Document History

Ver.	Ballot	Description	Adopted	Effective*
1.0.0	62	Version 1.0 of the Baseline Requirements Adopted	22-Nov-11	01-Jul-12
1.0.1	71	Revised Auditor Qualifications	08-May-12	01-Jan-13
1.0.2	75	Non-critical Name Constraints allowed as exception to RFC 5280	08-Jun-12	08-Jun-12
1.0.3	78	Revised Domain/IP Address Validation, High Risk Requests, and Data Sources	22-Jun-12	22-Jun-12
1.0.4	80	OCSP responses for non-issued certificates	02-Aug-12	01-Feb-13 01-Aug-13
--	83	Network and Certificate System Security Requirements adopted	03-Aug-13	01-Jan-13
1.0.5	88	User-assigned country code of XX allowed	12-Sep-12	12-Sep-12
1.1.0	--	Published as Version 1.1 with no changes from 1.0.5	14-Sep-12	14-Sep-12
1.1.1	93	Reasons for Revocation and Public Key Parameter checking	07-Nov-12	07-Nov-12 01-Jan-13
1.1.2	96	Wildcard certificates and new gTLDs	20-Feb-13	20-Feb-13 01-Sep-13
1.1.3	97	Prevention of Unknown Certificate Contents	21-Feb-13	21-Feb-13
1.1.4	99	Add DSA Keys (BR v.1.1.4)	3-May-2013	3-May-2013
1.1.5	102	Revision to subject domainComponent language in section 9.2.3	31-May-2013	31-May-2013

* Effective Date and Additionally Relevant Compliance Date(s)

Implementers' Note: Version 1.1 of these SSL Baseline Requirements was published on September 14, 2012. Version 1.1 of WebTrust's SSL Baseline Audit Criteria and ETSI Technical Standard Electronic Signatures and Infrastructures (ESI) 102 042 version 2.3.1 incorporate version 1.1 of these Baseline Requirements ~~and are currently in effect. *See* http://www.webtrust.org/homepage-documents/item27839.aspx *and also* http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.03.01_60/ts_102042v020301p.pdf.~~ .

The CA/Browser Forum continues to improve the Baseline Requirements, and we encourage all CAs to conform to each revision on the date specified without awaiting a corresponding update to an applicable audit criterion. In the event of a conflict between an existing audit criterion and a guideline revision, we will communicate with the audit community and attempt to resolve any uncertainty, and we will respond to implementation questions directed to questions@cabforum.org. Our coordination with compliance auditors will continue as we develop guideline revision cycles that harmonize with the revision cycles for audit criteria, the compliance auditing periods and cycles of CAs, and the CA/Browser Forum's guideline implementation dates.

3. References

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.~~

ETSI TS 102 042 ~~V2.1.1,~~ Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

ISO 21188:2006, Public key infrastructure for financial services -- Practices and policy framework.

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications~~, http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf.~~

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.

RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers, et al, June 1999.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.

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

X.509v3, ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

17. Audit

17.1 Eligible Audit Schemes

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

1. WebTrust Program for Certification Authorities ~~v2.0~~ audit;
2. ~~A national scheme that audits conformance to~~ ETSI TS 102 042 audit including DVCP, OVCP, EVCP or EVCP+;
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.