Reasons to Revoke

Trevoli Ponds-White

amazon trust services

Overview

- This will cover the “5 days” section of 4.9.1.1.
- Part One Goal: Review the methods to make sure we have a shared understanding of what outcome they achieve. This will enable us to be able to determine what changes may be appropriate.
- Part Two Goal: Ballot proposal to change two methods. Get feedback on the proposal to move forward with a ballot.
- Things to keep in mind:
    - Revocation reasons haven’t been updated in a long time. They were written before certificate life and validation reuse were shortened.
    - Reason 1: “*The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate*”.

Reason 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

Seems straight forward. The CA has rules. The subscriber breaks them. The certificate gets revoked.

Question for the future. Given that the CA makes the rules it's in their best interest to revoke inline with the level of risk they have identified. Does it make sense to have a 5 day requirement or does that encourage malicious compliance? In that the most efficient way to be compliant would be to have few or no rules.

Reason 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)

Questions:

1. What is acceptable proof for this method?
2. As a thought exercise if we add "domain controller/owner" to reason 1 does that satisfy the need for this reason? If not what additional benefit do we get from this?

Reason 10

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

What does this achieve beyond reasons 1 or 8?

Reason 11

"The CA is made aware of a material change in the information contained in the Certificate"

Certificates are point in time. What does this achieve beyond reasons 1 or 5?

Reason 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"*

Reason 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”

Clarity: 10 out of 10! No notes.

Reason 13

“The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate”

What does this achieve beyond reasons 1, 2, 5, or 8?

Reason 2: *“The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization”*

Reason 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”*

Section 9.6.3 requires that Subscriber Agreements require accurate information. So providing inaccurate information violates the Subscriber Agreement which is reason 8.

Reason 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”

5 days seems like an odd timeline for this reason, but the reason itself seems fine.

Reason 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”

This is clear but in practice does the 5 day timeline discourage people from adding additional requirements?

Reason 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”

The important aspect of this is already covered by reason 4.

Reason 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”*

Ballot Proposal

- Changes for reasons 6 and 7

Reason 6

“The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;”

This reason requires a ballot change. Ballots should have an effective date. Therefore we do not need this reason to have a 5 day period.

Two options:

1. Move to the 24 hour section.
2. Remove entirely. Since it requires a ballot this would not be an emergency done within 5 days regardless. Certificate lifetimes are shorter than they were when this was first written. If revocation of existing certificates is necessary that can be part of the ballot language.

Reason 7

“The CA obtains evidence that the Certificate was misused.”

Proposal: Remove it, it’s potentially duplicative without added detail to differentiate it from other reasons.

For the sake of this discussion we aren’t going to define “misused”.

Instead we will discuss what gap this reason fills that is not covered by other reasons.

What does reason 7 do that is not covered by these?

- *1) The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate
- *2) The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization
- *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
- 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
- 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
- 10) The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name
- 13) The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate
- 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

**24 hours section*