Code Signing Certificate Working Group

F2F 59

6 June 2023

Redmond

CA/BROWSER FORUM

Antitrust Compliance Statement

“As you know, this meeting includes companies that compete against one another. This meeting is intended to discuss technical standards related to the provision of existing and new types of digital certificates without restricting competition in developing and marketing such certificates. This meeting is not intended to share competitively-sensitive information among competitors, and therefore all participants agree not to discuss or exchange information related to:

1. Pricing policies, pricing formulas, prices or other terms of sale;
2. Costs, cost structures, profit margins,
3. Pending or planned service offerings,
4. Customers, business, or marketing plans; or
5. The allocation of customers, territories, or products in any way.”

CA/BROWSER FORUM

Agenda

1. Assign Minute taker (start recording)
2. Roll call
3. Antitrust Compliance Statement
4. Review Agenda
5. Approval of prior meeting minutes
6. Status
   a) Ballot CSC-18: Malware based revocation – Passed, IPR review
   b) Ballot: Remove SSL BR References
   c) Ballot: Signing Service
7. Certificate Transparency for code signing certificates
8. ITU-T X.509 version in CSBR
9. Time-stamping changes
10. High Risk language removal
11. Do we need EV
12. Other Items
13. Next meeting – 15 June or cancel?

Approval of Minutes

- 18 May 2023

CA/BROWSER FORUM

Ballot Status

- CSC-18 Malware Based Revocation
  - Passed
  - IPR through 23 June 2023
  - Effective 15 April 2024
  - https://cabforum.org/2023/05/24/ballot-csc-18-update-revocation-requirements/
- Import TLS BR References
  - https://github.com/cabforum/code-signing/pull/16/files
- Signing Service
  - Plan to address after above have passed
  - https://github.com/cabforum/code-signing/pull/12/files

Certificate Transparency (CT) for Code Signing

- Discuss transparency per SCITT
  - https://scitt.io/index
- Benefits of CT
  - Transparency to cover when certificate is issued, does it meet profile, etc.
  - Monitoring of certificate issuance
- Potential CT Issues
  - CT policy required?
  - Who will mange policy?
  - How many logs?
  - Monitors? What? Who?

ITU-T x.509 version

- S/MIME BR refer to the ITU-T X.509 (10/2012)
- TLS BRs (and by extension, the Code Signing BRs) refer to the ITU-T X.509 (08/2005).
- X.509 more recent updates are (10/2019).
- Update CSBRs?

Time-stamp change

- TSA private key use period
  - CSBR 6.3.2 state 15 months
- TSA certificate validity period
  - CSBR 6.3.2 state 135 months
- TSA CA offline or online?
  - CSBRs do not state requirement
  - CSBR 4.9.7 state “For the status of Timestamp Certificates: The Subordinate CA SHALL update and reissue CRLs at least once every twelve months” which insinuates offline
- TSA reject SHA-1 hashed timestamp requests?

High Risk change proposal

- Have we mitigated high risk certificate request by requiring private keys on hardware?
- Remove High Risk Region of Concern clauses as appendix is empty/unused?
- Remove undefined “high risk application” text?
- Remove “Takeover Attack” text?

Do we need EV?

- EV is complicated with cost to the CA/Subscriber and limited benefit to the Relying Parties
- Key EV benefit is Organization validation
- Can we remove EV, but increase Organization verification requirements for Code Signing
- Note S/MIME BRs require a unique OrgID identifier

Other items

- Any other items?

Next Meeting

- Thursday, 15 June 2023, 12:00 ET or cancel?

Thank you

CA/BROWSER FORUM

CSCWG Progress
(since last F2F)

In progress:

- CSC-18 Malware Based Revocation
  - Passed
  - IPR through 23 June 2023
  - Effective 15 April 2024
  - https://cabforum.org/2023/05/24/ballot-csc-18-update-revocation-requirements/
- Import TLS BR References
  - https://github.com/cabforum/code-signing/pull/16/files
- Signing Service
  - Plan to address after above have passed
  - https://github.com/cabforum/code-signing/pull/12/files

CSCWG Goals

- Certificate Transparency for code signing certificates
- ITU-T X.509 version in CSBR
- Time-stamping changes
- High Risk language removal
- Do we need EV?
- Open-Source Project Applicants
- Code Signing validity period