



## Certificate Revocation With CRLSet

---



Copyright © www.ine.com

# Keith Bogart

CCIE #4923



- ✉ [kbogart@ine.com](mailto:kbogart@ine.com)
- 🐦 [@keithbogart1](https://twitter.com/keithbogart1)
- 🌐 [linkedin.com/in/keith-bogart-2a75042](https://www.linkedin.com/in/keith-bogart-2a75042)

CCIE Routing & Switching



Copyright © [www.ine.com](http://www.ine.com)



# Topic Overview

---

- ▷ CRLSet Functionality
- ▷ CRLSet Example
- ▷ CRLSet Challenges

## CRLSet

- ▶ Google Chrome does not utilize CRLs or OCSP, it utilizes CRLSets.
- ▶ Google Chrome's method of checking for revoked Certificates.
- ▶ CRLSet is;
  - ▶ A carefully selected collection of revoked-certificate serial numbers published by many different certificate authorities.
  - ▶ Google's own, compiled/curated CRL which is automatically downloaded into Chrome browser.
  - ▶ Lists are auto-updated by regularly crawling the CRLs from the major CAs around the world.

Copyright © www.ine.com



The "Chromium Project" states that CRLSets, "are fetched infrequently (at most once every few hours)"

# CRLSet Example

```
{
  "Version": 0,
  "ContentType": "CRLSet",
  "Sequence": 1596,
  "DeltaFrom": 0,
  "NumParents": 53,
  "BlockedSPKIs": [
    [
      "GvVsmP8EPvkr6/9UzrtN1no1upVsgX8+bdPB5561hME=",
      "PtvZrOY5uhotStBHGHEf2IPoWbL79dE31CQEXnkZ37k=",
      "Jdoa1Yu/z7In2HI76FFUwY57qnQXtPnv+TzrXoafizk=",
      "1i5LVLuYp+5dX+uWM/mR08MwDpUU2t57DU+CjH1Pjoc=",
      "yP3cdcsb27WMB7TqhHKH9iZlndZrwQomrdm1db0go40="
    ]
  ],
  "NotAfter": 1398627981
}
019406d575cf285a3c2d8bbf8133e0cfae4839c99cc1815bdf244487259e7cd2
11270b1308d38971db8f728e2956c8d38c7
11270b612d8bed52a12dfa3ab5c9317c486a
11270e0d85729204151e40e55374d140b395
11272184dfda95993c83e575142b0d209185
112723158fe05c8de8c2bb7357a23c13b9d0
11272874436692a4fbd793d737c7ba4fd494
11272f54911df5a61d9ba8d0e9837093a23a
1127367d2d5a6e0b40c12686185e6bee8bc2
11274f9fca0f134199d919bcd5c834ef4c99
```

Copyright © www.ine.com



The first part is a short JSON-format file header identifying the file version, content type, the CRLSet's sequence number, the count of certificate authority CRL sets appearing after the header, a short list of explicitly blocked certificates, and an expiration date for the data.

What differentiates the "explicitly blocked" serial numbers from the larger list? From the Chromium Project, "...CRLSet can quickly block certificates in emergency situations. As a secondary function they can also contain some number of non-emergency revocations." So apparently the smaller list of explicitly blocked certs were done so due to some "emergency situation" (which is left to your imagination. Chromium developers won't say what their criteria is.)

As of 2014 Microsoft had a total of 353 Trusted Root Certificates (CA's). Compare that to the 53 in the list above.

## CRLSet Challenges

- ▷ CRLSet is only composed of a subset of the hundreds of Certificate Authorities that exist globally.
- ▷ CRLSet is space-constrained to about 24k Revoked Certificates (there are millions of revoked Certificates worldwide)
- ▷ Chrome implicitly trusts Certificates that are not within their CRLSet
- ▷ More information can be found at:

<https://www.grc.com/revocation/crlsets.htm>

Copyright © www.ine.com



To keep the CRLSet manageable, its size is strictly limited to 256k bytes. Consequently, an oft repeated admission by Google's engineers and spokespeople is that their CRLSet “does not contain all revoked certificates”.

-

Chrome will blindly trust every revoked certificate that was originally signed by more than four fifths of the certificate authorities Microsoft trusts.



Thanks for watching!