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

* Effective Date and Additionally Relevant Compliance Dates

Relevant Compliance Dates

Compliance	Summary Description (See Full Text for Details)
2013-01-01	For RSA public keys, CAs SHALL confirm that the value of the public exponent is an odd number equal to 3 or more.
2013-01-01	CAs SHALL support an OCSP capability using the GET method.
2013-01-01	CAs SHALL comply with the Network and Certificate System Security Requirements.
2013-08-01	OCSP Responders SHALL NOT respond "Good" for Unissued Certificates.
2013-09-01	CAs SHALL revoke any certificate where wildcard character occurs in the first label position immediately to the left of a "registry-controlled" label or "public suffix".
2013-12-31	CAs SHALL confirm that the RSA Public Key is at least 2048 bits or that one of the following ECC curves is used: P-256, P-384, or P-521. A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits MAY still serve as a trust anchor.
2015-04-01	CAs SHALL NOT issue certificates with validity periods longer than 39 months.
2015-11-01	Issuance of Certificates with Reserved IP Address or Internal Server Name prohibited.
2016-10-01	All Certificates with Reserved IP Address or Internal Server Name must be revoked.