

DELIVERABLE



Project Acronym: PEPPOL
Grant Agreement number: 224974
Project Title: Pan-European Public Procurement Online



PEPPOL Deliverable D1.3 Demonstrator and functional Specifications for Cross-Border Use of eSignatures in Public Procurement

Part 7: eID and eSignature Quality Classification



Revision: 2.2



Authors:

Germany: bremen online services
Norway: Difi
Italy: InfoCamere, InfoCert
France: ADETEF, DILA, Lex Persona, ANSSI, Esteral Consulting
Greece: University of Piraeus

Project co-funded by the European Commission within the ICT Policy Support Programme		
Dissemination Level		
P	Public	X
C	Confidential, only for members of the consortium and the Commission Services	

Revision History

Revision	Date	Author	Organisation	Description
1.0	2009/02/11			Complete version of D1.1 for internal quality assurance.
1.1	2009/02/27			D1.1 submitted to PEPPOL project management, approved with comments at project management meeting 2009/03/27.
1.2	2009/04/30			D1.1 for publication, updated according to comments.
1.3	2009/11/06			Formal update of D1.1 after EC approval.
1.8	2010/09/22			Complete D1.3 version edited from D1.1 part 7. For internal quality assurance.
1.9	2010/09/30			D1.3 submitted to PEPPOL project operating office (POO) for approval.
1.9.5	2010/11/05			D1.3 ready for publication, updated according to comments from POO. Uploaded for EC approval.
2.0	2010/07/15			Formal update after EC approval.
2.1	2011/08/30			Implementation of EC recommendations.
2.2	2012/04/25			Sharpening terms TSL vs. TL and finalising for hand over

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Statement of copyright



This deliverable is released under the terms of the **Creative Commons Licence** accessed through the following link: <http://creativecommons.org/licenses/by/3.0/>.

In short, it is free to

Share — to copy, distribute and transmit the work

Remix — to adapt the work

Under the following conditions

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).



Table of Contents

1	Summary and Structure of Document	5
1.1	Scope and Structure of Deliverable D1.3	5
1.2	Demonstrator Software Components and Documentation	5
1.3	Scope and Structure of this Document	6
1.4	Evolution of this Document and Changes from D1.1	6
1.5	List of Contributors	7
2	Signature Policies	9
3	Quality of eIDs	10
3.1	Two Parameters for eID Quality Profile	10
3.2	Certificate Quality Parameter (Claimed Quality)	10
3.3	Independent Assurance Parameter	12
3.4	Assessment of non-European Certificates	13
4	EU's Trusted List System	14
5	Cryptographic Quality	16
6	Signature Quality	17
6.1	Aggregated Quality	17
6.2	Examples	17
6.2.1	Example 1: Qualified Certificate and SSCD, Accredited CA	17
6.2.2	Example 2: Qualified Certificate, Accredited CA	17
6.2.3	Example 3: Qualified Certificate, Supervised CA	18
6.2.4	Example 4: NCP Certificate and SSCD, Certified CA	18
6.2.5	Example 5: NCP Certificate, External Compliance Report for CA	18
6.2.6	Example 6: LCP Certificate, Internal Compliance Report for CA	18
6.2.7	Example 7: Certificate from CA cross certified with US FBCA, medium Assurance Level ..	19
6.2.8	Example 8: Self issued Certificate with no documented Policy	19
7	Other Issues	20
7.1	Quality of the Actor Issuing an eID	20
7.2	Classification over Time	20
7.3	Who Shall Perform Quality Classification?	20
8	References	21
9	Appendix 1: FBCA Requirements Mapped to the PEPPOL Profile	23
10	Appendix 2: XML structure	25

1 Summary and Structure of Document

1.1 Scope and Structure of Deliverable D1.3

This document is a part of the multi-part deliverable D1.3 “Functional Specifications for Cross-Border Use of eSignatures in Public Procurement” issued by the PEPPOL¹ (Pan-European Public Procurement On-Line) project. PEPPOL is a 4-year (May 2008 – end April 2012²) large scale pilot under the CIP (Competitiveness and Innovation Programme) initiative of the European Commission. D1.3 is an updated version of the deliverable D1.1 “Requirements for Use of Signatures in the Procurement Processes” [PEPPOL-D1.1].

D1.3 consists of the following documents:

Part 1: Background and Scope

(Part 2: Not included – was the D1.1 part on E-tendering Pilot Specifications)

Part 3: Signature Policies

Part 4: Architecture and Trust Models

Part 5: XKMS v2 Interface Specification

Part 6: OASIS DSS Interface Specification

Part 7: eID and eSignature Quality Classification

The D1.3 deliverable is the second version of **functional specifications** for cross-border interoperability of e-signatures in Europe. The specifications are specifically targeted at cross-border public procurement, the topic of PEPPOL. However, a successful solution should be applicable also to other application areas in need of e-signature interoperability.

Signature interoperability in PEPPOL focuses on verification of e-signatures and their associated eIDs. Interoperability of signing solutions is not handled as it is assumed that all actors are capable of signing documents within their corporate infrastructure.

The specifications in deliverable D1.1 has guided the implementation and testing of e-signature interoperability solutions in PEPPOL. In the course of this work, the specifications have by necessity evolved, leading to the revised version published in this deliverable D1.3. These are the specifications for the solutions used for the e-signature interoperability pilots in PEPPOL [PEPPOL-D1.2] in the period 1st November 2010 to 30th April 2012.

The specifications are publicly available and comments from any interested party are most welcome. Note that further evaluation of the specifications of D1.3 is expected as a result of further work in PEPPOL and any party using or referring to the specifications must ensure that the latest version is used; contact the PEPPOL project for information.

1.2 Demonstrator Software Components and Documentation

In addition to the specifications in this deliverable D1.3, PEPPOL WP1 provides software components for cross-border validation of e-signatures:

¹ <http://www.peppol.eu>

² Originally, PEPPOL was scheduled for 3 years. The project has been prolonged twice, both times by 6 months.

PEPPOL D1.3 Part 7: eID and eSignature Quality Classification

- PEPPOL XKMS responder component (server side component) according to the specifications of D1.3 part 5 is provided as open source. The software component, source code and documentation are available on Joinup³,
- A free to use client side component for signature validation, available as a standalone version and a version for integration into other software applications.
- Open source software components for own development (XKMS requester, Report Agent, Verify Agent, Hashing API, System Configuration API)

The software components are used for PEPPOL's pilot demonstrators on e-signature interoperability as described in PEPPOL Deliverable D1.2 [PEPPOL-D1.2]. Attachments A and B to D1.2 provide documentation on respectively the XKMS responder and the validation client, other documentation is published along with the software.

1.3 Scope and Structure of this Document

The purpose of this document is to specify quality profiles for eID certificates (PKI based) and advanced (digital) electronic signatures. These profiles can be referred to in order to specify non-discriminatory acceptance (quality) criteria for use of signature in public e-procurement processes across borders in Europe; as well as for any other use of signatures..

The action plan of the EU Commission [COMM-01] targets firstly a “quick win” from the defined levels “qualified signature” and “advanced signature with qualified eID”. However, in the longer run a more elaborate quality system is needed since:

- An advanced signature, even using a qualified eID, may have varying quality properties;
- The qualified term is European only (although the concept seems to have some support in Asia), and for international interoperability this term alone is not sufficient;
- Non-qualified eIDs should be considered even when interoperability is limited to Europe, e.g. corporate PKIs of reasonable quality and non-qualified, public eIDs;
- Even qualified signatures may differ in quality, although it may be discussed to what extent qualified signatures may be refused on such grounds.

The signature quality profile is described in the context of a set of signature policies as described in Chapter 2. The PEPPOL profiles for eID quality and cryptographic quality are presented in Chapter 3 and 5, respectively. Together, these profiles will constitute a signature quality profile as described in Chapter 6. Chapter 4 outlines EU's system of Trusted Lists (TL) for issuers of qualified eIDs and implications to quality classification. Requirements to actors issuing eIDs, other than those that follow from requirements to certificate policies, are considered out of scope for PEPPOL, but are briefly discussed in Chapter 7. In Appendix 1 a mapping from the assurance levels of the US Federal Bridge Certification Authority (FBCA) to the PEPPOL eID quality profile is suggested. The PEPPOL XML structure for eID and signature quality is given in Appendix 2.

1.4 Evolution of this Document and Changes from D1.1

Note: This document, like the other parts of D1.3, continues the version numbers deriving from D1.1.

This document provides the PEPPOL quality classification system. Changes from the version presented in D1.1 are minimal:

³ Open source software, semantic assets and other interoperability solutions for public administrations, <https://joinup.ec.europa.eu/>.

PEPPOL D1.3 Part 7: eID and eSignature Quality Classification

- For eID quality level 4, D1.1 had a requirement for certified SSCD with NCP+ policy. This is now changed into a general requirement for hardware storage (which may or may not be a SSCD) of private keys. It is noted that quality level 4 could be split into two levels: NCP+ with hardware and NCP+ with SSCD.
- The section on TL (Trusted List) is expanded.
- Chapter 5 on cryptographic quality now refers to ETSI recommendations and has some other updates.
- Chapter 7 on other issues is slightly expanded.
- There are some other minor updates.

The following remarks from D1.1 part 3 are still valid:

- A quality classification system should be standardised. Since referral is made to ETSI standards, ETSI may be the most suitable standards body, although this needs consideration, and a global standards organisation may be more appropriate. PEPPOL will consider submission and follow up through a standards body; a standards process will necessarily lead to changes in the specifications.
- PEPPOL quality classification may also be incorporated in trust status lists such as described in D1.3 part 4 and chapter 4 of this document. This will better enable inclusion of non-qualified eIDs in such lists.

1.5 List of Contributors

The following organisations, in alphabetical order, have contributed to Deliverable D1.3:

- **ADETEF, France** <http://www.adetef.fr>
- **ANSSI, French Network and Information Security Agency, France** <http://www.ssi.gouv.fr>
- **bos, bremen online services, Germany,** <http://www.bos-bremen.de>
- **Difi, Agency for Public Management and eGovernment, Norway** <http://www.difi.no>
- **DILA, Direction de l'Administration Légale et Administrative Of French Prime Minister Office, France** <http://www.dila.premier-ministre.gouv.fr>
- **Esteral Consulting, France** <http://www.esteralconsulting.com>
- **InfoCamere, Italy** <http://www.infocamere.it>
- **InfoCert, Italy** <http://www.infocert.it>
- **Lex Persona, France** <http://www.lex-persona.com>
- **University of Piraeus, Greece** <http://www.unipi.gr>

The following persons (alphabetical ordering for each participating organisation) have contributed to the D1.3 work:

Jörg Apitzsch	bos	Piero Milani	InfoCamere	Alain Ducass	ADETEF
Nils Büngener	bos	Luca Boldrin	InfoCert	Ahmed Yacine	DILA
Mark Horstmann	bos	Daniele Mongiello	InfoCert	François Devoret	Lex Persona
Ralf Lindemann	bos	Lefteris Leontaridis	Univ. Piraeus	Julien Pasquier	Lex Persona

PEPPOL D1.3 Part 7: eID and eSignature Quality Classification

Dr Jan Pelz	bos	Dr Andriana Prentza	Univ. Piraeus	Sébastien Herniote	ANSSI
Lars Thölken	bos	Alain Esterle	Esteral Cons.	Jon Ølnes (editor)	Difi

D1.3 is a revised version of D1.1. The D1.3 team acknowledges the contributions of organisations and persons that helped producing D1.1 but are no longer active in PEPPOL's e-signature work. These are not listed above; please refer to D1.1 for the names.

2 Signature Policies

A signature policy⁴ defines a set of rules for the creation and validation of electronic signatures, under which a signature can be determined to be valid (signature acceptance). A signature policy may specify at which stages of a (business) protocol signatures shall/should/may/shall not be used, which protocol elements (e.g. documents) to sign, and the signature validation policy to apply to signatures. A signature policy according to ETSI must always be stated in a humanly readable form and parts of the policy may also be described in a form suitable for automated processing.

A signature validation policy defines quality requirements (cryptography, certificate policy etc.) and procedural rules (e.g. for path processing). Additionally, the policy may set requirements for the signature format⁵ to be used and information to be included in the SDO (signed data object), such as time-stamps, certificate information, revocation information and policy identifiers.

With respect to signature validation policies for public procurement, in 2007 IDABC [IDABC01] found 15 countries with public e-procurement tendering services in operation, where 6 required qualified signatures, 7 required advanced signatures (sometimes with the additional requirement of a qualified eID), while two countries required only authentication ("simple" e-signature). The services furthermore either listed one or a few eID issuers or were able to accept all domestic issuers and perhaps a few foreign issuers. The main change to this situation since 2007 is that more countries have established operational procurement services.

Part 3 of PEPPOL's D1.3 describes signature policies in full context. This document specifically addresses three aspects of a signature policy:

- eID quality, as derived from certificate policy and possibly other information sources;
- eID assurance level and supervision status (e.g. accredited or supervised issuer of qualified eID);
- Cryptographic quality of signature, hash and public key algorithm and key length.

This document contains a human readable representation of the requirements for assignment to quality and assurance level classes, as a framework to define these parts of signature policies accordingly. This document also includes specification (Appendix 2) of how to implement this in a processable way in order to convey requirements over validation interfaces (e.g. XKMS v2 or OASIS DSS interfaces as described by parts 5 and 6 of PEPPOL D1.3) and process assessments made by validation services. Definitions of enumerations for the values of quality parameters are outlined in D1.3 part 5 (XKMS).

The framework specified in this document is explicitly targeted at incorporating non-European eIDs, even though Europe is in focus for the PEPPOL project. Appendix 1 presents a case study on mapping of US Federal Bridge levels to the classification framework.

Based on the classification framework, non-discriminatory rules for acceptance of eIDs and e-signatures can be defined in signature policies, to replace present policies for national solutions, which refer to domestic issuers or national accreditation schemes.

To determine if an eID fulfils quality requirements, the issuer and its policy must be assessed towards the corresponding quality profile. The assessment method is targeted at easy assessment of issuers of qualified eIDs, while assessment of issuers of non-qualified eIDs may require some more effort.

⁴ Defined in ETSI TS 101 733 Annex C, see also ETSI TR 102 038, ETSI TR 102 272, ETSI TR 102 045.

⁵ Examples are XAdES (ETSI TS 101 903), CAdES (ETSI TS 101 733), PAdES (ETSI TS 102 778), PKCS#7 (RFC2315), CMS (RFC5652), XML DSIG (RFC3275), and PDF signatures.

3 Quality of eIDs

3.1 Two Parameters for eID Quality Profile

The starting point for PEPPOL's quality classification framework is the scheme developed by DNV [Olnes]. The main change from the DNV system is the separation of eID quality into two parameters:

- one parameter for the certificate quality level as claimed by the Certification Authority through its Certificate Policy and Certificate Practice Statement, and
- one parameter for the level of independent assurance that can be associated with the claimed quality level.

In this profile, eID quality is represented by a pair of numbers (x,y) where x is the certificate quality level (0-6; see 3.2) and y is the independent assurance level (0-7; see 3.3) as defined below.

The parameter for (claimed) eID quality is primarily based on certificate policy levels as defined by the ETSI standards [ETSI01] and [ETSI02].

Note that the CROBIES project has proposed a classification system [CROBIES5.2] similar to but slightly different from the one presented below. An alternative to PEPPOL was to change to the CROBIES scheme; however a decision has been taken to keep the system originally proposed in D1.1 part 7 and preferably leave definition of the final classification system to an appropriate standards body such as ETSI.

3.2 Certificate Quality Parameter (Claimed Quality)

0. Very low or non-determined level: Very low confidence or assessment not possible, usually because a certificate policy does not exist.

1. Low level: Low confidence in certificate but certificate policy exists or quality assessment is possible by other means.

2. Medium level: Certificates governed by a Certificate Policy in compliance with the ETSI TS 102 042 standard for LCP or a similar standard.

3. High level: Certificates governed by a Certificate Policy in compliance with the ETSI TS 102 042 standard for NCP or a similar standard.

4. High level +: Certificates governed by a Certificate Policy in compliance with the ETSI TS 102 042 standard for NCP+ or a similar standard.

5. Very high level: Certificates governed by a Certificate Policy in compliance with the ETSI TS 101 456 standard for QCP or a similar standard.

6. Very high level +: Certificates governed by a Certificate Policy in compliance with the ETSI TS 101 456 standard for QCP+ or a similar standard. (Use of a SSCD is mandated in the CP. Thus, this level supports qualified signatures according to the EU Directive on electronic signatures.)

Note:

LCP = Lightweight Certificate Policy

NCP = Normalised Certificate Policy

QCP = Qualified Certificate Policy

SSCD = Secure Signature Creation Device

PEPPOL D1.3 Part 7: eID and eSignature Quality Classification

The ETSI standard TS 101 456 [ETSI01] sets policy requirements to CAs issuing qualified certificates in accordance with the European e-signatures Directive [EC01]; this is the reference certificate policy QCP in the classification above. Annex I of this Directive specifies requirements for qualified certificates, and Annex II specifies requirements to CAs issuing qualified certificates. Additional requirements to use the qualified certificate with a secure signature creation device, as required by Annex III of the Directive, give the reference policy QCP+.

The ETSI standard TS 102 042 [ETSI02] sets policy requirements to CAs issuing certificates at the same quality level as that of qualified certificates, but without the legal constraints implied by the e-signature Directive and without requiring use of a hardware component for storage of private keys; this is the reference certificate policy NCP. Additional requirements to use the certificate with use of a hardware component (which might be an SSDD) give the reference policy NCP+.

Note: Level 4 (High level +, NCP+ policy) requires use of a hardware component for storage of private keys. This level could be separated into two levels: “NCP+” with a general hardware requirement and “NCP++” with an additional requirement on use of SSDD.

The reference certificate policy LCP incorporates less demanding requirements as specified in TS 102 042 [ETSI02].

The assessment of certificate quality in accordance with the classification defined above can be illustrated as in Figure 1 below.

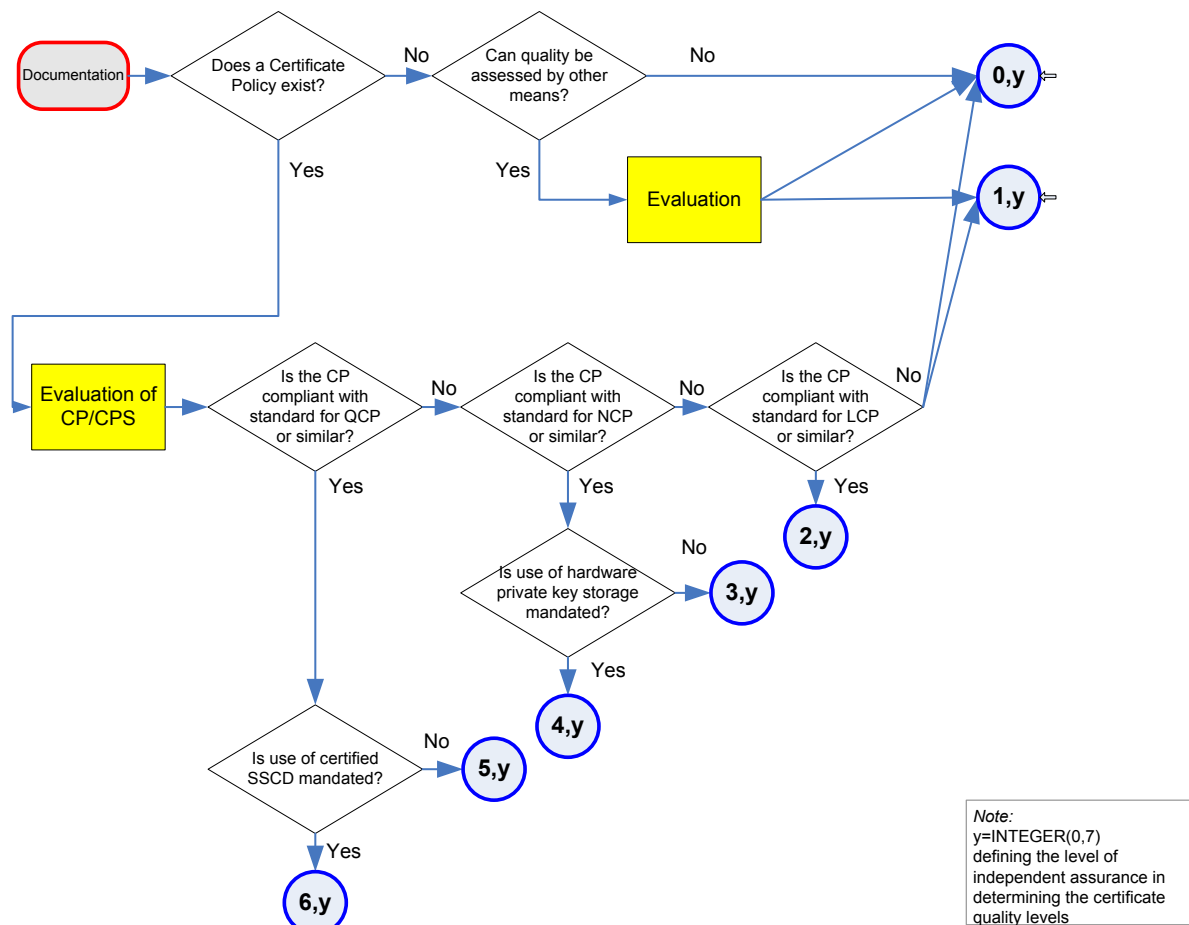


Figure 1 Assessment of certificate quality level

Note that information from the EU's Trusted List system (TL, see chapter 4) should be sufficient to assess that a certificate issuer is at quality level 5 or 6.

3.3 Independent Assurance Parameter

0. No independent assurance: self assessment only.

1. Independent document review: Statement of compliance issued by an independent, external unit based on document review only.

2. Internal compliance audit: Internal audit carried out periodically concludes compliance to applicable requirements.

3. Supervision without compliance audit: CA is supervised by a public, national or international authority according to applicable law to the CA.

4. External compliance audit: Audit carried out periodically by external, independent auditor concludes compliance to applicable requirements.

5. External compliance audit and certification: Audit carried out periodically by external, independent auditor concludes compliance to applicable requirements. CA operations are certified in accordance with a relevant standard; OR cross certification with a relevant bridge CA has been made; OR the CA has obtained membership in a PKI hierarchy as a result of appropriate assessment.

Note: Relevant standards include ETSI TS 101 456, ETSI TS 102 042, WebTrust Program for CAs, tScheme Approval Profile for CAs, ISO9001, and ISO27001.

6. Supervision with external compliance audit: Audit carried out periodically by external, independent auditor concludes compliance to applicable requirements. CA is supervised by a public, national or international authority according to applicable law to the CA.

7. Accreditation with external compliance audit: Audit carried out periodically by external, independent auditor concludes compliance to applicable requirements. CA is accredited by a public, national or international authority according to applicable law to the CA.

Note: Supervision and/or accreditation by a public, international authority (levels 3, 6 and 7) is not relevant at present, but will become relevant in the future if international schemes for such supervision/accreditation are established, e.g. by the EU Commission.

Supervision and accreditation are the two models described for issuers of qualified certificates according to the e-signature Directive. In the supervision model, an issuer declares conformance to requirements in order to be listed as issuer of QC and accepts (later) inspections from the authority. In the accreditation model, the authority must assess conformance before listing the issuer.

Discrimination between the two models supervision and accreditation for qualified certificates shall not take place; both shall be accepted as qualified. However, for other certificates (non-European but regarded as equivalent to QC) the distinction may be relevant.

Note that information from the EU's Trusted List system (TL, see chapter 4) should be sufficient to assess that a certificate issuer is at assurance level 6 or 7.

The assessment of independent assurance in accordance with this classification can be illustrated as in Figure 2.

PEPPOL D1.3 Part 7: eID and eSignature Quality Classification

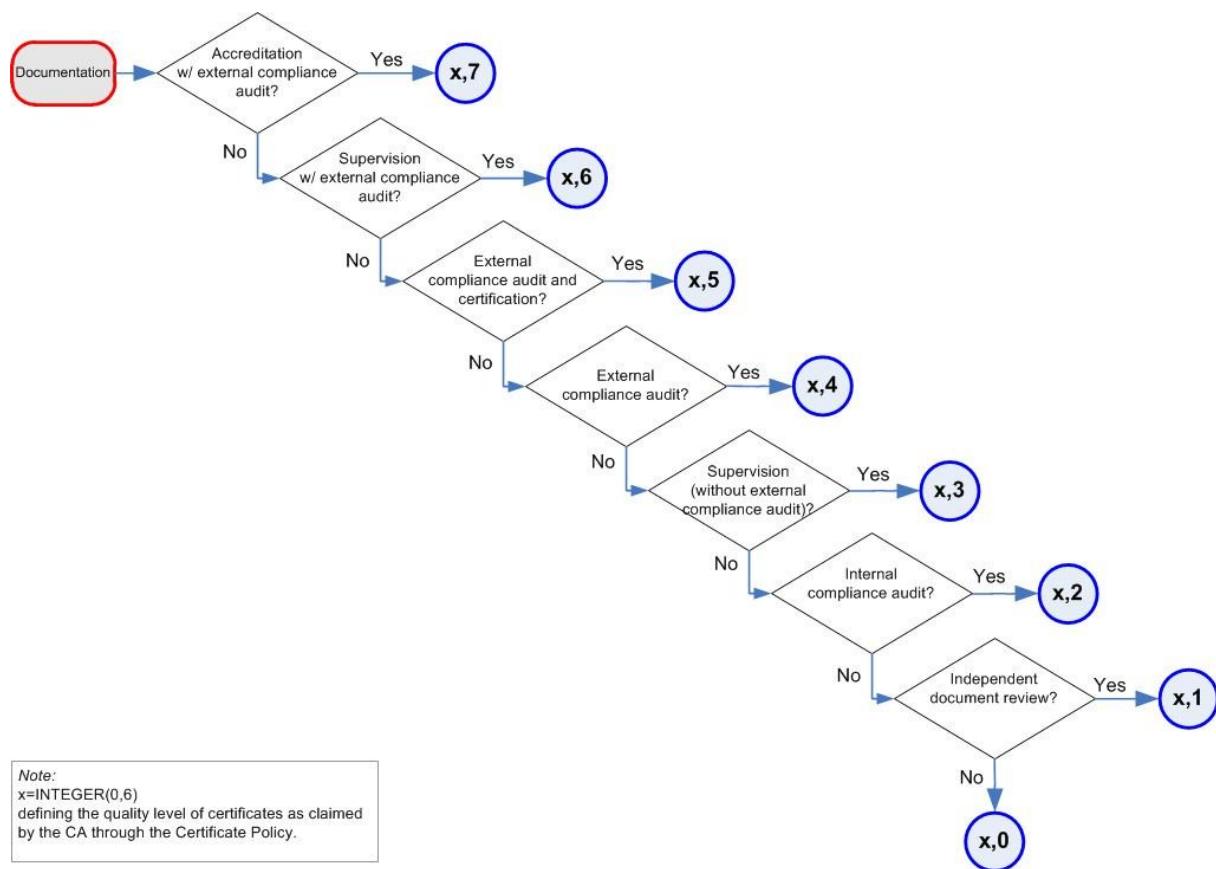


Figure 2 Assessment of independent assurance level

3.4 Assessment of non-European Certificates

The assessment criteria for certificate quality and independent assurance levels defined in 3.2 and 3.3 can be applied to non-European certificates as well, even if the term “qualified certificate” is not defined outside of Europe.

If the certificate policy of such a certificate does not make any claims as to compliance with one of the (European) ETSI standards (TS 102 042 for LCP/NCP/NCP+ or TS 101 456 for QCP/QCP+) or any other standard judged to be similar, the assessment of (claimed) certificate quality can be made by evaluation of the certificate policy through document review.

A case of particular interest is that of CAs that have been cross certified to one of the US Federal Bridge Certification Authority (FBCA) certificate policies [FBCA01]. A mapping between the quality levels (termed “assurance levels”) of FBCA and the PEPPOL quality profile is shown in Appendix 1.

Similar mappings should be made for quality levels defined in other parts of the world, notably Asia.

4 EU's Trusted List System

An immediate and prioritised action point in [COMM-01] is establishment of a pan-European system of Trusted Lists (TLs) covering qualified CAs. The format of the lists is according to [ETSI03]. Both human readable (PDF) and machine processable (XML) lists shall be issued. Status is as follows:

- The EU has established top level lists that include only pointers to the national TLs: Human readable⁶ and machine processable⁷.
- All EU/EEA countries will establish national lists. Lists are issued (and will eventually be signed) by the national authorities responsible for accreditation or supervision of issuers of qualified certificates.
- Only issuers of qualified certificates are covered. There have been initiatives at extending coverage to non-qualified CAs but apparently no country has this in scope at present. The [ETSI03] standard makes some provisions for inclusion of certain other trusted roles as well as for issuers of non-qualified certificates.

Annex L of [ETSI03] defines status codes for types of services, from which quality parameters can be derived and mapped to (in the current status of the TL system) to levels 5 or 6 as defined in section 3.2. In particular, the statuses "QCWithSSCD" and "QCNoSSCD" map directly to level 6 and 5 respectively. For some other status codes, further examination is necessary to determine the quality level, e.g. where only root-CAs are listed in the TL and not individual CAs.

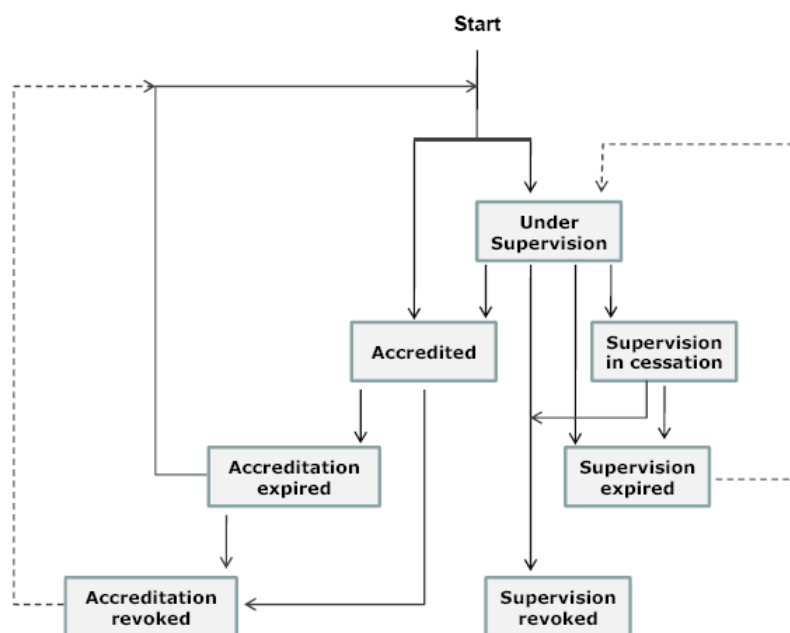


Figure 3 Expected supervision/accreditation status flow ([CROBIES2.1])

Concerning supervision/accreditation status, a status flow can be depicted as illustrated in Figure 3 (taken from [CROBIES2.1]) potentially adding states to the assurance parameters described in section 3.3. In order to not complicate the assurance parameters further, the additional states are not

⁶ https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf

⁷ https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

PEPPOL D1.3 Part 7: eID and eSignature Quality Classification

considered. These states may serve as “flags” to indicate a need to follow up quality classification of a particular issuer.

The “under supervision” and “accredited” states map to levels 6 and 7 respectively as described in section 3.3. Other states must be evaluated according to other levels in the scheme of section 3.3 depending on the available information about the certificate issuer.

Where certificate issuers are directly included in a TL, the status can be easily extracted. In other cases, e.g. when only root-CAs are listed, the accreditation/supervision status of each individual issuer cannot be obtained directly from the TL.

Note that the XKMS interface defined by D1.3 part 5 allows two different quality and status information types to be returned:

- Status taken from the appropriate TL when relevant, and/or
- Status according to the classification scheme defined in this document.

As stated, both alternatives may be returned for a qualified certificate.

5 Cryptographic Quality

The parameters of concern here are hash algorithm quality for the signed document and quality of the combination public key algorithm and key length for the user's key pair. Note that the hash algorithm is selected through the signing software and is not influenced by the eID used.

Public key algorithm and key length could be considered part of eID quality. A reason for separating this out is that even if one just looks at the qualified status, one may still be interested in the quality of the cryptography. E.g. Germany disapproves SHA-1 and RSA with keys shorter than 2048, while SHA-1 and RSA-1024 are still (end of 2010) in widespread use in other countries even for qualified signatures.

One could consider including parameters describing also the quality of the hash algorithm used by the CA to sign the eID certificate and the public key algorithm and key length for the CA's own certificate signing keys. Instead, it is assumed that CAs are subject to requirements for cryptographic strength and that fulfilling these requirements is part of eID quality. Note that at the time of writing (end of 2010) many CAs still use SHA-1 to sign certificates.

Based on ETSI recommendations [ETSI04] that are also aligned with US recommendations [NIST01], a quality classification is defined as follows:

Quality 0: Inadequate – should not be trusted.

Quality 1: Reasonably secure for 3 years.

Quality 2: Regarded as trustworthy for 5-10 years.

Quality 3-5: Increasing levels of security.

There are miscellaneous studies and recommendations on the strength of different algorithms. See <http://www.keylength.com> for comparison of different approaches. All studies and recommendations assume no inherent (undetected) weakness in the algorithms and no implementation flaws.

As examples of hash algorithms: MD5 = 0, SHA-1 = 1, SHA-224/256/384/512 = 2/3/4/5.

Examples of public key algorithms with key lengths: RSA-1024 = 1; RSA-2048 = 2; RSA-4096 = 4.

An option for representation of quality policies for cryptographic algorithms can be found in [RFC5698].

6 Signature Quality

6.1 Aggregated Quality

Excluding implementation issues of signing software and hardware, the quality of a signature consists of the three parameters: eID quality (in the scheme described in this document consisting of the two parameters quality and assurance level), hash quality, public key quality. Each of these parameters should be above a certain level for the signature to be accepted; this should be defined in the signature policy. The signature policy should normally not refer to specific algorithms, only to quality parameters.

The PEPPOL profile for digital signatures is then defined by the following parameters:

- **eID quality**, consisting of a certificate quality parameter ranging from 0 to 6 (ref. section 3.2) and an independent assurance parameter ranging from 0 to 7 (ref. section 3.3)
- **Hash quality**, ranging from 0 to 5 (ref. chapter 5)
- **Public key quality**, ranging from 0 to 5 (ref. chapter 5)

A notation for the signature quality is suggested as follows

$$\begin{aligned} \text{Signature quality} &= \{\text{eID quality, hash quality, public key quality}\} \\ &= \{(\text{certificate quality, independent assurance}), \text{hash quality, public key quality}\} \end{aligned}$$

6.2 Examples

6.2.1 Example 1: Qualified Certificate and SSCD, Accredited CA

A qualified electronic signature created with an SSCD and a qualified certificate issued by an accredited CA and using the SHA-224 hash algorithm and a cryptographic key length of 2048, would have signature quality parameters as follows:

- **eID quality:** (6,7) – meaning certificate quality level 6 and independent assurance level 7
- **Hash quality:** 2 – regarded as trustworthy for 5-10 years
- **Public key quality:** 2 – regarded as trustworthy for 5-10 years

With the notation suggested above, this signature example would have a signature quality:

$$\text{signature quality} = \{(6,7), 2, 2\}$$

6.2.2 Example 2: Qualified Certificate, Accredited CA

An advanced electronic signature created with a qualified certificate issued by an accredited CA and using the SHA-224 hash algorithm and a cryptographic key length of 2048, would have signature quality parameters as follows:

- **eID quality:** (5,7) – meaning certificate quality level 5 and independent assurance level 7
- **Hash quality:** 2 – regarded as trustworthy for 5-10 years
- **Public key quality:** 2 – regarded as trustworthy for 5-10 years

With the notation suggested above, this signature example would have a signature quality:



signature quality = $\{(5,7),2,2\}$

6.2.3 Example 3: Qualified Certificate, Supervised CA

An advanced electronic signature, created with a qualified certificate issued by a CA under supervision by a national authority and with external compliance audit, using the SHA-224 hash algorithm and a cryptographic key length of 2048, would have signature quality parameters as follows:

- **eID quality:** (5,6) – meaning certificate quality level 5 and independent assurance level 6
- **Hash quality:** 2 – regarded as trustworthy for 5-10 years
- **Public key quality:** 2 – regarded as trustworthy for 5-10 years

With the notation suggested above, this signature example would have a signature quality:

signature quality = $\{(5,6),2,2\}$

6.2.4 Example 4: NCP Certificate and SSCD, Certified CA

An advanced electronic signature, created with an SSCD and a certificate issued by a CA under a policy compliant with ETSI TS 102 042 for NCP+ as documented by an ETSI TS 102 042 certification, using the SHA-224 hash algorithm and a cryptographic key length of 2048, would have signature quality parameters as follows:

- **eID quality:** (4,5) – meaning certificate quality level 4 and independent assurance level 5
- **Hash quality:** 2 – regarded as trustworthy for 5-10 years
- **Public key quality:** 2 – regarded as trustworthy for 5-10 years

With the notation suggested above, this signature example would have a signature quality:

signature quality = $\{(4,5),2,2\}$

6.2.5 Example 5: NCP Certificate, External Compliance Report for CA

An advanced electronic signature, created with a certificate issued by a CA under a policy compliant with ETSI TS 102 042 for NCP as documented by an external compliance audit report, using the SHA-1 hash algorithm and a cryptographic key length of 1024, would have signature quality parameters as follows:

- **eID quality:** (3,4) – meaning certificate quality level 3 and independent assurance level 4
- **Hash quality:** 1 – regarded as reasonably secure for 3 years
- **Public key quality:** 1 – regarded as reasonably secure for 3 years

With the notation suggested above, this signature example would have a signature quality:

signature quality = $\{(3,4),1,1\}$

6.2.6 Example 6: LCP Certificate, Internal Compliance Report for CA

An advanced electronic signature, created with a certificate issued by a CA under a policy compliant with ETSI TS 102 042 for LCP as documented by an internal compliance audit report, using the SHA-1 hash algorithm and a cryptographic key length of 1024, would have signature quality parameters as follows:

- **eID quality:** (2,2) – meaning certificate quality level 23 and independent assurance level 2
- **Hash quality:** 1 – regarded as reasonably secure for 3 years

PEPPOL D1.3 Part 7: eID and eSignature Quality Classification

- **Public key quality:** 1 – regarded as reasonably secure for 3 years

With the notation suggested above, this signature example would have a signature quality:

signature quality = $\{(2,2)1,1\}$

6.2.7 Example 7: Certificate from CA cross certified with US FBCA, medium Assurance Level

An advanced electronic signature, created with a certificate issued by a CA which has been cross certified with the US Federal Bridge CA at the Medium assurance level, using the SHA-1 hash algorithm and a cryptographic key length of 1024, would have signature quality parameters as follows (ref. Appendix 1):

- **eID quality:** (3,5) – meaning certificate quality level 3 and independent assurance level 5
- **Hash quality:** 1 – regarded as reasonably secure for 3years
- **Public key quality:** 1 – regarded as reasonably secure for 3 years

With the notation suggested above, this signature example would have a signature quality:

signature quality = $\{(3,5)1,1\}$

6.2.8 Example 8: Self issued Certificate with no documented Policy

An advanced electronic signature, created with a certificate issued by a person or organisation without any documented certificate policy and independent assurance, using the SHA-1 hash algorithm and a cryptographic key length of 1024, would have signature quality parameters as follows:

- **eID quality:** (0,0) – meaning certificate quality level 0 and independent assurance level 0
- **Hash quality:** 1 – regarded as reasonably secure for 3years
- **Public key quality:** 1 – regarded as reasonably secure for 3 years

With the notation suggested above, this signature example would have a signature quality:

signature quality = $\{(0,0)1,1\}$

7 Other Issues

7.1 Quality of the Actor Issuing an eID

If desired, quality requirements may be imposed on the actor in charge of a CA, such as:

- Financial strength (will it survive and can it face liability claims),
- Insurance coverage,
- Owners and organisational structure (may include judgements about independence with respect to third party roles),
- Market penetration (number of eIDs and their usage frequency),
- Company reputation,
- Competence and knowledge,
- Infrastructure.

Such requirements are considered out of scope of PEPPOL.

A validation service could however offer such information in the response to a validation request as additional/auxiliary information.

7.2 Classification over Time

Cryptographic quality is reduced over time, a CA may change its service offering, or its supervision status may change. Thus, although frequent changes are not envisaged, quality is not static. When assessing the quality of an old signature, one essentially has two options:

- Assess quality rating at time of signing (or time of initial verification, see D1.3 part 3): was the signature acceptable at that time?
- Assess present quality rating: to what degree is the signature still secure and acceptable?

The choice of option is a policy decision. Note that the first option depends on storing either enough old status information on classification ratings separately or securely add the quality rating as metadata in or associated with the signed data object. In EU's TL system (see chapter 4), historical information will be kept in the TLs for CAs that have terminated their business or otherwise changed approval status.

7.3 Who Shall Perform Quality Classification?

Where relevant, information from TLs should guide the quality rating; i.e. an actor should adhere to the information in the relevant TL unless there is strong reason to believe that the information is misleading.

For CAs that are not included in any TL, other references may be sought, such as FBCA cross-certification or similar certifications and accreditations. Determining values for the rating can be done by a validation service provider or by some independent certification body; the latter is preferred. There is a possibility that different ratings will be reported from different validation services for the same eID, notably for independent assurance level for CAs without accreditations/supervision/certification. However, for cryptographic quality and the QCP levels, this should not be a problem.

8 References

- [COMM-01] Commission of the European Communities, Action-Plan on e-Signatures and e-Identification to Facilitate the Provision of Cross-Border Public Services in the Single Market, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, November 2008, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF>
- [CROBIES2.1] Sealed, time.lex, Siemens: Study on Cross-Border Interoperability of eSignatures (CROBIES), Trusted Lists Implementer's Guide. CROBIES deliverable 2.1, July 2010, http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd2.1.pdf
- [CROBIES5.2] Sealed, time.lex, Siemens: Study on Cross-Border Interoperability of eSignatures (CROBIES), Quality Classification Scheme for eSignature Elements. CROBIES deliverable 5.2, July 2010, http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd5.2.pdf
- [EC01] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- [ETSI01] ETSI: Electronic Signatures and Infrastructures (ESI); Policy Requirements for Certification Authorities issuing Qualified Certificates. ETSI TS 101 456 v1.4.1, 2006.
- [ETSI02] ETSI: Electronic Signatures and Infrastructures (ESI); Policy Requirements for Certification Authorities issuing Public Key Certificates. ETSI TS 102 042 v1.2.2, 2005.
- [ETSI03] ETSI: Electronic Signatures and Infrastructures (ESI); Provision of Harmonised Trust Service Provider Information. ETSI TS 102 231 v3.1.2, 2009.
- [ETSI04] ETSI: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms. ETSI TS 102 176-1 v2.0.0, 2007.
- [FBCA01] FBCA: X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), September 10, 2002, http://www.cio.gov/fkipa/documents/fbca_cp_09-10-02.pdf
- [IDABC01] Siemens, Time.lex: Preliminary Study on Mutual Recognition of eSignatures for eGovernment Applications (Final Study and 29 Country Profiles). IDABC, 2007.
- [NIST01] B. Burr: NIST Cryptographic Standards Status Report. April 2006, http://middleware.internet2.edu/pki06/proceedings/burr-nist_crypto_standards.ppt
- [Olnes] Ølnes, Jon et al.: Making Digital Signatures Work across National Borders. Paper published in Pohlmann, Reimer, Schneider: ISSE/Secure 2007, Securing Electronic Business Processes, pp. 287-296, October 2007, ISBN 978-3-8348-0346-7.
- [PEPPOL-D1.1] PEPPOL project: Requirements for Use of Signatures in Public Procurement Processes. PEPPOL Deliverable D1.1, April 2009, http://www.peppol.eu/work_in_progress/wp-1-esignature/results/deliverable-1.1/first-deliverable-of-wp1-has-been-released

PEPPOL D1.3 Part 7: eID and eSignature Quality Classification





- [PEPPOL-D1.2] PEPPOL project: Trans-national Verification Solution(s) – Prototype Documentation.
PEPPOL Deliverable D1.2, April 2010, http://www.peppol.eu/work_in_progress/wp-1-esignature/results/deliverable-1.2/d1.2-trans-national-verification-solution-s-prototype-documentation
- [RFC5698] T. Kunz, S. Okunick, U. Pordesch: Data Structure for the Security Suitability of Cryptographic Algorithms. RFC5698, November 2009, <http://tools.ietf.org/html/rfc5698>

9 Appendix 1: FBCA Requirements Mapped to the PEPPOL Profile

Table 1 below shows FBCA requirements for different quality levels (termed “assurance levels” by FBCA). A mapping to the PEPPOL eID quality profile defined in this document (chapter 3) is suggested.

Requirement/Level	Rudimentary	Basic	Medium	High
3.1.9 Authentication of individual identity	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address	Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or comparison with trusted information in a data base of user-supplied information (obtained and/or checked electronically, through other trusted means (such as the U.S. mail), or in-person); or by attestation of a supervisor, or administrative or information security officer, or a person certified by a state or Federal Entity as being authorized to confirm identities.	Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)	Identity established by in-person appearance before the Registration Authority or Trusted Agent; information provided shall be checked to ensure legitimacy Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)
4.4.3 CRLs - CRL issuance frequency (Routine & loss or compromise of private key)	NA & NA	Entity determined & within 24 hours notification	At least once each day & within 18 hours notification	At least once each day and within 6 hours notification
5.2.2 Separation of roles	No stipulation.	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, individuals who assume an Officer role may not assume an	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role.

PEPPOL D1.3 Part 7: eID and eSignature Quality Classification

		individual shall be assigned more than one identity.	Administrator or Auditor role. The CA system shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, or an Auditor and an Officer role. No individual shall be assigned more than one identity.	The CA system shall identify and authenticate its users and shall ensure that no user identity can: * Assume both the Administrator and Officer roles * Assume both the Administrator and Auditor roles * Assume both the Auditor and Officer roles. No individual shall have more than one identity.
6.1.8 Hardware/Software subscriber key generation	Software or Hardware	Software or Hardware	Software or Hardware	Hardware only
6.2.1 Standards for cryptographic module	FIPS PUB 140	FIPS PUB 140	FIPS PUB 140	FIPS PUB 140
a) for CA	Level 1 (hw or sw)	Level 2 (hw or sw)	Level 2 (hw)	Level 3 (hw)
b) for subscriber	NA	Level 1 (hw or sw)	Level 1 (hw or sw)	Level 2 (hw)
c) for RA	Level 1 (hw or sw)	Level 1 (hw or sw)	Level 2 (hw)	Level 2 (hw)
Corresponding to PEPPOL eID quality profile (ref 3.2):				
x: certificate quality level	1	2	3	4
y: independent assurance level	5	5	5	5

10 Appendix 2: XML structure

The PEPPOL XML structure for eID and signature quality is shown in the following.

```
<xs:element name="QualityLevelRequirements" type="QualityLevelType"/>
<xs:element name="QualityLevel" type="QualityLevelType"/>
<xs:complexType name="QualityLevelType">
  <xs:sequence>
    <xs:element name="CertificateQuality" type="xs:string"/>
    <xs:element name="IndependentAssurance" type="xs:string"/>
    <xs:element name="HashAlgQuality" type="xs:string"/>
    <xs:element name="PublicKeyAlgQuality" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
```

