TLS BRs, Section 4.9.1.1

… if one or more of the following occurs:

1. The Subscriber requests revocation (e.g. for key compromise, affiliationChanged, superseded, or cessationOfOperation). ~~in writing,~~ If the Subscriber requests revocation without specifying a CRLreason, ~~that~~ the CA SHOULD revoke the Certificate with ~~(~~CRLReason "unspecified (0)", which results in no reasonCode extension being provided in the CRL~~)~~;
2. ~~The Subscriber notifies~~ Tthe CA is made aware that the ~~original~~ certificate request or certificate issuance was not authorized, including cases where the CA failed to perform CAA checking correctly or where issuance occurred despite CAA records prohibiting it contrary to Section 3.2.2.8 (CAA Records), or where Validation of Authority was not performed in accordance with Section 3.2.5 ~~and does not retroactively grant authorization~~ (CRLReason #9, privilegeWithdrawn);
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. 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, including but not limited to those identified in Section 6.1.1.3(5) (CRLReason #1, keyCompromise);
5. 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Domain Name or IP address in the Certificate should not be relied upon (CRLReason~~-~~ #9 privilegeWithdrawn~~#4, superseded~~).

With the exception of Short-lived Subscriber Certificates, the CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days and use the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

6. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 (CRLReason~~-~~ #1 keyCompromise~~#4, superseded~~);
7. The CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
8. 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 (CRLReason #9, privilegeWithdrawn);

9. 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) (CRLReason #95, privilegeWithdrawncessationOfOperation);

10. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);

11. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #39, affiliationChangedprivilegeWithdrawn);

12. 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, in such cases, the CA SHALL first use any other subsection that applies, otherwise CRLReason #4, superseded, SHALL be used. -For example, iIf the Subscriber's private key, its parameters, or its generation method are flawed or exposed, the CA MUST use CRLReason #1, or if -(keyCompromise). If the Certificate contains incorrect subject identity information or if validation of domain authorization or control was not properly performed, then the CA MUST use CRLReason #93 (privilegeWithdrawnaffiliationChanged). For other general administrative or benign compliance-related reasons not covered elsewhereabove, the CA MUST use -(CRLReason #4 (,-superseded). Selection of CRLReason #4 does not require replacement of the Certificate;

13. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);

14. 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 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);

15. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement for a reason that is not otherwise required to be specified by this section 4.9.1.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or

16. 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 (CRLReason #1, keyCompromise).

TLS BRs, Section 7.2.2

reasonCode	RFC 5280 reasonCode value	Description
unspecified	0	Represented by the omission of a reasonCode Used when the Subscriber requests revocation but does not specify a reason or by the CA when revocation is required for a reason that does not fall within any other defined reason code. ~~MUST be omitted if the CRL entry is for a Certificate not technically capable of causing issuance unless the CRL entry is for a Subscriber Certificate subject to these Requirements revoked prior to July 15, 2023.~~
keyCompromise	1	Indicates that ~~it is known or suspected that~~ the Subscriber's Private Key has been, or is reasonably suspected of being, ~~has been~~ compromised or otherwise unreliable, including cases of weak keys, flawed generation, systemic vulnerabilities, or algorithm/parameter errors that undermine the certificate's cryptographic assurances.
~~affiliationChanged~~	~~3~~	~~Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed,~~ that domain validation was not properly performed, or that the CA has determined it must retract its assertion of any binding of identity, domain name, or IP Address in the Certificate, ~~but there is no cause to suspect that the Certificate's Private Key has been compromised.~~ This reason code is also used when the Subscriber's identity changes, but they still control the domain. For cases in which the

reasonCode	RFC 5280 reasonCode value	Description
superseded	4	~~Subscriber loses control or ownership of the domain entirely, cessationOfOperation is used.~~ Using “superseded” does not require that a replacement certificate exist or will be issued. Replacement may happen, but it is not a precondition. This code i~~l~~ndicates that the Certificate is being ~~replaced~~ revoked because ~~the subscriber is replacing it or that the CA is recommending replacement for~~ of administrative, lifecycle, or compliance reasons that do not involve key compromise, ~~affiliation change, cessation of operation,~~ subscriber misconduct, or ~~other~~ concerns about the certificate’s cryptographic or identity assurances. This includes documentation-only or process-alignment revocations (e.g., revoking certificates to match CPS wording) or other administrative ~~because: the Subscriber has requested a new Certificate, the CA has 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 these Baseline Requirements or the CA’s CP or CPS~~.
~~cessationOfOperation~~	~~5~~	~~Indicates that 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 prior to the expiration of the Certificate (i.e. website shutdown, domain transfer, or termination of a licensing or services agreement).~~
certificateHold	6	MUST NOT be included ~~if the CRL entry is for 1) a Certificate subject to these Requirements, or 2)~~

reasonCode	RFC 5280 reasonCode value	Description
privilegeWithdrawn	9	~~a Certificate not subject to these Requirements and was either A) issued on-or-after 2020-09-30 or B) has a notBefore on-or-after 2020-09-30~~. Indicates that: one or more of the identity validation steps set forth in Section 3.2 were not properly performed (e.g., 3.2.2.4/3.2.2.5 Domain Name/IP Address Validation, 3.2.2.8 CAA records, 3.2.5 ~~or~~ Validation of Authority, etc.); the Domain Name or IP Address should not be relied upon; or that there has been a subscriber-side infraction (without cause to suspect that the Certificate's Private Key has been compromised) ~~that has not resulted in keyCompromise~~, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

0 – unspecified

The CA MUST revoke the Certificate, and the CRL entry for the certificate MUST omit the reasonCode extension, which represents unspecified (0), in the following situations:

- A Subscriber requests revocation but does not provide any reason, and the CA has no other information that would justify a specific reason code.
- The CA's Certificate Policy (CP) or Certification Practice Statement (CPS) requires revocation for a reason that does not correspond to any other defined reason code.
- The CA's right or authority to issue certificates under these Requirements expires, is revoked, or is terminated, and the CA has made arrangements to continue publishing CRLs and OCSP responses.

The CA MUST NOT use this reason code if another reason code clearly applies.

In all of these situations, the CA SHOULD revoke the certificate within 24 hours and MUST revoke it within 5 days.

---

1 – keyCompromise

The CA MUST revoke the certificate, and the CRL entry for the certificate MUST include reason code **1**, representing keyCompromise, in the following situations:

- A Subscriber reports that the private key corresponding to the public key in the certificate has been lost, stolen, disclosed, or otherwise compromised.
- The CA obtains evidence, or has reasonable grounds to suspect, that the private key corresponding to the certificate has been compromised. This includes vulnerabilities in software, hardware, or protocols that can expose the contents of server memory or other storage, thereby placing the private key at risk of disclosure (for example, memory disclosure flaws such as Heartbleed).
- A method has been demonstrated that permits the derivation of the private key from the public key in the certificate.
- The certificate no longer complies with Section 6.1.5 or Section 6.1.6 of the Baseline Requirements because the private key was generated using weak or defective methods, or because insecure key parameters were used.

Revocation Timelines:

- When the compromise or suspected compromise relates to an individual Subscriber's private key, the CA MUST revoke the certificate within 24 hours of becoming aware of the situation.
- When the compromise arises from a systemic vulnerability or flaw in key generation, key storage, or cryptographic algorithms, such that multiple certificates or classes of certificates are affected, the CA MUST revoke the affected certificates within 5 days of becoming aware of the situation. Examples include large-scale vulnerabilities in cryptographic libraries or hardware (such as memory disclosure flaws or defective random number generators).

This reason code MUST be used for all cases of private key compromise or key unreliability. It MUST NOT be substituted with privilegeWithdrawn (9) or any other reason code.

---

3 – affiliationChanged

The CA MUST revoke the certificate, and the CRL entry for the certificate MUST include reason code **3**, representing affiliationChanged, in the following situations:

- A Subscriber's organization name, subject identity information, or other subject information in the certificate has changed, and there is no evidence of private key compromise.
- A Subscriber requests revocation because its identity information has changed, but the Subscriber still controls the domain name(s) in the certificate.
- There is a material change in the information contained in the certificate, and the certificate is no longer accurate, but there is no evidence of misconduct.
- The CA becomes aware that information in the certificate is inaccurate, and the inaccuracy results from benign or administrative causes (such as a corporate reorganization, renaming, or typographical error).

This reason code MUST NOT be used for domain validation failures, CAA failures, Validation of Authority failures, or Subscriber misconduct. Those situations are covered by privilegeWithdrawn (9).

In all of these situations, the CA SHOULD revoke the certificate within 24 hours and MUST revoke it within 5 days.

---

4 – superseded

The CA MUST revoke the certificate, and the CRL entry for the certificate MUST include reason code **4**, representing superseded, in the following situations:

- A Subscriber requests revocation because the certificate has been replaced with a new one, and there is no evidence of private key compromise, identity change, or cessation of operation.
- The CA determines that the certificate must be revoked for administrative or compliance reasons that do not involve key compromise, subject identity change, Subscriber misconduct, or loss of domain control.
- The CA revokes a certificate to align with its CP or CPS, or to satisfy a process-alignment or documentation requirement.

If a certificate is being revoked because the Subscriber has ceased operation or lost domain control, the CA MUST use cessationOfOperation (5) instead of superseded (4).

This reason code is also the appropriate code to use for benign, large-scale administrative revocations, such as mass revocations performed to correct or comply with documentation, align with stated practices, or otherwise replace certificates for compliance reasons where no other reason code applies.

In all of these situations, the CA SHOULD revoke the certificate within 24 hours and MUST revoke it within 5 days.

---

5 – cessationOfOperation

The CA MUST revoke the certificate, and the CRL entry for the certificate MUST include reason code **5**, representing cessationOfOperation, in the following situations:

- A Subscriber discontinues operation of the website or service associated with the certificate before the certificate's expiration.
- A Subscriber no longer owns or controls a domain name or IP address listed in the certificate. This includes situations where the domain name has been transferred to another party, where a licensing or services agreement has ended, or where the Subscriber has failed to renew the domain name.
- A Subscriber requests revocation because it has ceased operation or no longer owns or controls a domain name in the certificate.

This reason code takes precedence over superseded (4) when the cause of revocation is cessation of operation or loss of control over a domain or IP address.

In all of these situations, the CA SHOULD revoke the certificate within 24 hours and MUST revoke it within 5 days.

---

9 – privilegeWithdrawn

The CA MUST revoke the certificate, and the CRL entry for the certificate MUST include reason code **9**, representing privilegeWithdrawn, in the following situations:

- The CA issued a certificate when it was not authorized to do so, such as when issuance occurred despite Certification Authority Authorization (CAA) records prohibiting it (Section 3.2.2.8).
- The CA failed to perform Validation of Authority in accordance with Section 3.2.5.
- The CA obtains evidence that domain validation was not performed correctly and the authorization binding cannot be relied upon.
- A Subscriber provided false or misleading information in its certificate request.
- A Subscriber violated one or more material obligations under the Subscriber Agreement or Terms of Use.
- A Subscriber misused the certificate.

- A wildcard certificate was used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name.
- A Subscriber requests revocation because its authorization or privileges have been withdrawn.

This reason code MUST be used for authorization failures and Subscriber misconduct. It MUST NOT be used for benign identity changes (covered by affiliationChanged (3)) or private key compromise (covered by keyCompromise (1)).

When revocation is required due to unauthorized issuance (such as CAA or Validation of Authority failures), the CA MUST revoke the certificate within 24 hours. In all other situations in this category, the CA SHOULD revoke the certificate within 24 hours and MUST revoke it within 5 days.

With the exception of Short-lived Subscriber Certificates, the CA MUST revoke a Certificate in accordance with the following table.
Revocation reasons are listed in order of precedence: when multiple reason codes could apply to a situation, the CA MUST use the reason code that appears first in the table.

RFC 5280 `reasonCode`	**Description of Circumstance for Revocation**	**Revocation Timeline**
`keyCompromise` (1)	The CA obtains evidence that the Subscriber's Private Key is compromised, susceptible to compromise, or can be feasibly derived or exposed due to a flaw, weakness, widespread systemic vulnerability (e.g. Heartbleed), or a deficiency in the method used to generate or protect it.	MUST within 24 hours
`privilegeWithdrawn` (9)	The CA obtains evidence that the privilege to use the Certificate to represent an identity, domain, or IP address has been withdrawn, lost, or was never properly established. This includes Subscriber misuse of the Certificate, violation of material obligations under the Subscriber Agreement, or loss of legal or contractual entitlement to a domain or IP address; it also includes cases where the certificate request or issuance was not properly authorized, such as when the CA fails to properly perform validation of domain authorization or control, CAA checking under Section 3.2.2.8, Validation of Authority under Section 3.2.5, or other required authorization or verification procedures.	MUST within 24 hours
`affiliationChanged` (3)	The CA is made aware of a material change in the Subject Identity Information contained in the Certificate.	SHOULD within 24 hours, but MUST within 5 days
`superseded` (4)	The CA determines that the Certificate should be revoked for benign administrative, lifecycle, or compliance reasons not covered by keyCompromise, privilegeWithdrawn, or affiliationChanged as described above, and including documentation-related or process-alignment revocations, operational lifecycle management activities, or similar operational or administrative actions undertaken to maintain conformity with documented policies and procedures that do not affect the Certificate's cryptographic or identity assurances.	SHOULD within 24 hours, but MUST within 5 days
`cessationOfOperation` (5)	The Subscriber requests revocation because the subject or system represented in the Certificate has permanently ceased operation with no indication of key compromise.	SHOULD within 24 hours, but MUST within 5 days

RFC 5280 `reasonCode`	**Description of Circumstance for Revocation**	**Revocation Timeline**
`unspecified` (0)	The Subscriber requests revocation without specifying a reason or the reason for revocation does not fall within any of the revocation reason codes listed above in this section.	SHOULD within 24 hours, but MUST within 5 days