Study on Cross-Border Interoperability of eSignatures

(CROBIES)

Quality Classification Scheme for eSignature elements

A report to the European Commission

from SEALED, time.lex and Siemens

FINAL REPORT

Editing company: SEALED sprl,
VAT: BE 0876.866.142 – RPM: Tournai
12, rue de la Paix, B-7500 Tournai
olivier.delos@sealed.be, sylvie.lacroix@sealed.be

Date: 31/07/2010
Version: 1.0

Document information

Title:	CROBIES Work Package 5-2 **Quality Classification Scheme for eSignature elements**
Project reference:	CROBIES
Document archival code:	INFSO-CROBIES-FINALREPORT-WP5-2-SEALED-31072010_v1.0

Version control

Version	Date	Description / Status	Responsible
V0.1	29/05/2010	Draft Final Report	ODO, SLR
V1.0	31/07/2010	Final Report	ODO

References

Reference	Title
[1]	The European Directive 1999/93/EC of the European Parliament and the Council of the 13 December 1999 on a Community framework for electronic signatures. O.J. L 13, 19.1.200, p.12.
[2]	Study on the standardisation aspects of eSignature. A study for the European Commission (DG Information Society and Media) by SEALED, DLA Piper and Across communications, 22/11/2007.
[3]	Commission Decision 2003/511/EC "on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the EP and the Council". OJ L 175 15.7.2003, p.45.
[4]	Mandate M460, Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies applied to electronic signatures, 7 January 2010.
[5]	Study on the European Federated Validation Services. Framework contract ENTR/05/58-SECURITY, SC N°14 – Completion of the framework for signature validation services. February 2010 reports.

Definitions and Acronyms

Please refer to the Head Document for definitions and acronyms used throughout the present report.

Table of Contents

1 INTRODUCTION 3

1.1 CROBIES 3
1.2 Executive Summary 3
1.3 Target readership 5

2 THE PROPOSED SCHEME 5

3 USAGE OF THE QUALITY CLASSIFICATION SCHEME FOR ESIGNATURE ELEMENTS 12

4 RECOMMENDATIONS 13

Quality Classification Scheme for eSignature elements

1 Introduction

1.1 CROBIES

The CROBIES study looks at eSignature interoperability in general, but specifically in the context of cross-border use. While considering a consistent global and long term approach in proposed improvements at the legal, technical and trust levels, CROBIES is also focusing on quick wins that could substantially improve the interoperability of electronic signatures.

The CROBIES Study concentrates in particular on the following aspects through related work packages and their associated reports:

WP1. The proposal for a common model for supervision and accreditation systems of certification service providers (CSPs) issuing QCs (and other services ancillary to electronic signatures);

WP2. The establishment of a "Trusted List of supervised/accredited Certification Service Providers" (in particular issuing QCs);

WP3. Interoperable profiles of qualified certificates issued by supervised/accredited CSPs in Member States;

WP4. A proposed framework for interoperable Secure Signature Creation Devices (SSCDs); and

WP5. A proposed model for providing guidelines and guidance for cross-border and interoperable implementation of electronic signatures.

The global overview of the CROBIES study and of its approach is to be found in the "Head Document" of the study. The study is part of the *Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market* adopted by the European Commission on 28.11.2008[1] which aims at facilitating the provision of cross-border public services in an electronic environment. Readers are suggested to read this Head Document prior to reading the present report.

1.2 Executive Summary

A best practice for eSignature business stakeholders is to design a so-called "Signature Policy" when designing eSignature based applications. A Signature Policy aims at implementing the appropriate level of electronic signature in accordance with business requirements, associated policy or legal requirements, expected signature flow in concerned business e-process, and the associated risk assessment."[2] A Signature Policy aims at

[1] COM(2008) 798, http://ec.europa.eu/information_society/policy/esignature/action_plan/index_en.htm

[2] Signature Policy [ETSI TS 101 733] : set of rules for the creation and validation of an electronic signature that defines the technical and procedural requirements for electronic signature creation and validation, in order to meet a particular business need, and under which the signature can be determined to be valid. Further information on Signature Policies is provided in:

- ETSI TR 102 041 ("Signature Policies Report") and TR 102 045 ("Signature policy for extended business model")
- ETSI TS 101 733 ("CAdES") and TR 102 272 ("ASN.1 format for signature policies")
- ETSI TS 101 903 ("XAdES") and TR 102 038 ("XML format for signature policies")

identifying rules to be applied by signers when generating electronic signatures in a determined specific application domain or context and rules to be applied by verifiers to validate those electronic signatures. In this context, it is part of the establishment of those rules to identify requirements for specific quality criteria of eligible signature elements (e.g. supporting device, supporting certificates, cryptographic algorithms and parameters) and more generally the "quality" of eligible electronic signatures that are deemed to be implemented and accepted in the identified business application domain covered by the Signature Policy.

CROBIES proposes to formalise such a "Quality Classification Scheme for eSignature elements"[3] identifying a set of quality levels for major eSignature elements with the aim to support eSignature stakeholders in specifying requirements on the quality of an electronic signature implementation (e.g. in a signature policy context).

The proposed classification scheme is meant to be given as a proposal for further consideration and potential standardisation. It can be used:

- As a means for the signatory to express a claim as part of the signature which has to be assessed by the verifier against specific applicable threshold or minimal requirements with regards to the quality of or more, if not all of, considered signature elements[4];

- As a means to be used in the context of Signature Policies to express (minimal) requirements on specific signature element quality to be considered as part of the rules for the creation and verification of an electronic signature under which the signature can be determined to be valid.

The reader is referred to the model for designing signature policy and in particular to the CROBIES recommendation to extend this model towards a "guidance model for implementing electronic signatures and designing signature policies" described in its WP5.1 deliverable. Namely the business requirements, the associated legal requirements and the risk assessment that should be considered when implementing electronic signatures in support of an electronic business process will allow identifying specific requirements that will have an influence on the security and quality level that implemented electronic signatures will have to reach in order to be accepted as valid in the considered electronic business process. The need for meeting legal requirements of QES, specific Long Term Validity (LTV) requirements to be met, signatures to be applied by natural or legal persons are examples of such requirements that will have an influence on the security and quality level of electronic signature implementations. Those functional requirements are expected to be identified through an (extended) signature policy design process or through a similar process aiming to identify the requirements and rules to be adopted for creation, verification and LTV maintenance of electronic signatures in a specific business or application domain.

- IETF RFC 3125 ("Electronic signature policies")

Note that CROBIES WP5 proposes an extension of the concept to cover support of global guidance on eSignature implementation and Signature policy design.

[3] CROBIES initiated liaison and joint work approach with PEPPOL on this topic as PEPPOL drafted a similar purpose classification in its WP1 related to eSignatures (see http://www.peppol.eu/deliverables/wp-1/d1-1-part-3-signature-policies/view and http://www.peppol.eu/deliverables/wp-1/d1-1-part-7-eid-and-esignature-quality-classification/view).

[4] The signatory is indeed expected to have control on all the signature elements considered by the classification scheme (i.e., signing device, signing certificate, used signature cryptographic suite, long term validity solutions and signature application). E.g. in specific use cases

1.3 Target readership

The present report is mainly addressed to the ESO's to support their work in the context of the eSignature Mandate M460 [4]. Recommendations are specifically made with regards to rationalisation and improvements of existing eSignature standards for signature creation and verification products and services, as well as related guidelines and procedures.

The present report is also addressed to stakeholders willing to implement electronic signatures.

2 The proposed scheme

The proposed "Quality Classification Scheme for eSignature elements" uses a set of 7 signature element identifiers, namely "**a.b.c.d.e.f.g**" each of which being associated with 5 quality levels (from "1" to "5"[5]) which correspond to the identification of the quality level for the following eSignature elements:

a) The Signing Device;
b) The Certificate Provision (covering certificate policies, certificate quality and security level);
c) The Independent Assurance on the certificate provision (c);
d) The Signature Cryptographic Suite[6];
e) The Long Term Validity (LTV) solutions[7] associated to the electronic signature preservation;
f) The Signature Application; and
g) The Independent Assurance on the signature application (g).

The proposed "Quality Classification Scheme for eSignature elements" does not aspire to exhaustively represent the security of electronic signature systems but to assist in specifying or identifying the level of quality of a specific set of major elements that are part of the implementation of an electronic signature. This scheme may be used in the context of signature policy requirements.

Figure 1 below illustrates the proposed quality levels for the seven identified signature elements (i.e. the meaning of each and every value for the seven identifiers) as used in the Quality Identifier (QID) notation of the proposed scheme.

For the sake of interoperability and harmonisation with (well) established electronic authentication guidelines, the proposed scheme is looking for compatibility and relation with systems for classification of Identity Assurance as specified in NIST SP 800-63[8], US OMB 0404[9], Kantara initiative[10] and IDABC Authentication Policy[11]. CAB Forum "extended

[5] The "zero" value may be used to identify quality and/or security levels that are below the ones identified in level 1.
[6] The Signature Cryptographic Suite (K, S, V, H) is defined as the combination of the identification of the Signature Scheme (K, S, V) identifying three algorithms, namely the key generation algorithm (K), the signing algorithm (S) and the verification algorithm (V), together with the Hash function used (H). Meaning for the proposed value classification and "signature cryptographic suite" definition is based on/taken from D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), dated 30 March 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).
[7] It should be noted that (e) has an impact at least on the use of eSignature formats (e.g. used forms for X/C/PAdES) and of archiving systems.
[8] See http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.
[9] See http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf.
[10] See http://kantarainitiative.org/confluence/display/certification/Identity+Assurance+Certification+Program.

validation" guidelines should also be taken into account when further defining the criteria associated to the proposed levels.

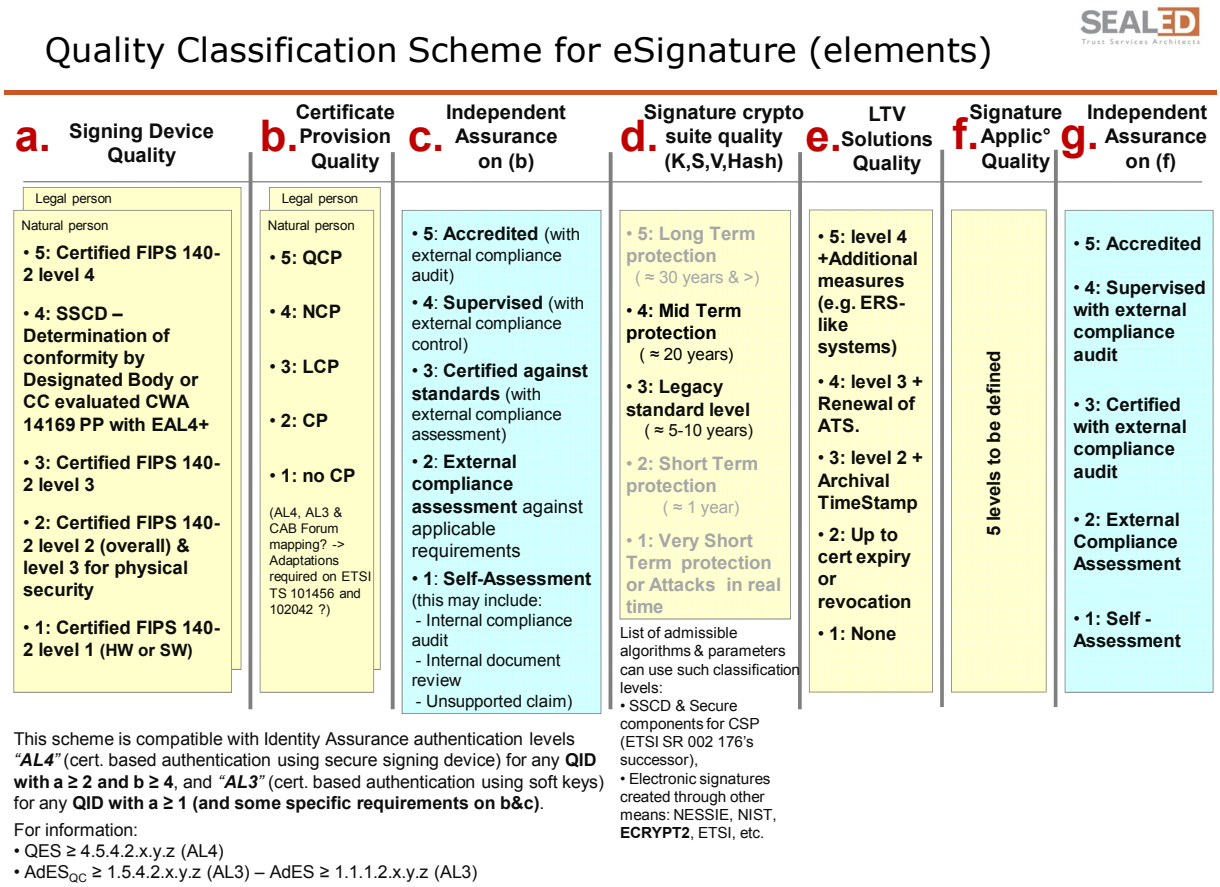

Figure 1

a. Signing Device Quality

The five quality levels for identifying the security level of the device used by the signer to create an electronic signature are defined as follows:

1) **Certified FIPS 140-2 level 1 software or hardware token**: a cryptographic key that is typically stored on disk or some other low-security media. The soft token or low-security media key should be encrypted under a key derived from some activation data (e.g. a password, a PIN-code). In this Signing Device Quality (SDQ) level 1, the cryptographic module is validated at FIPS 140-2 level 1 (or higher) and may be either a hardware device or a software module. Each signature shall require the entry of the password or other activation data and the unencrypted copy of the signing key shall be erased after each signature.

2) **Certified FIPS 140-2 level 2 overall and physical security at level 3 (or higher)**: A hardware device that contains a protected cryptographic key. Such SDQ level 2 tokens shall (i) require the entry of an activation data to activate the signing key, (ii) not be able to export the signing key, (iii) be FIPS 140-2 level validated with an

[11] See http://ec.europa.eu/idabc/en/document/3519/5927.

overall validation at FIPS 140-2 level 2 or higher and a physical security at level 3 or higher.

3) **Certified FIPS 140-2 level 3 (or higher)**: A hardware device that contains a protected cryptographic key. Such SDQ level 3 tokens shall (i) require the entry of an activation data to activate the signing key, (ii) not be able to export the signing key, (iii) be FIPS 140-2 level validated with an overall validation at FIPS 140-2 level 3 or higher.

4) **SSCD**: A hardware device that is a signature creation device that meets the requirements of Annex III of Directive 1999/93/EC [1]. This can be, e.g., a device CC evaluated against one of the CWA 14169 Protection Profiles with an assurance level EAL4+ or a device for which compliance with requirements of Annex III of Directive 1999/93/EC has been determined by a Member State's designated body according to the provisions laid down in the Directive.

5) **Certified FIPS 140-2 level 4**: A hardware device that contains a protected cryptographic key. Such SDQ level 5 tokens shall (i) require the entry of an activation data to activate the signing key, (ii) not be able to export the signing key, (iii) be FIPS 140-2 level validated with an overall validation at FIPS 140-2 level 4.

Note1: The above set of quality levels are proposed for Natural Person devices. As illustrated in Figure 1, a specific set of quality levels should be defined for Legal Person devices and it has been suggested that ISO 19790:2006 (equivalent to FIPS 140-2) type devices would be suitable for references in such a classification.

Note2: The level of control on the signature creation data activation (in addition but in relation with the device) can also be taken into account as an additional element on which quality levels could be defined. Those levels and associated quality criteria are likely to be significantly different with regards to natural person and legal person devices.

Note 3: The above levels are based on and mix US and EU defined levels (e.g. CC formal evaluations) that may not be easily compared to each other. Rationalisation and international harmonisation should take place at standardisation levels with regards to the review of those levels (in particular in the context of execution of mandate M460 [4]).

b. Certificate Provision Quality

The ETSI standard TS 101 456[12] sets policy requirements to CAs issuing qualified certificates in accordance with Directive 1999/93/EC; this is the reference certificate policy QCP in the classification below. Annex I of this Directive specifies requirements for qualified certificates, and Annex II specifies requirements to CAs issuing qualified certificates[13]. The ETSI standard TS 102 042[14] sets policy requirements to CAs issuing certificates at the same quality level as that of qualified certificates, but without the legal constraints implied by Directive 1999/93/EC and without requiring use of an SSCD; this is the reference certificate

[12] ETSI TS 101 456: Electronic Signatures and Infrastructures (ESI); Policy Requirements for Certification Authorities issuing Qualified Certificates.
[13] 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+.
[14] ETSI TS 102 042: Electronic Signatures and Infrastructures (ESI); Policy Requirements for Certification Authorities issuing Public Key Certificates.

policy NCP[15]. The reference certificate policy LCP incorporates less demanding requirements as specified in ETSI TS 102 042.

The five levels for identifying the quality of the certificate provision are defined as follows[16]:

1) **No CP level**: Very low confidence in certificate or quality assessment not possible, usually because a certificate policy does not exist.

2) **CP (Certificate Policy) level**: Low confidence in certificate but certificate policy exists or quality assessment is possible by other means.

3) **LCP (lightweight Certificate Policy) level**: Medium confidence in certificate governed by a Certificate Policy in compliance with the ETSI TS 102 042 standard for LCP or a similar standard. LCP relates to an ETSI TS 102 042 defined certificate policy which incorporates less demanding policy requirements than NCP or QCP levels.

4) **NCP (Normalised Certificate Policy) level**: Certificates governed by a Certificate Policy in compliance with the ETSI TS 102 042 standard for NCP or a similar standard. NCP relates to an ETSI TS 102 042 defined certificate policy which offers the same quality as that offered by the Qualified Certificate Policy (QCP) as defined in TS 101 456 but without the legal constraints implied by Directive 1999/93/EC and without requiring the use of a Secure Signature Creation Device (SSCD). ETSI TS 102 042 also defines an extended Normalized Certificate Policy (NCP+) which offers the same quality as that offered by the Qualified Certificate Policy (QCP) as defined in TS 101 456 but without the legal constraints implied by the Electronic Signature Directive (1999/93/EC) and, instead of requiring the use of a Secure Signature Creation Device, requires the use of a '*secure user device'*.

5) **QCP (Qualified Certificate Policy) level**: Certificates governed by a Certificate Policy in compliance with the ETSI TS 101 456 standard for QCP or a similar standard. QCP relates to an ETSI TS 101 456 defined certificate policy for qualified certificates which meets the requirements laid down in Annex I of Directive 1999/93/EC and are issued by a CA who fulfils the requirements laid down ion Annex II of the Directive. Qualified certificates issued under this policy may be used to support electronic signatures which "are not denied legal effectiveness and admissibility as evidence in legal proceedings", as specified in Article 5.2 of Directive 1999/93/EC. When those certificates are for use with SSCD which meets the requirements laid down in Annex III of the Directive, they may be used to support electronic signatures which "satisfy the requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data", as specified in Article 5.1 of Directive 1999/93/EC.

Note: As illustrated in Figure 1, the specific criteria and policy requirements for certificate provision may differ when considering natural persons or legal persons as certificate owners. When considering legal persons, the addition of criteria as defined in the CAB Forum "Extended Validation" guidelines can provide additional security. It is recommended that the relevant European standardisation framework shall be updated accordingly in the context of

[15] Additional requirements to use the certificate with a Secure User Device (SUD) give the reference policy NCP+.

[16] Note that in order to be fully in line with Kantara, NIST and OMB Identification Assurance AL4 and AL3 levels, there would be some adaptations required on ETSI TS 101 456 and 102 042 requirements (e.g. registration and initial identification of certificate owner).

the execution of the Mandate M460 for the rationalisation of the European eSignature standardisation framework [4].

c. Independent Assurance on Certificate Provision Quality

The five levels for identifying the Independent Assurance on the quality of the certificate provision are defined as follows:

1) **Self-Assessment**: Internal assessment carried out periodically concluding compliance to applicable requirements.

2) **External compliance assessment**: Audit carried out periodically by external, independent auditor concluding compliance to applicable requirements.

3) **Certification with external compliance audit**: Certification resulting from successful audit carried out periodically by external, independent auditor concluding compliance to applicable requirements. Certificate Provision quality is certified in accordance with a relevant standard with regards to the target quality level.

4) **Supervision with external compliance audit**: Supervision controls carried out periodically by external, independent controllers concludes compliance to applicable requirements, and in particular according to applicable law to certification service provider. This level covers EU Member State's appropriate systems allowing for supervision of certification service providers which are established on its territory and issue qualified certificates to the public as specified in Article 3.3 of Directive 1999/93/EC.

5) **Accreditation with external compliance audit**: Audit carried out periodically by external, independent auditor concludes compliance to applicable requirements, and in particular according to applicable law to certification service provider. This level covers 'voluntary accreditation' as specified in Directive 1999/93/EC.

d. Signature Cryptographic Suite Quality

The five levels for identifying the quality of the Signature Cryptographic Suite (K, S, V, H) [17] are defined as follows:

1) **Very Short Term protection or Attacks in real time**;

2) **Short Term protection (≈ 1 year)**;

3) **Legacy Standard level (≈ 5-10 years)**;

4) **Mid Term protection (≈ 20 years)**;

5) **Long Term protection (≈ 30 years and above)**.

[17] "Signature suite" is here defined as consisting of the following components (*K*, *S*, *V*, *H*):
- A Key generation algorithm *K*;
- A Signing Algorithm *S* with parameters and padding method;
- A Verification algorithm *V*; and
- A Hash Function *H*.

Note: Levels 1, 2 and 5 may not be relevant in practice.

Considering that meaning for the proposed 5 values and "signature cryptographic suite" definition is a simplified version from the one defined in D.SPA.13 ECRYPT2 report, it would be beneficial if recommendations on algorithms and parameters eligible for electronic signatures would use the above defined (d) set of values and value definitions to organize their recommendations.

For the sake of illustration and considering the D.SPA.13 ECRYPT2 report, the ECRYPT2 recommendations for signature suites eligible for electronic signatures would be interpreted as follows according to the proposed classification:

QID(e) values	Eligible signature suites
5.Long Term protection (=30 years and above)	no recommendations
4. (Medium term protection ≈20 years) *(new deployments)*	• ***RSA PKCS#1 v1.5** (use RSA PSS instead whenever possible)* o *Random choices of **p**,**q** of roughly the same size. **d** must not be small. **e** > 65536 recommended, smaller if performance is critical.* o *At least **224-bit hash function** and **|N| ≥ 2432** (new deployments)* • ***RSA-PSS*** o *Random choices of **p**,**q** of roughly the same size. **d** must not be small. **e** > 65536 recommended, smaller if performance is critical.* o *At least **224-bit hash function** and **|N| ≥ 2432** (new deployments)* • ***[DSA (FIPS PUB 186-3 as it will specify larger keys and hashes)]*** • ***ECDSA*** o *Parameters: see ECRYPT2 D.SPA.13 report* o *Curves over prime fields are recommended as a first choice, using a curve with a prime order sub-group with at least 224 bits*
3.(Legacy standard level ≈5-10 years)	• ***RSA PKCS#1 v1.5** (use RSA PSS instead whenever possible)* o *Random choices of **p**,**q** of roughly the same size. **d** must not be small. **e** > 65536 recommended, smaller if performance is critical.* o *At least **160-bit hash** function and **|N| ≥ 1024*** • ***RSA-PSS*** o *Random choices of **p**,**q** of roughly the same size. **d** must not be small. **e** > 65536 recommended, smaller if performance is critical.* o *At least **160-bit hash function** and **|N| ≥ 1024*** • ***DSA (FIPS PUB 186-2)*** o *Parameters: see ECRYPT2 D.SPA.13 report* o *For interoperability reason, not recommended to be used with other hash function than SHA-1* • ***ECDSA*** o *Parameters: see ECRYPT2 D.SPA.13 report* o *Curves over prime fields are recommended as a first choice, using a curve with a prime order sub-group with at least 160 bits*
≤ 2	no recommendations

Related general recommendations from ECRYPT2:

- *Not to use the same keys for encryption and signatures, not using the same keys with both RSA PSS and v1.5*
- *Even when parameters have been certified, it gives extra protection to verify the correctness of parameters to mitigate known attacks.*
- *Hash functions:*
  - *Phasing-out the use of MD5 hash function*
  - *SHA-1 should not be used in new deployments.*
  - *Signature applications with medium to high security should as soon as possible phase out use of SHA-1.*
  - *160-bit hash functions: RIPEMD-160*

- *≥ 224-bit hash functions: SHA-224, SHA-256, SHA-384, SHA-512, Whirlpool (512)*

e. LTV Solutions Quality

The five levels for identifying the quality of the Long Term Validity (LTV) Solutions associated to the preservation of electronic signatures (and signed documents) are defined as follows:

1) **No LTV Solution used**;

2) **Solution valid up to certificate expiry or revocation** (e.g. implementation of X/CAdES –C form of electronic signature or equivalent PAdES-LTV form);

3) **Solution meeting level 2 and including the use of Archival Timestamps** (e.g. implementation of X/CAdES –A form of electronic signature or equivalent PAdES-LTV form);

4) **Solution meeting level 3 and including the renewal of Archival Timestamps** (external secure archival mechanisms can be considered as an alternative to such renewal of archive timestamps provided they are of equivalent or higher quality);

5) **Solution meeting the level 4 and including the combination of Archival Timestamps and the use of external secure archival mechanisms (e.g. ERS-like solutions) and potential additional measures**.

f. Signature Application Quality

The five levels for identifying the quality of the Signature Application, being either a Signature Creation Application or a Signature Verification Application or both, are to be defined (e.g. on the basis of Protection Profiles to be defined in the context of the standardisation efforts related to the execution of Mandate M460 [4] and Evaluation Assurance Levels requirements).

g. Independent Assurance on Signature Application Quality

The five levels for identifying the Independent Assurance on the quality of the Signature Application are defined as follows:

1) **Self-Assessment**: Internal assessment carried out periodically concluding compliance to applicable requirements.

2) **External compliance assessment**: Audit carried out periodically by external, independent auditor concluding compliance to applicable requirements.

3) **Certification with external compliance audit**: Certification resulting from successful audit carried out periodically by external, independent auditor concluding compliance to applicable requirements. Signature Application quality is certified in accordance with a relevant standard with regards to the target quality level.

4) **Supervision with external compliance audit**: Supervision controls carried out periodically by external, independent controllers concludes compliance to applicable

requirements, and in particular according to applicable law to certification service provider.

5) **Accreditation with external compliance audit**: Audit carried out periodically by external, independent auditor concludes compliance to applicable requirements, and in particular according to applicable laws.

3 Usage of the Quality Classification Scheme for eSignature elements

The proposed **Quality Classification Scheme for eSignature elements** allows for the identification of levels or thresholds that would be recommended to be used:

- In Signature Policies for supporting requirements in terms of eligible eSignature quality;
- When establishing "Lists of admissible algorithms and parameters" in order to classify signature cryptographic suites according to QID(d) values.

This classification allows for identifying eligible electronic signatures meeting requirements of:

- **QES**: such electronic signatures should have a **Signature Quality Identifier** (QID) ≥ 4.5.4.2.x.y.z; taking into account that it is likely that SSCDs should be equipped with a Signature Suite with a quality (d) ≥ 3 at issuance time. Even if at the end of its life cycle the SSCD signature suite is of a quality (d) downgraded down to a 2-level, electronic signature generated at that time by means of such an SSCD can still be considered as acceptable (as QES), but in a "very short term" context only, when considering extreme cases from a "strict" legalistic point of view. However at that same time, such electronic signatures may not be considered as acceptable in a context of a more demanding signature policy.

- **AdES$_{QC}$**: such electronic signatures should have an Signature QID ≥ 1.5.4.2.x.y.z,

- **Business scenario based acceptable level of signatures**: e.g. PEPPOL Signature Policy requirement for eSignature quality in the context of PEPPOL, as identified in "PEPPOL D.1.1 Part 3: Signature Policies"[18] could be translated into a QID ≥ 1.2.2.3.x.y.z.

Combined with (trusted) time information at signature creation or verification time, the proposed Quality Classification Scheme gives a metric to assess the quality of an eSignature at any moment of its lifecycle.

Note that with regards to electronic signatures supported by SSCDs (e.g. QES), specific attention should be paid to the fact that at issuance time it is likely that an SSCD will be designed with a signature suite meeting a (d) value greater or equal to 3, when not 4. However during its lifetime which may go up to 5 years for current national eID cards allowing QES generation, it may be such that the SSCD signature suite will be downgraded to a lower (d) value, e.g. "2". This does not preclude verifiers to accept QES generated at that (d=2) time by such SSCDs but they are entitled to consider the quality level of the obtained signature against the security requirements applicable to the application domain in

[18] http://www.peppol.eu/deliverables/wp-1/d1-1-part-3-signature-policies/view.

which the received QES has to be validated and in particular the timeframe for which the signature should under these requirements be considered as valid (QES).

4 Recommendations

The CROBIES team recommends that:

1. **The above Quality Classification Scheme (or alike) to be considered for potential standardisation and that related work will be taken in account by ESOs when executing mandate M460 [4] for rationalisation of EU eSignature standardisation framework.**

2. This work should also be envisaged in the context of a broader action plan towards the comprehensive electronic identification, authentication and signature framework described in the CROBIES Head Document and in the EFVS study [5].

3. **Machine processable** way of providing recommendations with regards to algorithms and parameters eligible for electronic signatures (whether applicable to SSCDs, Secure components for trustworthy systems or for general purposes) should be also standardised, implemented, made available and maintained in order to further support efficient, interoperable and cross-border use of electronic signatures.