote Card Transactions, the wide variety of payment options using Payment Applications can still create complexity.

The diagram below provides an overview of the different Payment Application types, across both Local and Remote environments, and illustrates how they map to the relevant Acceptance Technologies.


FIGURE 9: OVERVIEW OF PAYMENT APPLICATIONS

2 THE SPS VOLUME AND ITS BOOKS

2.1 Introduction to the “SEPA Payments Standardisation Volume”

This set of Books assembled into a version of the SEPA Payments Standardisation Volume (hereafter referred to as the “Volume”) builds historically on the EPC SEPA Cards Framework made available in March 2006 and has contributed, through the formulation of policy guidelines, to setting the foundations for the SEPA (Single Euro Payments Area) for payments and cash withdrawals. The ambition of the Volume is to set common foundations for better interoperability and for gradual convergence of the technical standards which underpin the payment value chain from end-to-end.

Achieving greater standardisation in the European payment world is a necessity going forward, yet a formidable challenge. When undertaking this task, a number of conflicting dimensions have to be reconciled such as:

- The service experienced by both Customers and Acceptors may not be disrupted. Greater standardisation must remain transparent to Customers and should not negatively affect their user experience.
- Retailers have significantly invested in, and deployed, POI equipment (point of interaction (POI) or point of sale (POS)) as well as related software applications. The depreciation deadlines of equipment up to now reflect individual decisions rather than any grand European vision.
- Equally retailers should not all be perceived as being the same. The different requirements of their multiple professions and sectors result in specificities which must be translated into the products they deploy.
- Vendors appreciate standardisation yet want also to be able to differentiate their product and services from each other, and take advantage of innovation, in order to compete in the marketplace.
- Policy makers and regulators harbour significant expectations from standardisation: economies of scale achieved thanks to standard equipment certified and deployable at European scale should increase choice and competition, foster innovation, decrease costs and make payments an even more attractive proposition.
- Finally, SEPA is not an “island”. Standards for payments are not decided only in Europe, and stakeholders in Europe are concerned about the interoperability beyond Europe’s borders of the solutions they propose and/or implement.

The Volume attempts to reconcile these challenges by offering all stakeholders a pragmatic approach:

1. It supplies a set of core functional and security requirements (“SEPA payment standards”) across the payment value chain to meet the objective for achieving harmonised Europe-

wide certifications and approvals. This includes principles and a framework for a payment standardisation ecosystem.

2. These SEPA payment standards will represent the foundation stones on which market participants will be able to develop detailed implementation specifications to meet the requisite needs of the various market segments whilst allowing for competition. It will be the responsibility of each specification provider to ensure that these implementation specifications are in line with the standards referred to above.

2.2 Scope and Objectives of EPSG Work on Payments Standardisation

2.2.1 Scope

The scope of EPSG's work on payments standardisation in general, and of the present Volume in particular, is the definition and description of SEPA Payment Standards for harmonising card payment and cash withdrawal services, for the benefit of all stakeholders in the SEPA region. Additionally, the Volume gives support to the market regarding the implementation of regulatory requirements, through careful analysis of new regulations and, where appropriate, updates to the Volume requirements.

For security and interoperability reasons, the expectation of the Volume is that all Card Present transactions in Europe are [EMV] based. Although referred to in some Books, Magnetic Stripe is not endorsed by the EPSG and is mentioned only for completeness.

2.2.2 Objectives

The Volume's objective is to deliver a consistent Customer and Acceptor experience through harmonised functional and security requirements for Payment Services within its scope.

It will also provide a Payment Standardisation Ecosystem - including a conformance verification Framework - which will enable Volume conformance to be evidenced.

The functional and security requirements and the payment standardisation ecosystem also include functional architecture, description of processing flows as well as use and definitions for data elements.

The Volume demonstrates commitment from the main stakeholders of the European payment industry, represented in the EPSG, to adopt and deliver a consistent Customer and Acceptor experience. The EPSG calls upon all other relevant parties throughout the payment value chain to also support, adopt and implement these SEPA Payment Standards in order to achieve a true SEPA for payments.

2.2.3 Impact on the Different Stakeholders

Stakeholders in payments are notably: schemes, vendors of cards, payment applications, and/or acceptance solutions, retailers, acquirers, processors, issuers, certification entities, cardholders and consumers.

Any stakeholder wishing to present themselves as Volume conformant will have to conform with the set of requirements relevant for its activity. However it remains any stakeholder's discretionary business decision to select which services or options it implements, depending also on e.g., the environment or business interest.

2.2.4 Implementation of the Volume and Monitoring

During the preparation of this version of the Volume, the EPSG experts from the various sectors worked to define a recommended implementation path for the standards described therein. In the future, the EPSG will work on defining processes to monitor the Volume conformance and implementation.

2.2.5 Implementation Specifications

The current version of the Volume does not include implementation specifications. The choice of implementation specifications in line with the Volume is up to the market. Stakeholders will continue to be free to develop and select implementation specifications which will facilitate innovation and differentiation and to ensure active competition in the market, and innovation. However it is expected that these implementation specifications when applying to SEPA will be in conformance with the Volume requirements.

2.3 Maintenance of the Books

2.3.1 The Volume, a Set of Books

The Volume is a set of Books. Currently it is composed of:

Book 1 - ***General Principles and Definitions***

Contents: Overview of the objective of the Volume, its contents and a glossary.

Book 2 - ***Functional Requirements***

Contents: Functional requirements for Payment Instrument and for POI (Point of Interaction) to process Payment Services

Book 3 - *Data Elements*

Contents: This Book covers the Data Element requirements, their usage and references and identifications to be used in the messages.

Book 4 - *Security*

Contents: Security requirements for data protection, Terminal to Acquirer Protocols, PIN, Cards (contact and contactless), Consumer Device, Terminals/POI, Payment Gateways, Hardware Security Modules [HSMs] security requirements.

Book 5 - *Conformance Verification Process*

Contents: Description of the EPSG Payment Standardisation Ecosystem and the conformance processes (labelling, certification and type approval)

Book 6 - *Best Practices for Implementation*

Contents: Implementation guidelines, both general and per payment context.

Book 7 - *Payment Processing Framework*

Contents: Payment Processing framework, i.e. 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.

Annex - *Tokenisation for SEPA Payments*

Contents: The requirements for the adoption and implementation of Tokenisation in the SEPA region, including references to Global standards.

2.3.2 Maintenance cycles

1. Individual Books may be reviewed in a single year cycle depending on the urgency.
2. The maintenance of the Volume is managed by the EPSG Secretariat, with an Expert Team dedicated to each Book. Participation in these teams is open but based on expertise on the topic of the related Book.
3. Each publication (Full set or individual Books) will include in its preparation phase, a formal public consultation process. Relevant details (e.g., Guidance for the completion of the comments form) will be made available on the EPSG public website.

2.3.3 Intellectual Property Rights

The entire right, title and interest in and to the copyright and all related rights in the Volume resides exclusively with the EPSG. Neither potential or actual users of this Volume, nor any other person

shall assert contrary claims, or use the Volume in a manner that infringes or is likely to infringe the copyright held by the EPSG in the Volume.

The Volume can be reproduced, redistributed and transmitted in unmodified form for non-commercial purposes by any interested party, as long as the EPSG as its source is acknowledged and provided that prior written approval has been given by the EPSG. This Volume and all reproductions shall display the following copyright notice: “© 2025 European Payments Stakeholders Group AISBL. All Rights Reserved.”

This Volume and any associated document is being offered without any warranty whatsoever, and in particular, any warranty of non-infringement is expressly disclaimed. Any use of this document shall be made entirely at the implementer's own risk, and neither European Payments Stakeholders Group AISBL (“EPSG”), nor any of its members, shall have any liability whatsoever to any implementer for any damages of any nature whatsoever, directly or indirectly, arising from the use of this volume, nor shall EPSG or any of its members have any responsibility for identifying any intellectual property rights.

3 REFERENCES, ABBREVIATIONS AND DEFINITIONS

3.1 References

NB: The last version of a document always applies, except when a specific one is mentioned.

[BSI TR-02102-1] Cryptographic Mechanisms: Recommendations and Key Lengths

[BSI TR-02102-2] Cryptographic Mechanisms: Recommendations and Key Lengths – Part 2: Use of Transport Layer Security (TLS)

[CPA] EMV® Integrated Circuit Card Specifications for Payment Systems, Common Payment Application Specification

[CBP] Regulation (EU) 2019/518 of the European Parliament and of the Council of 19 March 2019 amending Regulation (EC) No 924/2009 as regards certain charges on cross-border payments in the Union and currency conversion charges

[EAA] Directive of the European Parliament and of the Council on the approximation of the laws, regulations and administrative provisions of the Member States as regards the accessibility requirements for products and services (COM/2015/0615 final - 2015/0278 (COD))

[EBA 1] EBA/GL/2014/12 Final guidelines on the security of internet payments

[ECB] ECB/EuroSystem Assessment guide for the security of internet payments

[ECB 2] EBA/RC/2014/05 Final recommendations for the security of payment account access services

[EMD] Electronic Money Directive - Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision on the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC

[EMV] EMV® Integrated Circuit Card Specifications for Payment Systems, including the Specification Bulletins

[EMV 3DS] EMV® 3-D Secure Specifications

[EMV B1] EMV® Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements

[EMV B2] EMV® Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management

[EMV B3] EMV® Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification

[EMV B4] EMV® Integrated Circuit Card Specifications for Payment Systems, Book 4, Cardholder, Attendant, and Acquirer Interface Requirements

[EMV A] EMV® Contactless Specifications for Payment Systems, Book A, Architecture and General Requirements

[EMV B]	EMV® Contactless Specifications for Payment Systems, Book B, Entry Point Specification
[EMV C2 to C8]	EMV® Contactless Specifications for Payment Systems, Book C-2 to C-8, Kernel 2 to 8 Specification
[EMV E]	EMV® Contactless Specifications for Payment Systems, Book E, Security and Key Management
[EMV CDCVM BP]	EMV® Consumer Device Cardholder Verification Method— Best Practices, March 2019
[EMV CDCVM SR]	EMV® Consumer Device Cardholder Verification Method Security Requirements
[EMV CMP CM]	EMV® Contactless Mobile Payment, Payment Card Management, White Paper
[EMV CMP SE]	EMV® Contactless Mobile Payment – PPSE and Application Management for Secure Element
[EMV GB60]	EMV® General Bulletin No. 60, Second Edition, July 2024
[EMV L1 CL]	EMV® Level 1 Specifications for Payment Systems, EMV Contactless Interface Specification
[EMV L1 CT]	EMV® Level 1 Specifications for Payment Systems, EMV Contact Interface Specification[EMV SBMP]EMV® Mobile Payment, Software-based Mobile Payment Security Requirements
[EMV SRC]	EMV Secure Remote Commerce Specifications and related documents, including API, JavaScript SDK, Version Management, Data Dictionary, and User Interface Guidelines and Requirements. [EMVCo-FW] EMV® Payment Tokenisation Specification – Technical Framework
[EN AR]	EN 301 549 V3.2.1 (2021-03) Accessibility requirements for Information and Communication Technology products and services
[EPC Crypto]	EPC342-08: Guidelines on algorithms usage and key management
[EPC Mobile WP]	EPC492-09: White paper Mobile Payments
[EPC MCP IIG]	EPC178-10: Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines
[EPC MSCT IG]	EPC269-19: Mobile Initiated SEPA (Instant) Credit Transfer Payments and Technical Interoperability Guidance (MSCT IG)
[EPC PS]	EPC343-08: EPC Privacy shielding for PIN entry
[EPC SCT Inst]	EPC004-16: SEPA Instant Credit Transfer – Scheme Rulebook
[EPC SQR]	EPC024-22: Standardisation of QR-codes for Mobile Initiated SEPA (Instant) Credit Transfers
[EPC TRP]	EPC088-22: EPC Guidance Document Improve Transparency for Retail Payment End-Users
[ETSI TS 119 312]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[ETSI TS 119 495] Certificates supporting PSD2 (Qualified Certificates for eIDAS)

[FIDO] fidoalliance.org

[FIPS 140-2] Security Requirements for Cryptographic Modules + Annexes

[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 (General Data Protection Regulation)

[IFR] Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions - J.O. May 2015

[IPR] Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 on instant credit transfers in euro

[ISO/IEC 18033] Information security — Encryption algorithms

[ISO/IEC 7810] Identification cards - physical characteristics

[ISO/IEC 7811] Identification cards - Recording technique

ISO/IEC 7811-1: Embossing

ISO/IEC 7811-2: Magnetic stripe - Low coercivity

ISO/IEC 7811-6: Magnetic stripe - High coercivity

ISO/IEC 7811-7: Magnetic stripe - High coercivity, high density

ISO/IEC 7811-8: Magnetic stripe - Coercivity of 51,7 kA/m (650 Oe)

ISO/IEC 7811-9: Tactile identifier mark

[ISO/IEC 7812] Identification cards - Identification of issuers

ISO/IEC 7812-1 Numbering system

ISO/IEC 7812-2 Application and registration procedures

[ISO/IEC 7813] Information technology - Identification cards - Financial Transaction cards

[ISO/IEC 7816-4] Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange

[ISO/IEC 7816-5] Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers

[ISO 8583] Financial transaction card originated messages - interchange message specifications

ISO 8583-1: Messages, data elements, code values

ISO 8583-2: Application and registration procedures for Institution Identification Codes (IIC)

ISO 8583-3: Maintenance procedures for messages, data elements and code values.

- [ISO 9564] Financial services - Personal Identification Number (PIN) management and security.
ISO 9564-1: Basic principles and requirements for card-based systems
ISO 9564-2: Approved algorithms for PIN encipherment
ISO/TR 9564-4: Guidelines for PIN handling in open networks
- [ISO/IEC 9797-1] Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher
- [ISO/IEC 14443] Information technology - Identification cards -- Contactless integrated circuit cards - Proximity cards
ISO/IEC 14443-1: Physical characteristics
ISO/IEC 14443-2: Radio frequency power and signal interface
ISO/IEC 14443-3: Initialization and anti-collision
ISO/IEC 14443-4: Transmission protocol
- [ISO/IEC 15408] Information technology - Security techniques - Evaluation criteria for IT security
ISO/IEC 15408-1: Introduction and general model
ISO/IEC 15408-2: Security functional components
ISO/IEC 15408-3: Security assurance components
- [ISO 11568] Financial services — Key management (retail)
- [ISO/IEC 18004] Information technology - Automatic identification and data capture techniques - QR-code bar code symbology specification
- [ISO 20022] Financial Services - Universal financial industry message scheme
ISO 20022-1: Metamodel
ISO 20022-2: UML profile
ISO 20022-3: Modelling
ISO 20022-4: XML schema generation
ISO 20022-5: Reverse engineering
ISO 20022-6: Message transport characteristics
ISO 20022-7: Registration
ISO 20022-8: ASN.1 generation
- [ISO 20038] Banking and related financial services — Key wrap using Advanced Encryption Standard (AES)
- [ISO 5201] Financial services — Code-scanning payment security
- [OMTP1] OMTP Trusted Environment (www.gsma.com)
- [OMTP2] OMTP Advanced Trusted Environment (www.gsma.com)
- [OMTP3] OMTP Security Threats on Embedded Consumer Devices (www.gsma.com)

[PCI ATM PIN]	Payment Card Industry Transaction Security Point of Interaction Security Requirements (PCI PTS POI), Information Supplement: ATM Security Guidelines
[PCI PIN]	Payment Card Industry PIN Security Requirements and Testing Procedures
[PCI PTS]	Payment Card Industry PIN Transaction Security
[PCI P2PE]	Payment Card Industry Point to Point Encryption
[PCI DSS]	Payment Card Industry Data Security Standard
[PCI PA-DSS]	Payment Card Industry Payment Application Data Security Standard
[PISA]	Eurosystem oversight framework for electronic payment instruments, schemes and arrangements
[PSD]	Payment Services Directive - Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market
[PSD2]	Payment Services Directive 2 - Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015
[RFC 5652]	Cryptographic Message Syntax (CMS)
[RFC 6749]	The OAuth 2.0 Authorization Framework
[RFC 8446]	The Transport Layer Security (TLS) Protocol Version 1.3
[RTS SCA/CSC]	Commission Delegated Regulation (EU) 2018/389 of 27 November 2017, supplementing [PSD2] with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

3.2 Abbreviations

Acronym	Standing for	Acronym	Standing for
A2I	Acquirer to Issuer	CDA	Combined DDA/Application Cryptogram Generation
AAC	Application Authentication Cryptogram	CDCVM	Consumer Device CVM
AAM	Active Account Management	COTS	Commercial Off-The-Shelf
ACS	Access control service	CP	Contactless Payment
AID	Application Identifier	CPA	Card Payment Application
ATC	Application Transaction Counter	CPoC	Contactless Payments on COTS
ATICA	Acquirer To Issuer Card Messages	CPS	Card Payment Scheme
ATM	Automated Teller Machine	CSC	Card Security Code
AVS	Address Verification Service	CSM	Clearing and Settlement Mechanism
BDH	Blinded Diffie-Hellman	CVM	Cardholder Verification Method
BDHLA	Blinded Diffie-Hellman Local Authentication	DCC	Dynamic Currency Conversion
BIN	Bank Identification Number	DCF	Digital Card Facilitator
C2T	Card to Terminal	DDA	Dynamic Data Authentication
CA	Certification Authority	DPA	Digital Payment Application
CAM	Card Authentication Method	DTMF	Dual Tone Multi Frequency
CAPE	Card Payment Exchange	ECC	Elliptic Curve Cryptography
CAT	Cardholder-Activated Terminal	EPSG	European Payments Stakeholders Group
CB	Certification Body	EAL	Evaluation Assurance Level
CC	Common Criteria	EMV	Europay Mastercard Visa
CCD	Common Core Definition		

EPA	Embedded Payment Application	MCC	Merchant Category Code
EPC	European Payments Council	MCP	Mobile Contactless Payment
EPP	Encrypting PIN Pad	MIT	Merchant Initiated Transaction
EULA	End User License Agreement	MNO	Mobile Network Operator
fDDA	Fast Dynamic Data Authentication	MOTO	Mail Order - Telephone Order
GSMA	GSM Association	MRP	Mobile Remote Payment
HMAC	Hash-based MAC	NFC	Near-Field Communications
HPP	Hosted Payment Page	OS	Operating System
HSM	Hardware Security Module	OTA	Over The Air
ICC	Integrated Circuit(s) Card	OTP	One Time Password
ICT	Instant Credit Transfer	P2P	Point-to-Point (Encryption)
ID&V	Identification and Verification	PAN	Primary Account Number
IF	Interchange Fee	PAR	Payment Account Reference
IIN	Issuer Identification Number	PCI	Payment Card Industry
IoT	Internet of Things	PED	PIN Entry Device
IFR	Interchange Fee Regulation	PII	Personally Identifiable Information
ISO	International Organisation for Standardisation	POI	Point of Interaction
JSON	JavaScript Object Notation	PPSE	Proximity Payment System Environment
JWE	JSON Web Encryption	PSD	Payment Services Directive
JWS	JSON Web Signature	PSD2	Payment Services Directive 2
KBA	Knowledge Based Authentication	PSE	Payment System Environment
KCV	Key Check Value	PSP	Payment Service Provider
MAC	Message Authentication Code		

PSU	Payment Service User	SRCPI	Secure Remote Commerce Participating Issuer
PTS	PIN Transaction Security	SRED	Secure Read and Exchange of Data
PVV	PIN verification value	SSL	Secure Socket Layer
REE	Rich Execution Environment	T2A	Terminal to Acquirer
RP	Remote Payment	TEE	Trusted Execution Environment
REE	Rich Execution Environment	TLS	Transport Layer Security
RNG	Random Number Generator	TOE	Target OF Evaluation (CC)
RSA	Rivest–Shamir–Adleman cryptography	TPM	Trusted Platform Module
SCA	Strong Customer Authentication	TPP	Third Party Provider
SCD	Secure Cryptographic Device	TRSM	Tamper-resistant security module
SCRIP	Secure Card Reader PIN	TSP	Token Service Provider
SCT Inst	SEPA Instant Credit Transfer	TSM	Trusted Services Management
SDA	Static Data Authentication	UI	User Interface
SE	Secure Element	UID	Unique Identifier
SEPA	Single Euro Payments Area	UPT	Unattended Payment Terminal
SMS	Short Message Service	XDA	Extended Data Authentication
SPoC	Software-based PIN entry on COTS		
SPS	SEPA Payments Standardisation		
SRC	Secure Remote Commerce		
SRCI	Secure Remote Commerce Initiator		

1 3.3 Definitions

- 2 This section contains all the definitions of terms used throughout the volume, except those
3 regarding Tokenisation, which are contained in the *Annex - Tokenisation for SEPA Card Payments*.
- 4 A number of definitions originate from [IFR]. These are identified by the reference number in
5 brackets used in Article 2 of the Regulation.
- 6 For example: (1) ‘acquirer’ means a payment service provider contracting with a payee to accept
7 and process card-based payment transactions, which result in a transfer of funds to the payee.

Concept	Definition
3-D Secure	The 3-D Secure authentication protocol is based on a three-domain model where the Acquirer Domain and Issuer Domain are connected by the Interoperability Domain for the purpose of authenticating a Cardholder or to provide identity verification and account confirmation during an e- or m-commerce transaction.

8 A.

AAC	Application Authentication Cryptogram, which is a Cryptogram generated by a Card Application. See [EMV B2].
Acceptance	In the field of payments, it refers to the process whereby a particular Payment Brand is accepted by a terminal, acceptor or other entity.
Acceptance Environment	Environment where the Payment transaction is conducted in the Acceptor’s domain. This Volume describes two Acceptance Environments: • Physical POI • Remote POI
Acceptance Technology	The source of and method by which Card Data is obtained. It may also include other processes.
Acceptor	A retailer or any other entity, firm or corporation that enters into an agreement with an Acquirer to accept Card Transactions as payment for goods and services (including cash withdrawals) and displays the Schemes acceptance logo. The Payment will result in a transfer of funds in their favour. The Acceptor may also be an entity operating as a Marketplace, provided that this is the entity that enters into an agreement with the Acquirer. Sometimes also referred to as Merchant. Note: For payments, Acceptor is defined as "Payee" in [PSD2].

Acceptor Initiated Transaction (AIT)	A Payment Transaction initiated by the Acceptor based on stored Account Data without the Customer interacting in the transaction process, i.e. an MIT or a transaction where the Acceptor is the payer. Examples of Payment Services that may be processed as AIT are: Pre-Authorisation Services, No-Show, subsequent transactions of Instalment Payments and Recurring Payments (processed as MITs), or Refund and Original Credit (processed as AIT where the Acceptor is the Payer).
Acceptor Name	The name of the Acceptor by which the Customer recognises the Acceptor. It is shown on displays to the Customer, printed on receipts or statements and is also used to identify trusted beneficiaries. For the purpose of Remote Transactions, it is unique for an individual Acceptor, at least at Acquirer level.
(Customer or Acceptor) Account Data	A data set allowing the identification of the (Customer or Acceptor) Payment Account used to perform Payment Services.
Account Data Retrieval	A Function which allows the POI or the PISP to retrieve Customer Account Data. For Card Transactions, this Function is used at the POI to retrieve Card Data.
Account Servicing Payment Service Provider	A Payment Service Provider providing and maintaining a payment account for a payer.
Account Takeover (Fraud)	A form of fraud where someone accesses another's personal banking service and changes the address and passcode on someone else's account, using stolen or fake identification documents.
Acquirer	A Payment Service Provider (PSP) contracting with an Acceptor to accept and process Card or ICT Transactions, resulting in a transfer of funds. <i>Note: In some cases, the Acquirer may also be an Acceptor. In the context of Payments messages of ISO 20022, the term Creditor Agent encompasses the Acquirer role.</i>
Acquiring	The service performed by an Acquirer.
Activated/Deactivated	Indicates that a Payment Service or a Function or an Acceptance Technology is supported (i.e. implemented) in the POI Application and is configured to be available or not for transaction processing.
Additional Authentication Device	A Chip Card accepting PED which may or may not be connected to the consumer device and which includes an EMV Card Authentication Application.
Address Data	Data entered and transmitted for MOTO transactions consisting of the numeric characters from the address.
App Kernel	A specific application that runs on the COTS device operating system needed to accept and process a Card Based Payment Transaction.

Application Cryptogram [AC]	A cryptogram generated by the Card Payment Application in response to a GENERATE AC command.
Application Identifier (AID)	A Data Element specified by ISO/IEC 7816-5 which in the context of the Volume encodes a unique identifier of a Payment Application
Application Profile	An Application Profile determines the configurable parameters which are used to process a Payment Service by the POI Application.
Application Programming Interface (API)	A specified interface within a software module that provides third parties (e.g. application developers) with a well-defined access to the functionalities of this software module.
Approval Body	A body which performs Type Approval.
ARQC	Authorisation ReQuest Cryptogram, which is a Cryptogram generated by a Card Application to request an online authorisation for the transaction. See [EMV B2].
Asymmetric Key Pair	Two mathematically related cryptographic keys, a public key and a private key, which, when used with the appropriate public key algorithm, can allow the secure exchange of information and message authentication, without the secure exchange of a secret.
ATICA	Acquirer To Issuer Card messages. A set of messages based on the ISO 20022 standard in the Acquirer to Issuer domain intended to support interoperability. During preparation of the Volume the ATICA messages had not been finalised.
ATM Cash Withdrawal	A service which allows the cardholder to withdraw cash at a cash dispensing device, i.e. an ATM. Also called “ATM Cash Disbursement”.
Attended Physical POI	An attendant (an agent of the Acceptor) is present at the Physical POI.
Authentication	The provision of assurance of the claimed identity of an entity or of data origin.
Authentication Application	Software or equivalent loaded on a Card or Consumer Device used to support the Authentication process in Payment Transactions. These are: • EMV Card Authentication Application (Physical Card), • (Mobile) Authentication Application (Consumer Device).
Authentication Code	In the context of the Volume, the Authentication Code is a unique value that links a transaction to a specific amount and to a specific Acceptor. Generally, it is based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements (e.g. a customer device or a physical card), as long as the security requirements are fulfilled.

Authentication Method	The method used for the authentication of an entity or data origin. Authentication Methods may be combined to perform SCA.
Authenticator	A security factor used in an authentication method such as: - Something you know, such as a password or passphrase - Something you have, such as a token device or smart card - Something you are, such as a biometric.
Authenticity	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.
Authorisation	A Function which allows the Acceptor to make a decision to proceed with a Payment Service or not, e.g. after receiving or not a payment guarantee. It can be processed offline by an EMV Card Payment Application or online to the Acquirer/Issuer or their agents. If processed online, the Authorisation may also result in a partial approval.
Automated Teller Machine (ATM)	An Unattended Physical POI that has online capability, accepts PINs, which allows authorised users, typically using machine-readable plastic cards, to withdraw cash from their accounts and/or access other services (e.g., to make balance enquiries, transfer funds or deposit money).

9 B.

Balance Enquiry	A service which allows the Customer to request information about their account balance.
Blinded Diffie-Hellman (BDH)	The Blinded Diffie-Hellman (BDH) key agreement is a variant of the Elliptic Curve Diffie-Hellman protocol. See [EMV E] for details.
Blinded Diffie-Hellman Local Authentication (BDHLA)	An ECC-based type of dynamic Offline Data Authentication where a dedicated cryptogram (built by an EMV Card Payment Application using transaction data) is authenticated locally by the POI Application using the session key for integrity obtained during a prior Blinded Diffie-Hellman key agreement. See [EMV E], where this method is referred to as “Local Authentication”.
BIN	Bank Identification Number (also referred to as IIN). It is the first part of the PAN, Primary Account Number, identifying the Issuer of the card. See ISO/IEC 7812 for more information.
Biometric	An identity verification method of a Customer based upon one or more intrinsic physical characteristics of that Customer, either biological and physiological (e.g. fingerprint, iris, face, vein and voice) or behavioural (e.g. signature dynamics, typing patterns) characteristics. For the Volume, only automatically verifiable biological and physiological Biometrics are presently considered.

Biometric Capture Device	A secure device that allows the capture of Biometric data from the Customer at the POI
Biometric Data	Physical or physiological (e.g. fingerprint, iris, face, vein and voice), or behavioural (e.g. signature dynamics, typing patterns) characteristics of a Customer/individual, which allow or confirm the unique identification of that Customer/individual. Biometric Data is Sensitive Personal Data. The Personal Data Processing of the Biometric Data must be performed in accordance with the specific regime provided in [GDPR].
Biometrics on Consumer Device	A Cardholder Verification Method where the biometric data is captured on the Consumer Device and verified against a biometric reference template by an application on the Consumer Device. Biometrics on Consumer Device is a type of CDCVM.
Biometrics via Sensor on Card	A Cardholder Verification Method where the biometric data is captured on a sensor embedded in the Physical Card and verified against a biometric reference template stored on the card.
Business Day	A day on which the relevant payment service provider of the Customer or the Payment Service Provider of the Acceptor involved in the execution of a payment transaction is open for business as required for the execution of a payment transaction.

10 C.

Cancellation (Payment Service)	A Payment Service which allows the Acceptor to cancel a previously approved transaction. Cancellation should only occur before the transaction is cleared to the issuer. It is sometimes called “Manual reversal”. Its primary function is to prevent the transaction being processed and to readjust the Customer Available Funds.
Cancellation (Technical Process)	A process that can be instigated by the Customer or the Acceptor at a POI to nullify a transaction, prior to Data Capture to the Acquirer typically using a “cancel” button on the POI.
Card	A Physical Card or a Virtual Card.
Card Account	A Payment Account to which a Card is issued and which is identified by Card Data.
Card Acquirer	See Acquirer.
Card Activation	An operation to activate a new card prior to usage or during first card usage.

Card Application	An EMV Card Payment Application or a (Mobile) Remote Card Payment Application.
Card Authentication	A Function by which an EMV Card Payment Application is authenticated by the POI Application (Offline Data Authentication), by an Additional Authentication Device and/or by the Issuer (EMV Online Authentication).
Card Based Language Selection (Optional)	A Function by which the language can be selected for on-screen dialogues or print-outs.
Card Data	Account Data identifying a Card Account.
Card Data Retrieval	A Function which allows the POI to retrieve Card Data.
Card Funds Transfer	A service which allows the Cardholder to use their card to transfer funds to and from their card account and where neither of the involved entities acts as a card acceptor (or professional payee). Sometimes referred to as 'Card Electronic Transfer'
Card Id Theft (Fraud)	A form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name.
Card Issuer	See Issuer.
Card Present	Transaction based on card-related information with the Card being physically presented to the Acceptor.
Card Not Present (CNP)	Transaction based on card-related information without the Card being physically presented to the Acceptor e.g., No-Show, MOTO, e- & m-Commerce.
Card On File	Specific case of Stored Account Data where Card Data is securely stored within the Acceptor's domain.
Card Pick-Up Advice	This Pick-up Advice service purpose is to inform the issuer that the card has been confiscated.
Card Processing Framework	A set of business principles and requirements applying to actors of the card payment value chain (e.g., Schemes, Processors, Acquirers, Issuers) in order to further facilitate an open and transparent market.
Card Reader	Data input device that reads data from a card-shaped storage medium.

Card Security Code (CSC)	A data element that uses secure cryptography to protect the integrity of the card. The code differs depending on the payment channel. There is a CSC on the Magnetic Stripe, a different one in the chip and a different one again when the payment is contactless. The CSC is also the last three or four digits of the number printed on the reverse of the card (usually found on the signature strip). These code values help validate two things: The customer has the credit card in his/her possession. The card account is legitimate. The Card Security Code can be static or dynamic. For the latter, the Card Security Code can be generated by the chip of the card (for physical cards only) or be generated or delivered by other means.
Card Transaction	A Payment Transaction using a Payment Card based Payment Instrument.
Card Validity Check	A service which allows the validity of the card to be checked. This transaction has no financial impact on the card account. Can also be referred to as a Card Account Status Check.
Cardholder	A Customer to whom a Card Application has been issued, or one who has been authorised to use the Card Application.
Customer Available Funds	The funds available for use by the Customer, taking into account the hold placed on the funds in respect of amount(s) authorised but not yet settled. Also referred to as "Open-to-Buy".
Cardholder Present	During the transaction, the Cardholder is present at the card Acceptor's premises or at an Unattended Terminal.
Cardholder Verification	Function used to verify whether the person using the payment application is the legitimate cardholder. Depending on the CVM, this function may be used as a factor towards SCA.
Cardholder Verification Method (CVM)	A method used to perform Cardholder Verification. Examples include Signature, PIN or No CVM Required.
Cash Advance (Attended)	A Payment Service at an attended POI which enables a Customer to receive cash against the open-to-buy funds on the account. POS cash advances are restricted to specific environments e.g., T&E acceptors and financial institutions. Also called Cash Disbursement.

Cash Deposit	A Payment Service which allows the Customer to deposit cash to their own account(s). It can take place • Either at a counter; • Or at an attended or unattended POI.
Cashback	See Payment with cashback.
Cashback Amount	See Payment with cashback.
Category of Card	A debit, credit, commercial or prepaid card, as defined in the [IFR]: IFR Art 10 §5
Certificate	Official attestation issued by a Certification Body that a Product or Solution has been successfully evaluated and demonstrated to be compliant with a given Implementation Specification.
Certification	The process of issuing a Certificate by a Certification Body following the successful assessment of the evaluation and/or test reports to attest the compliance of a given payment component (POI, card, etc.) with a given set of requirements and specifications. The Certification process is based on evaluations or tests performed by Security Evaluators and Test Laboratories, recognised and accredited by the Certification Body.
Certification Authority (CA)	Trusted third party that establishes a proof that links a public key and other relevant information to its owner using a Public Key Certificate.
Certification Body (CB)	The organisation reviewing the output of the evaluation process and issues a Certificate to attest that a Card, POI or any other payment component meets the given set of 'requirements' and 'implementation specifications'.
Charge Card	A card enabling its holder to make purchases and/or withdraw cash and have these transactions charged to an account held with the card issuer, up to an authorised limit. The balance of this account is then settled according to conditions agreed between the Card Issuer and the Cardholder. This type of Card is sometimes referred to as a 'Deferred Debit Card' or 'Delayed Debit Card'. According to the [IFR], these types of Card do fall under the category of 'Credit Card'.
Chargeback	A Function initiated by the Issuer requesting the Acquirer to credit the Issuer for the amount in question of a given transaction.

Chip Card (Smart Card)	A carrier into which one or more integrated circuits are inserted to perform processing and memory functions and which supports the contact interface and complies with [EMV L1 CT] (referred to as Contact Chip Card) and/or supports the contactless interface and complies with [EMV L1 CL] (referred to as Contactless Chip Card). A Chip Card which supports the contact and contactless interface is referred to as Dual Interface Card. A Contact Chip Card as well as a Dual Interface Card complies with [EMV L1 CT] and must be of the ID 1 form factor (as defined in ISO/IEC 7810). A Contactless Chip Card which does not support the contact interface may be of the ID 1 form factor (as defined in ISO/IEC 7810), a key fob, or another Form Factor. Note that a Mobile Device is not considered as Chip Card, even if it supports the contactless interface and complies with [EMV L1 CL]. The integrated circuits, also referred to as the "chip", carry an EMV Card Payment Application or EMV Card Authentication Application or both, which contains payment card data including but not limited to data equivalent to the Magnetic Stripe data. Also referred to as Smart Card.
Chip Contactless	An Acceptance Technology where Account Data is retrieved from the chip of a Chip Card over the contactless interface compliant with [EMV L1 CL]. In this case, the Chip Card is a Contactless Chip Card or a Dual Interface Card and may be of the ID 1 form factor (as defined in ISO/IEC 7810), a key fob, or another Form Factor.
Chip with Contact	An Acceptance Technology where Card Data is retrieved from the chip of a Chip Card over the contact interface compliant with [EMV L1 CT]. In this case the Chip Card is a Contact Chip Card or a Dual Interface Card and must be of the ID 1 form factor (as defined in ISO/IEC 7810).
Choice of Application	See article 8 as well as recital 40 of the IF Regulation [IFR]
Clearing	The process of exchanging financial transaction details between an Acquirer and an Issuer to facilitate both the posting of transactions to Customer's accounts and the reconciliation of an institution's settlement position.
Cleartext	See Plaintext.
Click to Pay Icon	A visual representation that identifies that SRC is available to the Customer.
Co-Badging	(31) 'co-badging' means the inclusion of two or more payment brands or payment applications of the same brand on the same card-based payment instrument;

Co-Branding	(32) 'co-branding' means the inclusion of at least one payment brand and at least one non-payment brand on the same card-based payment instrument;
Combined Data Authentication (CDA)	An RSA-based type of dynamic Offline Data Authentication where an EMV Card Payment Application combines the generation of a cryptographic value (dynamic signature) with the generation of an Application Cryptogram, for the POI Application to verify that it originates from a valid card. See [EMV B2].
Commercial Trade Name	The Acceptor Name as known and recognised by the Customer.
Common Core Definition (CCD)	CCD describes a minimum common set of card application implementation options, card application behaviours, and data element definitions sufficient to accomplish an EMV transaction. CCD is not a functional application specification.
Common Criteria (CC) Evaluation	The Common Criteria was developed through a combined effort of six countries: the United States, Canada, France, Germany, the Netherlands, and the United Kingdom. As an international standard (ISO/IEC 15408), it enables an objective evaluation to validate that a particular product or system satisfies a defined set of security requirements. Although the focus of the Common Criteria is evaluation, it presents a standard that should be of interest to those who develop security requirements.
Common Payment Application (CPA)	A functional specification for an EMV Card Payment Application that complies with the CCD requirements, and defines implementation options and Card Application behaviours.
Completion	A Function which provides information on how the transaction was completed. It includes all or some of the following steps: • Complete the transaction for the Payment Application • Inform Customer, Attendant and/or Acquirer about the result of the transaction • Deliver a receipt to Customer and/or Attendant
Compliance	Adherence of Products and Solutions to detailed specifications.
Commercial card	(6) 'commercial card' means any card-based payment instrument issued to undertakings or public sector entities or self-employed natural persons which is limited in use for business expenses where the payments made with such cards are charged directly to the account of the undertaking or public sector entity or self-employed natural person;

Consumer Device	An internet and/or NFC capable device used by the Customer to conduct Payment Services. It is either • a Mobile Device used for Mobile Contactless, Mobile QR Code or Mobile Remote Transactions, • An Electronic Device used for Remote Transactions It can be a carrier of Credentials or a Payment Application. It may include a user interface that enables the Customer to enter data.
Consumer Device Cardholder Verification Method (CDCVM)	Consumer Device Cardholder Verification Method is a form of CVM where the comparison of the method captured is compared with reference data on a Consumer Device itself The types of CDCVM defined in the Volume are: • Biometrics on Consumer Device • Offline Mobile Code • Offline Personal Code
Consumer Device with Browser over Internet	An Acceptance Technology for performing a (Mobile) Remote Payment transaction using the standard internet browser of the Consumer Device.
Consumer Device with Dedicated Application over Internet	An Acceptance Technology for performing a (Mobile) Remote Transaction using a dedicated application (e.g. a merchant application) on the Consumer Device.
Consumer-presented QR Code	Acceptance Technology where a QR Code is presented by the Customer, usually on their Mobile Device, and scanned by the Acceptor. The QR Code is calculated on data associated with the Customer or their Account.
Contact EMV Card Payment Application	An EMV Card Payment Application stored on a Physical Card supporting transaction processing for the "Chip with Contact" Acceptance Technology.
Contact (Payment) Transaction	A Payment Transaction processed using the Chip with Contact Acceptance Technology.
Contactless	If it is not necessary to distinguish the Payment Device in use, the term "Contactless" is used to refer to both Acceptance Technologies, the Chip Contactless Acceptance Technology and the Mobile Contactless Acceptance Technology, because they are both implementations of [EMV L1 CL] and communicate and behave the same.
Contactless (Payment) Transaction	A Payment Transaction processed using the Chip Contactless Acceptance Technology or the Mobile Contactless Acceptance Technology.
Contactless EMV Card Payment Application	An EMV Card Payment Application stored on a Physical Card supporting transaction processing for the "Chip Contactless" Acceptance Technology.
COTS Device	A publicly available Mobile Device (e.g., smartphone or tablet) and associated operating system designed using commercially available components that can facilitate card based payments but was not specifically designed for that purpose.

COTS Solution	A COTS solution is made up of the following components: - COTS Device - POI Application on the COTS Device - Back-end monitoring system - SCRP (where necessary)
COTS System Baseline	Summary of permitted COTS Device versions of hardware and firmware to be used as part of a COTS Solution submitted by the solution provider.
Counterfeit Card (Fraud)	A card that has been fraudulently manufactured, embossed or encoded to appear to be genuine but which has not been authorised by a card Scheme or issued by a member. A card originally issued by a member but subsequently altered without the issuer's knowledge or consent.
CPS Governance Authority	The Card Payment Scheme actor who is accountable for the overall functioning of the CPS and its coherence; it should ensure that all other actors follow the rules and apply relevant measures. The CPS standards allocate responsibility directly to the governance authority. The CPS rules may allow delegation of some of these responsibilities to other actors of the CPS. The governance authority should clearly define such cases and ensure that the choices of the other actors of the CPS are compliant with the overall CPS standards. The governance authority could be a specific organisation or entity or be represented by decision-making bodies of cooperating schemes.
Credit Card (Card With A Credit Function)	(34) 'credit card' means a category of payment instrument that enables the payer to initiate a credit card transaction;
Credit Card transaction	(5) 'credit card transaction' means a card-based payment transaction where the amount of the transaction is debited in full or in part at a pre agreed specific calendar month date to the payer, in line with a prearranged credit facility, with or without interest;
Cross-Border Payment Transaction	(8) 'cross-border payment transaction' means a card-based payment transaction where the issuer and the acquirer are located in different Member States or where the card-based payment instrument is issued by an issuer located in a Member State different from that of the point of sale;
Cryptographic Algorithm	A mathematical function that is applied to data to ensure confidentiality, data integrity and/or authentication. A cryptographic algorithm, using keys, can be symmetric or asymmetric. In a symmetric algorithm, the same key is used for encryption and decryption. In an asymmetric algorithm, different keys are used for encryption and decryption. The result from applying a cryptographic algorithm to a piece of data that can be used to hide the data, or to produce a digital signature to verify the origin and integrity of the data.
Cryptographic Key	The numeric value entered into a cryptographic algorithm that allows the algorithm to encrypt or decrypt a message.

Cryptographic Zone	The technique of using unique keys for communication between two organisations is referred to as zone encryption. A cryptographic zone defines a range for which a specific key is used.
Cryptography	Discipline that embodies principles, means, and mechanisms for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use.
Customer	Economic agent (natural or legal) buying goods or services and using Payment Services.
Customer Present	Customer being present to participate in performing a transaction.
CVM List	An issuer-defined list in the chip card's payment application profile indicating the hierarchy of preferences for verifying a cardholder's identity.

11 D.

Data Capture	A Function to transfer data captured at a Point of Interaction to the Acquirer for financial presentment.
Data Elements	A named basic unit of information built on standard structures having a unique meaning. The basic building blocks for messages.
Debit Card (Card With A Debit Function)	(33) 'debit card' means a category of payment instrument that enables the payer to initiate a debit card transaction excluding those with prepaid cards;
Debit Card Transaction	(4) 'debit card transaction' means a card-based payment transaction, including those with prepaid cards that is not a credit card transaction;
Decryption, Decipherment	Transformation of data by a cryptographic algorithm to retrieve data in its original state from cipher text.
Dedicated File (DF) Name	Identifies the name of the Dedicated File (DF) as described in ISO/IEC 7816-4
Deferred Payment	A combined service which enables the Acceptor to perform an authorisation for a temporary amount and a completion for the final amount within a limited time frame. Deferred Payment is available in attended and unattended environments. This is widely used in the petrol environment. This is also called "Outdoor Petrol" when used in the specific petrol sector.
Delayed Fulfilment/Settlement	An environment where there is a delay between the time the payment is initiated and in fulfilling the goods and services or in completing the settlement record.

DF Name	Dedicated File Name.
Digital Card	A digital representation of a Payment Card.
Digital Card Facilitator (DCF)	The SRC System participant which provides a Cardholder with access to Digital Card related data and other optional services.
Digital Payment Application (DPA)	A payment-enabled application that enables the initial interaction of a Customer with an Acceptor, marketplace or other service provider in order to use SRC to pay for goods or services through a Consumer Device.
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g., by the recipient.
Dynamic Authentication	Authentication method that uses cryptography or other techniques to create a one-per-transaction random authenticator (a so-called 'dynamic authenticator').
Dynamic Currency Conversion (DCC)	A feature which allows the Customer to select the currency of the transaction for a given Payment Service, choosing between the Customer's currency and the Acceptor's currency.
Dynamic Data Authentication (DDA)	An RSA-based method of dynamic Offline Data Authentication to authenticate an EMV Card Payment Application by the POI Application, using a Public Key Algorithm to generate a cryptographic value, including transaction specific data elements. See [EMV B2].

12 E.

e-Commerce	A Remote Transaction usually initiated by the Customer using an Electronic Device and conducted via a Virtual POI to buy products and services over the internet.
e-Purse - Loading/Unloading	Services which allow the Customer to transfer funds between an electronic purse and his payment account.
EEA issued cards	A Chip Card or Mobile Contactless EMV Card Payment Application issued in the EEA (European Economic Area).
Electronic Device	Personal device with communication capabilities such as internet, Wi-Fi, etc. Examples of Electronic Devices include personal computers.
Electronic Money (e-money)	A monetary value, represented by a claim on the issuer, which is: 1) Stored on an electronic device (e.g., a card or computer); 2) Issued upon receipt of funds in an amount not less in value than the monetary value received; and 3) Accepted as a means of payment by undertakings other than the issuer.

Electronic Money Institution (ELMI)	A legal person that has been granted authorisation under Title II of the Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions to issue electronic money.
Electronic Payment Instrument	A personalised device (or a set of devices), software and/or set of procedures agreed between the end user and the Payment Service Provider to request the execution of an electronic transfer of value. Typical examples of Electronic Payment Instruments are Payment Card, credit transfers, direct debits, e-money transfers and digital payment tokens. [PISA] Currently Payment Card and Instant Credit Transfer are the categories of Electronic Payment Instruments in the scope of the Volume.
Electronic Product ID	[IFR] Art 10 §5 Issuers shall ensure that their payment instruments are <u>electronically</u> identifiable and, in the case of newly issued card-based payment instruments, also visibly identifiable, enabling payees and payers to unequivocally identify which brands and categories of prepaid cards, debit cards, credit cards or commercial cards are chosen by the payer.
Embossed	Characters raised in relief from the front surface of a card.
EMV	An acronym describing the set of specifications developed by EMVCo, which is promoting a global standardisation of electronic financial transactions - in particular the global interoperability of Chip Cards. "EMV" stands for "Europay, Mastercard and Visa". EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.
EMV Card Authentication Application	An EMV Card Payment Application stored on a Physical Card to perform an Authentication for Remote Payments using an Additional Authentication Device.
EMV Card Payment Application	A Payment Application according to EMV associated with a PAN as Account Data and stored on a Physical Card or a Mobile Device, used for Local Transactions. Each EMV Card Payment Application is identified by an Application Identifier (AID). An EMV Card Payment Application stored on a Physical Card may be contact, contactless or both. - An EMV Card Payment Application is called a Contact EMV Card Payment Application if it supports transaction processing for the Acceptance Technology "Chip with Contact". - It is called a Contactless EMV Card Payment Application if it supports transaction processing for the "Chip Contactless" Acceptance Technology. An EMV Card Payment Application stored on a Mobile Device supports transaction processing for the "Mobile Contactless" Acceptance Technology and is called a Mobile EMV Card Payment Application.

EMV Online Authentication	Authentication of an EMV Card Payment Application using Application Cryptograms with online communication to the issuer. EMV Online Authentication includes the Card Authentication Methods • ARQC Authentication as specified in [EMV B2] and [EMV B3] as part of “Online Authorisation” (applicable to Chip Contact Acceptance Technology), and • “Remote Authentication” as specified in [EMV E] (applicable to the Contactless Acceptance Technologies).
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, UnionPay and VISA.
Encryption, Encipherment	(Reversible) Transformation of data by a cryptographic algorithm to produce cipher text, i.e., to hide the information content of the data.
End-To-End Interoperability	Seamless, standards-compliant exchange and processing of payment-related data and messages across all actors, systems, and platforms involved in a Payment Transaction, from the POI to final settlement.
European Payments Stakeholders Group (EPSG)	The Cards Stakeholders Group (CSG) was set up by the EPC in 2009 with the aim to be a dialogue platform dealing with European Cards Standardisation Matters and as a leading organisation in SEPA cards and terminal standardisation. Five industry sectors combine their efforts in writing and maintaining the "SEPA Cards Standardisation Volume", i.e. Retailers, Processors, the European Payments Council, Vendors and Schemes. The CSG was disbanded in the year 2016 and a separate legal entity was established under the name of European Cards Stakeholders Group (EPSG) AISBL in April 2016. In 2023, the EPSG expanded its scope beyond card payments and became the European Payments Stakeholder Group (EPSG), which now writes and maintains the “SEPA Payments Standardisation Volume”. The purpose of the EPSG, as a multi-stakeholder association, is to support and promote European card standardisation with market-driven implementation. The mission of the EPSG is to: - Maintain and evolve the Volume in line with market needs, reflecting the evolution of card payment technology; and - Promote Volume conformance throughout the payments value chain, to enable a more harmonised SEPA payment ecosystem. In order to fulfil its purpose and mission, the EPSG aims to organise the payments related standardisation dialogue amongst the stakeholders involved in the payment ecosystem and to liaise with regulatory and oversight authorities in relation to payment standards.

European Economic Area (EEA)	An area currently composed of the 28 European Union (EU) member states, as well as 3 of the 4 member states of the European Free Trade Association (EFTA): Iceland, Liechtenstein and Norway. One EFTA member, Switzerland, has not joined the EEA, but has a series of bilateral agreements with the EU which allow it also to participate in the internal market.
Evaluation Assurance Level	A level of reliability in the provision of the product security. The term mostly used by Common Criteria (ISO 15408) describes precise requirements for a security evaluation. A higher EAL number requires more efforts for an evaluation regarding the depth and methods.
Evaluation Methodology	A methodology that will be used to evaluate compliance and assurance level with a specific implementation specification,
Execution Scheme	The set of rules governing the settlement of ICT Transactions. The SCT Inst is an example of Execution Scheme.
Extended Data Authentication (XDA)	An ECC-based type of dynamic Offline Data Authentication where an EMV Card Payment Application combines the generation of a cryptographic value (dynamic signature) with the generation of an Application Cryptogram, for the POI Application to verify that it originates from a valid card. See [EMV B2].

13 F.

Face-To-Face Payment	See Local Payment
Face-To-Face Transaction	See Local Transaction
Fast Dynamic Data Authentication (fDDA)	An accelerated RSA-based method of Dynamic Data Authentication (DDA) that leverages DDA as defined in [EMV B2] specifications. Used in contactless transactions allowing the POI to issue READ RECORD commands, obtaining DDA related data from an EMV Card Payment Application to perform the DDA calculations after the Card or Mobile Device has left the field.
Financial Presentment	A Function which enables acquirers to send issuers the transactions details and the amounts due for the processed transactions. This is generally called "Clearing".
Floor Limit	A transaction amount in a specific currency, above which an online authorisation is required for a single transaction.
Form Factor	The physical characteristics of a Card or any Consumer Device.
'Four Party Payment Card Scheme'	(17) 'four party payment card scheme' means a payment card scheme in which card-based payment transactions are made from the payment account of a payer to the payment account of a payee through the intermediation of the scheme, an issuer (on the payer's side) and an acquirer (on the payee's side);

Framework Contract	A payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligations and conditions for setting up a payment account.
Function	A Function is a processing step or a sub-element of a Payment Service.
Funds	Banknotes and coins, scriptural money and electronic money as defined in [EMD]

14 G.

General Purpose Card	A Card that can be used by a Cardholder to pay bills, obtain cash at ATMs and make purchases everywhere it is accepted, including internet and mail order/telephone order to acceptors.
----------------------	---

15 H.

Hardware Security Module (HSM)	Physical equipment/components including a secure crypto processor and used within the cryptographic boundary to process security functions (including cryptographic algorithms and key generation).
Hashing	Computationally efficient function mapping binary strings of arbitrary length to binary strings of fixed length, such that it is computationally infeasible to find two distinct values that hash into the same value.

16 I.

IFR Product Type	Category of Cards as defined in the [IFR]: debit, credit, commercial or prepaid. IFR Art 10 §5
ISO IIN Blockholder	An ISO/IEC 7812 registered IIN Blockholder is an assigned owner of several IINs (BINs) for the purposes of issuing, sub licensing or otherwise assigning BINs for use by Card Issuers.
ISO IIN Card Issuer	An ISO/IEC 7812 registered IIN Card Issuer is an assigned owner of an IIN (BIN) for the purposes of issuing Primary Account Numbers (PANs).
Implementation Specification	Generally developed and managed by Specification Providers, implementation specifications are detailed description for applying standards and functional and optionally security requirements.
Imprint	Image of the embossed card data on the front of a card.

Instalment Payment	A Card Payment Service where the Customer authorises an Acceptor to split the Payment of a single purchase of goods or services in a finite number of periodic transactions, with a specified end date. Note: It is not considered an Instalment Payment if the Issuer performs multiple debits of a Customer's account for a single purchase of goods or services over an agreed period of time. In this case the Issuer authorises the complete Payment amount, and the splitting of the Payment amount is transparent for the card Acceptor/Acquirer.
Instant Credit Transfer (ICT)	A category of Payment Instrument governed by rules for making instant credit transfer payments from bank accounts to other bank accounts.
Instant Credit Transfer (ICT) Scheme	A Scheme using Instant Credit Transfer as Payment Instrument.
Instant Credit Transfer (ICT) Transaction	A Payment Transaction using an Instant-Credit-Transfer-based Payment Instrument. The initiation of an ICT Transaction may be based on various Acceptance Technologies as described in Section 1.8, including QR Code and Mobile Contactless.
Instant Credit Transfer (ICT) Payment Application	A Mobile Proximity ICT Payment Application or a (Mobile) Remote ICT Payment Application.
Integrated Circuit(s)	Electronic component(s) designed to perform processing and/or memory functions.
(Data) Integrity	The property that data has not been altered or destroyed in an unauthorised manner.
Interchange Fee (IF)	(10) 'interchange fee' means a fee paid for each transaction directly or indirectly (i.e. through a third party) between the issuer and the acquirer involved in a card-based payment transaction. The net compensation or other agreed remuneration is considered to be part of the interchange fee.
International Organization For Standardisation (ISO)	Non-governmental organisation consisting of a network of the national standards institutes of over 150 countries, with one member per country and a central secretariat in Geneva, Switzerland, that coordinates the system.
Interoperability	The ability of two or more components involved in the payment systems to exchange the agreed information and to use the information that has been exchanged in order to complete a payment, a transaction or a service and exchange value between payment participants.

Issuer	A Customer's ASPSP contracting with the Customer to provide them with a Payment Instrument to initiate and process Card or ICT Transactions, resulting in a transfer of funds. <i>Note: In the context of Open Banking, the Customer's ASPSP may provide a dedicated interface (typically an API according to PSD2) to initiate the transfer of funds, but they do not necessarily issue a personalised device (e.g. a Payment Application) to the Customer used to initiate an ICT Transaction.</i> <i>Note: In the context of Payments messages of ISO 20022, the term Debtor Agent or Instructing Agent encompasses the Issuer role.</i>
Issuer Application Data	Payment system defined application data for transmission from the chip card to the issuer in an online transaction.
Issuer Authentication Data	Data sent from the issuer to the ICC as a result of online issuer authentication.

17 J.

18 K.

Kernel	A piece of POI Application software that contains the interface routines, security and control functions to interact with a Payment Application. A Kernel interacting with EMV Card Payment Applications as defined in the EMV specification, is called an EMV Kernel. The functionality of a POI Application that supports functions like the printer and display, and building messages to send to the acquirer, is not considered part of the kernel.
Kiosk	Unattended self-service booths with computers that dispense information or make sales via a touch screen. Any modern vending machine that accepts Payment Cards or ICT can be called a kiosk.
Know Your Customer (KYC)	The process by which financial institutions and other regulated entities verify the identity of their clients.

19 L.

Labelling	Optional Volume conformance process based on self-assessment for detailed implementation specifications.
-----------	--

Laboratory	In the context of the SPS Volume, an entity accredited by the Certification Body to evaluate a given card payment component (POI, card) against the requirements defined in a given implementation specification or standard. The Laboratory issues an evaluation report to the card or POI vendor and the Certification Body for certification.
Language Selection	A Function which allows selecting, automatically (Payment Device-based Language Selection without Customer or attendant interaction) or manually (Manual Language Selection by the Customer or attendant), the language used on the POI for communication with the Customer.
Liability	The obligation to pay an amount owing. The term 'liability' is also used to refer to the party that is responsible for covering or absorbing an amount in respect of a fraud or Customer dispute.
Local AIT	An AIT conducted at the Acceptor's Physical POI.
Local Card Payment	A Card Payment initiated at the Acceptor's Physical POI. This concept is the opposite of Remote (Card) Payment.
Local Transaction	A Transaction initiated and completed at the Acceptor's Physical POI.
Local Customer Present	Local Transaction performed by the Customer.
Luhn algorithm	Also known as the "modulus 10" or "mod 10" algorithm, a simple checksum formula used to validate a variety of identification numbers, such as credit card numbers (created by IBM scientist Hans Peter Luhn)

20 M.

m-Commerce	A Remote Transaction initiated by the Customer using a Mobile Device and conducted via a Virtual POI to buy products and services over the internet.
MACing	A function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following properties: - for any key and any input string the function can be computed efficiently; - for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the input string may have been chosen after observing the value of the first $i-1$ function values (see ISO/IEC 9797-1)
Magnetic Stripe	Acceptance Technology where Card Data is retrieved from the magnetic stripe of a Magnetic Stripe Card.

Magnetic Stripe Card	A card carrying a Magnetic Stripe which complies with ISO/IEC 7810, 7811, 7812, 7813. Out of scope of the Volume.
Magstripe Fallback	Refers to the scenario where a chip card cannot be read on a chip-enabled terminal, so the terminal gathers the information from the Magnetic Stripe and generates a Magnetic Stripe transaction. The Scenario is referred to as operating in fallback mode.
Manual Entry	Acceptance Technology where Card data is keyed in manually at the time of the transaction by the Attendant or by the Cardholder.
Marketplace	A Marketplace is a physical or virtual place that brings together Customers and sellers and may process Transactions and receive settlement on behalf of those sellers. The sellers can be Acceptors or can rely on the services of the Marketplace operator being the Acceptor.
Means Of Distance Communication	It refers to any means which, without the simultaneous physical presence of the payment service provider and the payment service user, may be used for the conclusion of a payment services contract.
Means Of Payment	Assets or claims on assets that are accepted by a payee as discharging a payment obligation on the part of a payer vis-à-vis the payee. See also Payment Instrument.
Merchant	See Acceptor.
Merchant Agreement	A contract between a Merchant (Acceptor) and an Acquirer containing their respective rights, duties and obligations of participation in the scheme payment system.
Merchant Initiated Transaction (MIT)	A Card Transaction initiated by the Acceptor in the role of the payee, without the Cardholder interacting in the transaction process. The MIT shall be based on a pre-agreed mandate between Acceptor and Cardholder (See separate definition MIT Mandate).
Merchant Service Charge	(12) 'merchant service charge' means a fee paid by the payee to the acquirer in relation to card-based payment transactions;
Merchant-presented QR Code	Acceptance Technology where a QR Code is displayed by the Acceptor and scanned by the Customer's Mobile Device. The QR Code contains (static or dynamic) data to identify the Acceptor and the transaction.
Message	A named based unit of information which is transmitted as a whole during the execution of a Protocol. The basic building blocks for protocols.
MIT Mandate	An agreement between Acceptor in the role of the payee and Cardholder allowing the Acceptor in the role of the payee to initiate one or a series of MITs through a specific Card and for a specific purpose. Note: If the Mandate is set up electronically, SCA is required.

(Mobile) Authentication Application	An Application stored on or accessed via a (Mobile) Consumer Device used to support the authentication process in a (Mobile) Remote Card or ICT Transaction or - only for a Mobile Authentication Application - in a Local conventional ICT Transaction. It supports transaction processing for the Acceptance Technologies “Browser over Internet” and “Merchant-presented QR Code”.
Mobile Code	Mobile Code is a CVM which is dedicated to mobile payments (Mobile Contactless Payments (MCPs) or Mobile Remote Payments (MRPs)). The mobile code is entered via the keyboard of the Mobile Device. A distinction is made between Offline Mobile Code and Online Mobile Code: • An Offline Mobile Code may be used for Local Transactions and for m-commerce transactions. It is verified in one of the following ways: ○ The Mobile Code is verified offline by a dedicated application such as the MCP/MRP or Authentication Application in a secure environment via the Mobile Device, ○ The correct entry of the Mobile Code is implicitly validated through a cryptographic derivation verified online by the issuer. • An Online Mobile Code may only be used for e-commerce transactions. It is transmitted in a secure way and verified online by the issuer. An offline Mobile Code is a type of CDCVM.
Mobile Contactless	Acceptance Technology where Account Data is retrieved from a Mobile Contactless Payment (MCP) Application on a Mobile Device over the contactless interface compliant with [EMV L1 CL].
(Mobile) Contactless EMV Card Payment Application	A Mobile Contactless EMV Card Payment Application or a Contactless EMV Card Payment Application.
Mobile Contactless EMV Card Payment Application	An EMV Card Payment Application stored on a Mobile Device supporting transaction processing for the Acceptance Technology “Mobile Contactless”. A Mobile Contactless EMV Card Payment Application may be used for processing Card Transactions or ICT Transactions according to EMV. ICT Transactions are processed as shown in FIGURE 8 in Section 1.8.
Mobile Contactless ICT Payment Application	A type of Mobile Proximity ICT Payment Application processing ICT Transactions using the Acceptance Technology “Mobile Contactless” as shown in Figure 7 in Section 1.8, not according to EMV. Each Mobile Contactless ICT Payment Application is identified by an Application Identifier (AID) and can be selected using PPSE and AID.
(Mobile) Contactless Payment Application	A Contactless EMV Card Payment Application or a Mobile Contactless Payment Application.

Mobile Contactless Payment Application (MCP)	A Mobile Contactless EMV Card Payment Application or a Mobile Contactless ICT Payment Application.
Mobile Proximity ICT Payment Application	A non-EMV Payment Application stored on a Mobile Device, used for Local ICT Transactions. A Mobile Proximity ICT Payment Application supporting transaction processing for - the "Mobile Contactless" Acceptance Technology is called a Mobile Contactless ICT Payment Application. - the "Merchant-presented QR Code" and/or "Consumer-presented QR Code" Acceptance Technologies is called a Mobile QR Code ICT Payment Application. A Mobile Proximity ICT Payment Application may support one or more of the above Acceptance Technologies.
Mobile QR Code ICT Payment Application	A type of Mobile Proximity ICT Payment Application processing ICT Transactions using the Acceptance Technology "Merchant-presented QR Code" and/or "Consumer-presented QR Code" as shown in FIGURE 5 and FIGURE 6 in Section 1.8.
Mobile Device	Consumer device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth, not limited to mobile phones, smart phones and tablets.
Mobile Device for Acceptance	Acceptor controlled device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth ... Examples of Mobile Devices for Acceptance include MPOS, mobile phones, smart phones and tablets. Also referred to as a 'Mobile Acceptance Device'
Mobile ICT Application	A Mobile Authentication or Payment Application used to process ICT Transactions.
Mobile Remote Payment (MRP)	A remote payment initiated through a Mobile Device.
Mobile Payment Application	A Payment Application stored on/or accessed via a Mobile Device. These are: - Mobile Contactless Payment Application (MCP), - Mobile QR Code ICT Payment Application, - Mobile Remote Payment Application.

(Mobile) Remote Card Payment Application	A type of (Mobile) Remote Payment Application used to perform a Card Transaction. It supports transaction processing for the Acceptance Technology “(M)RP Application over Internet”.
(Mobile) Remote ICT Payment Application	A type of (Mobile) Remote Payment Application used to perform an ICT Transaction. It supports transaction processing for the Acceptance Technology “(M)RP Application over Internet” or “Merchant-presented QR Code”.
(Mobile) Remote Payment Application ((M)RP)	A Payment Application stored on/or accessed via a (Mobile) Consumer Device used to perform a (Mobile) Remote Transaction. A (Mobile) Remote Payment Application used to perform • Card Transactions is called a (Mobile) Remote Card Payment Application, • ICT Transactions is called a (Mobile) Remote ICT Payment Application.
Mobile Remote Payment - Basic Mobile Commerce	A mobile remote payment using a static authentication method.
Mobile Remote Payment - Secured Mobile Commerce	A mobile remote payment using a dynamic authentication method.
Mobile Remote Transaction	A Remote Transaction initiated through a Mobile Device.
Mobile Wallet	A service accessed through a Mobile Device which allows the wallet holder to securely access, manage and use a variety of services/applications including payments. This service may reside on a Mobile Device owned by the Customer or may be remotely hosted on a secured server (or a combination thereof) or an acceptor website.
Money Remittance	A payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.

MOTO	A Remote Card Transaction conducted in the Acceptor's environment using Manual Entry of Card Data with the Customer usually interacting remotely for Mail Order or Telephone Order (MOTO). The Card Data is key manual entered either by the Acceptor via a Physical POI or a Virtual Terminal. If DTMF is used, Card Data is entered by the Customer via a Virtual Terminal. For some Payment Services, MOTO transactions may be initiated by the Acceptor based on Stored Card Data, e.g., MITs like No-Show, subsequent transactions of Instalment Payments and Recurring Payments.
------	---

21 N.

Near Field Communication (NFC)	A contactless communication interface and protocol specified in ISO/IEC 18092 and ISO/IEC 21481
No CVM Required	A Cardholder Verification Method as defined in [EMV].
No-Show	A service which allows the Acceptor to charge the Customer's account if they fail to cancel or use a reservation for car hire or a room rental.

22 O.

Offline Biometric Verification	A Cardholder Verification Method defined in [EMV], where the biometric data is captured on a Biometric Capture Device and sent to and verified offline by the Physical Card against a biometric reference template stored on the Physical Card
Offline Card Transaction	See Offline Transaction.
Offline Data Authentication	A process whereby an EMV Card Payment Application is authenticated by the POI Application, using public key technology. The following forms of Offline Data Authentication are defined by EMV: • Methods based on RSA: SDA, DDA, CDA and fDDA. • Methods based on ECC: XDA and BDHLA.
Offline Enciphered PIN	An Offline PIN whereby the PIN is transmitted to the card encrypted using an RSA- or ECC-based Public Key Algorithm at the POI's PIN Entry Device. See [EMV B2].
Offline Only Terminal	A chip terminal that is not capable of sending an online authorisation request and where all transactions have to be approved offline.

Offline PIN	A Cardholder Verification Method where the PIN entered by the Cardholder is verified by the Card against a reference PIN stored on the Card. There are two types: Offline Plaintext PIN or Offline Enciphered PIN.
Offline Plaintext PIN	An Offline PIN whereby the PIN is transmitted to the card in plaintext.
Offline Transaction	A Card Transaction which is authorised offline by an EMV Card Payment Application.
One-off Payment	The basic Payment Service which allows the Customer to pay for the purchase of goods and services from an Acceptor using their Payment Instrument.
One Stop Shopping	A concept associated with the SEPA for Cards objective of the ECB. "One Stop Shopping" per service implies that a component (card/terminal) certified in one SEPA country as SEPA compliant could be deployed all over SEPA without additional costs and formalities.
Online Capable Terminal	A POI that supports both offline and online processing. This type of POI can authorise a payment locally and can also go online to the Acquirer/Issuer for authorisation when required.
Online Card Transaction	See Online Transaction.
Online PIN	A Cardholder Verification Method where the PIN entered on the PIN Entry Device of the Physical POI is sent as an encrypted PIN in an authorisation request to the Issuer or delegated entity for validation of the Cardholder's identity.
Online Transaction	A transaction that is approved or declined at a POI following a real-time dialogue between the acquirer and issuer (or its agent). This requires that POI is connected online during the transaction phase to the acquirer, to send the request and to receive the response.
Open Banking	Within the PSD2 framework in Europe, it is the regulated practice of enabling secure access to payment account information and payment initiation services by authorised Third-Party Providers (TPPs), based on the consent of the Payment Service User (retail or corporate customer). <i>Note: Ongoing legislative developments, including the proposed PSD3 and the Payment Services Regulation (PSR), may impact the Open Banking framework as the Volume undergoes review.</i>

Open-Loop Versus Closed-Loop Payments Networks	General purpose and limited-purpose payments networks primarily operate under two different business models. Open-loop payments networks, for example Card Schemes, are multi-party and operate through a system that connects two financial institutions - one that Issues the Payment Instrument to the Customer, known as the issuing financial institution or Issuer, and one that has the banking relationship with the Acceptor, known as the acquiring financial institution or Acquirer - and manages information and the flow of value between them. In a typical Closed-loop payments network, the payment services are provided directly to Acceptors and Customers by the owner of the network without involving third-party financial institution intermediaries.
Original Credit	A service which allows the Acceptor to perform a credit to a Customer's account. An original credit is not preceded by another payment.
Over the air (OTA)	A method of distributing software to mobile phones and provisioning handsets with the settings necessary to access messaging services.

23 P.

Partial Approval	An Authorisation response of an amount that is less than the amount expected.
Pass-Through Wallet	A mobile wallet that transmits the Customer's Payment Credential (usually tokenised) to the Acceptor for processing.
Payee	(13) 'payee' means a natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction;
Payer	(14) 'payer' means 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;
Payment Account	(22) 'payment account' means an account held in the name of one or more payment service users which is used for the execution of payment transactions, including through a specific account for electronic money as defined in point 2 of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council (1);
Payment Amount	The amount to be paid for the purchase of goods or services.

Payment Application	Software or equivalent loaded on a Payment Device enabling Payment Transactions to be initiated and allowing the Customer to perform Payment Services. These are (see Section 1.9): • EMV Card Payment Application ○ Contact EMV Card Payment Application (Physical Card), ○ Contactless EMV Card Payment Application (Physical Card) ○ Mobile Contactless EMV Payment Application (Mobile Device) • Mobile Proximity ICT Payment Application (Mobile Device) ○ Mobile Contactless ICT Payment Application ○ Mobile QR Code ICT Payment Application • (Mobile) Remote Payment Application (Consumer Device) ○ (Mobile) Remote ICT Payment Application ○ (Mobile) Remote Card Payment Application See also (21) ‘payment application’.
Payment Brand	Any material or digital name, term, sign, symbol or combination of them, capable of denoting under which rules Payment Transactions are carried out. For Payment Card, the Payment Brand and underlying rules are defined by a Payment Card Scheme. For Instant Credit Transfer, the Payment Brand and underlying rules may also be defined by a Scheme (PSP scheme), or, in absence of a Scheme, the rules rely on published “Open Banking” standards and regulation, and the Payment Brand may be generic (linked to the “Open Banking” standards) or defined by the PISP.
Payment Card	A category of Payment Instrument governed by the rules defined by a Payment Card Scheme.
Payment Card Industry (PCI)	A consortium of the following card Schemes, Visa, Mastercard, American Express, JCB and Discover, which became formalised as the PCI Security Standards Council or PCI-SSC and which manages various aspects related to common industry security requirements.
Payment Card Scheme	(16) ‘payment card scheme’ means a single set of rules, practices, standards and/or implementation guidelines for the execution of card-based payment transactions and which is separated from any infrastructure or payment system that supports its operation, and includes any specific decision-making body, organisation or entity accountable for the functioning of the scheme; <i>Note: A Payment Card Scheme is a Scheme using Payment Card as Payment Instrument.</i>
Payment Completion	A Payment Service which is part of the Pre-Authorisation Services. It is used to finalise the transaction using the final amount.
Payment Context	A set of functional and security requirements related to Payment Services in a specific transaction environment. Payment contexts are identified either based on specific sector, market or transactional volume requirements.

(Payment) Credentials	The information - generally confidential - used by a Customer for the purposes of authentication.
Payment Device	The medium from where or through which Customer Account Data is retrieved when performing a Payment transaction. These are Card and Consumer Device.
Payment Gateway	A service operated by an Acquirer that switches authorisation requests and clearing records between the Acceptor and the Acquirer.
Payment Initiation Service Provider (PISP)	A Payment Service Provider offering services to initiate a Payment Order at the request of the Payment Service User with respect to a Payment Account held at another Payment Service Provider.
Payment Institution	A legal person that has been granted authorisation in accordance with Article 10 of the Payment Services Directive to provide and execute payment services throughout the Community.
Payment Instrument	Any personalised device(s) and/or set of procedures agreed between the Payment Service User and the Payment Service Provider and used in order to initiate a Payment Order (PSD2 and IFR (19)). Only Electronic Payment Instruments are in the scope of the Volume. Currently the Volume covers the following categories of Payment Instruments: • Payment Card and • Instant Credit Transfer.
Payment Order	Any instruction by a Payer or Payee to its Payment Service Provider requesting the execution of a Payment Transaction.
Payment Page	A page presented through the Virtual POI to the Customer which enables the entry of Account Data via the Consumer Device.
Payment Service	A process to perform or support financial transactions based on Account Data, e.g. Card Data in the Card environment.
Payment Service Provider (PSP)	(24) 'payment service provider' means any natural or legal person authorised to provide the payment services listed in the Annex to Directive 2007/64/EC or recognised as an electronic money issuer in accordance with Article 1(1) of Directive 2009/110/EC. A payment service provider can be an issuer or an acquirer or both. <i>Note: As Issuer or Acquirer, a PSP can be a member of a Payment Card Scheme or Instant Credit Transfer Scheme.</i>
Payment Service User	(25) 'payment service user' means a natural or legal person making use of a payment service in the capacity of either payer or payee, or both;
Payment Services	Initiation and/or execution of payment transactions, cash withdrawal and other services as defined in the Payment Services Directive.

Payment Solution	A combination of Payment Instrument (Payment Card or Instant Credit Transfer), Payment Brand, and Acceptance Technology (e.g., NFC, Chip Contact, QR Code).
Payment Standardisation Ecosystem	The complex of the SEPA payments community interacting with its environment in the field of Volume conformance.
Payment System	A funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions.
Payment Transaction	A transaction used to perform a Payment Service. A Payment Transaction is a Local (Payment) Transaction or a Remote Transaction.
Payment Token	A Payment Token can be an EMV Payment Token as defined by EMV® Payment Tokenisation Specification – Technical Framework or a surrogate value for a PAN.
Payment Token - EMV® Payment Tokenisation	[EMVCo-FW v2] In the EMV® Payment Tokenisation Specification – Technical Framework an EMV® Payment Token is a surrogate value for a PAN that is a variable length, ISO/IEC 7812- compliant numeric issued from a designated Token BIN or Token BIN range and flagged accordingly in all appropriate BIN tables. A Payment Token must pass basic validation rules of a PAN including the Luhn check digit. Payment Tokens must not collide or conflict with a PAN.
Payment Transaction	(26) ‘payment transaction’ means an action, initiated by the payer or on its behalf or by the payee of transferring funds, irrespective of any underlying obligations between the payer and the payee;
Payment With Aggregated Amount	A feature which allows the Acceptor or the Acquirer in specific payment contexts to submit a payment by summing up (aggregating) several underlying amounts based upon the same card to obtain the final amount.
Payment With Cashback	A service available in a retail environment which allows the Customer to obtain cash from the Acceptor in conjunction with a Payment (also referred to as Cashback). The Customer receives the extra cash amount (referred to as Cashback amount) in notes and/or coins along with the goods or services. For a Payment with Cashback, the transaction amount is the sum of the Payment amount and the Cashback amount. The service is only available in a Cardholder present environment. In some countries, the service is prohibited by law.
Payment With Deferred Authorisation	A feature whereby the Acceptor postpones the online authorisation until a later time but performs the authorisation before submission for clearing/settlement. It is used for Payments performed on airlines/cruise ships and other types of acceptance environments that are not online at all times.
Payment With Deferred Clearing	A feature where the Acquirer postpones the clearing of the transaction. It is used for example for the payment of health expenses.

Payment With Increased Amount	A feature which allows the Customer to increase the amount to pay by adding an extra amount, for example where a gratuity (tip) is added.
Payment With Loyalty Information	A feature which allows an Acceptor to accept payment with loyalty or reward for their customers or other loyalty programmes.
Payment With Purchasing Or Corporate Card Data	A feature to include data related to a specific activity. This is often in support of the use of a company purchasing or corporate card. The additional data can be for example: VAT, reference numbers, e-invoicing or sector specific data.
Personal Code	This method is a CVM which is dedicated to e-commerce. The personal code is entered via the keyboard of the electronic device. The check is made either online by the Issuer or offline by a dedicated application such as Authentication Application in a secure environment via the electronic device. An offline Personal Code is a type of CDCVM.
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 (for example, IP address, cookies, and RFID), 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. For the purpose of the Volume, Personal Data includes for example: details identifying the Customer, such as the name, address, contact details, relevant ID numbers, the card details, including its number and expiry date, PAN and PAR, any transactions and their history.
Personal Identification Number (PIN)	A personal and confidential numerical code which the user of a payment instrument may need to use in order to verify their identity.
Personal / Mobile Code Try Limit	A parameter indicating the maximum number of consecutive incorrect personal / mobile code attempts allowed.
Personal / Mobile Code Try Counter	The number of personal / mobile code attempts is recorded and the Personal / Mobile Code Try Counter represents the remaining number of attempts allowed. The Personal / Mobile Code Try Counter is reset to the Personal / Mobile Code Try Limit after successful personal / mobile code verification.
Personally Identifiable Information	Information that can be utilised to identify an individual, such as, but not limited to name, address, social security number, phone number.
Physical Card	A Chip Card or a Magnetic Stripe Card or both. It is a carrier of Card Data. If it is a Chip Card, it contains an EMV Card Payment Application or an EMV Card Authentication Application or both.

Physical POI	The initial point where Account Data is retrieved in the Acceptor's Domain. A Physical POI consists of hardware and software which enables a Customer and/or an Acceptor to perform a Local Payment transaction. This is also referred to as a Physical/EMV Terminal. It may be Attended or Unattended. NB: Some Physical POI might also be used to initiate MOTO transactions.
PIN Block	A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length and may contain a subset of the PAN. ISO 9564 contains the standards to which the PIN block must adhere.
PIN Bypass	The activity of bypassing the input of a PIN.
PIN Change/Unlock	The PIN Change/Unlock service provides the Cardholder the capability to change or un(b)lock their PIN.
PIN Entry Device (PED)	A secure device that allows Cardholders to enter a PIN.
PIN Transaction Security (PTS)	PTS is a set of modular evaluation requirements managed by PCI Security Standards Council, for PIN acceptance POI terminals.
PIN Verification Value (PVV)	Discretionary value encoded in Magnetic Stripe of Payment Card.
Plaintext	Unenciphered/unencrypted information.
Point of Interaction (POI)	A POI is a Physical POI or a Remote POI.
POI Application	An application consisting of software and data used to perform Payment Services. Depending on the architecture of the POI (Physical or Remote), the POI Application may be implemented on one component or distributed on several components. The POI Application may be integrated with a sale system or may be standalone. A POI Application on a Physical POI for processing Local Transactions may be referred to as Physical POI Application. A POI Application on a Virtual POI may be referred to as Virtual POI Application. A POI Application on a Physical POI or a Virtual Terminal for processing MOTO transactions is referred to as MOTO Application.

Point of Sale (POS)	(29) ‘point of sale’ means the address of the physical premises of the merchant at which the payment transaction is initiated. However: (a) in the case of distance sales or distance contracts (i.e. e-commerce) as defined in point 7 of Article 2 of Directive 2011/83/EU, the point of sale shall be the address of the fixed place of business at which the merchant conducts its business regardless of website or server locations through which the payment transaction is initiated; (b) in the event that the merchant does not have a fixed place of business, the point of sale shall be the address for which the merchant holds a valid business licence through which the payment transaction is initiated; (c) in the event that the merchant does not have a fixed place of business nor a valid business licence, the point of sale shall be the address for correspondence for the payment of its taxes relating to its sales activity through which the payment transaction is initiated;
Pre-Authorisation Services	A service composed of 3 linked steps: • Pre-Authorisation • Update Pre-Authorisation (potentially with several occurrences) • Payment Completion The Pre-Authorisation allows the Acceptor to reserve an amount in order to secure sufficient funds to complete a subsequent payment. It is used only to secure the amount since the final amount of the actual payment is not known (e.g., car rental, hotel, video rental, etc.). The Update Pre-Authorisation allows the Acceptor to update the amount of a Pre-Authorisation. This may either increase or decrease (potentially to zero) the previously authorised amount. The Payment Completion allows the Acceptor to finalise the payment.
Prepaid Card	(35) ‘prepaid card’ means a category of payment instrument on which electronic money, as defined in point 2 of Article 2 of Directive 2009/110/EC, is stored.
Prepaid Card - Loading & Unloading	A service which allows the Cardholder to transfer funds to or from a prepaid card account.
Presentment	See Financial Presentment
Primary Account Number (PAN)	A series of digits which identify a Customer account or relationship. This number contains a maximum of 19 digits according to ISO/IEC 7812.
Priority Selection	An automatic selection mechanism made by the Payee in its equipment for the categories of cards or related Payment Instruments accepted by the payee.
Private Key	The secret component of an asymmetric key pair. The private key is always kept secret by its owner. It may be used to digitally sign messages for authentication purposes.

Processing	(27) 'processing' means the performance of payment transaction processing services in terms of the actions required for the handling of a payment instruction between the acquirer and the issuer; Note: Processing may include clearing, sorting, netting, matching and/or settlement.
Processing Entity	(28) 'processing entity' means any natural or legal person providing payment transaction processing services;
Processor	In the context of Payment Services, a Processor is a Service Provider mainly acting on behalf of the Acquirer and/or the Issuer or in the Inter-PSP Domain (e.g., routing services between Acquirers and Issuers).
Product Type	See [IFR] Product Type
Products and Solutions	Concept covering any type of products, services and solutions offered by "Solution Providers" to Customers and/or stakeholders of the SEPA payment transaction chain.
Protocol	A pre defined sequence of exchanged messages between two communicating parties required to implement a function. - Some protocols are executed in the A2I domain, some could be in the Terminal-to-Acquirer or in the Card-to-Terminal domain. - The payment processing requires the execution of different protocols. Several models of usage of protocols exist that provide either clearing, authorisation or both services. Protocols consist of a different set of message types (i.e. advices, requests, reversals, charge-backs, etc.)
Proximity Payment	See Contactless Payment.
Proximity Payment System Environment (PPSE)	A standard data structure defined in [EMV B] that is used by a contactless POI, i.e. a POI supporting the contactless Acceptance Technologies, to determine which of the supported applications may be used for a Payment Transaction. On a contactless Payment Device, i.e. a Payment Device supporting a contactless Acceptance Technology, the PPSE contains the list of all Payment Applications supported over the contactless interface, and is returned in response to the SELECT command for the PPSE.
Pseudonymisation	The Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Public Key	The public component of an asymmetric key pair. The public key is usually publicly exposed and available to users. A certificate to prove its origin often accompanies it.
Public Key Algorithm	Cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible. This is also sometimes referred to as asymmetric algorithm.
Public Key Certificate	A digital signature on a public key by a Certificate Authority and intended to prove to the public key recipient, the origin and integrity of the public key.

24 Q.

QR Code	A two-dimensional code consisting of black modules arranged in a square pattern on a white background. A Quick Response (QR) Code is an example of a 2D code as specified in [ISO/IEC 18004]. In the context of ICT, the QR Code is used as an Acceptance Technology in one of two modes: • Merchant-presented QR Code, • Consumer-presented QR Code. <i>QR Code</i> is a registered trademark of Denso Wave Inc.
Quasi-Cash Payment	A Payment Service which allows the Customer to obtain items which are representative of actual cash and directly convertible to cash. Examples include gaming chips, travellers cheques.

25 R.

Reader Contactless Floor Limit	Indicates the contactless floor limit of the reader for a specific AID. If the transaction amount is greater than the Reader Contactless Floor Limit, then the reader requires online processing for the transaction. As defined in Book B.
Reconciliation	A service which enables two entities (Acceptor, Acquirer, Issuer or their agents) to seek an agreement on financial totals (amounts, number of transactions).
Recurring Payment	A Payment Service where the Customer authorises an Acceptor to charge their account on a recurring basis and without a specified end date. This applies to Payments and Deferred Payments performed on a recurring basis.
Reference Exchange Date	The exchange date which is used as the basis to calculate any currency exchange and which is made available by the Payment Service Provider or comes from a publicly available source.

Reference Interest Date	The interest date which is used as the basis for calculating any interest to be applied and which comes from a publicly available source which can be verified by both parties to a payment service contract.
Referral	A function where a Card-based processing of a Payment Service is completed with a voice conversation to obtain an approval code. This Function does not necessarily involve the EMV Card Payment Application or the Customer.
Refund	A Payment Service which allows the Acceptor to reimburse the Customer partially or totally. Refund is linked to a previous Transaction.
Relay attack	An attack where valid payment data is intercepted in one environment (for example, at a POI terminal or a consumer device), then manipulated or repeated and re transmitted or “relayed” to another environment where it is used fraudulently.
Remote AIT	An AIT conducted at the Acceptor's Remote POI.
Remote (Card) Payment	A Card Payment which is performed as Remote (Card) Transaction. A Remote Payment is always initiated by the Cardholder. Therefore it is either e- or m-Commerce or MOTO. The concept is the opposite of Local (Card) Payment.
Remote Payment - Basic Electronic Commerce	A Remote Payment using a static authentication method.
Remote Payment - Mobile	A Remote Payment initiated through a Mobile Device.
Remote Payment - Secured Electronic Commerce	A Remote Payment using a dynamic authentication method.
Remote POI	The initial point where Account Data is retrieved in the Acceptor’s domain for Remote Transactions. The Remote POI exists in a variety of technical platforms which enable a Customer and/or an Acceptor to generate a Remote Transaction. The Remote POI is either a Virtual POI or a Virtual Terminal.
Remote Transaction	A Payment Transaction conducted at the Acceptor's Remote POI. A Remote Transaction is usually initiated by the Customer in which case the Remote Transaction is either e- or m-Commerce or MOTO.
Reversal	The partial or complete nullification of the effects of a previous Authorisation or Data Capture Transaction. A Reversal is sometimes also referred to as an authorisation adjustment.
Risk Assessment	Structured process of identifying, evaluating, and prioritising potential security and technical risks that could affect the secure, reliable, and compliant implementation and operation of payment systems and related components.

Risk-Based Authentication	The use of statistical models via transaction, location, device and profile data to make a customer authentication decision without active customer participation in the decision-making process (refer to as Transaction Risk Analysis in Article 18 of the EC Delegated Regulation 2018/389)
---------------------------	--

26 S.

Scheme	Set of formal, standardised, and common technical and business rules, enabling the transfer of value between end users by means of Payment Instruments. It is easily identifiable at the Point of Interaction by payers and payees, and in general by the rest of the payment chain participants. The Payment Instruments are used to perform the Payment Services described in the Volume.
Scheme Participant	A party having signed a Licence Agreement with a Scheme in order to provide Payment Services for Payment Brands of the Scheme.
Secure Channel	A security mechanism described in [EMV E] to provide confidentiality between the POI Application and the EMV Card Payment Application for contactless transactions.
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 three different form factors of SE: Universal Integrated Circuit Card (UICC), embedded SE and microSD. Both the UICC and microSD are removable.
Secure Environment	A system which implements the controlled storage and use of information. A secure environment is used to protect personal and/or confidential data. In the context of Remote Payments it may be located in the Consumer Device, such as a SE, a TPM or a TEE, or in a remote secured server.
Secure Remote Commerce (SRC)	A method of performing a payment or secure purchase of goods or services during a remote payment that involves a DPA checkout and a consumer device, as defined by the EMV® Secure Remote Commerce Specification.

Security Evaluator	An organisation formally recognised and accredited by a Certification Body to assess Products and Solutions for compliance with a specific Implementation Specification. A Security Evaluator must meet the following key criteria: • Impartiality – It must operate without any affiliation to the organisation under evaluation to ensure an impartial assessment. • Transparent methodology – The evaluation methodology used to determine compliance must be openly published and publicly accessible. • Operational independence – The evaluation process must be conducted free from any management control or influence by a particular Approval Body.
Selection of the Payment Brand	The function which allows the selection of a Payment Brand by the Customer as well as an Application Profile of the POI used to process a Payment Service for a Payment Transaction. For the Acceptance Technologies Chip with Contact, Chip Contactless and Mobile Contactless, this function allows the selection of a Payment Application based on AID supported by both the Payment Device and the POI.
Semi-Attended	The Customer conducts the transaction at the Point of Interaction without the participation of an attendant (agent of the Acceptor or of the Acquirer). However an attendant is present to provide assistance to the Customer if necessary. Therefore, for the purpose of this document, Semi-Attended is categorised as Attended.
Sensitive Payment Data	Data which allows control over the Payment Account or which may be used to carry out fraud.
Sensitive Personal Data (Special Category of Personal Data)	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The Personal Data Processing of the Sensitive Data must be performed in accordance with the [GDPR] including the requirement to obtain explicit consent.
SEPA For Cards	A key objective of the ECB for enabling Payment Service Users in Europe (such as cardholders and acceptors) to use general purpose cards to make and receive payments and cash withdrawals in Euro throughout the SEPA area with the same ease and convenience than they do in their home country.
SEPA Instant Credit Transfer (SCT Inst)	The Instant Credit Transfer governed by the rules defined in [EPC SCT Inst] for making instant credit transfer payments in euro throughout the SEPA from bank accounts to other bank accounts. For further reference see [EPC MSCT IG].
Service Code	Three-digit value as defined in [ISO/IEC 7813].

Service Provider	An entity that provides communications, processing, storage, consulting, and any other service to the Value Chain.
Settlement	The completion of a transaction or of processing with the aim of discharging Acquirers' and Issuers' obligations through the transfer of funds.
Signature	A Cardholder Verification Method using a manual verification of the Cardholder's handwritten signature.
Signature on File	Consent given by the Customer when entering into a contract with the Acceptor for the delivery of goods or services and which will be charged for at a later stage(s).
Single Euro Payments Area (SEPA)	The Single Euro Payments Area (SEPA) stands for the European Union (EU) payments integration initiative. The SEPA vision was set out by EU governments in the Lisbon Agenda, March 2000, which aims to make Europe more dynamic and competitive.
Smart Card	See Chip Card.
Solution	A Product or a Service.
Solution Provider	An entity selling Software or Hardware related to Payment Services and/or products.
Specification Provider	Organisation which: • develops Implementation Specifications based upon the high level requirements specified in the Volume for use by Solution Providers to develop products or solutions; • provides a maintenance process, notably for interoperability and/or security issues linked to the implementation specifications; • has its own certification body or a relationship (formal or informal) with an external certification body to certify products and solutions.
SRC Candidate List	A list of Digital Cards and related data that are eligible for a specific checkout.
SRC Initiator	The SRC System participant which presents an SRC Candidate List and potentially facilitates the retrieval of Payment Data.
SRC Participating Issuer	A card Issuer that has its Payment Cards enrolled in SRC Systems.
SRC Programme	Responsible for the policies and processes associated with the oversight of SRC participants within an SRC System.
SRC System	A technical platform that manages an SRC Profile for each enrolled Customer and facilitates the payment information exchange among all its participants.

Staged Wallet	A mobile wallet that is a Payment Instrument that may either be pre-funded by the wallet holder or be linked to another Payment Instrument. When it is linked to a Card as other Payment Instrument, a Payment consists of two separate Payment Transactions. The first Payment Transaction is used to credit the Cardholder's Staged Wallet with the required Payment Amount using the linked Card. In a second Payment Transaction the Cardholder's wallet is debited and the Acceptor is credited.
Standards	Document approved by a recognised body that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.
Static Authentication	An authentication method which always uses the same authenticator.
Static Data Authentication (SDA)	An RSA-based type of Offline Data Authentication where the POI validates a cryptographic value stored on the Card by the Issuer (as defined in [EMV B2]). It protects against some types of counterfeit fraud but does not protect against skimming.
Stored Account Data	Acceptance Technology where (tokenised) Account Data have been provided prior to the transaction and stored securely for later use. This Acceptance Technology is used for AIT. In the specific scenario where Card Data is securely stored within the Acceptor's domain, this can also be referred to as Card on File.
Strong Authentication	A dynamic authentication method which involves at least 2 independent authenticators. This means that at least one of them is dynamic.
Strong Customer Authentication (SCA)	An authentication based on the use of two or more elements (Authentication Methods) 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 [PSD2]. Cardholder Verification Methods described in [EMV] may be used as a factor towards SCA, but other factors may be required.
Surcharging/Rebate	A feature which allows the Acceptor to charge a fee or give a rebate to the Customer in relation to a given Payment Service.
Switch	The routing centre that transfers authorisation requests, approvals and payment transaction information to the appropriate receiver.
Symmetric Algorithm	An algorithm in which the key used for encryption is identical to the key used for decryption. DES is the best known symmetric encryption algorithm.

27 T.

Tamper Resistant Security Module (TRSM)	A Tamper-Resistant Security Module (TRSM) is a device that incorporates physical protections to prevent compromise of Cryptographic Security Parameters therein contained.
TC	Transaction Certificate, which is a Cryptogram generated by a Card Application. See [EMV B2].
Technology Selection	A Function which allows to select the acceptance technology (e.g., chip, Magnetic Stripe, etc.) to be used to process a service for a transaction.
Terminal	See POI.
Terminal Risk Management (TRM)	Offline checks performed by the terminal to determine whether a transaction should proceed further. Examples are floor limit checking and exception file checking.
Test Laboratory	In the context of the SEPA Cards Ecosystem, it relates to an organisation accredited by a Certification Body to test or evaluate "Products and solutions".
Test plan	A test plan is a document detailing a systematic approach to testing a "product or solution".
Test script	A test script is a set of instructions that will be performed on the "product or solution" to test that it functions as expected.
Third Party Processor	See Third Party Service Provider
Third Party Provider (TPP)	See Third Party Service Provider
Third Party Service Provider	A Processor or other service provider who stores, processes, and/or transmits data for processing a Payment Service (sometimes also referred to as Third Party Provider or Third Party Processor)[different from the PSD definition]
Three-Party Card Scheme	(18) 'three party payment card scheme' means a payment card scheme in which the scheme itself provides acquiring and issuing services and card-based payment transactions are made from the payment account of a payer to the payment account of a payee within the scheme. When a three party payment card scheme licenses other payment service providers for the issuance of card-based payment instruments or the acquiring of card-based payment transactions, or both, or issues card-based payment instruments with a co-branding partner or through an agent, it is considered to be a four party payment card scheme;
Transaction Amount	The amount to be authorised when performing a financial transaction.

Transaction Initialisation	A Function which allows selection of the Payment Service for the next transaction and where the transaction amount is set, transaction data is initialised and processing of the Payment Service is started.
Transaction Risk Analysis	Evaluation of the risk related to a specific transaction taking into account criteria such as, for example, customer payment patterns (behaviour), value of the related transaction, type of product and payee profile.
Transaction Reference	The reference number used to identify a given transaction that allow the Acceptor or Acquirer to keep track of their transactions.
Transaction Sequence Counter	Counter maintained by the POI Application that is incremented by one for each transaction.
Transit Payment	A payment occurring in a public transport environment usually working offline and requiring high speed transactions.
Truncated PAN	Method of rendering the full PAN unreadable by permanently removing a segment of PAN data. Truncation relates to protection of PAN when stored in files, databases etc. Only the last 4 digits of the PAN are printed.
Trusted Execution Environment (TEE)	A separate execution environment that runs alongside the operating system (OS). The TEE provides security services to the OS environment and isolates access to resources from the Rich OS and its applications. It is to be noted that a TEE protects against malicious software but does not provide the hardware protection of an SE.
Type Approval	The process which a product or solution must undergo in order to obtain the authorisation for deployment from a given card payment scheme or Approval Body.

28 U.

Unattended Physical POI	The Customer is present and conducts the transaction at the Physical POI, without the participation of an attendant representing the Acceptor or the Acquirer (e.g., kiosks, vending machines, petrol pumps (UPT), etc.).
Unique Identifier (UID)	Identifier linking a Pre-Authorisation transaction and subsequent transactions of a Pre-Authorisation service.
Unsolicited Available Funds	A feature which allows the card issuer to provide account balance information in the authorisation response message.

29 V.

Value Chain	A chain of activities by different Service Providers and Vendors in order to deliver a Payment Service.
-------------	---

Value Date	A reference time used by a payment service provider for the calculation of interest on the funds debited from or credited to a payment account.
Vendor	See Solution Provider.
Virtual Card	A card-based payment solution where card data is issued without a physical card, which can be used for e- & m- commerce.
Virtual POI	The initial point where Card Data is retrieved in the Acceptor's domain. A Virtual POI consists of hardware and software which enables a Cardholder and/or Acceptor to perform a Remote Transaction. If the Remote Transaction is initiated by the Cardholder it is an e- or m-Commerce Transaction where the Card Data enters the Acceptor's domain via a Consumer Device for e- or m-commerce. The Virtual POI includes a Payment Page which may be presented to the Cardholder from either a Payment Gateway or the Acceptor's website. The Virtual POI may also facilitate (redirection) services to support Authentication of the Cardholder by the Card Issuer for e-and m-Commerce. A Virtual POI may also enable the Acceptor to perform Remote Transactions based on Stored Card Data, e.g. MITs like No-Show, subsequent transactions of Instalment Payments and Recurring Payments or Remote Transactions where the Acceptor is the payer like Refund and Original Credit.
Virtual Terminal	A MOTO Application used by the Acceptor to enter Card Data. It comprises a Payment Page hosted by an Acquirer or TPP for the entry of Card Data by the Acceptor for MOTO Transactions. A Virtual Terminal can also be used by the Cardholder, but only for Telephone Orders if DTMF technology is used. A Virtual Terminal may also enable the Acceptor to perform Remote Transactions based on Stored Card Data, e.g. MITs like No-Show, subsequent transactions of Instalment Payments and Recurring Payments or Remote Transactions where the Acceptor is the payer like Refund and Original Credit.
Visual Product ID	[IFR] Art 10 §5 Issuers shall ensure that their payment instruments are electronically identifiable and, in the case of newly issued card-based payment instruments, also <u>visibly</u> identifiable, enabling payees and payers to unequivocally identify which brands and categories of prepaid cards, debit cards, credit cards or commercial cards are chosen by the payer.
Voice Authorisation	See Referral
Volume Conformance	When a Product, Service or implementation Specification has been developed in accordance with the requirements of the SEPA Payments Standardisation Volume it is conformant with the Volume.
Volume Conformance Verification Process	The processes by which the SEPA Cards Community interacts with its environment for verifying the SPS Volume conformance.

30 W.

31 X.

XML	The acronym used for “Extensible Markup Language”, a computer metalanguage used to simplify the transmission of formatted data.
-----	---

32 Y.

33 Z.

34	4 FIGURES	
35	FIGURE 1: VOLUME OVERVIEW.....	12
36	FIGURE 2: VOLUME AND SRC INTEGRATION	19
37	FIGURE 3: ICT TRANSACTION MODELS IN THE CONSUMER-TO-BUSINESS DOMAIN	20
38	FIGURE 4: ICT TRANSACTION – GENERAL ONE-OFF PAYMENT FLOW (MODEL 1)	21
39	FIGURE 5: OPEN BANKING-BASED ICT TRANSACTION – MERCHANT-PRESENTED QR CODE	23
40	FIGURE 6: OPEN BANKING-BASED ICT TRANSACTION – CONSUMER-PRESENTED QR CODE	24
41	FIGURE 7: OPEN BANKING-BASED ICT TRANSACTION – BLE OR NON-EMV-BASED NFC ACCEPTANCE	25
42	FIGURE 8: OPEN BANKING-BASED ICT TRANSACTION – NFC AT POI – EMV-TECHNOLOGY-BASED	26

43