Code Signing Certificate Working Group

F2F 57

October 2022

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.

Agenda

- Assign Minute taker (start recording)
- Roll call
- Antitrust Statement
- Approval of prior meeting minutes – 6 October
- Election of Chair and Vice-chair
- Signing Service
- Plans for the next 2-years
- Other Items
- Next Meeting

Signing Service Status

Status

- Signing Service ballot has been drafted to address issues discussed in previous meetings – https://github.com/cabforum/code-signing/pull/12/files
- Issue regarding verification vs. audit to be discussed

Signing Models

- Subscriber uses token or server HSM - verification
- Subscriber uses cloud service - verification
- Signing services hosts HSM - audit
- Signing Service hosts HSM with protected Private Keys in cloud service – audit, except cloud service
- Signing Service uses cloud service to generate and store Private Keys - audit, except cloud service

Signing Service Requirements

- Generation Subscriber Key Pair in hardware crypto module
- Operate the hardware crypto module to a standard
- Provide the Subscriber secure access to activate their Private Key for signing

Signing Service – Cloud-based Key Generation

- Cloud-based key generation is allowed
- How do we determine what cloud-based key generation is?
- Can the CA can provide cloud-based key generation?
- If the CA provides cloud-based key generation, then what audit requirements apply?

2-Year Goals

- Revocation due to signed malware
- Signing Service requirements
- Remove references to TLS BRs
- Time-stamp updates
- High Risk Applicants (may be resolved with private key generation on hardware crypto module)
- Open-Source Project Applicants
- Code Signing validity period
- Short-lived certificates
- CT for code signing certificates

Other items

Next Meeting

- Thursday, 3 November 2022, 12:00 ET (OR should we cancel and schedule 17 November?)

Thank you

CA/BROWSER FORUM

CSCWG Progress
(since last F2F)

- Subscriber Private Key Protection (effective date extended to 1 June 2023)

CSCWG Goals

- Revocation due to signed malware
- Signing Service requirements update
- Remove references to TLS BRs
- Time-stamp updates
- High Risk Applicants
- Open-Source Project Applicants