Diff of
http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html
and
http://www.mozilla.org/projects/security/certs/policy/WorkInProgress/InclusionPolicy.html

Change 1

Version 2.0	<title>Mozilla CA Certificate Inclusion Policy</title>
Version 2.1	<title>DRAFT Mozilla CA Certificate Inclusion Policy</title>

Change 2

Version 2.0	<h1 id="page-title">Mozilla CA Certificate Inclusion Policy (Version 2.0)</h1>
Version 2.1	<h1 id="page-title">DRAFT Mozilla CA Certificate Inclusion Policy (Version 2.1)</h1>

Change 3

Version 2.0	invalid public keys (e.g., DSA certificates with 2048-bit primes, or RSA certificates with public exponent equal to
Version 2.1	invalid public keys (e.g. DELETE (bug #724038): , DSA certificates with 2048-bit primes, or RSA certificates with public exponent equal to

Change 4

Version 2.0	
Version 2.1	 enforce multi-factor authentication for all accounts capable of directly causing certificate issuance or implement technical controls operated by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses;

Change 5

Version 2.0	
Version 2.1	 maintain a certificate hierarchy such that the included certificate does not directly issue end-entity certificates to customers (e.g., the included certificate signs intermediate issuing certificates);

Change 6

Version 2.0	
Version 2.1	DELETE (Redundant with BR11.1):

Change 7

Version 2.0	
Version 2.1	

Change 8

Version 2.0	
Version 2.1	 Each externally-operated subordinate CA must either be audited in accordance with Mozilla's CA Certificate Policy or be technically constrained. Any external third party that can directly cause the issuance of a certificate must be treated as an externally-operated subordinate CA. Each externally-operated subordinate CA that is not technically constrained must be

	publicly disclosed, along with the subordinate CA's corresponding Certificate Policy or Certification Practice Statement and public attestation of the subordinate CA's conformance to the stated certificate verification requirements and other operational criteria by a competent independent party or parties with access to details of the subordinate CA's internal operations. The subordinate CA's certificate verification requirements and operational criteria must satisfy the requirements of Mozilla's CA Certificate Policy. The CA's Certificate Policy or Certification Practice Statement must indicate where the list of publicly disclosed subordinate CAs may be found on the CA's website. For an externally-operated subordinate CA to be considered technically constrained, the subordinate CA certificate (and any intermediate certificates chaining up to that certificate) must include an Extended Key Usage (EKU) extension specifying the extended key usage(s) it is authorized to issue certificates for, and the EKU must not included the anyExtendedKeyUsage KeyPurposeId. The CA must also have additional technical and contractual restrictions in place to ensure that the subordinate CA fully complies with Mozilla's CA Certificate Policy. Such controls must be documented in the CA's Certificate Policy or Certification Practice Statement, and reviewed by a competent independent party as part of the CA's annual audit. If certificates chaining up to the technically constrained externally-operated subordinate CA certificate may be used for TLS WWW server authentication, then the EKU of the subordinate CA's intermediate certificate(s) must include id-kp-serverAuth. Additionally, the subordinate CA's intermediate certificate(s) must also include X.509 dNSName Name Constraints as specified in RFC 5280, and the Name Constraints must only include domains for which the CA has confirmed that the subordinate CA has registered or has been authorized by the domain registrant to act on the registrant's behalf. If certificates chaining up to the technically constrained externally-operated subordinate CA certificate may be used for email protection, then the EKU of the subordinate CA's intermediate certificate(s) must include id-kp-emailProtection. Additionally, the subordinate CA's intermediate certificate(s) must also include rfc822Name Name Constraints as specified in RFC 5280, and the Name Constraints must only include email addresses or mailboxes for which the CA has confirmed that the subordinate CA is authorized to use. If certificates chaining up to the technically constrained externally-operated subordinate CA certificate may be used for signing of downloadable executable code, then the EKU of the subordinate CA's intermediate certificate(s) must include id-kp-codeSigning. Alternate methods of technical controls that are intended to be used instead of Name Constraints must be publicly reviewed and approved according to Mozilla's process that begins with submitting a bug report into the mozilla.org Bugzilla system, filed against the "CA Certificates" component of the "mozilla.org" product. Mozilla's wiki page, <cite>Applying for root inclusion in Mozilla products,</cite> provides further details about how to submit a formal request.

Change 9

Version 2.0	
Version 2.1	 CA operations and issuance of certificates to be used for SSL-enabled servers must also conform to the current version of the <cite> CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. </cite> In the event of inconsistency between Mozilla's CA Certificate Policy requirements and the Baseline Requirements, Mozilla's CA Certificate Policy takes precedence. The items listed below will be accepted as reason for not following the Baseline Requirements. If you find an inconsistency that is not listed here, notify Mozilla by sending email to certificates@mozilla.org so the item can be considered. - Mozilla's CA Certificate Policy defining a competent and independent auditor takes precedence over Baseline Requirement #17.6, Auditor Qualifications. - Name Constraints do not need to be marked as critical at this time.

Change 10

Version 2.0	<a href="https://wiki.mozilla.org/Module_Owners_Activities_Modules#CA_Certificates_Module">
Version 2.1	<a href="https://wiki.mozilla.org/Modules/Activities">

Change 11

Version 2.0	<a href="https://wiki.mozilla.org/Module_Owners_Activities_Modules#Governance_Module">
Version 2.1	<a href="https://wiki.mozilla.org/Modules/Activities">

Diff of
http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html
and
http://www.mozilla.org/projects/security/certs/policy/WorkInProgress/MaintenancePolicy.html

Change 1

Version 2.0	<title>Mozilla CA Certificate Maintenance Policy</title>
Version 2.1	<title>DRAFT Mozilla CA Certificate Maintenance Policy</title>

Change 2

Version 2.0	<h1 id="page-title">Mozilla CA Certificate Maintenance Policy (Version 2.0)</h1>
Version 2.1	<h1 id="page-title">DRAFT Mozilla CA Certificate Maintenance Policy (Version 2.1)</h1>

Change 3

Version 2.0	change in regards to verification procedures for issuing certificates, or when the ownership control of the CA changes. To notify us
Version 2.1	change in regards to verification procedures for issuing certificates, when the ownership control of the CA's certificate(s) changes, or when ownership control of the CA's operations changes. To notify us

Diff of
http://www.mozilla.org/projects/security/certs/policy/EnforcementPolicy.html
and
http://www.mozilla.org/projects/security/certs/policy/WorkInProgress/EnforcementPolicy.html

Change 1

Version 2.0	<title>Mozilla CA Certificate Enforcement Policy</title>
Version 2.1	<title>DRAFT Mozilla CA Certificate Enforcement Policy</title>

Change 2

Version 2.0	<h1 id="page-title">Mozilla CA Certificate Enforcement Policy (Version 2.0)</h1>
Version 2.1	<h1 id="page-title">DRAFT Mozilla CA Certificate Enforcement Policy (Version 2.1)</h1>

Change 3

Version 2.0	Mozilla may, at its sole discretion, disable or remove a certificate at any
Version 2.1	Mozilla may, at its sole discretion, disable (partially or fully) or remove a certificate at any

Change 4

Version 2.0	three trust bits (Websites, Email, Code Signing). To initiate the disablement or removal of a certificate, a representative of Mozilla will submit a bug report to
Version 2.1	three trust bits (Websites, Email, Code Signing). Disablement or removal of a certificate may be initiated by submitting a bug report to