The following text is being added to version 2.8 of Mozilla's Root Store Policy.

6.1.1 End-Entity TLS Certificate CRLRevocation Reasons

This section applies to revocations that are performed after October 1, 2022. Revocation entries that appeared on a CRL prior to October 1, 2022, do NOT need to be changed as a result of this section.

When an end-entity TLS certificate (i.e. a certificate capable of being used for TLS-enabled servers) is revoked for one of the reasons below, the specified CRLReason MUST be included in the reasonCode extension of the CRL entry corresponding to the end-entity TLS certificate. When the CRLReason code is not one of the following, then the reasonCode extension MUST NOT be provided.

- keyCompromise (RFC 5280 CRLReason #1)
- privilegeWithdrawn (RFC 5280 CRLReason #9)**
- cessationOfOperation (RFC 5280 CRLReason #5)
- affiliationChanged (RFC 5280 CRLReason #3)
- superseded (RFC 5280 CRLReason #4)

The CA's subscriber agreement for TLS end-entity certificates MUST inform certificate subscribers about the revocation reason options listed above and provide explanation about when to choose each option. Tools that the CA provides to the certificate subscriber MUST allow for these options to be easily specified when the certificate subscriber requests revocation of their certificate, with the default value being that no revocation reason is provided (i.e. the default corresponds to the CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL).

** The privilegeWithdrawn reasonCode does not need to be made available to the certificate subscriber as a revocation reason option, because the use of this reasonCode is determined by the CA and not the subscriber.

If the certificate is revoked for a reason not listed below, then the reasonCode extension MUST NOT be provided in the CRL.

keyCompromise

The CRLReason keyCompromise MUST be used when one or more of the following occurs:

- the CA obtains verifiable evidence that the certificate subscriber's private key corresponding to the public key in the certificate suffered a key compromise;
- the CA is made aware of a demonstrated or proven method that exposes the certificate subscriber's private key to compromise;
- there is clear evidence that the specific method used to generate the private key was flawed;
- the CA is made aware of a demonstrated or proven method that can easily compute the certificate subscriber's private key based on the public key in the certificate (such as a Debian weak key, see https://wiki.debian.org/TLSkeys); or
- the certificate subscriber requests that the CA revoke the certificate for this reason, with the scope of revocation being described below.

The scope of revocation depends on whether the certificate subscriber has proven possession of the private key of the certificate. A CSR alone does not prove possession of the certificate's private key for the purpose of initiating a revocation.

- If anyone requesting revocation for keyCompromise has previously demonstrated or can currently demonstrate possession of the private key of the certificate, then the CA MUST revoke all instances of that key across all subscribers.
- If the certificate subscriber requests that the CA revoke the certificate for keyCompromise, and has not previously demonstrated and cannot currently demonstrate possession of the associated private key of that certificate, the CA MAY revoke all certificates associated with that subscriber that contain that public key. The CA MUST NOT assume that it has evidence of private key compromise for the purposes of revoking the certificates of other subscribers, but MAY block issuance of future certificates with that key.

When the CA obtains verifiable evidence of private key compromise for a certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, the CA SHOULD update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension. Additionally, the CA SHOULD update the revocation date in a CRL entry when it is determined that the private key of the certificate was compromised prior to the revocation date that is indicated in the CRL entry for that certificate. Note: Backdating the revocationDate field is an exception to best practice described in RFC 5280 (section 5.3.2); however, this policy specifies the use of the revocationDate field to support TLS implementations that process the revocationDate field as the date when the certificate is first considered to be compromised.

Otherwise, the keyCompromise CRLReason MUST NOT be used.

privilegeWithdrawn

The CRLReason privilegeWithdrawn MUST be used if one or more of the following occurs and has not resulted in keyCompromise as described above.

- the CA obtains evidence that the certificate was misused;
- the CA is made aware that the certificate subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use;
- the CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name;
- the CA is made aware of a material change in the information contained in the certificate;
- the CA determines or is made aware that any of the information appearing in the certificate is inaccurate; or
- the CA is made aware that the original certificate request was not authorized and does not retroactively grant authorization.

Otherwise, the privilegeWithdrawn CRLReason MUST NOT be used.

cessationOfOperation

The CRLReason cessationOfOperation is intended to be used when the website with the certificate is shut down prior to the expiration of the certificate, or if the subscriber no longer owns or controls the domain name in the certificate. This revocation reason is intended to be

used in the following circumstances:

- the certificate subscriber no longer controls, or is no longer authorized to use, all of the domain names in the certificate;
- the certificate subscriber will no longer be using the certificate because they are discontinuing their website; or
- the CA is made aware of any circumstance indicating that use of a fully-qualified domain name or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a domain name registrant's right to use the domain name, a relevant licensing or services agreement between the domain name registrant and the applicant has terminated, or the domain name registrant has failed to renew the domain name).

Unless the keyCompromise CRLReason is being used, the CRLReason cessationOfOperation MUST be used when:

- the certificate subscriber has requested that their certificate be revoked for this reason; or
- the CA has received verifiable evidence that the certificate subscriber no longer controls, or is no longer authorized to use, all of the domain names in the certificate.

Otherwise, the cessationOfOperation CRLReason MUST NOT be used.

affiliationChanged

The CRLReason affiliationChanged is intended to be used to indicate that the subject's name or other subject information in the certificate has changed, but there is no cause to suspect that the certificate's private key has been compromised.

Unless the keyCompromise CRLReason is being used, the CRLReason affiliationChanged MUST be used when:

- the certificate subscriber has requested that their certificate be revoked for this reason; or
- the CA has replaced the certificate due to changes in the certificate's subject information and the CA has not replaced the certificate for the other reasons: keyCompromise, superseded, cessationOfOperation, or privilegeWithdrawn.

Otherwise, the affiliationChanged CRLReason MUST NOT be used.

superseded

The CRLReason superseded is intended to be used to indicate when:

- the certificate subscriber has requested a new certificate to replace an existing certificate; or
- the CA obtains reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the certificate should not be relied upon; or
- the CA has revoked the certificate for compliance reasons such as the certificate does not comply with this policy, the CA/Browser Forum's Baseline Requirements, or the CA's

CP or CPS.

Unless the keyCompromise CRLReason is being used, the CRLReason superseded MUST be used when:

- the certificate subscriber has requested that their certificate be revoked for this reason; or
- the CA has revoked the certificate due to domain authorization or compliance issues other than those related to keyCompromise or privilegeWithdrawn.

Otherwise, the superseded CRLReason MUST NOT be used.