ECSG001-17
(Vol Ref. 8.A01.00)

01.03.2017

SEPA CARDS STANDARDISATION (SCS) "VOLUME"

STANDARDS' REQUIREMENTS

ANNEX 01

SEPA CARDS TRANSACTION FLOWS

Payments and Cash Withdrawals with Cards in SEPA

Applicable Standards and Conformance Processes

Abstract	This document is an Annex to the Volume. It describes some aspects of general transaction flows and contains no requirements.
Document Reference	ECSG001-17
Issue	Annex 01 to SCS Volume - v8.A01.00
Date of Version	1 March 2017
Reason for Issue	Publication
Reviewed by	Approved for publication by the ECSG Board of 9 February 2017
Produced by	ECSG Secretariat
Owned and Authorised by	ECSG
Circulation	Public

Version number	Dated	Reason for revision
Change history of the Volume		
0.1-0.6	22/12/2016	ET Meetings to finalise draft
0.7	31/12/2017	Board Distribution (+editorial changes)
0.8	16/01/2017	Legal Review Version
0.9	24/01/2017	Board Approval Version
v8.A01.00	09/02/2017	First ECSG published version of Annex 01 - Volume v8.0

Table of Contents

1. Introduction

1.1. Background

The European public authorities have devised the concept of “SEPA for Cards”, the purpose of which is to enable Payment Service Users in Europe (such as cardholders and acceptors), to use general purpose cards to make and receive payments and cash withdrawals throughout SEPA with the same ease and convenience as they do in their home country.

In response to the SEPA for Cards concept, the European Payments Council (EPC) created the Cards Stakeholders Group (CSG) in the year 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.

The CSG was disbanded in the year 2016 and a separate legal entity was established under the name of European Cards Stakeholders Group (ECSG) AISBL in April 2016. The ECSG is composed of market representatives from the five main cards related sectors: Payment Service Providers (gathered in the EPC), Processors, Merchants (Acceptors), Schemes and Vendors. The main task of the ECSG is to maintain the SEPA Cards Standardisation (SCS) Volume, a set of Books each describing an important aspect of how SEPA for Cards should be achieved. This can be from a functional, security or conformance perspective.

The Volume is aimed at the entire cards industry active in Europe and provides SEPA standards, which need to be adopted in order to achieve the SEPA for cards. The Volume also represents the efforts made by the market in understanding the requirements that are part of the Interchange Fee Regulation, such as e.g., Art. 7.5 that requires: “Processing entities within the Union shall ensure that their system is technically interoperable with other systems of processing entities within the Union through the use of standards developed by international or European standardisation bodies. In addition, payment card schemes shall not adopt or apply business rules that restrict interoperability among processing entities within the Union.”

1.2. Purpose

The purpose of this document is to provide a ***simplified, high level overview*** of a transaction describing why and where transactions using the same underlying technology (e.g., EMV based ‘Chip and PIN’) may differ in behaviour. International standards include different options which facilitate a variety of risk management approaches. These can result in implementation differences creating different experiences for the customer. Even within SEPA for Cards, there will always be implementation variations from a Payment Service Users perspective for **commercial and technical reasons.**

It is expected that the reader of this document has an understanding of card based payments, is familiar with the specifications and standards mentioned in this document and has read the SCS Volume.

Note that this document covers physical cards as well as card based transactions initiated through a consumer device.

In this document the definitions, abbreviations and references of Book 1 apply.

2. SELECTION OF THE PAYMENT APPLICATION

The first step undertaken when a Card-based Payment Instrument is presented for Payment (hereafter referred to as a ‘Card’), is an agreement between the Payer and Payee as to which Payment Application is to be used for that transaction.

The user experience during selection of the application may vary for several reasons:

- The capabilities of the acceptance device (e.g., touchscreen multi-function device or standalone POI with minimum display);
- The technology and form factor of the Card (e.g., EMV Contact Chip Card or NFC enabled mobile Phone);
- The number of Payment Applications present on the same Card based payment instrument;
- The environment of use (e.g., Supermarket checkout, outdoor petrol, MOTO, or ecommerce).

For e- and m- commerce environments it is common to have a payment page during the check-out process where the cardholder is required to manually enter their payment information on a secure payment page.

3. CARDHOLDER VERIFICATION AND CARD AUTHENTICATION

Cardholder Verification is performed to ensure that the person presenting the Card is the legitimate cardholder.

Card Authentication is performed to authenticate Chip Card data either by the POI Application (Offline Card Authentication), by an Additional Authentication Device and/or by the Issuer (Online Card Authentication).

3.1. Local Transactions

The Cardholder Verification Method, or CVM, is used to evaluate whether the person presenting a payment instrument, such as a payment card, is the legitimate cardholder. An understanding of CVMs is critical to all stakeholders in the payments ecosystem:

- Issuers need to understand CVMs so they can decide which CVMs to support and in what priority order, based on their business needs.
- Acceptors need to ensure that their terminals can support the minimum CVM requirements of the Card Schemes that they accept. Acceptors also need to ensure that their staff can assist customers at the point of sale.
- Acquirers, processors, and value added resellers need to ensure that their terminals support the minimum CVM requirements of the Card Schemes.

3.1.1. Physical cards

A typical SEPA Card may support some or all of the following Cardholder Verification Methods:

- **Online PIN**
- **Offline PIN**
- **Signature**
- **No CVM required.**

The Card's CVM list helps determine which CVM method is performed. The POI reads the list and typically performs the first CVM in the list that it supports (for a detailed explanation of CVM processing please refer to the SCS Volume).

When used over the contact interface, in most cases, PIN is required when a Card personalised with this configuration is used. The difference between Offline and Online PIN is transparent to the cardholder. However, for POIs that do not support PIN (e.g., outside of the SEPA region), a signature would be required. For POIs that support neither PIN nor Signature (e.g., a vending machine or on street parking machine) the cardholder would not be required to provide verification.

When used over the contactless interface, and for transactions below the Reader CVM Required limit (see section 4.1.1), the cardholder would not be required to provide verification. In environments that support online PIN, for transactions above the Reader CVM Required limit, the cardholder would be required to enter their PIN.

It is clear, therefore, that a Card could require different methods of Cardholder Verification, dependant on the environment in which the Card is being used.

3.1.2. Mobile Device

A Mobile Device performing a Contactless based transaction may support all of the following Cardholder Verification Methods

- **CDCVM, for example Biometrics, or Mobile Code verified offline by a dedicated Application**
- **Online PIN**
- **Online Mobile Code**
- **No CVM required**

When using a Mobile Device personalised with this configuration, the cardholder would generally not be required to provide any verification for transactions below the Reader CVM Required limit, provided that no other risk parameters influence the need for a CVM. For transactions above the Reader CVM Required limit (see section 4.1.1) the cardholder would; enter their PIN on the POI, perform CDCVM, or enter an Online Mobile Code. (Note: cardholders often have the option to always require a verification on their mobile device regardless of the transaction amount, this option can be built into the mobile phone operating system or their mobile wallet)

Card Authentication is performed according to the SCS Volume requirements.

3.2. Remote Transactions

When conducting Remote Transactions, the clear boundaries between Cardholder Verification (Cardholder Verification Method) and the Authentication of the payment instrument (Card Authentication) that exist in the Local Transaction environment have become blurred.

For example, authentication of the Card can be combined with verification of the cardholder through the use of an Additional Authentication Device provided by the Issuer. The Card is inserted into the device and the cardholder is then required to enter a PIN. The entering of the PIN generates a one-time code for manual entry into the secure payment page.

For that reason both Cardholder Verification and Card Authentication are discussed here.

The following CVM methods may be considered for e- and m-commerce:

- Mobile code verified off-line in a secure environment by the mobile device (e.g., by a dedicated (M)RP Application or Authentication Application);
- Mobile code verified on-line by the issuer. The verification may take place :
    - via the card network (standard authorisation message);
    - via the internet using a secure channel (outside the card network).
- Offline PIN verification performed in combination with an authentication mechanism (e.g., using an additional authentication device).

In remote transactions, authentication of the payment instrument may be combined with the verification of the cardholder[1]. The Authentication method may use static or dynamic data:

- A **static authentication method** using a *static authenticator* such as Card Security Code (CSC) printed on a physical card. The authentication verification is performed by the issuer. The CSC is manually entered into the consumer device or may be provided by the (M)RP / Authentication Application;
- A **dynamic authentication method** where the "dynamic *authenticator*" may be
    - A One Time Password (OTP) generated by the issuer or its agent and sent by a different channel to the cardholder (e.g., SMS, e-mail, different device);
    - The result of a random challenge / response mechanism. This may be implemented in different ways:
        - An *Additional Authentication Device*. When an authentication device is used, the cardholder inserts their payment card into the additional device and enters their PIN. The authentication device then generates a response which the cardholder is required to enter during the transaction on their consumer device. This response is authenticated by the issuer.
        - A dedicated *Authentication Application.* If an Authentication Application is available via the consumer device, a dynamic authentication method (e.g., challenge/response method) is initiated by the issuer or its agent and is handled automatically by the Authentication Application in a *secure environment*. The cardholder is requested to enter their mobile code during the transaction process.

A Risk Based Authentication method is increasingly used. Issuers are adopting Risk Based Authentication by which every transaction is evaluated for potential risks and, depending on the outcome of the analysis, appropriate measures can be taken. With Risk Based Authentication, both consumer device authentication checks ("is this a known consumer device, what browser is used, is

[1] This section may be impacted by the EBA RTS on SCA

the IP address known?”- referred to as ‘Passive Authentication’ in Book 4) and transaction characteristic checks (“is this a usual transaction for this cardholder, is this an Acceptor type the cardholder regularly visits, what country is the Acceptor in?”) are implemented. Often, the Cardholder may not be aware that Risk Based Authentication is being performed, which provides a seamless cardholder experience.

4. RISK MANAGEMENT AND TRANSACTION ANALYSIS

4.1. Local Transactions

Risk Management parameters are used by both the acceptors and issuers to help determine how a transaction should be processed, for example;

- Is there a need to have the issuer authorise the transaction online (in real time)?
- Is there a need for the cardholder to verify themselves, and if so, what Cardholder Verification Method(s) shall be used?

Risk management parameters exist both in the POI and on the card, and both are used to help determine the outcome of a transaction.

POI risk parameters are configurable and may be updated from time to time to reflect changes in the market, for example a specific market may request an increase to the contactless CVM required limit (see 4.1.1). POI risk parameters are set to values defined by the relevant Card Scheme, Acquirer and Acceptor.

Card Issuers will offer different products targeted at different customer bases. Card products will have different levels of risk associated with their use (e.g., credit versus debit) and Card Issuers will often have different levels of risk that they are prepared to accept, and will set Card risk parameters accordingly. Card based risk parameters are configured during card personalisation and set to values determined by the issuer.

4.1.1. POI Risk Parameters

The following POI Risk Parameters are the most commonly used:

- **Terminal floor limit**
- **Reader Contactless Floor Limit**
- **Reader CVM required Limit**
- **Reader Contactless Transaction Limit**

These risk parameters are used by the POI to help determine whether a transaction requires an online authorisation, whether a CVM is required for this specific transaction, or whether a transaction is allowed over the contactless interface.

Additional POI Risk Parameters may also be used.

4.1.2. Card Risk Parameters

The number and scope of the Risk Parameters available to Issuers is much greater than those available in the POI. This is to allow the Issuer to determine where and when their Card may be used and to set rules based on their risk appetite and on the type of Card Product they have issued.

Whilst some Card Risk Parameters are commonly used, several others are proprietary and so they are not defined here. It is also important to note that the processing of the Card Risk Parameters is transparent to the Acceptor and to the Cardholder, and in all cases the outcome of Card Risk Management will result in one of three outcomes, a decline, an offline approval, or a request for an online approval. The reason for the decision is internal to the Card.

Issuers may determine, for example, based on the specifics of the transaction whether:

- **A CVM is required**
- **The transaction requires an online authorisation**
- **The transaction is allowed on the contactless interface or must switch to the contact chip**
- **What happens if a transaction that requires an online authorisation cannot go online**
- **How many, and to what value, may transactions be performed offline**

4.1.3. Results of Risk Analysis

Once the risk management functions (and other application functions such as Cardholder Verification, offline data authentication etc.) have been performed, the POI and Card make the first decision on how the transaction should proceed, this process is known as Terminal (or Card) Action Analysis. Note that the outcome of Risk Management is only one input into this process. Other factors, such as the outcome of Cardholder Verification also play a part.

In an EMV based environment, the 3 possible outcomes are to either

- Decline offline
- Approve offline
- Require online authorisation

The responses to an online authorisation to the issuer would typically be to either authorise or decline the transaction.

It is possible for the issuer to request a voice referral in the online authorisation response, though this is becoming less widely used, as being able to authenticate the chip card and verify the cardholder through the data contained within the authorisation request message is making a referral largely redundant.

It is also possible for a Card to decline a transaction following an online authorisation (even if the issuer has authorised the transaction), if the Card detects a problem with the cryptogram returned by the issuer, though this is an exception and so will not be discussed further in this document.

The results of Card and Terminal (POI) Action Analysis are combined so that where there is a transaction event for which a corresponding action is required to be taken by either the Card or the POI, the most restrictive action is taken, in this order

- An offline decline
- An online authorisation
- An offline approval

The following are examples showing how, when either the card or the POI require a specific action to be taken, the transaction is completed accordingly.

Example 1 Transaction over Terminal floor limit

POI Configuration. Transaction over floor limit = send online for authorisation.

Card Configuration. Transaction over floor limit = no action required (approve offline).

Transaction flow = The transaction is over the terminal floor limit so the POI's configuration setting (to send the transaction online for authorisation) over-rides the Card setting to approve offline. The transaction is sent online for authorisation.

	Event	POI Setting	Card Setting	Transaction outcome
Example 1	**Transaction over floor limit**	Send online for authorisation	No action required	Send online for authorisation

Example 2 Cardholder verification failure

POI Configuration. Cardholder Verification Fails = send online for authorisation.

Card Configuration. Cardholder Verification Fails = Decline transaction.

Transaction flow = Cardholder verification has failed, and the card configuration requires that the transaction is declined. Although the POI settings would send this transaction online for authorisation if either the Card or the POI decline a transaction this cannot be overruled. The transaction is declined.

	Event	POI Setting	Card Setting	Transaction outcome
Example 2	**Cardholder verification failed**	Send online for authorisation	Decline	Declined

Example 3 Expired card.

POI Configuration. Expired Application = Decline transaction

Card Configuration. Expired Application = Send online for authorisation.

Transaction flow = Although the card issuer has configured the Card to be sent online when expired, the POI configuration is more restrictive and requires the transaction to be declined. The transaction is declined.

	Event	POI Setting	Card Setting	Transaction outcome
Example 3	**Expired application (on card)**	Decline	Approve offline	Declined

4.2. Remote Transactions

In many ways the setting of Risk Parameters in e- and m- commerce is much simpler than in the Local Transaction Environment. For example, for many Card Schemes currently all e- and m-commerce and MOTO transactions operate to a zero floor limit, this negates the need for managing any offline risk parameters.

4.2.1. Virtual POI Risk Parameters

The following risk Parameters are the most commonly used in the Virtual POI

- **Floor Limit**
- **Acquirer CVM Limit**

These risk parameters are used by the Virtual POI to help determine whether a transaction requires an online authorisation or whether a CVM is required for this specific transaction.

Additional POI Risk Parameters may also be used.

This section will be updated after the EBA RTS on SCA

4.2.2. Card Risk Parameters

The Personal / mobile code is the most commonly used Risk Parameter.

5. Online Processing

Online processing is performed to ensure that the issuer can review transactions and reject those that are outside acceptable levels of risk.

The most significant advantage EMV based transactions give over magnetic stripe transactions in the online phase of the transaction, is in the use of cryptography for the issuer to authenticate the validity of the data coming from the card and the POI. The cryptograph provides evidence that neither the Card nor the POI have been tampered with. It also provides the issuer with the opportunity to respond to the Card with an authentication cryptogram in the response message which in turn allows the Card to validate that the response message came from the genuine issuer.

6. FURTHER READING

[EPC MCP IIG]. EPC178-10: Mobile Contactless SEPA Card Payments Interoperability Implementation. Guidelines.