CCADB News - CABF F2F June 2020

ALV for Intermediate Certificates

Thanks to all of you who have resolved failures reported via the Audit Letter Validation (ALV) tool in the CCADB. A lot of progress has been made in regards to running ALV on intermediate certificates, and new audit statements are providing the information in a format that improves ALV accuracy.

The most common problems resulting in ALV errors are:

- SHA256 fingerprints cannot be found in the audit statements because
    - The PDF is not text-searchable
    - The SHA256 Fingerprints have linefeeds in them
    - The fingerprints are not listed for all of the certs (results in a CA Compliance Bug)
- ALV unable to find the audit period dates.

For SHA256 and audit period date format specifications, see Section 5.1 of the CCADB Policy.
https://www.ccadb.org/policy#51-audit-statement-content

To see if your CA has intermediate certs that ALV did not find in the corresponding audit statements, go to your CCADB homepage and look in the CA Task List section 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.

Information about what to do if there are failures listed:
https://wiki.mozilla.org/CA/Audit_Statements#Intermediate_Certificates

Auditor Qualifications

Some of you may notice that your Audit Case or Root Inclusion Case has the message: "Auditor Verification Date is blank". This is because we recently added a field to Auditor Location objects called "Date Qualifications Verified", which will be used to remind us to check each auditor's qualifications every year. This field can only be edited by a root store operator, and we will enter this date whenever we confirm that the auditor is still qualified to perform ETSI or WebTrust audits as described here:
https://wiki.mozilla.org/CA/Audit_Statements#Auditor_Qualifications
Request for feedback:
https://groups.google.com/d/msg/mozilla.dev.security.policy/jBFkGwPXF-Y/pM7qbns1AgAJ

Instructions for viewing list of qualified auditors in CCADB: Open any Audit Case or Root Inclusion Case via the 'Cases' tab. In the Custom Links section click on the 'List All Auditors' link.
Notes:

- This list is based on reviews/updates performed by root store operators, and the list may be changed at any time by any participating root store operator. If you do not see your auditor listed, contact the applicable root store operator.
- This list is not intended to be published in any form.
- Currently 'Date Qualifications Verified' is empty for all ETSI auditors, because I am waiting for feedback on the auditor-verification process for ETSI.)

To Do: Display the "Date Qualifications Verified" field in the 'Auditor Information' section on intermediate cert pages, and add the corresponding warning messages for when the auditor verification date is empty or old.

Multiple CP/CPS Documents

Currently CCADB only allows for one CP URL and one CPS URL per root certificate, so we have been working on updating the CCADB to enable many-to-many mapping between policy documents and root certificates. One or more policy documents may be provided and associated with one or more root certificates and policy OIDs.

- Screen Shots

Timeline: Rollout to production in July 2020. One-time migration from existing fields to new Policy Document objects.

Request: Would like to have at least one CA try this in Sandbox before we roll it out to production. Please send email to Kathleen if you can sign up to try this out.