EverTrust and Entrust Deliver an OCSP Performance Tool

HIGHLIGHTS

EverTrust OCSP is a complete, PKI-agnostic, and high-performance solution for digital certificate validation. A native integration with Entrust nShield HSMs allows the securing of the OCSP signer's private keys.

- Supports multiple PKI providers
- Offers flexible and agile implementation
- Standards compliant

The Problem

With the exponential increase in the use of certificates in both on-premises and cloud environments, certificate verification and validation become major issues in terms of security and performance. Because the use of certificate revocation lists (CRLs) is being phased out, more and more applications require the Online Certificate Status Protocol (OCSP).

PKI solutions implement an OCSP responder that checks the status of certificates, but it is often difficult to dissociate the responder from the PKI, making it impossible to work with other PKI providers. In other words, this implementation cannot provide a solution for hybrid, distributed, and agile environments.

The Challenge

Conforming to infrastructure requirements

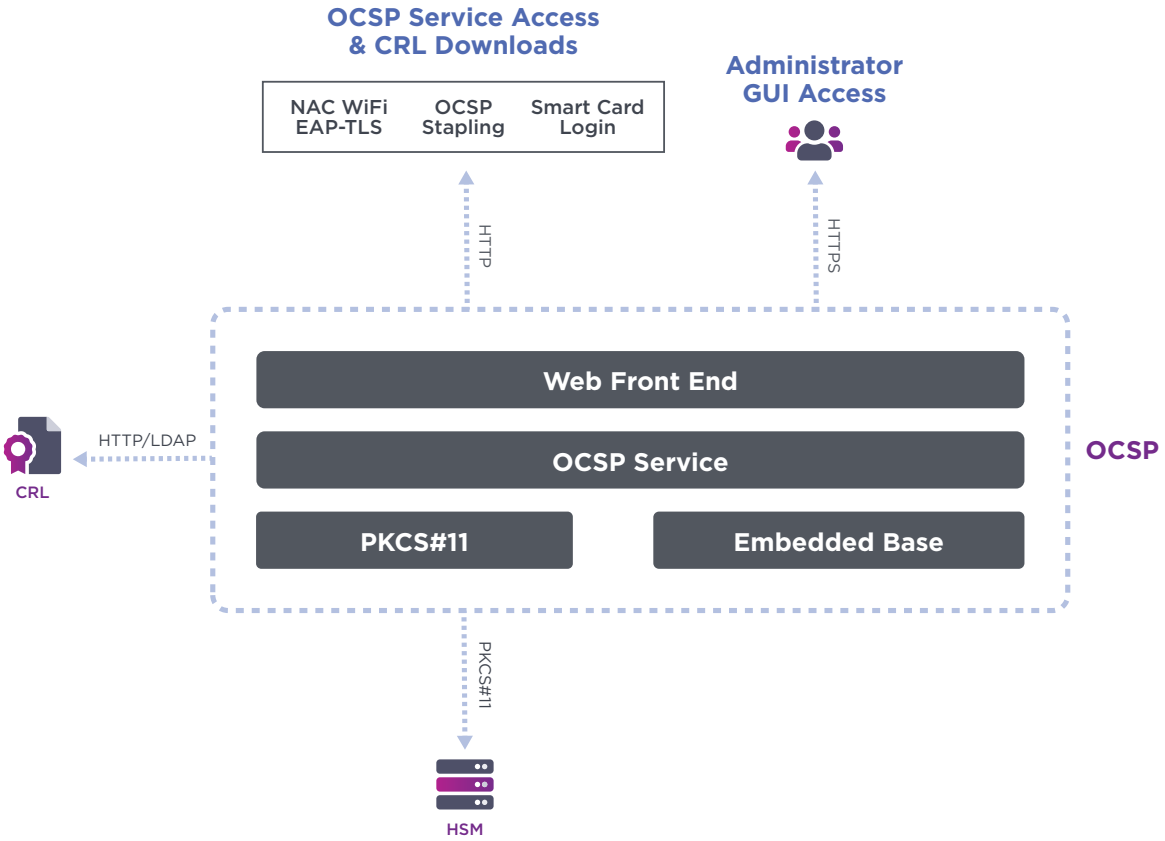
The main challenge is to provide a solution that conforms to infrastructure requirements, including:

- Independence of the underlying systems (PKI)
- Deployment in distributed mode in order to be as close as possible to the requestor
- Scalability and efficiency
- Simplicity and ease of management

EVERTRUST

Learn more about our HSMs at entrust.com/HSM

Deploy, secure, and scale Online Certificate Status Protocol



The Solution:

EverTrust OCSP and Entrust nShield HSMs

EverTrust OCSP is a versatile OCSP responder, compliant with RFCs 5019 and 6960, that can be integrated with any PKI platform. It is designed to retrieve revocation information based on CRLs. The simple and intuitive web interface allows organizations to manage the complete lifecycle of OCSP signing keys that are stored in an Entrust nShield® hardware security module (HSM).

EverTrust OCSP supports the following standards:

- X509v3
- CRL v2
- PKCS#11
- OCSP stapling
- REST APIs
- TLS v1.2/1.3 for admin interface access
- HTTP and LDAP for CRL download

It also supports different deployment options:

- Kubernetes/Docker
- VM or Bare Metal with Red Hat EL6/7/8
- Virtual appliance via an OVA

OCSP protocol is “stateless” so EverTrust OCSP can simply be upgraded to active/active high availability by adding nodes and positioning a load balancer on the front end. The solution can be easily adapted to the volume and performance required in the client environment.

Learn more about our HSMs at entrust.com/HSM

Deploy, secure, and scale Online Certificate Status Protocol

Why use Entrust nShield HSMs with EverTrust OCSP?

Trust in the OCSP response is essential in the certificate validation mechanism, so the integrated solution allows for creation of signing keys using an Entrust nShield HSM. This architecture combines the reliability and performance of the OCSP response with the security of a FIPS- and Common Criteria-certified HSM.

Encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material.

nShield HSMs integrate with EverTrust OCSP to provide logical and physical protection of keys. The combination delivers an auditable method for enforcing security policies.

nShield HSMs enable customers to:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed
- Deliver superior performance to support demanding applications

Entrust nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With nShield HSMs you can:

- Provide a tightly controlled, tamper-resistant environment for safeguarding and managing encryption keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, and CNG)

About EverTrust

Managing a huge volume of certificates is time-consuming and a major source of errors. That's why EverTrust, a software company specialized in digital trust, has developed a suite of products that allow the scheduling of the certificate lifecycle and the verification of their status. We fight daily for the generalization of the use of certificates on all on-premises and cloud ecosystems by facilitating the orchestration of the lifecycle. EverTrust solutions allow you to strengthen the trust in your infrastructure.

For more information visit **evertrust.fr**

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223