ETSI SR 003 091 V1.1.2 (2013-03)

Electronic Signatures and Infrastructures (ESI);
Recommendations on Governance and
Audit Regime for CAB Forum Extended Validation
and Baseline Certificates

Reference
RSR/ESI-0003091v112

Keywords
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

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 Special Report (SR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Introduction

Security is recognized 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 referred to as Transport Layer Security - TLS), secondly the security of code sent 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 Recommendation ITU-T X.509 [i.10]) which binds a public key to a known identity relating to the organization responsible for the web site or code issued by a trusted service provider called a Certification Authority (CA).

The CA Browser (CAB) Forum, an association of Certification Authorities and Web Browser providers, recognizing the importance of 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, in the case of EV, code signing. They do not, however, specify general best practices for the security certification authorities covering needs for topics such as key management, personnel security and physical security. Nor do they specify practices for how conformity to the guidelines and best practice for Certification Authorities is audited.

As part of the series of standards in support of electronic signatures, ETSI 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.4]) to assist certification authorities and auditors in interpreting the application of TS 102 042 [i.1] to the CAB Forum EV. It is also planned to produce similar guidelines for the use of TS 102 042 [i.1] with the CAB Forum Baseline. In addition, ETSI has published general guidelines and requirements for trust service provider conformity assessment (TS 119 403 [i.5]) along with specific guidance on the conformance assessment of Extended Validation certificates.

The use of the ETSI specification TS 102 042 [i.1] has been formally recognized by the CAB Forum for use with their Extended Validation and Baseline guidelines, as one the options for auditing compliance.

A governance infrastructure has been established across Europe for the "supervision" and "accreditation" of "Certification Service Providers" under the European Electronic Signatures Directive 1999/93/EC [i.11]. This scheme is primarily aimed at trust service providers issuing Qualified Certificates supporting Advanced Electronic Signatures as defined in this Directive. However, in some countries the "accreditation" scheme is flexible enough to be extensible to support trust service providers issuing other forms of certificate such as CAB Forum Baseline and Extended Validation certificates.

The present document discusses how the "accreditation" scheme established under the Electronic Signatures Directive [i.11] (cf. Article 3(2)), or an equivalent commercially based scheme, may be used alongside the ETSI specifications mentioned above for audit and governance of Certification Authorities issuing CAB Forum Baseline or Extended Validation Certificates.

1 Scope

The present document describes a recommended Governance and Audit Regime for the CAB Forum Extended Validation and Baseline certificates based on the application of ETSI Specifications (see informative references). The present document also recommends an interim approach to governance which may be applied in situations where the audit and governance infrastructure, as required by ETSI specifications, does not exist.

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.

Not applicable.

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] CA/Browser Forum: "Guidelines For The Issuance And Management Of Extended Validation Certificates".

[i.3] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

[i.4] 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.5] ETSI TS 119 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General requirements and guidance".

[i.6] 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.7] ISO/IEC 17021: "Conformity assessment - Requirements for bodies providing audit and certification of management systems".

[i.8] EN 45011: "General requirements for bodies operating product certification systems (ISO/IEC Guide 65:1996)".

[i.9] ISO DIS 17065: "Conformity assessment -- Requirements for bodies certifying products, processes and services".

[i.10] Recommendation ITU-T X.509: "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate framework".

[i.11] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.12] ISO 32000: "Document management -- Portable document format".

[i.13] ISO 27001: "Information technology -- Security techniques -- Information security management systems -- Requirements".

[i.14] ETSI TR 103 123: "Electronic Signatures and Infrastructures (ESI); Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 042 [i.1] and TS 119 403 [i.5] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 102 042 [i.1] and TS 119 403 [i.5] apply.

4 Basis for EV and Baseline Audit

4.1 EV Audit

An audit is to be carried out on Certification Authorities issuing Extended Validation Certificates. It is recommended that this audit is based on the checklist given in annex A of TR 101 564 [i.4]. This brings together the requirements of TS 102 042 [i.1] and the CAB Forum Guidelines for Extended Validation Certificates [i.2]. It should be noted, however, that the base documents should be used as the reference in case of uncertainty over requirements.

4.2 Baseline Audit

An audit is to be carried out on Certification Authorities issuing SSL Baseline Certificates. It is recommended that this audit is based on the checklist given in annex A of TR 103 123 [i.14]. This brings together the requirements of TS 102 042 [i.1] and the CAB Forum Guidelines for SSL Baseline Certificates [i.3]. It should be noted, however, that the base documents should be used as the reference in case of uncertainty over requirements.

5 Audit Process/Conformity Assessment

It is recommended that the audit is carried out by a conformity assessment body accredited by the national accreditation body in the sense of Article 4 of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 [i.6]. Additionally, these national accreditation bodies are members of the European Cooperation for Accreditation (EA). The conformity assessment body should have an accreditation certificate from the national body for assessments against TS 102 042 [i.1], CAB Forum Guidelines for Extended Validation Certificates [i.2], and CAB Forum Baseline Requirements [i.3]. It should perform the assessment in line with the procedures defined in TS 119 403 [i.5]. In the absence of an accreditation scheme for these specifications a body accredited to carry out conformity assessments against ISO 27001 [i.13] may be considered sufficient provided that it can be demonstrated that the auditors have the necessary qualifications needed to carry out audits as specified in TS 119 403 [i.5], clause 6.2 including knowledge of PKI techniques, X.509 and identity registration.

Where possible the audit should be carried out in line with TS 119 403 [i.5] otherwise the audit should at least be carried out in line with ISO/IEC 17021 [i.7] or EN 45011 (ISO guide 65) [i.8].

NOTE: EN 45011 [i.8] is currently under revision as ISO/IEC DIS 17065 [i.9].

An audit report should be produced recording the results of the audit. A suggestion for the content of the report is given in TR 101 564 [i.4], annex B. Based on the audit report, the conformity assessment body should publish the results of conformity assessment in form of a certificate that includes at minimum the names of CA and audited certification service, the relevant specification ([i.1] and [i.2] or [i.3]) and the certificate policy (e.g. EVCP), as well as the geographical location (e.g. address) of the CA's headquarter.

In line with TS 119 403 [i.5] an audit should be carried out at least every 3 years or when there is a major change to the Certification Authority. Surveillance activities are required on an annual basis.

6 Assessment Status Notification

ISO 17021 [i.7] and EN 45011 [i.8] require that conformity assessment bodies make publically accessible (or provide on request) a directory of valid conformity assessments. Where there exists a notification scheme, in line with TS 119 403 [i.5], the scheme operator should require the national conformity assessment bodies within that scheme to send it the results of the conformity assessments. The scheme operator should publish all results in a single list as described in TS 119 403 [i.5].

In the case that no such notification scheme is available, a conformity certification should be published by the Conformity Assessment Body only, preferably in PDF format protected by its digital signatures specified in ISO 32000 [i.12]. It is also requested that Conformity Assessment Bodies inform ETSI ESI secretariat of the location of the publication of this information for linking to from ETSI web page: http://www.etsi.org/WebSite/Technologies/CertificationAuthoritiesandCertificationServiceProviders.aspx.

From the assessment status notification application providers may establish their own lists of trusted root certificates for use by their application(s). The requirements of the trusted root programs of applications providers should also be taken into account. Information on the root certificate programs of major web browser and application providers is available as follows:

- Microsoft™ Root certificate Program: http://social.technet.microsoft.com/wiki/contents/articles/3281.introduction-to-the-microsoft-root-certificate-program.aspx.
- Mozilla™ (including Firefox and Thunderbird): http://www.mozilla.org/projects/security/certs/policy/.
- Opera: http://www.opera.com/docs/ca/.
- Apple™: http://www.apple.com/certificateauthority/ca_program.html.
- Google™: http://www.chromium.org/Home/chromium-security/root-ca-policy.
- Oracle™: http://www.oracle.com/technetwork/java/index-139231.html.
- Adobe™ Approved Trust List (AATL): http://www.adobe.com/security/approved-trust-list.html.

7 Governance

The competence of the Conformity Assessment Body to carry out audits should be accredited by a National Accreditation body coordinated through the European Cooperation for Accreditation (EA) and regulated under Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 [i.6].

Where there exists a national or international TSP notification scheme in line with TS 119 403 [i.5] which oversees reporting from conformity assessment bodies then the operator of that scheme should be responsible for its notifications.

In the short term each Conformity Assessment Body may be responsible for applying its own policy for notifying its own conformity assessments in line with its accreditation.

Annex A: Bibliography

ETSI TS 103 090: "Electronic Signatures and Infrastructures (ESI); Conformity Assessment for Trust Service Providers issuing Extended Validation Certificates".

History

Document history		
V1.1.1	April 2012	Publication
V1.1.2	March 2013	Publication