PEPPOL Deliverable D1.1

Requirements for Use of Signatures in Public Procurement Processes

Part 7: eID and eSignature Quality Classification

Version 1.2

PEPPOL WP1 2009-04-30

Borderless eProcurement

Let's make it happen!

Table of Contents

1 Summary and Structure of Document ... 3
1.1 Scope and Structure of Deliverable D1.1 ... 3
1.2 Scope and Structure of This Document ... 3
1.3 Evolution of This Document ... 4
1.4 Version, List of Contributors ... 4
2 Signature Policies ... 6
3 Quality of eIDs ... 7
3.1 Starting Point – DNV Classification Scheme ... 7
3.2 eID Quality Profile ... 8
3.2.1 Certificate Quality Parameter (Claimed Quality) ... 8
3.2.2 Independent Assurance Parameter ... 9
3.3 Assessment of non-European Certificates ... 11
3.4 Trust Status List of QCSPs ... 11
4 Cryptographic Quality ... 13
5 Signature Quality ... 14
5.1 Examples ... 14
5.1.1 Example 1: Qualified Certificate and SSCD, Accredited CA ... 14
5.1.2 Example 2: Qualified Certificate, Accredited CA ... 14
5.1.3 Example 3: Qualified Certificate, Supervised CA ... 15
5.1.4 Example 4: NCP Certificate and SSCD, Certified CA ... 15
5.1.5 Example 5: NCP Certificate, External Compliance Report for CA ... 15
5.1.6 Example 6: LCP Certificate, Internal Compliance Report for CA ... 15
5.1.7 Example 7: Certificate Issued by CA Cross Certified with the US FBCA at Medium Assurance Level ... 16
5.1.8 Example 8: Self Issued Certificate with no Documented Policy ... 16
6 Quality of the Actor Issuing an eID ... 17
7 References ... 18
8 Appendix 1: FBCA Requirements Mapped to the PEPPOL Profile ... 19
9 Appendix 2: XML structure ... 21

1 Summary and Structure of Document

1.1 Scope and Structure of Deliverable D1.1

This document is a part of the multi-part deliverable D1.1 "Requirements for Use of Signatures in the Procurement Processes" issued by the PEPPOL[1] (Pan-European Public Procurement On-Line) project. PEPPOL is a three-year (May 2008 – May 2011) large scale pilot under the CIP (Competitiveness and Innovation Programme) initiative of the European Commission. D1.1 consists of the following documents:

Part 1: Background and Scope

Part 2: 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 D1.1 deliverable is the first 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, if the resulting solution is successful it is believed that it will 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 guide the implementation, testing, and piloting of e-signature interoperability solutions to be done by PEPPOL. The specifications are publicly available and comments from any interested party are most welcome. Note that since the specifications of D1.1 by necessity will evolve as a result of further work in PEPPOL, any party using or referring to the specifications must ensure that the latest version is used; contact the PEPPOL project for information.

1.2 Scope and Structure of This Document

The purpose of the document is to specify a quality profile for digital signatures that can be used to set requirements to and make assessments of the quality of digital signatures in public e-procurement across borders in Europe.

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;
- Even qualified signatures may differ in quality, although it may be discussed to what extent qualified signatures may be refused on such grounds;

[1] http://www.peppol.eu

- 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, e.g. corporate PKIs of reasonable quality and non-qualified public eIDs.

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 4, respectively. Together, these profiles will constitute a signature quality profile as described in Chapter 5. 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 6. 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.

1.3 Evolution of This Document

This document provides the first version of a PEPPOL quality classification system. The following evolution of this document is expected:

- Further alignment with D1.1 parts 5 (XKMS) and 6 (OASIS DSS) should be done in order to incorporate quality classification in requests and responses. Further evolution of the quality system must be expected in this work.
- A quality classification system should be standardized. Since referral is made to ETSI standards, ETSI may be the most suitable standards body, although this needs consideration, and a global standards organization 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.
- Quality classification may also be incorporated in trust status lists such as described in D1.1 part 4. This will enable inclusion of non-qualified eIDs in such lists.

1.4 Version, List of Contributors

Version 1.0	2009/02/11	Complete version for internal quality assurance.
Version 1.1	2009/02/27	Submitted to PEPPOL project management, approved with comments at project management meeting 2009/03/27.
Version 1.2	2009/04/30	For publication, updated according to comments.

The following organizations, in alphabetical order, have contributed to Deliverable D1.1.

- **bremen online services, Germany,** http://www.bos-bremen.de
- **CNIPA, Italy** http://www.cnipa.it
- **DGME, French Ministry of Finance** http://www.references.modernisation.gouv.fr/
- **DNV, Norway** http://www.dnv.com

The following persons (alphabetical ordering for each participating organization) have contributed to the work:

Jörg Apitzsch	bos	Uwe Trostheide	bos	Dr. Daniele Tatti	CNIPA
Markus Ernst (co-editor)	bos	Jens Wothe	bos	Mario Terranova	CNIPA
Mark Horstmann	bos	Martine Schiavo	DGME	Anette Andresen	DNV
André Jens	bos	Stefano Arbia	CNIPA	Dr. Leif Buene	DNV
Dr. Jan Pelz	bos	Giovanni Manca	CNIPA	Jon Ølnes (editor)	DNV
Marco von der Pütten	bos	Adriano Rossi	CNIPA		

2 Signature Policies

A signature policy[2] 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). The main purpose of a signature policy is to define quality requirements (cryptographic requirements, certificate policy requirements, requirements for use of smart cards etc.). A signature policy may also list trusted eID issuers. Additionally, the policy may set requirements for the signature format[3] to be used and information to be included in the SDO (signed data object), such as time-stamps, eID information, revocation information and policy identifiers. 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.

IDABC [IDABC01] finds 15 countries with e-procurement services in operation, where 6 require qualified signatures, 7 require advanced signatures (sometimes with the additional requirement of a qualified eID), while two countries require only authentication. The services furthermore either list one or a few eID issuers or are able to accept all domestic issuers and perhaps a few foreign issuers.

Part 4 of PEPPOL's D1.1 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. supports qualified signature);
- 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 D1.1) and process assessments made by validation services. In D1.1 part 5 (XKMS) definitions of enumerations for the values of quality parameters are outlined.

The framework specified in this document is explicitly targeted at incorporating even 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 this 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 explicitly targeted at easy assessment of issuers of qualified eIDs, while assessment of non-qualified issuers may require some more effort.

The assessment job must be done for all eID issuers that shall be available for PEPPOL pilots, i.e. preferably at least all issuers of qualified eIDs in Europe. A Trust Status List distribution service (see D1.1 part 4) can be used to populate a validation service with this information.

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

[3] Examples are XAdES (ETSI TS 101 903), CAdES (ETSI TS 101 733), PKCS#7 (RFC2315), CMS (RFC2630), XML DSIG (RFC3275), and PDF signatures.

3 Quality of eIDs

3.1 Starting Point – DNV Classification Scheme

Validity of an eID certificate is given by successful cryptographic processing based on the CA's (eID issuer) public key, plus checks on validation period for certificate and revocation status; however this gives no indication in itself about the quality of the eID. Correspondingly, the quality of an eID or a signature based on this eID is not assessed by merely verifying that the cryptographic processing yields a positive answer.

A possible starting point, which also serves as an illustration of the problem, for quality classification is the scheme developed by DNV [DNV01], consisting of 7 quality classes:

0. Inadequate or non-determined level: Very low confidence or assessment not possible, usually because a certificate policy does not exist. Many corporate PKIs will be placed in this category.

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

2. Medium non-approved level: Medium confidence certificates with no formal registration/approval status.

3. High non-approved level: Certificate quality is at or very close to qualified level but certificate issuer is not registered/approved by assigned inspectorate/authority according to applicable law to the issuer.

4. Non-qualified approved level: Certificate is not marked as qualified but certificate issuer is registered/approved by assigned inspectorate/authority according to applicable law to the issuer (according to a registration/approval scheme for issuers of non-qualified certificates).

5. Qualified approved level: Certificates are marked as qualified and the issuer is registered/ approved by assigned inspectorate/authority according to applicable law to the issuer. Private key environment is not certified as SSCD (Secure Signature Creation Device) according to CEN CWA 14169.

6. Qualified signature level: Certificates are marked and registered as for level 5, and use of a certified SSCD according to CEN CWA 14169 is mandated. Thus, this level supports qualified signatures according to the EU Directive on electronic signatures.

The division into distinct classes is useful but the scheme needs enhancement at least on the following issues:

- There is a lack of formal criteria for levels 0-3,
- There may be a need to convey quality even for qualified eIDs as quality differs (note e.g. the case of SHA-1 use in Germany[4]),
- Thus, there is a need to separate quality and approval status,
- The scheme should be enhanced to accommodate non-European eIDs,
- Existing certification schemes such as WebTrust, T-scheme, Federal Bridge in the US, SAFE Bridge-CA, and more should be acknowledged,

[4] In Germany it was decided to abandon use of the SHA-1 hash algorithm by end of 2008. This algorithm is in Germany no longer accepted to sign qualified eIDs and qualified signatures. The rest of the world will in general replace SHA-1 by the end of 2010.

- The assurance level for the quality should be indicated, such as “self assessment”, “document evaluation only”, “compliance audit performed”, etc.

3.2 eID Quality Profile

A “PEPPOL profile” for eID quality is defined as an extension of the DNV eID quality classification scheme mentioned above. This profile defines quality in terms of two independent 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 3.2.1) and y is the independent assurance level (0-7; see 3.2.2) as defined below.

3.2.1 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. (Use of a SSCD is mandated in the CP.)

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 = Normalized Certificate Policy
QCP = Qualified Certificate Policy
SSCD = Secure Signature Creation Device

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 an SSCD; this is the reference certificate policy NCP. Additional requirements to use the certificate with an SSCD give the reference policy NCP+.

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.

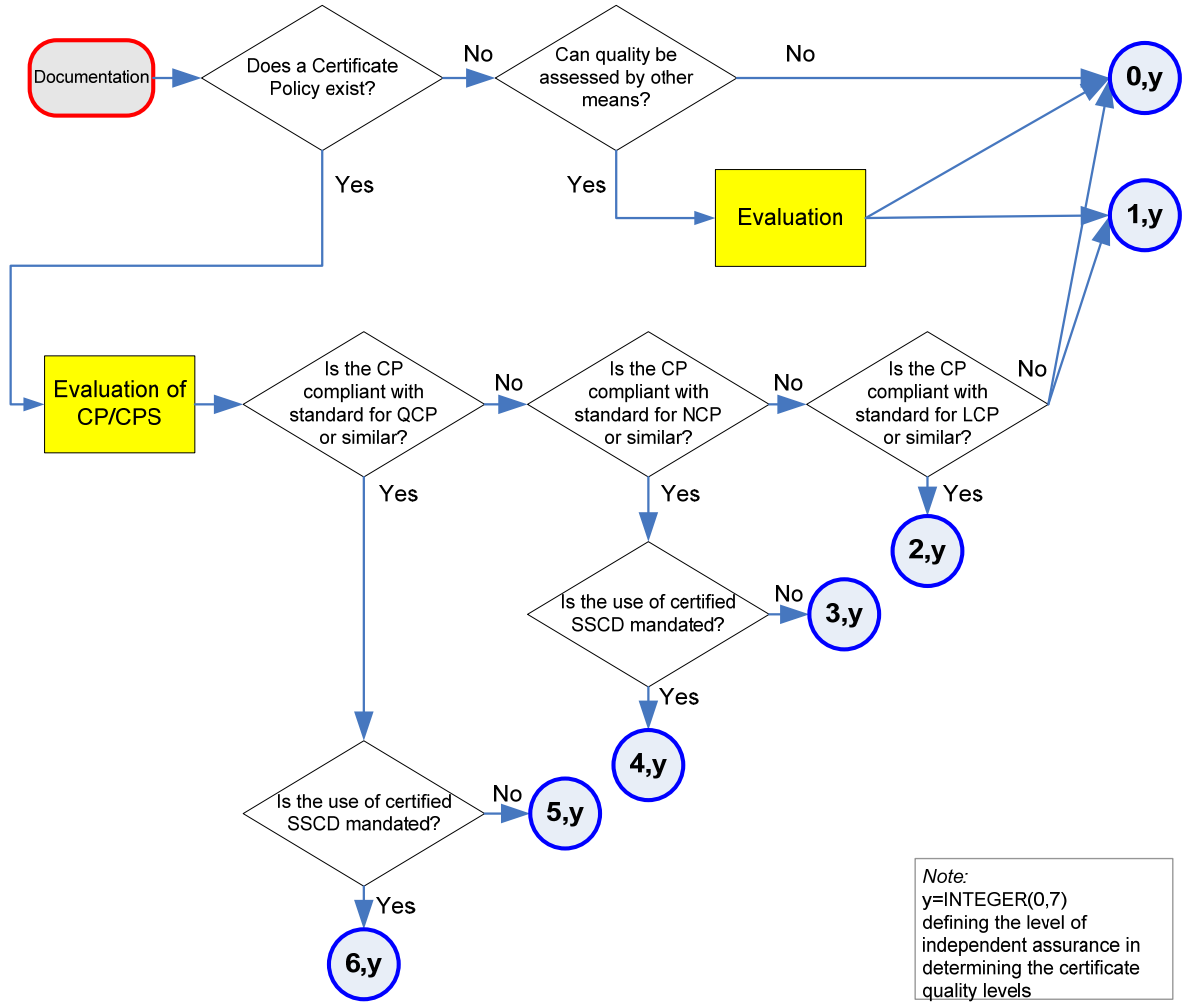

Figure 1 Assessment of certificate quality level

3.2.2 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, 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.

Comment: 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.

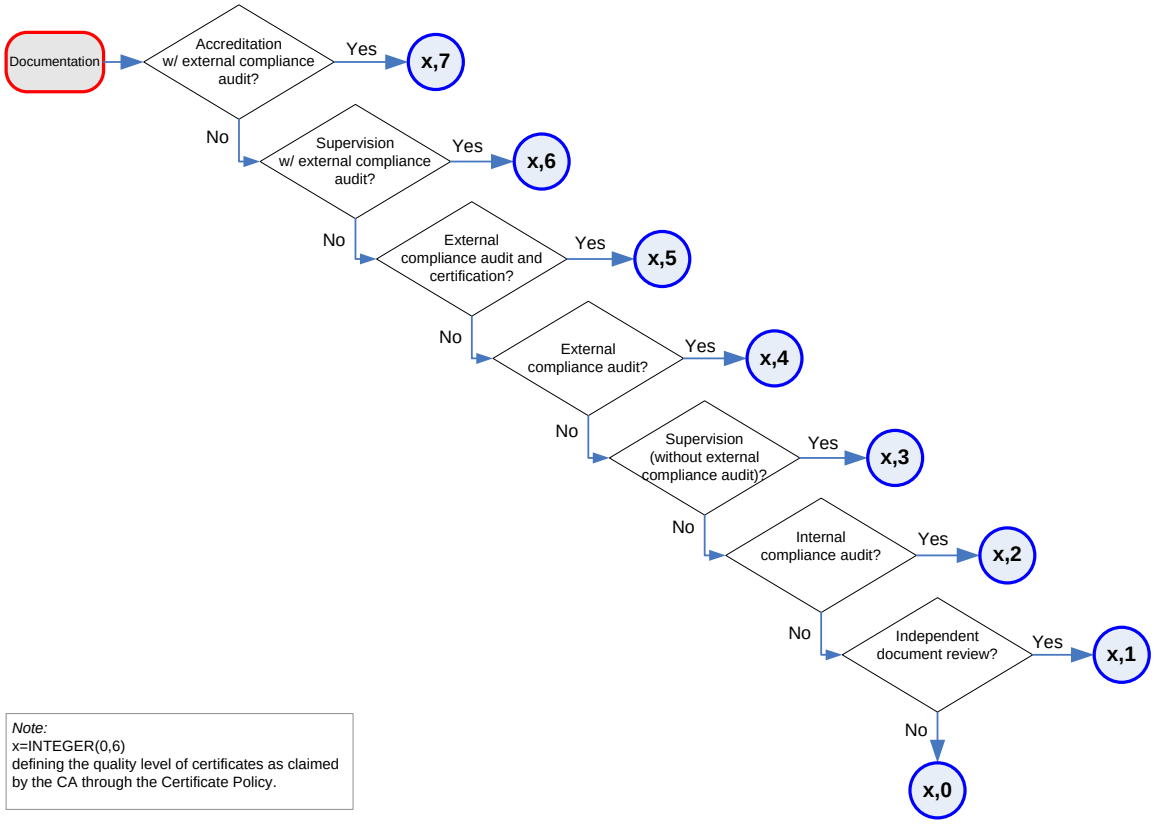

Figure 2 Assessment of independent assurance level

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.

Note that 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, regarded as equivalent to qualified) the distinction may be relevant.

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

3.3 Assessment of non-European Certificates

The assessment criteria for certificate quality and independent assurance levels defined in 3.2.1 and 3.2.2 can be applied to non-European certificates as well, even if the term “qualified certificate” is not defined outside of Europe.

If the Certificate Policies of such certificates do 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 Certificate Policies through document reviews.

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.

3.4 Trust Status List of QCSPs

Work is in progress to define a Common Template for Trust Status Lists of supervised and/or accredited Qualified Certificate Service Providers (QCSPs) [SEALED01]. This Common Template shall provide a common way for Member States of providing information about both supervised and accredited QCSPs. This information is aimed at supporting the validation of qualified electronic signatures (QES) and advanced electronic signatures (AdES) supported by a qualified certificate. The expected supervision/accreditation status flow for a service is illustrated in Figure 3 below (taken from [SEALED01]).

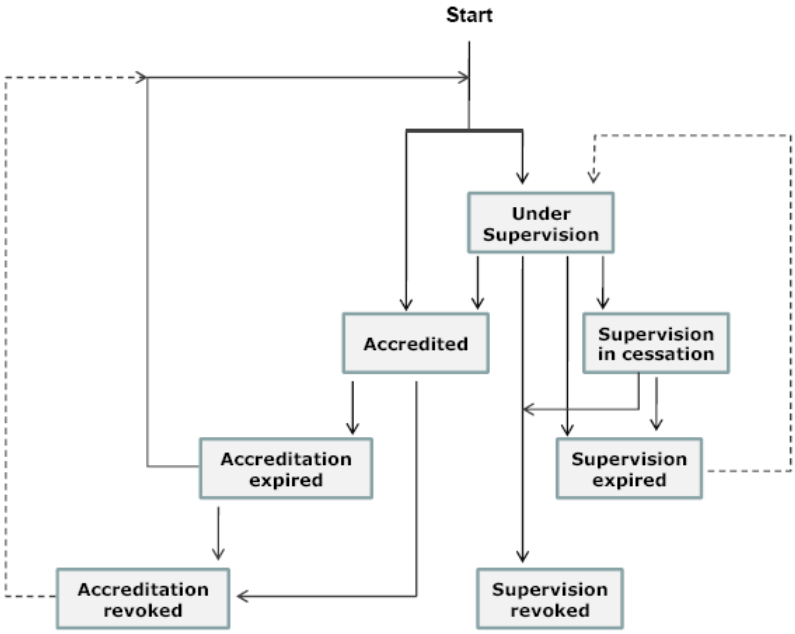

Figure 3 Expected supervision/accreditation status flow ([SEALED01])

Such Trust Status Lists will significantly ease the assessment of independent assurance levels described in 3.2.2. However, for eID quality classification the indication of assurance levels should be "supervision" (with or without compliance audits, levels 6 and 3 respectively) and "accreditation" (level 7) and no intermediate status indication. Intermediate status indications could serve as a flag for the maintenance activities related to eID classification.

4 Cryptographic Quality

The parameters of concern here are hash algorithm quality for the signed document (hash algorithm for the eID certificate is considered part of eID quality), and quality of the combination public key algorithm and key length. Note that the eID does not influence the selection of hash algorithm for document; this is selected through the signing software.

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 (refer the German case on SHA-1 hash; Germany also disapproves RSA with keys shorter than 2048).

Adapted from US recommendations [NIST01] that seem to be agreed to by most European countries as well, a starting point for quality classification can be 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 seem to be agreed judgements about which algorithms should go in which classes. This assumes 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.

5 Signature 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. chapter 3.1.1) and an independent assurance parameter ranging from 0 to 7 (ref. chapter 3.1.2)
- **Hash quality**, ranging from 0 to 5 (ref. chapter 4)
- **Public key quality**, ranging from 0 to 5 (ref. chapter 4)

PEPPOL suggests a notation for the signature quality as follows

Signature quality = {eID quality, hash quality, public key quality}

= {(certificate quality, independent assurance), hash quality, public key quality}

5.1 Examples

5.1.1 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:

signature quality = {(6,7),2,2}

5.1.2 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}

5.1.3 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}

5.1.4 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}

5.1.5 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 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 = {(3,4)1,1}

5.1.6 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 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 = {(2,2)1,1}

5.1.7 Example 7: Certificate Issued by CA Cross Certified with the US FBCA at 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}

5.1.8 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}

6 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 organization 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 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

[DNV01] Ølnes, Jon et al.: Making Digital Signatures Work across National Borders. Paper published in Pohlmann, Reimer, Schneider: ISSE/Secure 2007, Securing Electronic Busines Processes, pp. 287-296, October 2007, ISBN 978-3-8348-0346-7.

[EC01] Directive 1999/93/EC of the European Parilament 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

[FBCA01] FBCA: X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), September 10, 2002, http://www.cio.gov/fpkipa/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

[SEALED01] Sealed, Technical Specifications for the Proposed Common Template for the “Trusted List” of Supervised/Accredited QCSPs, version 0.72, January 2009 (to be published in version 1.0 later in 2009).

8 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 (3.2) 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	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 bove. Individuals may assume more than	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

		role, however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No individual shall be assigned more than one identity.	one role, however, individuals who assume an Officer role may not assume an 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.	Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. 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**

9 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>
```