

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.