Browser News - Mozilla

CA/B Forum Virtual F2F
October 2020

Ben Wilson

A Root Store Policy

We have started the public discussion on mozilla.dev.security.policy regarding proposed changes to Mozilla's Root Store Policy, as indicated in GitHub with the 2.7.1 label.

Cradle-to-grave audits:

- audits from CA key pair generation until no longer trusted by Mozilla's root store (directly or transitively) or until all copies of the CA private key have been completely destroyed, as evidenced by a Qualified Auditor's key destruction report, whichever occurs sooner
- for inclusion, CAs must provide evidence of full compliance with past and present Mozilla and CABF Requirements (contiguous annual audits) and an auditor-witnessed root key generation ceremony report

Audits must include:

- all known incidents that occurred or were still open/unresolved at any time during the audit period
- all CAs "capable of issuing EV certificates", which means:
  - subordinate CA under an EV-enabled root
  - contains no EKU or the id-kp-serverAuth EKU or anyExtendedKeyUsage
  - certificatePolicies extension with CABF EV OID of 2.23.140.1.1, the anyPolicy OID, or the CA's EV policy OID
- all facility site locations that were examined (e.g. Toronto datacenter)
- documentation of individual auditor qualifications sufficient for Mozilla to determine the competence, experience, and independence of the Qualified Auditor

Other requirements:

- perform domain validation at least every 395 days
- section 4.9.12 of a CA's CP/CPS MUST clearly specify the methods that parties may use to demonstrate private key compromise.

B Auditor Qualifications

CA Audits are one of the primary mechanisms relied upon by Mozilla to ensure that a CA is operating securely and in compliance with our policies. Therefore it is important that auditors be qualified to perform the required audits. Currently, in conjunction with verifying audit statements, we are also verifying the qualifications of the auditor, as described here, https://wiki.mozilla.org/CA/Audit_Statements#Auditor_Qualifications, and we will start being more thorough, as indicated by Github Issue #192.

For ETSI auditors, this means that the National Accreditation Body (NAB) must host a website that contains the accreditation documentation for the Conformity Assessment Body (CAB) which is the auditor. And that accreditation documentation must explicitly refer to ETSI EN 319 403, ETSI EN 319 401, ETSI EN 319 411-1, and ETSI EN 319 411-2. For details see https://wiki.mozilla.org/CA/Audit_Statements#Standard_Check

C Inclusion Request Status

There are approximately 42 CAs going through the root inclusion process - https://wiki.mozilla.org/CA/Dashboard and https://wiki.mozilla.org/CA/Application_Process

- Ben is reviewing CAs in the information verification and detailed review phases, and leading the public discussion phase:

  Initial Phase
  - Initial request - 3

  Information Verification Phase
  - Updating information in the CCADB - 2
  - Need audit - 3
  - Fixing test websites - 2
  - Awaiting completion of verification phase - 5

  Detailed Review Phase
  - Awaiting CPS Review - 8
  - Amending CPS - 7
  - Final review before public discussion phase - 2

  Public Discussion Phase
  - Public discussion - 1

  Other
  - On hold - 5
  - Unresponsive - 4

D CRLite

CRLite is enabled in Firefox Nightly and Beta for gathering telemetry, but not yet used to enforce revocation checks. CRLite pushes end-entity revocation information to clients, allowing clients to do revocation checking in a fast and private way. Please refer to the series of Mozilla Security Blog posts, and to Thyla van der Merwe's presentation at the Real World Crypto conference for more information.

E Using Mozilla's Root Store

We have published Mozilla's root store in a way that is easy to consume by downstreams by adding new links in https://wiki.mozilla.org/CA/Included_Certificates, which says:

> *If you are **embedding our root store**, you need to know that we have imposed some restrictions on certain CAs or certificates which are not encoded in certdata.txt. These are documented on a best-efforts basis.*
>
> *CCADB Data Usage Terms*
>
> - *Can I use Mozilla's set of CA certificates?*
>   - *PEM of Root Certificates in Mozilla's Root Store with the Websites (TLS/SSL) Trust Bit Enabled (TXT)*
>   - *PEM of Root Certificates in Mozilla's Root Store with the Websites (TLS/SSL) Trust Bit Enabled (CSV)*
>   - *PEM of Root Certificates in Mozilla's Root Store with the Email (S/MIME) Trust Bit Enabled (TXT)*
>   - *PEM of Root Certificates in Mozilla's Root Store with the Email (S/MIME) Trust Bit Enabled (CSV)*

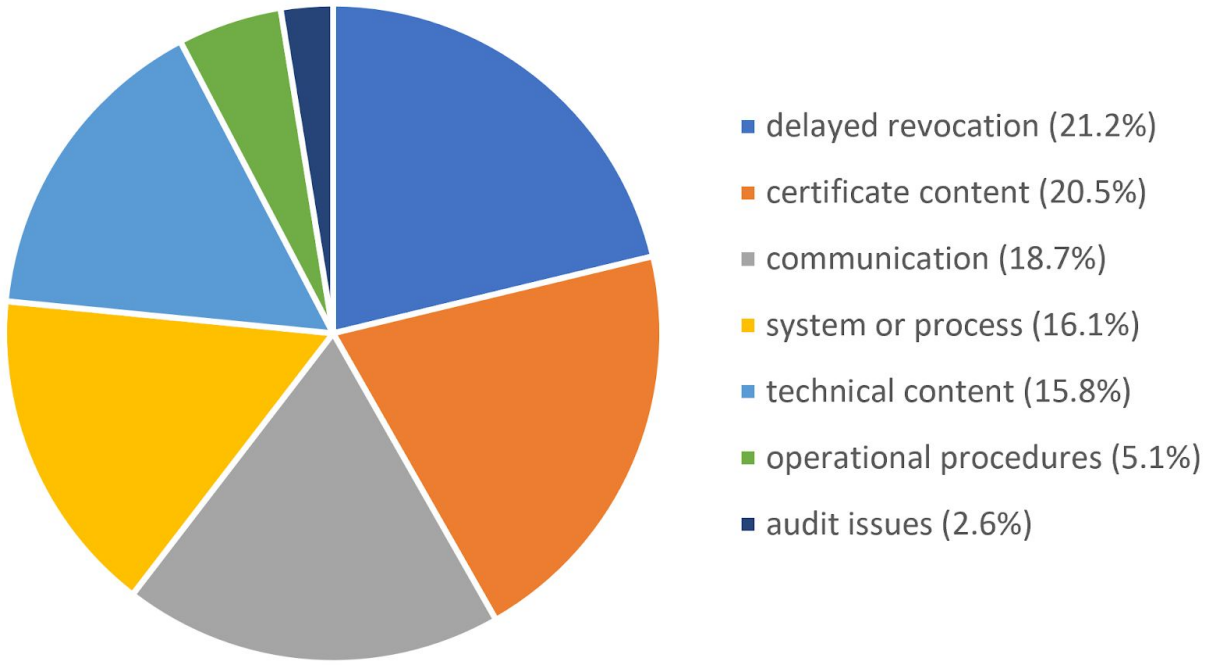
F CA Compliance

Prompt and thorough communication is always important. Mozilla expects CAs to file an initial response/report as soon as possible (https://wiki.mozilla.org/CA/Responding_To_An_Incident), and then follow up with an incident report as soon as the incident has been "diagnosed and (temporary or permanent) measures have been put in place," but "certainly within two weeks of the initial issue report".[1] Thorough communication especially requires detailed responses to items 6 and 7 of the "Incident Report" template - identify and disclose systemic issues and root cause(s) and provide a detailed timeline of remediation tasks.[2]

Communicate status updates frequently. A bug's "whiteboard" entry will indicate whether a "next update" has been set (e.g. [ca-compliance] - Next Update - 1-June 2020), then it is expected that action will be taken by the CA and that an updated status will be reported by then, or sooner. If no "next update" is listed, then the CA is expected to provide a weekly status update.

Review of CA Compliance Bugs in Bugzilla

The pie chart below illustrates the case types from approximately 273 Bugzilla CA incident cases updated since January 1, 2020. They have been categorized at a high level to make it easier to analyze them. “Delayed revocation” represented 21.2% of the CA incidents filed in Bugzilla. The category for “Certificate content” accounted for 20.5% of the incidents, and “Communication” was at 18.7%. “System or process” and technical-related content errors in certificates attributed to about 16% each. Pie charts, further below, help further explore and illustrate the sub-issues (except pie charts were not prepared for Audit issues, Delayed revocation, and Operational procedures).

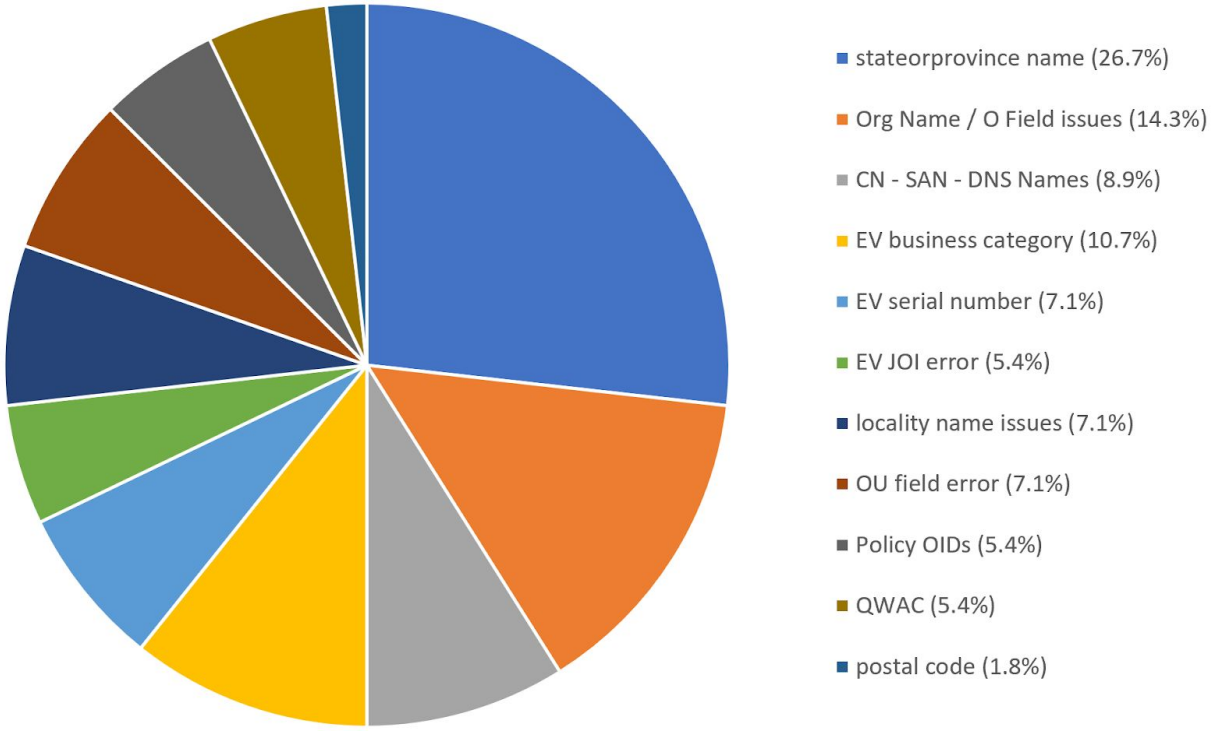


Pie Chart: Categorization of Incident Reports

Delayed revocation: failure to revoke certificates within timeframes set by BR § 4.9.1.
Certificate content: incorrect information placed in the subject DN, SAN, EV fields, etc.
Communication (audit scope and disclosure): delayed or inadequate reporting or communication, miscommunication by CAs with auditors regarding scope of intermediate CAs to be included in audits, and poor communication practices with relying parties
System or process: failure of a system or process to accomplish its intended purpose, i.e., validation, issuance, OCSP response, revocation, logging, patching,
Technical content: non-compliance with a certificate-related technical specification, i.e., invalid or mismatched encodings, algorithms, key usages, EKUs, etc.
Operational procedures: audit findings mentioning inadequate operational controls
Audit issues: Delayed audits, potential delays, and audit gaps. This category does not include: missing intermediates CAs in audit reports, which were categorized under “Communication”, or audit findings, which were categorized under “Operational procedures” or “System process”.

1. Certificate-content Category

The certificate-content category of 56 incidents (20.5% of 273 incidents) can be further divided mainly into issues related to the failure to validate the location information or putting the wrong information into OV and EV certificates, although 8.9% were related to errors with domain names placed in CNs and SANs. As illustrated, 26.7% in this category were related to having the wrong state or province name in the certificate. Next was Organization names or O field errors with 14.3%. Incorrect locality names attributed to 7%.



Pie Chart: Certificate-Content

EV-specific errors: wrong business category (10.7%), improper EV serial number (7.1%), and wrong description for the jurisdiction of incorporation (5.4%) total to 23.2.

CN - SAN - DNS Names: improper information or mis-formatted entries in the CN or SAN

OU Name: Four incidents indicated that an improper OU entry was in the OU field.

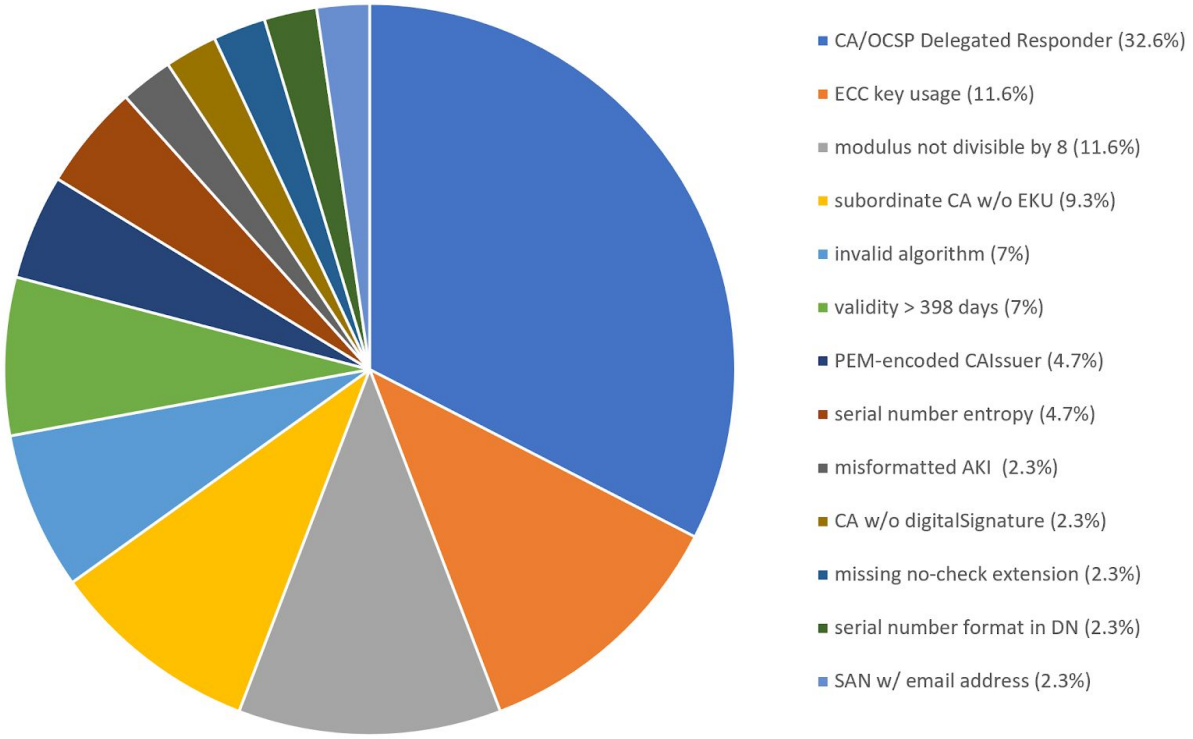
Policy OIDs: Three incidents involved having the wrong policy OIDs in certificates.

QWAC: Three incidents referenced that a QWAC certificate had wrong information.

Postal code: At least one incident of an incorrect postal code was reported.

2. Technical-related certificate content issues

A large portion (32.6%) of the 43 technical formatting errors is attributed to the CA-with-OCSP-responder-EKU issue that affected fourteen CAs at the beginning of July. Other notable incident reports included having the keyEncipherment key usage in ECC certificates (5 incidents) and having an RSA modulus size not divisible by 8 (5 incidents).



Pie Chart: Technical-related content issues

subordinate CA w/o EKU: subordinate CAs must have an EKU, MRSP, §5.3

invalid algorithm: e.g. SHA-256 hash with ECC P-384 signing key, RSASSA-PSS,

validity > 398 days: effective 9-1-2020, end entity certificates must not have validity > 398 days

PEM-encoded CAIssuer: supposed to be DER-encoded as required by RFC 5280, §4.2.2.1

serial number entropy: certificates must have a serial number of more than 64 bits of entropy

misformatted AKI: AKI must not include keyID and the issuer's name and serial number

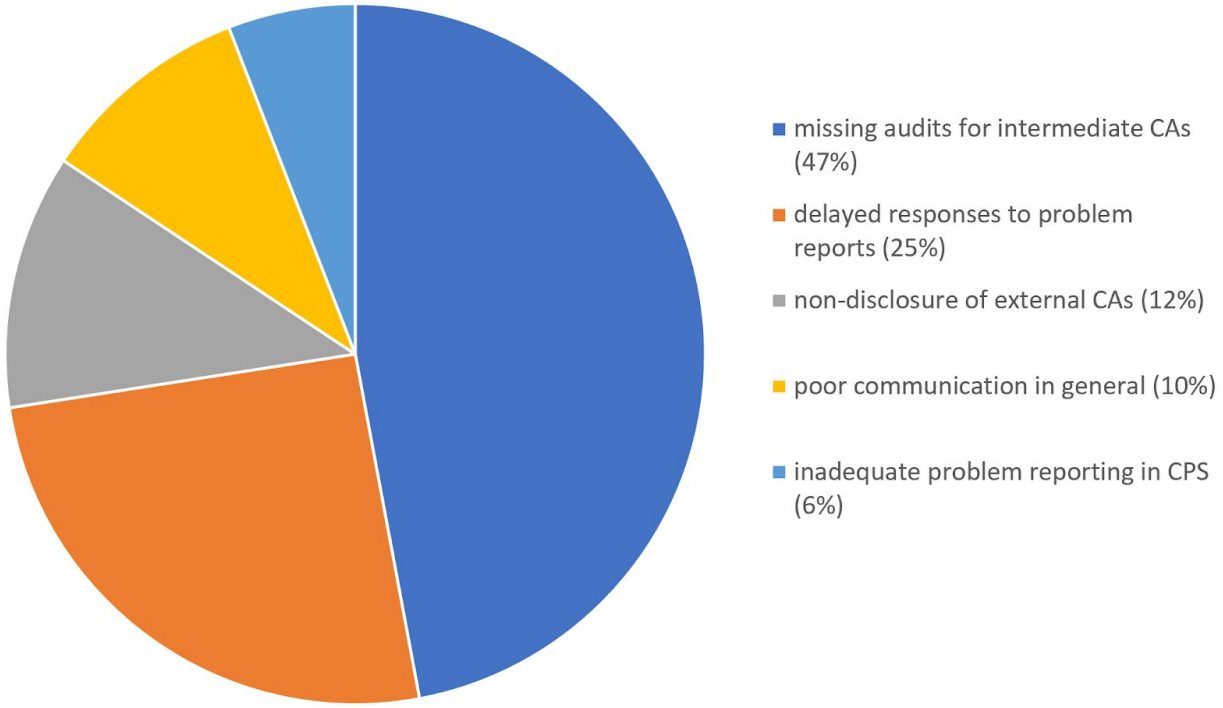
CA w/o digitalSignature key usage bit needed for CA to sign OCSP responses

missing no-check extension: OCSP responder certificate required to have by BR §4.9.9

3. Communication-Related Category

In the communication-related category, about 47% of these were due to not including intermediate CAs in audits (also ALV - audit letter validation errors). Twenty-five percent (25%) of this category was attributable to delays and other problems in responding to certificate problem reports and revocation requests.

If you combine the 47% for missing intermediate CAs in audit letters with the 12% of problems related to the improper disclosure of externally operated CAs, then 59% of these incidents are related to the inaccurate CA reporting of subordinate CAs.



Pie Chart: Communication-related problems

Missing audits for intermediate CAs: mainly missing intermediate CAs (e.g. SHA2 certificate hashes) in audit letters and ALV failure

Delayed responses to problem reports: not providing preliminary report within 24 hours

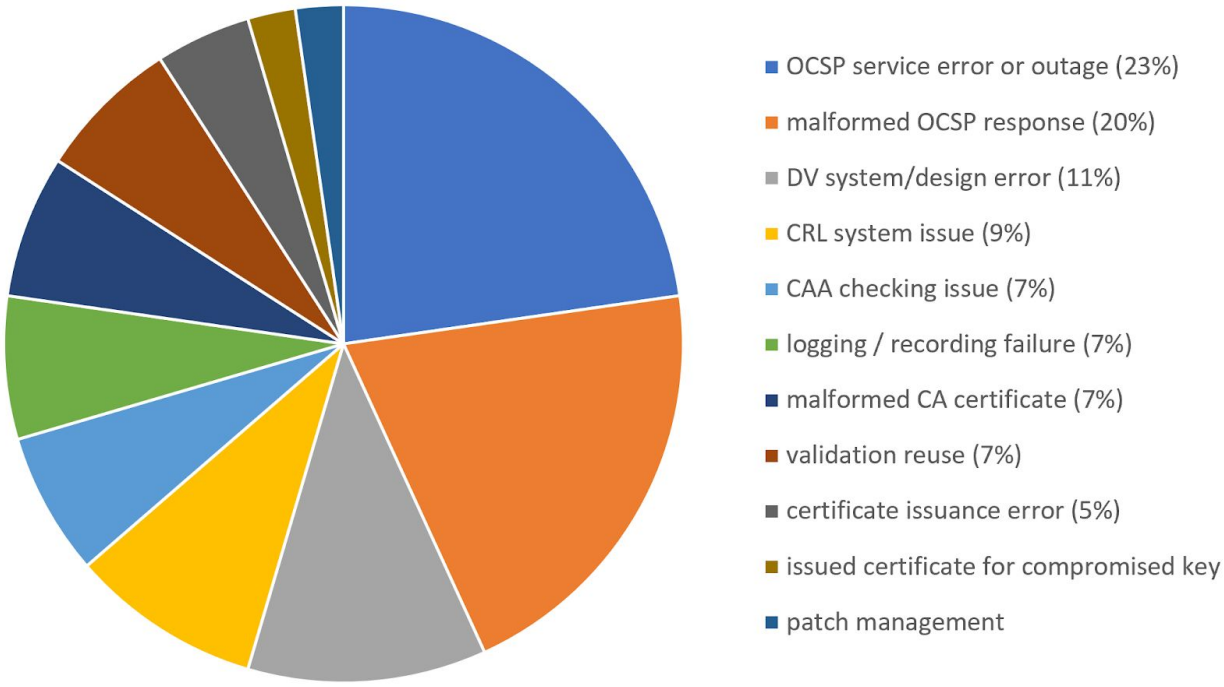
Non-disclosure of external CAs: inadequate or inconsistent disclosure of externally-operated intermediate CAs

Poor communication in general: confusion about applicable requirements, repeated delays in providing status updates, timely completing incident reports, etc.

Inadequate problem reporting in CPS: CPS lacks adequate problem reporting instructions

4. System or Process Issues

I categorized 44 incidents as related to a failed system or process. About 43% of these were attributable to OCSP problems (23% OCSP service error or outage and 20% malformed OCSP responses). Bad system design or operation of domain validation systems attributed to 11% of incidents in this category. Nine percent suffered problems with CRLs. CA checking, logging/recording, CA certificate creation, and validation reuse issues each attributed to 7% of the problems.



Pie Chart: System/Process Issues

OCSP service error or outage: Incorrect OCSP responses or OCSP unavailable

Malformed OCSP response: Variety of content and status errors, incorrect encoding, etc.

DV system/design error: Certificate mis-issuance due to failure to perform domain validation

CRL system issue: Variety of errors, expired CRLs, unrevocation, RFC 5280 non-compliance

CAA checking issue: lack of evidence of CAA checking and CAA-checking bugs

Logging/recording failure: failed logging, lack of evidence, failed videorecording

Malformed CA certificate: lack of procedures to ensure compliance with CA format/content

Validation reuse: failed system/process to control improper validation reuse

Certificate issuance error: duplicate serial number, Debian weak key