CCADB News - CABF F2F November 2019

ALV for Intermediate Certificates

- “Audit Letter Validation (ALV)” button added to intermediate certificate records.
    - ALV checks Standard Audit and BR Audit (when ‘Derived Trust Bits’ contains “Server Authentication”)
    - Plan to add ALV checks for EV SSL Audits soon, which will take EV Policy OIDs into account to determine if the intermediate cert should be in the parent’s EV audit statement.
- New CA Task List Item: “Intermediate Certs with Failed Audit Letter Validation”
    - CAs are responsible for the audits of their subordinate CAs.
    - This task list item is focussed on certs for which the SHA-256 fingerprint was not found in the required audit statements.
- DETAILS:
    - Mozilla.dev.security.policy announcement
    - Automated process run nightly to run ALV on non-expired, non-revoked intermediate certs when ‘Date ALV Processed’ is older than the date of the relevant audit statements
    - Derived Trust Bits are determined from the cert’s EKU if present, otherwise they are based on the applicable root certs’ trust bits. (cross-signed roots also taken into account)
    - For the intermediate certs with “Audits Same as Parent”, CCADB will look up the cert hierarchy to find the parent cert that has the audit statements. Then ALV will be run to ensure that the intermediate cert is indeed in those audit statements that are applicable according to the “Derived Trust Bits” field.

Audits

To improve the success rate of ALV, please have your auditors use the following format guidelines in all future audit statements. This is especially important now that we have extended ALV to intermediate certs.

- **Dates**
    - Accepted date formats (month names in English):

Month DD, YYYY	example: May 7, 2016
DD Month YYYY	example: 7 May 2016
YYYY-MM-DD	example: 2016-05-07

    - No extra text within the date, such as “7th” or “the”
- **SHA256 Thumbprint**
    - No colons, no spaces, and no linefeeds
    - Uppercase letters
    - Should be encoded in the document (PDF) as “selectable” text, not an image

This will be added to the CCADB Policy soon.

Updated CCADB Policy to add exceptions to providing audit information for intermediate certs in CCADB:

- The SHA-256 fingerprint of the certificate is specifically listed as in scope in the audit statements of the parent certificate, and the “Audits Same as Parent” checkbox is checked; or
- The certificate has expired; or
- The certificate is technically-constrained as described in section 7.1.5 of the CA/Browser Forum Baseline Requirements, or
- The certificate has been revoked, and the corresponding record in the CCADB has been updated with the correct revocation status.

Verify Revocation

Added a “Verify Revocation” button to intermediate certificate records, which will check the CRL of the certificate to make sure that the revocation information provided in the CCADB matches the information in the CRL. If the certificate does not contain a CRL URL, then you can add the URL to the “Alternate CRL” field.

Policy Identifiers

We would like to have better indication about which CP/CPS documents apply to certificates within a CA hierarchy, so we added fields to CCADB records listing the Policy OID values extracted from the certificate PEM.

- Added ‘Policy Identifiers’ field to root and intermediate cert records in the “Certificate Data” section.
    - Automatically filled in when PEM for the record is added or updated.
- Added ‘Policy Identifiers’ field to CA Owner records in the “Other CA Information” section.
    - Automatically filled in based on the CA’s root and intermediate cert records.
    - Unique identifiers, sorted alphanumerically.
- Screen Shots

CP/CPS Objects and Associations

- Enabling 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
- “Add CP/CPS Documents” button in Audit Cases (and root inclusion cases)
    - For each CP/CPS Document that you add, provide:
        - Document Type (CP, CPS, CP/CPS)
        - Document Link
        - Document Last Update Date

        - Associated Trust Bits (Secure Email, Server Authentication Client Authentication, Code Signing, etc.)
        - Policy Identifiers (pick list from CA Owner's Policy Identifiers)
    - Then identify which root certs (CA hierarchies) the document applies to.
        - "Select applicable root certificates (Count of previously selected and saved root certificates: 4)"
    - Add as many Policy Documents as needed - current versions only.
- When a root store operator finishes processing the Case, the document objects and associations will get copied to the corresponding root cert records.
- CAs will be able to modify and add policy documents and associations throughout the year. Those will get copied to the next Case that the CA creates, based on the associated root certs.