4.9.1.1 Reasons for Revoking a Subscriber Certificate

A CRLReason MUST be included in the reasonCode extension of the CRL entry corresponding to a Certificate that is revoked after October 1, 2022. Revocation reason code entries for Certificates revoked prior to October 1, 2022, do NOT need to be added or changed.

When the CRLReason code is not one of the following, then the reasonCode extension MUST NOT be provided:

keyCompromise (RFC 5280 CRLReason #1) (see section 4.9.1.1.2);

privilegeWithdrawn (RFC 5280 CRLReason #9);**

cessationOfOperation (RFC 5280 CRLReason #5) (i.e. the Subscriber will no longer be using the Certificate because they are discontinuing their website);

affiliationChanged (RFC 5280 CRLReason #3) (i.e. identifying information about the Subscriber in the Certificate has changed); or

superseded (RFC 5280 CRLReason #4) (i.e. the Subscriber requests a new Certificate to replace an existing Certificate).

The Subscriber Agreement, or an online resource referenced therein, MUST inform Subscribers about the revocation reason options listed above and provide explanation about when to choose each option. Tools that the CA provides to the Subscriber MUST allow for these options to be easily specified when the 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 Subscriber as a revocation reason option, because the use of this reasonCode is determined by the CA and not the Subscriber.

4.9.1.1.1 Subscriber-Requested Revocation

The CA SHALL revoke a Certificate within 24 hours if the Subscriber requests in writing that the CA revoke the Certificate.~~one or more of the following occurs:~~

4.9.1.1.2 Revocation for Key Compromise

The CA SHALL revoke a Certificate within 24 hours and include the CRL revocation reason code for keyCompromise as specified in RFC 5280, if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate because of Key Compromise, with the scope of revocation being described below;

2. ~~The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;~~

~~3.~~ The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;

43. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see <https://wiki.debian.org/SSLkeys>); or

4. The CA is made aware of a demonstrated or proven method that exposes the Subscriber’s Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

The scope of revocation depends on whether the 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 Key Compromise 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 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 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 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 Key Compromise occurred 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, these Requirements specify 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 CRL revocation reason code for keyCompromise MUST NOT be used.

4.9.1.1.3 Certificate not Authorized

The CA SHALL revoke a Certificate within 24 hours and include the CRL revocation reason code for privilegeWithdrawn as specified in RFC 5280, if the Subscriber notifies the CA or the CA is made aware that the original certificate request was not authorized and that the Subscriber does not retroactively grant authorization.

4.9.1.1.4 Validation Unreliable

The CA SHALL revoke a Certificate within 24 hours and include the CRL revocation reason code for superseded as specified in RFC 5280, if

~~5. T~~the CA obtains 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.

4.9.1.1.5 Privilege Withdrawn

The CRL revocation reason code privilegeWithdrawn is intended to be used, as determined by the CA, when there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Subscriber provided misleading information in their certificate request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

The CA SHOULD revoke a C~~c~~ertificate within 24 hours and MUST revoke a Certificate within 5 days and include the CRL revocation reason code for privilegeWithdrawn as specified in RFC 5280 if one or more of the following occurs:

1. ~~The Certificate no longer complies with the requirements of [Section 6.1.5](#615-key-sizes) and [Section 6.1.6](#616-public-key-parameters-generation-and-quality-checking);~~

~~2.~~ The CA obtains evidence that the Certificate was misused;

~~3~~2. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;

~~4. 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);~~

53. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;

~~6~~4. The CA is made aware of a material change in the information contained in the Certificate; or

~~7. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;~~

~~8~~5. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate.~~;~~

Otherwise, the privilegeWithdrawn CRLReason MUST NOT be used.

See also section 4.9.1.1.3 requiring revocation within 24 hours if the original certificate request was not authorized and the Subscriber does not retroactively grant authorization.

4.9.1.1.6 cessationOfOperation

The CRL revocation reason code cessationOfOperation is intended to be used when the CA has not revoked the Certificate for keyCompromise or privilegeWithdrawn and 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.

The CA SHALL revoke a Certificate within 24 hours if the Subscriber requests in writing that the CA revoke the Certificate for cessationOfOperation. Otherwise, the CA SHOULD revoke a Certificate within 24 hours and MUST revoke a Certificate within 5 days and include the CRL revocation reason code for cessationOfOperation as specified in RFC 5280, if:

1. the CA has received verifiable evidence that the Subscriber no longer controls, or is no longer authorized to use, all of the domain names in the Certificate;

2. the Subscriber will no longer be using the Certificate because they are discontinuing their website; or

3. ~~4. T~~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)~~;~~.

Otherwise, the cessationOfOperation CRL revocation reason code MUST NOT be used.

4.9.1.1.7 affiliationChanged

The CRLReason affiliationChanged is intended to be used when the CA has not revoked the Certificate for keyCompromise, privilegeWithdrawn, or cessationOfOperation and the subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that there has been a Key Compromise.

The CA SHALL revoke a Certificate within 24 hours if the Subscriber requests in writing that the CA revoke the Certificate for affiliationChanged. Otherwise, the CA SHOULD revoke a Certificate within 24 hours and MUST revoke a Certificate within 5 days and include the CRL revocation reason code for affiliationChanged as specified in RFC 5280 if the CA is made aware that the Certificate's Subject Identity Information has changed.

Otherwise, the affiliationChanged CRLReason MUST NOT be used.

4.9.1.1.8 superseded

The CRL revocation reason code superseded is intended to be used when the CA has not revoked the Certificate for keyCompromise, privilegeWithdrawn, cessationOfOperation,or affiliationChanged, and the CA has revoked and replaced the Certificate due to domain authorization or compliance reasons, such as when the Certificate no longer complies with Section 6.1.5 or Section 6.1.6.

The CA SHALL revoke a Certificate within 24 hours if the Subscriber requests in writing that the CA revoke the Certificate for superseded. Otherwise, the CA SHOULD revoke a Certificate within 24 hours and MUST revoke a Certificate within 5 days and include the CRL revocation reason code for superseded as specified in RFC 5280 when the CA has revoked and replaced the Certificate because of domain authorization or compliance issues, or because the Certificate does not comply with these Requirements or the CA's Certificate Policy and/or Certification Practice Statement, or because revocation is otherwise required by these Requirements or the CA's Certificate Policy and/or Certification Practice Statement.

Otherwise, the superseded CRLReason MUST NOT be used.

See also section 4.9.1.1.4 requiring revocation within 24 hours if the CA obtains 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.

4.9.1.1.9 Other Circumstances

Except as revoked for the reasons set forth in the previous sections 4.9.1.1.1 through 4.9.1.1.8, the CA SHOULD revoke a Certificate within 24 hours and MUST revoke a Certificate within 5 days if

~~9. T~~the CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository.~~;~~

~~10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or~~

~~11. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.~~