

# Technical Proposal

**Title : Phase 1b – ETSI Quick fixes to electronic signatures profiles**  
**Specific agreement number : SA/ETSI/ENTR/460/2010-11**  
**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 Domain 5 (Electronic Signatures) of the EC’s 2010 to 2013 ICT Standardisation Work Programme.

A joint ETSI / CEN programme for implementing mandate M/460 is described in the document "Joint CEN-ETSI response to mandate M/460".

This identifies the need for certain actions to be carried out urgently within a general programme to establish a framework for electronic signature referred to as “phase 1b – ETSI quick fixes”. The “quick fixes” work plan is primarily aimed at providing urgent 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.

In implementing the Services Directive (Directive 2006/123/EC) the need has been identified for the use of Advanced Electronic Signatures (AdES) across Europe. For this to be achieved consistently across Europe, a common profile needs to be established for the use of AdES by EU member states.

### 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 one of a number of “quick fixes” to ensure that the deficiencies identified in studies 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. Separate proposals are being submitted for a rationalised framework and other quick fixes by ETSI and CEN, within a 4 year programme to complete the rationalised framework.

In implementing the Services Directive (Directive 2006/123/EC) the urgent need has been identified for the profiles for the use of Advanced Electronic Signatures (AdES) across Europe. It is most urgent to identify common requirements for the direct exchange of signed information across Europe, but it is also necessary to identify the further requirements needed to maintain the validity of the signatures over the long term.

### **3. Objective**

In line with mandate M/460 this technical proposal covers Urgent Quick fixes - to be performed very 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.

The objective of this action is to specify a Baseline Profile (ETSI Technical Specifications) for all the Advanced Electronic Signatures, i.e. CAdES, XAdES, PAdES and Associated Signatures, which corresponds to the minimum basic requirements in the context of the “Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market” (EU Services Directive henceforth), and provide the same basic features with minimal number of options or no options at all. This is required because there is a clear need to specify the Baseline Profile for AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the Services Directive.

This action will result in the publication of eight ETSI Technical Specifications, whose contents are further detailed in section 7 of this proposal.

This activity will fit in the joint CEN-ETSI programme under mandate M/460 to establish a rationalised framework for electronic signatures as described in the "Joint CEN ETSI response to mandate M/460" document.

## **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.

Of particular concern for ensuring interoperability across Europe for applications such as the implementation of the Services Directive, as well as use for business applications such as eInvoicing, is the definition of common profiles for the use of Advanced Electronic Signatures (AdES).

## **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 4 experts. Collectively, the STF will need to possess an in-depth established knowledge of the following areas:

- Deep knowledge for each of the following specifications: ETSI TS 101 733, ETSI TS 101 903, ETSI TS 102 778.
- Expertise in ETSI TS 102 704, ETSI TS 102 904.
- Expertise in implementation of the aforementioned specifications.
- Knowledge of the Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market and of the implementing measures based on Article 8 of the Directive.

The four experts will be collectively involved in the scoping, requirements gathering and fulfilment mechanisms definition tasks. This will ensure that coherence is maintained across all of the developed ETSI TS.

Each of the four experts will be appointed as the chief editor of the two documents defining one of the profiles (i.e. work items DTS/ESI-000091 and RTS/ESI-000103; DTS/ESI-000092 and RTS/ESI-000104, DTS/ESI-000093 and RTS/ESI-000105; or DTS/ESI-000094 and RTS/ESI-000106).

The work will run under one STF recruited following the procedures in the ETSI Directives. It will be 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 3 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 will 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 but possibly in working sessions to be hosted at the ETSI HQ premises). Work will be performed in between face-to-face meetings, mainly using virtual meetings with on-line collaborative working tools. Discussions with the technical body will mainly be carried out over the e-mail list of the TC and at the TC ESI face-to-face meetings. In addition to this, the progress of the work will require collaboration with the EU Service Directive expert group and other stakeholders to be identified at the beginning of the work.

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

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.

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 eSign 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 by the STF experts or ETSI TC ESI members on the activity;
- an evaluation of any feedback received from stakeholders (as outlined in the paragraph on stakeholder engagement below);
- project progress in relation to the schedule specified;

### **Proposed Benchmarks**

- a) 3 progress reports produced by the STF for TC ESI about the progress of the work, which will be produced for each TC ESI meeting for the duration of the action, plus a minimum of 2 reports to the CEN-ETSI eSign Coordination Group.
- b) A first version of the ETSI deliverables (4 ETSI TS) without the long-term properties to be circulated to ETSI TC ESI for approval at the end of Phase 1.
- c) The revised version of the ETSI deliverables (4 ETSI TS) with the long-term properties to be circulated to ETSI TC ESI for approval at the end of Phase 2.
- d) 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 (including the Services Directive expert group, major EU piloting projects dealing with electronic signatures, international standardisation organisations – IETF, OASIS, W3C – and industry).

### **Proposed Benchmarks**

- a) At least 15 contributions received from other stakeholders to the work
- b) Support by TC ESI plenary to the STF reports in 3 TC ESI plenary meetings (15 to 20 attendees).
- c) At least 40 comments provided to the draft versions of the ETSI deliverables circulated by the STF to stakeholders.

### **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) Preparation of at least one paper to be presented to relevant conferences/workshops.
- b) Regular news (at least 2 editions) will be provided on the ETSI web site and/or portal and to the common web site developed and hosted by a CEN National Member.

## 7. Work plan, milestones and deliverables

The work will be divided in three phases, namely:

1. Phase 0: set up of the STF.
2. Phase 1: Baseline Profiles without long-term related properties.
3. Phase 2: Complete Baseline Profiles including long-term related properties.

Phases 1 and 2 will include two tasks each. The table below provides details of proposed tasks, deliverables, milestones, relation of deliverables to milestones, and milestones descriptions.

List of Tasks, Deliverables and Milestones					
Task	Task name	Deliverable	Type	Milestone	Milestone Description
T0	Team set-up			M0	Set up of the STF
T1.1	Gathering Requirements for AdES Signatures Baseline Profiles			M1a	Progress Report to TC ESI, including gathered requirements.
T1.2	Production of AdES and Associated Signatures Baseline Profiles without long-term related properties	D1 D2 D3 D4	ETSI TS	M1c /IR	Draft for approval of V1 profiles.  Interim Report to EC/EFTA
		Interim Report to EC/EFTA	Report to EC/EFTA		
T2.1	Gathering Requirements for Long Term AdES Signatures Baseline Profiles			M2a	Progress Report to TC ESI, including gathered requirements.
T2.2	Production of AdES and Associated Signatures Long Term Baseline Profiles	D5 D6 D7 D8	ETSI TS	M2d/FR	Published ETSI TSs of V2 baseline profiles for XAdES, CAdES, PAdES and Associated Signatures.  Final Report to EC/EFTA
		Final report to EC/EFTA	Report to EC/EFTA		

### Tasks, Deliverables and Milestones

The **Deliverable D1**, work item number **DTS/ESI-000091**, is an ETSI Technical Specification (TS).

Its title is "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile". It will be published as v1.1.1 and will be the first version without the long-term related properties. The scope of this deliverable is a profile of ETSI TS 101 903, XML Advanced Electronic

Signatures (XAdES), addressing requirements for pan-European use of electronic signatures including support of the Services Directive (Directive 2006/123/EC), for direct exchange of signed information.

The **Deliverable D2**, work item number **DTS/ESI-000092**, is an ETSI Technical Specification (TS).

Its title is "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile". It will be published as v1.1.1 and will be the first version without the long-term related properties. The scope of this deliverable is a profile of ETSI TS 102 778, PDF Advanced Electronic Signatures (PAdES), addressing requirements for pan-European use of electronic signatures including support of the Services Directive (Directive 2006/123/EC), for direct exchange of signed information.

The **Deliverable D3**, work item number **DTS/ESI-000093**, is an ETSI Technical Specification (TS).

Its title is "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile". It will be published as v1.1.1 and will be the first version without the long-term related properties. The scope of this deliverable is a profile of ETSI TS 101 733, CMS Advanced Electronic Signatures (CAdES), addressing requirements for pan-European use of electronic signatures including support of the Services Directive (Directive 2006/123/EC), for direct exchange of signed information.

The **Deliverable D4**, work item number **DTS/ESI-000094**, is an ETSI Technical Specification (TS).

Its title is "Electronic Signatures and Infrastructures (ESI); Associated Signatures Baseline Profile". It will be published as v1.1.1 and will be the first version without the long-term related properties. The scope of this deliverable is a profile of ETSI TS 102 918, Associated Advanced Electronic Signatures (to be published by end 2010), addressing requirements for pan-European use of electronic signatures including support of the Services Directive (Directive 2006/123/EC), for direct exchange of signed information.

The **Deliverable D5**, work item number **RTS/ESI-000103**, is an ETSI Technical Specification (TS).

Its title is "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile". It is a revision of the ETSI TS produced by **DTS/ESI-000091** and will be published as v2.1.1. The scope of this deliverable is a profile of ETSI TS 101 903, XML Advanced Electronic Signatures (XAdES), addressing requirements for pan-European use of electronic signatures including support of the Services Directive (Directive 2006/123/EC), for direct exchange of signed information. This version will add the long-term related properties.

The **Deliverable D6**, work item number **RTS/ESI-000104**, is an ETSI Technical Specification (TS).

Its title is "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile". It is a revision of the ETSI TS produced by **DTS/ESI-000092** and will be published as v2.1.1. The scope of this deliverable is a profile of ETSI TS 102 778, PDF Advanced Electronic Signatures (PAdES), addressing requirements for pan-European use of electronic signatures including support of the Services Directive (Directive 2006/123/EC), for direct exchange of signed information. This version will add the long-term related properties.

The **Deliverable D7**, work item number **RTS/ESI-000105**, is an ETSI Technical Specification (TS).

Its title is "Electronic Signatures and Infrastructures (ESI); CAAdES Baseline Profile". It is a revision of the ETSI TS produced by **DTS/ESI-000093** and will be published as v2.1.1. The scope of this deliverable is a profile of ETSI TS 101 733, CMS Advanced Electronic Signatures (CAAdES), addressing requirements for pan-European use of electronic signatures including support of the Services Directive (Directive 2006/123/EC), for direct exchange of signed information. This version will add the long-term related properties.

The **Deliverable D8**, work item number **RTS/ESI-000106**, is an ETSI Technical Specification (TS).

Its title is "Electronic Signatures and Infrastructures (ESI); Associated Signatures Baseline Profile". It is a revision of the ETSI TS produced by **DTS/ESI-000094** and will be published as v2.1.1. The scope of this deliverable is a profile of ETSI TS 102 918, Associated Advanced Electronic Signatures (to be published by end 2010), addressing requirements for pan-European use of electronic signatures including support of the Services Directive (Directive 2006/123/EC), for direct exchange of signed information. This version will add the long-term related properties.

The work plan includes 2 months at the start for setting up the STF and a further two months at the end for the full approval and publication of the documents. The duration of this proposed action is estimated to be 14 months. The following legend summarizes the codes found in the table showing the timing of the project.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Phase 0 Milestone		M0												
Phase 1 Activities					M1a		M1b	M1c		M1d				
Phase 2 activities									M2a		M2b	M2c		M2d
Progress report								IR						FR

Milestones (at end of month)

- M0 – STF Setup complete
- M1a – Requirements gathering complete
- M1b – D1 to D4 Draft ready for final approval
- M1c – D1 to D4 Approved by ESI
- M1d – D1 to D4 Published
- M2a – Requirements gathering complete
- M2b – D5 to D8 Draft ready for final approval
- M2c – D5 to D8 Approved by ESI
- M2d – D5 to D8 Published
- IR - Intermediate report
- FR - Final report

Activity involving funded STF highlighted in Yellow

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 8 months after the start of the action and will provide a status report on the activity performed along with the latest drafts of the 4 ETSI



deliverables that will be available at this point in time. Full resource usage for the period concerned will be provided and given in full following the DG Enterprise Cost Control Strategy.

The Final Report will be provided to the EC/EFTA 14 months after the start of the action detailing the activity performed since the Interim Report along with the publication versions of the 8 ETSI adopted Technical Specifications and a report on the performance indicators as outlined in clause 6 of this technical proposal. The Final Report will outline the full resource usage details and on acceptance of the report an external audit certificate will also be provided along with a complete declaration under the DG Enterprise Cost Control Strategy.

The following table outlines the estimated resources required for each task.

Task	Task Name	Experts Man/days
T1.1	Gathering Requirements for AdES Signatures Baseline Profiles	20
T1.2	Production of AdES and Associated Signatures Baseline Profiles without long-term related properties	20
T2.1	Gathering Requirements for Long Term AdES Signatures Baseline Profiles	20
T2.2	Production of AdES and Associated Signatures Long Term Baseline Profiles	20
	<b>Total</b>	<b>80</b>

**Resources required**

**7.1 Work plan details**

**7.1.1 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: 2 months.
- Planned timescale: T0 + 2 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.

This phase also includes the creation and publication of a web page on the STF section of the ETSI Portal which introduces the work of the STF, the objectives, its' Terms of Reference and work plan. It will also highlight drafts that will be made available for public comment within the constraints of the ETSI rules and on agreement with the CEN-ETSI eSign Coordination Group. The final deliverables (ETSI TS) will be freely available for download from the ETSI Documentation Service (EDS on line).

**Planned timescale:** T0 + 2 months

### 7.1.2 Task T1.1: Gathering Requirements for AdES Signatures Baseline Profiles

This task will include the following activities:

1. **Scoping.** The team will scope the Baseline Profiles. This scope will determine the forms (AdES-BES, AdES-EPES, etc) and the properties to be included in each form. This scoping activity will be performed by mapping the requirements in the EU into the features provided by AdES forms and properties.
2. **Requirements fulfilment mechanisms.** Once defined the scope of the Baseline Profiles, the team will select the specific mechanisms for fulfilling the requirements where more than one is possible according to the specific AdES signature specification. The basic principle for this activity will be to reduce the amount of options, if possible to zero, for minimizing interoperability problems. Nevertheless, legacy implementations shall also be taken into account so that the resulting specifications do not jeopardize already running systems.

**Effort:** 20 Man days

**Planned timescale:** T0 + 5 months

### 7.1.3 Task T1.2: Production of AdES and Associated Signatures Baseline Profiles without long-term related properties

This task will include the following activities:

1. **Drafting.** The editors shall draft initial versions of the Baseline Profiles D1, D2, D3, and D4.
2. **Gathering Feedback.** The consolidated drafts will be circulated to ETSI ESI and a set of selected stakeholders for gathering comments.
3. **Comments dispositions.** The comments raised by ETSI ESI and selected stakeholders will be reviewed and resolved by the team, which will provide a disposition of comments document.
4. **Production of consolidated versions.** Implementation of disposition of comments and production of consolidated versions of the AdES and Associated Signatures Baseline Profiles without long-term related properties.
5. **Approval and publication by ETSI**

**Effort:** 20 Man days

**Planned timescale:** T0 + 10 months

### 7.1.4 Task T2.1: Gathering Requirements for Long Term AdES Signatures Baseline Profiles

This task will include the following activities:

1. **Extended scoping.** As in the previous phase this scope will determine the AdES evolved forms and the properties to be included in each form as required for long term signatures.

2. **Requirements fulfilment mechanisms.** Identification of additional mechanism required for extending the lifetime of a signature for given periods. All the remarks done for Task T1.1 of Phase 1 regarding minimum (ideally zero) options and consideration of legacy implementations are also valid for this phase.

**Effort:** 20 Man days

**Planned timescale:** T0 + 9 months

### **7.1.5 Task T2.2: Production of AdES and Associated Signatures Long Term Baseline Profiles**

This task will include the following activities:

1. **Drafting.** The editors shall draft initial extensions of the Baseline Profiles generated in Task 1.2 in D5, D6, D7, and D8.
2. **Gathering Feedback.** These D5, D6, D7, D8 drafts will be circulated to ETSI ESI and a set of selected stakeholders for gathering comments.
3. **Comments dispositions.** The comments raised by ETSI ESI and selected stakeholders will be reviewed and resolved by the team, which will provide a disposition of comments document.
4. **Production of final TSs.** Implementation of disposition of comments and production of the corresponding completed ETSI TSs for XAdES, CAdES, PAdES and Associated Signatures Baseline Profiles.
5. **Approval and publication by ETSI**

**Effort:** 20 Man days

**Planned timescale:** T0 + 14 months for the publication of all 4 ETSI TS