

OCSP - Online Certificate Status Protocol

OCSP ist ein Protokoll zur Online-Überprüfung des aktuellen Zustands eines Zertifikats. Mit der Statusabfrage über OCSP wird ermittelt, ob ein Zertifikat noch gültig oder gesperrt ist. Im Gegensatz zur Statusabfrage über Sperrlisten (CRL) erlaubt OCSP eine einfache und vor allem zeitlich aktuelle Statusprüfung. Dies ist besonders für Transaktionen wichtig, bei denen grosser Wert auf Vertraulichkeit, Integrität und Authentizität gelegt wird. Das OCSP-Protokoll wurde von der IETF spezifiziert und standardisiert (RFC 2560). OCSP ist unter Windows Vista das bevorzugte Protokoll zur Statusabfrage von Zertifikaten.



Maximale Sicherheit und Flexibilität

Der Validation Server von Keyon unterstützt beliebig viele File-, AD, LDAP- oder HTTP(S)- Statusquellen von beliebig vielen internen oder externen CA's. Mehrstufige Zertifikathierarchien sowie Cross-Zertifikate sind ebenfalls unterstützt. Alle gängigen X.509-Erweiterungen werden interpretiert. Der Schlüssel zur Signierung von OCSP Antworten kann in einem HSM oder in einem Soft Token gespeichert werden.

Weit verbreitetes Standardprotokoll

Microsoft nutzt ab Windows Vista bevorzugt das OCSP zur Statusabfrage von Zertifikaten. Dies gilt auch für Adobe Acrobat und andere Applikationen, die grossen Wert auf eine sichere, nachvollziehbare und aktuelle Prüfung der Zertifikate legen. Im Umfeld von rechtsgültigen Signaturen gemäss ZertES ist OCSP eine zwingende Voraussetzung für die Prüfung von elektronischen Signaturen.

Webbasierte Administration

Die Administration erfolgt über eine Weboberfläche mit zertifikatsbasierter Authentifizierung. Beliebige viele Benutzer können konfigurierbaren Gruppen mit fein granularen Rechten zugeordnet werden.



OCSP Client Lösungen

Mit dem PKI Framework (C, C++, Java, .NET) von Keyon können Ihre bestehenden Applikationen schnell und kostengünstig um die OCSP Funktionalität erweitert werden. Microsoft CAPI basierte Applikationen (Outlook, IE, etc.) unter Windows XP werden mit dem Plugin von Keyon OCSP fähig. Windows Vista unterstützt OCSP standardmässig.

Skalierbare und performante Lösung

Unter Verwendung eines HSM können mehrere hundert OCSP-Anfragen pro Sekunde beantwortet werden. Eine Integration in Load-Balancing oder Cluster-Systeme garantiert eine hohe Verfügbarkeit und Performance. Alle aktuellen Statusinformationen werden lokal in einem Cache abgelegt, um im Falle eines Neustarts als Basis für die Validierungsinformationen sofort und unabhängig von anderen Komponenten zur Verfügung zu stehen.

OCSP Validation Server

- Sichere, nachvollziehbare und aktuelle Prüfung von X.509 Zertifikaten
- Kombinieren von beliebig vielen Statusquellen (File, AD, LDAP, HTTP(S), Black- und Whitelists)
- Unterstützung von PKCS#11 Tokens
- Als Software- oder Hardware Appliance Lösung erhältlich (SafeNet Luna SP)