1   **SEPA CARDS STANDARDISATION (SCS) "VOLUME"**

2   # BOOK 5

3   CONFORMANCE VERIFICATION PROCESSES

4

5   *Payments and Cash Withdrawals with Cards in SEPA*

6   *Applicable Standards and Conformance Processes*

7

8   © European Payments Council/Conseil Européen des Paiements AISBL.
9   Any and all rights are the exclusive property of
10   EUROPEAN PAYMENTS COUNCIL - CONSEIL EUROPEEN DES PAIEMENTS AISBL.

11

12

13

Abstract	This document contains the work on SEPA cards standardisation to date
Document Reference	EPC020-08
Issue	Book 7.5.2.50
Date of Version	26 May 2016
Reason for Issue	Consultation
Reviewed by	CSG
Produced by	CSG Secretariat
Owned and Authorised by	EPC
Circulation	Public

14

Change History of Book 5		
6.5.0.x	2012-2013	Working version of Book 5
7.5.1.0	12.12.2013 (published 07.01.2014)	EPC Published version – Volume v7.0
7.5.1.05	11.02.2015 (published 10.03.2015)	Version distributed with Volume v7.05 set. <u>Not</u> used for consultation.
7.5.2.1	08.12.2015	EPC Published version – Volume v7.1
7.5.2.11-7.5.2.5	16.12.2015-	Working Version 2015-2016

15

16

17

18 | **Table of Contents**

47

48

49	**1** **GENERAL**

50   **1.1   Book 5 - Executive summary**

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

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

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

61   • Card Payment Schemes/Approval Bodies

62   • Specification Providers

63   • Certification Bodies

64   Three conformance verification processes are covered in this Book:

65   • Labelling process: This process confirms that a given Implementation Specification is in line
66   with the Volume requirements. An Implementation Specification is generally developed
67   and managed by Specification Providers who may request a label.

68   • Certification process: This process is used to verify that a Solution developed by a Solution
69   Provider has been evaluated and proven to be compliant with a given implementation
70   specification. The bodies responsible for confirming this compliance are the Certification
71   Bodies which can be either part of or independent of the Specification Provider's
72   organisation.

73   • Approval process: This process is used by an AB to grant a Solution Type Approval for use
74   in a CPS based upon the acceptance of the certification of that Solution. In order to verify
75   that the Implementation Specifications expected in the environment or scheme have been
76   correctly implemented. The bodies responsible for awarding Type Approval are the
77   individual CPS/AB.

78   It is assumed for the purposes of this Book that an independent body responsible for reviewing and
79   monitoring the conformance of particular processes with the relevant sections of the Volume will
80   be established. For the purpose of this iteration of the Volume, such a Volume conformity body
81   will be described as the "Volume Conformance Management Committee" or "VCMC".

82

83 **1.2 Description of changes since the last version of Book 5**

84 This version of Book 5 is unmodified from the v7.1 release (December 2015). Feedback on this
85 release during the 2016 public consultation is welcomed by the CSG.

86 ## 2 INTRODUCTION TO THE CONFORMANCE ECOSYSTEM

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

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

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

101 **3 OVERALL PROCESS DESCRIPTION OF THE CONFORMANCE ECOSYSTEM**

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

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

106 CPS/AB (CPS/AB):

107 • make the list of required/recognised detailed implementation specifications publicly
108 available, along with the corresponding certification/Type Approval process;

109 • "Type Approve" the solutions evaluated and certified against these specifications.

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

111 1. Identify the High Level principles for scheme solution objectives that need to be
112 adhered to for the solution being developed;

113 2. Identify the functional (interoperability) & security requirements (among available
114 specifications or by building in-house requirements) that the product will adhere to;

115 3. Identify Implementation Specifications the solution needs to comply with;

116 4. Develop complying solutions with detailed specifications;

117 5. Submit the product for Evaluation/Tests performed by accredited Laboratories;

118 6. Obtain the evaluation report(s) which can then be submitted to the certification body;

119 7. Submit the report(s) for certification against the applicable Implementation
120 Specifications;

121 8. List the specifications and implementation options/parameters/configurations to which
122 the product conforms, has been certified for, and for which it is requesting Type
123 Approval (by CPS/AB);

124 9. Request/facilitate end-to-end testing to finalize the solution validation to obtain the
125 authorisation for deployment.

126   The target approval and certification ecosystem is shown below for POIs:
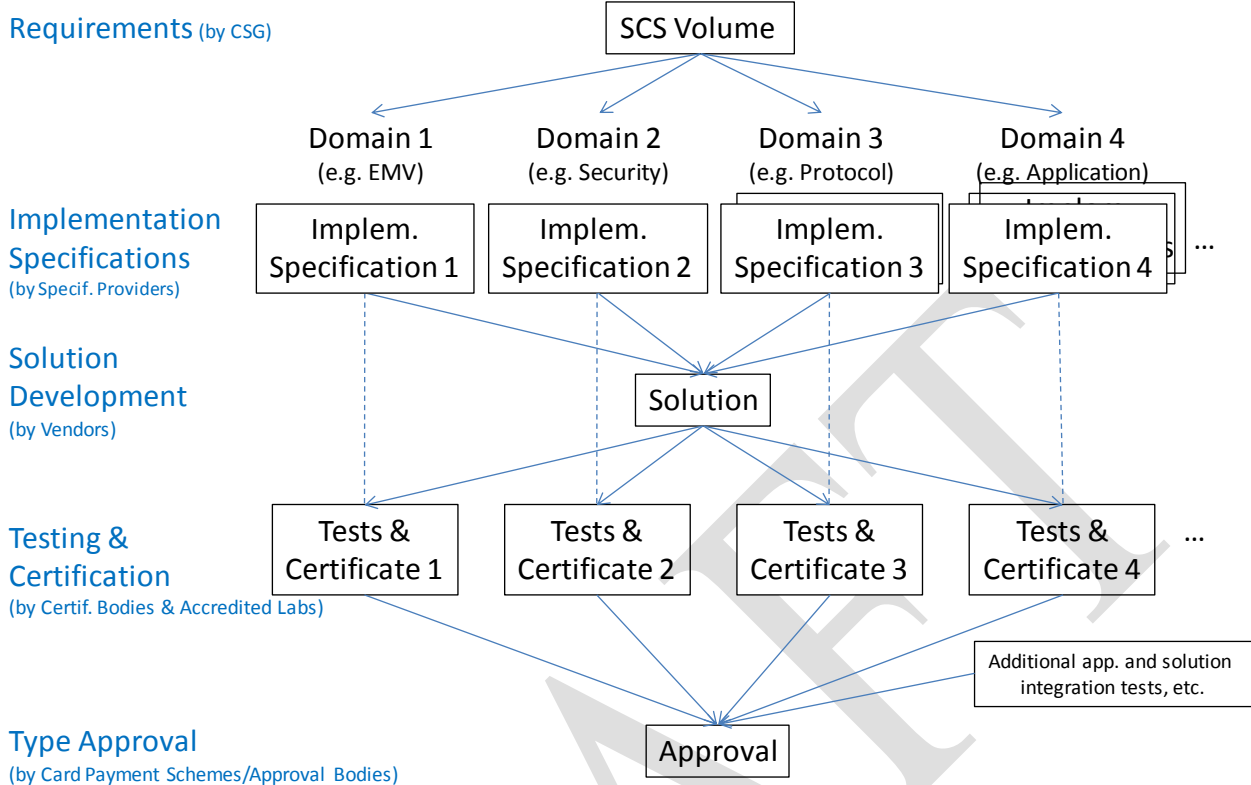
127

128   Figure 1: The Type Approval and Certification Ecosystem

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

132   The above process for certification and Type Approval is expected to be as depicted in

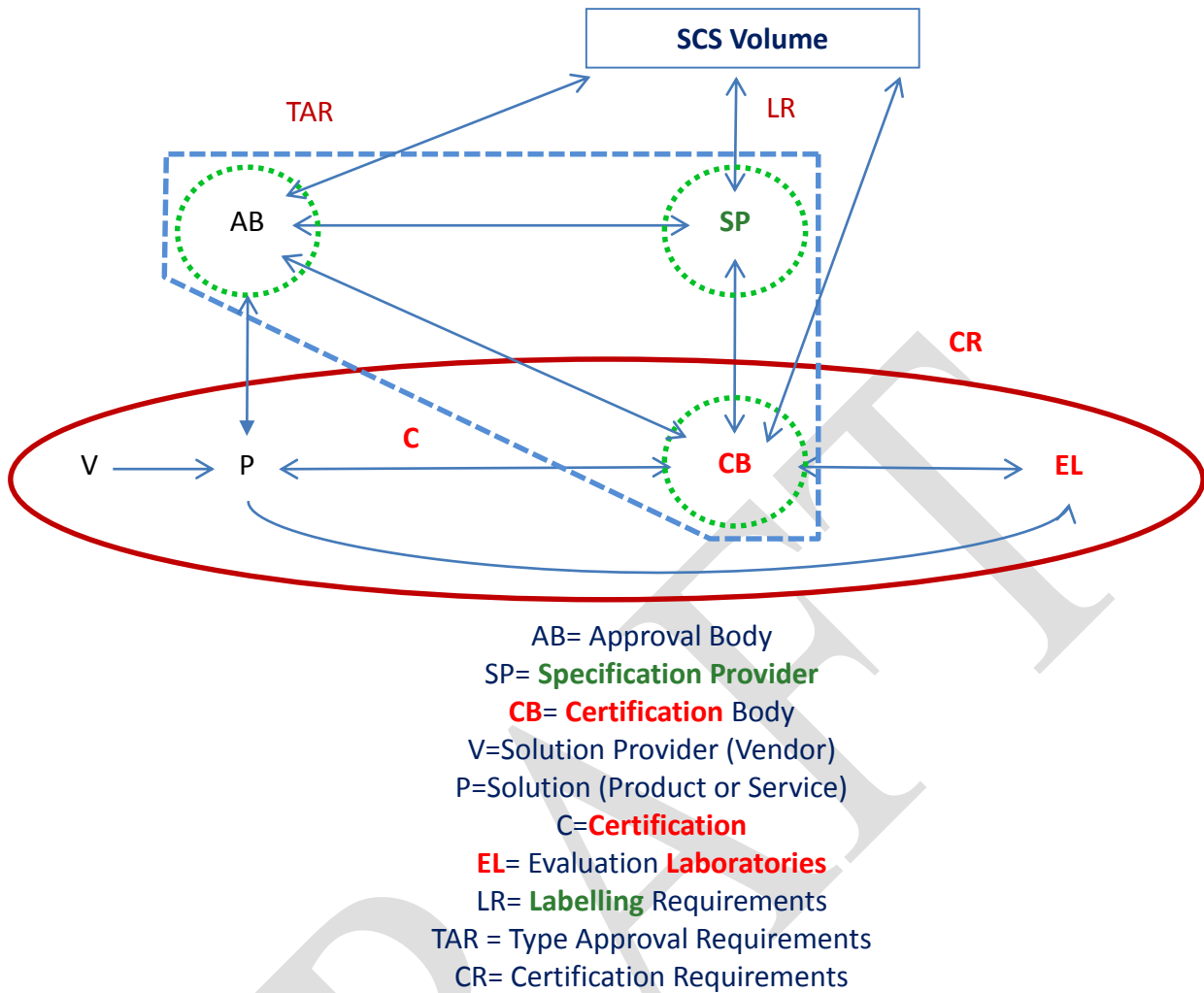133   Figure 2 and explained in detail in section 3.1.

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

134

135   Figure 2: The Conformance Ecosystem

136   **3.1   Conformance Ecosystem**

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

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

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

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

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

151 • Uses or develops Implementation Specifications based upon the high level requirements
152 specified in the Volume for use by Solution Providers to develop solutions;
153 • Provides a maintenance process, notably for interoperability and/or security issues linked
154 to the implementation specifications;
155 • Has its own certification body or a relationship (formal or informal) with an external
156 certification body to certify solutions.

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

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

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

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

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

172

173 # 4 CONFORMANCE PROCESSES

174 ## 4.1 The Volume Labelling Process

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

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

184 ### 4.1.1 Rationale

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

187 The Labelling process aims at confirming that

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

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

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

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

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

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

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

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

214 **4.1.2   Labelling Process Description**

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

218 The aim of this Label is to demonstrate that:

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

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

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

234   • A Conformance Document (including its maintenance process), in the form of a checklist,
235   describing its conformance with the Volume, including:
236   o The scope of the Implementation Specification (e.g., The part of the card transaction
237   value chain, for instance the POI to Acquirer protocol) and the set of services
238   covered (e.g., POS, remote internet);
239   o A list of the Volume requirements applying to the Implementation Specification.
240   • The Implementation Specification documentation;
241   • A Governance Manual describing the governance established and how the organisation will
242   implement the procedural requirements described below;
243   • Proof of existence of all required elements described in section 4.1.4.

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

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

4.1.3 VCMC Responsibilities within the Labelling process

251 Within the Labelling process the VCMC will perform the following tasks:

252 • Receive Labelling requests from Specification Providers;

253 • Verify that all necessary documentation has been provided;

254 • Grant a label after positive review;

255 • Make labels publicly available;

256 • Ensure certificates granted to solutions by certification bodies are made publicly available;

257 • Update labels granted and certificates granted to solutions;

258 • Manage disputes.

4.1.4 Requirements on Specification Providers

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

4.1.4.1 Protection of Intellectual Property Rights

263 The Specification Provider shall publicly state its IPR provisions.

4.1.4.2 Establishment of a Governance Structure

265 The Specification Provider

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

275 It is recommended that the Specification Provider:

276 • Provides implementation guidance and best practices;

277 • Establishes solution providers user groups and organises regular user groups meetings, for
278   the coordination of the evolution of the implementation specifications;

279 • Provides technical support services to solution providers in order to facilitate the
280   specifications implementation;

281 • Optionally provides test tools aiming to facilitate the development by solution providers.

282 **4.1.4.3 Maintenance of the Implementation Specification**

283 The Specification Provider:

284 • Shall ensure the Implementation Specification maintains conformance with the latest
285   published version of the Volume;

286 • Shall establish a Release Management process for new versions which should focus
287   specifically on migration issues as every change impacts multiple parties and this shall be
288   done every time a new version is required to keep in alignment with the Implementation
289   Specification;

290 • Shall provide procedures for identification and management of issues;

291 • Should ensure that relevant stakeholders (e.g., Solution Providers) may provide input and
292   comment on the evolution of the Specifications.

293 **4.1.4.4 Establishment of a Certification process for solutions developed against the Implementation**

294   **Specification**

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

297 • A sustainable Certification framework for Solution Providers developing solutions against
298   the Implementation Specifications, which may include:
299   o The definition of the different phases of the certification (e.g., Test with simulator,
300   test by accredited laboratories, field test);
301   o The list of deliverables to be provided by Solution Providers;
302   o The list of deliverables produced during the certification process;
303   o The establishment of testing laboratories accreditation, contractual and monitoring
304   process (e.g., Technical scope, contractual agreement) and the publication of a list
305   of accredited laboratories.
306 • The management of the Certification process which may include,
307   o Ensuring the follow-up of each ongoing Certification process, within the time frames
308   agreed in the service description;
309   o Publishing, on a public site the list of certified solutions and the functionalities they
310   are certified for;
311   o Defining a validity period for issued certificate.

312 **4.1.4.5 Ensuring interoperability of solutions**

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

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

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

321 • Card to POI: any card with any POI;
322 • POI to Acquirer: any POI with any Acquirer;
323 • Acquirer to Issuer: any Acquirer with any Issuer.

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

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

329 **4.2 The Certification Process**

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

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

336 A Certification Body must meet all of the following requirements:

337 - The entity providing certification services acts for more than one AB.
338 - Certification Bodies shall apply ISO 17065 standard (Conformity assessment - Requirements
339 for bodies certifying products, processes and services).
340 - Where Certification Bodies use external laboratories and testing facilities the Certification
341 Body shall require their accredited Laboratories to maintain conformance with the ISO
342 17025 standard.[1]

---

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

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

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

354 Where the Specification Provider and the Certification Body are not managed in the same
355 organisation, coordination shall be established in order to meet the requirements expressed in
356 section 4.1.4.4 and the principles expressed in the paragraph above.

357 **4.3   The Type Approval Process**

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

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

362 **4.3.1   Implementation Specifications recognised by Approval Bodies**

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

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

367   • Merchant sector;

368   • Type of transactions.

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

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

376 **4.3.2   Type Approval activity**

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

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

381 It is expected that the Type Approval phase is:

382 - An administrative activity: verifying that the Product presented for Type Approval by a
383   Requester (e.g., A POI Vendor, a Processor) has the required certificates for that scheme
384   (e.g., For a POI: a CC Security Certificate, the PCI SSC Certificate, the EMVCo level 1 and level
385   2 approvals, the Functional Certificates of the Implementation Specification supported);
386 - A final validation activity: having the opportunity to perform end-to-end or interoperability
387   testing of the product;
388 - To conduct a pilot deployment if necessary in an operational environment, potentially in
389   collaboration with the Requester; the aim of this pilot being to ensure that the product
390   supports transactions under responsibility of the AB according to the product rules of a
391   given payment scheme. An authorisation for using a given solution for transactions under
392   the responsibility of that AB;
393 - A risk assessment activity based upon the results of the above activities, and any potential
394   issues or weaknesses that may have been raised either during the evaluation or certification
395   of the product, service or solution.

396 These conditions should be publicly available.

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

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

401 **4.4   Information to be made public**

402 **4.4.1   VCMC**

403 When established, the VCMC is expected to make public

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

409   **4.4.2   Approval Body**

410   The AB will make public

411   -   The domain of applicability and scope of the Type Approval process;
412   -   The Required/Recognised set of Implementation Specifications, with optional "context"
413   specificities;
414   -   The list of approved solutions with reference to applicable Implementation Specifications;
415   -   Governance and participation principles;
416   -   Its interoperability policy.
417   The AB will compile in a matrix one or several sets of accepted Implementation Specifications.

418   **4.4.3   Specification Provider**

419   The Specification Providers will make public

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

426   **4.4.4   Certification Body**

427   The Certification Bodies will make public

428   -   Supported specifications;
429   -   Description of the certification process;
430   -   The process by which the certifications may be obtained;
431   -   List of approved laboratories;
432   -   Accreditation process (process on how to become an approved lab);
433   -   Certificate lifecycle (if applicable);
434   -   Maintenance process for laboratories;
435   -   List of certified solutions;
436   -   Governance principles.

437 | **5   FIGURES**

440

441   ∽∾