Code Signing Certificate Working Group

F2F 56

June 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
- Progress and Goals
- Fall Election
- Signing Service
- High Risk Applicants
- Time-stamp Updates
- Other Items
- Next Meeting

CSCWG Progress

- Subscriber Private Key Protection
- CSBR to Pandoc/RFC 3647 format

CSCWG 2022 Goals

- Signing Service requirements
- High Risk Applicants
- Remove references to TLS BRs
- Time-stamp updates
- Open-Source Project Applicants

Fall Election

- Chair and Vice-chair positions are open
- Assume current Chair and/or Vice-chair can be nominated

Signing Service Requirements

Scope

- Performed by the CA or a trusted third party
- Not a CA requirement, so not a function of a Delegated Third Party
- Remove references when not required to limit implied scope
- Not a Subscriber, so all Private Keys are only associated to certificate Subscriber
- Not an RA, so will not receive certificate requests from an Applicant – CA or Delegated Third Party RA will receive certificate requests
- Signing Request requirements will not be specified in the CSBRs

Signing Service Requirements

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?

High Risk Applicants (Take-over Attacks)

- Take-over attacked means Subscriber cannot use method 3 (software key generation). Note this method goes away on 15 November 2022
- CA must verify that method 3 is no longer used by a Take-over Subscriber
- After 15 November 2022, propose to remove this section as the Take-over attack methodology has been removed

Time-stamp Updates

- Microsoft policy
- Rekey requirement
  - Currently max. 15 months
- Certificate validity period
  - Currently max. 135 months
  - To support Java, we could consider rekey period (15 months) plus certificate validity period (39 months), so 54 months
- Time-stamp CA online/offline clarification
  - CSBRs allow for 12-month CRLs
- Should the TSA provide a TSA practices statement (TPS)?
  - Format could follow RFC 3628 or ETSI EN 319 421

Other items

Next Meeting

- Thursday, 16 June 2022, 12:00 ET (should we cancel?)

Thank you

CAB CA/BROWSER FORUM