# Code Signing Working Group

F2F (Virtual) 54

October 2021

CA/BROWSER FORUM

# Agenda

- Assign Minute taker (start recording)
- Roll call
- Antitrust Statement
- Goals and Progress
- Subscriber Keys
- Signing Service
- Parking Lot Items
- Other Items
- Next Meeting

# Goals and Progress

- Merge non-EV and EV requirements - DONE
- Rationalize EV requirements - DONE
- Address move to 4096-bit RSA - DONE
- Cleanup and clarify requirements - DONE
- Update Subscriber Private Key Protection requirements
- Update Signing Service requirements
- Move CSBR to Pandoc/RFC 3647 format – Update in draft
- CSBR less dependent on SSL BRs and SSL EVGs

# Subscriber Key Protection Requirements

- Key generation performed on a crypto module
- Crypto module may be operated by the Subscriber, Cloud Provider or Signing Service
- CA must verify the key was generated on a crypto module, for example
  - CA ships HSM with preinstalled key pair
  - CA provides Signing Service
  - Subscriber provides certificate request over hardware crypto service provider (CSP)
  - Subscriber uses HSM key attestation
  - Subscriber provides report of cloud key protection solution

# Signing Service Requirements

- Does not import private keys
- Secure authentication to allow Subscriber to generate the key pair or activate the private key for signing
- Logs all access, operations and configuration on the private key itself
- Logs must be available to the Subscriber
- Audit – Are these required?  CSBR, NetSec, WebTrust for CA, and ETSI audits

# CSCWG Parking Lot

| Section | Description | Owner | Priority | Comments | Ballot |
|---|---|---|---|---|---|
| 16.3 | Subscriber private key protection should be updated. Cloud-based key protection should be considered. | Ian | 1 | Presented on 6/18/20. Recommend removing CC and adding eIDAS. Outcome is that the reqts for keys would be the same for EV and non EV. Ian to propose language. | CSC-6 |
| 7.2 | Signing Service warranties should be separated from the CA warranties | Bruce/Ian | 1 | Will be address in Signing Service update ballot | |
| 13.2.1 | Invalidity Date | Corey | 1 | Windows does not support Invalidity Date. Ballot to provide calrification in CSBRs. | |
| All | Move CSBRs to RFC 3647 format and into pandoc format | Corey | 1 | | |
| 11.1.1 | Refers to non-EV CS certificates, has a requirement for additional validation for companies less than three years old (we've discussed this recently), but this requirement is missing for EV code signing certificates. | Tim H | 2 | Ballot to resolve that non-EV requirement is higher tha EV requirement | |
| 4 | SSL BR and SSL EV Guidelines versions | Bruce | 2 | Need plan to update CSBRs with latest acceptable versions of the SSL BR/EVGs | |
| 13 | Certificate suspension | Dimitris | 2 | Reference to SSL BRs may make the requirement about certificate suspension unclear. Could be resolved with a ballot indicating that certificate suspension is not allowed | |
| 11.5 | High risk certificate requests should either be removed or updated to provide common methods for all CAs. | Ian | 2 | | |
| 9.2.1 | CSBR 9.2.1 states "No stipulation". Update CSBRs to ensure SAN is not allowed. | Tim H | 2 | | |
| 9.2. | Email address in subject DN | Tim H | 2 | | |
| 11.1.2 | How to identify individuals working on open source code as part of a consortium? | Ian | 3 | Brought up by Microsoft rep at virtual F2F. Hard to get EV for these entities. Is there another way? Need separate meeting to brainstorm. Many open-source people need these. | |
| 9.2.4 | Should we address including givenName and surName in certificates? | | 4 | an to go back to platform team to check behavior. What does Microsoft need? Impacts? Value? Currently in Org field. Do we need this? | |

# Other items

# Next Meeting

- Thursday, 21 October 2021, 12:00 ET

# Thank you

CA/BROWSER FORUM