EPC020-08 11.02.2015

(Vol Ref. 7.1.1.05)

SEPA CARDS STANDARDISATION (SCS) "VOLUME"

BOOK 1

GENERAL

Payments and Cash Withdrawals with Cards in SEPA

Applicable Standards and Conformance Processes

Abstract	This document contains the work on SEPA cards standardisation to date
Document Reference	EPC020-08
Issue	Book 7.1.1.05
Date of Version	11 February 2015
Reason for Issue	Consultation
Reviewed by	CSG
Produced by	CSG Secretariat
Owned by	EPC
Circulation	Public

Table of Contents

1 GENERAL

1.1 Volume - Document change history

Version number	Dated	Reason for revision
Change history of the Volume **before** splitting into several Books (2012)		
3.0	05.12.2008	Resolution covering the Volume approved at 17.12.2008 Plenary and announcing some editorial changes in the upcoming months
3.1	17.02.2009	IPR issues - Part 2 (annexes not published)
3.2	02.03.2009	Migration of some contents of Part 2 into Part 1 (definitions, A2I study on ISO 20022)
3.2.1	15.03.2009	Layout and corrections
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 NB: Volume BoR v 5.0 of Chapter 5 on the SEPA single set of security requirements has been updated in order to include both cards and terminal requirements; Volume BoR version 5 of Chapter 5 is made available for consultation on further additions.
5.5	01.06.2011	Version for public consultation
5.6	17.10.2011	Version for review by the CWG
5.7	01.11.2011	Version for review by the CSG
5.8	08.11.2011	Final CSG/CWG Validation
5.9	14.11.2011	Version for the approval process for publication, by CoCo and Plenary
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

Change history of Volume		
6.1.0.01		Working version of Book 1
7.1.1.00		EPC approved version - Volume v7.0
7.1.1.01		Working version 2014
7.1.1.05		Consultation version for CSG GM Approval - Feb 2015

43

44

1.2 Executive summary

Goal and Addressees - This document (The "Volume") is ultimately designed for the benefit of Payment Service Users in Europe (such as cardholders and merchants), *enabling them to use general purpose cards to make and receive payments and cash withdrawals in euro 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.

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

Card Services - The Volume provides functional requirements applicable to transactions either initiated by a Card[1]at the card acceptor's terminal as Card Present transactions, or, in future versions, as Card Not Present (remote) transactions. These transactions result in the provision to the cardholder and merchant of the so-called "Card Services" specified in the Volume and processed through a succession of Functions.

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 out of the sole influence of the EPC and CSG and appropriate harmonisation measures can only be taken by the relevant regulatory authorities.

In the incorporation of e- & m-commerce into this version of the Volume, the CSG took into consideration the recommendations being addressed in the SecuRe Pay work, as well as the ongoing discussions related to security in PSD2.

[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.

This Volume aims to take into account the recent publication of the EBA Final guidelines on the security of internet payments[2], based on the earlier SecuRe Pay recommendations. The Volume includes cross references as appropriate. Since the SecuRe Pay Recommendations for the security of mobile payments were at the time of publication of the current version of the Volume not yet finalised, the CSG is awaiting final publication of those recommendations prior to addressing them in the Volume.

The consultation period and maintenance process will also be used to ensure continued alignment with these publications.

In the event that inconsistencies would be identified, the text of the relevant regulatory documents shall prevail.

Volume Conformance via Labelling (i.e. a voluntary self-assessment process), Certification and Type Approval - Managing the Volume is an intensive self-regulatory project based on market consensus. Whilst favouring technical interoperability and convergence, all contributors must work in accordance with applicable rules and regulations governing competition matters.

A check of SEPA conformance is currently not performed by Regulators. The Volume requirements are thus not formally imposed on market stakeholders. However, its rules are defined by market experts, and the ECB and the European Commission provide guidance and actively contributed to this work. Consequently strong market support is expected.

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

Schemes, Acquirers and Terminal Vendors should consider the usability for visually impaired when designing Payment Solutions. This is especially important for local transactions.[3]

Implementation monitoring - Migration dates and overall deadlines are also supplied in this release of the Volume as agreed by the different CSG 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 will be organised and conformance results made public on the internet.

[2] EBA/GL/2014/12

[3] To assist visually impaired customers, the "5" key must 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.

Please note that 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***.

Volume Maintenance principles - Future Volume reviews will continue to take into consideration the interest of all stakeholders involved in the card business and the use of card services. It will also be regularly updated to ensure alignment with the relevant European rules and regulations. A full revision of the Books composing the Volume will be organised in 2015, after the revised Payment Services Directive will be released. Such a revision is expected to last two years ending with Volume v8.0 expected to be published in 2017. In the meantime, individual Books may be updated in between depending on the urgency. In both cases, a formal public consultation process will be organised.

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.

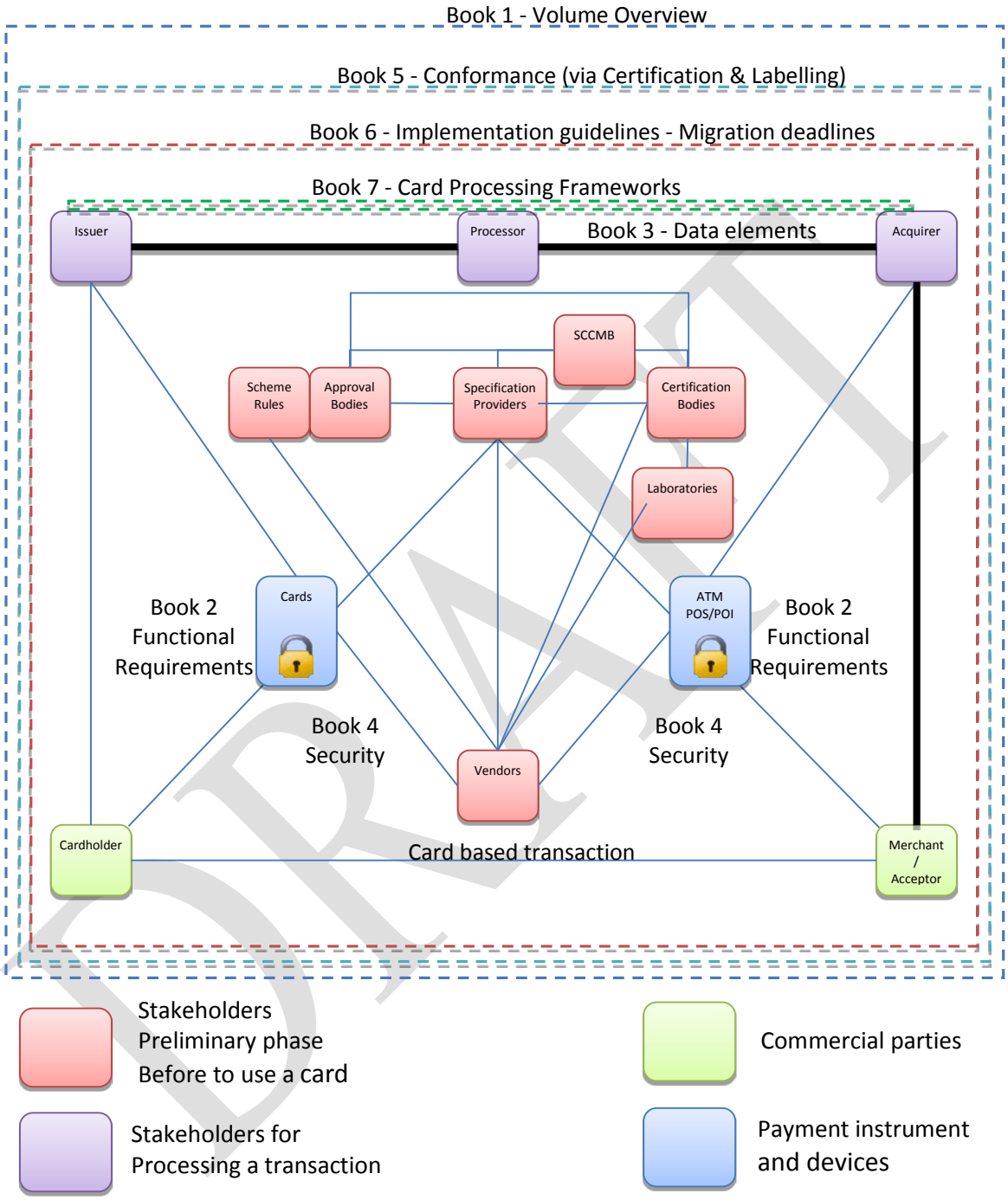

FIGURE1: VOLUME OVERVIEW

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

- Book 1 - ***General***
- 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***

1.3 Description of changes since the last version of Book 1

Change history of Book 1		
7.1.2.00		Working version 2014/2015 Intended to improve the concepts definition and wording of Volume v7.0 (F2F) and to integrate Remote Payments

2 THE SCS VOLUME AND ITS BOOKS

2.1 Introduction to the "SEPA Cards Standardisation Volume"

This set of Books bundled into a version of the SEPA Cards Standardisation Volume (hereafter referred to as the "Volume") builds on the EPC SEPA Cards Framework that has been available since 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 foundations for 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 these equipments up to now naturally reflect more individual decisions 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.
- Manufacturers 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 the card standardisation ecosystem. It will be up to each market participant to decide whether become SCS Volume conformant and henceforth, to respect all published requirements according to their activities.
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 effectively in line with the standards referred to above.

2.2 Scope and Objectives of CSG Work on Cards Standardisation

2.2.1 Context

At an early stage of the standardisation process, the European Payments Council published the SEPA Cards Framework (SCF) to establish high level principles and rules. When implemented by banks, schemes, processors and other stakeholders such as retailers, these will enable Payment Service Users in Europe (such as cardholders and merchants) to use general purpose cards to make or receive payments and cash withdrawals in euro throughout the SEPA area with the same ease and convenience as they do in their home country.

The SCF acknowledges that a further piece of work is required so that the commitment to cardholders that there are "no differences whether they use their card(s) in their home country or somewhere else within SEPA" is delivered in the most efficient manner by banks and schemes. The necessity for deeper standardisation has also been highlighted by European policy makers. The Volume was created as a more detailed publication that complements the SCF.

2.2.2 Scope

The scope of EPC's work on cards standardisation in general, and of the present Volume in particular, is the definition and description of SEPA Cards Standards for the interoperability of card payment and cash withdrawal services, provided or implemented by the different stakeholders including Volume compliant card schemes, issuers, acquirers, processors, vendors and merchants.

2.2.3 Objectives

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

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

The functional and security requirements and the card standardisation ecosystem are called the "SEPA Cards Standards". They also include functional architecture, description of processing flows as well as uses and definitions for data elements.

These SEPA Cards Standards represent a commitment from the main stakeholders of the European card industry represented in the CSG for adoption and implementation. The CSG Members call upon all other relevant parties throughout the card payment value chain also to support, adopt and implement these SEPA Cards Standards in order to achieve a true SEPA for cards.

2.2.4 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 these Cards Standards. 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.

2.2.5 Implementation of the SEPA Cards Standards and Monitoring

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

2.2.6 Implementation Specifications

The current version of the SEPA Cards Standards does not include implementation specifications. The choice of implementation specifications in line with the SEPA Cards Standards is up to the market. Stakeholders will continue to be free to develop and select implementation specifications which will allow for differentiation and 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***

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, Terminals/POI, Payment Gateways, Hardware Security Modules [HSMs] and Contactless security requirements.

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

Contents: Description of the CSG 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.

2.3.2 Maintenance cycles

1. A full revision of all Books will start in 2015, will last two years and will conclude with the publication of Volume v8.0. Target date for publication will be 2017.

However individual Books may be reviewed in a single year cycle in 2015/2016 depending on the urgency.

2. The maintenance of the Volume is organised by the CSG 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 CSG and EPC public websites.

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 EPC.

Neither potential or actual users of this Volume, nor any other person shall assert contrary claims, or deal with the Volume in a manner that infringes or is likely to infringe the copyright held by the EPC in the Volume.

Parts of the present document are based on contributions by the participants to the EPC Cards Standardisation Process. When invited to participate in the EPC Cards Standardisation Process, participants were informed and agreed that one of the primary objectives of the work undertaken is to ensure that European banks and other stakeholders, including the schemes in which they participate, have open and free access to, and free usage of, the standardisation work performed. In order to maximize efficiency all participants also acknowledged that the work to be undertaken would capitalize to the greatest extent possible on existing initiatives, with the additional objective to recognize the needs of all relevant stakeholders, coordinate work underway, agree deadlines and monitor deliverables.

Whilst acknowledging the provenance of such material as originating with the participants thereto, the intellectual property rights, copyright and rights of development and disposal reside exclusively with the EPC.

The Volume can be reproduced, redistributed and transmitted for non-commercial purposes by any interested party, as long as the EPC as its source is acknowledged and provided that prior written approval has been given by the EPC.

3 REFERENCES, ABBREVIATIONS AND DEFINITIONS

3.1 References

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

[CPA]	EMV Integrated Circuit Card Specifications for Payment Systems, Common Payment Application Specification
[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
[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 C4]	EMV Contactless Specifications for Payment Systems. (Book C-1 to C-4)
[EMV D]	EMV Contactless Specifications for Payment Systems (Book D)
[EMV M1]	EMVCo Handset Requirements for Contactless Mobile Payment
[EMV M2]	EMVCo Application Activation User Interface
[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
[FIPS 140-2]	Security Requirements for Cryptographic Modules + Annexes
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 7816-5	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 Version 3.0
[PCI P2PE]	Payment Card Industry Point to Point Encryption Version 1.0
[PCI DSS]	Payment Card Industry Data Security Standard Version 3.0
[PCI PA-DSS]	Payment Card Industry Payment Application Data Security Standard Version 3.0

[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]	European Commission proposal for a revised PSD.

3.2 Abbreviations

Acronym	Standing for
A2I	Acquirer to Issuer
AAC	Application Authentication Cryptogram
AID	Application Identifier
ATC	Application Transaction Counter
ATICA	Acquirer To Issuer Card Messages
ATM	Automated Teller Machine
AVS	Address Verification Service
BIN	Bank Identification Number
C2T	Card to Terminal
CA	Certification Authority
CAM	Card Authentication Method
CAT	Cardholder-Activated Terminal
CB	Certification Board
CC	Common Criteria
CCD	Common Core Definition
CDA	Combined DDA/Application Cryptogram Generation
CPA	Card Payment Application
CPS	Card Payment Scheme
CSC	Card Security Code
CSG	Cards Stakeholders Group
CVM	Cardholder Verification Method
DCC	Dynamic Currency Conversion
DDA	Dynamic Data Authentication
DTMF	Dual Tone Multi Frequency
EMV	Europay MasterCard Visa
EPA	Embedded Payment Application
EPC	European Payments Council
EPP	Encrypting PIN Pad
GSMA	GSM Association
HPP	Hosted Payment Page
HSM	Hardware Security Module
ICC	Integrated Chip Card
IF	Interchange Fee
IIN	Issuer Identification Number
ISO	International Organisation for Standardisation
(M)CP	(Mobile) Contactless Payment
MRP	(Mobile) Remote Payment
MNO	Mobile Network Operator
MOTO	Mail Order - Telephone Order
MRP	Mobile Remote Payment
NFC	Near-Field Communications
OS	Operating System
OTA	Over The Air
OTP	One Time Password
P2P	Point-to-Point (Encryption)

PAN	Primary Account Number	SCS	SEPA Cards Standardisation
PCI	Payment Card Industry	SDA	Static Data Authentication
PED	PIN Entry Device	SE	Secure Element
POI	Point of Interaction	SMS	Short Message Service
PPSE	Proximity Payment System Environment	SSL	Secure Socket Layer
PSD	Payment Services Directive	T2A	Terminal to Acquirer
PSE	Payment System Environment	TEE	Trusted Execution Environment
PSP	Payment Service Provider	TOE	Target OF Evaluation (CC)
PSU	Payment Service User	TPM	Trusted Platform Module
PTS	PIN Transaction Security	TPP	Third Party Provider
PVV	PIN verification value	TRSM	Tamper-resistant security module
REE	Rich Execution Environment	TSM	Trusted Services Management
SCF	SEPA Cards Framework	UPT	Unattended Payment Terminal

372

373

3.3 Definitions

Concept	Definition
3-D Secure	An XML-based protocol designed to be an additional security layer for remote transactions. It was developed by Visa with the intention of improving the security of internet payments and offered to customers as the Verified by Visa service. Services based on the protocol have also been adopted by MasterCard, under the name MasterCard SecureCode, by JCB International as J/Secure and by American Express as SafeKey.

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, merchant or other entity.
Acceptance Environment	Environment where the Card transaction is conducted in the Acceptor's domain. This Volume describes two Acceptance Environments: • Physical POI • Remote POI
Acceptance Technology	The source of and method by which Card Data is obtained. It may also include other processes.
Acceptor	A retailer or any other entity, firm or corporation that enters into an agreement with an Acquirer to accept Card Transactions as payment for goods and services (including cash withdrawals) and displays the card schemes acceptance logo. The Payment will result in a transfer of funds in their favour. Sometimes also referred to as Merchant.
Account Takeover (Fraud)	A form of fraud where someone accesses another's personal banking service and changes the address and passcode on someone else's account, using stolen or fake identification documents.
Acquirer	A Payment Service Provider or one of their agents that enters into a contractual relation with an Acceptor and an Issuer via the Card Payment Scheme, for the purpose of accepting and processing Card Transactions. In some cases, the Acquirer may also be an Acceptor.
Acquiring	The service performed by an Acquirer.

Activated/Deactivated	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.
Additional Authentication Device	A Chip Card accepting PED which may or may not be connected to the consumer device and which includes an EMV Card Authentication Application.
Application Cryptogram [AC]	A cryptogram generated by the Card Payment Application in response to a GENERATE AC command.
Application Identifier (AID)	An AID uniquely identifies an EMV application for local transaction which the terminal supports according to ISO/IEC 7816-5. Every AID has an associated card scheme and parameters relating to how the application needs to be processed. A terminal may contain any number of EMV applications, and the list of each supported AID is used during Candidate List Creation to generate a list of applications that are mutually supported by both the terminal and the card.
Application Profile	An Application Profile determines the configurable parameters which are used to process a Card Service by the POI Application.
Approval Body	A body which performs Type Approval.
ARQC	Authorization Request Cryptogram, which is a Cryptogram generated by the card application. See [EMV B2].
Asymmetric Key Pair	Two mathematically related cryptographic keys, a public key and a private key, which, when used with the appropriate public key algorithm, can allow the secure exchange of information and message authentication, without the secure exchange of a secret.
ATICA	Acquirer To Issuer Card messages. A set of messages in the field of Acquirer-to-Issuer and based on the ISO 20022 standard. When the Volume version 7 was being prepared the ATICA messages were still under development.
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.
(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”.

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).

376 *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	An identity verification method of a Cardholder based upon one or more intrinsic physical features of that Cardholder.
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.

377 *C*

Cancellation (Service)	A 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”.
Cancellation (Technical Process)	A process that can be instigated by the cardholder or the merchant to nullify a transaction, during or after the transaction has been processed. Its primary function is to prevent the payment being processed and to remove the block on the cardholders "open to buy".
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: • 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 Data	A data set used to perform a Card Service that allows the identification of the Cardholder and their account. Card Data consists of the PAN and other data elements.
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) Payment	Payment 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	See Stored Card Data
Card Pick-Up Advice	This Pick-up Advice service purpose is to inform the issuer that the card has been confiscated.
Card Processing Framework	A set of business principles and requirements applying to actors of the card payment value chain (e.g. Schemes, Processors, Acquirers, Issuers) in order to further facilitate an open and transparent market.
Card Reader	Data input device that reads data from a card-shaped storage medium.
Card 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. The Members of the Card Scheme can issue or Acquire transactions performed within the Scheme. Any party may join a Card Scheme, as long as the rules of that Card scheme are met.

Card Security Code	A data element that uses secure cryptography to protect the integrity of the card. The code differs depending on the payment channel. There is a CSC on the magnetic stripe, a different one in the chip and a different one again when the payment is contactless. The CSC is also the last three or four digits of the number printed on the reverse of the card (usually found on the signature strip). CVV2/CVC2/CID provides a security feature for "card not present" transactions. It is a three or four digit value which provides the payment processor with a cryptographic check of the card's authenticity. The terms are generally used interchangeably. CVV2 stands for "Card Verification Value 2", CVC2 stands for "Card Validation Code 2", and CID stands for "Card Identification Number". For American Express, the code is a four digit number on the front of the card above the account number. For Visa, MasterCard, Discover and CB the code is a three digit number that appears at the end of the account number (if present) on the back of the card. These code values help validate two things: The customer has the credit card in his/her possession. The card account is legitimate. CVV2/CVC2/CID is printed only on the card - it is not contained in the magnetic stripe information, nor does it appear on sales receipts or statements. Using the CVV2/CVC2 value can help minimize the risk of unknowingly accepting a counterfeit card or being a victim of fraud. The Card Security Code can be static or dynamic. For the latter, the Card Security Code can be generated by the chip of the card (for physical cards only) or be generated or delivered by other means.
Card 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	A Person or entity to whom a Card Application has been issued, or one who has been authorised to use the Card Application.
Cardholder Available Funds	It relates to the Cardholder available funds (sometimes called "open to buy") to cover the Card Transaction. The available funds are adjusted by the Card Issuer to reflect the transaction process with the card.
Cardholder Environment	The source from where Card Data is retrieved when performing a Card transaction. These are Physical Card, Virtual Card and Consumer Cardholder 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.
Cardholder Verification Method (CVM)	The method to be used to perform Cardholder Verification. This may include signature, PIN or no CVM required. Function used to verify evaluate whether the person using the card is the legitimate cardholder.
Cards Stakeholders Group (CSG)	The Group (CSG) 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.
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 merchants and financial institutions. Also called Cash Disbursement.
Cash Deposit	A Card Service which allows the cardholder to deposit cash to his own card account(s). It can take place • Either at a counter; • Or at an attended or unattended POI.A service which allows the cardholder to withdraw cash in an attended environment, e.g. at a POI or at a bank counter.
Cashback	See Payment with cashback.
Cashback Amount	See Payment with cashback.
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 (Delayed Debit 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'.
Chargeback	A Function which allows an Issuer to refuse a transaction. Chargeback refers to the transfer of liability from the Issuer back to the Acquirer, and is a monetary return of a transaction for a specific reason.
Chip Card (Smart Card)	A Physical Card which is an Integrated Circuit Card and complies with EMV Book 1 and/or EMV Book D or both in case of a Dual Interface Card. A Chip Card is sometimes referred to as a type of payment Card that has integrated circuits embedded within. The circuits, also referred to as the "chip" contain payment card data including but not limited to data equivalent to the magnetic stripe data. See Smart Card.
Chip Contactless	An Acceptance Technology where Card Data is retrieved from the chip of an IC Card over the contactless interface. In this case, the carrier of the chip may be a Chip Card of the ID 1 form factor (as defined in ISO/IEC 7810), a key fob, or another Form Factor.
Chip with Contact	An Acceptance Technology where Card Data is retrieved from the chip of an IC Card over the contact interface compliant with [EMV B1].
Clearing	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.
Cleartext	See Plaintext.
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 the acceptor, potentially the acquirer and also potentially the cardholder with information on how the transaction was completed.
Compliance	Adherence of Products and Solutions to detailed specifications.
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.
Conformance Verification Process	The processes by which the SEPA Cards Community interacts with its environment for verifying the SCS Volume conformance.
Consumer Device	An internet capable device used by the Cardholder to conduct Card Services. It is either • a Mobile Device used for Mobile Contactless or Mobile Remote Transactions , • An Electronic Device used for Remote Transactions. It can be a carrier of Credentials or a Card Application. It includes a user interface that enables the Cardholder to enter data. This is sometimes referred to as Cardholder Controlled Device or Cardholder Operated Device.
Contactless Payment	A payment processed using the Chip Contactless Acceptance Technology or the Mobile Contactless Acceptance Technology the radio frequency enabled component of the chip instead of the contact component, to process the payment. The Contactless Acceptance Technologies are based on the ISO 14443 standard.
Contactless With Mobile	Card data is retrieved from a Mobile Contactless Payment (MCP) application in a mobile device over the contactless interface. See Contactless Payment.

Counterfeit Card (Fraud)	A card that has been fraudulently manufactured, embossed or encoded to appear to be genuine but which has not been authorised by a card scheme or issued by a member. A card originally issued by a member but subsequently altered without the issuer's knowledge or consent.
CPS Governance Authority	The Card Payment Scheme actor who is accountable for the overall functioning of the CPS and its coherence; it should ensure that all other actors follow the rules and apply relevant measures. The CPS standards allocate responsibility directly to the governance authority. The CPS rules may allow delegation of some of these responsibilities to other actors of the CPS. The governance authority should clearly define such cases and ensure that the choices of the other actors of the CPS are compliant with the overall CPS standards. The governance authority could be a specific organisation or entity or be represented by decision-making bodies of cooperating schemes.
Credentials	The information - generally confidential - provided by a Cardholder or PSP for the purposes of authentication.
Credit Card (Card With A Credit Function)	A card that enables a cardholder to make purchases and/or withdraw cash up to a prearranged credit limit. The credit granted may be either settled in full by the end of a specified period, or settled in part, with the balance taken as extended credit (on which interest is usually charged).
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.

378 *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)	A card enabling its holder to make purchases and/or withdraw cash and have these transactions directly and immediately debited from the accounts.
Decryption, Decipherment	Transformation of data by a cryptographic algorithm to retrieve data in its original state from cipher text.
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.
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.

379 *E*

E-Commerce	A Card Not Present (remote) transaction initiated by the Cardholder using a Consumer Device and conducted via a Virtual POI to buy products and services over the internet. If the Consumer Device is an Electronic Device, this is referred to as an E-Commerce transaction.
EFTPoS Terminal	A terminal which captures payment information by electronic means and transmits such information either online or offline. “EFTPoS” stands for “electronic funds transfer at point of sale”.
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 .
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	A Card Application according to EMV and stored on a Physical Card. Each EMV Card Payment Application is identified by an Application Identifier (AID). An EMV Card Payment Application may be contact, contactless or both. An EMV Card Payment Application is called a Contact Card Payment Application if it supports transaction processing for the Acceptance Technology "Chip with Contact". It is called a Contactless EMV Card Payment Application if it supports transaction processing for the "Chip Contactless" Acceptance Technology.

EMV Online Mutual Authentication ("OMA")	Authentication of the chip card 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.
e-Purse - Loading/Unloading	Services which allow the cardholder to transfer funds between an electronic purse and his card account.
Evaluation Methodology	A methodology that will be used to evaluate compliance and assurance level with a specific implementation specification,

380 *F*

Face-To-Face (Card) Payment	See Local (Card) Payment
Face-To-Face (Card) Transaction	See Local (Card) Transaction
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 appearance of a cardholder device.
Four party card scheme	A Card Scheme which includes the following stakeholders: The Cardholder, the Issuer (who has a relationship with the Cardholder), the Acceptor and the Acquirer (who has a relationship with the Acceptor). The Scheme defines the rules which apply to all parties; there are no limitations as to who may join the scheme, as long as the requirements of that scheme are met.
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]

381 *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 merchants.

382 *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.
Honour All Cards	Rule under which Acceptors are required to accept all the different types of cards that are valid and branded by the same Card Payment Scheme.

383 *I*

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 service which allows the card 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.
(Data) Integrity	The property that data has not been altered or destroyed in an unauthorised manner.

Interchange Fee (IF)	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. When calculating the amount of interchange fees, the net compensation or other agreed remunerations will be considered as 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	A PSP or one of their agents that supplies the Card payment account and the Card Services (including Card data) to the Cardholder, and is a member of a Card Payment Scheme. The Issuer enters into a contractual relationship with a Cardholder and guarantees payment to the Acquirer for transactions that are in conformity with the rules of the relevant 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.

384 *J*

385 *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.

386 *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 (Card) Payment	A Card Payment initiated at the Acceptor's Physical POI (sometimes referred to as 'Face to Face' transactions). This concept is in opposition with Remote (Card) Payment.
Local (Card) Transaction	A Card Transaction initiated at the Acceptor's Physical POI (sometimes referred to as 'Face to Face' transactions).
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)

387 *M*

m-Commerce	A Card Not Present (remote) transaction initiated by the Cardholder using a Consumer Device and conducted via a Virtual POI to buy products and services over the internet. If the Consumer Device is a Mobile Device, this is referred to as an M-Commerce transaction.
MACing	A function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following properties: • for any key and any input string the function can be computed efficiently; • for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the input string may have been chosen after observing the value of the first i-1 function values (see ISO/IEC 9797-1)
Magnetic Stripe	Acceptance Technology where a type of card is capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card.

Magnetic Stripe Card	A Physical Card carrying a magnetic stripe which complies with ISO 7810, 7811, 7812, 7813.
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.
Man-In-The-Middle Attack (Fraud)	The man-in-the-middle attack in cryptography and computer security is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.
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.
Mobile Code	This method 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. The check is made offline by a dedicated application such as the MCP/MRP or Authentication Application in a secure environment via the Mobile Device or online by the issuer.
Mobile Contactless	Acceptance Technology where Card Data is retrieved from a Mobile Contactless Payment (MCP) Application in a Mobile Device over the contactless interface.
Mobile Contactless Card Payment Application	A Card Application according to EMV and stored in a Secure Element on a Mobile Device[4]. Each Mobile Contactless Card Payment Application is identified by an Application Identifier (AID). It supports transactions processing for the Acceptance Technology “Mobile Contactless”.

[4]The storage of a Mobile contactless application according to HCE (Host Card Emulation) is not covered in the current release of the Volume.

Mobile Device	Consumer device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth … Examples of Mobile Devices include mobile phones, smart phones and tablets.
Mobile Payment (m-Payment)	A payment where a Mobile Devices used at least for the initiation of the payment order and potentially also for the authentication and transfer of funds.
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	Mobile wallet contains information supporting payment services generally performed from or via a Mobile Device.
Money Remittance	A payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.
MOTO	A Card not present transaction conducted in the Acceptor's environment using Manual Entry with the cardholder interacting remotely for Mail Order or Telephone Order (MOTO). The Card Data is key entered either by the Acceptor or by the Cardholder (if DTMF is used) via a Physical POI or Virtual Terminal.

388 *N*

Near Field Communication (NFC)	A contactless communication interface and protocol specified in ISO/IEC 18092 and ISO/IEC 21481
No CVM Required	No Cardholder Verification Method is required.

No-Show	A service which allows the card acceptor to charge the cardholder's account due to the fact that the cardholder does not use the service within the specified time and has not cancelled the guaranteed reservation within the specified period. It is used e.g. for hotel or car rental reservations.

389 *O*

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. Three forms of offline data authentication are defined by EMV: SDA, DDA and CDA.
Offline Enciphered PIN	The PIN entered to verify the cardholder's identity is encrypted using public key cryptography at the POI/PIN Pad then decrypted inside the chip and verified by the chip-processor.
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 card verifies a PIN that is entered by the cardholder; the PIN is stored in the card. There are two methodologies - Offline plaintext PIN or Offline Enciphered PIN.
Offline Plaintext PIN	The PIN entered to verify cardholder's identity is checked by the chip-processor. The PIN is transmitted to the card in plaintext.
Offline Transaction	A card transaction which is not authorised on-line with the Card Acquirer/Issuer but offline by the Card Application.
One Stop Shopping	A key 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 for meeting additional requirements.
Online Capable Terminal	APOI 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. The PIN entered to verify cardholder's identity is checked by sending an encrypted PIN to the Issuer or delegated entity for validation as part of an authorisation request.

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 merchant, 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 merchants 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.
OSeC	A market initiative (currently pilot) that, based on the Volume requirements, has been created to coordinate an implementation of an evaluation and certification framework whose purpose is to help building a single scheme for security in payment terminals and cards, and multiple recognition of security certification by card schemes and banking organisations across Europe.

390 *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 7813.
Passive Authentication	An authentication method without direct Cardholder interaction, which can be used in combination with other authentication methods. This may include analysing historical data about both the Cardholder and the Acceptor alongside analysing transaction specifics e.g., transaction amount, consumer device characteristics (logical, physical and usage), and location (e.g., geo-location, IP address).
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	An account held in the name of one or more payment service users which is used for the execution of payment transactions.
Payment Amount	The amount to be paid for the purchase of goods or services.

Payment Card	A physical card that offers 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 Completion	See Completion.
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 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	A tool or a set of procedures enabling the transfer of funds from a payer to a payee. The payer and the payee can be one and the same person. See also means of payment. [different from the PSD definition]
Payment Order	Any instruction by a payer or payee to his 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 Product	Product defined by a Payment Scheme.
Payment Service Provider (PSP)	Bodies referred to in Article 1(1) and legal and natural persons benefiting from the waiver under Article 26 of the Payment Services Directive.
Payment Service User	A natural or legal person making use of a payment service in the capacity of either payer or payee, or both. See Payment Services Directive.
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 Transaction	An act, initiated by the Cardholder or by the Acceptor, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the Cardholder and the Acceptor.
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 till after the transaction. It is used for Payments performed on airlines/cruise ships and other types of acceptance environments that are not online at all times.
Payment With Deferred Clearing	A feature where the Acquirer postpones the clearing of the transaction. It is used for example for the payment of health expenses.
Payment With Increased Amount	A feature which allows the 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 offline by a dedicated application such as an RP or Authentication Application in a secure environment via the electronic device or online by the issuer.
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.
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 plastic card which may have a Magnetic Stripe, a Chip Card or both. It is a carrier of Card Data and, if it is a Chip Card, of an EMV Card Payment Application or EMV Card Authentication Application or both.

Physical POI	The initial point where Card Data is retrieved in the Acceptor's Domain. A 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.
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	An Acquirer dedicated 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. A POI Application on a Physical POI for processing Local Transactions may be referred to as Physical POI Application. A POI Application on a Virtual POI may be referred to as Virtual POI Application. A POI Application on a Physical POI or a Virtual Terminal for processing MOTO transactions is referred to as MOTO Application

Pre-Authorisation Services	A service composed of 3 linked steps: • Pre-Authorisation • Update Pre-Authorisation (potentially with several occurrences) • Payment Completion The Pre-Authorisation allows the Acceptor to reserve an amount in order to secure sufficient funds to complete a subsequent payment. It is used only to secure the amount since the final amount of the actual payment is not known (e.g. car rental, hotel, video rental, etc.). The Update Pre-Authorisation allows the Acceptor to update the amount of a Pre-Authorisation. This may either increase or decrease (potentially to zero) the previously authorised amount. The Payment Completion allows the Acceptor to finalise a payment.
Prepaid Card	A card on which a monetary value can be loaded in advance and stored either on the card itself or on a dedicated account on a computer. Those funds can then be used by the holder to make purchases. See also multi-purpose prepaid card.
Prepaid Card - Loading & Unloading	A service which allows the cardholder to transfer funds to or from a prepaid card account.
Presentment	See Financial Presentment
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	The performance of all of the actions required in accordance with the rules of a system for the handling of a transfer order from the point of acceptance by the system to the point of discharge from the system. Processing may include clearing, sorting, netting, matching and/or settlement.
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).
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.
Proximity Payment	A card payment where the communication between the card and the terminal does not take place over a contact interface, but through a proximity contactless communication between the card and the terminal.
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.

391 *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.

392 *R*

Reconciliation	A Service which enables two entities (Acceptor, Acquirer, Issuer or their agents) to seek an agreement on financial totals (amounts, number of transactions).
Recurring Payment	A Card Service where the Cardholder authorises an Acceptor to charge their account on a recurring basis and without a specified end date.
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.
Remote (Card) Payment	A Card Payment which is either e- & m-Commerce or MOTO. The concept is in opposition with Local (Card) Payment.

Remote Payment - Basic Electronic Commerce	A Remote Payment using a static authentication method.
Remote Payment - Mobile	A Remote Payment initiated through a Mobile Device.
Remote Payment - Secured Electronic Commerce	A Remote Payment using a dynamic authentication method.
Remote POI	The initial point where Card Data enters the Acceptor's domain for Remote Transactions. The Remote POI exists in a variety of technical platforms which enable a Cardholder and/or an Acceptor to generate a Remote Transaction. The Remote POI is either • A Virtual POI including a Payment Page, accessed by the Cardholder using a Remote Device for e- & m-Commerce or • A Virtual Terminal used by the Acceptor for MOTO.
Remote Transaction	A Card Transaction which is either e- & m-Commerce or MOTO.
Retailer Card	A card issued by a merchant for use at specified merchant outlets.
Return Card Advice	The Return Card Advice purpose is to inform the issuer that the card has been returned to cardholder.
Return Card To Cardholder Request	The Return Card to Cardholder Request purpose is to get authorisation to return card to cardholder.
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.

393 *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)	A tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. There are three different form factors of SE: Universal Integrated Circuit Card (UICC), embedded SE and microSD. Both the UICC and microSD are removable.
Secure Environment	A system which implements the controlled storage and use of information. A secure environment is used to protect personal and/or confidential data. In the context of Remote Payments it may be located in the Consumer Device, such as a SE, a TPM or a TEE, or in a remote secured server.
Selection of the Application	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. 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.
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.
SEPA Cards Standards	The functional and security requirements and conformance process requirements as well as the implementation guidelines described in the SEPA Cards Standardisation Volume are called the “SEPA Cards Standards”.
SEPA For Cards	A key objective of the ECB for enabling Payment Service Users in Europe (such as cardholders and merchants) 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 or four-digit value in the magnetic stripe that follows the expiration date of the payment card on the track data. It is used to define service attributes, differentiating between international and national interchange or identifying usage restrictions.
Sensitive Payment Data	Data which allows control over the Cardholder Account or which may be used to carry out fraud.
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	The Cardholder's handwritten signature to approve a transaction.
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	Organisation which: • develops Implementation Specifications based upon the high level requirements specified in the Volume for use by Solution Providers to develop products or solutions; • provides a maintenance process, notably for interoperability and/or security issues linked to the implementation specifications; • has its own certification body or a relationship (formal or informal) with an external certification body to certify products and solutions.
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	Acceptance Technology where PAN and Expiry Date has been provided prior to the transaction and stored securely for later use. This Acceptance Technology is used for Card Not Present transactions. This is often referred to as Card on File.
Strong Authentication	A dynamic authentication method which involves at least 2 independent authenticators. This means that at least one of them is dynamic.

Strong Customer Authentication	According to the EBA guidelines [EBA 1], this is a procedure based on the use of 2 or more of the following elements - categorised as knowledge, ownership and inherence: 1. Something only the user knows, e.g. static password, code, PIN 2. Something only the user possesses, e.g. token, smart card, mobile phone 3. Something the user is, e.g. biometric characteristic, such as a finger print. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data.
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.

394 *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 accredited organisation that is mandated to test "Products and solutions" related to cards against a list of specifications. The latter are defined by Implementation Specifications Provider in conformance with the last published version of the Volume and its Bulletins.
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	A Card Scheme including the following stakeholders: the Cardholder, the Issuer (who has a relationship with the Cardholder), the Acceptor and the Acquirer (who has a relationship with the Acceptor), but the Issuer and the Acquirer are the same entity.
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.
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.

395 *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.).
Unsolicited Available Funds	A feature which allows the card issuer to provide account balance information in the authorisation response message.

396 *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 an alternative, temporary card number with a reduced validity period, limited usage and a pre-defined spending limit is generated which can be used for e- & m- commerce.
Virtual POI	The initial point where Card Data enters the Acceptor's domain via a Consumer Device for e- & m-commerce. It consists of hardware and software which enables a Cardholder to perform an e-and m-Commerce Transaction. It includes a Payment Page which may be presented to the Cardholder from either a Payment Gateway or the Acceptor's website. The Virtual POI may also facilitate (redirection) services to support Authentication of the Cardholder by the Card Issuer for e-and m-Commerce.

Virtual Terminal	A MOTO Application used by the Acceptor to enter Card Data. It comprises a Payment Page hosted by an Acquirer or TPP for the entry of Card Data by the Acceptor for MOTO Transactions. A Virtual Terminal can also be used by the Cardholder, but only for Telephone Orders if DTMF technology is used.

397 *W*

Wallet Solutions	Solutions that allow a customer to register data relating to one or more payment instruments in order to make payments with several e-merchants.

398 *X*

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

399 *Y*

400 *Z*

401

1 FIGURES