CCADB News - CABF F2F February 2019

CCADB Policy

Section 5.1 was added to the CCADB Policy to specify the information that must be in audit statements, and the format for SHA256 thumbprints and dates. Please make sure your auditors are aware of these requirements.
https://www.ccadb.org/policy#51-audit-statement-content

ALV for Intermediate Certificates

The following two fields are set by running Audit Letter Validation (ALV) on an intermediate certificate record in the CCADB. CAs may cause ALV to be run on the record by clicking on the "Audit Letter Validation [ALV]" button. Additionally CCADB has automated processes that are triggered when new audit statements are provided that will check for intermediate certificate records that need ALV validation.

- Standard Audit ALV Found Cert
    - This field will be set to PASS when ALV finds both the SHA-256 Fingerprint for that certificate and the name and version of the applicable ETSI or Webtrust standard in the audit statement.
- BR Audit ALV Found Cert
    - This field will only be set when the "Derived Trust Bits" field has 'Server Authentication' in its list.
    - This field will be set to PASS when ALV finds both the SHA-256 Fingerprint for that certificate and the name and version of the applicable ETSI or Webtrust standard in the BR audit statement.
- Note: We plan to extend this to EV audits within the next few months
- Acceptable names and versions of audit standards can be found on the brower's webpages.
    - Microsoft: https://aka.ms/auditreqs
    - Mozilla: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/#31-audits.

On your CA Task List on your CCADB homepage look for "Intermediate Certs with Failed ALV Results", if it is not 0, then click on "Check failed Audit Letter Validation (ALV) results" to see a table listing the certificate records that need attention.

- Microsoft: TBD
- Mozilla: https://wiki.mozilla.org/CA/Audit_Letter_Validation

Multiple CP/CPS Documents

We are working to enable the ability for CAs to specify many CP/CPS urls. Currently CCADB only allows for one CP URL and one CPS URL per root cert. The new capability will enable many-to-many mapping between CP/CPS documents and root certificates.

- Currently only available in Sandbox, **looking for CA volunteers to try this new functionality in Sandbox and provide feedback.**
- Screen Shots

Audits

ALV assumes that SHA256 thumbprints are listed in the audit statement PDF for the certificates **that were in scope** of the audit. So we have a few questions:

- Do any audit statements (ETSI or WebTrust) list SHA256 thumbprints for certificates that are not in scope of the audit or that have reduced audit scope?
- If yes, would it be reasonable to prescribe a prefix or postfix to be added to such SHA256 thumbprints? E.g
    - 001686CD181F83A1B1217D305B365C41E3470A78A1D37B134A98CD547B92DAB3**
- If this is only occurring in CA Management Assertions, then would it be reasonable to to prescribe a prefix or postfix to be added to the SHA256 thumbprints for the certs that were not audited or audited to reduced scope?