

Baseline requirements Version 1.0 Errata

1. Auditor Qualification Requirements

Effective 1 Jan 2013

A. In Section 3 (References), add:

ETSI Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General Requirements and Guidance, available at: http://www.etsi.org/deliver/etsi_ts/119400_119499/119403/01.01.01_60/ts_119403v010101p.pdf

Change the WebTrust reference to:

WebTrust for Certification Authorities Version 2.0, available at <http://www.webtrust.org/homepage-documents/item27839.aspx>

B. In Section 17.3, add a new first paragraph:

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 9.3.1.

C. Delete Section 17.1 and insert:

17.1 Eligible Audit Schemes

The CA SHALL undergo an audit in accordance with one of the following schemes:

1. WebTrust for Certification Authorities v2.0;
2. A national scheme that audits conformance to ETSI TS 102 042;
3. A scheme that audits conformance to ISO 21188:2006; or
4. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided

that the audit either (a) encompasses all requirements of one of the above schemes or (b) consists of comparable criteria that are available for public review.

Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Auditor, as specified in Section 17.6.

D. Delete Section 17.6 and insert:

17.6 Auditor Qualifications

The CA's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 171.);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ETSI TS 119 403, or accredited to conduct such audits under an equivalent national scheme, or accredited by a national accreditation body in line with ISO 27006 to carry out ISO 27001 audits;
5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;

6. Bound by law, government regulation, or professional code of ethics; and

7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

2. Name constraints criticality flag

Effective 8 June 2012

Delete the following text from the "Subordinate CA Certificate" section of Appendix B:

"All other fields and extensions MUST be set in accordance with RFC 5280."

AND replace it with the following:

"F. nameConstraints (optional).

If present, this extension SHOULD be marked critical*.

All other fields and extensions MUST be set in accordance with RFC 5280.

* Non-critical Name Constraints are an exception to RFC 5280 that MAY be used until the Name Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide."

3. Updates to Domain and IP Validation, High Risk Requests, and Data Source in the Baseline Requirements

Effective 22 June 2012.

A. Replace the definition of "Domain Authorization" in Section 4 of the Baseline Requirements with the following:

"Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

B. Add the following new definitions to Section 4 of the Baseline Requirements:

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate."

C. Replace Section 11.1 of the Baseline Requirements with the following:

"11.1.1 Authorization by Domain Name Registrant

For each Fully-Qualified Domain Name listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by:

1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;
2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;

3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;
4. Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN;
5. Relying upon a Domain Authorization Document;
6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN; or
7. Using any other method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant is the Domain Name Registrant or has control over the FQDN to at least the same level of assurance as those methods previously described.

Note: For purposes of determining the appropriate domain name level or Domain Namespace, the registerable Domain Name is the second-level domain for generic top-level domains (gTLD) such as .com, .net, or .org, or, if the Fully Qualified Domain Name contains a 2 letter Country Code Top-Level Domain (ccTLD), then the domain level is whatever is allowed for registration according to the rules of that ccTLD.

If the CA relies upon a Domain Authorization Document to confirm the Applicant's control over a FQDN, then the Domain Authorization Document MUST substantiate that the communication came from either the Domain Name Registrant (including any private, anonymous, or proxy registration service) or the Domain Name Registrar listed in the WHOIS. The CA MUST verify that the Domain Authorization Document was either (i) dated on or after the certificate request date or (ii) used by the CA to verify a previously issued certificate and that the Domain Name's WHOIS record has not been modified since the previous certificate's issuance.

11.1.2 Authorization for an IP Address

For each IP Address listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant has control over the IP Address by:

1. Having the Applicant demonstrate practical control over the IP Address by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the IP Address;
2. Obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC);
3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name under Section 11.1.1; or
4. Using any other method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant has control over the IP Address to at least the same level of assurance as the methods previously described."

D. Replace Section 11.3 of the Baseline Requirements with the following:

"11.3 Age of Certificate Data

Section 9.4 limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 11 to verify certificate information, provided that the CA obtained the data or document from a source specified under Section 11 no more than thirty-nine (39) months prior to issuing the certificate."

E. Replace Section 11.5 of the Baseline Requirements with the following:

"11.5 High Risk Requests

The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements."

F. Replace Section 11.6 of the Baseline Requirements with the following:

11.6 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA SHOULD consider the following during its evaluation:

- 1) The age of the information provided,
- 2) The frequency of updates to the information source,
- 3) The data provider and purpose of the data collection,
- 4) The public accessibility of the data availability, and
- 5) the relative difficulty in falsifying or altering the data.

Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under Section 11.

G. Replace Section 14.2.1 of the Baseline Requirements with the following:

"14.2.1 General

The CA MAY delegate the performance of all, or any part, of Section 11 of these Requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 11. Before the CA authorizes a Delegated Third Party to perform a delegated function, the CA SHALL contractually require the Delegated Third Party to:

- 1) Meet the qualification requirements of Section 14.1, when applicable to the delegated function;
- 2) Retain documentation in accordance with Section 15.3.2;

3) Abide by the other provisions of these Requirements that are applicable to the delegated function; and

4) Comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.

The CA SHALL verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 and the document retention and event logging requirements of Section 15.

If a Delegated Third Party fulfills any of the CA's obligations under Section 11.5 (High Risk Requests), the CA SHALL verify that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as the CA's own processes."

H. Replace Section 11.2.1 of the Baseline Requirements with the following:

"11.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation.

The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

Alternatively, the CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable."

I. Replace Section 11.2.2 of the Baseline Requirements with the following:

"11.2.2 DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by reliable documentary support;
or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable."

J. Replace Section 11.2.4 of the Baseline Requirements with the following:

"11.2.4 Verification of Individual Applicant

If an Applicant subject to this Section 11.2 is a natural person, then the CA SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

The CA SHALL verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The CA SHALL inspect the copy for any indication of alteration or falsification.

The CA SHALL verify the Applicant's address using a form of identification that the CA determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. The CA MAY rely on the same government-issued ID that was used to verify the Applicant's name.

The CA SHALL verify the certificate request with the Applicant using a Reliable Method of Communication."