ETSI TS 119 403 V1.1.1 (2012-03)

Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General requirements and guidance

Reference
DTS/ESI-000075

Keywords
conformity, e-commerce, electronic signature, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Introduction

As a response to the adoption of Directive 1999/93/EC [i.1] on a Community framework for electronic signatures in 1999, and in order to facilitate the use and the interoperability of eSignature based solution, the European Electronic Signature Standardization Initiative (EESSI) was set up to coordinate the European standardization organisations CEN and ETSI in developing a number of standards for eSignature products.

The European Directive on a community framework for Electronic Signatures [i.1] (also denoted as "the Directive" in the rest of the present document) defines an electronic signature as: "data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication".

Commission Decision 2003/511/EC [i.9], on generally recognised standards for electronic signature products, was adopted by the Commission following the results of the EESSI. This decision fostered the use of eSignature by publishing "generally recognised standards" for electronic signature products in compliance with article 3(5) of the Directive but has a limited impact on the mapping of the current state of the European standardisation on eSignatures, which also covers ancillary services to eSignature, and the legal provisions and requirements laid down in Directive 1999/93/EC [i.1].

In particular, to support the use of Electronic Signatures a range of documents have been published by ETSI specifying policy requirements for providers of trusted services used in support of electronic signature, termed Certification Service Providers (CSP) in the Directive on Electronic Signatures. In order to assess the Conformity of a more generic range of trust service providers (TSPs) to one, or more specification it is necessary for the operation of the TSP to be assessed against their policy requirements. The present document specifies general requirements for Conformity Assessment independent of the form of TSP and provides guidance for the supervision and assessment of a TSP supporting electronic signatures.

1 Scope

The present document specifies requirements and guidance for the assessment of a Trust Service Provider (TSP) through the Conformity assessment against an ETSI document specifying policy and security requirements for a particular class of trust service (e.g. policy requirements for certification authorities issuing qualified certificates as in TS 101 456 [i.3]).

Requirements and guidance set out in the present document are independent of the class of trust service provided. Other documents may extend or refine the requirements specified in the present document to provide requirements and/or guidance for a particular class of service.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ISO/IEC 17021:2011: "Conformity assessment - Requirements for bodies providing audit and certification of management systems".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.2] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[i.3] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[i.4] Commission decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the "points of single contact" under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market and its amending Decision of 28 July 2010.

[i.5] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

[i.6] CA/Browser Forum: "Guidelines for the issuance and management of extended validation certificates".

[i.7] ETSI TS 102 231 (V3.1.2): "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[i.8] IAF Mandatory Document for the Certification of Multiple Sites Based on Sampling.

[i.9] Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognized standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council.

[i.10] Commission Decision 2010/425/EU amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted list of certification service providers supervised/accredited by Member States.

[i.11] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".

[i.12] CWA 14172-2: "EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

assessor: person who assesses conformity to requirements as specified in a given policy requirements document

competence: ability to apply knowledge and skills to achieve intended results

conformity assessment: process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled

NOTE: From Regulation (EC) No 765/2008 [i.5].

conformity assesssment body: independent body of assesors accredited by a National Accreditation Body as having the competence to carry out an assessment in line with the present document

NOTE: This is equivalent to Conformity Assessment Body as specified in Regulation (EC) No 765/2008 [i.5].

national accreditation body: national body that performs accreditation of Conformity Assessment Bodies with authority derived from the State

NOTE 1: From Regulation (EC) No 765/2008 [i.5].

NOTE 2: In the context of supervision under Directive 1999/93 [i.1], the equivalent role of the national accreditation body for evaluating the competence of a Conformity Assessment Body with regards Certification Services may be taken on a body established for the purpose of supervision.

technical expert: person who provides specific knowledge or expertise to the assessor

trust service: electronic service which enhances trust and confidence in electronic transactions

NOTE: Such Trust Services are typically but not necessarily using cryptographic techniques or involving confidential material.

trust service provider: entity which provides one or more electronic Trust Services

Trust Service status List (TSL): list of the Trust Service status information from which interested parties may determine whether a Trust Service has been assessed as operating in conformity with recognised criteria for a given trust service which is protected to assure its authenticity and integrity

trust service status Notification Body (Notification Body): body which issues a trust service status list (or lists) based on the results of conformity assessment of a Trust Service Provider

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

EC	European Commission
CSP	Certification Service Provider

NOTE: See reference [i.1].

TSP	Trust Service Provider
EESSI	European Electronic Signature Standardization Initiative
EA	European Co-operation for Accreditation
CWA	CEN Workshop Agreement
QC	Qualified Certificate
TSL	Trust-services Status List
TL	Trusted List

4 Introduction to TSP conformity assessment

This clause discusses the basic elements of TSP Conformity Assessment. Normative requirements are given in latter clauses.

4.1 Assessment model

The basic element for assessment of a conformity a TSP to standardised policy requirements is illustrated in figure 1.

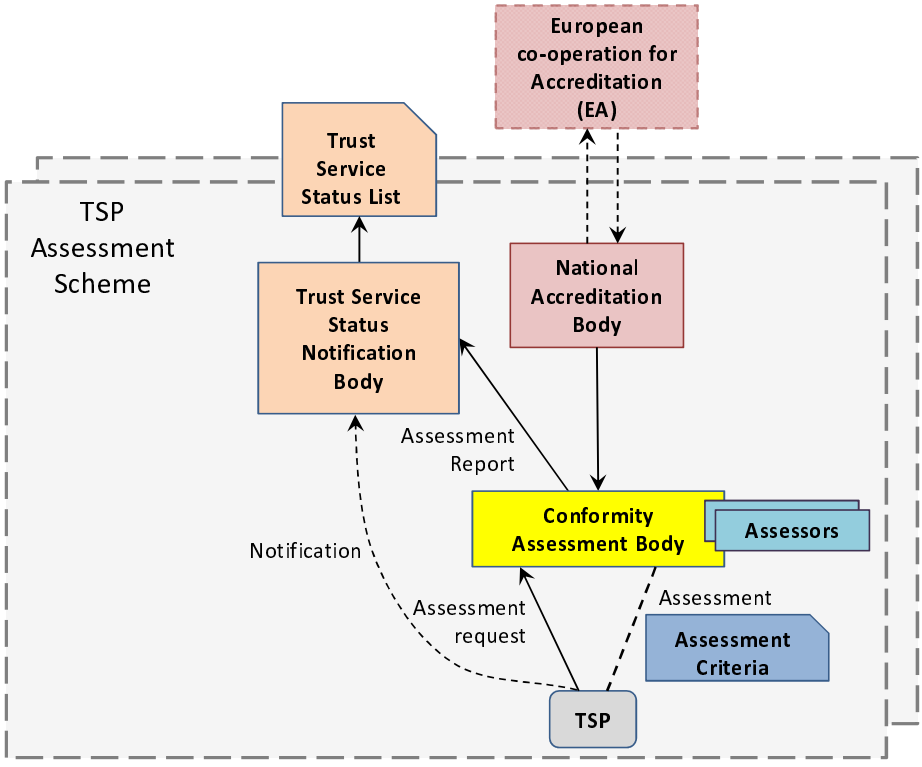

Figure 1: Model for Trust Service provider Conformity Assessment

Within the context of a nation or region a scheme for assessment of a TSP against standardised requirements for a given trust service (or set of trust services), a TSP Assessment Scheme, may be established. This consists of the following elements:

Conformity Assessment Body: This is an independent body of assessors which carries out the assessment of a TSP against standardised requirement for the provision of a particular trust service (e.g. as specified in TS 101 456 [i.3]). The competence of Conformity Assessment Body to carry out such an assessment is accredited by a National Accreditation Body. One or more Conformity Assessment Bodies may be recognised under a TSP Assessment Scheme. The results of a conformity assessment is notified to a Trust Status Notification Body.

National Accreditation Body: This is a national body that that performs the accreditation of Conformity Assessment Bodies with authority derived from the State. The accreditation assesses the competency of the Conformity Assessment Body to carry out assessments under the requirements identified in clauses 5 and 6 below.

NOTE: Generally, a National Accreditation Body is established under Regulation (EC) No 765/2008 [i.5]. However, in the context of supervision under Directive 1999/93 [i.1], the responsibility for evaluating the competence of a Conformity Assessment Body for assessing Certification Services may be taken on by the body established for the purpose of supervision.

Trust Service Status Notification Body: This is a body responsible for notification of the trust status of a TSP for a given trust service based on the results of a Conformity Assessment Body.

Guidance on the application of these, or equivalent, bodies to the supervision of Certification Service Providers under Directive 1999/93/EC [i.1] and related Trust Service Status Notification in the context of the Commission decision 2009/767/EC [i.4] is described in annex A. The present document provides no restriction on the provision of the above responsibilities to one or more bodies concerned with supervision of CSPs under Directive 1999/93/EC [i.1].

4.2 TSP Conformity Assessment in context

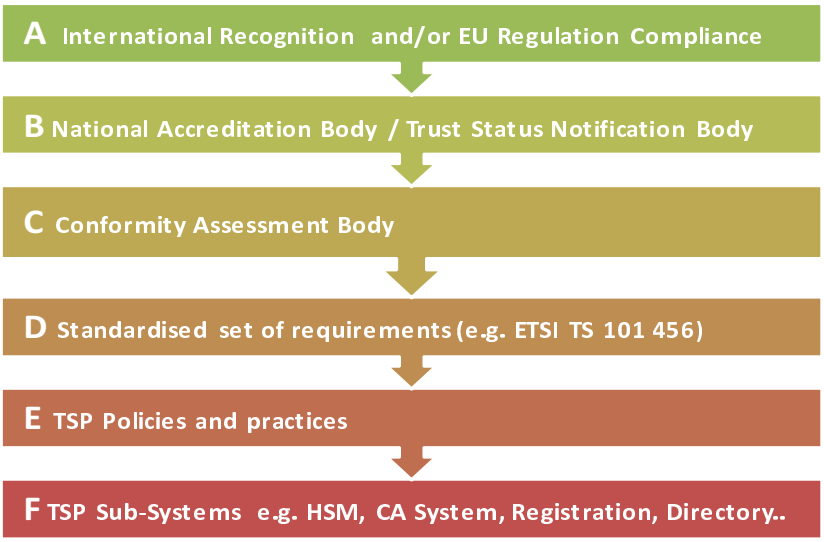

Figure 2: TSP Conformity Assessment in context

Conformity Assessment of a TSP is to be carried out in the general context as identified in figure 2:

a) The Conformity Assessment is carried out within in the international context which provides cross recognition of the assessment. This includes pan European regulations provided for the international framework for the accreditation of assessment laboratories and Conformity Assessment Bodies through the European Cooperation for Accreditation (EA).

NOTE 1: It is the object that European cross recognition is eventually extended Internationally through the International Accreditation Forum.

b) Within each European Nation there are bodies concerned with the operation of TSP assessment. This includes:

- a body which delivers accreditation of Conformity Assessment Bodies, recognised internationally through EA which accredits a range of assessment bodies both within and outside the IT arena (National Accreditation Body);
- a body concerned with Trust Status Notification Body concerned with notification to interested parties the trust status a TSP's trust service.

NOTE 2: The function of these bodies within the context of the EU Directive 1999/93 may be undertaken by a supvisory body as described in annex A.

c) The assessment of the TSP is carried out by assessors under the management of a Conformity Assessment Body. These assessors checks the TSPs policies, practices and how their application (see e) is conformant to the assessment criteria such as standardised policy requirements (see d).

d) The assessment of TSP is carried out against the standardised set of requirements for a particular class of TSP service (e.g. CSP issuing qualified certificates such as currently specified in TS 101 456 [i.3]).

e) The assessment is applied to a TSP amongst other through its documented policies and practices and evidence of how these are being applied against the standardised policy requirements.

f) The TSP may build upon existing sub-systems, for example hardware (cryptographic) security modules, which have already been assessed against specific requirements of that subsystem. Such existing assessment will be taken into account when assessing a TSP.

The present document is concerned primarily with the assessment of TSPs by Conformity Assessment Bodies as identified in "c" in the context of the national infrastructure for TSP assessment. This assessment includes requirements for the competence of the assessor and the procedures for carrying out the assessment.

5 Assessment process

5.1 General requirements

Requirements as per ISO/IEC 17021:2011 [1], clause 9.1 apply.

The assessment of the TSPs management system can be combined with assessments of other management systems. This combination is possible provided it can be demonstrated that the assessment satisfies all requirements for confirming that the TSP meets the requirements of the applicable specification(s). All elements of the TSP's management system should appear clearly and be readily identifiable in the assessment reports. The quality of the assessment should not be adversely affected by the combination of the assessments.

5.2 Assessment process model

The model provides a framework that can be used as an EU-wide common basis for setting-up both TSP Assessment schemes. This model relies on:

1) a common set of Conformity criteria;

2) a common assessment process;

3) a common understanding of the TSP responsibilities.

5.2.1 The conformity criteria

This refers to the criteria against which the provision of certification services by a TSP will be assessed.

Those criteria should:

- take into account specificities of the type of trusted service to be assessed;
- be organized under the form of a check-list for the sake of facility for both the assessor and the TSP to be assessed;
- be publicly available; and
- be based on standards.

The common sets of **Conformity Criteria** are provided in separate documents which specify policy requirements for a specific trust service.

These Conformity Criteria are summarised under the form of a checklist that can be used by the TSP itself to prepare for an assessment (i.e. serve as a basis for a self-declaration) and by the assessor when conducting the assessment.

5.2.2 The assessment process

This refers to the way Conformity Assessment Body carries out an assessment.

This covers:

- the process flow;
- the guidance and related rules to be observed by the Conformity Assessment Body when conducting assessments;
- specific characteristics with regards to the TSP assessment process, like:
  - the frequency of evaluations/audits;
  - the depth of such evaluations/audits;
  - the associated fees; and
  - the procedures related to complaints from either the market or the assessed TSPs.

The assessment process is further detailed in clause 5.3.

The application of this assessment process to Conformity Assessment in the context of Directive 1999/93 [i.1] is given in annex A.

5.2.3 Responsibilities of the parties

The National Accreditation Body shall ensure that the Conformity Assessment Body is competent to carry out Conformity Assessment for the trust services being assessed.

The Conformity Assessment Body shall carry out assessment of the TSP using conformity criteria relevant to the trust service (or services) being assessed.

The TSP shall ensure that its trust service is conformant to the relevant conformity criteria and assist the Conformity Assessment Body in carrying out the assessment.

The Trust Service Status Notification Body shall ensure that a trust status list is made available to interested parties which reflects the latest Conformity Assessment of TSPs within the scope of the assessment scheme. The Trust Service Status Notification Body shall also ensure that authenticity and integrity of the trust status list is maintained.

5.3 The assessment process

5.3.1 General Overview

The Conformity Assessment process flow is depicted in figure 3.

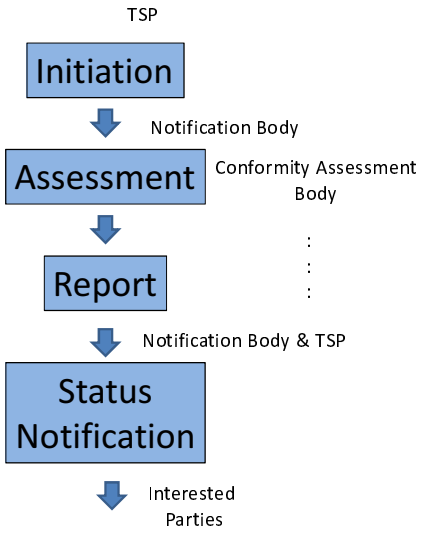

Figure 3: Conformity Assessment process flow

Initiation: The assessment process is in principle initiated by the TSP informing the Notification Body of its intentions and initiating an assessment process with the Conformity Assessment Body.

Assessment: Once the Conformity Assessment Body is designated and agreed, the assessment is performed.

Assessment report: An assessment report is established by the Conformity Assessment Body and submitted to the Notification Body and TSP.

Evaluation of the Assessment report: The assessment report is evaluated by the Notification Body.

Notification of the assessment conclusions and status notification: Based on the recommendations in the Assessment report, the Notification Body will update the trust status of the TSP for the assessed trust service.

5.3.2 Initiation

This corresponds to the information to the Notification Body of a TSP intention to be assessed.

The notification of start of the provision of services should be submitted to the Trust Service Status Notification Body at least 1 month before the intended commencement of the service. An application is submitted to the Conformity Assessment Body.

It is recommended that on initiation the TSP provides information to, the Conformity Assessment Body and, depending on confidentiality restrictions, to the Trust Service Status Notification Body. This information should include administrative and identification information about the TSP and information on the basis of which it is possible to initiate the assessment. It is recommended that the following documentation, together with the notification, is provided:

- **Administrative and identification information** related to the TSP being either a public entity or a legal or natural person, when it is established in accordance with the national law: this includes but may not be limited to the name of the TSP, company information as registered in accordance with national laws, organization and company structure, capital, balance sheet and annual reports, contact information, etc.

- **Information on the basis of which it is possible to base the assessment:** this should include information allowing an assessment of the factual, technical, security, personnel and organizational qualifications of the TSP service to which the supervision system applies. This information is recommended to be organized around the following two components:
  - A statement of the trust service (or services to be assessed).
  - The **Full Practices Statement** describing the practices the TSP employs in providing its trust services.
  - The TSP **Self-Declaration** of compliance with the applicable conformance criteria, based on the checklist.

5.3.3 Assessment process

Once having been designated and accepted by the TSP, the assessors team performs the Conformity Assessment in accordance to the trust services to be assessed.

The objective of the assessment is to confirm that the TSP complies with the applicable assessment criteria. This includes confirmation that the implemented TSPs system conforms to the requirements of the applicable legal provisions, technical standard(s) and is achieving the TSPs policy objectives in compliance with the assessment criteria.

This assessment should include visits to the site(s) of the TSP (see also clause 5.3.3.2.1 on multi-site sampling).

The Conformity Assessment Body and the TSP should agree when and where assessment process is conducted.

Assessors should perform their Conformity Assessment of the TSP's services system in at least two stages:

- Assessment stage 1: This stage focuses on the review of the TSP assessed services system documentation as it has been documented through the initiation notification and potentially augmented by a specific set of elements specifically required at this stage. On the basis of the observations made at the TSP's site in this stage, assessors shall draft a preliminary assessment report and a plan for conducting stage 2 (on-site) assessment.
- Assessment stage 2: This stage consists in an on-site assessment that aims to validate the preliminary assessment report findings and to complete the evaluation/audit assessment of the TSP assessed services against the assessment criteria.

Assessors should review, prior to commencement of the assessment that the TSP's (assessed services) system is documented, implemented, and operational and can be shown to be operational.

5.3.3.1 Assessment stage 1

In this stage of the assessment, assessors should obtain and review the documentation on the TSP's assessed service system as notified to the Notification Body respectively during initiation phase and potentially augmented with specific type of information as part of stage 1 initiation. Assessors should make the TSP aware of the further types of information and records that may be additionally required for verification during assessment stage 1.

The objectives of assessment stage 1 are to provide a focus for planning of assessment stage 2 by gaining an understanding of the structure and extent of the TSP's assessed service system. Assessment stage 1 includes but should not be restricted to document review. Other elements that could be included in assessment stage 1 are verification of records regarding legal entity, arrangements to cover liability, contractual relationships between TSP and potential contractors operating or providing sub-component services, internal/external audits or certifications, management review, and further investigations with regards to the preliminary assessment of the self-declared partial compliances or non compliances.

Assessors and the TSP should agree when and where assessment stage 1 is conducted.

5.3.3.1.1 Collecting and verifying information

In order to provide a basis for the decision to confirm that the TSP meets the requirements of the applicable standard(s) for issuing TSOs, Assessors should require clear reports that provide sufficient information to make that decision.

Reports from the assessment team to the Conformity Assessment Body are required at stage 1 in the assessment process. In combination with information held on file, these reports should at least contain:

a) A description of the organisational structure of the TSP, including the use made and organisational structure of other parties (subcontractors) that provide parts of the service.

b) An account of the assessment including a summary of the document review.

c) An account of the assessment of the TSP's information security risk analysis.

d) An account of the assessment of the TSP's organisational reliability.

e) Assessment time used and detailed specification of time spent on document review and assessment of the implementation of the TSP's management system.

f) Clarification of nonconformities.

g) Assessment enquiries that have been followed, rationale for their selection, and the methodology employed.

h) Recommendation by the assessment team to Conformity Assessment Body concerning the confirmation on whether the TSP meets the requirements of the applicable standard(s) for issuing TSOs.

NOTE 1: Text based on CWA 14172-2 [i.12], G.2.13.

Assessors should review before the assessment what records are considered as confidential or sensitive by the TSP such that the assessment team could not examine these records during the assessment of the TSP. The Assessors should judge whether the records that can be examined warrant an effective assessment. If Assessors concludes that an effective assessment is not warranted, the body should inform the TSP that the assessment could take place only when the TSP has accepted appropriate access arrangements to confidential or sensitive information.

NOTE 2: Text based on CWA 14172-2 [i.12], G.2.6.

In every case, the document review should be completed prior to the commencement of assessment stage 2.

The results of assessment stage 1 should be documented in a written report including the detailed plan and planning for conduction of assessment stage 2. This report is submitted by the Conformity Assessment Body to the Notification Body for review, validation and decision on proceeding with assessment stage 2 and for selecting assessment team members with the necessary competence based on a proposal from the Conformity Assessment Body.

Once validated by the Notification Body, assessors should make the TSP aware of assessment stage 2 planning and of the further types of information and records that may be required for detailed verification during assessment stage 2.

5.3.3.2 Assessment stage 2

This stage always takes place at the site(s) of the TSP. On the basis of observations documented in the report on assessment stage 1, Assessors drafts an assessment plan for the conduct of assessment stage 2.

The objectives of assessment stage 2 are:

a) To confirm that the TSP adheres to its own policies, objectives and procedures.

b) To confirm that the implemented TSP's management system conforms to the requirements of the applicable standard(s) and is achieving the TSP's policy objectives.

5.3.3.2.1 Multi-site sampling

The organisational structure of the TSP could be such that the same activity is performed at a number of sites or that similar or different activities are performed at a number of sites operated by different legal entities. Assessors undertaking the Conformity Assessment may opt for assessing a sample of these sites. In this case, assessors should maintain procedures that include the full range of issues below in the building of their sampling programme.

NOTE 1: See also IAF Mandatory Document for the Certification of Multiple Sites Based on Sampling [i.8].

Prior to undertaking its first assessment **based on sampling**, Assessors should publish the sampling methodology that it employs. The procedures of Assessors should ensure that the initial review of the Conformity Assessment contract with or mission against the TSP identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined in accordance with the provisions below.

Where a TSP has a number of similar sites that support the provision of its certification services, the following requirements should be fulfilled:

a) All sites of the TSP are operating under the same or similar TSP's management system that is centrally administered and audited and subject to central management review.

b) All sites have undergone internal auditing in accordance with the TSP's internal auditing procedures.

c) A representative number of sites have been sampled by Assessors, taking into account the requirements below:

   i) the results of internal audits of head office and the sites;

   ii) the results of management review;

   iii) variations in the size of the sites;

   iv) variations in the business purpose of the sites;

   v) complexity of the TSP's management system;

   vi) complexity of the information systems at the different sites;

   vii) variations in working practices;

   viii) variations in activities undertaken;

   ix) potential interaction with critical information systems or information systems processing sensitive information;

   x) differing legal requirements.

d) The sample should be partly selective based on the above in point c) and partly non-selective and should result in a range of different sites being selected, without excluding the random element of site selection.

e) Every site of the TSP that is subject to significant threats to assets, vulnerabilities or impacts should be included in the sampling programme.

f) The surveillance programme should be designed in the light of the above requirements and should, within a reasonable time, cover all sites of the TSP.

g) In the case of a non-conformity being observed either at the head office or at a single site, the corrective action procedure should apply to the head office and all sites of the TSP organisation.

h) The Conformity Assessment process should address the TSP's head office activities to ensure that a single management system applies to all sites and delivers central management at the operational level. The Conformity Assessment should address all the issues outlined above.

NOTE 2: Text based on CWA 14172-2 [i.12], G.2.7.

5.3.3.3 Assessment report to the Notification Body

The assessment report produced by the Assessors is passed to the Notification Body. The assessment conclusions can be of three natures:

1) Passed: the assessed trust service is "certified conformant".

2) Failed with severe non-conformities: the assessed trust service is not certified conformant.

3) Passed with pending non-conformities: Successful assessment status is conditioned to the implementation of corrective actions within a determined delay in function of the type and criticality of the correction(s).

The Conformity Assessment Body that assesses whether the TSP meets the requirements of the applicable standard(s) - should incorporate a level of knowledge and experience in all areas that is sufficient to evaluate the assessment processes and associated recommendations made by the assessment team. Confirmation that the TSP meets the requirements should not be given in cases where **unresolved nonconformities remain.**

The Conformity Assessment Body should **have clear procedures laying down the circumstances and conditions in which the confirmation that the TSP meets the requirements will be maintained**. If on surveillance or reassessment nonconformities are found to exist, the TSP should effectively correct such nonconformities within a time agreed. If correction is not made within the time agreed, confirmation of compliance with the requirements should be reduced, suspended or withdrawn. The time allowed to implement corrective action should be consistent with the severity of the nonconformity and the risk to the assurance of products or services meeting specified requirements.

The **documented statement confirming that the TSP meets the requirements** should be confined to declared scopes, activities and locations and should provide a short description of the TSP's organisation including identification of the legal entity and, if applicable, identification of the part of the legal entity that provides the TSP services. In addition, identification and locations should be provided and scope and activities should be described of other parties (subcontractors) that provide parts of the services.

5.3.4 Assessment conclusions and assessment status notification

Assessment conclusions and potential recommendations and/or requests for corrective actions are communicated by the Conformity Assessment Body to the TSP for implementation.

Whenever the current trust status is required to be changed, the Notification Body updates its Trust Status List based on the Conformity Assessment report.

Notification Body should not make other public statements of the capability of successfully assessed TSPs.

Assessed TSPs are permitted to keep details of their internal processes and information security measures confidential when applicable.

5.4 Regular surveillance activities

The Notification Body or the Conformity Assessment Body shall define a **programme of periodic surveillance** and reassessment at sufficiently close intervals to verify that TSPs continue to comply with the requirements. There shall be a period of no greater than one year for periodic surveillance.

Assessed TSP should submit a self-declaration annually (or at least the relevant delta from the previous self-declaration) to the Notification Body.

At each surveillance visit, the implementation of a part of the TSP's management system should be verified in each of the areas addressed in the assessment criteria (e.g. for CSP, the applicable standard regarding Certification Practice Statement, key management life cycle, public key certificate management life cycle, CSP management and operation, insurance coverage and organisational requirements).

In addition, a sample of records relating to the operation of TSP over the historical period since the previous assessment should be examined by the assessor.

The reports arising from surveillance during the period between the initial assessment and the reassessment should build up to cover in totality that the TSP meets the requirements of the applicable assessment criteria for issuing TSOs.

Surveillance reports should contain assessment information on clearing of nonconformities revealed previously.

5.5 Incident related surveillance activities

If an incident is detected by the TSP audit and monitoring systems which could potentially impact on the authenticity or integrity of the Trust Service Tokens issued or to be issued by the TSP, then the TSP shall be obliged to inform the Notification Body of such an incident with all information relevant that incident that it has available.

NOTE 1: Further work is required in refining the type of incidents to be reported.

On such notification, the Notification Body may update the trust status to indicate that the Conformity Assessment may be suspended pending further investigation of the TSP. The Notification Body should initiate a surveillance audit to be carried out by a Conformity Assessment Body and shall update the Trust Status List based on the conclusions as to whether the TSP remains conformant or is taking sufficient steps to remove the immediate risk.

Appropriate steps should be taken by the Notification Body to avoid other TSPs being vulnerable to similar security incidents.

NOTE 2: Appropriate steps may include making the report available to Conformity Assessment Bodies known to European Notification Bodies, and requesting changes to the standardised assessment criteria to avoid the risk.

5.6 Re-assessment

There should be a full re-assessment of the TSP at most every 3 years and under the following circumstances:

- whenever there are major changes of the scope;
- whenever there are major changes on the services provided under the scope;
- whenever there is included a new service in the scope;
- when there have been major change of IT systems or business processes used by TSP; or
- when there has been a significant complaint upheld by the TSP Conformity Assessment Body.

6 Requirements on TSP Conformity Assessment Body

This clause states requirements of bodies that may assess Conformity of implementations of the present document.

Principles regarding impartiality, competence, responsibility, openness, confidentiality and responsiveness to complaints as per ISO/IEC 17021:2011 [1] apply.

Requirements of ISO/IEC 17021:2011 [1], clauses 5 to 8 (included) apply with the following additions.

6.1 Assessors' code of conduct

Assessors deployed for performing TSP assessments should observe a Code of Conduct fulfilling at least the following:

a) To act in a trustworthy and unbiased manner in relation to both the body by which the assessor is employed, contracted or otherwise engaged and any other organisation involved in an assessment performed by him/her or by personnel directly under his/her control.

b) To act independently and impartially; to disclose to the body deploying him/her any relationships he/she may have or may have had with the organisation to be assessed and to decline any assignment that could cause or could be perceived as causing conflict of interest.

c) Not to accept any inducement, gift, commission, discount or any other profit from organisations assessed, from their representatives, or from any other interested person, nor knowingly allow personnel for whom he/she is responsible to do so.

d) Not to disclose the observations, or any part of them, of the assessment team for which he/she is or was responsible or of which he/she is or was part, or any other information obtained in the course of an assessment, to any third party unless authorised in writing by both the assessed organisation and the body by which the assessor is or was deployed.

e) Not to act in any way prejudicial to the reputation or interest of the body by which the assessor is or was deployed.

In the event of any alleged breach of the code of conduct, to co-operate fully in any formal enquiry procedure.

NOTE: The above is based on CWA 14172-2 [i.12], G.2.3.

6.2 Competence criteria for assessors

Each individual assessor deployed by an independent body for performing Conformity Assessment should be qualified based on the following criteria:

a) Academic qualifications should have been gained by a programme of studies consisting of a range of inter-related topics in which understanding is achieved by a predefined progression or route. It should be expected that where the assessor has accrued extensive experience and supplementary professional education and training, the requirement for academic qualifications would be significantly outweighed by their practical experience in the field.

b) Having at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to Public Key Infrastructure and Information Security Management.

c) Having demonstrated understanding of the applicable standards.

d) Having demonstrated understanding of the concepts of management systems in general.

e) Having demonstrated understanding of the issues related to various areas of Public Key Infrastructure, Information Security Management, and organisational reliability.

f) Having demonstrated understanding of the principles and processes related to risk assessment and risk management.

g) Having successfully followed a training course of at least five days on the subject of management system assessment and the management of assessment processes.

h) Having the following personal attributes: objective, mature, discerning, analytical, persistent, and realistic. The candidate should be able to put complex operations in a broad perspective and should be able to understand the role of individual units in larger organisations.

i) Having knowledge and attributes to manage the assessment process.

j) Having the ability and processes to maintain own knowledge and skills of Public Key Infrastructure, Information Security Management, and management system assessment.

k) Prior to assuming responsibility for performing as an assessor, the candidate should have gained experience in the entire process of CA assessment. This experience should have been gained by participation under supervision of qualified (lead) assessors in a minimum of **four** assessments for a total of at least **20** days, including documentation review, implementation assessment and assessment reporting.

l) All relevant experience should be current.

An assessor performing as assessment team leader (Lead Assessor) should additionally fulfil the following requirements:

m) Having acted as qualified assessor in at least three complete TSP assessments.

n) Having demonstrated to possess adequate knowledge and attributes to manage the assessment process.

o) Having demonstrated the capability to communicate effectively, both orally and in writing.

Satisfaction of more than one of these criteria may be demonstrated.

NOTE 1: The aboved is based on CWA 14172-2 [i.12], G.2.2.

Assessment teams shall be competent for the duties assigned to them. The following requirements apply to the assessment team as a whole. In each of the following areas at least one assessor in the team should satisfy Assessors's criteria for taking responsibility within the assessment team:

1) managing the team (Lead Assessor);

2) demonstrated knowledge of the legislative and regulatory requirements and of legal compliance in the particular field of certification service and information security;

3) demonstrated knowledge of the current technical state-of-art regarding Public Key Infrastructure;

4) demonstrated knowledge in technologies applicable to the TSP service being assessed;

5) demonstrated knowledge of performing information security related risk assessments so as to identify assets, threats and the vulnerabilities of the TPS and understanding their impact and their mitigation and control;

6) demonstrated knowledge of organisational reliability issues.

The assessment team should be competent to trace indications of security incidents in the TSP operations back to the appropriate elements of the CSP management system.

An assessment team may consist of one person provided that the person meets all criteria set out above.

Assessors should maintain professional liability/errors and omissions insurance enough to cover liabilities.

NOTE 2: The above is based on CWA 14172-2 [i.12], G.2.4.

6.3 Guidance on the use of technical experts

In order to ensure that the assessment team has at its disposal all necessary expertise, Technical Experts with specific knowledge regarding the following subjects:

a) knowledge of the legislative and regulatory requirements and of legal compliance in the particular field of certification service and information security;

b) knowledge of the current technical state-of-art regarding Public Key Infrastructure;

c) knowledge in technologies applicable to the TSP service being assessed; and

d) knowledge of performing information security related risk assessments so as to identify assets, threats and the vulnerabilities of the TPS and understanding their impact and their mitigation and control.

Those not satisfying all qualification criteria for individual assessors (clause 6.2, from a) to o)), may be used to assist the assessment team. Such Technical Experts should at all times be responsible to the Lead Assessor and not function independently of Assessors in the team.

NOTE: The above is based on CWA 14172-2 [i.12], G.2.5.

7 Cross border assessments

7.1 Assessment of TSPs relying on components services operating in other countries

A TSP operations may not be limited to a single country and/or may involve component services (e.g. for CSP, certificate generation, registration services, card personalisation) provided by independent service providers. For example, a TSP issuing qualified certificates in country A may support users in another country B who are registered through a separate TSP which provides registration and card production services.

The present document proposes a scheme whereby assessment should be carried out on a TSP whose operations may be split across borders and/or may involve independent bodies.

Where a Trust Service Provider (TSP) is offering (sub-) component certification services to users to another TSP primary service, the TSP offering the sub-component services may be initially assessed independent of the TSP providing the primary service. In such a situation the assessment of the primary service shall still include the assessment of the sub-components. However, this primary assessment may take the report of sub-component service as evidence that the requirements are met. This evidence shall include a check-list specifically addressing the TSP primary service policy requirements specific to the TSP component service as well as the generic requirements which are independent of the TSP. The primary TSP shall have contractual arrangements to requirements that the sub-component meets its obligations under the TSP's policy. The assessor may require to check sub-component TSPs to ensure that the requirements are carried out, and the contractual arrangements should include provisions to allow this to be carried out.

7.2 TSPs notified in one state and assessed in another

A TSP might request Conformity Assessment under an accredited Conformity Assessment Body of a Member State other than where it is established and/or comes under the remit of the Notification Body. This could happen:

- when the Member State in which the TSP is established has decided not to establish a National Accreditation Body for TSP Conformity Assessment;
- when the national Conformity Assessment bodies do not perform accreditation in respect of the Conformity Assessment activities for TSPs;
- when the Conformity Assessment bodies have not successfully undergone accreditation Conformity Assessment activities.

A Conformity Assessment Body shall answer any request of information on the assessment process received from the TSP Notification Body of the Member State in which the TSP is established. In such cases, the Trust Status Notification Body may participate as an observer. TSP Conformity Assessment Body in one state should make available reports, complaints and other relevant information to the Notification Body in another and vice versa. This may be direct or via the TSP.

A TSP Conformity Assessment Body may request another Conformity Assessment Body to carry out part of the assessment activity. In such a case, Conformity Assessment report shall be issued by the requesting body.

The parties should ensure that status and other information in the Trust status List is consistent.

NOTE: In Directive 1999/93 [i.1], article 7 requires that "*Member States shall ensure that certificates which are issued as qualified certificates to the public by a CSP established in a third country (i.e. not in a EU Member State) are recognised as legally equivalent to certificates issued by a CSP established within the Community if:*

a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or

b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or

c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations. a certification service provider (CSP)".

The present document proposes a scheme whereby a Conformity Assessment Body can satisfy option (a) directly, similarly it could be used as the basis for a process to satisfy option (c) and option (b) is effectively covered by the process identified in clause 7.1.

8 Guidance and Conformance Requirements

8.1 Guidance to Supervisory Bodies

It is recommended supervisory bodies operating under Directive 1999/93 [i.1] (see annex A) that:

a) Where it is required to carry out an assessment (evaluation), this should be conducted in line with clause 5.

b) Supervisory bodies should appoint assessors (evaluators) which meet requirements identified in clause 6.

c) The Trust Service Status Notification Body (trusted list owner):

   i) should publish information on the trust status of the TSP (CSP) based on notifications from the TSP (CSP) and assessment (evaluation) reports;

   ii) should publish the policy for setting the trust status from notifications from the TSP and assessment (evaluation) reports from conformity assessment (evaluation) bodies;

   iii) should ensure the authenticity and integrity of trust status information (trusted list);

   iv) shall conform to Commission Decision 2009/767/EC [i.4] with amendment Commission Decision 2010/425/EU [i.10] for the publication in the trusted list (National Trusted List).

NOTE: Terminology as used in applicable legislation added in brackets. See annex A for discussion on conformity assessment with the context of applicable European legislation and mapping between terminology used in the present document and terminology used in applicable European legislation.

8.2 Requirements for Conformity Assessment

Where a full conformity assessment is to be carried out:

a) The assessment shall be conducted in line with clause 5.

b) The Conformity Assessment Body shall be accredited by a National Accreditation Body to meet the requirements identified in clause 6.

c) The Trust Service Status Notification Body:

   1) shall publish information on the trust status of the TSP based on notifications from the TSP and assessment reports;

   2) shall operate to a published policy for setting the trust status from notifications from the TSP and assessment reports from conformity assessment (evaluation) bodies;

   3) shall ensure the authenticity and integrity of trust status information.

Annex A (informative): Guidance on Conformity Assessment within the context of the European Legislation

NOTE: A table mapping the terms of the present document to the terms of the Directive and the Decision is provided at the end of this annex.

A.1 Certification Services Provider versus Trust Services Provider

Directive 1999/93/EC [i.1] on a Community framework for electronic signatures (hereafter "the Directive ") mainly focuses on certification-service-providers issuing qualified certificates but it also applies to "an entity or legal or natural person who issues certificates or provides other services related to electronic signatures" (article 2.11). By so extending the basic principles the Directive 1999/93/EC can be made applicable to several other types of services ancillary to electronic signatures. These services may encompass but should not be limited to, e.g. the issuance and management of Qualified Certificates as defined in the Directive [i.1], the issuance and management of Extended Validation Certificates as defined by the Certification Authority/Browser Forum [i.6] provision of registration services, time-stamping services, directory services, validation services, the provision of electronic signature software and hardware including signature-creation devices, and computing services or consultancy services related to electronic signatures.

NOTE: The term CSP in the Directive refers to a TSP as defined in the present document, providing Trust Services related to electronic signatures.

A.2 CSP Conformance assessment under the Directive

Two mechanisms are identified in the Directive to provide CSP conformance assessment to the Directive Requirements. They are referred to as **CSP Supervision** and **CSP Voluntary accreditation**.

A.2.1 CSP Supervision

Article 3.3 of the Directive [i.1] requires that "*Each Member State **shall ensure** the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public". Consideration (13) of the Directive [i.1] states that "Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme*".

One or more CSP Supervisory Body(ies) is (are) appointed by the Member State administration.

Characteristics of CSP Supervision are:

1) CSP Supervision is **mandatory** in all Member States for CSPs issuing **Qualified Certificates to the public** (no obligation for CSPs issuing non-Qualified Certificates).

2) It applies to CSPs established in the Member State.

3) The way the supervision system is established is **left to the Member State**.

4) CSP supervision is an obligation for the Member States and is not a result of a request from the CSP.

5) Does **not** make the provision of certification-services subject to **prior authorisation**.

6) Evaluators may be appointed by the CSP Supervisory Body or the CSP itself and are not required to be accredited by a national body.

Depending on the way Member States are organised, combination of conditions 3. and 5. may lead to situations where the CSP may start operation before any actual evaluation has been performed.

The freedom in operating the supervision system in a Member State may create a substantial negative impact on the interoperable, cross-border use and mutual recognition of services related to electronic signatures and hence electronic signatures supported by such services. It is the aim of the present document to significantly reduce the differences in requirements, rules and procedures of supervision systems across Member States.

There might be some time elapsing between the start of the CSP activities (the notification) and the actual evaluation by the Supervisory Body; during this time the Supervisory Body is responsible for the supervision (in particular, the Supervision Status in the Trusted List is "under supervision" as from the beginning). The Supervisory Body needs accurate information as from the notification in order to limit the risk of letting a non-conform CSP operate before the actual evaluation can be performed.

In the supervision scheme initiation corresponds to the entrance on the market of a certification services of a CSP and the means by which the body in charge of the supervision of such services becomes aware of the new CSP's services and starts to supervise the CSP. Article 3 of the Directive 1999/93 [i.1] sets out that "*Member States shall not make the provision of certification services subject to prior authorization* but *shall ensure the establishment of an appropriate system that allows for supervision of CSPs which are established on its territory and issue qualified certificates to the public*". This obligation aims to mitigate the significant risk of entrance in the market of a non compliant CSP issuing QC, and hence to facilitate the initiation of supervision through a notification by CSPs (subject to supervision) of the start of their activities to relevant National CSP Supervisory Body.

A.2.2 CSP Voluntary Accreditation

While an "appropriate" system of supervision is mandatory for certification-service-providers issuing qualified certificates to the public, "*Member States **may introduce** or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive.*" (Directive 1999/93EC [i.1], article 3.2).

Voluntary accreditation is defined in article 2.13 as "any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body". Directive 1999/93 EC further states that certification-service-providers should be left free to adhere to and benefit from such accreditation schemes and does not oblige certification-service-providers to apply to be assessed under any applicable accreditation scheme. "voluntary accreditation" is thus requested by the CSP.

NOTE: In accordance with regulation 765/2008 [i.5], the term "voluntary accreditation" as mentioned in Directive 1999/93 [i.1] is not to be considered as accreditation in the sense of the regulation 765/2008. It is rather to be considered as the term "**Conformity Assessment"** in the present document.

Characteristics of Voluntary Accreditation:

1) voluntary accreditation is initiated by a request from the CSP;

2) does not make the provision of certification-services subject to prior authorisation, but the CSP is not entitled to exercise the particular rights stemming from the permission requested via voluntary accreditation until it has received the decision by the body;

3) voluntary accreditation can relate to any type of CSP (not only to CSPs issuing Qualified Certificates);

If claiming accredited status the CSP may not start operating before any assessment has been performed and accepted by the National Assessment Scheme. However, the CSP may operate with status "supervised" before being accredited.

In the accreditation scheme, a CSP may elect to have its operations pass a conformity assessment (known as voluntary accreditation as per the Directive) and hence audited by an Conformity Assessment Body accredited by the National Accreditation Body. If taking the accreditation path then the Supervisory Body in which the CSP is established should be informed of its intentions. A CSP may elect to be assessed some time after notification to the CSP Supervisory Body and its effective supervision by this body.

A.3 Obligation of Member States to notify to the EC

Article 11 of the Directive [i.1] requires that:

"Member States shall notify to the Commission and the other Member States the following:

a) information on national voluntary accreditation schemes, including any additional requirements pursuant to article 3(7);

b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in article 3(4);

c) the names and addresses of all accredited national certification service providers".

The EC notification page available at:

http://ec.europa.eu/information_society/policy/esignature/eu_legislation/notification/index_en.htm provides at least information (in effect only business addresses) about the supervised/accredited CSPs issuing QCs and the bodies responsible for supervision and/or accreditation in the country. This notified information, based on article 11, which is aimed mainly at relying parties is available in an unsecure manner has been de facto updated by a commission decision. Commission Decision 2009/767/EC [i.4] and its amending Decision of 28 July 2010, establishes a list of links (called List of Trusted Lists or LoTL) compiled by the European Commission pointing towards each Member State's Trusted List providing mandatory and harmonised information on the supervision/accreditation schemes and contains at least information related to the certification service providers issuing qualified certificates to the public who are supervised/accredited by them as detailed in clause 4.2.6.

A.4 Trusted Lists and National CSP Assessment Scheme

The Directive provides the qualified electronic signature (i.e. "advanced electronic signature which is based on a qualified certificate (QC) and which is created by a secure signature-creation device" as defined in [i.1], article 5.1) with a specific legal value: the equivalence to a handwritten signature. However, in the absence of trustworthy information about the supervised or accredited status of CSPs issuing QCs, the relying party could not know if a signature is really qualified without investing unreasonable auditing resources. Based on TS 102 231 [i.7] Commission Decision 2009/767/EC [i.4] and its amendment, Commission Decision 2010/425/EU [i.10], establish a legal basis and a template for Member States' national Trusted Lists of supervised and/or accredited CSPs. With regards to CSPs issuing QCs, Trusted Lists ensure that the services listed by them are by definition supervised and/or accredited. Therefore, QCs issued by these services are trustworthy, and thus the legal value of qualified signatures supported by such QCs can no longer be reasonably contested by any relying party. Additional information on other supervised/accredited services from CSPs not issuing QCs to the public (e.g. CSPs providing Time Stamping Services and issuing Time Stamp Tokens, CSPs issuing non-Qualified or Extended Validity certificates, providing registered e-mail or Long-Term Preservation Services, etc.) may be included in the Trusted List at national level on a voluntary basis.

Commission Decision 2009/767/EC [i.4] mandates Member States to designate a scheme operator to establish, maintain and publish and sign their Trusted List of certification-service-providers issuing qualified certificates to the public who are supervised by the CSP Supervisory Body and/or, if a voluntary accreditation system is established in the Member State, accredited by a CSP Accreditation Body. Under this decision one single Trusted List is to be maintained and published per Member State by a National Scheme Operator. The Commission maintains and publishes a 'compiled list' of Member States' Trusted Lists. This signed list, that is also called List of Trusted Lists, contains pointers to each national Trusted List as notified to the Commission by Member States.

In the present document, the rules controlling the Trusted List are defined by the Scheme Operator.

The assessment results are entered in the national Trusted List under Commission Decision 2009/767/EC [i.4] are required to comply with the status process flow as specified in this decision amended by Commission Decision 2010/425/EU [i.10].

A.5 Conformance assessment on policy requirements

The standardization framework associated with Directive 1999/93/EC [i.1] defines a comprehensive set of policy requirements for the provision of the range of services which underpin the provision of electronic signatures. This includes certificate and time-stamp issuance, registered electronic mail, long-term archiving, etc. These policy requirements include both technical requirements specific to the service as well as requirements on procedures covering service provider management and operation relating to information security and to organizational reliability and competence of personnel. The minimum policy requirements relating to CAs issuing Qualified Certificates are specified in TS 101 456 [i.3]. Similarly, TS 102 042 [i.2] specifies minimum policy requirements relating to CAs issuing Public Key and Extended Validation Certificates. Also, TS 102 023 [i.11] specifies policy requirements for time-stamping authorities. Policy requirements for other types of electronic signature services are to be added for other types of CSP service.

To gain confidence that these policy requirements are appropriately applied an independent assessment may be required to assure that the service provider meets the policy requirements relating to its services. In the present document it is described how conformance assessment may be achieved based upon assessment of the service provider by a team of assessors deployed by a body independent of the CSP. The assessor team performs conformance assessment against the requirements of the applicable standard (s) and reports its findings to the CSP Supervisory Body or CSP Accreditation Body which results in the publication of the trust status by the National Assessment Scheme operator in a Trusted List (see clause 4.2.6).

A.6 Applicability of Conformity Assessment to CSP Supervision and to CSP Voluntary Accreditation

A.6.1 Supervision

The process flow of supervision, the guidance and related rules to be observed by the supervisory body and the supervisory body's own personnel or external evaluators are detailed in clause 5.2.

A.6.2 Voluntary Accreditation

The present document specifies that Voluntary Accreditation is managed by an accredited audit body under the responsibility of the CSP Accreditation Body. The team of assessors for CSP Voluntary Accreditation is called CSP Auditors in the present text. Auditors are required to be independent and the Conformity Assessment Body accredited by a National Accreditation Body (in this case the CSP Accreditation Body) as set out in clauses 6.1.b) and 5.2.3 of the present document.

NOTE 1: In accordance with regulation 765/2008 [i.5], the term "voluntary accreditation" as mentioned in Directive 1999/93 [i.1] is not to be considered as accreditation in the sense of the regulation 765/2008. The terms "voluntary accreditation" in the Directive refers to the term "Conformity Assessment" in the present document.

The present document specifies that the Conformity Assessment of CSPs and providers of related trust services to standard policies and practices is performed by auditors. The auditors operate within a national scheme which publishes the results of the assessment. The scheme operator and/or its auditors are "accredited" as operating to standard audit practices by a National Accreditation Body (e.g. UKAS in UK, ENAC in Spain, DAkkS in Germany, NAT in Hungary. See full list at http://www.european-accreditation.org/content/ea/members.htm). The National Accreditation Bodies operate under common practices and have cross recognition through the European co-operation for Accreditation (EA) and all are members of the International Accreditation Forum.

NOTE 2: The International Accreditation Forum, Inc. (IAF) is the world association of Conformance Assessment Accreditation Bodies and other bodies interested in conformance assessment in the fields of management systems, products, services, personnel and other similar programmes of conformance assessment. Its primary function is to develop a single worldwide program of conformance assessment which reduces risk for business and its customers by assuring them that accredited certificates may be relied upon.

A.6.3 Specific interpretation of clauses for CSP Supervision and CSP voluntary Accreditation

As stated above, clauses 5 and 6 applies to CSP Voluntary Accreditation and may apply to CSP Supervision.

For the sake of clarity, when relevant, the reader will find here after a complement of information on these clauses in the framework of the Directive [i.1] and Decision [i.4]. When no complement of information or further interpretation is required, the reader is required to refer to the body text.

A.7 Definitions mapping

The terms defined in the main body of the present document may be related to terms used with EU legislation relating to electronic signatures as follows:

NOTE: This is informative aiming to clarify the relationship to the Directive 1999/93 [i.1] terminology and is currently under review.

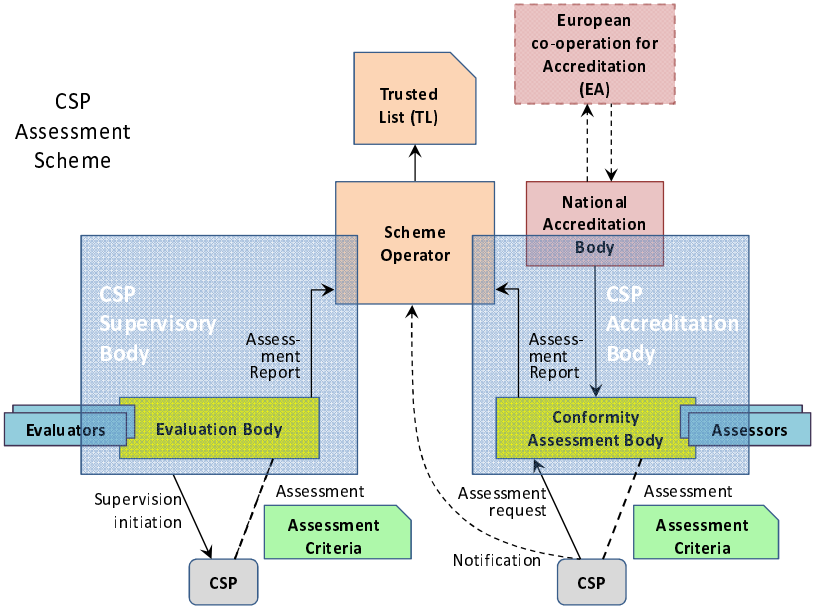

Figure A.1: Assessment Model Applied to EU Directive on E-Signatures

Table A.1: Terminology between Directives and the present document

In the present document	In the directive or the decision
CSP supervision and/or accreditation bodies may include directly or indirectly: • National Accreditation Body. • Conformity Assessment Body. • Trust Service Status Notification Body (Notification Body).	CSP related National bodies: • CSP Supervisory Body. • CSP (voluntary) Accreditation Body. • Scheme Operator (i.e. the Body in a Member State that is designated to establish, edit and maintain, and protect the trusted list). The mapping depends on the national application of the Directive/Decision: • As per the Directive the Supervisory body can also be the (Voluntary) Accreditation Body; • As per the Decision, the Trusted List owner can be the supervisory body or the Accreditation Body. In some cases, the Supervisory body, the (Voluntary) Accreditation Body and the Trusted List owner can be one single body.
Conformity Assessment Body	The term Assessment body covers bodies responsible for performing an assessment, audit or evaluation on behalf of the CSP Supervision / Accreditation body.
TSP (Trust Services Provider) providing Trust Services related to electronic signatures.	CSP (Certification Services Provider)
Conformity Assessment	Voluntary Accreditation
Assessors	The term Assessors covers both the Evaluators performing CSP Supervision and Auditors performing CSP Voluntary Accreditation.
Trust Service Status Notification Body (Notification Body).	Scheme Operator (or TSL issuer as per TS 102 231 [i.7]).
Trust Status List.	Trusted List (TL) (Profile of Trust-services Status List as per TS 102 231 [i.7] (TSL)).

Annex B (informative): Bibliography

- ISO/FDIS 19011:2011(E): "Guidelines for auditing management systems".
- ISO/IEC 27006:2007: "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems".
- IETF/RFC 2119 (March 1997): "Key words for use in RFCs to indicate Requirement Levels", S. Bradner.

History

Document history		
V1.1.1	March 2012	Publication