

Cryptomathic OCSP Responder 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.

Traditionally, revocation has been implemented by publishing Certificate Revocation Lists (CRLs). Practical and security issues can arise due to size of the CRLs and the delay in updating relying parties. To address this, the Online Certificate Status Protocol (OCSP) was developed to provide real-time certificate status information, for the required certificates only.

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

Benefits

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

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

Simple integration – standards-based query interface available directly or via HTTP. 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 FIPS-certified HSMs.

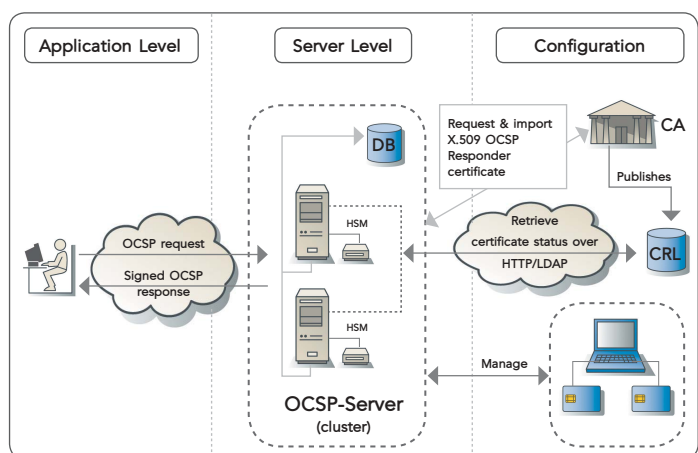


System Architecture

In order to answer certificate status requests, the Cryptomathic OCSP Responder retrieves up-to-date CRLs from any existing CA via HTTP or LDAP.

Operational and administration tasks are carried out via the OCSP Responder Administration Client. This provides a graphical user interface for system configuration, key management, CA integration and audit tasks. Secure 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 roles, with critical commands under dual controls. These controls are coupled with a tamper-evident audit log of all system operations. ►



Architectural overview



Technical Specifications

Key Management

- 1024-4096 bit RSA 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

- RFC2560 (OCSP) interface
- Optional HTTP proxy
- X.509 CRL retrieval via HTTP or LDAP

Administrator Controls

- Secure remote administration client
- Chip-card administrator authentication
- Role-based separation of duties
- Dual access control for critical operations
- Tamper-evident audit log

Operational Features

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

Operating Environment

- Microsoft Windows Server 2003 Service (Server)
- Windows 2000/XP with .NET framework (Administration Client)

Hardware Security Modules

- nCipher nShield and nethsm
- IBM 4758 and 4764
- SafeNet (Eracom) ProtectServer Orange/Gold
- Other PKCS#11 compliant hardware

Supported Databases

- Microsoft SQL Server 2000/2005
- Oracle 8, 9i or 10g

- ▶ FIPS-certified 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 OCSP 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.

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 20 years' experience, we have assisted our customers by providing systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing, and advanced key management through best-of-breed security software and services.

Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with its established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

www.cryptomathic.com

