CA/BROWSER FORUM

Revocation timelines for CP/CPS discrepancies

F2F#67 10 March 2026 | Houston, Texas

Presenter: Dimitris Zacharopoulos (HARICA)

Prior discussions

- F2F#65 minutes
- F2F#66 minutes

Indicative case (not so far from reality)

- When the Forum first introduced the reduced certificate validity to 398 days, the Forum discussed the “1-sec-off” issue and introduced more complex language that said "SHOULD.... 397 days, ... SHALL 398 days". The idea was to highlight that CAs must not follow the exact limits of the BRs but should go above and beyond, implementing stricter rules to those written in the BRs
- Several CAs changed their CP/CPS documents and added the language "SHALL.... 397 days", assuming that they would now make the SHOULD into a SHALL and go "above and beyond" to what the BRs required. Some CAs made the "SHALL... **90 days**" (definitely "above and beyond" to what the BRs required)
- Effectively, these CAs documented their current practice, issuing certificates valid for 397 or 90 days.
- Guess what... These CAs detected an issue with the validity calculation, and their certificates were valid for an additional second (397 days +1sec, 90 days +1sec). The CAs are in violation with their own CP/CPS and must revoke all affected certificates within 5 days.
- If the CA wanted to be "safe" they should write in their CP/CPS exactly what was written in the BRs "SHOULD.... 397 days, ... SHALL 398 days", so that if in practice they issued 397 days + 1 second, it would not be a violation (thus no revocation needed)
- This means that the CA would not document their effective practice and Relying Parties would not know exactly what the CA effectively does but would have to rely on a "range" (up to 398 days and that's it).

Dilemma

- A CA that documents its exact practice (e.g., “397 days”) increases its exposure relative to a CA that simply mirrors the BR language.
- In effect, transparency and precision increase CA compliance risk without increasing security.
- How does the ecosystem benefit from incentivizing specific, detailed and not vague documentation?

Can security impact be assessed?

- How to assess security impact to the WebPKI ecosystem when a CP/CPS deviation takes place?
- Almost impossible to articulate. Attempts were made to assess impact:
  - 1-bit entropy serial number entropy despite using SHA-2
  - 1-second more in the validity of certificates
  - Certificates with same content and validation (due to CP/CPS mistake)
  - Allowed Key Usage (KeyEncipherment) in RSA Certificates but removed from the CP/CPS by mistake
- If the community is unable or unwilling to evaluate the security impact on these extreme examples, it's impossible to assess for other deviations.
- Browsers consider this a "risk transfer"

Baseline Requirements

- Some requirements are vague
  - 3.2.2: *“The CA SHALL inspect any document relied upon under this Section for alteration or falsification.”*
  - 4.2.1: *“The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.”*
  - 4.9.3 Procedure for revocation request
- Some are very detailed
  - 3.2.2.4.18 Agreed-Upon Change to Website v2
  - 3.2.2.8.1 DNSSEC Validation of CAA Records
  - 7.1.3 Algorithm object identifiers

Proposal (high-level)

- Allow CAs to specify stricter and more specific, detailed policies/practices but also allow them to define different revocation timelines
- Instead of allowing a “universal” extended revocation timeline for CP/CPS deviations, that are otherwise compliant with the BRs, allow the CA to explicitly define (allow-list)
  - Some cases may not result in revocation at all
- If revocation timeline is not defined, default to 5 days

Proposal (BRs language)

UPDATES TO 4.9.1.1:

- 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~~ (CRLReason #4, superseded)
- ~~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);~~

ADD THE FOLLOWING TO 4.9.1.1:

- The CA MAY document different revocation provisions in their Certificate Policy and/or Certification Practice Statement for specific policies and practices that are stricter than the policies and practices defined in these Requirements.
- If the CA is made aware that the Certificate was not issued in accordance with the CA's Certificate Policy and/or Certification Practice Statement and no alternative revocation provisions are defined, the CA SHALL revoke the Certificate within 5 days and use CRLReason #4 (superseded).

Community feedback

- “Relying parties may have relied on the CP/CPS contents when using a certificate”
  - RPs will know the **exact revocation timeline** of **specific** CP/CPS deviations that are otherwise allowed by the TBRs before relying on a certificate