|  |  |
| --- | --- |
| ETSI_logo_Office_Colour_Small | ToR STF CQ (ESI) |
| Version: 0.2 |
| Author: TC ESI - EC/EFTA – Date:30 May 2018  |
| Last updated by: Youssouf Sakho – Date: 23 July 2018  |
| page 1 of  |

Terms of Reference - Specialist Task Force

STF CQ (ESI)

Standards for machine-processable signature policy formats and the global acceptance of European Trust Services

Summary information

|  |  |
| --- | --- |
| Funding | **EC/EFTA. Specific agreement N°ETSI/2017-05.** Total budget 159 651,29 EUR* Manpower budget: 84 650 €
* Travel budget: 30 000€
* Workshop (subcontractor): 45 000€
 |
| Time scale | Start date: Mid-October 2018End date: 31 March 2020 |
| Work Items  | DTS/ESI-0019172-3: ASN.1 format for signature policiesDTS/ESI-0019172-2: XML format for signature policiesDTR/ESI-000123: Global Acceptance of EU Trust Services |

**Part I – Policy relevance and expected market impact**

# Policy relevance

The actions being proposed fit into the Annual Union Work Programme (AUWP) and the EC Rolling Plan for ICT Standardisation (2017), in particular, within the “Electronic identification and trust services including e-signatures” policy area of the “Key enablers” cluster.

The proposed actions address actions 1, 2, 3 and 5 of the above-mentioned section of the Rolling Plan for ICT Standardisation (2017) to meet the new regulatory requirements of the Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions, including electronic signatures (referred to as the eIDAS Regulation in the rest of this proposal).

Creating standards relating to the machine-processable consumption of signature policies (i.e. TS 119 172-2 “Signature Policies. Part 2: XML format for signature policies” and TS 119 172-3 “Signature Policies. Part 3: ASN.1 format for signature policies”) are identified as important in action 1 and action 2 of this section of the Rolling Plan for ICT Standardisation (2017) and are the prime focus of this proposal. Such standards are a continuation of the TS 119 172-1 v1.1.1 (2015-07) that defines the building blocks of signature policy and specifies a table of contents for human readable signature policy documents. This continuation work aims to specify an XML format and an ASN.1 format for those parts of the signature policy that may be structured and are worth being automatically processed by both signing and validating applications. Having machine-processable formats will facilitate implementation of signature creation/validation under different signature policies.

The European Commission’s 2016 communication document “ICT Standardisation Priorities for the Digital Single Market” (COM(2016) 176) highlights that common standards ensure the interoperability of digital technologies and are the foundation of an effective Digital Single Market. Also actions 3 and 5 of of the Rolling Plan for ICT Standardisation (2017) stress that "the internationalisation and promotion of related European standards should be favoured" and that information should be disseminated to raise awareness and promote the take-up of EU related standards. It is therefore essential to have support from European experts in the relevant international standardisation and other fora which are working on ICT priority areas. The internationalisation of EU trust services on global level is also an important task. In order to establish the single digital market, the acceptance of the European Trust Services by the global software vendors and trust application providers like Mozilla, Google, Microsoft, Amazon, Adobe and Oracle is crucial.

# Rationale

Regulation (EU) No. 910/2014 identified the building of trust in the online environment as key to economic and social development. Standards need to be available to ensure solutions that are interoperable and provide consistent levels of trust. Whilst the regulation provides a common set of requirements, it does not identify how these requirements may be met with existing technology. Standards provide a generally accepted means of meeting requirements with existing technology, whilst if necessary the market can develop alternative solutions as new technology emerges which may later be absorbed into the generally accepted standards.

Work under Mandate M/460 Phase II resulted in the publication of several standards on signature policies and for trust services.

## Internationalisation of Trust Services

ETSI standards on Trust Services are being adopted throughout Europe in support of the eIDAS Regulation (EN 319 403, EN 319 401, EN 319 411), and use of the Trusted Lists TS 119 612 in EC CID 2015/1505 laying down technical specifications and formats relating to trusted lists. These are based on use of Public Key Infrastructure (PKI technologies using ITU-T X.509). However, cross recognition of the EU approach to PKI standards at an international level is yet to be achieved. A number of international, regional and sector specific communities adopting Public Key Infrastructure (PKI) technologies based on ITU-T X.509 exist which need to achieve cross recognition with European Trust Services to achieve end to end security. This includes:

* The CA/Browser forum
* Root certificate programmes of global application providers such as Mozilla, Google, Microsoft, Amazon, Adobe and Oracle
* Sector specific global PKI such as SafeBiopharma
* US federal PKI and associated programs such as National Strategy for Trusted Identities in Cyberspace (NSTIC)
* Far eastern communities such as Asia PKI Consortium, Association of South East Asian Nations, Chinese Electronic Certification Services Systems, Japan Institute for Promotion of Digital Economy and Community
* Arab PKI forum and other middle eastern communities
* Common Market for Eastern and Southern Africa
* ISO/IEC JTC1 SC 27 guidance on PKI service providers

Through further activities in promoting the use of EU standards internationally and facilitating cross recognition with other internationally based PKI schemes, such as those listed above, it will be possible for the EU players in the trust service market to work internationally. It is the aim of this work to focus on the detailed technical interoperability and trust issues rather than the legal and political coordination between the EU and other nations.

## Standards for machine processable signature policy formats

The purpose of a signature policy is to describe the requirements imposed on or committing the involved actors (signers, verifiers, relying parties and/or potentially one or more trust service providers) with respect to the application of signatures to documents and data that will be signed in a particular context, transaction, process, business or application domain, in order for these signatures to be considered as valid or conformant signatures under this signature policy.

ETSI TS 119 172-1 defines the building blocks of signature policy and specifies a table of contents for human readable signature policy documents. It allows documenting the decisions resulting from an analysis driven by a business or application context on how the concerned signature(s) needs to be implemented to meet the needs of the specific business application or electronic process it(they) support. It also specifies the means for the creation, augmentation or long term management and verification of all the features of the concerned signature(s).

As digital signatures are mainly treated and processed by applications, it is critical to allow the machine processable conversion and treatment of the rules having been established and documented by business process owners. This is highlighted in the Regulation (EU) No. 910/2014 Article 33 item 1(b) which states that “*Qualified validation service for qualified electronic signatures* *may only be provided by a qualified trust service provider who: (b) allows relying parties to receive the result of the validation process in an* ***automated*** *manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service*”.

Back into 2002, TC ESI published ETSI TR 102 038: “TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies”, followed by ETSI TR 102 272: “Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies” in 2003. These deliverables were implemented by a good number of stakeholders, who regularly raised a number of technical comments to TC ESI on their usage. These deliverables are now out of date and need a complete rework. Now that ETSI TS 119 172-1 has been published, there is a clear demand to provide again standards for translating the human readable signature policies in machine processable ones.

# Objective

## Internationalisation of EU Trust Services

The objective of the proposed tasks on internationalisation is facilitating the global recognition and trust of EU PKI Trust Services, supporting eIDAS Regulation based on EU standards (in particular EN 319 411, EN 319 401, EN 319 403 and TS 119 612). Thus enabling EU Trust services to operate not only within the internal European market, but also within the global market for trustworthy online services supporting PKI services for trust services such as web site authentication, electronic signatures and seals, code signing, secure email. This task seeks to facilitate cross recognition between EU Trust services and other PKI communities such as listed in section 2.1 above.

More specifically, the objective of this task is produce the following deliverables:

1. a technical report [WI DTR/ESI-000123TR “Global Acceptance of EU Trust Services”] to assess the relevant differences between existing global PKI schemes (such as those listed in 2.1) and the EU standards for policy requirements, assessment scheme and trust status defined in ETSI EN 319 411, EN 319 411, EN 319 403 and TS 119 612, and identify opportunities to further steps which could be taken to increase the European foothold in the global market for Trust Services.
2. Reports of three internationally based workshops with EU stakeholders and representatives of interests in global PKI schemes (such as those listed in 2.1). One workshop will be held in the US, another in Japan and the third one in the Middle-East where a number of the key stakeholders in global PKI market are based.

## Standards for machine processable signature policy formats

The objective of this part of the proposal is to specify XML and ASN.1 formats for signature policies to allow the automatic processing of the relevant aspects defined by such a policy during the creation, augmentation and validation of digital signatures.

More specifically this task is aiming at producing the following deliverables:

* ETSI TS 119 172-2: “Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 2: XML format for signature policies”,
* ETSI TS 119 172-3: “Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 3: ASN.1 format for signature policies”,

These two specifications will firstly satisfy the requirements specified in ETSI TS 119 172-1 in terms of contents, and secondly, will take into consideration the comments raised to ETSI by implementers and users of ETSI TR 102 038 and ETSI TR 102 272 regarding missing pieces, ambiguities, and potential improvements identified as a result of their usage in real systems.

# Market impact

Regulation (EU) No. 910/2014 identified the building of trust in the online environment as key to economic and social development. Standards need to be available to ensure solutions that are interoperable and provide consistent levels of trust. If a common basis for the provision and use of trust services is not available through standards it is very likely there will be fragmentation in the market with different nations and market sectors establishing their own solutions, as has already been seen for electronic signature services operating under the earlier Directive 1999/93/EC.

Without XML and ASN.1 technical specifications on formats for signature generation policy, signature augmentation policy, and signature validation policy, it will not be possible for the EU TSP market to provide interoperable solutions to the consideration of such policies in supporting signature generation and validation applications.

The European work on standardisation, however, cannot be viewed in isolation. Most of the EU's primary trading partners, including notably some large emerging economies, have recognised how important standard-setting is for market access and for boosting the competitiveness of their industries, and so they invest heavily in standard-setting and certification infrastructures. The promotion of European standards at international level will allow easier mutual recognition of trust services with countries which lie outside of the EU.

**Part II – Execution of the work**

# Working method / approach

## Specialist Task Force (STF)

ETSI will perform this work with the support of an ETSI STF, reporting the milestones to the ETSI ESI Technical Committee (TC ESI), according to the planned TC meeting agenda (as described in clause 7) and additional dates agreed by the TB chairman. TC ESI will play an active role in steering and contributing to this work.

Coordination with various stakeholders including European member states, standards organizations and European projects will be necessary to achieve the best outcome of this work and the widest possible collection of views amongst all parties concerned (see section 7 for further details). In particular, the STF, under TC ESI supervision, will aim to continue liaison with obvious EU stakeholders including the Member State and EU commission representatives through the eIDAS (technical) experts group, and CEF PKI-related building blocks, as well as working with stakeholders in the global PKI schemes listed in section 2.1 of this proposal.

## Other types of activity than STFs

The E-SIGNATURES\_NEWS mailing list, set up during phase I of the execution of Mandate M/460, will continue to exist and will be used to keep stakeholders informed on the progress of the work. Stakeholders will be consulted at various points during the work. They will in particular be consulted when drafts of the deliverables are issued for public comment so as to get their comments and feedback (this may not apply to all deliverables). The drafts will therefore be made publicly available on the ETSI TC ESI open server area at a number of stages throughout its development when agreed by TC ESI. Electronic comments will be encouraged via the contact list. A register of comments received through this list will be maintained by the STF.

Members of the STF will attend meetings relating to key global PKI schemes and international workshops will be organised to bring in stakeholders from global schemes.

## Expertise required, (qualification required, mix of skills)

The STF work will be performed by a team of contracted providers. The providers will be selected to possess an in-depth established knowledge of the following domains:

* Signature Policies:
	+ ETSI TS 119 172-1.
	+ ETSI TR 102 038 and ETSI TR 102 272.
	+ XML and ASN.1.
	+ digital signature formats, especially ETSI EN 319 122 (CAdES), ETSI EN 319 132 (XAdES), and ETSI EN 319 142 (PAdES), and associated containers as specified in ETSI EN 319 162 (ASiC).
	+ ETSI EN 319 102-1.
* Internationalisation of EU trust services:
	+ ETSI EN 319 411, EN 319 403, EN 319 401.
	+ Alternative conformity assessment schemes such as WebTrust for Certification Authorities Principles and Criteria and ISO/IEC 27000.
	+ Trust service status list concepts and specifications (ETSI TS 119 612).
	+ Internationally significant PKI schemes such as those listed in section 2.1
* The team will also provide capability in project management, report writing, consensus building, presentation skills, working in an international environment and experience in liaising with other international organisations.

The STF Leader will be responsible for co-ordinating the execution of the tasks assigned to the individual providers, according to the requirements in the technical annex of the action grant and following the technical direction given by TC ESI.

The other experts will be organised in the following STF Tasks (or group of tasks):

1. STF Lead.
2. Production of ETSI TS 119 172-2
3. Production of ETSI TS 119 172-3
4. Production of DTR/ESI-000123, Technical Report on Global Acceptance of EU Trust Services
5. Workshops on Global Acceptance of EU Trust Services

## Previous work

ETSI TC ESI published in 2002 ETSI TR 102 038: “TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies”, which defined an XML Schema for defining a signature policy. In 2003, ETSI TC ESI published ETSI TR 102 272: “Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies”, which defined an ASN.1 structure for defining a signature policy. In 2015, ETSI TC ESI published ETSI TS 119 172-1: “Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents”.

For a number of years ETSI has been developing policy requirements standards for EU trust services starting in 2000 with the first version of TS 101 456 which was specifically aimed at requirements for PKI services meeting the specific requirements of Directive 1999/93. Since then ETSI has worked with other parties such as the US federal PKI and the CA Browser Forum to produce standards which are more appropriate to the global environment in particular TS 102 042 which was derived from TS 101 456. With the introduction of the new eIDAS Regulation 910/2014 a new European standard was produced EN 319 411 for Trust Service Providers (TSPs) issuing (PKI) certificates with part 1 being aimed at the general market and part 2 addressing specific requirements of the regulation. Generic policy requirements for TSP was placed in EN 319 401 which was referenced by EN 319 411 as appropriate to TSPs issuing certificates. At the same time new standards were produced for conformity assessment of Trust Service Providers (EN 319 403) and for trusted lists of TSPs (TS 119 612). There has been some success with obtaining some cross recognition of these new services in some international schemes (e.g. CAB Forum and SafeBiopharma). However, there remain barriers to full cross recognition, particularly for qualified trust services and use of trusted lists outside the EU, and there is as yet not acceptance of the work of ETSI in the International Standards forum.

# Performance indicators

Information that will act as performance indicators against the contracted activity will be provided by the STF in the following cases:

Effectiveness and efficiency:

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

the number of meetings held in relation to this work:

* + the number of participants;
	+ the number of presentations and technical contributions made on the activity by STF;
* an evaluation of feedback received;
* project progress in relation to the specified schedule

**Proposed effectiveness and efficiency benchmarks**

1. Reports produced by the STF for TC ESI about the progress of the work. A report will be produced for each TC ESI meeting held during this activity (expected to be at least 3 reports a year).
2. Draft versions of the deliverables to be circulated to ETSI TC ESI for comments, namely: early draft, stable draft and complete draft.
3. 90% of the tasks and other milestone-related schedule on time (less than 5 days after the planned dates).

Stakeholder engagement and satisfaction:

An analysis will be given of the balance of stakeholder representation in the activity and the number of liaison activities performed (especially at the international level).

* Comments provided to the draft versions of the deliverables circulated by the STF, expected to include at least 5 comments.

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**

1. at least 2 presentations at international fora meetings.
2. Organization of three international workshops and reports from the events
3. At least 1 public consultation (ETSI, stakeholder contact list) on the key draft documents.

# Work plan, milestones and deliverables

## Deliverables

Reports to be submitted to the EC/EFTA:

* The Interim report will be submitted at the latest 9 months after the date of signature.
* A final report will be submitted at the latest 15 months after the date of signature.

## Table 1 shows the deliverables of this project. Section 7.2 “

## Work plan

Table **3** shows the detailed work plan for this project. It is formed by tasks.

Note: T0 is used to denote the start of the project in the milestones below. ” provides additional information of the purported content for each deliverable.

**Table** **1: List of deliverables**

| Deliverable ID | Type | Title and Contents | Observations |
| --- | --- | --- | --- |
| **119 172-2**DTS/ESI-0019172-2 | TS | **Title:** Electronic Signatures and Infrastructures (ESI);Signature Policies; Part 2: XML format for signature policies**Content:** TS 119 172-1 describes the different building blocks for human readable signature policy documents. Some of these elements can be translated directly in input for signature creation / augmentation or validation processes, like the used / accepted trust anchors or elements to be included into the signature. The goal of this document to capture these elements in machine processable form, **more precisely in XML format**. This allows to use these signature policies directly as input to the signature creation / augmentation or validation process. |  |
| **119 172-3**DTS/ESI-0019172-3 | TS | **Title:** Electronic Signatures and Infrastructures (ESI);Signature Policies; Part 3: ASN.1 format for signature policies**Content:**  TS 119 172-1 describes the different building blocks for human readable signature policy documents. Some of these elements can be translated directly in input for signature creation / augmentation or validation processes, like the used / accepted trust anchors or elements to be included into the signature. The goal of this document to capture these elements in machine processable form, **more precisely in ASN.1 format**. This allows to use these signature policies directly as input to the signature creation / augmentation or validation process. |  |
| **WI DTR/ESI-000123** | TR | **Title: Global Acceptance of EU Trust Services****Content:** This report will assess the relevant differences between existing global PKI schemes and the EU standards for policy requirements, assessment scheme and trust status defined in ETSI EN 319 411, EN 319 401, EN 319 403 and TS 119 612, and identify opportunities to further steps which could be taken to increase European foothold in the global market for Trust Services. The following PKI schemes and standards are considered probable targets:* The CA/Browser forum
* Root certificate programmes of global application providers such as Mozilla, Google, Microsoft, Amazon, Adobe and Oracle
* Sector specific global PKI such as SafeBiopharma
* US federal PKI and associated programs such as National Strategy for Trusted Identities in Cyberspace (NSTIC)
* Far eastern communities such as Asia PKI Consortium, Association of South East Asian Nations, Chinese Electronic Certification Services Systems, Japan Institute for Promotion of Digital Economy and Community
* Arab PKI forum and other middle eastern communities
* Common Market for Eastern and Southern Africa
* ISO/IEC JTC1 SC 27 guidance on PKI service providers
 |  |
| **Not a formal ETSI publication** |  | **Title: Reports on the 3 International workshops on global acceptance of EU Trust Services****Content**: three reports of the 3 international workshops with EU stakeholders and representatives of interests in global PKI schemes (such as listed above). It is proposed to hold one workshop in US, one in Japan and one in Southern Europe or Middle-East where a number of the key stakeholders in the global PKI market are based. |  |

Table 2: List of deliverables

| Deliverable ID | Title and Contents | Publisher |
| --- | --- | --- |
| Interim Report (IR1) | **Title**: Interim Report**Content**: This report will include:1. The report on the activities performed, on the coordination of the STF activity and the production of the expected deliverables in the different areas of the framework.2. Latest drafts of the available deliverables. 3. Report of specific meetings held with EU groups, projects, recognised standards organizations or other organisations representing communities of interest  | No formal publication |
| Final Report (FR) | **Title**: Final Report **Content**: This report will include:* 1. The report on the activities performed, on the coordination of the STF activity and the production of the expected deliverables in the different areas of the framework.
	2. Published versions of ETSI deliverables (as in Table 1).
	3. Detailed report of the performance indicators outlined in clause 6 of this proposal including the initiatives for dissemination of the work done.
	4. Reports of workshops held
	5. Report of specific meetings held with EU groups, projects, recognised standards organizations or other organisations representing communities of interest
 | No formal publication |

##

## Work plan

Table **3** shows the detailed work plan for this project. It is formed by tasks.

Note: T0 is used to denote the start of the project in the milestones below.

**Table** **3: Tasks**

| Task | Description and methodology | Deliverables |
| --- | --- | --- |
|  | STF Organization |  |
| .1 | STF SetupETSI and the TC ESI chair will interview the candidate providers and select those to best meet the work plan.ETSI will make service contract arrangements for the selected STF providers. **Start**: T0 **End** T0+3 |  |
| 1.2 | STF LeadThe STF lead will:* Plan the work of the STF members, ensuring that the timescales of the STF deliverables are met
* Organise STF meetings to discuss the drafts, recording any major issues and resolutions of the STF, identifying and progressing the actions of STF members
* Report to TC ESI and the Secretariat on the work of the STF,
* Represent, or arrange other STF members to represent, the STF at other external meetings.

**Expertise required:*** proven record of standards project delivery, strong knowledge of project management, report writing, consensus building, presentation skills
* Ability to lead and manage a team of experts

**Effort Required: 13 650 EUR****Milestones:** **Start**: T0+3  **M1.1** Interim report T0+9 **M1.2** Final report: T0+15 |  |
|  | Production of Technical Specifications for XML format for signature policies |  |
|  | **Description:** The goal of this task is to produce the deliverable TS 119 172-2: “Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 2; XML format for signature policies”. This deliverable will fully specify a XML format for describing a signature policy based on the signature policy building blocks defined in ETSI TS 119 172-1: “Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents”. | TS 119 172-2DTS/ESI-0019172-2 |
|  | **Methodology:** The STF will use the following inputs for its work on this task:* ETSI TS 119 172-1: “Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents”, for identifying the required building blocks of a signature policy
* Take into account EN 319 102-1 to see which information is specifically important for the automatic processing of signature creation / validation algorithms.
* ETSI TR 102 038: “TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies”.
* The comments raised by stakeholders that implemented the aforementioned ETSI TR in order to extract requirements for the new deliverable in terms of new features that the former ETSI TR did not provide, ambiguities that the new deliverable should avoid, errors that the new deliverable should not incur in, etc.

The STF will first identify the semantics that the XML and the ASN.1 formats need to express. For doing this ETSI TS 119 172-1 will be used as reference. This part of the work will be common to the production of the deliverables ETSI TS 119 172-2 and ETSI TS 119 172-3.Once this is done, ETSI TR 102 038 will be reviewed in order to check what parts of these semantics were already covered in this document. The STF will afterwards propose an XML Schema for a signature policy based on the previous findings and a thorough review of the comments received from stakeholders who implemented and used ETSI TR 102 038.Note: after TS 119 172 parts 2 and 3 are published, it will be in TC ESI remit to decide on the status of TR 102 038 and TR 102 272 (e.g. make them historical, withdraw them)While defining the XML format, care will be taken in ensuring as much alignment as possible between this format and the ASN.1 format specified in the ETSI TS 119 172-3.**Effort required: 18 000 EUR****Intermediate and final Milestones:****Start**: Immediately after establishment of the project team.**M2.1**: Consolidated draft for ESI: end of T0 +7 months**M2.2**: Consolidated draft for public review: end of T0 +10 months**M2.3**: Final draft for ESI approval: end of T0 +13 months**M2.4:** TS published: end of T0 +15 months |  |
|  | Production of Technical Specifications for ASN.1 format for signature policies |  |
|  | **Description:** The goal of this task is to produce the deliverable TS 119 172-3: “Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 3; ASN.1 format for signature policies”. This deliverable will fully specify an ASN.1 format for describing a signature policy based on the signature policy building blocks defined in ETSI TS 119 172-1: “Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents”. | TS 119 172-3DTS/ESI-0019172-3 |
|  | **Methodology:** The STF will use the following inputs for its work:* ETSI TS 119 172-1: “Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents”, for identifying the required building blocks of a signature policy.
* Take into account EN 319 102-1 to see which information is specifically important for the automatic processing of signature creation / validation algorithms.
* ETSI TR 102 272: “Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies”.
* The comments raised by stakeholders that implemented the aforementioned ETSI TR in order to extract requirements for the new deliverable in terms of new features that the former ETSI TR did not provided, ambiguities that the new deliverable should avoid, errors that the new deliverable should not incur in, etc.

As already mentioned in the description of task 2, the first common work for these two tasks will be the identification of the semantics that the ASN.1 and the XML format need to express. For doing this, ETSI TS 119 172-1 will be used as reference. Once this is done, ETSI TR 102 272 will be reviewed in order to check what parts of these semantics were already covered in this document. The project team will afterwards propose the ASN.1 definition for a signature policy based on the previous findings and a thorough review of the comments received from stakeholders who implemented and used ETSI TR 102 272.Note: after TS 119 172 parts 2 and 3 are published, it will be in TC ESI remit to decide on the status of TR 102 038 and TR 102 272 (e.g. make them historical, withdraw them)As mentioned in task 2, while defining the ASN.1 format, care will be taken in ensuring as much alignment as possible between this format and the XML format specified in ETSI TS 119 172-2.**Effort required: 18 000 EUR** **Intermediate and final Milestones:****Start**: Immediately after establishment of the project team**M3.1**: Consolidated draft for ESI: end of T0 +7 months**M3.2**: Consolidated draft for public review: end of T0 +10 months**M3.3**: Final draft for ESI approval: end of T0 +13 months**M3.4:** TS published: end of T0 +15 months |  |
|  | Production of Report on Global Acceptance of EU Trust Services |  |
|  | **Description**: The global PKI and other related trust schemes will be assessed against the EU standards EN 319 411-1 & -2, EN 319 401, EN 319 403 and TS 119 612 to identify the relevant differences and identify opportunities to further steps which could be taken to increase European foothold in the global market for Trust Services. | **WI DTR/ESI-000123** |
|  | **Methodology:** The STF will get in touch with all the other PKI related trust schemes and standards considered relevant to global acceptance of EU Trust Services to collect all the relevant information on the policies, conformity assessment procedures, and means of indicating trust status. Where considered appropriate individual members of the team will attend meetings or visit key personnel concerned with the relevant PKI schemes. Whilst centring on PKI related trust services the report will consider how the same approach could be applied to other trust services.The analysis will take account of the compatibility of the trust policy requirements for the different schemes, and also how the trust is managed for membership of the scheme whether by a form of trust list or other technique such as bridge certificate bridges or certificate transparency.The following PKI schemes and standards are considered probable targets:* The CA/Browser forum
* Root certificate programmes of global application providers such as Mozilla, Google, Microsoft, Amazon, Adobe and Oracle
* Sector specific global PKI such as SafeBiopharma
* US federal PKI and associated programs such as National Strategy for Trusted Identities in Cyberspace (NSTIC)
* Far eastern communities such as Asia PKI Consortium, Association of South East Asian Nations, Chinese Electronic Certification Services Systems, Japan Institute for Promotion of Digital Economy and Community
* Arab PKI forum and other middle eastern communities
* Common Market for Eastern and Southern Africa
* ISO/IEC JTC1 SC 27 guidance on PKI service providers

For each scheme the following information will be produced:* An overview of the scheme including the scope of and key features
* Relationship with EU standards EN 319 411-1 & -2, EN 319 401, EN 319 403 and TS 119 612
* Main differences which impact acceptance of EU Trust Services
* Opportunities for increasing adoption of EU standards

**Effort Required:** **23 000 EUR**5 travels to international meetings anticipated to e.g. CAB Forum, Asia PKI Consortium, Arab PKI forum, ISO/IEC JTC1 SC27**Intermediate and final Milestones:****Start**: Immediately after establishment of the project team**M4.1**: Consolidated draft for ESI: end of T0 +6 months**M4.2**: Consolidated draft for public review: end of T0 +10 months**M4.3**: Final draft for ESI approval: end of T0 +13 months**M4.4:** TR published: end of T0 + 15 months |  |
|  | International workshops on global acceptance of EU Trust Services |  |
| 5 | Three internationally based workshops with EU stakeholders and representatives of interests in global PKI schemes will be organised in conjunctions with representatives of the most relevant PKI schemes. One workshop will be held in US, another in Japan and the third one in hosted by ETSI for Middle East and other non-EU countries in the EMEA region where a number of the key stakeholders in global PKI market are based. A report will be produced following each workshop. | International Workshops |
|  | **Methodology:** The workshops will be organised by the STF members. The agenda and scheduling will be agreed with representative of the PKI schemes considered most relevant.Expect number of attendees per workshop: 100 attendees**Effort Required:** **12 000 EUR** 3 expert travel to US3 expert travel to Southern Europe or Middle East3 expert travel to JapanSubcontracting costs for the 3 workshops: 15,000€ \* 3 for organising and hosting costs including room, catering, promotional material, etc.**Intermediate and final Milestones:****Start**: Immediately after establishment of the project team**M5.1**: Consolidated draft of supporting material: end of T0 +6 months**M5.2**: Workshops: between T0+6 months and T0+16 months (approximate)**M5.3**: Reports on Workshops and further recommendations |  |

Table : Calendar for tasks and milestones

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Task | T0 | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | +16 | +17 | +18 |
| 1.1 Setup |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.2 STF lead  |  |  |  |  |  |  |  |  |  | M1.1 |  |  |  |  |  | M1.2 |  |  |  |
| 2 XML policies |  |  |  |  |  |  |  | M2.1 |  |  | M2.2 |  |  | M2.3 |  | M2.4 |  |  |  |
| 3 ASN.1 policies |  |  |  |  |  |  |  | M3.1 |  |  | M3.2 |  |  | M3.3 |  | M3.4 |  |  |  |
| 4 global acceptance |  |  |  |  |  |  | M4.1 |  |  |  | M4.2 |  |  | M4.3 |  | M4.4 |  |  |  |
| 5 workshops |  |  |  |  |  |  | M5.1 |  |  |  |  |  |  |  |  |  | M5.2 |  | M5.3 |

**Part III: Financial part**

# Financial provisions in the EC/EFTA contract

## Total action costs

The total action costs estimated for this action amounts to 159 651,29 € based on the lump sum of 640,51 € per unit and the requirement for 179 units to carry out the actions described plus 45 000 € in subcontracting. EFTA is to provide a 5% co-financing (7982,56 €) and hence the EC contribution (95%) will be 151 668,73 €.

## Direct (eligible) costs

N/A

## Travelling costs

N/A

## Equipment necessary to implement the action

N/A

## Cost of consumables and supplies necessary to implement the action

N/A

## Other costs and services necessary to implement the action

N/A

## Subcontracting to external organisations

Subcontracting costs for the 3 workshops: 15,000€ \* 3 (= 45 000 €) for organising and hosting costs including room, catering, promotional material, etc.

# Annex – Notes on International Activities

* ISO/IEC JTC 1 SC 27 WG 4 was taking a different path when they started updating TR 14516 with some ISO members proposing solutions which did not fully align with ETSI standards. In April 2016, the project on ISO TS 14516 was cancelled, due to concerns of many EU nations that it did not align with EU standards, and so a new Study Period on Information security guidance for PKI service providers was established. There is an opportunity to influence this new activity to ensure alignment with EU standards if appropriates inputs made to make ISO aware of the benefits of the current EU approach.
* While acceptance of ETSI certificate policies (EN 319 411, EN 319 401 with EN 319 403) by CA/B Forum was achieved in July 2016, they need to be updated to alignment with the requirements as set out by ISO 27000. As it stands, acceptance by the global software vendors and trust application providers like Mozilla, Google, Microsoft, Amazon, Adobe and Oracle remains a challenge, particularly with the general reluctance to recognise EU qualified level of certificates for web site authentication and the non-adoption of the EU trusted list based on TS 119 612. The push towards wider international acceptance of the trusted list of qualified certificates will be aided by alignment of the requirements of the CA/B Forum and audit of qualified certificates and as held in the EU Trusted List.
* Discussions have been held with US experts looking towards alignment PKI schemes supporting EU and US requirements for communities such as for the Biopharma industry, as well as the US national governmental programmes such as Federal PKI and the National Strategy for Trusted Identities in Cyberspace (NSTIC) and certain barriers exist still which inhibit the ability of industry to meet US and EU requirements.
* Liaison and collaboration will be sought with the following regional organisations all around the world:
	+ The [**Asia PKI Consortium**](http://www.apkic.org/)(APKIC) is transformed from Asia PKI Forum (APKIF), which was jointly established by Japan, China, Korea, Chinese Taipei and Singapore in June 2001. In addition to the PKI Trust Models, the Guidelines also list technical standards for the infrastructure, and the manner in which they should be adopted.

**Contact**: Secretariat of APKIC, Ms. Eva Chan, evachan@hkpkiforum.org.hk.

* + [**ASEAN Community**](http://asean.org/) (Association of South East Asian Nations): The ASEAN Community groups ten Member States namely Indonesia, Malaysia, Philippines, Singapore, Thailand, Brunei Darussalam, Viet Nam, Lao PDR, Myanmar, and Cambodia. They established a CA-CA Interoperability Framework and project in ASEAN as part of the eASEAN initiative.

**Contact**: Secretary-General of ASEAN, H.E. Le Luong Minh, c/o ASEAN Committee in Brussels, Ambassador of Malaysia to Belgium, malbrussels@kln.gov.my.

* + - **People's Republic of China**: Following a series of workshops on the development of Electronic Certification Services Systems in the EU and China in 2008 and 2009, more recently an EU-China conference on mutual recognition of electronic signature certificates was organised in 2013 as part of the EU-China Trade Project II. EUCTP II is the third major EU-China trade related technical assistance project since 2000. From 2010 to 2015, project activities will support the Chinese government's trade reform and sustainable development agenda by working under the EU-China economic and trade dialogues, amongst other aspects, to facilitate harmonisation with international standards. It should be looked out whether the EU has plans for supporting/organising follow-up to such workshops.

**Contact**: DG Trade

* + - **Office of the Government Chief Information Officer of the Government of the Hong Kong Special Administrative Region** - Guangdong-Honk Kong mutual recognition arrangement: To better protect the interest of users of certification services and enhance their confidence in electronic transactions, a Voluntary Certification Authority Recognition Scheme was established by the Government of the Hong Kong Special Administrative Region pursuant to the Electronic Transactions Ordinance ("ETO"). A Trust List sets out the certificate types that have been granted mutual recognition status, method for verification of mutual recognition status and detailed verification information provided by the issuing recognised certification authorities.

**Contact**: Certification Authority Recognition Office, Office of the Government Chief Information Officer, caro@ogcio.gov.hk.

* + Japan: The JIPDEC in Japan not only adopted the ETSI TS 102 042 CP, they also implemented an Audit scheme based on the ETSI Framework.
	Contact: s.hamaguchi@cosmos-corp.com
* **Middle East**
	+ [**Arab PKI Forum**](http://www.aicto.org/arab-pki-forum): The Arab ICT Organization “AICTO” 17 Arab countries out of 22 members of the League of Arab States. They have set up the “Arab Network” of Electronic Certification Bodies in the region with the objectives of
		- Gathering the Arab agencies/bodies of e-certification and PKI within a common network to exchange the related experiences between Arab countries.
		- Establishing regional conventions ensuring the mutual recognition of the digital signatures even between Arab countries or other foreign countries.
		- Harmonizing laws related to e-signature and e-transactions between Arab countries on the one hand and with the laws of the European Union on the other hand.

**Contact**: Engineer Mohamed Ben Amor, Secretary-General of the Arab ICT Organization, contact@aicto.org.

* + **GCC countries**: All six GCC countries have each initiated modern Identity management systems to develop a new personal identification card that would act as the trusted identification document. Each of them have set up a national PKI certification authority enabling eAuthentication and digital signatures. Interoperability and alignment of policies and practices is part of the general GCC ICT interoperability model. Most of the national PKIs aim to align to international standards and conformity assessment practices.

**Contacts**:

* + - Samir Pawaskar, CS Policy and Standards Section Head, State of Qatar, ictQatar, Ministry of Transport and Communications, spawaskar@motc.gov.qa
		- Dr. Ali M. Al-Khouri, Director General, Emirates Identity Authority, United Arab Emirates, ali.alkhouri@emiratesid.ae
* **Africa**:
	+ [COMESA](http://www.comesa.int/): The Common Market for Eastern and Southern Africa (COMESA) is a free trade area that comprises of 19 Member States from North to South of Africa) that came together with the aim of Promoting Regional integration through trade and the development of natural and human resources for the benefit of all the people in the region. Key activities of the COMESA cybersecurity program include the production of guidelines for the “development of PKI legislations, regulations and standards” (2014-2015) and the establishment of a regional Controller of Certification Authorities (2016). The key activities roadmap also includes the organisation of training of trainers for the judicial system with Council of Europe (not done yet as of May 2016).

**Contact**: Leonard Chitundu – Telecommunications Officer COMESA Secretariat, info@comesa.int.

# Document history

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Date** | **Author** | **Status** | **Comments** |
| 0.1 | 30-05-2018 | TC ESI | Approved by EC  |  |
| 0.2 | 23-07-2018 | Youssouf Sakho | Approved by EC | Editorials before publication of the Collective Letter |