EPC020-08 11.02.2015

(Vol Ref. 7.5.1.05)

SEPA CARDS STANDARDISATION (SCS) "VOLUME"

BOOK 5

CONFORMANCE VERIFICATION PROCESSES

Payments and Cash Withdrawals with Cards in SEPA

Applicable Standards and Conformance Processes

Abstract	This document contains the work on SEPA cards standardisation to date
Document Reference	EPC020-08
Issue	Book 7.5.1.05
Date of Version	11 February 2015
Reason for Issue	Information only (not for consultation)
Reviewed by	CSG
Produced by	CSG Book 5 Expert Team
Owned by	EPC
Circulation	Public

Change history of Book 5		
6.5.0.x		Working version of Book 5
7.5.1.0		EPC Published version – Volume v7.0
7.5.1.05		Version distributed with Volume v7.05 set. Not for consultation.

Table of Contents

1 GENERAL

1.1 Book 5 - Executive summary

The overall aim of the SEPA standardisation process is to deliver "Solutions" (i.e. products and services or any combination of them) which can be used throughout SEPA by all the different Card Payment Schemes. To achieve this, the products must be based on common requirements and processes as detailed in the other Books of the Volume. In addition the products must also comply with Implementation Specifications and have associated Certificates which need to be presented to Card Payment Schemes (CPS)/Approval Bodies (AB) in order to be granted a Type Approval for use by that CPS.

Book 5 of the Volume details requirements on conformance verification processes.

In this Book, the card standardisation ecosystem is described to present the role and responsibilities of each organisation involved, especially the roles of:

- Card Payment Schemes/Approval Bodies
- Specification Providers
- Certification Bodies

Three conformance verification processes are covered in this Book:

- Labelling process: This process confirms that a given Implementation Specification is in line with the Volume requirements. An Implementation Specification is generally developed and managed by Specification Providers who may request a label.
- Certification process: This process is used to verify that a Solution developed by a Solution Provider has been evaluated and proven to be compliant with a given implementation specification. The bodies responsible for confirming this compliance are the Certification Bodies which can be either part of or independent of the Specification Provider's organisation.
- Approval process: This process is used by an AB to grant a Solution Type Approval for use in a CPS based upon the acceptance of the certification of that Solution. In order to verify that the Implementation Specifications expected in the environment or scheme have been correctly implemented. The bodies responsible for awarding Type Approval are the individual CPS/AB.

It is assumed for the purposes of this Book that an independent body responsible for reviewing and monitoring the conformance of particular processes with the relevant sections of the Volume will be established. For the purpose of this iteration of the Volume, such a Volume conformity body will be described as the “SEPA Cards Certification Management Body” or “SCCMB”.

1.2 Description of changes since the last version of Book 5

This version of Book 5 is provided for completeness to enable alignment with the v7.05 release of the Volume books. The content of this version is unmodified from the Book 5 supplied as part of the Volume v7.0 release.

The CSG does not currently intend to update Book 5 for the Volume release 7.1, thus requests that no feedback be supplied for this book during the 7.05 consultation.

2 INTRODUCTION TO THE CONFORMANCE ECOSYSTEM

The Volume provides high level requirements which any "Solution" (i.e. products and services or any combination of them) must conform to in order to be considered Volume conformant. These high level requirements are used by a Specification Provider to create a detailed implementation specification involving relationships with accredited Evaluation Laboratories and Certification Bodies. The Specification Provider may submit their specification for recognition and Labelling by the SCCMB. It is the individual CPS/AB which will issue the actual Type Approval for any particular Solution.

The Conformance Ecosystem details a process with all key actors and process stages clearly identified. Any Solution Provider wishing to deliver a Solution must successfully complete all the steps defined in the ecosystem in order for their Solution to meet the needs of the Volume.

In order to achieve this there are several critical steps that must be successfully completed, and the following sections define in more detail the relationships between the various actors involved, all the necessary steps required and how this can lead to the Type Approval of the Solution Providers Solution.

3 OVERALL PROCESS DESCRIPTION OF THE CONFORMANCE ECOSYSTEM

This section provides a high level introduction to the overall process a Solution Provider must successfully complete in order to obtain Type Approval.

Type approval is the final stage of the process which a solution must undergo in order to obtain approval from a given CPS or Approval Body (AB).

CPS/AB (CPS/AB):

- make the list of required/recognised detailed implementation specifications publicly available, along with the corresponding certification/Type Approval process;
- "Type Approve" the solutions evaluated and certified against these specifications.

The Solution Provider will do/provide the following as necessary:

1. Identify the High Level principles for scheme solution objectives that need to be adhered to for the solution being developed;
2. Identify the functional (interoperability) & security requirements (among available specifications or by building in-house requirements) that the product will adhere to;
3. Identify Implementation Specifications the solution needs to comply with;
4. Develop complying solutions with detailed specifications;
5. Submit the product for Evaluation/Tests performed by accredited Laboratories;
6. Obtain the evaluation report(s) which can then be submitted to the certification body;
7. Submit the report(s) for certification against the applicable Implementation Specifications;
8. List the specifications and implementation options/parameters/configurations to which the product conforms, has been certified for, and for which it is requesting Type Approval (by CPS/AB);
9. Request/facilitate end-to-end testing to finalize the solution validation to obtain the authorisation for deployment.

The target approval and certification ecosystem is shown below for POIs:

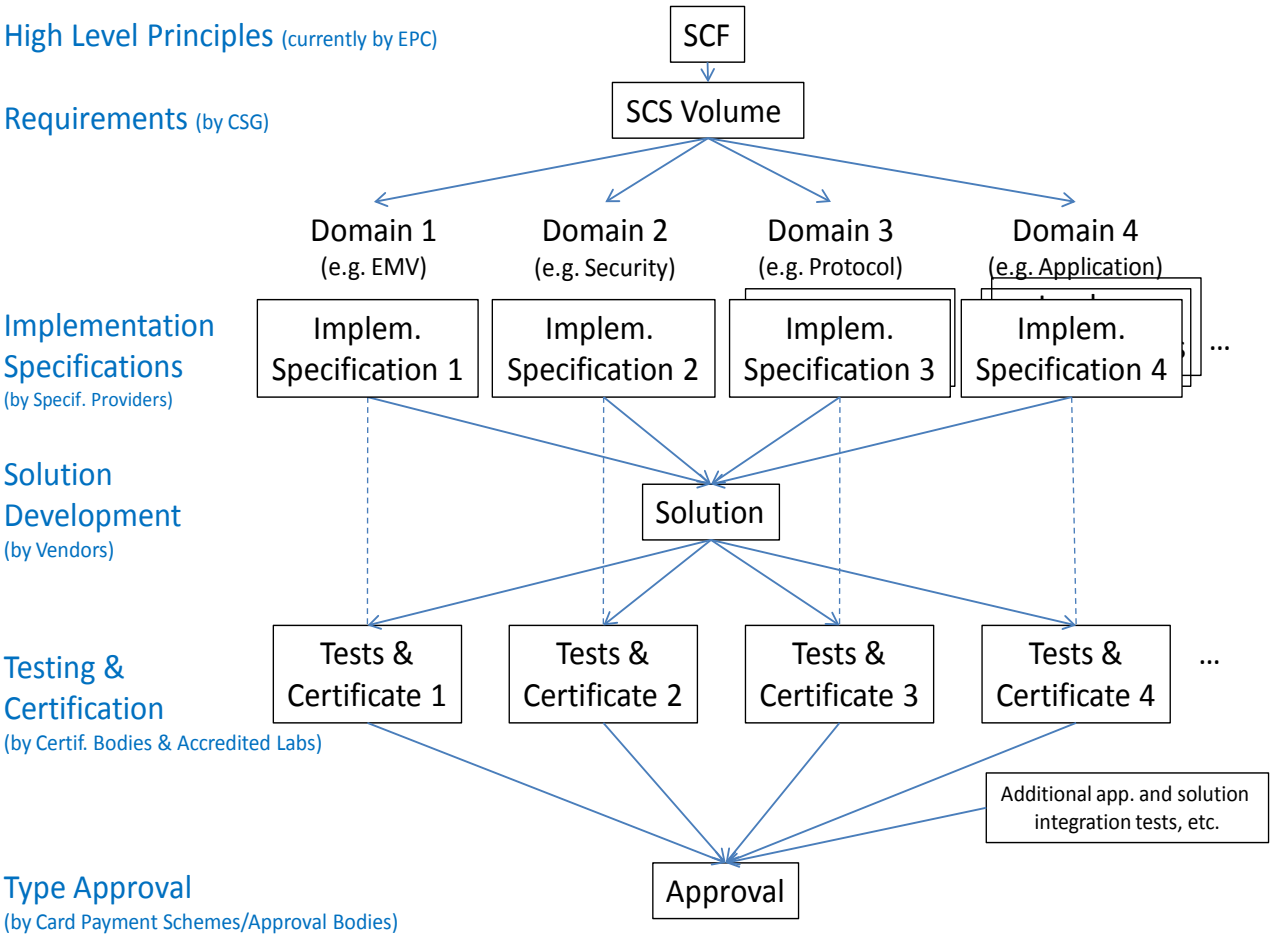
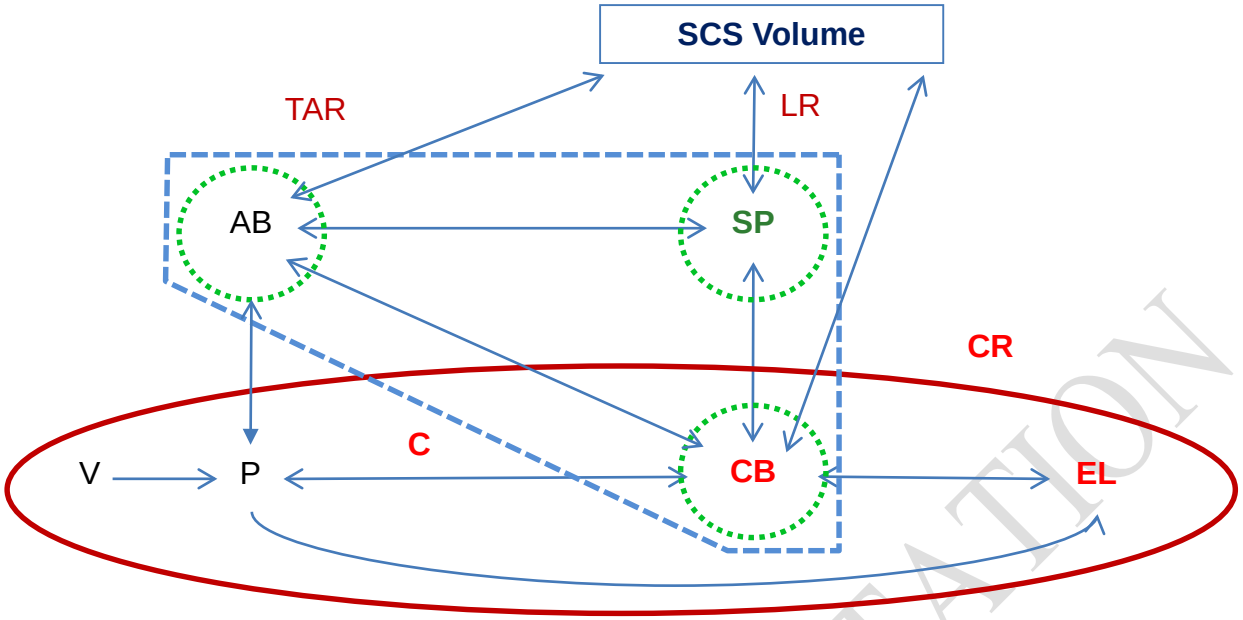


Figure 1: The Type Approval and Certification Ecosystem

Figure 1 shows that products may need to have several certificates (one per domain). In given domains there might be several possible alternative Implementation Specifications and therefore several alternative certifications possible.

The above process for certification and Type Approval is expected to be as depicted in Figure 2 and explained in detail in section 3.1.



AB= Approval Body
SP= **Specification Provider**
CB= **Certification** Body
V=Solution Provider (Vendor)
P=Solution (Product or Service)
C=**Certification**
EL= Evaluation **Laboratories**
LR= **Labelling** Requirements
TAR = Type Approval Requirements
CR= Certification Requirements

Figure 2: The Conformance Ecosystem

3.1 Conformance Ecosystem

A **Card Payment Scheme/Approval Body** is an organisation that is subject to Oversight and Regulation and which is responsible for Risk Assessment, which cannot be delegated. It also ensures end-to-end interoperability of all approved solutions of the card payment chain. Therefore it:

- Selects the required/recognised Implementation Specifications;
- Relies upon the certification processes of solutions against these Implementation Specifications;
- Is responsible for issuing Type Approval for solutions certified by one or more certification bodies for a particular market or CPS.

A **Certification Body** is an organisation responsible for:

- Issuing certificates to confirm that solutions have been successfully tested against a given implementation specification. This process is based on evaluations or tests performed by laboratories accredited by the certification body.

A **Specification Provider** is an organisation which:

- Uses or develops Implementation Specifications based upon the high level requirements specified in the Volume for use by Solution Providers to develop 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 solutions.

The tasks to ensure the above mentioned functions can either be in the same organisation or in several separate organisations, such as:

1. One or several independent organisations purely for the production of the Implementation Specification (detailed technical specifications);
2. One or several independent organisations for the certification of the solutions.

Note that several Implementation Specifications may be developed based on the requirements contained in the Volume as several alternative Implementation Specifications (e.g. POI to Acquirer protocols) can coexist in the market. It will be up to the market to decide on the future evolution of such Implementation Specifications.

Solution Providers offer solutions based on Implementation Specifications for one or several components of the card payment value chain (e.g. a card, a POI, an acquirer host). Some solutions may integrate several Implementation Specifications, for instance a POI should at least integrate the POI application, the POI to Acquirer protocol, and the POI to card protocol.

The Conformance Ecosystem as described above applies to both functional and security related aspects.

4 CONFORMANCE PROCESSES

4.1 The Volume Labelling Process

The Volume defines high level functional and security requirements. Based on these requirements detailed Implementation Specifications can be developed against which a Solution Provider, such as a POI Vendor, is able to develop solutions, such as a POI terminal. The conformance of a solution with an Implementation Specification is controlled by the Certification process. The Labelling process, which is optional, verifies that an Implementation Specification and its governance and maintenance processes conform to the requirements of the Volume.

The management of the Labelling process will be undertaken by the Labelling entity (SCCMB). The Specification Providers are the entities who will submit their specification and process to the Labelling process.

4.1.1 Rationale

Within the context of SEPA, the Volume defines high level requirements (functional and security) that apply to card payment transactions of CPS.

The Labelling process aims at confirming that

- The Implementation Specification conforms with the high level requirements of the Volume;
- The Specification Provider has established a governance and maintenance process to ensure the relevant procedural requirements of the Volume are met.

Specification Providers are organisations producing Implementation Specifications used by Solution Providers to develop solutions. The Volume defines "procedural" requirements applying to those Specification Providers and aiming to ease the deployment in the market of solutions implementing those Implementation Specifications.

When a Solution Provider decides to develop a solution that meets an Implementation Specification which has been labelled by the SCCMB, then the Solution Provider can be confident that the technical specifications and the governance structure established by the Specification Provider conform with the Volume.

The proposed ecosystem highlights the role and responsibility of the Specification Providers. They are expected to provide detailed Implementation Specifications and indicate how certification of solutions is to be carried out. Any entity may be a Specification Provider and if so, is expected to meet the requirements of the Labelling process.

The Labelling process contributes to the emergence of specifications which are open and transparent to any stakeholder active in SEPA.

Specification Providers in the ecosystem will publish (e.g. via a website) relevant information and specifications for interested stakeholders.

Another important characteristic of the ecosystem is that several alternative Implementation Specifications may coexist within the card payment value chain facilitating an open market of conformant standards, for instance the POI-Acquirer protocol.

An Implementation Specification with a Volume Label which addresses the needs of interested stakeholders (e.g. functionality, maintainability…) could result in the reduction of the number of Implementation Specifications supported throughout SEPA.

4.1.2 Labelling Process Description

Whilst the Labelling process is optional, any Specification Provider which wishes to have a Volume Label for a given Implementation Specification must undergo the "Labelling" process defined in the Volume.

The aim of this Label is to demonstrate that:

1) The Implementation Specification conforms with the high level requirements of the Volume.
2) The Specification Provider has established procedures compliant with the procedural requirements described below which are aimed at ensuring
    a. The setup of a governance structure open to stakeholders interested by the implementation of the specification (e.g. Solution providers);
    b. The maintenance of the implementation specification;
    c. The availability of information to solution providers about how their solutions will be certified;
    d. The interoperability of solutions once they are deployed in the field, for instance that any poi may interact with any acquiring processor if both support the same implementation specification.

This Labelling process is based on the principles of a self-declaration procedure by the Specification Provider.

The Specifications Provider shall provide the Labelling Entity (SCCMB) with:

- A Conformance Document (including its maintenance process), in the form of a checklist, describing its conformance with the Volume, including:
    - The scope of the Implementation Specification (e.g. The part of the card transaction value chain, for instance the POI to Acquirer protocol) and the set of services covered (e.g. POS, remote internet);
    - A list of the Volume requirements applying to the Implementation Specification.
- The Implementation Specification documentation;
- A Governance Manual describing the governance established and how the organisation will implement the procedural requirements described below;
- Proof of existence of all required elements described in section 4.1.5.

The Labelling Entity (SCCMB) will manage the process for confirming conformance to the Volume based on evidence provided by the Specification Provider.

On a regular basis and at least annually, the Specification Provider shall check if there is any significant change in the Volume or its Implementation Specification or its related procedures (e.g. governance, maintenance) which would require the specification provider to reapply for a Volume Label.

4.1.3 SCCMB Responsibilities within the Labelling process

Within the Labelling process the SCCMB will perform the following tasks:

- Receive Labelling requests from Specification Providers;
- Verify that all necessary documentation has been provided;
- Grant a label after positive review;
- Make labels publicly available;
- Ensure certificates granted to solutions by certification bodies are made publicly available;
- Update labels granted and certificates granted to solutions;
- Manage disputes.

4.1.4 Implementation Considerations

CPS/AB are not obliged to recognise or use a specification to which a label has been given. This is because the SCS Volume only defines high level requirements. As such an interpretation of the high level requirement by a particular Specification Provider may not meet all the detailed program needs and requirements of a particular CPS/AB. In addition whilst a label may be applied to a Specification Providers Implementation requirements, it could also be that the list of high level requirements used to develop the Implementation Specifications does not cover all the requirements or specific needs of the CPS/AB.

A proprietary specification is either reserved for private use or made available under non publicly available licence. Proprietary specifications are not expected to be subjected to the Labelling process. While even though such specifications may be conformant to the Volume, they are meant to be used only on a proprietary basis or are only made available under license.

4.1.5 Requirements on Specification Providers

The Specification Provider applying for a Volume Label will have to demonstrate that it has implemented procedures compliant with the following procedural requirements.

4.1.5.1 Protection of Intellectual Property Rights

The Specification Provider shall publicly state its IPR provisions.

4.1.5.2 Establishment of a Governance Structure

The Specification Provider

- Shall have a governance procedure for defining and agreeing the specification, implementation and procedural requirements;
- Shall have a governance manual containing the relevant operational rules (e.g. Voting rules, responsibilities, users groups or stakeholders consultation) that are applicable to all stakeholders;
- Shall make public its criteria for participation;
- Shall define a licensing policy for the implementation of its implementation specification and shall ensure its open access to any solution provider under fair reasonable and non-discriminatory ("frand") conditions.

It is recommended that the Specification Provider:

- Provides implementation guidance and best practices;
- Establishes solution providers user groups and organises regular user groups meetings, for the coordination of the evolution of the implementation specifications;
- Provides technical support services to solution providers in order to facilitate the specifications implementation;
- Optionally provides test tools aiming to facilitate the development by solution providers.

4.1.5.3 Maintenance of the Implementation Specification

The Specification Provider:

- Shall ensure the Implementation Specification maintains conformance with the latest published version of the Volume;
- Shall establish a Release Management process for new versions which should focus specifically on migration issues as every change impacts multiple parties and this shall be done every time a new version is required to keep in alignment with the Implementation Specification;
- Shall provide procedures for identification and management of issues;
- Should ensure that relevant stakeholders (e.g. Solution Providers) may provide input and comment on the evolution of the Specifications.

4.1.5.4 Establishment of a Certification process for solutions developed against the Implementation Specification

The Specification Provider, independently or in cooperation with Certification Bodies, through their formal or informal relationship, provides or indicates:

- A sustainable Certification framework for Solution Providers developing solutions against the Implementation Specifications, which may include:

- The definition of the different phases of the certification (e.g. Test with simulator, test by accredited laboratories, field test);
- The list of deliverables to be provided by Solution Providers;
- The list of deliverables produced during the certification process;
- The establishment of testing laboratories accreditation, contractual and monitoring process (e.g. Technical scope, contractual agreement) and the publication of a list of accredited laboratories.

- The management of the Certification process which may include,
  - Ensuring the follow-up of each ongoing Certification process, within the time frames agreed in the service description;
  - Publishing, on a public site the list of certified solutions and the functionalities they are certified for;
  - Defining a validity period for issued certificate.

4.1.5.5 Ensuring interoperability of solutions

Interoperability aims to ensure that when various solutions are brought together into a specific environment that all of the components will work as specified. Operational and Specification ranges can result in components at either end of the range coming together. It is critical that these components and solutions work as well as all other options.

It is the responsibility of the CPS/AB to define or coordinate an interoperability policy.

Interoperability aims to ensure that any product or solution of one side shall be able to interact with any product or solution of the other side, supporting the same Implementation Specification, such as e.g.

- Card to POI: any card with any POI;
- POI to Acquirer: any POI with any Acquirer;
- Acquirer to Issuer: any Acquirer with any Issuer.

In this instance Card represents all methods by which a cardholder can undertake a payment, e.g. Chip and PIN, Contactless, or any other permitted method.

The CPS should provide procedures for an operational follow-up to all relevant parties, especially Specification Providers to identify potential interoperability issues and establish procedures that need to be followed to solve them.

4.2 The Certification Process

This section details requirements on “Certification” which is the process required to validate that a solution (e.g. POIs and cards) complies with a set of Implementation Specifications and requirements.

The rules to be applied by the Certification Bodies acting in the European card standardisation ecosystem are described hereafter. These requirements address the Certification Bodies, which can either be independent or part of the Specification Provider organisations.

A Certification Body must meet all of the following requirements:

- The entity providing certification services acts for more than one AB.
- Certification Bodies shall apply ISO 17065 standard (Conformity assessment - Requirements for bodies certifying products, processes and services).
- Where Certification Bodies use external laboratories and testing facilities the Certification Body shall require their accredited Laboratories to maintain conformance with the ISO 17025 standard.[1]

The methodology, used by Certification bodies or their laboratories, to evaluate the compliance of solutions against Implementation Specifications must be openly and publicly available and the conduct of any evaluations against this methodology must be independent of any management direction from any specific AB.

Where the Specification Provider and the Certification Body are managed in the same organisation, the following principles must be applied in order to give confidence in the certification activities: impartiality, confidentiality, openness and fair treatment of complaints and appeals. Separation should exist between certification operation (the recognition and management of the laboratory and the delivery of the certificate) and specification writing. This can be achieved either by separating the organisation performing those tasks or by different groups within the same organisation.

Where the Specification Provider and the Certification Body are not managed in the same organisation, coordination shall be established in order to meet the requirements expressed in section 4.1.5.4 and the principles expressed in the paragraph above.

4.3 The Type Approval Process

This section aims to clearly define the scope of the Type Approval Process performed by CPS/AB after solutions have been certified (functional and security).

Type Approval is defined as a final validation, performed by an AB, before the product or solution may be deployed and used.

4.3.1 Implementation Specifications recognised by Approval Bodies

Each AB is expected to make public on its website the list of Implementation Specifications it requires/recognises as being able to support transactions under its responsibility.

For supported Implementation Specifications, AB should define clearly where they apply, including but not limited to which

- Merchant sector;

[1] A laboratory may be part of a Certification Body.

- Type of transactions.

It is assumed that AB have internal processes to analyse and evaluate Implementation Specifications that are relevant to their payment schemes.

It is further assumed that AB will not add unreasonable and unjustifiable requirements to either the Implementation Specifications or the requirements of the Volume. Should additional requirements be identified in or made to any Implementation Specifications or to the Volume, AB will bring these to the change management processes of the specification or of the Volume as specified in Book 1.

4.3.2 Type Approval activity

The AB will publish on a public website the scope of its Type Approval activity and the procedures to be used by a Solution Provider (e.g. a POS provider, a Processor) or other entity.

A CPS/AB is responsible to ensure end-to-end interoperability of all approved solutions of the card payment chain.

It is expected that the Type Approval phase is:

- An administrative activity: verifying that the Product presented for Type Approval by a Requester (e.g. A POI Vendor, a Processor) has the required certificates for that scheme (e.g. For a POI: a CC Security Certificate, the PCI SSC Certificate, the EMVCo level 1 and level 2 approvals, the Functional Certificates of the Implementation Specification supported);
- A final validation activity: having the opportunity to perform end-to-end or interoperability testing of the product;
- To conduct a pilot deployment if necessary in an operational environment, potentially in collaboration with the Requester; the aim of this pilot being to ensure that the product supports transactions under responsibility of the AB according to the product rules of a given payment scheme. An authorisation for using a given solution for transactions under the responsibility of that AB;
- A risk assessment activity based upon the results of the above activities, and any potential issues or weaknesses that may have been raised either during the evaluation or certification of the product, service or solution.

These conditions should be publicly available.

The AB will publish on a publicly accessible website the list of approved solutions (making reference to the specific Implementation Specifications).

An AB may remove or suspend Type Approval under specific conditions (e.g. specific vulnerabilities or threats, a certificate expired or a certificate has been withdrawn).

4.4 Information to be made public

4.4.1 SCCMB

When established, the SCCMB is expected to make public

- The list of "Labelled" Implementation Specifications (their Specification Providers and where appropriate, the associated Certification Bodies);
- The list of "Certificates" granted to solutions having implemented labelled implementation specifications or the link to the public website of the Certification Body where these can be found.

4.4.2 Approval Body

The AB will make public

- The domain of applicability and scope of the Type Approval process;
- The Required/Recognised set of Implementation Specifications, with optional "context" specificities;
- The list of approved solutions with reference to applicable Implementation Specifications;
- Governance and participation principles;
- Its interoperability policy.

The AB will compile in a matrix one or several sets of accepted Implementation Specifications.

4.4.3 Specification Provider

The Specification Providers will make public

- The process by which the specifications may be obtained;
- The licence terms and conditions;
- The exact references and version of such specifications;
- The process by which the certifications may be obtained;
- The maintenance process of the above, if applicable;
- The governance and participation principles.

4.4.4 Certification Body

The Certification Bodies will make public

- Supported specifications;
- Description of the certification process;
- The process by which the certifications may be obtained;
- List of approved laboratories;
- Accreditation process (process on how to become an approved lab);

- Certificate lifecycle (if applicable);
- Maintenance process for laboratories;
- List of certified solutions;
- Governance principles.

5 FIGURES