Mozilla News

CA/B Forum F2F, Meeting 63 in Seattle, WA
October 8, 2024

Ben Wilson

Link to Previous Mozilla May 2024 Face-to-Face briefing - https://cabforum.org/2024/05/28/minutes-of-the-f2f-62-meeting-in-bergamo-italy-may-28-29-2024/3-May-2024-Mozilla-News.pdf

CA Compliance - https://wiki.mozilla.org/CA/Incident_Dashboard
Current open bugs can be found in the Incident Dashboard (currently 72 are open - as of October 1, 2024). They are categorized as follows:

Type of Incident	Count
Audit Delays and Findings	**5**
CA Misissuance	**2**
CRL Failures	**8**
DV Misissuance	**4**
OV Misissuance	**9**
EV Misissuance	**3**
Leaf Revocation Delays	**22**
OCSP Failures	**3**
Policy Failures	**9**
S/MIME Misissuance	**9**
Uncategorized	**3**

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

Status	Count
Received - Initial Status	11
Information Verification	12
In Public Discussion (D-Trust closes 2024-10-24)	1
TOTAL	**24**

Revisions to Mozilla Root Store Policy

https://github.com/mozilla/pkipolicy/labels/3.0

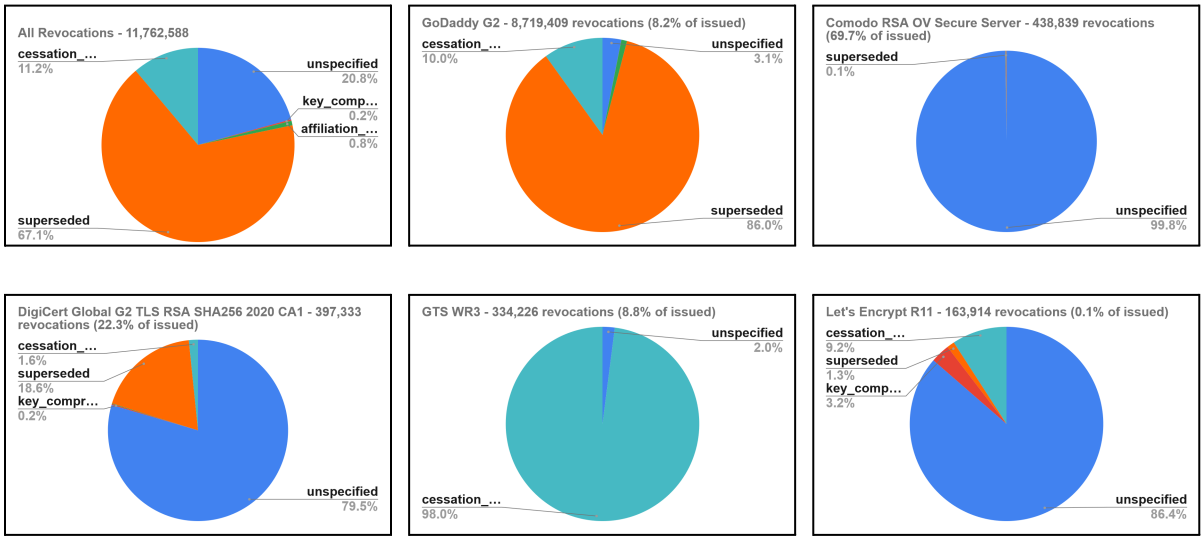
Issue #	Description
263	MRSP § 3.3 - CPs/CPSes must follow the common outline of section 6 of RFC 3647 and "contain no sections that are entirely blank, having no text or subsections"
270 and 271	MRSP § 2.4 -Initial incident reports should be filed as soon as possible but no later than 72 hours after discovery and full incident reports must be posted within two weeks of the incident
275	MRSP §§ 3 and 7.1 - Put greater emphasis on period-of-time audits
276	MRSP § 6 - Address delayed revocation
278	MRSP § 2 or 2.3 - Reference certificate linting requirements (a la TLS BRs and https://github.com/cabforum/smime/issues/212)
279	MRSP §§ 1.1 and/or 7.1 - Phase out dual-purpose (TLS / S/MIME) root CAs
281	MRSP § 5.1 - Add P-521 as supported
283	MRSP § 7.1 - Require new inclusion applications to support automation

CRLite

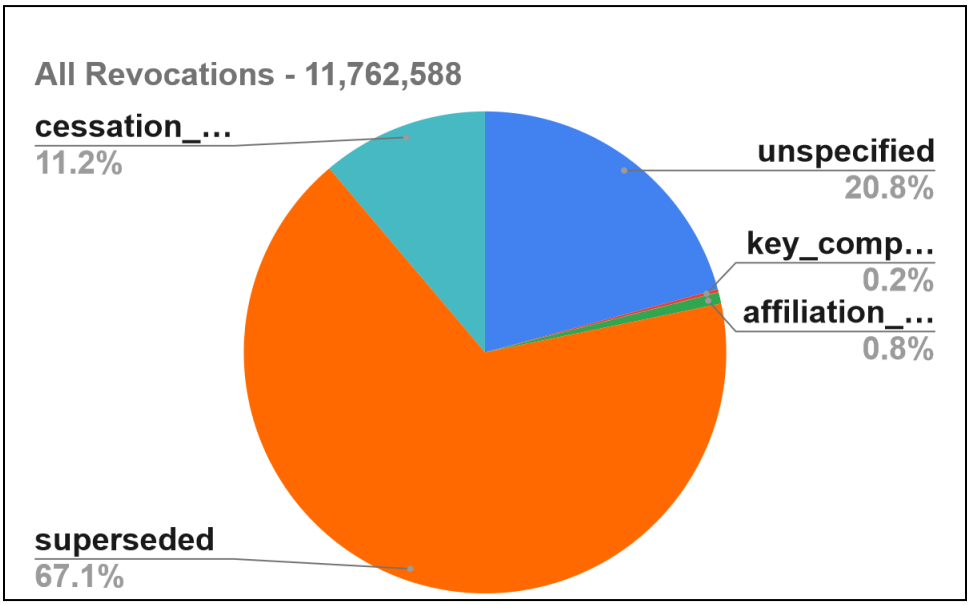
Currently, we are examining three types of revocations. One with all reason codes. One with everything but "unspecified" reason codes. And third, mainly those revocations with "priority" reason codes of keyCompromise, cessationOfOperation, and privilegeWithdrawn. We need to be able to focus revocation reasons on those that are security-sensitive, rather than those that are just ordinary or administrative.

Revocation Reason Codes

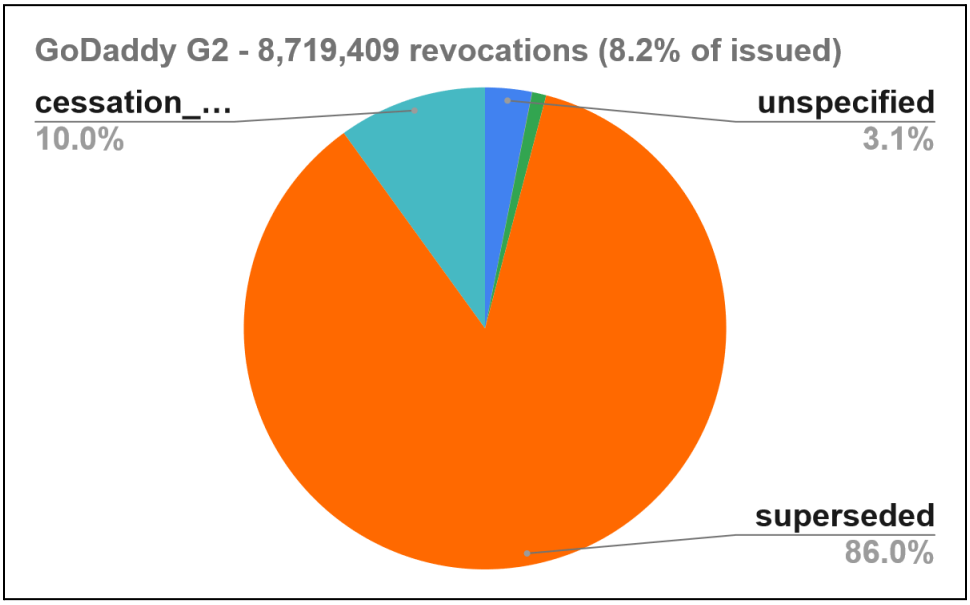
There is quite a range of approaches to revocation reason codes among CAs with the largest numbers of revocations, as illustrated below.



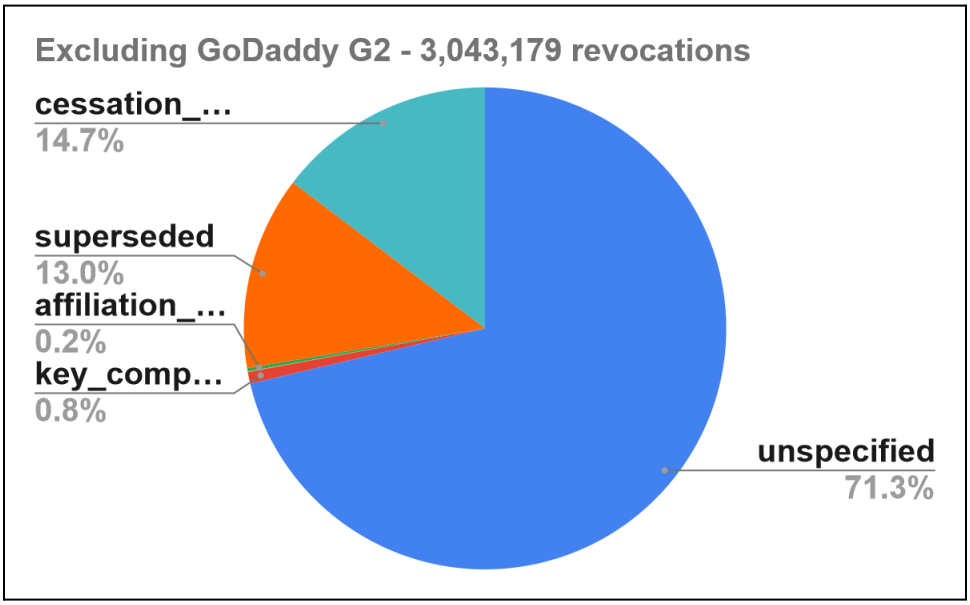
Data sets have been collected on August 29 and October 2, 2024. There were 783 issuing CAs in the data set with 11,762,588 revocations of 816,349,158 certificates in the August data set. The October data set contained 864,889,438 issued certificates of which 10,682,882 certificates had been revoked. The following pie charts are based on the August 2024 data set.
Sixty-seven percent (67%) of the revocations had the reason code of “superseded”. About twenty-one percent (21%) were unspecified, and eleven percent (11%) were for cessation_of_operations. The pie chart below does not show 1,084 (.01%) revocations that were for privilege_withdrawn. This pie chart shows an overall distribution that is really a conglomerate of revocations by various different CAs.



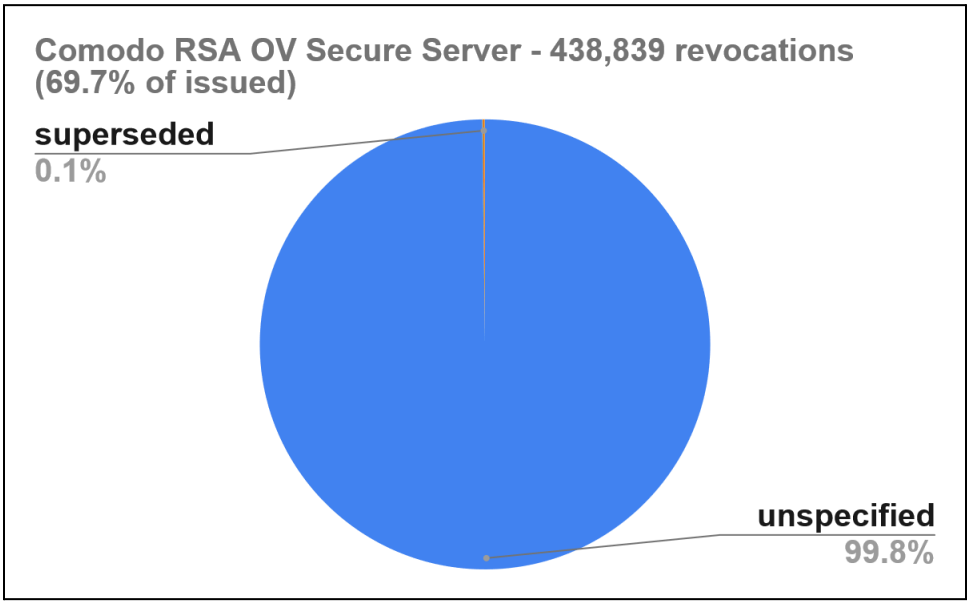
The **Go Daddy Secure Certificate Authority - G2** (GoDaddy G2) had 8,719,409 revocations, or 74% of all revocations in the data set. Eighty-six percent of the revoked certificates were for reason code “superseded”. (The pie chart below does not show 977 (.01%) revocations that were for key_compromise or the 140 revocations that were for privilege_withdrawn.)



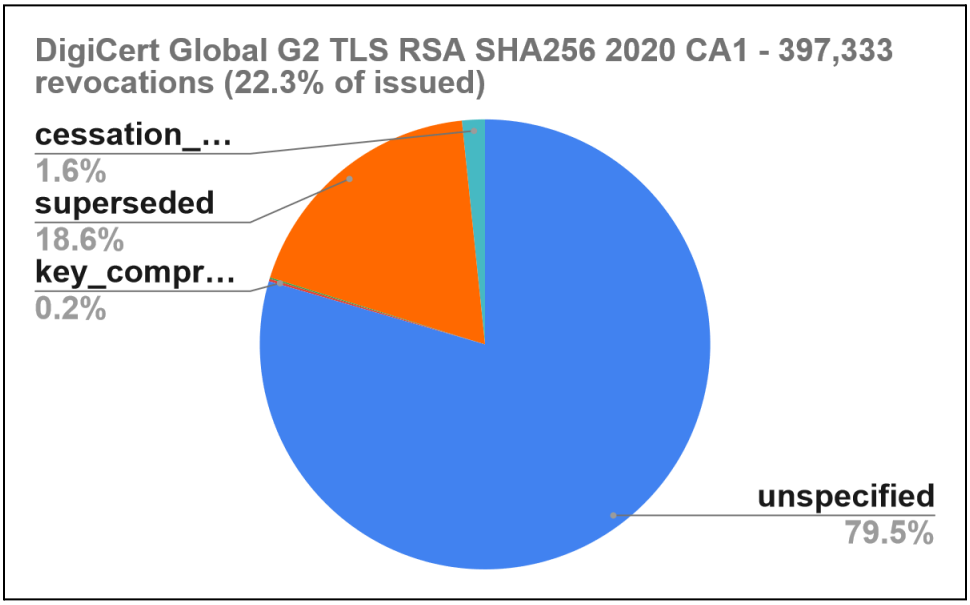
If we remove the GoDaddy G2 revocations from our analysis, then 71.3% of the revocation reasons are “unspecified”. (The pie chart below does not show 944 revocations (.03%) for privilege_withdrawn.)



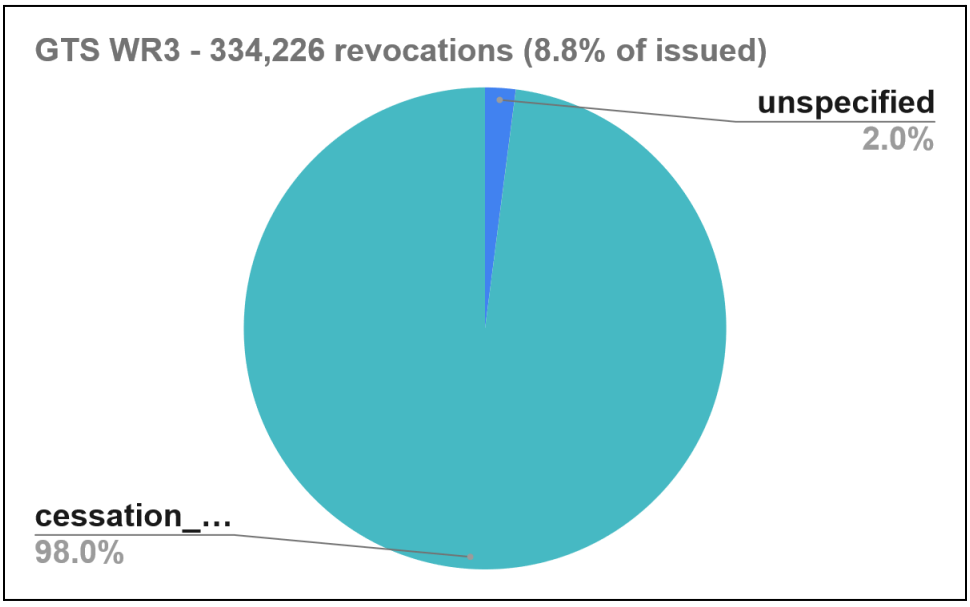
The **COMODO RSA Organization Validation Secure Server CA** represented 3.7% of the revocation data set. Nearly all (99.8%) of the revoked certificates had an “unspecified” reason code. (The pie chart below does not show 55 revocations for key-compromise, 0 for privilege_withdrawn, 156 for affiliation_changed, and 147 for cessation_of_operation.)



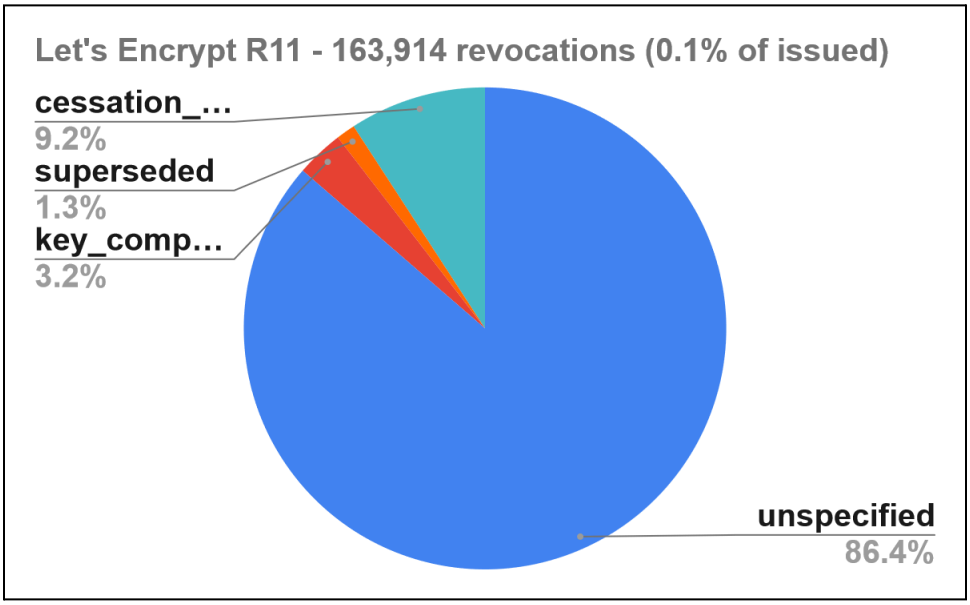
The **DigiCert Global G2 TLS RSA SHA256 2020 CA1** represented 3.4% of the revocation data set and had 79.5% of its revoked certificates with an unspecified reason code. The next largest category of revocation reason codes was “superseded” with 18.6%. (Not shown in the pie chart below are privilege_withdrawn (1) and affiliation_changed (407).)



The **Google Trust Services (GTS) WR3 CA** represented 2.8% of the revocation data set. Ninety-eight percent of the revocations by this CA were for cessation_of_operations, and two percent of the revocation reasons were unspecified. (Not illustrated in the pie chart below are the following: 7 with key_compromise, 0 with privilege_withdrawn, 0 with affiliation_changed, and 10 with superseded reason codes.)



Let's Encrypt R11 represented 1.4% of the revocation data set. (The other top 4 Let's Encrypt CAs–R3, E5, E6, and R10) had very similar reason-code distributions.) There were no revocations for privilege_withdrawn or affiliation_changed.



Conclusion: More guidance and harmonization in designating revocation reason codes are needed. We should identify action items to improve the use of revocation reason codes. We should consider modifying the TLS Baseline Requirements.

Mozilla CA Certificate Program: **https://wiki.mozilla.org/CA**

Our Email Address: **certificates@mozilla.org**

Thanks!

Ben