SEPA CARDS STANDARDISATION (SCS) "VOLUME"

BOOK 1

GENERAL

PART OF THE APPROVED VERSION OF SCS VOLUME V7.0

Payments and Cash withdrawals with Cards in SEPA

Applicable Standards and Conformance Processes

Volume v7.0 and its constituent Books supersede the SEPA Cards Standardisation Volume v6.0.

Abstract	This document contains the work on SEPA cards standardisation to date
Document Reference	EPC020-08
Issue	Book 7.1.1.00
Date of Version	12 December 2013
Reason for Issue	Publication
Reviewed	Approved for publication by the EPC Plenary of 12 December 2013 and endorsed by the CSG GM of 7 November 2013
Produced by	CSG Secretariat
Owned and Authorised by	EPC
Circulation	Public

Table of Contents

1 GENERAL 3

1.1 Volume - Document change history 3

1.2 Executive summary 5

1.3 Description of changes since the last version of Book 1 9

2 THE SCS VOLUME AND ITS BOOKS 10

2.1 Introduction to the "SEPA Cards Standardisation Volume" 10

2.2 Scope and Objectives of CSG Work on Cards Standardisation 11
2.2.1 Context 11
2.2.2 Scope 11
2.2.3 Objectives 11
2.2.4 Impact on the Different Stakeholders 12
2.2.5 Implementation of the SEPA Cards Standards and Monitoring 12
2.2.6 Implementation Specifications 12

2.3 Maintenance of the Books 13
2.3.1 The Volume, a Set of Books 13
2.3.2 Maintenance cycles 13
2.3.3 Intellectual Property Rights 14

3 REFERENCES, ABBREVIATIONS AND DEFINITIONS 15

3.1 References 15

3.2 Abbreviations 17

3.3 Definitions 19

4 FIGURES 46

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

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 support of this action, the Volume will be aligned with the Recommendations for the security of internet payments published on 31 January 2013 by the European Central Bank (ECB) and agreed amongst the European overseers and supervisors represented in the European Forum on the Security of Retail Payments (SecuRe Pay).

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.

[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.

A check of SEPA conformance is currently not performed by Regulators. The Volume requirements are thus not formally imposed on the 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.

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.

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 January 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 will be published in January 2014 as a stable release ready for market implementation.

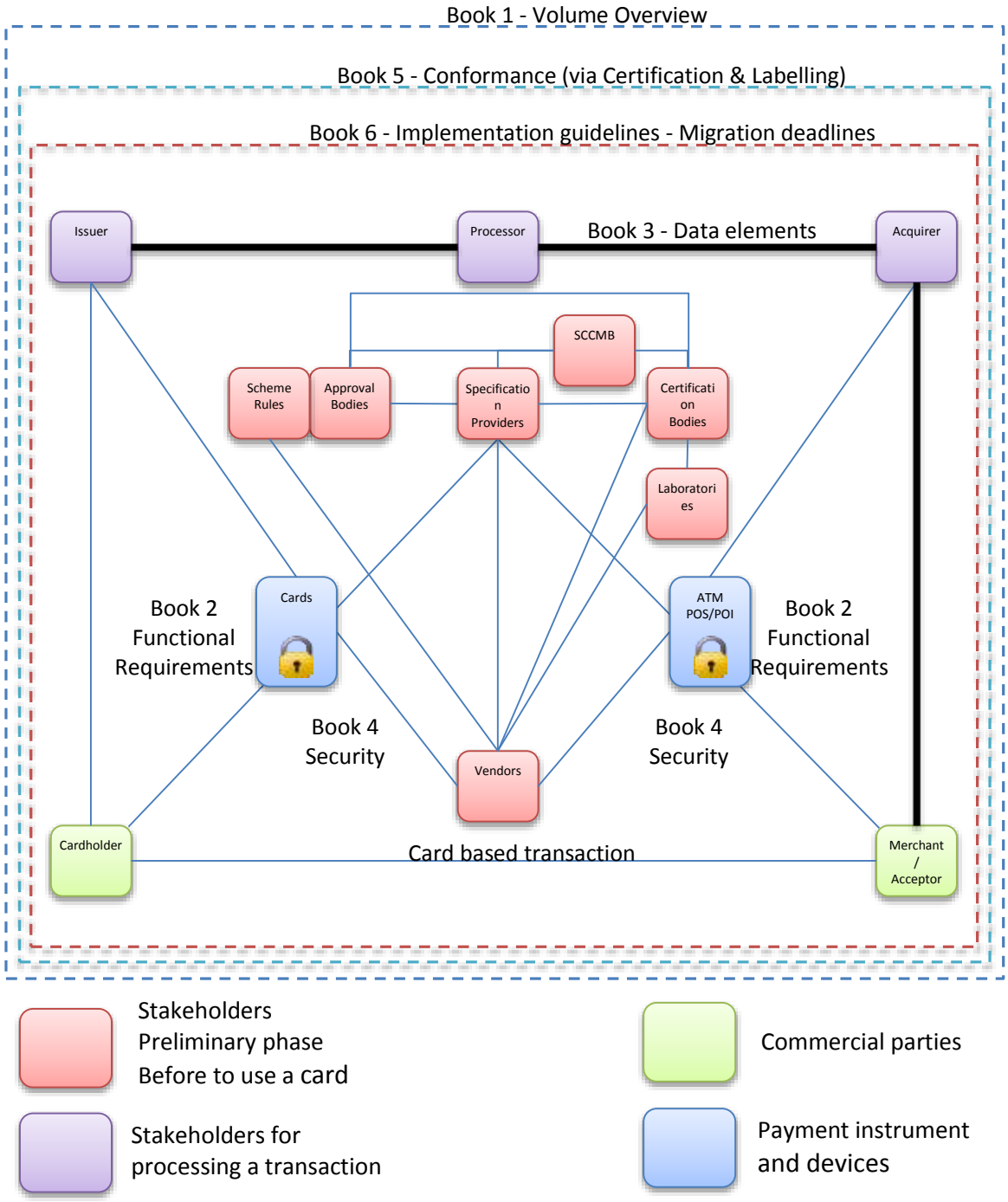

FIGURE 1: VOLUME OVERVIEW

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***

1.3 Description of changes since the last version of Book 1

None (first version of Book 1).

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 at times 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 to make use of these standards, yet those who do will be able - as a result of a self-assessment process - to declare their solutions or services as being Volume-compliant.
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***

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.

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 2014 and 2015 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.

3 REFERENCES, ABBREVIATIONS AND DEFINITIONS

3.1 References

[CPA] EMV Integrated Circuit Card Specifications for Payment Systems, Common Payment Application Specification, Version 1.0, December 2005

[EMV] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, November 2011

[EMV B1] EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements, Version 4.3, November 2011

[EMV B2] EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3, November 2011

[EMV B3] EMV Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification, Version 4.3, November 2011

[EMV B4] EMV Integrated Circuit Card Specifications for Payment Systems, Book 4, Cardholder, Attendant, and Acquirer Interface Requirements, Version 4.3, November 2011

[EMV A] EMV Contactless Specifications for Payment Systems. Book A, Version 2.2, June 2012

[EMV B] EMV Contactless Specifications for Payment Systems. Book B, Version 2.2, June 2012

[EMV C1] EMV Contactless Specifications for Payment Systems. Book C-1, Version 2.2, June 2012

[EMV C2] EMV Contactless Specifications for Payment Systems. Book C-2, Version 2.2, June 2012

[EMV C3] EMV Contactless Specifications for Payment Systems. Book C-3, Version 2.2, June 2012

[EMV C4] EMV Contactless Specifications for Payment Systems. Book C-4, Version 2.2, June 2012

[EMV D] EMV Contactless Specifications for Payment Systems. Book D, Version 2.2, June 2012

[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

[PCI PTS] Payment Card Industry PIN Transaction Security Version 3

[PCI P2PE] Payment Card Industry Point to Point Encryption Version 1

[PCI DSS] Payment Card Industry Data Security Standard

[PCI PA-DSS]	Payment Card Industry Payment Application Data Security Standard
[PSD]	Payment Services Directive - Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.

3.2 Abbreviations

Acronym	Standing for
A2I	Acquirer to Issuer
AID	Application Identifier
ATC	Application Transaction Counter
BIN	Bank Identification Number
C2T	Card to Terminal
CAM	Card Authentication Method
CC	Common Criteria
CDA	Combined DDA/Application Cryptogram Generation
CPS	Card Payment Scheme
CSC	Card Security Code
CSG	Cards Stakeholders Group
CVM	Cardholder Verification Method
DDA	Dynamic Data Authentication
EPA	Embedded Payment Application
EPC	European Payments Council
EPP	Encrypting PIN Pad
GSMA	GSM Association
ICC	Integrated Chip Card
MCP	Mobile Contactless Payment
MNO	Mobile Network Operator
MOTO	Mail Order - Telephone Order
MRP	Mobile Remote Payment
NFC	Near-Field Communications
OTA	Over The Air
OTP	One Time Password
P2P	Point-to-Point (Encryption)
PAN	Primary Account Number
PCI	Payment Card Industry
PED	PIN Entry Device
POI	Point of Interaction
PPSE	Proximity Payment System Environment
PSD	Payment Services Directive
PSE	Payment System Environment
PSP	Payment Service Provider
PSU	Payment Service User
PTS	PIN Transaction Security
REE	Rich Execution Environment
SCF	SEPA Cards Framework
SCS	SEPA Cards Standardisation
SDA	Static Data Authentication
SE	Secure Element
SMS	Short Message Service

SSL	Secure Socket Layer	TOE	Target OF Evaluation (CC)
T2A	Terminal to Acquirer	TSM	Trusted Services Management
TEE	Trusted Execution Environment		

3.3 Definitions

Concept	Definition
3-D Secure	3-D Secure is 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.
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 taking place, which can occur at the Acceptor's POI (attended, unattended,...) or at cardholder controlled devices (telephone, computer, mobile device, etc).
Acceptance Technology	The source of and method by which Card Data is obtained. It may also include other processes.
Accepting Device	Any device that processes payment card transactions, regardless whether the card and cardholder are present or not.
Acceptor	See Card Acceptor.
Account Takeover (Fraud)	A form of fraud where someone accesses another's personal banking service and changes the address and passcode on someone's else account, using stolen or fake identification documents.
Acquirer	See Card Acquirer.
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.
Alias	For remote payments, an alias is basically a pseudonym for the beneficiary that can be uniquely linked to the beneficiary's name and to the identification of the beneficiary's payment account in case of remote card payments.
Application Cryptogram [AC]	A cryptogram generated by the card in response to a GENERATE AC command.

Application Profile	An Application Profile determines the configurable parameters which are used to process a Card Service. The POI Application chooses the Application Profile for a transaction based primarily on the selected AID (Card Application Identifier) for chip based transactions, and on the BIN/BIN range for PAN based transactions, on the Card Service to be performed and the Acceptance Technology being used.
Application Selection	A Function which technically allows selecting an application supported by both the card and the POI for the Acceptance Technologies Chip with Contact, Chip Contactless and Contactless with Mobile and selecting an Application Profile for all Acceptance Technologies, to be used to process a service for a transaction. For remote transactions the application selection does not cover the selection process as defined in EMV, but instead the selection of a mark/card product by the cardholder.
Approval Body	A body which performs Type Approval.
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	An attendant (an agent of the card acceptor) is present at the Point of Interaction and participates in the transaction by entering transaction-related data.
Authentication	The provision of assurance of the claimed identity of an entity or of data origin. Process of verifying the identity of an individual, device or process. Authentication typically occurs through the use of one or more authentication factors 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.
Authentication Application	A dedicated application to support the authentication process in a remote payment transaction. The authentication application may be hosted in a (mobile) device or in the cloud, to avoid the usage of an external authentication device.
Authentication Credentials	Combination of the user ID or account ID and the authentication factor(s) used to authenticate an individual, device or process.
Authentication Method	The method used for the authentication of an entity or data origin.

Authenticator	A security factor used in an authentication method. Typical examples are tokens, mobile codes/passcodes, etc.
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 to the Chip card 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 terminal device 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).
Balance Inquiry	A service which allows the cardholder to request information about his account balance.
BIN	Bank Identification Number (also referred to as IIN). See ISO/IEC 7812 for more information.
Biometric	Biometric is a cardholder's identity verification method based upon one or more intrinsic physical features.
Brand	A Brand denotes a product (especially a card) or family of products that have been licensed by its owner for use in a given territory.
Business Day	A day on which the relevant payment service provider of the payer or the payment service provider of the payee involved in the execution of a payment transaction is open for business as required for the execution of a payment transaction.
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 Scheme (or Card Payment Scheme)	A card payment scheme is a technical and commercial arrangement resulting in a set of functions, procedures, arrangements, rules and devices that enable a holder of a payment card to effect a payment and/or cash withdrawal transaction with a third party other than the card issuer. The Members of the Card Scheme can issue or Acquire transactions performed within the Scheme.

Card (Payment Card)	A device physical or virtual that can be used by its holder to perform a Card Service, e.g. pay for goods and services or to withdraw cash, irrespective of the form factor of the device.
Card Acceptor	A retailer or any other entity, firm or corporation that enters into an agreement with an acquirer to accept payment cards, when properly presented, as payment for goods and services (including cash withdrawals) and which will result in a transfer of funds in its favour.
Card Acquirer	Payment service provider, as defined in the Payment Services Directive or other undertaking and that enters into a contractual relation with a card acceptor and the card issuer via the CPS, for the purpose of accepting and processing card transactions. In some cases, the card acquirer may act as a card acceptor itself.
Card Activation	Card Activation is an operation to activate a new card prior to usage or during first card usage.
Card Application	It denotes the software for processing the Card Services on the cardholder device, provided the cardholder device has the ability to process transactions. Each Card application is identified by an Application Identifier (AID). A Card application may be contact, contactless or both. A Card application is called contact Card application if it supports transaction processing for the Acceptance Technology "Chip with Contact". It is called contactless Card application if it supports transaction processing for the "Contactless" Acceptance Technologies, where the term "Contactless" is used to refer to both Acceptance Technologies, the Chip Contactless Acceptance Technology and the Contactless with Mobile Acceptance Technology.
Card Authentication	A Function by which a chip card is authenticated to the POI (Offline Card Authentication) and/or the Issuer (Online Card Authentication).
Card Based Language Selection (Optional)	A Function by which the language can be selected for on-screen dialogues or print-outs.
Card Based Remote Payment	During the payment transaction, the Cardholder is neither present at the card acceptor's premises nor at an Unattended Terminal. Usually this means the payment transaction is initiated at the cardholder's computer, tablet or mobile.
Cardholder Available Balance	It relates to the cardholder available balance (sometimes called "open to buy") to cover the card purchase. The available balance is adjusted by the card issuer to reflect the purchase process with the card.
Card Data	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)	Identity theft is 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 Pick-Up Advice	This Pick-up Advice service purpose is to inform the issuer that the card has been confiscated.
Card Reader	Data input device that reads data from a card-shaped storage medium.
Card Security Code	The Card Security Code is 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 Card Service is 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 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	Person or entity to whom a payment card has been issued, or one who has been authorised to use the payment card.
Cardholder Not Present (CNP) Payment	Payment transaction based on card-related information without the card being physically presented to the Acceptor i.e. MOTO, E and M Commerce.
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 evaluate whether the person using the card is the legitimate cardholder.
Cardholder Verification Method (CVM)	The method to be used to verify the cardholder's identity. This may include signature, PIN or no CVM required.
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 service which allows the cardholder to withdraw cash in an attended environment, e.g. at a POI or at a bank counter. Also called Cash Disbursement.
Cash Deposit	A 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.
Cashback	Cashback is a service available in a retail environment whereby the cardholder can ask for an amount to be added to the transaction total and receives that amount in cash. The service is only available in a cardholder present environment. In some countries, the service is prohibited by law.
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.

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 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	Card data is retrieved from the chip of an IC Card over the contactless interface.
Chip with Contact	Card data is retrieved from the chip of an IC Card over the contact interface compliant with [EMV B1].
Cleartext	See Plaintext.
Combined DDA/Application Cryptogram Generation (CDA)	A type of offline data authentication where the card combines generation of a cryptographic value (dynamic signature) for validation by the terminal with generation of the Application Cryptogram to verify that it came from a valid card.
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.

Compliance	Adherence of Products and Solutions to detailed specifications.
Completion	A Function which provides the acceptor, potentially the acquirer and also potentially the cardholder with information on how the transaction was completed.
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. The word Compliance is used for adherence of Products and Solutions to detailed specifications.
Conformance Verification Process	The processes by which the SEPA Cards Community interacts with its environment for verifying the SCS Volume conformance.
Consumer Device	A form factor that contains a payment application that can be used for card payment – cards, phones and other types of devices.
Contactless Payment	A payment processed using the radio frequency enabled component of the chip instead of the contact component, to process the payment. Based on the ISO 14443 standard.
Contactless Transaction	See Contactless Payment.
Contactless With Mobile	Card data is retrieved from a Mobile Contactless Payment (MCP) application in a mobile device over the contactless interface.
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 customer or PSP for the purposes of authentication. Credentials can also mean the physical tool containing the information (e.g. one-time-password generator, smart card), or something the user memorises or represents (such as biometric characteristics).

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).
Cryptogram	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 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.
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	A mathematical and computer science discipline to encrypt data. It is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "One Way". Examples of industry tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys) RSA, (1024 bits and higher), ECC (160 bits and higher) and EIGamal (1024 bits and higher).
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.
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.
Data Encryption Standard (Des)	The public domain symmetric key cryptography algorithm of the National Institute for Standards and Technology.
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	Applying an algorithm and a secret key to transformed data to return it to its original state.

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	Result of using asymmetric keys and a cryptographic algorithm to transform data so that the recipient of the data can prove the origin and integrity of that data. It is used to protect the sender and the recipient against forgery by third parties and to protect the sender against forgery by the recipient.
Dynamic Authentication	Authentication method that uses cryptography or other techniques to create a one-per-transaction random 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 public key technology 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: DDA and CDA.
E-Commerce	The buying and selling of products and services by businesses and consumers over the internet.
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 Money	A monetary value, represented by a claim on the issuer, which is: 1) stored on an electronic device (e.g. a card or computer); 2) issued upon receipt of funds in an amount not less in value than the monetary value received; and 3) accepted as a means of payment by undertakings other than the issuer.
Electronic Money Institution (ELMI)	A legal person that has been granted authorisation under Title II of the Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions to issue electronic money .

Electronic Signature (Digital Signature)	A string of data, generated by a cryptographic method, which is attached to an electronic message in order to guarantee its authenticity, identify the signatory and link the content to that signatory (thereby protecting the recipient against repudiation by the sender).
Elliptic Curve Cryptography (ECC)	A public key cryptosystem approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller in 1985. It requires smaller keys and is significantly faster to process than RSA. It is used for data encryption and authentication.
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 Offline CDA	With CDA the card generates a dynamic signature of transaction data including the cryptogram, in order to provide the protection of DDA while also assuring that an intermediate (wedge) device has not altered important data going between the card and POI Application.
EMV Offline DDA	With DDA the POI Application verifies a dynamic signature (i.e. different for each transaction) generated by the card using its private key, in order to authenticate the validity of the Chip data and of the card.
EMV Offline SDA	With SDA the POI Application verifies a static signature (i.e. the same for every transaction) of card data, in order to assure that this data has not been altered.
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.
Encryption, Encipherment	Applying an algorithm, secret key to data to transform or hide the original 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,

Face-To-Face Payment	A payment where the Cardholder and the Acceptor or it's agent (or it's device) are in the same physical location. Antonym: remote payment.
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 currency amount above which an online authorisation is required for a single transaction.
Form Factor	The physical appearance of the cardholder device used.
Four-Party Card Scheme	A card scheme where the stakeholders involved are: 1) the cardholder; 2) the issuer; 3) the acquirer; 4) the card acceptor. By contrast, in a three-party card scheme, the issuer and the acquirer are always the same entity. See also card scheme, three-party card scheme.
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 Article 1(3)(b) of Directive 2000/46/EC.
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.
Hashing	It is a mathematical function in which a non-secret algorithm takes any arbitrary length message as input and produces a fixed length output, usually called a "hash Code" or "message digest". A hash function should have the following properties. 1) It is a computationally infeasible to determine the original input given only the hash code. 2) It is computationally infeasible to find two inputs that give the same hash code. This process is used to render cardholder data unreadable by converting data into a fixed-length message digest via strong Cryptography.

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.
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.
Integrity	The quality of being protected against accidental or fraudulent alteration or the quality of indicating whether or not alteration has occurred.
International Organisation Of 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.
ISO 20022	The ISO Standard for Financial Services Messaging. It describes a Metadata Repository containing descriptions of messages and business processes, and a maintenance process for the Repository Content.
ISO 8583	ISO 8583 is an ISO standard for Financial transaction card originated messages. It has been published in 3 different versions (87,93,03).
Issuer	The Payment Service Provider that issues cards and is a member of a CPS. The Issuer enters into a contractual relationship with a cardholder. The Issuer makes payment cards available to cardholders, authorises transactions at POIs or Automated Teller Machines (ATMs) and guarantees payment to the acquirer for transactions that are in conformity with the rules of the relevant 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.

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.
Labelling	Optional Volume conformance process based on self assessment for detailed implementation specifications.
Laboratory	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.
M-Commerce	E-Commerce performed over a Mobile Device.
MACing	Action of using a short piece of data to verify that the contents of a message has not changed from when it was created by the sender until it was received by the recipient. See ISO/IEC 9797-1 for further information.
Magnetic Stripe	A magnetic stripe card is a type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. The magnetic stripe, sometimes called swipe card or magstripe, is read by swiping past a magnetic reading head. Data encoded in the magnetic stripe or chip used for authentication and/or authorisation during payment transactions. Can be the magnetic stripe image on a chip or the data on the Track 1 and/or Track 2 portion of the magnetic stripe.
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	Card data is keyed in manually at the time of the transaction.

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	Any person, firm or corporation which has contracted with an Acquirer to originate transactions through acceptance of payment cards as payment for goods or services and displays the card schemes acceptance logo.
Merchant Agreement	A contract between a merchant and an acquirer containing their respective rights, duties and obligations of participation in the scheme payment system.
Mobile Code	This method is an offline 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 to verify cardholder's identity. The check is made by a dedicated application such as an the MCP/MRP or Authentication Application in a secure environment via the mobile device. In EMV this is also referred to 'Consumer Device CVM'.
Mobile Contactless Card Payment Application	An application residing in a secure environment performing the payment functions related to an MCP, as dictated by the MCP issuer.
Mobile Device	Personal 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 cardholder controlled Mobile Device is used at least for the initiation of the payment order and potentially also for the transfer of funds.
Mobile Remote Payment (MRP)	A remote payment initiated by a mobile device whereby the transaction is conducted over a telecommunication network (e.g., GSM, mobile internet,....)
Mobile Remote Card Payment Application	An application residing in a secure environment performing the payment functions related to an (M)RP, as defined by the issuer.
Mobile Remote Payment - Basic Mobile Commerce	A mobile remote payment whereby goods, services, etc. are purchased using a static authentication method.
Mobile Remote Payment - Secured Mobile Commerce	A mobile remote payment using a dynamic authentication method.
Mobile Wallet	Mobile wallet contains information supporting payment services generally performed from or via a mobile device. Also referred to as 'Digital Wallet'.

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	Customer not present transactions via Mail Order or via the telephone [Telephone Order].
Multi-Purpose Prepaid Card (Electronic Purse)	A prepaid card which can be used at the outlets of several service providers for a wide range of purposes. See also prepaid card.
Near Field Communication (NFC)	A short-range high frequency wireless communication technology which enables the exchange of data between devices over about a 10 centimetre distance. The technology is a simple extension of the ISO/IEC 14443 proximity-card standard (proximity card, RFID) that combines the interface of a smartcard and a reader into a single device.
Next Generation (EMVCo)	A EMVCo project enabling the next generation of Card specifications.
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.
Offline Card Transaction	See Offline Transaction.
Offline Data Authentication	A process whereby the card is validated at the point of transaction, using RSA 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 with the Card chip.
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	A chip POI that supports both offline and online processing. This type of POI can authorise a payment locally and can also go online to the Acquirer/Issuer for authorisation when required.
Online Card Transaction	See Online Transaction.
Online PIN	A Cardholder Verification Method. 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 an accepting device following a real-time dialogue between the acquirer and issuer (or its agent). This requires that the accepting device 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 effect 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.
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.

Payer	A natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order.
Payment	The basic service which allows the cardholder to pay for the purchase of goods and services from a card acceptor using his card.
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 Application	Any application that stores, processes, or transmits cardholder data.
Payment Card	A device that offers the cardholder the ability to make payments for goods and services, either at an accepting device or remotely (via mail order, telephone order, Internet - these are known as “card-not-present” transactions) or to access cash at an ATM.
Payment Card Industry (PCI)	A consortium of the following payment schemes, Visa, MasterCard, American Express, JCB and Discover, which became formalized 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 fu0nctional and security requirements described in the Volume applicable to Cards and POIs in a specific transaction environment. Payment contexts are identified either based on specific sector, market or transactional volume requirements.
Payment Credentials	Remote Payment related data provided by the issuer to a consumer (cardholder).
Payment Gateway	A service operated by an Acquirer or a third party 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.
Payment Order	Any instruction by a payer or payee to his payment service provider requesting the execution of a payment transaction.
Payment Product	Product defined by a Payment Scheme.

Payment Service Provider	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 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 amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC ("PSD").
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 payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.
Payment With Aggregated Amount	A feature which allows the card 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 which allows the cardholder to obtain cash from the card acceptor in conjunction with a payment. Also called a "Cashback transaction". The cardholder receives the extra cash amount in notes and/or coins along with the goods/services.
Payment With Deferred Authorisation	A feature where the card acceptor postpones the authorisation of the transaction after the card is no longer available. It is used for Payments performed on airlines/cruise ships and other types of acceptance environments that are not able to be connected 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 a card acceptor to accept payment with loyalty or reward for his 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 remote electronic payments (e-commerce). The personal code is entered via the keyboard of an electronic device to verify cardholder's identity. The check is made by a dedicated application such as a Remote Payment or Authentication Application in a secure environment via the electronic device. A personal code may also be referred to as a 'passcode' or 'password'.
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 his/her identity. In electronic transactions, this is seen as the equivalent of a signature.
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.
Pharming (Fraud)	Pharming is an attack intended to redirect a website's traffic to another, bogus site.
Phishing (Fraud)	Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.
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 for 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 his PIN.
PIN Entry Device (PED)	A secure device that allows cardholders to enter a PIN.
Plaintext	Unenciphered/unencrypted information.
POI Application	POI software for processing the Card Services, compliant with the functional requirements in this document. Depending on the architecture of the POI, the POI Application may be implemented on one component or distributed on several components.
Point-Of-Interaction (POI)	POI Acronym for "Point of Interaction," the initial point where data is read from a card or card data is entered. An electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder or an acceptor to perform a card transaction. The acceptor controlled POI may be attended or unattended. The card data can be entered on a controlled device such as a computer or mobile phone.

Pre-Authorisation Services	A service composed of 2 mandatory and one optional steps: • Pre-Authorisation • Update Pre-Authorisation (optional and potentially with several occurrences) • Payment Completion The Pre-Authorisation allows the card acceptor to reserve an amount for a specified period of time in order to secure that sufficient fund is available to complete a subsequent payment. The pre-authorisation is used only to secure the amount since neither the final amount nor the final date and time of the actual payment are known (e.g. car rental, hotel, video rental, etc.). The Update Pre-Authorisation allows the card acceptor to update the validity and amount of a pre-authorisation. The Payment Completion allows the card 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.
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 Certificate	An asymmetric transformation of the public key by a Certificate Authority and intended to prove to the public key recipient the origin and integrity of the public key.
Public Key Pair	The two mathematically related 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.
PVV	PIN verification value. Discretionary value encoded in magnetic stripe of payment card.
Quasi-Cash Payment	A service which allows the cardholder to obtain items which are directly convertible to cash. For example these can be gaming chips.
Reconciliation	A Service which enables two entities (card acceptor, acquirer, issuer or their agents) to seek an agreement on financial totals (amounts, number of transactions).
Recurring Payment	A service where the cardholder authorises an acceptor to charge the cardholder's 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 or the Cardholder.
Refund	A service which allows the card acceptor to reimburse the cardholder partially or totally. Refund is linked to a previous transaction.
Remote Cardholder Verification	A technology based on a secured architecture that enables the card acceptor's plug-in to check that the cardholder is registered with a secure payment system. It provides the internet details of the cardholder authentication entity (issuing bank or delegated entity). The Remote Cardholder Verification can be either static or dynamic.

Remote Payment	A payment initiated by a device whereby the transaction is conducted over a (tele)communication network (e.g. internet, …) and which can be made independently from the acceptor and cardholder's location.
Remote Payment - Basic Electronic Commerce	A remote payment where goods, services, etc. are purchased over electronic systems such as the internet and other computer networks without using a secured architecture.
Remote Payment - Mobile	See Mobile Payment, Mobile Remote Payment, Mobile Remote Payment – Basic Mobile Commerce, Mobile Remote Payment, Secure Mobile Commerce.
Remote Payment - Moto	A remote payment whereby goods, services, etc. are purchased by mail or telephone order.
Remote Payment - Secured Electronic Commerce	A remote payment whereby goods, services, etc. are purchased over electronic systems such as the internet and other computer networks using a dynamic authentication method.
Remote Transaction	See Remote Payment.
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	A reversal is the partial or complete nullification of the effects of a previous authorization or Data Capture Transaction. A reversal is sometimes also referred to as an authorisation adjustment.
RSA	A public key cryptosystem developed by Rivest, Shamir, and Adleman. It is used for data encryption and authentication.
Secure Element	A secure element (SE) is 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 mobile payments it may be located in the mobile device, such as a secure element or a trusted execution environment, or in a remote secured server.

SecuRe Pay	European Forum on the Security of Retail Payments composed of the European Overseers and Supervisors who agreed on the Recommendations on internet payments published in January 2013 by the ECB.
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.
Settlement	Financial compensation between two parties based on the Financial Presentment. Settlement is a monetary flow which is out of scope of this document.
Signature	The cardholder's handwritten Signature.
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	A card with an embedded microprocessor (chip) loaded with the information necessary to enable payment transactions.
Solution	A Product or a service.
Solution Provider	Software or Hardware vendor selling cards and/or terminal related 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 Data Authentication (SDA)	A type of offline data authentication where the terminal validates a cryptographic value placed on the card by the issuer. Protects against some types of counterfeit fraud but does not protect against skimming. That authentication method that uses always the same authenticator.
Stored Card Data	Card data is retrieved from stored data. This Acceptance Technology is used for Cardholder Not Present transactions.
Strong Authentication	An authentication method which involves, according the SecuRe Pay Recommendations, at least two independent authenticators.
Supported	Indicates that a Card Service or a Function is implemented in the POI Application.
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 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.
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.
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	A type of accepting device.
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" under test to test that it functions as expected.
Three-Party Card Scheme	A card scheme involving the following stakeholders: 1) the cardholder; 2) the card scheme itself, which acts as issuer and acquirer; 3) the accepting party. This contrasts with a four-party card scheme, where the issuer and the acquirer are separate entities and are separate from the card scheme itself. See also card scheme, four-party card scheme.
Transaction Certificate (TC)	Cryptogram generated by the card at the end of either an online or offline approved transaction and can be used by the retailer or acquirer as proof that the card approved the 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 off line and requiring high speed transactions.
Triple Data Encryption Standard (TDES)	The data encryption standard used with a double-length DES key. Sometimes referred to as TDEA or DES3.
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.
Two Factor Authentication	Method of authenticating a user whereby two factors are verified.

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.
Unattended	The cardholder is present and conducts the transaction at the Point of Interaction without the participation of an attendant representing the acceptor or the acquirer (e.g. vending machines, petrol pumps, etc.).
Unsolicited Available Funds	A feature which allows the card issuer to provide account balance information in the authorisation response message.
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	"Vendors" develop products or solutions, eligible for type approval process.
Virtual Card	A card-based payment solution where an alternative, temporary card number with a validity period, limited usage and a pre-defined spending limit is generated which can be used for internet purchases.
Virtual Terminal	A virtual terminal is web-browser-based access to an acquirer, processor or third party service provider website to authorise payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.
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.
XML	The acronym used for “Extensible Markup Language”, a computer metalanguage used to simplify the transmission of formatted data.

4 FIGURES

FIGURE 1: VOLUME OVERVIEW 7