Browser News - Mozilla

CA/B Forum F2F
February 26, 2024

Ben Wilson

Link to Previous Mozilla October 2023 Face-to-Face briefing - https://cabforum.org/uploads/2023-October-Mozilla-Browser-News.pdf

Re-Cap from Last Update

- **Root CA Lifecycles** - Ben is working on a CCADB design document to create Root Program and CA task lists for retiring roots, which would be based on a report of key generation dates. From the reports we could use the CCADB for calendaring/alerting sufficiently in advance about the need to remove or distrust a root (e.g. heads-up alerts by year 13 and highlight for year 14). For this to work, we will have to ensure that CA operators have populated the Key Generation Date field in the CCADB.
- **S/MIME Compliance, Incidents and Audits** - We are still going through a transition phase in which CA operators have discovered that they did not foresee the complications they would face in creating BR-compliant issuance systems. However, going forward we will be scrutinizing these incident reports more closely. We have received a few audits for compliance with the S/MIME Baseline Requirements.
- **Submission of Compliance Self-Assessments** - CAs should be updating the CCADB with links to their most recent Compliance Self Assessment. The most recent version of the Compliance Self Assessment is at https://www.ccadb.org/cas/self-assessment.

CA Compliance - https://wiki.mozilla.org/CA/Incident_Dashboard

Current open bugs can be found in the Incident Dashboard (currently less than 30 are open).

Bugzilla incidents that were open between October 1, 2023, and February 1, 2024, have been categorized as follows:

Type of Incident	Count
[ov-misissuance] and/or [ev-misissuance]	19
[smime-misissuance]	15
[leaf-revocation-delay]	9
[dv-misissuance] and/or [ov-misissuance]	8
[policy-failure]	8

[audit-finding]	7
[crl-failure] and/or [ocsp-failure]	7
[disclosure-failure]	2
[uncategorized]	2
[ca-misissuance]	1
[audit-delay]	1
TOTAL	**79**

This table is illustrated by the following pie chart.

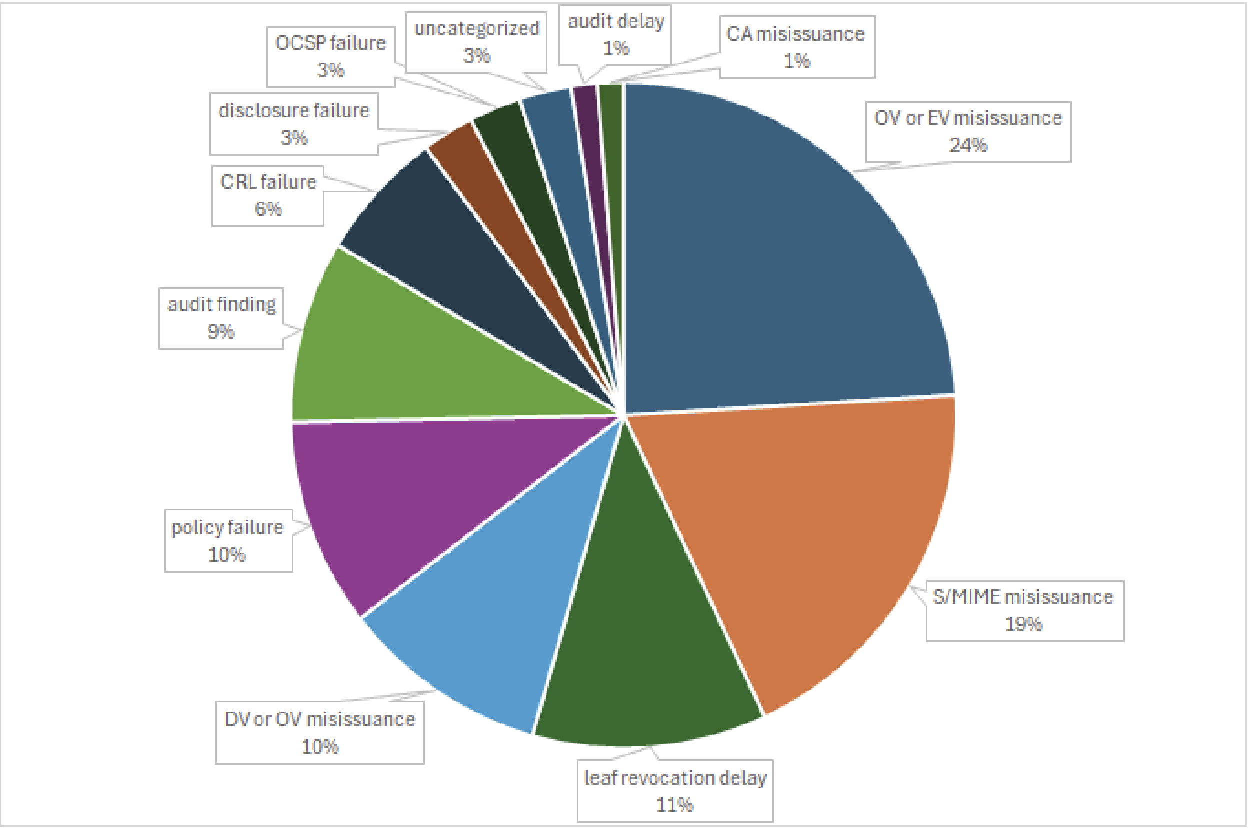

Chart: Type of Compliance Incident

At some point we may re-categorize these tags for compliance incidents so that they are more descriptive. The new Incident Reporting Template, https://www.ccadb.org/cas/incident-report#incident-report-template, has been helpful in categorizing underlying causes of compliance incidents. As you can see, the majority of incidents are characterized as mis-issuances. So, I further divided this group based on the information provided by CAs in their incident reports. The following is an illustrative pie chart.

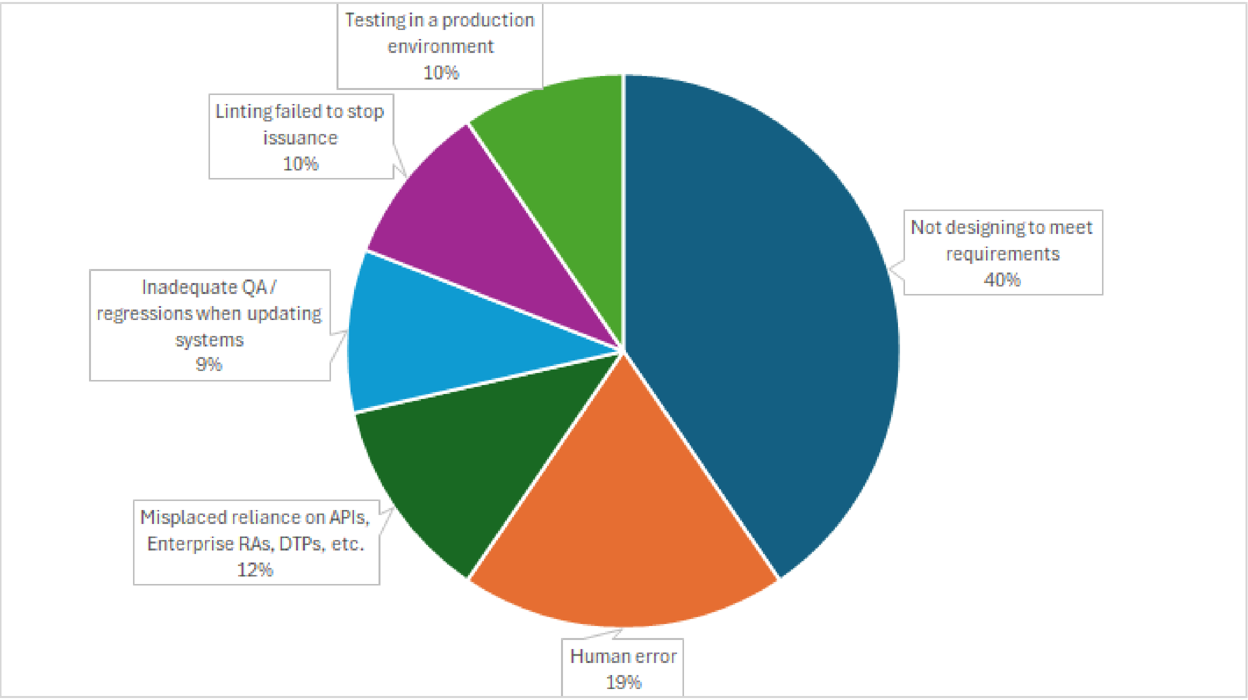

Chart: High-level Causes of Certificate Mis-issuance Incidents

Causes of Certificate Mis-issuance over Last 6 Months

Not designing to meet requirements (e.g. S/MIME BRs):

New Requirements – The adoption of the S/MIME Baseline Requirements was occasioned by delayed implementation and faulty code design practices (not being thorough enough in reviewing S/MIME BRs and identifying needed code/profile changes due to the S/MIME BRs). For example, one CA operator identified that updating its data re-use checks for S/MIME certificate issuance fell through the cracks.

Updates to Requirements – The adoption of v. 2.0 of the TLS Baseline Requirements (i.e. the "Profiles" ballot) was occasioned with erroneous conclusions that the changes were minimal and that no changes would be needed for certificate profiles. For example, there were misplaced assumptions about attribute order, and some CA operators indicated that they did not allocate sufficient time and resources to comply on a timely basis.

Older/Existing Requirements– Some CAs still have trouble complying with long-standing requirements. For example, some had poorly designed processes for using WHOIS, submitting certificates to CT, and using information in CSRs (the latter resulting in certificates containing OUs or garbled information). Recently, some CA operators experienced misunderstandings about how they were using Delegated Third Parties for domain validation.

Other Causes of Certificate Mis-issuance

Human error:

Simple human error will always be the cause of a few incidents. Reasons given for these human-caused incidents include: typos, lack of training, performing redundant/repetitive processes without preparation for edge cases, need to quickly change or bypass automated processes (e.g. human error in updating flat file because internal clients were unable to dynamically respond to DV challenges), and human error not caught by pre-issuance linting.

Misplaced reliance on APIs, Enterprise RAs, DTPs, IDPs, etc.:

Soome CA operators were caught with surprise that their APIs for Enterprise RAs/Technically-Constrained CAs: (1) lacked functionality, (2) that field values (CNs, CP OIDs, etc.) submitted by third parties (RAs, identity providers, and others) were not screened prior to issuance, and (3) that these parties were not sufficiently informed or failed to follow CA-provided guidance.

Inadequate Quality Assurance / regressions when updating systems:

When CAs were trying to revise systems to meet the S/MIME Baseline Requirements, or version 2.0 of the TLS BRs, they did not perform adequate quality assurance on the new processes that were introduced, this resulted in certificate mis-issuance of S/MIME and TLS certificates due to regressions and certificate profile errors (e.g. incorrect common names in S/MIME certificates).

Pre-linting failed to stop issuance:

A few CAs experienced problems relying on outdated linters to comply with BR v. 2.0. The comments were that it would be good if linters were more comprehensive before BR effective dates so that CAs had time to integrate them into their processes.

Testing in a production environment:

At least five CAs experienced mis-issuances because they were testing their issuance systems using their production environments. Testing in a production environment is not recommended because it requires extreme care to avoid mis-issuances–in performing your testing you might mis-issue a certificate.

CA Inclusion Requests - https://wiki.mozilla.org/CA/Dashboard

Status	Count
Received - Initial Status	8
Information Verification and CP/CPS Review Needed	13
Ready for Discussion (Cybertrust Japan)	1
In Public Discussion (Firmaprofesional)	1
TOTAL	**23**

Completed inclusion requests: SSL.com's 2022 Roots, Eviden/Atos Root CAs, Sectigo's Roots (R46/E46), Deutsche Telekom Security Roots, TrustAsia Roots, Commscope's Roots, and D-Trust S/MIME Roots

Related NSS/Firefox versions and Bugzilla bugs are listed here: **https://wiki.mozilla.org/NSS:Release_Versions#Root_Cert_Inclusions_into_Mozilla_Product_Releases**

Mozilla Root Store Policy (MRSP) v.3.0 Issues

Period-of-time key lifecycle management reports - GitHub Issue #275
Improve discussion in MRSP of how CA operators can prove cradle-to-grave CA key protection by complying with expectations and requirements for period-of-time audit reporting (just for CA key protection, but does not involve issuance activity). This might include an effort to address "parked" CA keys.

Policy on incident reports consistent with CCADB Policy - GitHub Issues #270 and #271
These issues are relatively minor. The MRSP will be revised either by using nearly identical language from the CCADB Policy or by pointing to the CCADB Policy. See https://www.ccadb.org/cas/incident-report.

Other News

After almost 16 years working on Mozilla's Root Store Program and 8 years working on the CCADB, Kathleen Wilson is retiring as of February 29, 2024. We are greatly indebted and extremely thankful to Kathleen for the work she has done.

Our Email Address: certificates@mozilla.org

Thanks!