

Overview

X.509 INTERNET PUBLIC KEY INFRASTRUCTURE ONLINE CERTIFICATE STATUS PROTOCOL (RFC 2560) PKI-technologies are gaining more and more importance for securing critical corporate online transactions. Quick revocation of certificates is one of the most important aspects. CertControl is the secure and efficient alternative for using CRL-technologies with difficult administration. All advantages offered by OSCP (central validity management, improved data protection, reduced network occupancy and detailed accounting) are fully available.

Through the use of proven technologies such as the Apache webserver on such platforms as Solaris, Linux and Windows NT, high operational stability can be attained, as practice has shown.

✓ BENEFITS

Things to say

- Speed
- Stability
- Extensibility
- High availability
- Interoperability with all major operating systems
- Identrus compliant
- Efficient caching
- Open architecture
- Flexible forwarding
- Policy driven

More things to say

- Less fraud, therefore costs due to fraud can be minimized.
- High degree of confidence in transactions.
- Reduces liability
- Increases efficiency
- Helps to manage risks
- Cost effective
- HSM Support
- Less network traffic: client only requests needed information.
- Central, fast and flexible risk management
- Reduced complexity in user applications

! HIGHLIGHTS

Adaptable solution

CertControl can be used on various platforms and can be adapted to specific customer requirements very easily. CertControl has been realised as Apache webserver plug-in which means that it is highly efficient at reasonable cost.

High operational stability

Through the use of proven technologies such as the Apache webserver on such platforms as Solaris, Linux and Windows NT, high operational stability can be attained, as practice has shown.

Performance / scalability

The use of the entire functionality of the Apache webserver technology and state-of-the-art crypto hardware allows for good scalability. Both the requirements of internal PKIs as well as national and international trust centers with several millions of enquiries per hour are fulfilled by CertControl.

CertControl

Technical Reference

Software-Basis

Apache 1.3.19
 Apache SSL (mod_ssl)
 Apache clustering (optional)
 Apache load-balancing (optional)
 Apache proxying (optional)
 OpenSSL 0.9.6a

Standards

Online Certificate Status Protocol
 X.509 Internet Public Key Infrastructure
 IETF PKIX RFC 2560
 identrus IT-OCSPCR 4.7
 OCSPv2 (partial)
 DPD, DPV, SCVP (planning)

Operating Systems

Windows NT 4.0 SP3 and up
 Windows 2000
 Solaris 2.7
 Solaris 8
 intel - Linux
 HP-UX (optional)
 AIX (optional)
 S/390-Linux (optional)

Management

SNMP Traps
 E-Mail alarming (optional)
 SNMP v3 (optional)
 Tivoli (traps only, optional)

OCSP-Functions

chaining
 proxying
 hiding
 caching
 OCSP over SSL
 multiple CA's

Access Control

multiple responder (virtual host)
 certificate based (signed OCSP-requests)
 certificate based (SSL client authentication)
 HTTP-basic authentication (username, password)
 IP-Address based
 NTLM authentication
 custom modules

Revocation Information

LDAP (CRL-based)
 HTTP (CRL-based)
 Baltimore UniCERT direct (positive check)
 ValiCert VPUBLISH (CRL-based)
 Oracle (generic, positive check)
 emergency revoked status
 OCSP forwarding
 custom functions (PHP, Perl, Binaries)

Crypto Accelerator (HSMs)

PKCS#11 (generic)
 Baltimore Keyper
 nCipher nFast
 nCipher nShield

Logging, Accounting

Standard Web-Server Logging
 flexible, configurable logging
 Web-Status screen

Configuration GUI

Web-GUI (webmin-based)
 Windows-GUI (optional)
 Baltimore-style Windows GUI (optional)
 text configuration file compatibility ValiCert Validator
 XETI-Libraries
 Baltimore (UniCERT, KeyTools, MailSecure)
 Netscape PSM

Extensibility

standard cgi-bin interface for custom checks
 standard Apache modules
 proprietary module interface API
 proprietary revocation info API

Scalability

Apache multitasking/multithreading
 child control in terms of CPU and memory usage
 automatic, optimal child forking