ETSI TS 103 090 V1.1.1 (2012-04)

Electronic Signatures and Infrastructures (ESI); Conformity Assessment for Trust Service Providers issuing Extended Validation Certificates

Reference
DTS/ESI-000108

Keywords
conformity, e-commerce, electronic signature,
extended validation certificates, 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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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).

The present document covers Conformity Assessment for Trust Service Providers (TSP) issuing extended validation certificates.

Introduction

Electronic commerce is emerging as the future way of doing business between companies across local, wide area and global networks. Trust in this way of doing business is essential for the success and continued development of electronic commerce. It is therefore important that companies using this electronic means of doing business have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their business partners. In this respect the electronic signature is an important security component that can be used to protect information and provide trust in electronic business.

The CA/Browser (CAB) Forum, an association of Certification Authorities and Web Browser providers, recognising the importance ensuring the authenticity of such Certificates have issued Guidelines for issuance and management of Certificates. Initially guidelines were issued at the "Extended Validation"(EV) level for web sites requiring enhanced security, and more recently second guidelines were issued at a "Baseline" level providing a general baseline for securing access to any web site using SSL/TLS. These guidelines specify requirements addressing particular concerns over use of certificates for web site access and code signing. They do not, however, specify general best practices for how conformity to the guidelines and best practice for Certification Authorities is audited.

Security is then recognised as a vital part of electronic commerce. This includes two essential security functions: firstly the security of access to web services using the Secure Socket Layer (SSL) protocol (now called Transport Layer Security - TLS), secondly the security of code send to users to support advanced functions using code signing. Both of these functions depend on the security of a "Public Key Certificate" (or Certificate as specified in ITU-T Recommendation X.509 [i.4]) which binds a security key to a known identity relating to the organisation responsible for the web site or code issued by a trusted service provider called a Certification Authority (CA).

ETSI, as part of the series of standard in support of electronic signatures, has developed a specification (TS 102 042 [i.1]) on "Policy Requirements for Certification Authorities issuing public key certificates". This specifies general best practices for certification authorities covering topics such as key management, personnel security and physical security. In addition, ETSI has published specific guidance on use of TS 102 042 [i.1], with the CAB Forum guidelines for Extended Validation Certificates (TR 101 564 [i.2]) to assist certification authorities and auditors in interpreting the application of TS 102 042 [i.1] to the CAB Forum EV Guidelines. The use of the specification TS 102 042 [i.1] has been formally recognised by the CAB Forum for use with their Extended Validation guidelines.

In order to assess the conformance of TSPs issuing Extended Validation Certificates, it is necessary for the operation of the TSP to be audited against this policy requirements. The present document specifies requirements and provided guidance for the carrying out of such audits. It builds on the general requirements for conformity assessment of TSPs specified in TS 119 403 [1] using the approach for "voluntary accreditation" making reference to these requirements and adding additional requirements as appropriate.

1 Scope

The present document specifies requirements and provides guidance for the supervision and assessment of a Trust Service Provider (TSP) issuing Extended Validation Certificates (EVC) through the use of audit against TS 102 042 [i.1].

It references general requirements from TS 119 403 [1] and adds further requirements as appropriate to EVC.

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 referenced 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] ETSI TS 119 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General requirements and guidance".

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

[i.2] ETSI TR 101 564: "Electronic Signatures and Infrastructures (ESI); Guidance on ETSI TS 102 042 for issuing extended validation certificates for auditors and CSPs".

[i.3] Guidelines for The Issuance and Management of Extended Validation Certificates, CA Browser Forum.

[i.4] ITU-T Recommendation X.509: "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks".

3 Definitions and abbreviations

3.1 Definitions

For the purpose of the present document, the terms and definitions given in TS 102 042 [i.1] and TS 119 403 [1] apply.

3.2 Abbreviations

For the purpose of the present document, the abbreviations given in TS 102 042 [i.1] and TS 119 403 [1] apply.

4 Introduction

This clause discusses the approach taken in TSP Conformity Assessment for issuing EVC.

The Conformity Assessment for Extended validation Certificates (EVC) applies the general system for TSP Accrediation as illustrated in figure 1.

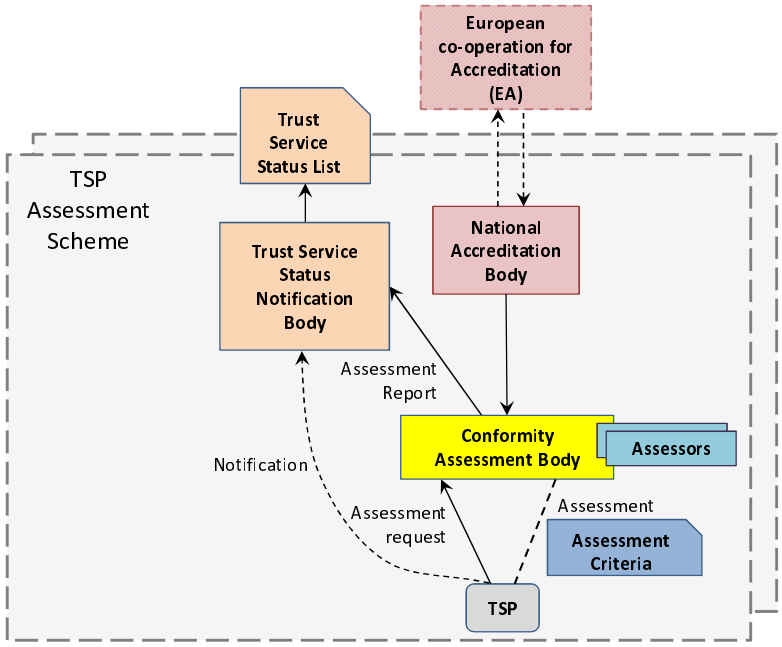

Figure 1: Organisational Structure of TSP Assessment

5 Assessment process

The assessment of the TSP issuing EVC shall be carried out as specified in clause 5 of TS 119 403 [1].

It is recommended that the checklist used for the assessment is based on TR 101 564 [i.2], Annex A.

It is recommended that the assessor produces an audit report addressing the topics identified in TR 101 564 [i.2], Annex B.

5.1 Additional audit requirements for EVC

Additional requirements on audit of TSPs issuing EVCs shall be taken into account as indicated in section 14.1.1 of EVCG [i.3]. This section specifies that before issuing EVCs, the TSP shall have a currently valid TS 102 042 [i.1] certification and then complete a point in time readiness audit against the TS 102 042 [i.1] with the EVC conformant if needed.

The TSP can use the checklist of TR 101 564 [i.2], Annex A to be prepared for this assessment process (i.e. serving as a basis for self-declaration).

These requirements shall be in accordance with clause 5.3 of TS 119 403 [1].

5.2 Publication of the Assessment report

The assessment report is provided to the Notification Body. In addition, the report may be provided to the browsers or application software providers by the TSP no later than three months after the end of the audit period as indicated in section 14.1.3 (3) of EVCG [i.3]. In the event of a delay greater than these three months, the TSP shall provide an explanation signed by the auditing body if requested.

5.3 Regular Surveillance activities

The Notification Body and the TSP should define a programme of periodic surveillance and reassessment at sufficiently close intervals to verify that TSPs continue to comply with the requirements. This programme should meet the requirements of clause 5.4 of TS 119 403 [1] and section 14.1.2 of EVCG [i.3].

5.4 Incidents handling

The TSP shall be obliged to inform the Notification Body with all the information relevant of the incident without any unnecessary delay and follow the requirements of clause 5.5 of TS 119 403 [1].

It is also recommended to notify the browsers or application software vendors.

5.5 Reassessment

The TSP audit shall follow the requirements of clause 5.6 of TS 119 403 [1].

6 Requirements on TSP conformity assessment body

The Conformity Assessment Body shall meet the requirements specified in clause 6 of TS 119 403 [1].

6.1 Competence criteria and qualification

In order to ensure that the team of assessors has at its disposal all necessary expertise, they shall meet the requirements of clause 6.2 of TS 119 403 [1] and section 14.1.4 of EVCG [i.3].

7 Cross Border Assessments

The TSP audit shall meet the requirements specified in clause 7 of TS 119 403 [1].

Annex A (informative): Self-declaration

Besides the classical administrative and identification information related to the TSP, yet another significant piece of information is recommended to be required from the TSP in the context of the initiation phase of the supervision of the TSP's services, namely the **Self-declaration of compliance against supervision criteria** of TS 102 042 [i.1]. The self-declaration of compliance could be based on a check-list organised according to the following template indicated on Annex A of TR 101 564 [i.2].

On the start of activities of a TSP issuing EVCs into the market, it is however the responsibility and obligation of the Notification Body to implement its appropriate supervision system and to perform the appropriate controls foreseen in its supervision system upon reception of a notification of the provision of certification services subject to supervision. When notification information is inexistent, incomplete, insufficient or not satisfactory with regards to compliance with the supervision criteria, and when the consecutive supervision control reveals that the TSP fails to comply with the supervision criteria, it is up to the Notification Body to take the appropriate measures to enforce corrective actions on the TSP or require the cessation of the related activities in accordance with national legislation.

The described set of notification information should actually be considered as advantageous for the TSP as the communication of a clear list of obligations for the business of TSPs issuing EVCs have to be clear and known in advance hence he has the ability to perform, before starting its activities, a self declaration on the basis of a check-list. This offers the TSP the advantage of a better preparation, from earliest stages of the conception, building and implementation of the certification services issuing EVCs and allowing TSP to maximise the chance for successful supervision.

A self declaration is not considered as evidence for conformity in line with CAB Forum EV guidelines.

History

Document history		
V1.1.1	April 2012	Publication