



ONLINE CERTIFICATE STATUS PROTOCOL

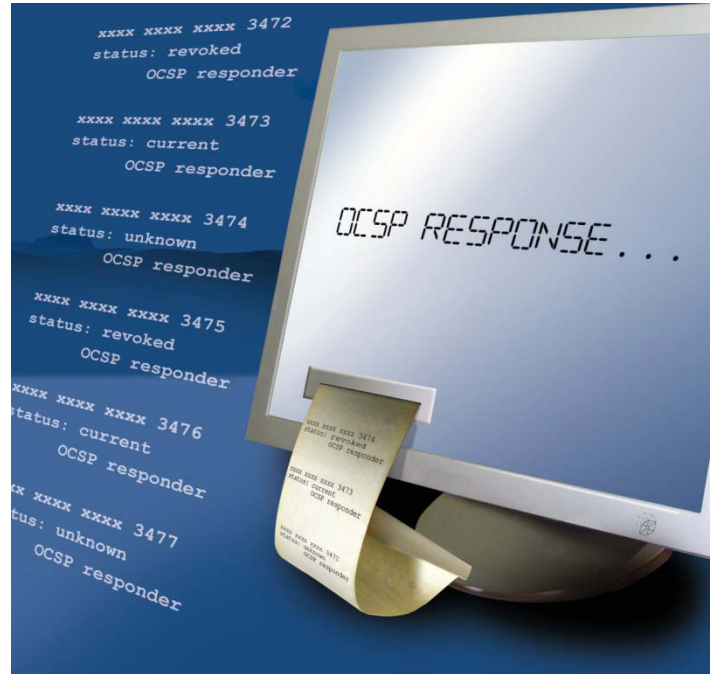
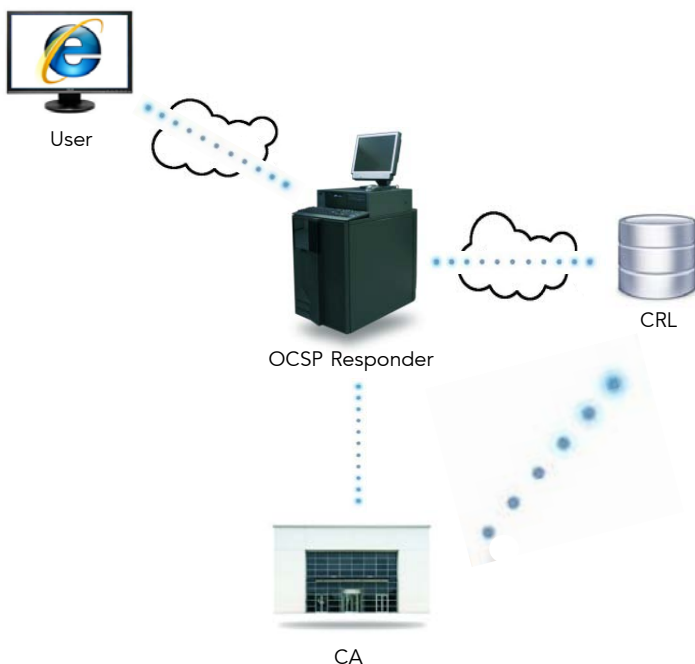
Digital certificates play a central role in the security of many applications and systems, ranging from enterprise PKIs to digital rights management and electronic passports. Accordingly, the ability to revoke certificates on demand is also crucial to these applications.

The Online Certificate Status Protocol (OCSP) is one of two internet protocols for distributing certificate authentication information. The older method, which OCSP has superseded in many instances, is a Certificate Revocation List (CRL). With this earlier method a (potentially large) CRL was periodically posted to the network and had to be frequently downloaded to keep the list up-to-date at the client end – a major limitation.

OCSP was developed to overcome this limitation by providing a more efficient way of distributing the authentication information of a certificate.

When a user first opens an application such as a web browser the OCSP sends a request for information regarding the status of the certificate. The server, which contains the certificate status information, sends back a response of either 'current', 'expired', or 'unknown'. As an OCSP response contains less information than the traditional CRL, OCSP can provide real-time information regarding the revocation status of a certificate.

The Cryptomathic OSCP Responder delivers OCSP services to the most demanding applications. It combines strong security with high performance and availability, whilst integrating seamlessly with new or existing PKI deployments.



Cryptomathic OSCP Responder

The Cryptomathic OSCP Responder provides real-time certificate status information, via the OCSP protocol, by checking the CRLs of specified Certificate Authorities via HTTP or LDAP.

Operational and administration tasks are carried out via the OCSP Responder Administration Client (manual import of CRLs via administration client is also supported). This provides a secure and graphical user interface for system configuration, key management, and CA integration. Remote administration reduces the need for server access.

Strong administrator authentication is provided by means of chip-card based access control. In addition, administrator functions are divided into separate rolls with critical commands under dual control. These controls are coupled with an audit log of all system operations. Hardware Security Modules (HSMs) are used to protect the confidentiality of all system keys and to protect all sensitive application data stored in the system database.

Following Cryptomathic's proven architecture, the OSCP Responder can employ multiple HSMs and several servers operated as a load-balanced cluster for high availability and improved throughput. Back-up and disaster-recovery scenarios are supported through standard HSM and database tools.

TECHNICAL SPECIFICATIONS

Key Management

- RSA 1024-4096 bit keys (limit set by HSM)
- Hardware protection of all OCSP signing keys

Certificates

- Certification of OCSP signing keys using PKCS#10 certificate request and X.509 certificate import

Interfaces

- RFC 2560 (OCSP) interface
- X.509 CRL retrieval via HTTP or LDAP

Administrator Controls

- Secure remote administration client
- Chip-card administrator authentication
- Dual access control for critical operations

Operational Features

- Scale-out clustering for high availability and performance
- Support for multiple HSMs
- Simple backup and disaster recovery

Operating Environment

- Microsoft Windows

Hardware Security Modules

- Thales / nCipher

Supported Databases

- Microsoft SQL

BENEFITS

The Cryptomathic OCSP Responder offers the following benefits:

Real-time status information – avoids risks associated with CRL update delays.

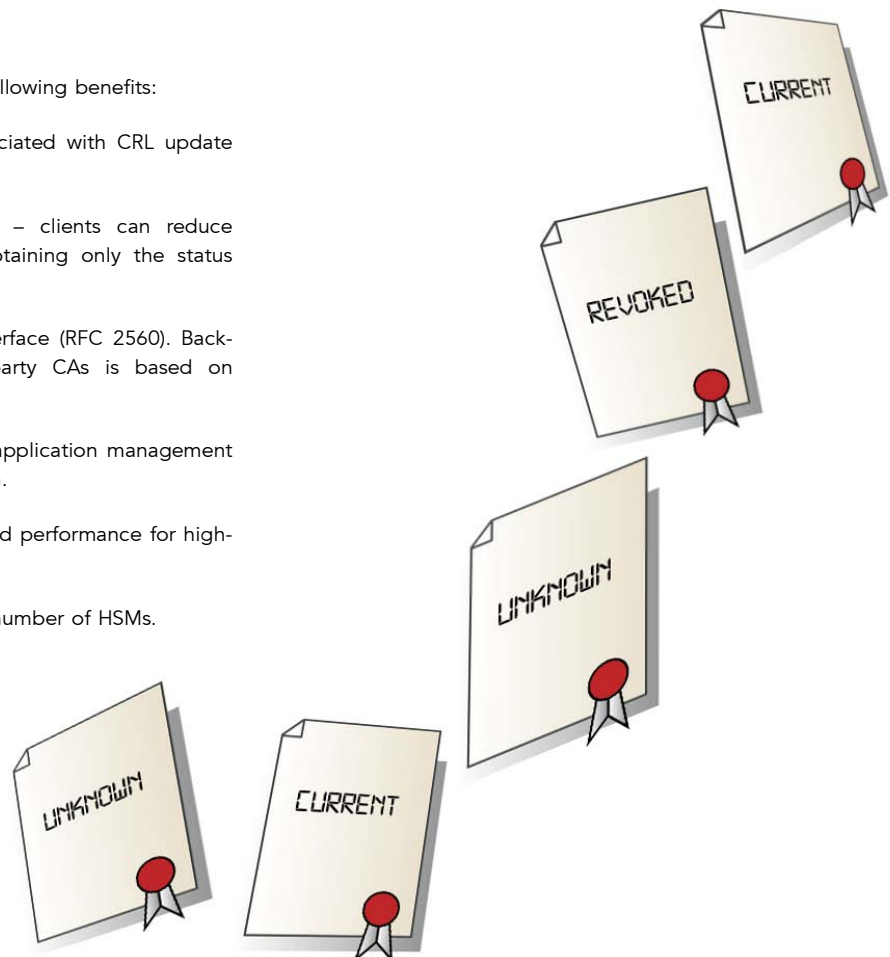
Retrieves status of requested certificates only – clients can reduce network traffic, storage and processing by obtaining only the status information they need.

Simple integration – standards-based query interface (RFC 2560). Back-end integration with Cryptomathic or third-party CAs is based on standard CRLs.

Remote administration client – allows everyday application management to be conducted outside the secure server room.

Scale-out clustering – assures high availability and performance for high-volume, mission-critical applications.

Hardware Security Modules (HSMs) – supports a number of HSMs.



ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With over 20 years' experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing

and advanced key management utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at cryptomathic.com