Technical Proposal

Title : Phase 1b – ETSI Quick fixes to electronic signatures standards
Specific agreement number : SA/ETSI/ENTR/460/2010-12
Organisation : ETSI
Date : 09/08/2010

Part I – Policy relevance and expected market impact

1. Policy relevance

The proposed actions outlined in this technical proposal address the Electronic Signature Mandate M/460 requirement for a "rationalised European eSignature standardisation framework" and the electronic signatures (domain 5) of the EC's 2010-2103 ICT Standardisation Work Programme

It specifies in detail the "phase 1b – ETSI quick fixes" work plan primarily aimed at providing quick technical fixes to existing electronic signatures standards, in line with the description of mandate M/460 first aims and with the result of the CROBIES study.

This proposal does not include activities to be carried out by CEN under the mandate.

2. Rationale

The Directive 1999/93/EC on a Community framework for electronic signatures was adopted by the European Parliament and the Council in December 1999. The purpose of the Directive is to establish a legal framework for eSignature and for certification-services providers in the internal market. Several internal market instruments (e.g. Services Directive, Public Procurement, eInvoicing) rely in their functioning on the framework set by the Directive. Activities in CEN and ETSI, initiated under the European Electronic Signature Standardization Initiative (EESSI), produced a set of standards addressing the requirements for implementing the electronic signatures Directive. Following on from studies on the standardisation aspects of e-signatures and Cross-Border Interoperability of eSignature (CROBIES), and other EU activities applying electronic signatures, the need has been identified for a "Rationalised European eSignature Standardisation Framework" to be implemented in a 4 year programme. This framework is to ensure that all the necessary standards are provided in a clear, coherent and accessible framework to maximise the interoperability, including progression of existing specifications to European Norms and the provision of implementation guidelines.

As well as recognising the need for a rationalised framework, the need was identified that certain areas of standardisation relating to electronic signatures should be updated as soon as possible to ensure that deficiencies identified in the existing standards are addressed. For example, certain details of profiling Certificate standards require further clarification to

achieve full interoperability, a basis for conformance assessment and testing has yet to be established for all areas of eSignature standardisation, and certain specifications that have lapsed because of lack of support, need to be brought up to date with current practice. Awaiting the development of the Rationalised Framework before addressing these deficiencies will inhibit the use of electronic signatures in a way that is interoperable across Europe and result in further divergence of implementations of the eSignatures Directive.

This proposal is for "quick fixes" to ensure that the deficiencies identified in studies in on the standardisation aspects of e-signatures and Cross-Border Interoperability of eSignature (CROBIES) are addressed as soon as possible, in parallel with establishing a more long term Rationalised Framework for eSignature standardisation. This will ensure that known technical areas that are inhibiting cross-border interoperability are addressed before there is further divergence in implementations.

3. Objective

The overall aim of this proposed action is to provide quick fixes for electronic signature (eSignature) standardisation. The establishment of a rationalized standardization framework is covered by another technical proposal (phase 1a).

In line with mandate M/460 this technical proposal covers Quick fixes - to be performed rapidly leading to a quick and easy improvement of the functionality of the existing e-Signature standardisation deliverables, bringing them up to date with current practices.

A high level description of this proposed work and other work planned in response to mandate M/460 are described in the CEN-ETSI joint answer document which is provided as an informative annex to this proposal.

Subsequent phases will be derived from the gap analysis performed separately (in phase 1a) and should include the following activities:

- Development of guidelines for each of the areas of the rationalised framework;
- Supporting the progression of the e-signature specifications through to European Norms (EN);
- Further activities needed to complete the rationalised framework as identified in phase 1a.
- Procedures and practices for conformance assessment and interoperability testing of signature creation and verification systems as well as certification service providers. Also, preparation of interoperability tests events (both remote and face-to-face) of signature creation and verification systems, including the necessary infrastructure.

The proposed work plan on quick fixes is based on an Initial Rationalised Framework structure as proposed in mandate M/460 and taking into account the final deliverables of CROBIES.

An update of the Initial Rationalised Framework structure is proposed as the basis for this Phase 1b proposal. It is expected that this structure will change as a result of the framework activity. It is illustrated below. Identification of the topics where Quick Fixes are considered necessary is indicated by "QFn".

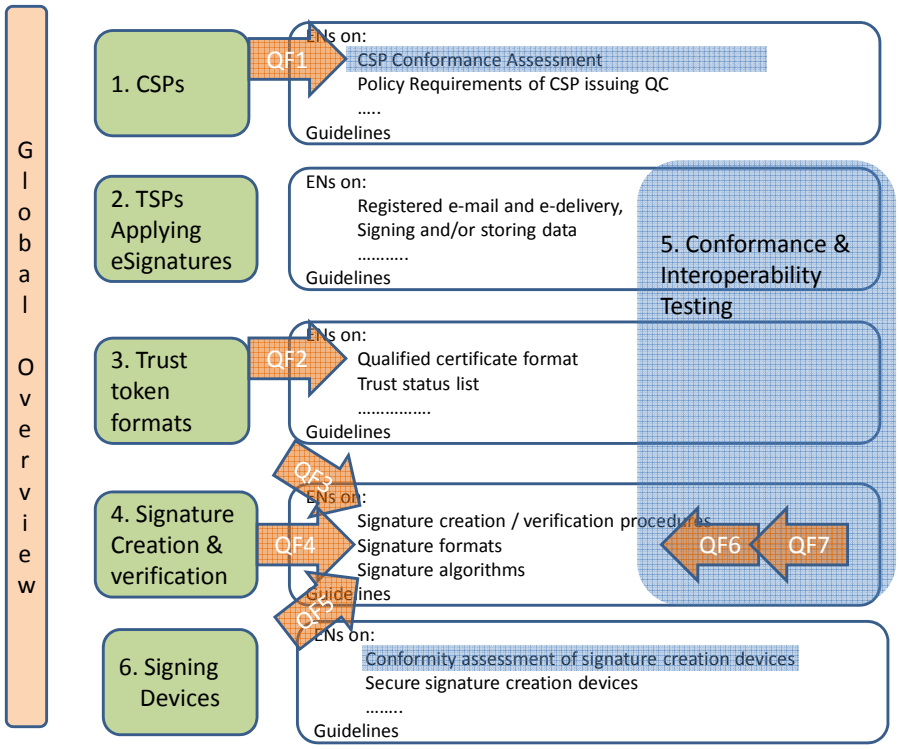


Figure 1 - Illustration of Initial Framework with Quick Fixes

Following consideration of the final deliverables of CROBIES on these areas the following have been identified as requiring "quick fixes" (QF) to be addressed by ETSI in this Phase 1b:

QF1) General Guidance and Requirements on Certificate Service Provider (CSP) conformity assessment

The objective of this quick fix is to produce an ETSI Technical Specification (ETSI TS) updating CWA 14172-2 and CWA 14172-8 to provide a common basis for guidance on conformance assessment, including requirements on auditors, for all forms CSPs including qualified, non-qualified, time-stamp, and validation authorities. This is required to provide a common framework for guidance on CSP Issuing Qualified Certificates (as identified in the deliverable of CROBIES WP1) which can also meet the urgent market need for guidance of conforming assessment of other forms of CSP (e.g. CSP issuing Extended Validation Certificates). This is expected to include the use of auditors' reports with a criteria conformance checklist.

CWA 14172-2, the current EESSI specification for Conformity Assessment Guidance, has expired and the content is out of date. Without this quick fix there will be no common basis of assessment of CSP and further divergence will occur between the national accreditation and supervisory schemes for electronic signatures. This quick fix is needed urgently to provide a common set of requirements for carrying out of audit of CSP issuing qualified certificates (against ETSI TS 101 456) as well as auditing other forms of CSPs (against ETSI TS 102 042 and other similar policy requirements). This is having a significant impact on cross recognition of accredited and supervised CSP both across Europe and internationally (e.g. CA Browser forum Extended validation certificates).

QF2) Interoperable qualified certificate profile

The objective of this quick fix is to update the qualified certificate profile standards ETSI TS 101 862 and ETSI TS 102 280 to address concerns identified in the CROBIES report. This includes issues related to identification of legal and physical entities in relation to these standards as well as updated requirements on current standardized information, which identifies that a certificate is a qualified certificate and to link the certificate with use of a Secure Signature Creation Device (SSCD), which is needed to avoid uncertainty over the acceptability of the signature in relation to legal requirements.

ETSI TS 101 862 and ETSI TS 102 280 are core standards for the implementation of certificates and certification services supporting cross boarder implementations of electronic signatures. Internationally recognized and harmonized qualified as well as non qualified certificates issued to natural as well as legal persons are fundamental to the overall goal to achieve interoperable electronic signatures. The CROBIES study has identified a number of areas of great importance, which need immediate attention. Several core standards on which ETSI TS 101 862 and ETSI TS 102 280 depends, have been updated since their last publication which affects specific information provided in the ETSI standards.

The consequence of not updating the ETSI TS 101 862 and ETSI TS 102 280 is that the process to enhance the interoperability of electronic identity certificates will be delayed and that member states may introduce their own variants which may create barriers which harms interoperability. From the experience gained during the TSL (Trust Status List) Plugtests event held in 2009, a clear lack of semantic interoperability was identified. It was partially mitigated with the introduction of the TSL. The lack of semantic interoperability will worsen unless the requirements for identifying natural and legal person in Qualified Certificate (QC) and non-QC will be fulfilled in a standard and common way.

QF3) Procedures for Signature Verification

The objective of this quick fix is to develop a technical specification specifying how to verify a digital signature within a given policy context. This is required because signature verification is depending on many different standards and other influencing factors and there is currently no common basis for verification. To verify an advanced electronic signature, knowledge of XAdES (XML Advanced Electronic Signature)/CAdES (CMS Advanced electronic signature) or PAdES (PDF Advanced electronic signature) together with standards on TSLs, signature policies or qualified certificates (in addition to basic standards like X.509, CMS or XML-Signature) can be necessary and there is no coherent description of how the different aspects are brought together to make a verification decision, particularly when verifying signature held over the medium to long term. This document will provide requirements for conducting advanced electronic signatures verification.

This Technical Specification is urgently needed to avoid further misinterpretation and the consequent non-interoperability of implementations that results of such misinterpretations. Past interoperability events have made this need obvious: Past AdES (advanced electronic signature) as well as the TSL-Plugtests or, regarding QCs, CROBIES have clearly proven that interoperability is, sometimes even on a basic level, not coming for free.

QF4) Signature algorithms maintenance

The objective of this quick fix is to maintain the guidance on signature algorithms given in ETSI TS 102 176-1. It is important that the maintenance of this guidance is continued due to the progress of cryptographic analysis and the discovery of weaknesses in signature algorithms meaning that use of an old version could lead to potential weaknesses in system depending on this specification.

NOTE: It is planned that a restructuring of the maintenance process and the establishing of a new organisational model for Algo lists (including the identification of the body in charge) according to the CROBIES Proposal in WP 5-3 will be covered in phase 2. The current aim of the phase 2 activities is to standardise the method for maintaining the Algo list in the long term in line with whatever new arrangement is agreed by the EU. It is not necessarily the plan of ETSI to maintain the list in the long term. This quick fix is to keep the current ETSI maintained list up to date in the short term.

The work is to produce three European Norms (ENs) and four ETSI Technical Specifications (TS) as described in section 7 of this proposal.

The estimated total effort for each quick fix and project management is as follows (see section 7 for details of the work breakdown):

QF1: 105 man-days
QF2: 65 man-days
QF3: 90 man-days
QF4: 10 man-days
Project management: 25 man-days

ETSI has submitted two further separate proposals for quick fixes relating to:

- Interoperability and conformance testing ("Phase 1b – ETSI Quick fixes - testing of electronic signatures standards").
- Baseline Profile for AdES formats ("Phase 1b – ETSI Quick fixes to electronic signatures profiles)

4. Market impact

The definition of a rationalised framework for electronic signature standards will allow business stakeholders to easily implement and use products and services based on electronic signatures. It will allow a harmonized use of electronic signatures in line with directive 1999/93/EC and will favour the take up of electronic signature standards by the industry. This will result in a simplified access of enterprises and citizens to cross-border electronic public services. This rationalised framework will provide a long term work plan for the provision of all the standards and guidelines necessary to establish a harmonised framework for simplified access across European borders.

However, some urgent “fixes” are recognised as being necessary to allow the market to work towards an optimal solution in the short term. These fixes will ensure that for those areas of

standardisation where known deficiencies exist in the current set of specifications the deficiencies can be addressed as soon as possible.

Without these quick fixes, areas where full interoperability is not possible will remain for some time and hence further frustration will occur with the full capabilities of electronic signatures not being realised in a timely manner.

Part II – Execution of the work

5. Working method / approach

The work is to be carried out in an ETSI Specialist Task Force (STF) comprising up to 7 experts. The STF will be recruited in accordance with the ETSI Directives and procedures and this will be in line with the Framework Partnership Agreement. Collectively, the STF will need to possess an in-depth established knowledge of the following domains:

QF1) General Guidance and Requirements on CSP conformity assessment:

- Knowledge of IT Audit and security assessment techniques as applied to CSPs.
- Knowledge of policy criteria used as basis of assessment such as ETSI TS 101 456 or ETSI TS 102 042 or CAB Forum Extended Validation certificates as well as in EU projects such as STORK and PEPPOL.
- Knowledge of one or more National CSP assessment schemes.

QF2) Certificate profiles:

- Thorough expertise in the theory and practice of Public Key Infrastructure standards and implementations. In particular expertise in the core IETF X.509 profile RFC 5280 and the IETF Qualified Certificate profile RFC 3739.
- Thorough knowledge of the ETSI Certificate profile standards (TS 101 862 and TS 102 280) is also required.

QF3) Procedures for Signature Verification:

- Thorough knowledge of theory and practice of Public Key Infrastructure standards and implementations.
- Knowledge of X.509, CadES/XAdES/PAdES, signature policies and other related standards is required.

QF4) Signature algorithms maintenance:

- cryptography, electronic signature standardization
- knowledge of ETSI TS 101 176-1

The work will run under one STF led by an STF leader who will be appointed during the set-up of the STF. The STF will report on its activities at each TC ESI meeting (estimated to be 7 meetings over the duration of the action). TC ESI will then ensure that the CEN-ETSI eSign

CG is informed on the progress of the work. When invited, the STF leader may occasionally attend the CEN-ETSI eSign CG meetings to report on specific issues.

The STF will hold face-to-face meetings (probably co-located with TC ESI meetings). Work will be performed in between face-to-face meetings, mainly using virtual meetings with on-line collaborative tools. Discussions with the parent technical body will mainly be carried out over the e-mail list of the TC and at the TC ESI meetings.

In addition to this, the progress of the work will require collaboration with various stakeholders identified as follows (the list is not exhaustive and will be refined at the beginning of the action and reported on in the Interim and Final Reports to the EC/EFTA):

QF1) General Guidance and Requirements on CSP conformity assessment: CSPs, national accreditation and supervisory bodies, CAB Forum, Webtrust, ISO, FISCALIS, the Forum of European Supervisory Authorities for Electronic Signatures (FESA).
QF2) Certificate profiles: IETF, STORK.
QF3) Procedures for Signature Verification: ISO, IETF, W3C, OASIS.
QF4) Signature algorithms maintenance

It is proposed to liaise with stakeholders through contacts of the TC ESI membership as well as regular consultation with the various organizations involved.

STF experts plan to attend the following organizations' meetings: one FISCALIS meeting, one CAB Forum meeting, and one IETF meeting. Meetings with the STORK project, the EU Service Directive expert group and possible other stakeholders will also be organized.

The result of these liaisons and meetings will be discussed within the STF using virtual meeting collaborative means. The work will also include voluntary participation of TC ESI members.

The work of this STF will be coordinated with the activities of the STF concerned with the overall framework for the mandate M/460 through the project management task (see clause 7.6 Phase 1a, Task 5 in the ETSI proposal 2010-10).

Progress reports on the activities and results under this action will be provided to the EC/EFTA as part of the ESO reporting to the CEN-ETSI Coordination Group (on a six monthly basis as required by mandate M/460).

6. Performance indicators

As required, by the grant agreement, information will be provided that will act as performance indicators against the contracted activity in the following cases:

Effectiveness:

Details will be provided, throughout the lifetime of the proposed action, on:

- the number of meetings held in relation to this work:
  - the number of participants;
  - the number of presentations made on the activity by STF members as well as other TC ESI members;
- an evaluation of any feedback received;
- project progress in relation to the schedule specified;

Proposed Benchmarks

a) Reports produced by the STF for TC ESI about the progress of the work, which will be produced for each TC ESI meeting. A report will b produced for each TC ESI meeting held during this activity (expected to be at least 6 reports), plus a 6-monthly report to the CEN-ETSI eSign Coordination Group (expected to be at least 4 reports).

b) Three draft versions of the ETSI deliverables (4 TS and 3 ENs) to be circulated to ETSI TC ESI for comments, namely: an initial draft, a consolidated draft and the final version for public approval.

c) 90% of the tasks and other milestone-related schedule on time (less than 5 days after the planned dates).

Stakeholder engagement:

An analysis will be given of the balance of stakeholder representation in the activity and the number of liaison activities performed

Proposed Benchmarks

a) Contributions received from other stakeholders to the work (these stakeholders are identified in clause 5 of this proposal). It is anticipated that there will be contributions from at least 20 stakeholders.
b) Support by TC ESI plenary to the STF reports. There will be at least 6 reports and the TC ESI plenary will have at least 15 members represented.
c) Comments provided to the draft versions of the ETSI deliverables circulated by the STF. This is expected to be at least 60 technical comments and does not include the Public Enquiry phase comments to the ENs.

Dissemination of results:

Information will be provided on the effectiveness of activities related to the dissemination of project deliverables and efforts made to raise industry awareness of the activity.

Proposed Benchmarks

a) The STF will contribute to relevant conferences/workshops to disseminate the project results identified over the duration of the action. At least 2 submissions will be proposed to conferences/workshops.
b) Regular news (at least 2 editions) will be provided on the ETSI web site and/or portal
c) Press releases will be used to announce the availability of the adopted ETSI TS and ENs (2 anticipated).

7. Work plan, milestones and deliverables

This action proposes the following tasks, deliverables and relation to milestones (T0 = date of signature followed by number of months into the action):

List of Tasks, Deliverables and Milestones					
WP	**Task**	**Task name**	**Deliverable**	**Type**	**Milestone**
		Team set-up			M0
QF1	T1.1	CSP Conformance Information gathering			M1A
	T1.2	CSP Conformance 1st Draft	D1	ETSI TS	M1B
	T1.3	CSP Conformance Consultation and Revision	D1	ETSI TS	M1C, M1D
	T1.4	CSP Conformance Policy Criteria Maintenance	D2, D3	EN	M1C
	T1.5	Application to QC including checklist			M1C
	T1.6	Two-step approval procedure for EN	D2, D3	EN	M1E, M1F, M1G, M1H
QF2	T2.1	EN 301 862	D4,	EN	M2A and M2B
	T2.2	Update of TS 102 280	D5	ETSI TS	M2A and M2B, M2C
	T2.3	Two-step approval procedure for EN	D4	EN	M2D, M2E, M2F, M2G
QF3	T3.1	Identification of relevant standards and use case selection			
	T3.2	Table of content	D6	ETSI TS	M3A
	T3.3	Production of detailed procedures	D6	ETSI TS	M3B, M3C
QF4	T4	TS 102 176-1 Maintenance	D7	ETSI TS	M4A, M4B, M4C

The **Deliverable D1,** work item number **DTS/ESI-000075,** is an ETSI Technical Specification (TS), which contains the deliverables produced in tasks T1.2, T1.3 and T1.5. Its title will be "Electronic Signatures and Infrastructures (ESI); Conformity Assessment requirements and guidance". This document will supersede CEN CWA 14172:2 and CWA 14172-8 which have expired to provide requirements and guidance on conformance assessment of CSPs including CSPs issuing qualified and other forms of certificate, CSPs providing services in support of electronic signatures (e.g. time-stamping). The document will be first published as an ETSI TS for quick availability to market actors. The document will be migrated to EN status in phase 2.

The **Deliverable D2,** work item number **DEN/ESI-000087,** is a European Norm (to be EN 301 456), which contains the deliverables produced in tasks T1.4. Its title is "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates". It defines policy requirements on the operation and management

practices of certification authorities (CAs) issuing qualified certificates such that subscribers, subject certified by the CA and relying parties may have confidence in the applicability of the certificate in support of electronic signatures. This document will be an update and the conversion of ETSI TS 101 456 into an EN (EN 301 456).

The **Deliverable D3,** work item number **DEN/ESI-000088,** is a European Norm (EN 302 042), which contains the deliverables produced in tasks T1.4. Its title is "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates". It defines policy requirements on the operation and management practices of certification authorities (CAs) issuing and managing public key certificates such that subscribers, subject certified by the CA and relying parties may have confidence in the applicability of the certificate in support of cryptographic mechanisms. This document will be an update and the conversion of ETSI TS 102 042 into an EN (EN 302 042).

The **Deliverable D4,** work item number **DEN/ESI-000089,** is a European Norm (EN 301 862), which contains the deliverables produced in tasks T2.1 and T2.2. Its title is "Electronic Signatures and Infrastructures (ESI); Qualified Certificate profile". It defines a profile for Qualified Certificates, based on the technical definitions in RFC 3739, that may be used by issuers of Qualified Certificates complying with Annex I and II of the European Electronic Signature Directive 1999/93/EC. This document will be an update and the conversion of ETSI TS 101 862 into an EN (EN 301 862).

The **Deliverable D5,** work item number **RTS/ESI-000090,** is an ETSI Technical Specification (TS), which contains the deliverables produced in tasks T2.1 and T2.2. Its title is "Electronic Signatures and Infrastructures (ESI); X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons". It is a revision of ETSI TS 102 280 and will address updates in referenced standards as well as concerns identified in the CROBIES report. The need to convert this document to an EN is not obvious at this point in time and will be analysed during the phase 1a. For this reason, ETSI TS 102 280 will remain as an ETSI TS for this phase.

The **Deliverable D6,** work item number **DTS/ESI-000074,** is an ETSI Technical Specification (TS), which contains the deliverables produced in tasks T3.2 and T3.3. Its title is "Electronic Signatures and Infrastructures (ESI); Signature verification procedures and policies". This specification will provide requirements for conducting advanced electronic signatures verification. It will define how the different aspects and related standards are brought together to make a verification decision, particularly when verifying signature held over the medium to long term. This document will supersede CEN CWA 14171 (except aspects related to protection profile that will be addressed by CEN) which has expired.
The document will be published as TS for quick availability to market actors. The possibility to migrate this document to the EN status will be analysed during phase 1a.

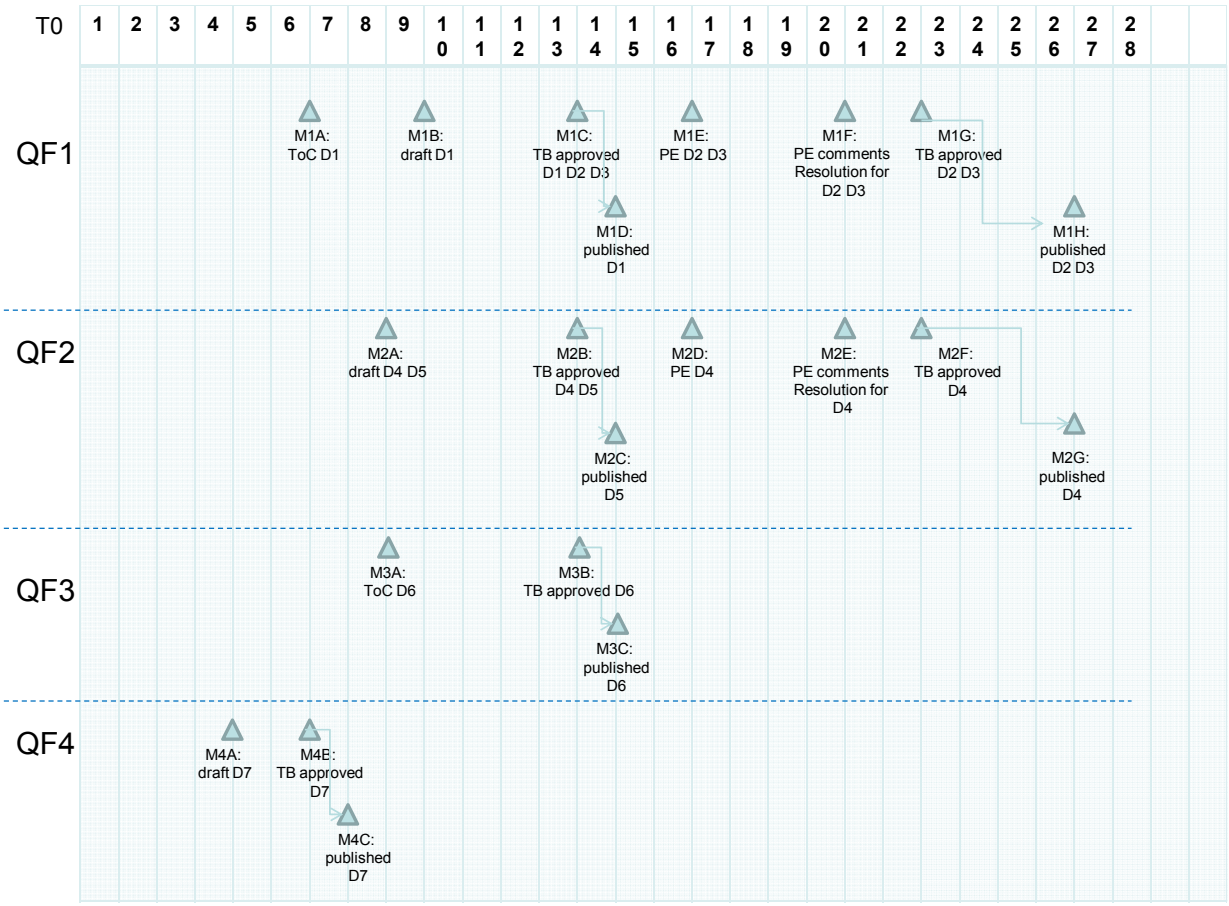
The **Deliverable D7,** work item number **RTS/ESI-000080-1,** is an ETSI Technical Specification (TS), which contains the deliverables produced in tasks T5. Its title is "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms". The document defines a list of hash functions and a list of signature schemes, as well as the recommended combinations of hash functions and signatures schemes in the form of "signature suites".
It is an update of TS 102 176-1 and includes recommendations on signature algorithms. This document evolving on a regular basis, its status remains as an ETSI TS.

The following table and graphic summarises the main time flow and milestones. It assumes a 28 months duration (including the time required to create the STF and recruit/select the experts). The milestone due dates are the number of months elapsed following the start of project).

Final Milestone		*TC approval of Deliverables*
Intermediate Milestone		*Progress Report / Interim Report (IR)*

1	2	3	4	5	6	7	8	9	10	11	12	13
		M0	M4A		M1A M4B	M4C: D7publication	M2A M3A	M1B			Interim Report	M1C M2B M3B

14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
M1D, M2C, M3C: D1, D5, D6 publication		M1E M2D				M1F M2E		M1G M2F				ENs publication		Final report



The outcome of this action will be the provision of an Interim report and a Final Report to the EC/EFTA. The Interim Report will be provided 12 months after the start of the action and will provide a status report on the activity performed along with the latest drafts of the ETSI

deliverables that will be available at this point in time. Full resource usage information will also be provided via the DG Enterprise Cost Control Strategy on EC acceptance of the Interim Report.

The Final Report will be provided to the EC/EFTA 28 months after the start of the action detailing the activity performed since the Interim Report along with the publication versions of the ETSI adopted Technical Specifications and European Norms. The Final Report will also provide an analysis and report on the performance indicators as outlined in clause 6 of this proposal. On acceptance of the Final Report the full resource usage details will also be provided following the DG Enterprise Cost Control Strategy along with the required external audit certificate and declaration of the real costs incurred.

7.1 Phase 1b - Set-up of the STF

Technical experts will be recruited to participate in the STF and the allocation of resources to the tasks will be reviewed and agreed. The bulk of the activity once the selected experts have been contracted will be to agree on the division of responsibilities.

- Planned duration: 3 months.
- Planned timescale: T0 + 3 months following the date of signature of the EC/EFTA grant agreement.

This task will include the Call for Experts. This will be disseminated in an ETSI Collective Letter, distributed by ETSI, and be placed on the web, in order to obtain the widest possible expertise.

7.2 Phase 1b QF 1 - CSP requirements and conformity assessment

The objective of this quick fix is to produce an ETSI Technical Specification updating CWA 14172-2 and CWA 14172-8 to provide a common basis for guidance on conformance assessment, including requirements on auditors, for all forms CSPs including qualified, non-qualified, time-stamp, and validation authorities. This is required to provide a common framework for guidance on CSP Issuing Qualified Certificates (as identified in deliverable of CROBIES WP1) which can also meet the urgent market need to guidance of conforming assessment of other forms of CSP (e.g. CSP issuing Extended Validation Certificates). This quick fix will also address the migration of ETSI TS 101 456 and ETSI TS 102 042 to ENs.

Phase 1b Task 1.1 CSP Conformance Information gathering

This task will involve collection of information on national accreditation / supervisory schemes as well as other relevant international schemes and standards (e.g. CAB Forum, Webtrust, ISO 27000 …). This information will be analysed against CWA 14172 to identify issues to be addressed.

Deliverable D1: Table of content of the draft ETSI TS (DTS/ESI-000075) on General Guidance and Requirements on CSP conformity assessment

Effort: *20 Man days*
Planned timescale: T0 + 6 months

Phase 1b Task 1.2 CSP Conformance 1st Draft

The 1st complete draft of General Guidance and Requirements on CSP conformity assessment will be produced.

Deliverable D1: First complete draft of the ETSI TS on General Guidance and Requirements on CSP conformity assessment for review by stakeholders (national authorities, FISCALIS, CAB Forum).

Effort: *20 Man days*
Planned timescale: T0 + 9 months

Phase 1b Task 1.3 CSP Conformance Consultation and Revision

The first draft will be provided to stakeholders for consultation. The document will be updated based on comments received. The following stakeholders will be targeted as reviewers: national authorities, FISCALIS, CAB Forum.
The consultation will be done by email in addition to attendance to meetings of FISCALIS and CAB Forum.

Deliverable D1: ETSI TS on General Guidance and Requirements on CSP conformity assessment.

Effort: 20 Man days
Planned timescale: T0 + 13 months

Phase 1b Task 1.4 CSP Conformance Policy Criteria Maintenance

The work on CSP conformance may result in the need to update existing criteria for CSPs including ETSI TS 101 456 and ETSI TS 102 042. Those documents will be updated and will be migrated to EN status (EN 301 456 and EN 302 042).

Effort: 16 Man days

Deliverable: TB approved draft EN 301 456 (D2) and draft EN 302 042 (D3).

Planned timescale: T0 + 13 months

Phase 1b Task 1.5 Application to QC including checklist

This work is to apply the general requirements for CSP requirements and conformity assessment to Qualified Certificates. In particular, an auditors' report template, including check list, will be produced for assessment of CSPs issuing qualified certificates as per ETSI TS 101 456.

Effort: 14 Man days

Deliverable D1: Annex to ETSI TS on General Guidance and Requirements on CSP on CSP issuing Qualified Certificates

Planned timescale: T0 + 13 months

Phase 1b Task 1.6 Two-step approval procedure for EN

The TB approved draft ENs 301 456 and 302 042 will go through the two-step approval procedure (i.e. Public Enquiry (lasting 3-4 months) followed by National Voting (2 months).

Effort: 15 man days
Deliverables: published D2 and D3
Planned timescale: T0 + 26 months

Phase1 QF1: Tasks, Activities and Milestones

Task	Activity	Milestone	Experts Man/days
T1.1	CSP Conformance Information gathering	M1A	20
T1.2	CSP Conformance 1st Draft	M1B	20
T1.3	CSP Conformance Consultation and Revision	M1C	20
T1.4	CSP Conformance Policy Criteria Maintenance	M1C, M1D	16
T1.5	Application to QC including checklist	M1C, M1D	14
T1.6	Two-step approval procedure for EN	M1E, M1F, M1G, M1H	15
	Total		105

MILESTONE M1A: end of task 1.1 (T0 + 6 months)
Deliverable:
Table of Contents of ETSI TS General Guidance and Requirements on CSP conformity assessment (D1)

MILESTONE M1B: end of task 1.2 (T0 + 9 months)
Deliverable D1:
D1: 1st draft of ETSI TS General Guidance and Requirements on CSP conformity assessment

MILESTONE M1C: end of task 1.3/1.4/1.5 (T0 + 13 months)
Deliverables D1 D2 D3:
D1: TB approved ETSI TS General Guidance and Requirements on CSP conformity assessment
TB approved draft EN 301 456 (D2) and draft EN 302 042 (D3) for public enquiry

MILESTONE M1D: publication of D1 (T0 + 14 months)

MILESTONE M1E: start public enquiry for D2 and D3 (T0 + 16 months)

MILESTONE M1F: beginning of public enquiry comments resolution for D2 and D3 (T0 + 20 months)

MILESTONE M1G: TB approval of D2 and D3 for vote (T0 + 22 months)

MILESTONE M1H: D2 and D3 publication (T0 + 26 months)

7.3 Phase 1b QF 2 - Certificate profiles

Phase 1b Task 2.1 - Update of ETSI TS 101 862 and conversion to EN 301 862

This task will produce deliverable D4 EN 301 862 which will be a migration of ETSI TS 101 862 with updates. These updates cover:

- General overview, including reference updates
- Updated requirements on indication that a certificate is issued as a qualified certificate (QC)
- Updated requirements on indication that a certificate is associated with a private key that is operated within a Secure Signature Creation Device (SSCD)
- Further certificate profile requirements for qualified certificates issued to natural persons in accordance with input to the rationalized framework.
- Investigating methods for identification of a subject as a legal or physical entity as well as other identity expression aspects.

Deliverable D4: TB approved draft ETSI EN 301 862 for public enquiry
Effort: 30 Man days
Planned timescale: T0 + 13 months

Phase 1b Task 2.2 - Update of ETSI TS 102 280

Production of ETSI TS 102 280 update, which covers;

- General overview, including reference updates.
- Updated requirements incorporated from obsolete standards
- Updated requirements on algorithm support
- Further certificate profile requirements for certificates issued to natural persons in relationship to existing standards framework in accordance with input to the rationalized framework.

Deliverable D5: ETSI TS 102 280 update
Effort: 25 Man days
Planned timescale: T0 + 13 months

Phase 1b Task 2.3 Two-step approval procedure for EN 301 862

The TB approved draft EN 301 862 will go through the two-step approval procedure (i.e. Public Enquiry (lasting 3-4 months) followed by National Voting (2 months).

Effort: 10 man days
Deliverables: published D4
Planned timescale: T0 + 26 months

Phase1b QF2: Tasks, Activities and Milestones

Task	Activity	Milestone	Experts Man/days
T2.1	production of prEN 301 862	M2A and M2B	30
T2.2	Update of TS 102 280	M2A and M2B, M2C	25
T2.3	Two-step approval procedure for EN	M2D, M2E, M2F, M2G	10
	Total		65

MILESTONE M2A: T0 + 8 months
Deliverables D4 and D5:
D4: Draft EN 301 862
D5: Draft update of ETSI TS 102 280

MILESTONE M2B: T0 + 13 months
Deliverables D4 and D5:
D4: TB approved draft EN 301 862 for public enquiry
D5: TB approved TS 102 280

MILESTONE M2C: publication of D5 (T0 + 14 months)

MILESTONE M2D: start public enquiry for D4 (T0 + 16 months)
MILESTONE M2E: beginning of public enquiry comments resolution for D4 (T0 + 20 months)

MILESTONE M2F: TB approval of D4 for vote (T0 + 22 months)

MILESTONE M2G: D4 publication (T0 + 26 months)

7.4 Phase 1b QF 3 - Creation/verification procedures and policies

Phase 1b Task 3 – TS: Procedures for Signature Verification

Description

The objective of this quick fix is to develop a technical specification specifying how to verify a digital signature within a given policy context. This is required because signature verification is depending on many different standards and other influencing factors and there is currently no common basis for verification. To verify an advanced electronic signature, knowledge of XAdES/CAdES or PAdES together with standards on TSLs, signature policies or qualified certificates (in addition to basic standards like X.509, CMS or XML-Signature) can be necessary and there is no coherent description of how the different aspects are brought together to make a verification decision, particularly when verifying signature held over the medium to long term. This document will provide requirements for conducting advanced electronic signatures verification.

An important point is to take requirements on signature algorithms into account: how to support the creation and validation processes with information on algorithm/key length strength resp. weaknesses. This will deal with questions like how to handle validation on a date beyond which use of the algorithm or key length used is not recommended. Since this is

a complex topic that has not been considered so far, we will focus in this phase on how to tackle the problem.

This task will include the following activities:

1) Identification of relevant standards that provide input into the specification. Some of these standards will be standards developed by other standardisation organisations like ISO, IETF, W3C or OASIS. Example use cases will be identified and existing specified procedures examined against these use cases to identify specific issues that need to be addressed. From this analysis, a decision on how to deal with such standards will then be taken.
2) Development of an outline for the document. Decision on which points of the outline to be filled in this phase at which level and which to be filled later.
3) Production of the detailed procedures.

Deliverable
D6 ETSI TS – Procedures for Signature Verification (DTS/ESI-000074)

Effort
90 Man Days
Planned timescale: T0 + 13 months

Phase1b QF3: Tasks, Activities and Milestones

Task	Activity	Milestone	Experts Man/days
T3.1	Identification of relevant standards and use case selection		30
T3.2	Table of content	M3A	10
T3.3	Production of detailed procedures	M3B, M3C	50
	Total		90

MILESTONE M3A: End of Task 3.2 (T0 + 8 months)
Deliverable D6:
Table of content – TS Procedures for Signature Verification

MILESTONE M3B: End of Task 3.3 (T0 + 13 months)
Deliverable D6:
TB approved TS Procedures for Signature Verification

MILESTONE M3C: publication of D6 (T0 + 14 months)

7.5 Phase 1b QF 4 - Signature Algorithms

Phase 1b Task 4 – ETSI TS 102 176-1 Maintenance

Description
The objective of this quick fix is to maintain the guidance on signature algorithms given in ETSI TS 102 176-1. It is important that the maintenance of this guidance is continued due to the progress of cryptographic analysis and the discovery of weaknesses in signature algorithms meaning that use of an old version could lead to potential weaknesses in system depending on this specification.

ETSI TS 102 176-1 must be maintained due to the progress of cryptographic analysis and the discovery of weaknesses in signature algorithms until final conclusion is reached on long term provision of guidance on algorithms for electronic signatures.

Deliverable:

- ETSI TS 102 176-1 with updated security parameters and time tables for appropriate signature algorithm suites (work item RTS/ESI-000080-1)

Effort*: 10 Man Days*
Planned timescale: T0 + 6 months

Phase1b QF4: Tasks, Activities and Milestones

Task	Activity	Milestone	Experts Man/days
T5	TS 102 176-1 Maintenance	M4A, M4B, M4C	10
	total		10

MILESTONE M4A: T0 + 4 months
Deliverable D7:
Draft TS 102 176-1

MILESTONE M4B: T0 + 6 months
Deliverable D7:
TB approved TS 102 176-1

MILESTONE M4C: T0 + 7 months, published D7

7.6 Phase 1 Technical project management

The STF leader will coordinate the different tasks of this action. He/she will prepare the reports to TC ESI and the interim and final reports for EC/EFTA.

Effort*: 25 Man Days*

Deliverable: Progress reports at major milestones.