

EJBCA_{PKI}

OCSP responder

Ensure certificate status verification in a timely and reliable fashion

PrimeKey Solutions AB is the originator and main developer of the world-wide used Enterprise Java Beans Certification Authority (EJBCA) - a full featured industrial strength open-source J2EE based PKI implementation.

With it's technology, coverage of supported standards, multilingual interface, support for databases and directories, EJBCA is rapidly gaining the leading role as the PKI implementation of choice for commercial enterprises, governmental institutions and other organizations all over the world.

Organizations that deploy a certificate infrastructure must also provide means for users to verify validity of the certificates used. Normally this is done by means of Certificate Revocation Lists (CRL), where CA periodically publishes the list of revoked certificates. However, use of CRLs may be inconvenient or inadequate in certain situations - in such cases organizations may opt to use EJBCA **OCSP responders**.

Key Benefits

Timeliness of verification

- where periodicity of CRL is not sufficient
- certificate status data is replicated in OCSP status database as soon as CA changes the status

Save Time and Money

- open source - no software licenses
- shorten development time

Scalability and reliability

- support for leading HSMs
- clustering allows for service availability even with extreme loads

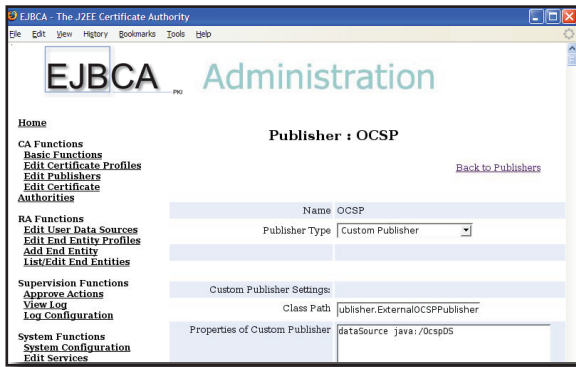
There are two factors that affect certificate validation using CRLs:

-First, the user has to have access to the latest published CRLs from the entire chain of issuing CAs for a particular certificate that is to be verified. Such lists may be located with different publishers.

-Second, in cases of large-scale infrastructures, CRLs may contain lots of data on numerous certificates that have been revoked.

Thus, there are several possible points where malfunction may cause failure of the verification of the entire certificate chain, and also, network traffic gets unnecessarily increased.

Online Certificate Status Protocol (OCSP) was written with intention to offer a service where users can check validity of a certificate, where the service itself has the access to the latest published CRLs. Using OCSP, network traffic needed to verify a certificate status is reduced.

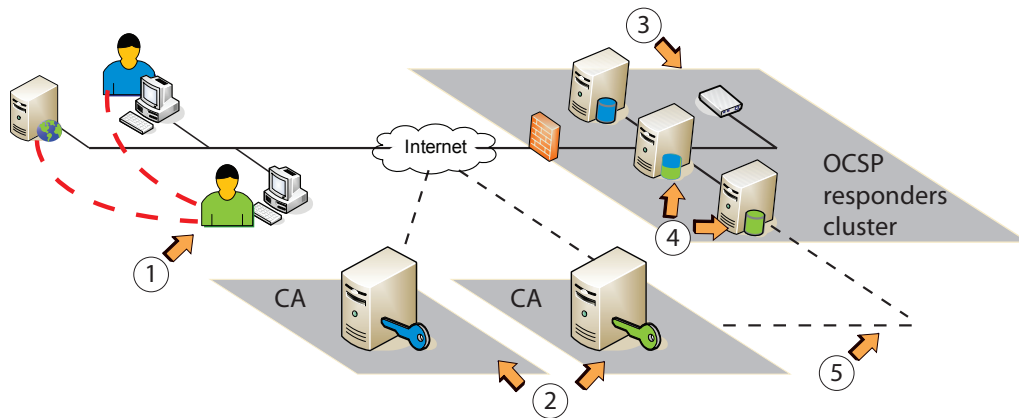


EJBCA can be configured to support variety of publishers, including OCSP responders.

What organizations should use OCSP responders?

OCSP responders should be used within those organizations that want to assure the real time status of the certificates used to, say, complete transactions or perform digital signatures. Additional good reason for use of OCSP responders is to increase network performance.

With PrimeKey OCSP responder it is possible to have your CA immediately publish change of status for a certificate - independently of the creation of CRLs. This feature is already built in with EJBCA and for other CAs works by means of adaptors.



How does it work in practice?

End users have their digital certificates to, say, send digitally signed documents or to securely access web servers (1) to perform some transactions. Observe that the certificates may be issued by different certificate authorities (2). In order to ensure that the certificates of other parties are valid, users and servers check the real time status with the OCSP responders (3) that can be clustered and equipped with hardware security modules (HSM) to provide high performance and protection of signing keys. The OCSP responders cluster can serve one or more CAs (4), depending on the requirements, and update of its local databases, either by means of collecting CRLs or by secured communication with a CA (5), which then updates status database as soon as administrators change validity of a certificate with the CA.

What needs to be done by the customer?

- The most important thing is to identify the performance requirements. Depending on the nature of appliance, there may occur steep peaks in the usage of status verifications.
- Decide if your organization will use HSMs, and in that case which HSMs to choose.
- Plan for integration with existing CA infrastructure, if needed.
- Decide which service agreement level best suits your organization.

PrimeKey can assist with all those tasks.

Contact us via e-mail
OCSP@primekey.se
 Visit us at **www.primekey.se**
 Read more about EJBCA and OCSP at
www.ejbca.org

 PrimeKey Solutions

Anderstorpsvägen 16
 171 54 Solna
 Sweden