Den Danske Stat Tillidstjenester

The Danish State Trust Services

Checking for revoked certificates OCSP or CRL

Version 1.0

January 2023

AGENCY FOR DIGITAL GOVERNMENT
MINISTRY OF FINANCE

Content

1 Introduction

X.509 certificates can be revoked after they have been issued prior and to expiry. There can be many reasons for the revocation of a certificate, but common revocation reasons can be subject name change, loss of access to corresponding private or cessation of operation. Before a relying party should trust a certificate, it is therefore necessary to validate the certificate's revocation status at time of the use of the corresponding private key.

This document compares two different standard mechanisms for verifying the revocation status of a certificate namely Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL).

The document lists cons and pros of the mechanisms in different use cases.

2 Intended audience

The intended readers are security architects which have the responsibility of choosing which of the two mechanisms to use in a specific application or solution. It is assumed that the reader is familiar with the general concepts of public key infrastructure.

3 Certificate Revocation List (CRL)

Certificate Revocation List (CRL) has always been an integrated part if the X.509 standard. CRLs are lists of serial numbers of revoked certificates accompanied with the revocation time and optionally a revocation reason. The revocation reason may be set to "unspecified" e.g. due to privacy reasons. CRLs are always digitally signed to ensure integrity if the CRLs and usually it is the issuing CA which signs the CRLs.

CRLs includes an issue time and a next update time. Note that there is no expiry time on a CRL since a CRL may be replaced any time after issuance e.g. if a certificate is revoked in the meantime. As long as nobody can see into the future, nobody can predict if a new updated CRL will be issued. The next update time in the CRL indicates to a relying party that an updated CRL can be expected to be issued before the next update time. The next update time is not dictating a security policy for the relying party. A relying party using CRLs should assess how often there shall be checked for an updated CRL.

CRLs are typically distributed via HTTP or HTTPS and sometimes via LDAP. Note that since the integrity is secured directly in the CRL via the digital signature and since CRLs are typically not considered confidential, there is no specific security requirements to the distribution protocol with regards to integrity and confidentiality.

CRL includes at least serial numbers all revoked certificates which is not expired. In some cases, CRLs may even include serial numbers of expired certificates due requirements in certificate policies. This implies that CRL may become very large over time. CAs will typically have measures to ensure that CRLs do not become impractically large e.g. by creating multiple issuing Cas in a hierarchy under a common root CA.

Location of a CRL for a specific certificate can normally be found as a reference in the certificate's cRLDistributionPoints extension.

CRL technology is typically a good solution in a server environment:

- Performance. Downloading CRL and processing of CRL can be done independent of the use of data from the CRLs.

- Availability. If for some reasons the server cannot retrieve CRLs the system can flag a warning and the service can continue without affecting the users while the issue is being solved.
- Privacy. The CA's log will not include any information on which certificates (if any) are being validated in a certain server application.

You can create a scheduled cron job which downloads and verifies the CRL and then insert the serial numbers of revoked certificate in a data structure which if fast and easy to access for your application(s). The cron job can also flag problem of accessing the CRL from the CA while the application using the data will still work.

4 Online Certificate Status Protocol (OCSP)

OCSP was first standardized in RFC2560 in 1999 and updates have been added over time.

OCSP conceptionally consists of a OCSP responder (server) and a OCSP client. The client requests the status of one or more specific certificates and get a signed response from the OCSP responder. Typically, clients only request the status of exactly one certificate and many OCSP responders have a policy of only accepting one serial number per request.

OCSP responses tells if a certificates status is good, revoked, or unknown. Note that the status "good" only indicates that the certificate was not revoked. E.g., there might not even exist a certificate with the given serial number, or the certificate might have expired. The "unknown" status indicates that the OCSP responder does not have information of the status of the certificate in question. E.g. if the issuer is unrecognized by the OCSP responder.

The client can either be a relying party or the certificate subject herself. The latter can be useful as a proof to relying parties that the certificate is not revoked such that the relying party does not need to make a OCSP request or check a CRL. This is sometimes denoted OCSP stapling. OCSP stapling are typically used by servers in the TLS protocol and to create self-contained electronically signed documents as seen in the AdES standards for the so-called LTV- and LTA-formats.

The relevant OCSP responder for a specific certificate can normally be found as a reference in the certificate's authorityInformationAccess extension.

OCSP is typically a good solution for in less performance critical application with fewer requests and in solutions where OCSP stapling can be utilized. If OCSP is used in server solutions with a synchronous communication with the users, it is important to take into consideration:

- Responsiveness. Is the extra time for retrieving and parsing the OCSP response during an interaction with the end user acceptable?
- Availability. Is there a fallback solution if the OCSP responder cannot be reached? And if the fallback solution is using CRL, could the CRL replace the use of OCSP to make the solution simpler and more robust?
- Privacy. Can it be justified in the DPIA that data of which certificates are used in the solution is logged at the OCSP responder or is it mitigated e.g. by using OCSP stapling?

5 Using CRL or OCSP

There is a general misconception that OCSP is more secure than using CRL. This might not at all be the case and with regards to availability in a server environment this may even be the opposite case. If a CRL cannot be reached this can be detected and prior to CRL next update time (or whenever the applications security policy requires updated information) alerts can be set. If the solution is based on OCSP, the application will typically stop working as soon as the OCSP responder cannot be reached unless some fallback is implemented.

For server applications it is in general recommended to consider using the CRL over OCSP for performance and availability reasons.

In general OCSP responses are considerably smaller that CRLs. Applications using some kind of stapling or embedding certificate status data in signed data e.g. PAdES LTA-format should consider using OCSP over CRL to reduce the size of status data.