

**SEPA CARDS STANDARDISATION (SCS) “VOLUME”
STANDARDS’ REQUIREMENTS**

BOOK 1

GENERAL PRINCIPLES AND DEFINITIONS

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

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

Abstract	This document contains the work on SEPA cards standardisation to date
Document Reference	ECSG001-18
Issue	Book 1 – v10.0
Date of Version	1 October 2022
Reason for Issue	Publication
Reviewed by	ECSG Board – 22 September 2022
Produced by	ECSG Secretariat – Volume Sub-Group
Owned and Authorised by	ECSG
Circulation	Public

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

Version number	Dated	Reason for revision
9.5	23.11.2021 (published in December 2021)	Consultation version December 2021-March 2022
10.0	01.10.2022	ECSG Published version - Volume v10.0

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

Table of Contents

1	GENERAL	6
	Terms of Use	6
1.1	Executive summary	7
1.1.1	Goal and Addressees.....	7
1.1.2	Volume	7
1.1.3	Card Services	7
1.1.4	Security	8
1.2	Volume Conformance via Labelling	8
1.3	Volume Maintenance principles	9
1.4	Description of changes since the last version of Book 1	12
1.5	Volume Compliance with European Regulations and Directives	13
1.5.1	Volume impact	13
1.5.2	Work in progress	14
1.5.3	High-Level Summary of PSD2-related content	14
1.5.3.1	Merchant Initiated Transactions (MITs)	15
1.6	Tokenisation.....	15
1.7	SRC (Secure Remote Commerce).....	16
1.7.1	SRC summary presentation.....	16
1.7.2	SRC inclusion in the Volume	16
2	THE SCS VOLUME AND ITS BOOKS.....	18
2.1	Introduction to the “SEPA Cards Standardisation Volume”	18
2.2	Scope and Objectives of ECSG Work on Cards Standardisation	19
2.2.1	Scope	19
2.2.2	Objectives.....	19
2.2.3	Impact on the Different Stakeholders	20
2.2.4	Implementation of the Volume and Monitoring	20
2.2.5	Implementation Specifications	20
2.3	Maintenance of the Books	20
2.3.1	The Volume, a Set of Books	20
2.3.2	Maintenance cycles.....	21
2.3.3	Intellectual Property Rights	22
3	REFERENCES, ABBREVIATIONS AND DEFINITIONS.....	23

3.1	References	23
3.2	Abbreviations.....	27
3.3	Definitions.....	30
4	FIGURES	69

1 GENERAL**Terms of Use**

The European Cards Stakeholders Group (ECSG) AISBL, an industry association actively working on cards standardisation in the Single Euro Payments Area (SEPA), publishes the SEPA Cards Standardisation Volume (“the 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 ECSG 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 ECSG 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 Card 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.

Neither the ECSG 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.

You agree to defend, indemnify and hold harmless the ECSG 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 ECSG 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 cardholders and acceptors), *enabling them to use general purpose cards 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 cards 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 ECSG in understanding requirements that are part of European regulatory activity, such as the Interchange Fee Regulation [IFR], the PSD 2[PSD2] 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 Cards Stakeholders Group (ECSG) which is composed of market representatives from the five main cards 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 Card Services

The Volume describes functional requirements applicable to transactions either initiated by a Card¹ at the card acceptor's terminal as Card Present (local) transactions, or as Card Not Present (remote) transactions. These transactions result in the provision of the so-called "Card Services" to the cardholder and acceptor, as specified in the Volume.

¹ A "Card" refers to all form factors of a device or payment instrument that can be used by its holder to perform a Card Service.

1.1.4 Security

Trust in a card as 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, card 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 ECSG. 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 ECSG website², as well as Book 5 (Conformance Verification Processes) of the Volume.

The Volume conformance process (labelling via the ECSG) 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 payment products and solutions for transactions initiated in the SEPA area will in future be conformant with the requirements described in the Volume. A migration roadmap is therefore required to move from the current implementations to the future vision mindful of a desire to maintain interoperability with non SEPA general purpose cards.

Functional requirements of the Volume may be waived for people with disability, in order to provide them with equal access to cards 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.³

² <https://www.e-csg.eu/labelling-process-description>

³ 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.

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 ECSG Sectors. In order to make sure that the market evolves in due time, 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 years 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.



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 - ***Implementation Guidelines***

Book 7 - ***Card Processing Framework***

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

1.4 Description of changes since the last version of Book 1

This version of Book 1 has been updated with information relating to Compliance with European Regulations and Directives. Some definitions have been completed/enhanced/aligned in view of [PSD2], [RTS SCA/CSC], as well as [GDPR] as well as other changes in definitions to align with the updates that have occurred to the respective books.

Information is supplied on the ECSG initiative for Tokenisation, plus general editorial changes have occurred due to various layout modifications.

This version also described the inclusion of the new EMVCo specifications on SRC (Secure Remote Commerce) in the Volume

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 Card services are fully compliant to those regulations. This version of the Volume has been drafted with particular attention given to [PSD2] and the [GDPR], their deadlines and the 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 ECSG has analysed the impact of the [PSD2] and [RTS SCA/CSC] on the ECSG SEPA Cards Standardisation “Volume” and the outcome of that effort is contained in the present version.

Apart from defining requirements, the ECSG 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 card payments. It should be noted, however, that the ECSG 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 ECSG 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 SCS Volume may seem limited. This is due to the following factors:

- The ECSG remit is card payments only, while the [PSD2] has a much wider scope, including all types of electronic payments.
- The ECSG 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 card 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 ECSG.
- Some aspects that may indeed be in scope of the ECSG work, were considered too early to be standardized. Future versions of The Volume will re-evaluate these aspects accordingly.

The ECSG 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.

1.5.2 Work in progress

The EBA (European Banking Authority) has opened a Q&A Tool mechanism through which guidance on the open questions will gradually be made public over the next months. Some of the questions and answers may be such that the ECSG needs to work and incorporate the clarifications into the ECSG 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 Cardholder 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 Card Payments*, has been playing a critical role in the task of enhancing the

security of card payments. A specific Tokenisation business requirement has also been added to Book 7.

1.7 SRC (Secure Remote Commerce)

1.7.1 SRC summary presentation

SRC are a new EMVCo set of specifications related to remote commerce and the underlying card payment.

SRC aims to deliver the confidence experience with EMV chip and contactless in a remote environment globally (means e/mCommerce).

SRC is based on the principle of the interconnection of the issuing and acceptance platforms through a 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 minimizing the local storage of static Payment Data

This principle has the potential to increase security and frictionless of the transactions, reducing shopping cart abandonment. A recognizable 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 standardized APIs and SDKs.

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

- The SRC system, a technical platform operating an SRC Programme from a Payment system, orchestrating the services between the Digital Card Facilitator on the issuing side and the SRC Initiator on the acceptance one.
- The SRC Participating Issuer (SRCPI), the PSP issuer
- The Digital Card Facilitator (DCF): the consumer device where the digital card is enrolled. It can be a wallet on a mobile (mCommerce) or even a proxy in its browser for a Merchant WEB site
- The Digital Payment Application (DPA): the merchant remote payment application
- The SRC Initiator (SRCI): the merchant provider (ie payment gateway)

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 card payment process, the impacts of SRC are low as it is shown in this figure

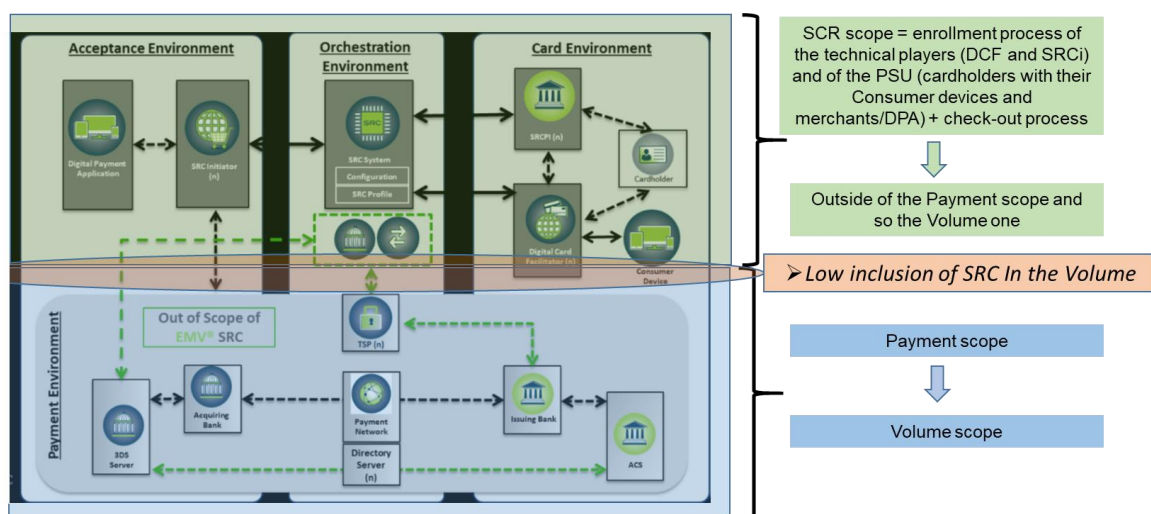


FIGURE 2: VOLUME AND SRC INTEGRATION

2 THE SCS VOLUME AND ITS BOOKS

2.1 Introduction to the “SEPA Cards Standardisation Volume”

This set of Books assembled into a version of the SEPA Cards 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 with cards. The ambition of the Volume is to set common foundations for better interoperability and for gradual convergence of the technical standards which underpin the card value chain from end-to-end.

Achieving greater standardisation in the European card 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 cardholders and card acceptors may not be disrupted. Greater standardisation must remain transparent to cardholders 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. In addition, in a number of countries retailers have recently completed a migration to EMV.
- 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 with cards an even more attractive proposition.
- Finally, SEPA is not an “island”. Standards for cards 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 cards standards”) across the cards value chain to meet the objective for achieving harmonised Europe-wide certifications and approvals. This includes principles and a framework for a card standardisation ecosystem.
2. These SEPA cards 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 ECSG Work on Cards Standardisation

2.2.1 Scope

The scope of ECSG’s work on cards standardisation in general, and of the present Volume in particular, is the definition and description of SEPA Cards 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 ECSG and is mentioned only for completeness..

2.2.2 Objectives

The Volume’s objective is to deliver a consistent cardholder and acceptor experience through harmonised functional and security requirements for cards services within its scope.

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

The functional and security requirements and the card 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 card industry, represented in the ECSG, to adopt and deliver a consistent cardholder and acceptor experience. The ECSG calls upon all other relevant parties throughout the card payment value chain to also

support, adopt and implement these SEPA Cards Standards in order to achieve a true SEPA for cards.

2.2.3 Impact on the Different Stakeholders

Stakeholders in card payments are notably: card schemes, vendors of cards & card acceptance solutions, retailers, acquirers, processors, issuers, certification entities, cardholders and consumers.

Any stakeholder wishing to present themselves as Volume compliant will have to comply with the set of Cards related 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 ECSG experts from the various sectors worked to define a recommended implementation path for the standards described therein. In the future, the ECSG 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: Card functional requirements and requirements for POI (Point of Interaction) to process card 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 cardholder data protection, Terminal to Acquirer Protocols, PIN, Cards (contact and contactless), Terminals/POI, Payment Gateways, Hardware Security Modules [HSMs] security requirements.

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

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

Book 6 - ***Implementation Guidelines***

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

Book 7 - ***Card Processing Framework***

Contents: Card 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 Card 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 ECSG 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 ECSG 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 ECSG. 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 ECSG 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 ECSG as its source is acknowledged and provided that prior written approval has been given by the ECSG. This Volume and all reproductions shall display the following copyright notice: “© 2016 European Cards 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 Cards Stakeholders Group AISBL (“ECSG”), 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 ECSG 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.

[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
[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)
[EMV B]	EMV® Contactless Specifications for Payment Systems (Book B)
[EMV C1 to C7]	EMV® Contactless Specifications for Payment Systems (Book C-1 to C-7)
[EMV CDCSVM BP]	EMV® Consumer Device Cardholder Verification Method— Best Practices, March 2019
[EMV CDCSVM 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 L1 CL]	EMV® Level 1 Specifications for Payment Systems, EMV Contactless Interface Specification
[EMV SBMP]	EMV® Mobile Payment, Software-based Mobile Payment Security Requirements v 1.1, September 2018
[EMV SB185]	EMV® Specification Bulletin No. 185, Biometric Terminal Specification
[EMVCo-FW v2]	EMV® Payment Tokenisation Specification – Technical Framework v2
[EMVCo]	EMV Secure Remote Commerce Specifications – API V 1.2
[EMVCo]	EMV Specifications – JavaScript SDK V 1.2
[EMVCo]	EMV Secure Remote Commerce Specifications – Version Management v 1.0
[EMVCo]	EMV Secure Remote Commerce Specifications – Data Dictionary v 1.0
[EMVCo]	EMV Secure Remote Commerce Specifications v 1.1
[EMVCo]	EMV Secure Remote Commerce User Interface Guidelines and Requirements v1.1.
[EPC Crypto]	EPC342-08: Guidelines on algorithms usage and key management
[EPC PS]	EPC343-08: EPC Privacy shielding for PIN entry
[EPC Mobile WP]	EPC492-09: White paper Mobile Payments
[EPC MCP IIG]	EPC178-10: Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines
[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
[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 encypherment
 - 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 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
[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 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
[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.
[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	CDCVM	Consumer Device CVM
AAC	Application Authentication Cryptogram	COTS	Commercial Off-The-Shelf
AAM	Active Account Management	CP	Contactless Payment
ACS	Access control service	CPA	Card Payment Application
AID	Application Identifier	CPoC	Contactless Payments on COTS
ATC	Application Transaction Counter	CPS	Card Payment Scheme
ATICA	Acquirer To Issuer Card Messages	CSC	Card Security Code
ATM	Automated Teller Machine	CVM	Cardholder Verification Method
AVS	Address Verification Service	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	ECSG	European Cards Stakeholders Group
CAT	Cardholder-Activated Terminal	EAL	Evaluation Assurance Level
CB	Certification Board	EMV	Europay MasterCard Visa
CC	Common Criteria	EPA	Embedded Payment Application
CCD	Common Core Definition	EPC	European Payments Council
CDA	Combined DDA/Application Cryptogram Generation	EPP	Encrypting PIN Pad
		EULA	End User License Agreement

fDDA	Fast Dynamic Data Authentication	MRP	Mobile Remote Payment
GSMA	GSM Association	NFC	Near-Field Communications
HMAC	Hash-based MAC	OS	Operating System
HPP	Hosted Payment Page	OTA	Over The Air
HSM	Hardware Security Module	OTP	One Time Password
ICC	Integrated Circuit(s) Card	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
MCC	Merchant Category Code	PTS	PIN Transaction Security
MCP	Mobile Contactless Payment	PVV	PIN verification value
MIT	Merchant Initiated Transaction	REE	Rich Execution Environment
MNO	Mobile Network Operator	RP	Remote Payment
MOTO	Mail Order - Telephone Order		

REE	Rich Execution Environment	TRSM	Tamper-resistant security module
RNG	Random Number Generator	TSP	Token Service Provider
SCA	Strong Customer Authentication	TSM	Trusted Services Management
SCD	Secure Cryptographic Device	UI	User Interface
SCRP	Secure Card Reader PIN	UID	Unique IDentifier
SCS	SEPA Cards Standardisation	UPT	Unattended Payment Terminal
SDA	Static Data Authentication		
SE	Secure Element		
SMS	Short Message Service		
SPoC	Software-based PIN entry on COTS		
SRC	Secure Remote Commerce		
SRCI	Secure Remote Commerce Initiator		
SRCPI	Secure Remote Commerce Participating Issuer		
SRED	Secure Read and Exchange of Data		
SSL	Secure Socket Layer		
T2A	Terminal to Acquirer		
TEE	Trusted Execution Environment		
TLS	Transport Layer Security		
TOE	Target OF Evaluation (CC)		
TPM	Trusted Platform Module		
TPP	Third Party Provider		

3.3 Definitions

This section contains all the definitions of terms used throughout the volume, except those regarding Tokenisation, which are contained in the *Annex - Tokenisation for SEPA Card Payments*.

A number of definitions originate from [IFR]. These are identified by the reference number in brackets used in Article 2 of the Regulation.

For example: (1) 'acquirer' means a payment service provider contracting with a payee to accept 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.

A.

AAC	Application Authentication Cryptogram, which is a Cryptogram generated by the card application. See [EMV B2].
Acceptance	In the field of cards, it refers to the process whereby a particular brand of card is accepted by a terminal, acceptor or other entity.
Acceptance Environment	Environment where the Card transaction is conducted in the Acceptor's domain. This Volume describes two Acceptance Environments: <ul style="list-style-type: none"> • 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 card schemes acceptance logo. The Payment will result in a transfer of funds in their favour. Sometimes also referred to as Merchant. Note: For payments, Acceptor is defined as "Payee" in [PSD2].

Acceptor Initiated Transaction (AIT)	<p>A Card Transaction initiated by the Acceptor based on stored Card Data, i.e. an MIT or a transaction where the Acceptor is the payer.</p> <p>Examples of Card 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).</p>
Acceptor Name	<p>The name of the Acceptor by which the Cardholder recognises the Acceptor.</p> <p>It is shown on displays to the Cardholder, printed on receipts or statements and is also used to identify trusted beneficiaries.</p> <p>For the purpose of Remote Transactions, it is unique for an individual Acceptor, at least at Acquirer level.</p>
Account Takeover (Fraud)	<p>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.</p>
Acquirer	<p>(1) 'Acquirer' means a payment service provider contracting with a payee to accept and process card-based payment transactions, which result in a transfer of funds to the payee;</p> <p>Note: In some cases, the Acquirer may also be an Acceptor.</p>
Acquiring	<p>The service performed by an Acquirer.</p>
Activated/Deactivated	<p>Indicates that a Card 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.</p>
Additional Authentication Device	<p>A Chip Card accepting PED which may or may not be connected to the consumer device and which includes an EMV Card Authentication Application.</p>
Address Data	<p>Data entered and transmitted for MOTO transactions consisting of the numeric characters from the address.</p>
Application Cryptogram [AC]	<p>A cryptogram generated by the Card Payment Application in response to a GENERATE AC command.</p>
Application Identifier (AID)	<p>A Data Element specified by ISO/IEC 7816-5 which in the context of the Volume encodes a unique identifier of an EMV Application</p>
Application Profile	<p>An Application Profile determines the configurable parameters which are used to process a Card Service by the POI Application.</p>
Approval Body	<p>A body which performs Type Approval.</p>
ARQC	<p>Authorisation Request Cryptogram, which is a Cryptogram generated by the Card Application to request an online authorisation for the transaction. See [EMV B2].</p>

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 (POI)	An attendant (an agent of the card acceptor) is present at the Physical POI and participates in the transaction by entering Card Service-related data.
Authentication	The provision of assurance of the claimed identity of an entity or of data origin.
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.
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 Card Service or not. It can be processed off line by the Card 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).

B.

Balance Enquiry	A service which allows the cardholder to request information about their account balance.
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	<p>An identity verification method of a Cardholder based upon one or more intrinsic physical characteristics of that Cardholder, either biological and physiological (e.g. fingerprint, iris, face, vein and voice) or behavioural (e.g. signature dynamics, typing patterns) characteristics.</p> <p>For the Volume, only automatically verifiable biological and physiological Biometrics are presently considered.</p>
Biometric Capture Device	A secure device that allows the capture of Biometric data from the cardholder at the POI
Biometric Data	<p>Physical or physiological (e.g. fingerprint, iris, face, vein and voice), or behavioural (e.g. signature dynamics, typing patterns) characteristics of a Cardholder/individual, which allow or confirm the unique identification of that Cardholder/individual.</p> <p>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].</p>
Biometrics on Consumer Device	<p>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.</p> <p>Biometrics on Consumer Device is a type of CDCVM.</p>
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.
Brand (also Card Payment Brand)	A product (especially a card) or family of products that have been licensed by their owner for use in a given territory.
Business Day	A day on which the relevant payment service provider of the cardholder 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.

C.

Cancellation (Card Service)	A Card Service which allows the card 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 Cardholder Available Funds.
Cancellation (Technical Process)	A process that can be instigated by the cardholder 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	An account held by a PSP which will be used for one or more Card Services and which is related to a specific Cardholder. A Card Account 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	Software and associated Card Data used to perform a Card Service, including the following types: <ul style="list-style-type: none"> • EMV Card Payment Application (Physical Card) • Mobile Contactless EMV Payment Application (Mobile Device) • EMV Card Authentication Application (Physical Card) • (Mobile) Authentication Application (Consumer Cardholder Device) • (Mobile) Remote Payment Application (Consumer Remote Cardholder Device).
Card Authentication	A Function by which a chip Card Data is authenticated by the POI Application (Offline Card Authentication), by an Additional Authentication Device and/or by the Issuer (Online Card Authentication).
Card Based Language Selection (Optional)	A Function by which the language can be selected for on-screen dialogues or print-outs.
Card-Based Payment Instrument	(20) ‘card-based payment instrument’ means any payment instrument, including a card, mobile phone, computer or any other technological device containing the appropriate payment application which enables the payer to initiate a card-based payment transaction which is not a credit transfer or a direct debit as defined by Article 2 of Regulation (EU) No 260/2012;
Card Based Payment Transaction	(7) ‘card-based payment transaction’ means a service based on a payment card scheme's infrastructure and business rules to make a payment transaction by means of any card, telecommunication, digital or IT device or software if this results in a debit or a credit card transaction. Card-based payment transactions exclude transactions based on other kinds of payment services;

Card Data	A data set used to perform a Card Service that allows the identification of the Card account to which the Card was issued.
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 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 Card Data where 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 Present	Transaction based on card-related information with the Card being physically presented to the Acceptor.
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 Scheme (or Card Payment Scheme or Scheme)	A card payment scheme is a technical and commercial arrangement (often referred to as the "rules") between parties in the Card Value Chain, resulting in a set of functions, procedures, arrangements, rules and devices that enable a Cardholder to perform a payment transaction, and/or cash withdrawal or any other Card Service. Any party may join a Card Scheme, as long as the rules of that Card scheme are met.

Card Security Code (CSC)	<p>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.</p> <p>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).</p> <p>These code values help validate two things: The customer has the credit card in his/her possession. The card account is legitimate.</p> <p>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.</p>
Card Service	A process to perform or support financial transactions based on Card Data in the Card environment.
Card Standardisation Ecosystem	The complex of the SEPA cards community interacting with its environment in the field of Volume conformance.
Card Transaction	A transaction used to perform a Card Service. A Card Transaction is a Local (Card) Transaction or a Remote Transaction.
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	<p>A Person or entity to whom a Card Application has been issued, or one who has been authorised to use the Card Application.</p> <p>Note: Cardholder is defined as "Payer" in [PSD2].</p>
Cardholder Available Funds	The funds available for use by the Cardholder, 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 Environment	The source from where Card Data is retrieved when performing a Card transaction. These are Physical Card, Virtual Card and Consumer Device.
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 card 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 Card Service at an attended POI which enables a Cardholder 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 Card Service which allows the cardholder to deposit cash to their own card account(s). It can take place <ul style="list-style-type: none"> • 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
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 card payment component (POI, card, etc.) with a given set of requirements and specifications.
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 Card 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)	<p>A carrier into which one or more integrated circuits are inserted to perform processing and memory functions and which</p> <p style="padding-left: 40px;">supports the contact interface and complies with [EMV B1] (referred to as Contact Chip Card)</p> <p style="padding-left: 40px;">and/or supports the contactless interface and complies with [EMV D] (referred to as Contactless Chip Card).</p> <p>A Chip Card which supports the contact and contactless interface is referred to as Dual Interface Card.</p> <p>A Contact Chip Card as well as a Dual Interface Card complies with [EMV B1] and must be of the ID 1 form factor (as defined in ISO/IEC 7810).</p> <p>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.</p> <p>Note that a Mobile Device is not considered as Chip Card, even if it supports the contactless interface and complies with [EMV D].</p> <p>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.</p> <p>Also referred to as Smart Card.</p>
Chip Contactless	<p>An Acceptance Technology where Card Data is retrieved from the chip of a Chip Card over the contactless interface compliant with [EMV D]. 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.</p>
Chip with Contact	<p>An Acceptance Technology where Card Data is retrieved from the chip of a Chip Card over the contact interface compliant with [EMV B1]. 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).</p>
Choice of Application	<p>See article 8 as well as recital 40 of the IF Regulation [IFR]</p>
Clearing	<p>The process of exchanging financial transaction details between an acquirer and an issuer to facilitate both the posting of transactions to cardholders' accounts and the reconciliation of an institution's settlement position.</p>
Cleartext	<p>See Plaintext.</p>
Click to Pay Icon	<p>A visual representation that identifies that SRC is available to the Cardholder.</p>
Co-Badging	<p>(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;</p>

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)	A type of offline dynamic data authentication where the card combines generation of a cryptographic value (dynamic signature) for validation by the POI with the generation of an Application Cryptogram to verify that it originates from a valid card. See [EMV B2].
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 issuer payment application that complies with the CCD requirements, and defines card applications, 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: <ul style="list-style-type: none"> • Complete the transaction for the Card Application • Inform Cardholder, Attendant and/or Acquirer about the result of the transaction • Deliver a receipt to Cardholder 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	(3) 'consumer' means a natural person who, in payment service contracts covered by this Regulation, is acting for purposes other than the trade, business or profession of that person;

Consumer Device	<p>An internet and/or NFC capable device used by the Cardholder to conduct Card Services. It is either</p> <ul style="list-style-type: none"> • a Mobile Device used for Mobile Contactless or Mobile Remote Transactions, • An Electronic Device used for Remote Transactions <p>It can be a carrier of Credentials or a Card Application. It may include a user interface that enables the Cardholder to enter data.</p> <p>This is sometimes referred to as Cardholder Controlled Device or Cardholder Operated Device.</p>
Consumer Device Cardholder Verification Method (CDCVM)	<p>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</p> <p>The types of CDCVM defined in the Volume are:</p> <ul style="list-style-type: none"> • Biometrics on Consumer Device • Offline Mobile Code • Offline Personal Code
Contactless	<p>If it is not necessary to distinguish the Cardholder Environment 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 D] and communicate and behave the same.</p>
Contactless Payment	<p>A payment processed using the Chip Contactless Acceptance Technology or the Mobile Contactless Acceptance Technology.</p>
(Mobile) Contactless Payment Application	<p>A Mobile Contactless Card Payment Application or a Contactless EMV Card Payment Application</p>
COTS Device	<p>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.</p>
COTS Solution	<p>A COTS solution is made up of the following components:</p> <ul style="list-style-type: none"> - COTS Device - Payment Application on the COTS Device - Back-end monitoring system - SCRIP (where necessary)
COTS System Baseline	<p>Summary of permitted COTS Device versions of hardware and firmware to be used as part of a COTS Solution submitted by the solution provider.</p>

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	<p>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.</p> <p>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.</p>
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.

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.
----------	--

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 card 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 Cardholder 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 cardholder to select the currency of the transaction for a given Card Service, choosing between the cardholder's currency and the card acceptor's currency.
Dynamic Data Authentication (DDA)	A method of offline data authentication used by a chip enabled device to validate the authenticity of the chip data and the card, using a public key algorithm to generate a cryptographic value, including transaction specific data elements, validated by the POI to protect against counterfeit or skimming. Two forms of offline dynamic data authentication are defined by EMV B2: DDA and CDA.

E.

e-Commerce	A Remote Transaction usually initiated by the Cardholder 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 cardholder to transfer funds between an electronic purse and his card account.
EEA issued cards	A Chip Card or MCP Application issued in the EEA (European Economic Area).
Electronic Device	Personal device with communication capabilities such as internet, Wi-Fi ... Examples of Electronic Devices include PCs...
Electronic 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 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 Card Authentication Application	A Card Application based on EMV and stored on a Physical Card to perform an Authentication for Remote Payments using an Additional Authentication Device.
EMV Card Payment Application	<p>A Card Application according to EMV and stored on a Physical Card. Each EMV Card Payment Application is identified by an Application Identifier (AID).</p> <p>An EMV Card Payment Application may be contact, contactless or both.</p> <p>An EMV Card Payment Application is called a Contact Card Payment Application if it supports transaction processing for the Acceptance Technology "Chip with Contact".</p> <p>It is called a Contactless EMV Card Payment Application if it supports transaction processing for the "Chip Contactless" Acceptance Technology.</p>
EMV Online Authentication	Authentication of the Card Application using Application Cryptograms with online communication to the issuer.
EMVCo	An LLC formed in 1999 by Europay International, MasterCard International and Visa International to enhance the EMV Integrated Circuit Card Specifications for Payments Systems. It manages, maintains, and enhances the EMV specifications jointly owned by the payment systems. It currently consists of American Express, Discover, JCB, MasterCard, Union Pay and VISA.
Encryption, Encipherment	(Reversible) Transformation of data by a cryptographic algorithm to produce cipher text, i.e., to hide the information content of the data.

European Cards Stakeholders Group (ECSG)	<p>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.</p> <p>The CSG was disbanded in the year 2016 and a separate legal entity was established under the name of European Cards Stakeholders Group (ECSG) AISBL in April 2016.</p> <p>The purpose of the ECSG, as a multi-stakeholder association, is to support and promote European card standardisation with market-driven implementation.</p> <p>The mission of the ECSG is to:</p> <ul style="list-style-type: none"> - Maintain and evolve the Volume in line with market needs, reflecting the evolution of card payment technology; and - Promote Volume conformance throughout the card payments value chain, to enable a more harmonised SEPA card payment ecosystem. <p>In order to fulfil its purpose and mission, the ECSG aims to organise the card payments related standardisation dialogue amongst the stakeholders involved in the card ecosystem and to liaise with regulatory and oversight authorities in relation to card payment standards.</p>
European Economic Area (EEA)	<p>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.</p>
Evaluation Assurance Level	<p>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.</p>
Evaluation Methodology	<p>A methodology that will be used to evaluate compliance and assurance level with a specific implementation specification,</p>

F.

Face-To-Face (Card) Payment	See Local (Card) Payment
Face-To-Face (Card) Transaction	See Local (Card) Transaction

Fast Dynamic Data Authentication (fDDA)	An accelerated method of Dynamic Data Authentication (DDA) that leverages DDA as defined in [EMV 4.3] specifications. Used in contactless transactions allowing the POI to issue READ RECORD commands, obtaining DDA related data from the Card 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 Card service.
Funds	Banknotes and coins, scriptural money and electronic money as defined in [EMD]

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.
----------------------	---

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.

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 requirements.
Imprint	Image of the embossed card data on the front of a card.
Instalment Payment	A Card Service where the Cardholder 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 cardholder'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.
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 card industry area 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	(2) 'issuer' means a payment service provider contracting to provide a payer with a payment instrument to initiate and process the payer's card-based payment transactions; Note: This PSP can be a member of a Card Payment Scheme.
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.

J.

K.

Kernel	A piece of terminal application software that supports the EMV payment application functions as defined in the EMV specifications. The non-EMV functionality 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 cards can be called a kiosk.

L.

Labelling	Optional Volume conformance process based on self-assessment for detailed implementation specifications.
Laboratory	In the context of the SCS 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 (Card based Language Selection without cardholder or attendant interaction) or manually (Manual Language Selection by the cardholder or attendant), the language used on the POI for communication with the cardholder.
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 cardholder 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 Card Transaction	A Card Transaction initiated at the Acceptor's Physical POI.
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)

M.

m-Commerce	A Remote Transaction initiated by the Cardholder 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: <ul style="list-style-type: none"> 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.
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;
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	A Card Application stored or accessed via a (Mobile) Consumer Device used to support the authentication process in a Remote Transaction. It supports transaction processing for the Acceptance Technology "Consumer Device with Credentials and Authentication Application".
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: <ul style="list-style-type: none"> • An Offline Mobile Code may be used for Local Transactions and for m-commerce transactions. It is verified in one of the following ways: <ul style="list-style-type: none"> ○ 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 Card Data is retrieved from a Mobile Contactless Payment (MCP) Application in a Mobile Device over the contactless interface compliant with [EMV D].

Mobile Contactless Card Payment Application	A Card Application according to EMV and stored on a Mobile Device. Each Mobile Contactless Card Payment Application is identified by an Application Identifier (AID). It supports transactions processing for the Acceptance Technology “Mobile Contactless”.
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	<p>Acceptor controlled device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth ...</p> <p>Examples of Mobile Devices for Acceptance include MPOS, mobile phones, smart phones and tablets.</p> <p>Also referred to as a ‘Mobile Acceptance Device’</p>
(Mobile) EMV Payment Application	<p>Software and associated Card Data used to perform a Card Service, including the following types (for Physical Cards or for Mobile Devices):</p> <ul style="list-style-type: none"> • EMV Card Payment Application (Physical Card) • Mobile Contactless EMV Payment Application (Mobile Device)
Mobile Remote Payment (MRP)	A remote payment initiated through a mobile device.
(Mobile) Remote Card Payment Application	A Card Application stored on/or accessed via a (Mobile) Remote Device used to perform a (Mobile) Remote Transaction. It supports transaction processing for the Acceptance Technology “Consumer Device with (M)RP 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 cardholder 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	<p>A Remote Transaction conducted in the Acceptor's environment using Manual Entry with the Cardholder usually interacting remotely for Mail Order or Telephone Order (MOTO).</p> <p>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 Cardholder via a Virtual Terminal.</p> <p>For some Card 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.</p>
------	--

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 card acceptor to charge the cardholder's account if a cardholder fails to cancel or use a reservation for car hire or a room rental.

O.

Offline Biometric Verification	A Cardholder Verification Method defined in [EMV SB185], 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 the card is validated at the point of transaction, using public key technology to protect against counterfeit or skimming. Four forms of offline data authentication are defined by EMV: SDA, DDA, CDA and fDDA.
Offline Enciphered PIN	An Offline PIN whereby the PIN is transmitted to the card encrypted using public key cryptography at the POI's PIN Entry Device.
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 the Card Application.
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-Loop Versus Closed-Loop Payments Networks	General purpose and limited-purpose payments networks primarily operate under two different business models. Open-loop payments networks, such as international schemes, are multi-party and operate through a system that connects two financial institutions - one that issues the card to the cardholder, 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 cardholders by the owner of the network without involving third-party financial institution intermediaries.
Original Credit	A service which allows the card acceptor to perform a credit to a cardholder's account. An original credit is not preceded by another card payment.
Over the air (OTA)	A method of distributing software to mobile phones and provisioning handsets with the settings necessary to access messaging services.

P.

PAN	Primary Account Number (see Payment Card Numbers). A series of digits which identify a customer account or relationship. This number contains a maximum of 19 digits according to ISO/IEC 7812.
Partial Approval	An Authorisation response of an amount that is less than the amount expected.

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; Note: Payee is called "Acceptor" in the Volume.
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; Note: Payer is called "Cardholder" in the Volume.
Payment	The basic service which allows the cardholder to pay for the purchase of goods and services from a card acceptor using their card application or credentials.
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	(21) 'payment application' means computer software or equivalent loaded on a device enabling card-based payment transactions to be initiated and allowing the payer to issue payment orders;
Payment Brand	(30) 'payment brand' means any material or digital name, term, sign, symbol or combination thereof, capable of denoting under which payment card scheme card-based payment transactions are carried out;
Payment Card	(15) 'payment card' means a category of payment instrument that enables the payer to initiate a debit or credit card transaction; Note: This Payment Card can offer the cardholder the ability to make payments for goods and services, either at an accepting device or remotely (via MOTO, e- or m-commerce - these are known as "card-not-present" transactions) or to access cash at an ATM.
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;
Payment Completion	A Card 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 Card 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 Cardholder for the purposes of authentication.
Payment Gateway	A service operated by an Acquirer that switches authorisation requests and clearing records between the Acceptor and the Acquirer.
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	(19) 'payment instrument' means 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;
Payment Order	(23) 'payment order' means any instruction by a payer to its payment service provider requesting the execution of a payment transaction;
Payment Page	A page presented through the Virtual POI to the Cardholder which enables the entry of Card Data via the Consumer Device.
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;
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	Execution of payment transactions, cash withdrawal and other services as defined in the Payment Services Directive.
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 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 a 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 Cardholder to obtain cash from the Acceptor in conjunction with a Payment (also referred to as Cashback). The Cardholder 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 on line 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 Cardholder 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 Cardholder, 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 Card Data is retrieved in the Acceptor's Domain. A Physical POI consists of hardware and software which enables a Cardholder and/or an Acceptor to perform a Local Card 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.
Plaintext	Unenciphered/unencrypted information.

Point of Interaction (POI)	A POI is a Physical POI or a Remote POI.
POI Application	<p>An application consisting of software and data used to perform a Card Service. 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.</p> <p>A POI Application on a Physical POI for processing Local Transactions may be referred to as Physical POI Application.</p> <p>A POI Application on a Virtual POI may be referred to as Virtual POI Application.</p> <p>A POI Application on a Physical POI or a Virtual Terminal for processing MOTO transactions is referred to as MOTO Application</p>
Point of Sale (POS)	<p>(29) 'point of sale' means the address of the physical premises of the merchant at which the payment transaction is initiated. However:</p> <p>(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;</p> <p>(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;</p> <p>(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;</p>
Pre-Authorisation Services	<p>A service composed of 3 linked steps:</p> <ul style="list-style-type: none"> • Pre-Authorisation • Update Pre-Authorisation (potentially with several occurrences) • Payment Completion <p>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.).</p> <p>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.</p> <p>The Payment Completion allows the Acceptor to finalise the payment.</p>
Preferred Application	Application selected by the Payee through the Priority Selection mechanism as defined in the [IFR].

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
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 Card 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 cardholders and/or stakeholders of the SEPA card transaction chain.
Protocol	A pre defined sequence of exchanged messages between two communicating parties required to implement a function. <ul style="list-style-type: none"> Some protocols are executed in the A2I domain, some could be in the Terminal-to-Acquirer or in the Card-to-Terminal domain. The card processing requires the execution of different protocols. Several models of usage of protocols exist that provide either clearing, authorization or both services. <p>Protocols consist of a different set of message types (i.e. advices, requests, reversals, charge-backs, etc.)</p>
Proximity Payment	See Contactless Payment.

Proximity Payment System Environment (Contactless Only)	A standard application that is used by contactless terminals to determine which of the active applications should be used for payment. On a contactless card, it contains the list of all card applications supported by the contactless interface, and is returned from the card in response to the reader issuing a 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.
PIN Transaction Security (PTS)	PTS is a set of modular evaluation requirements managed by PCI Security Standards Council, for PIN acceptance POI terminals.
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.
PVV	PIN verification value. Discretionary value encoded in Magnetic Stripe of payment card.

Q.

Quasi-Cash Payment	A Card Service which allows the cardholder to obtain items which are representative of actual cash and directly convertible to cash. Examples include gaming chips, travellers cheques.
--------------------	---

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	<p>A Card Service where the Cardholder authorises an Acceptor to charge their account on a recurring basis and without a specified end date.</p> <p>This applies to Payments and Deferred Payments performed on a recurring basis.</p>
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 Service is completed with a voice conversation to obtain an approval code. This Function does not necessarily involve the Card Application or the Cardholder.
Refund	A Card Service which allows the card acceptor to reimburse the cardholder 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	<p>The initial point where Card Data is retrieved in the Acceptor's domain for Remote Transactions.</p> <p>The Remote POI exists in a variety of technical platforms which enable a Cardholder and/or an Acceptor to generate a Remote Transaction.</p> <p>The Remote POI is either a Virtual POI or a Virtual Terminal.</p>

Remote Transaction	A Card Transaction conducted at the Acceptor's Remote POI. A Remote Transaction is usually initiated by the Cardholder 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-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)

S.

Scheme Participant	A party having signed a License Agreement with a Card Scheme in order to provide Card Services for Card Payment Brands of the Scheme. Examples of Scheme Participants are Acquirers and Issuers.
Secure Element (SE)	<p>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.</p> <p>There are three different form factors of SE: Universal Integrated Circuit Card (UICC), embedded SE and microSD. Both the UICC and microSD are removable.</p>
Secure Environment	<p>A system which implements the controlled storage and use of information. A secure environment is used to protect personal and/or confidential data.</p> <p>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.</p>
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.
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 Consumer and facilitates the payment information exchange among all SRC System participants.
Selection of the Application	<p>For the Acceptance Technologies Chip with Contact, Chip Contactless and Contactless with Mobile, it is the function which allows the selection of an application supported by both the card and the POI as well as an Application Profile used to process a service for a transaction.</p> <p>For the Acceptance Technologies referred to as e- & m-Commerce, it is the function which allows the selection of a brand/card product by the cardholder.</p>
Semi-Attended	The cardholder conducts the transaction at the Point of Interaction without the participation of an attendant (agent of the card acceptor or of the acquirer). However an attendant is present to provide assistance to the cardholder if necessary. Therefore, for the purpose of this document, Semi-Attended is categorised as Attended.
Sensitive Payment Data	Data which allows control over the Cardholder Account or which may be used to carry out fraud.
Sensitive Personal Data (Special Category of Personal Data)	<p>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.</p> <p>The Personal Data Processing of the Sensitive Data must be performed in accordance with the [GDPR] including the requirement to obtain explicit consent.</p>
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.
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 cardholder 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 Card services and/or products.
Specification Provider	<p>Organisation which:</p> <ul style="list-style-type: none"> • 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.
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)	A type of offline Card 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 Card Data	<p>Acceptance Technology where PAN or Payment Token and Expiry Date have been provided prior to the transaction and stored securely for later use. This Acceptance Technology is used for Card Not Present transactions.</p> <p>In the specific scenario where the data is securely stored within the Acceptor's domain, this can also be referred to as Card on File.</p>
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 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]. The Cardholder Verification function may be used as a factor towards SCA, but other factors may be required.
Surcharging/Rebate	A feature which allows the card acceptor to charge a fee or give a rebate to the cardholder in relation to a given Card Service.
Switch	The routing centre that transfers authorisation requests, approvals and card 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.

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 the 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 Card Data in the context of Authorisation and Settlement for a Card 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 Card Service for the next transaction and where the transaction amount is set, transaction data is initialised and processing of the Card 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.

U.

Unattended (POI)	The Cardholder 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.

V.

Value Chain	A chain of activities by different Service Providers and Vendors in order to deliver a Card 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	<p>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.</p> <p>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.</p> <p>The Virtual POI includes a Payment Page which may be presented to the Cardholder from either a Payment Gateway or the Acceptor's website.</p> <p>The Virtual POI may also facilitate (redirection) services to support Authentication of the Cardholder by the Card Issuer for e-and m-Commerce.</p> <p>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.</p>

Virtual Terminal	<p>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.</p> <p>A Virtual Terminal can also be used by the Cardholder, but only for Telephone Orders if DTMF technology is used.</p> <p>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.</p>
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 Cards 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 SCS Volume conformance.

W.

X.

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

Y.

Z.

4 FIGURES

FIGURE 1: VOLUME OVERVIEW	10
FIGURE 2: VOLUME AND SRC INTEGRATION	17