Project proposal
eSign Phase 1B – "Quick-fixes"

1. Context

This proposal is submitted in the frame of the standardization mandate M/460 to the ESOs in the field of information and communication applied to electronic signature.

It is part of a common response from CEN and ETSI with regards to phase 1 of this mandate.

The different phases of the answer to the mandate, the split of responsibilities between CEN and ETSI and the CEN ETSI coordination are described in the CEN-ETSI joint response document.

The European Commission Mandate M/460 invites the European Standardisation Organisations (ESOs) - CEN, CENELEC and ETSI – to prepare a coherent set of standards, specifications and guidelines in a rationalized European eSignature standardization framework to achieve the interoperability of eSignature at intra-community level.

CEN and ETSI have formally accepted the Mandate. CENELEC did not accept the Mandate and therefore will not take part in standards developments under this particular Mandate.

CEN and ETSI will develop standards (EN) and technical specifications and guidelines requested as far as possible within the timescale required in the Mandate.

Mandate M/460 requires the definition of a rationalized European eSignature standardization framework comprising at least a global overview of the framework with relationship between the eSignature Directive requirements and the standards, information on how to address the signatures standards, implementation guidelines and conformity assessment guidance.
CEN and ETSI have agreed to jointly develop the response and work programme under this Mandate.

2. Objectives and impact

2.1 Objectives

The objective of the proposal is to develop within CEN/TC 224 standards in response to urgent needs required by the electronic signature market grow in Europe, as well as several European regulations such as the EC electronic invoicing directive and the implementation of the EC services directive and the EC Data Protection Directive.

This proposal is part of CEN ETSI coordinate response to the standardization mandate M/460 to the ESOs in the field of information and communication technologies applied to electronic signatures.

This proposal refers to phase 1b which aims to respond to urgent needs and represent CEN proposal to cower phase 1b in complement to CEN proposal in response to urgently update the standards listed by Decision 2003/511/EC.

As it is focussed to some urgent needs (phase 1b), this proposal does not take into account possible new proposals that the ESOs would identify in preparing a standardization Work Program in response to the mandate.

Furthermore, it shall be recognised that the evaluation and certification of the Protection Profiles shall be done in accordance to the current version 3.1 of Common Criteria within a certificate authorizing CC-Certification Scheme.

2.2 Relevance

The work plan proposed in this document addresses the Electronic Signature Mandate M/460 requirement for a “rationalised European eSignature standardisation framework”.

It specifies in detail the contribution of CEN in phase 1a aimed at defining the structure for the rationalised framework for e-signature standardisation, in line with the description of Mandate M/460 first aims (clause 2.2).

The different phases of the answer to the mandate, the split of responsibilities between CEN and ETSI and the CEN ETSI coordination are described in the CEN-ETSI joint response document.

As of today the electronic signatures standardization landscape is rather complex and does not offer a clear mapping with the requirements of directive 1999/93/EC on a community framework for electronic signatures. The current multiplicity of standardisation deliverables together with the lack of usage guidelines, the difficulty in identifying the appropriate standards and lack of business orientation is detrimental to the interoperability of electronic signatures. Also because many of the documents have yet to be progressed to full European norms, their status may be considered uncertain.

The certification of the relevant PPs is a major enhancement of the upcoming standards in the market. Products certified against these PPs can proof the fulfilment of relevant security requirements of the e-signature directive 1999/93/EC.

Therefore, the evaluation and certification according to Common Criteria is a necessary pre-condition for the use of the update standards within the framework of e-signatures.

The different phases of the answer to the mandate, the split of responsibilities between CEN and ETSI and the CEN ETSI coordination are described in the CEN-ETSI joint response document.

2.3 Indicators

1) At each Step (CEN Enquiry and Formal Enquiry):
Number of countries expressing a vote: at least 5
Result of the vote: Positive

Through the CEN rules, the members of CEN/TC 224 are committed to involve all stakeholders, including Member States, in the formal review and approval of the draft deliverables.

2) The minimum number NSB represented at CEN TC 224 Meeting will be: 4

3) Progress report provided to the Commission every 6 months and especially at month 6, 12 and 18

2.4 Impact

A certified PP-SSCD will be used in the European e-signature market to prove the compliance of SSCDs to the requirements of the e-signature directive. At the time being, PPs following an older version of the CC are already in use. The older version for CC can soon not be used any longer for evaluation and certification of SSCDs. Therefore, a certified PP-SSCD based on the current CC-version is needed urgently.

If no certified PP-SSCD exists, formal compliance to the Protection Profile cannot be shown.

The impact of the proposed standards will be important as it address urgent needs required by the development and the harmonisation of growing markets such as:

- Electronic secure mail server which permit mail can not be repudiated with massive implementations in some European countries that would be developed at short term in support to new national regulations (national transposition of EC Directives like the DIRECTIVE 2009/136/EC)

3. Description of the different tasks

3.1 Introduction

As of today the electronic signatures standardization landscape is rather complex and does not offer a clear mapping with the requirements of directive 1999/93/EC on a community framework for electronic signatures. The current multiplicity of standardisation deliverables together with the lack of usage guidelines, the difficulty in identifying the appropriate standards and lack of business orientation is detrimental to the interoperability of electronic signatures. Also because many of the documents have yet to be progressed to full European norms, their status may be considered uncertain.

It resulted in a lack of truly interoperable e-signature applications and in a lack of trust in the existing framework. We particularly face problems with the mutual recognition and cross-border interoperability of electronic signatures. A few interoperability events have been held. These have yet to be developed to the extent that they provide full conformance tests and cover all areas of standardization.

3.2 Scope

The answer to mandate M/460 is divided in two phases:

- Phase 1 will define primarily the rationalized framework with a gap analysis and a resulting final work programme. Phase 1 will also address issues which urgently need an update.

- Phase 2 will implement the final work programme as defined in Phase 1.

3.2.1. Phase 1

Phase 1 is composed by actions related to the development of a rationalised framework (phase 1a) and actions of standardization related to response to urgent needs (phase 1b).

3.2.1.1 Phase 1a – Rationalized Framework

Phase 1a is aimed at establishing a structure for a rationalised framework for electronic signature (eSignature) standardisation. This will include the following activities:

1. Inventory of eSignature standards;

2. Rationalised structure for the European e-signatures standardisation documents;

3. Gap analysis – assessment of the existing e-signatures standardisation deliverables and future work plan.

Phase 1a is not addressed by the present proposal.

3.2.1.2 Phase 1b – Quick fixes

Phase 1b is related to "quick fixes" which consist for CEN into two actions:

- CEN/TC 224 proposal for updating standards that are referred in the context of Commission Decision 2003/511/EC of 14.7.2003 "*on the publication of reference numbers of generally recognised standards for electronic signature products […]*" which is attended to be updated

- Additional CEN "quick fixes" in response to identified urgent needs which do not enter into the packages of CEN/TC 224 standards needed to be developed in the context of an update of Commission Decision 2003/511/EC of 14.7.2003 "*on the publication of reference numbers of generally recognised standards for electronic signature products […]*"

The detail of theses actions is as follows:

3.2.1.2.1 Quick fixes needed for reference in the context of revision of Commission Decision 2003/511/EC of 14.7.2003

It consists into the content that CEN has submitted as a separate proposal in the context of the ICT 2010-2013 CEN/CENELEC Work program. It forms a response to the need to establish updated normative references that may be used for a revision of the Commission Decision 2003/511/EC of 14.7.2003 "on the publication of reference numbers of generally recognised standards for electronic signature products.

Following a request of the EC, this content – not described hereafter as it is a separate proposal - may be understood as an independent selfconsistent proposal but it may also be incorporated as part of CEN quick fixes phase 1b response with regards to the coordinated CEN ETSI response to mandate M/460.

*Context Note: The Commission Decision 2003/511/EC of 14.7.2003 "on the publication of reference numbers of generally recognised standards for electronic signature products […]" complements article 3.5[1] of the Directive 1999/93/EC on a Community framework for electronic signatures (the Directive). The Decision lists three "**Generally Recognised Standards**" for electronic signature products that Member States shall presume are in compliance with the requirements laid down in:*

**** Annex II f** to the Directive (i.e. security of Certification Services Providers):*

- *— **CWA 14167-1 (March 2003):** security requirements for trustworthy systems managing certificates for electronic signatures — Part 1: System Security Requirements*
- *— **CWA 14167-2 (March 2002):** security requirements for trustworthy systems managing certificates for electronic signatures — Part 2: cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)*

**** Annex III** (i.e. security of signature creation device like smartcards):*

- *— **CWA 14169 (March 2002):** secure signature-creation devices (SSCD).*

---

1 Art. 3.5: "*The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards*."

The three standards listed by Decision 2003/511/EC were produced in the framework of the EESSI. They were then assigned together with other CWAs by CEN/BT to CEN/TC224 for their maintenance and their conversion as ENs. At the time being, CEN/TC224/WG17 in charge among others of the update of these three particular CWAs was not able to complete its task due to limited resources.

3.2.1.2.2. Additional CEN "quickfixes" in response to identified urgent needs which do not enter into the packages of standards needed for reference by a revision of Commission Decision 2003/511/EC of 14.7.2003

As explained previously, with respect to the EC request to distinguish as a self consistent proposal the set of standards to be establish as a response in relation with revision of Commission Decision 2003/511/EC of 14.7.2003, a limited additional work is proposed and described here after to cower urgent market needs which do not enter into packages of standards necessary to be used for reference by a revision of the EC decision:

1. Establishement of new standards and related to server signing

   The needs for security requirements for server Signing Operations, i.e. advanced electronic signatures made by a server rather than a human being cower Applications requiring using such devices for secure signing include eInvoicing, eProcurement and other services under the Service Directive (2006/123/EC).

   These security requirements shall be developed as a separate standard of CSP security requirements standard, nevertheless to be included into the 14167 series.

   However, it may be recognised that some security requirements may apply either to a CSP or to a "signing server" such as those requirements that apply to the cryptographic module. Definition of signing server security requirements may then impacts several standards (14167 series) that need to be develop for responding to the context of revision **of** Commission Decision 2003/511/EC of 14.7.2003 (see 3.1.2.1).

   This financial proposal concentrated only on the part specific for server signing which is expected to become a new standard, as a new part of 14167 series. Furthermore this work need also to develop requirements related to the other parts of 14167 (2, 3 and 4), in relation with server signing needs. It may be consolidated that the work needed to update these standards will be taken in to account in the context of EC decision without supplementary resources *.

   * This suppose however that the proposal CEN phase 1b " Quick fixes needed for reference in the context of revision of Commission Decision 2003/511/EC of 14.7.2003" is accepted.

Note: the work of the current proposal (2010-33) is depending on the work carried on TS 14167 part 2 to 4 in the CEN project proposal 2010-31. On the contrary, the proposal 2010-31 could be carried even if 2010-33 is not accepted.

3.2.2. Phase 2

Phase 2 is not addressed by this proposal. A general overview on phase 2 may be found in the Joint CEN ETSI Report in response to the Mandate M/460 that gives a first description of expected actions related to phase 2).

3.3 Workplan & Milestones

3.3.1 Overview

The work consists in:

Item A) completing the different standards listed by CEN/TC 224/WG 16 and CEN/TC 224/WG 17 which are not at the same level for each document, the objective is to publish ENs for well advanced documents and to publish TSs for the other ones. As the final objective is to have ENs, all documents published as TSs will be immediately converted as ENs in a fast track process with no update of the text within phase 2.

Item B) ensuring evaluation of produced documents that are protection profiles for certification purpose. This work will be assumed by evaluation facilities and certification agencies external to CEN.

PT B is mentioned in reference to the other proposals being understood that the new part of 14167 cowered by that proposal does not require CC evaluation.

3.3.2 Rational and detailed program of work

Experts of CEN/TC224/WG17 are currently working on standard 14169 split in 6 parts (an introductory one followed by five protection profiles). This decision was taken because it is easier to handle several protection profiles covering different situations, especially for their evaluation and certification. Consequently, the drafting work related to 14169 is on the way to be completed

Regarding CWA 14167 parts 1 and 2, CEN/TC224/WG16 has not yet started their update due to the limited resources of the working group. As part 2 was further split in parts 2 and 4 after the publication of the Decision, update of CWA 14167-4 has to be achieved too. Moreover, in the framework of the splitting proposed for the future 14169 standard, SSCD type 1 of the original CWA 14169 is no more covered and it would make more sense to address it in the framework of the update of CWA 14167-3 and to merge 14169 type 1 with 14167-3. As a consequence, update of CWA 14167-3 has to be included in this application too.

With regards to the two new items aims by that proposal, these different parts impacted are listed hereafter. It is indicated whether the EN status is possible to get in a limited time and when an evaluation and certification is needed.

Work Item	**Title**	Item A **Status to be obtained through the action**	**Item B** **Common Criteria Evaluation needed**
14167 -1 **	**Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signature**	**CEN TS**	**No**
14167 -2 *	**Cryptographic module for CSP signing operations with backup-protection profile - CMCSOB-PP***	**CEN TS**	**Yes**
14167 -3 *	**Cryptographic module for CSP key generation services – protection profile – CMCKG-PP***	**CEN TS**	**Yes**

14167 -4 *	**Cryptographic module for CSP signing operations -protection profile - CMCSO-PP***	**CEN TS**	**Yes**
14167 -x	**Secure requirements for server signing**	**New CEN TS**	No

**incorporation of security requirements related to the use of CSP and/or other servers for responding to secure signing server needs and particular application for certificate generating*

** indicated for information and coherence only – no specific need related to server signing as security requirement will be included into a new part

3.3.3 Tasks

The work will comprise several steps (see part 8 of this application for a complete timetable) including:

a) drafting by PT A and circulation within WG17
b) resolution(s) from TC224 that the Protection Profiles are ready for evaluation (except for 14167-1)
c) insertion of comments by PT A and circulation within WG17
d) Evaluation and certification of Protection Profiles by PT B
e) CEN vote
f) incorporation of possible CCMC comments by PT A
g) publication of the EN/CEN TS standard

Once all comments are incorporated, the evaluation and certification process will be halted temporarily and the WG draft will be submitted to CEN for vote. (end of step e).

In step f) necessary changes induced by comments coming from CMC will be performed by PT A.
The objective is to have European Standards and certificates for Protection Profiles at the end of the process.

3.3.4 Timetable

A roadmap has already been produced by CEN/TC224 in order to accommodate the standardisation process and the evaluation/certification process of Protection Profiles.

Among the different possible options for the sequences of the steps of both processes, the one selected and described below intends to:

- ✓ Avoid the cost of a second evaluation by presenting a stable draft already commented by CEN Members;
- ✓ Optimise the standardisation process by initiating the CEN votes after the evaluation step.

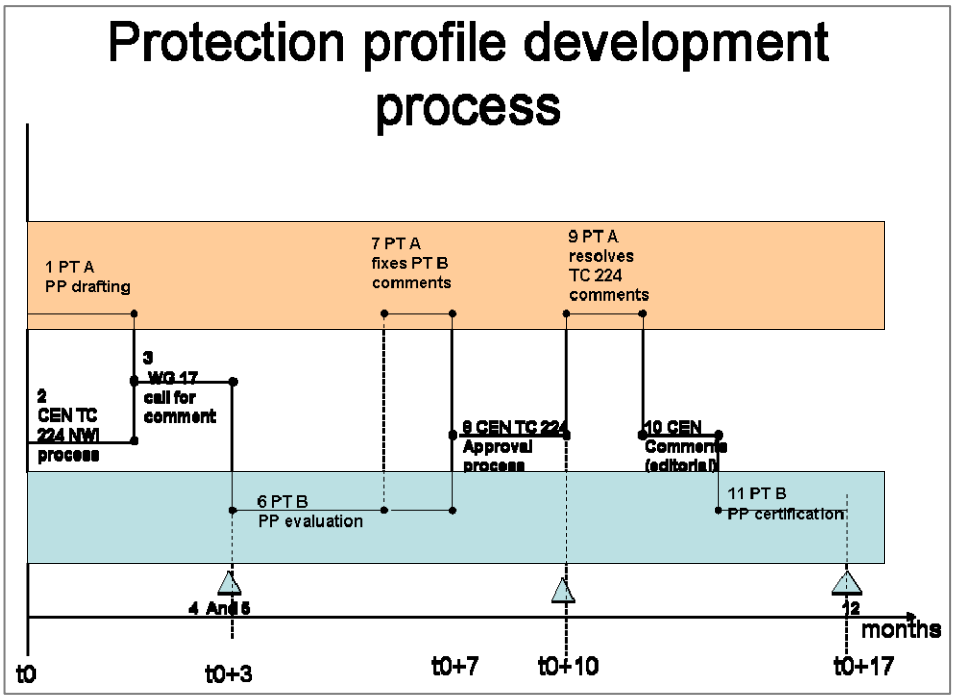
This roadmap will be used by WG 16/ resp. WG 17 and the TC 224 secretary for their actions and will be circulated for information by WG 16/ resp. WG 17 to the different actors involved in the evaluation/certification process.

3.3.5 Roadmap for obtaining CEN TS

Step #	Item	Duration
1	The protection profile is drafted/finalised by PTA. The PP is drafted with the CEN template.	
2	The NWI is ideally launched during this period of time in order to start the CEN timeframe matrix as late as possible.	
3	After approval of the NWI, a call for comments within WG 17 will be launched.	2 months
4	After WG 17 decision, then WG 17 will circulate the draft PP within TC 224 in order to inform that the PP is ready for evaluation. Comments from TC 224 are highly encouraged during this step. Comments in later steps may have a negative impact on the timing of the project.	1 month
5	WG17 applies on behalf of TC 224 as the formal developer for certification. TC224 secretariat is copied for information.	
6	Evaluation and certification (stage 1) by PT B. Comments sent to WG17 are circulated to TC 224 for information.	4 months (incl. step 8)
7	Comments fixed by PT A.	
8	CEN TC approval	3 months
9	Comments made during TC approval are resolved by PT A.	2 months
10	Incorporation of possible CEN Management Centre comments. CMC will have to halt the publication process. With this end the new draft will not be sent to CMC at the completion of step 13 but at step 15.	2 months
11	Evaluation and certification (stage 2) and certificate issued No further changes by CMC are possible.	3 months
12	Publication of the TS.	

3.3.6 Time schedule

Work of these two new parts may be initiated together with work on 14167 such as all the actions related to development of CEN TS through phase 1b may require 17 months.



To ensure resulting standards be available in time with publication of the revised decision, all this action will be developed in 18 month with resulting deliverables as CEN TS [2]

3.4 Deliverables

The 3 progress reports will contain:
The status of development of each deliverables at the moment of the issue of the progress report

Note : due to the long voting procedure all the documents will be processed in parallel at the same time and not in a queue

The final deliverables will be:

Publication as TS of one document.

- TS 14167-part x : Secure requirements for server signing

Contribution to others parts of 14167 as mentioned.

4. Execution of the different tasks

4.0 Organisation & relationship

[2] The conversion of CEN TS into EN may be part of further work to be done through the mandate

CEN/TC 224 will be responsible for the technical monitoring of the drafting performed by PT A. Evaluation and certification must be done by experts that are different from the drafting experts for the reason of independence. No co-ordination with other working groups will be necessary.
As tasks of both PT A and PT B are closely connected, CEN/TC 224 will also be responsible of their coordination.

- Project Team A will be appointed to finalize the drafting of European standards (CEN/ENs or CEN/TSs) by a team of 3 to 6 experts (item A)

- Project Team B will be in charge of the evaluation and certification of the Protection Profiles (Item B).