

TC OCSP Responder

For Real-Time Certificate Validation

TC OCSP Responder – For Fast Certificate Validity Checks

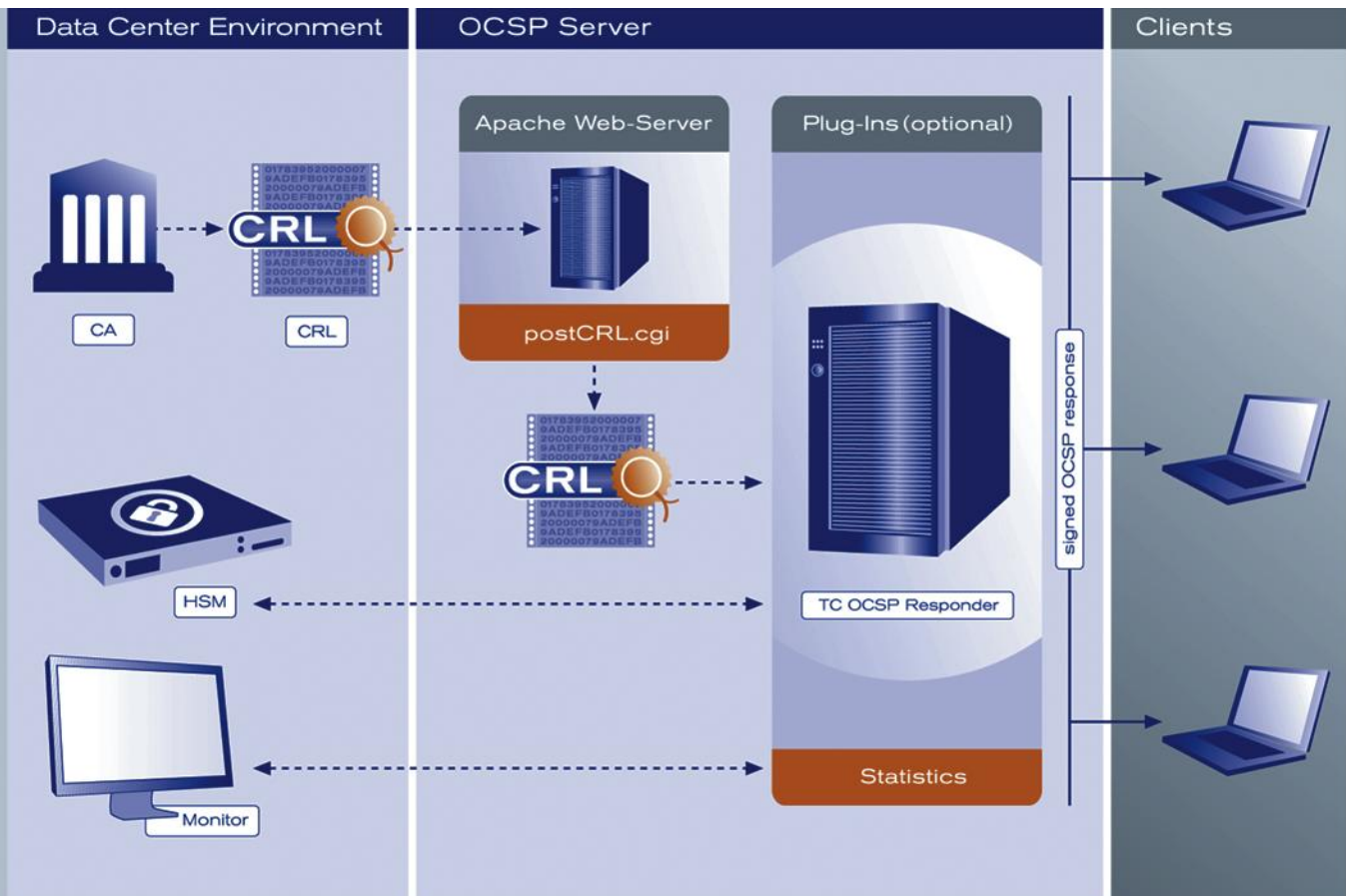
Every Public Key Infrastructure (PKI) is only as good as the certificates behind it. Only a valid certificate is a secure certificate. Thus, validation becomes the critical factor of success within a PKI. With the Online Certificate Status Protocol (OCSP), the validity of a certificate can be checked easily and automatically in real-time. The OCSP Responder enables the easy use of OCSP in your existing PKI.

Security – Thanks to Validation

The basis of any functioning PKI is the use of valid certificates for secure and confidential user communication. The key to the success of a PKI thus lies in reliable certificate revocation and validation. Larger, more mature PKIs often contain many invalid certificates, which means that fast and reliable validations of certificates used are a critical PKI success factor.

Certificate Revocation Lists (CRLs) provide information about blocked certificates. To check a certificate's status, the complete CRL is transmitted and checked for the requested certificate. Particularly in large, dynamic PKIs the CRLs are large and contain a lot of data, which makes validation using CRLs wasteful in terms of both data storage space and time.

It's another story altogether with Online Certificate Status Protocol validation. OCSP uses the latest version of each CRL as a basis for certificate validation. CRLs can be imported from any directory level and are a basic component of Certificate Authorities (CA) and all CA software. The OCSP Responder imports the latest CRL once, saves the information internally in an optimized format, and can send a validation response in real-time as soon as it receives an OCSP status request. The OCSP Responder is compatible with industry standards and can be easily integrated into any CA.



TC OCSP Responder

For Real-Time Certificate Validation

→ Features & Benefits:

- > Scalable for millions of users
- > Only low bandwidth required between responder and client
- > Supports signed and linked event log entries, as well as rotating log files
- > High performance
- > Can be configured to support a wide variety of validation models
- > Interface for CRL upload and automatic processing integration

→ Standard Compliance:

- > Fulfills ISIS-MTT standards
- > Fulfills IdenTrust requirements
- > Supports OMA Online Status Protocol Mobile Profile Candidate Version 1.0
- > Supports CRLv1, CRLv2 and Delta CRLs
- > Interoperable with Windows Vista
- > Supports Multi-CRL / Multi-CA
- > OCSP (IETF RFC 2560)
- > SSL 2.0, 3.0, TLS 1.0
- > X.509 v3 Digital Certificate Format
- > RSA PKCS#1, PKCS#10, PKCS#11, PKCS#12

→ System Requirements:

Platform Availability

- > Linux (32bit and 64bit)
- > Solaris (8 or newer, 32bit and 64bit)

Hardware Security Modules (HSM) with standardized PKCS#11 interface

- > nCipher
- > Eracom
- > AEP
- > others

The Technological Advantage of PGP TrustCenter

- * TC OCSP Responder supports a separate monitoring interface, which is used to check the responder status and view user statistics.
- * TC OCSP Responder is easily extensible with user-specific modules via a plug-in client API. These modules can perform additional checks, evaluate extra request fields and write additional response data in the OCSP validation response.
- * Plug-in available for UniCert 5.2. This plug-in reads the certificate revocation status directly from the CA database, circumventing the extra step of checking CRLs – plus the validation response is always based on the latest certificate revocation status.

The Advantages of Working with PGP TrustCenter

PGP TrustCenter provides digital trust between employees, clients and suppliers doing business electronically through on-demand certificate management services. The company's solutions enable a wide range of digital trust applications to provide strong authentication, secure e-mail, digital signatures, data encryption and support compliance with privacy and other regulations. PGP TrustCenter was the first to provide digital certificate management through a Software as a Service model and remains the leader through its breakthrough economics, versatility and implementation speed for enterprises. Unlike traditional PKI and private certificate authority options, PGP TrustCenter solutions can be implemented in 70% less time and 70% less cost.

This document is for information only and without responsibility. PGP TrustCenter reserves the right to change scope of services.