KeyOne

Validation Authority

Description

KeyOne VA is suitable for critical processes of electronic signature validation since it provides evidential value and greater efficiency in the verification of the status of the digital certificates.
KeyOne VA is designed to:

- Provide reliable information on the status of a digital certificate
- Process information form one or multiple CAs using CRLs or CA records
- Facilitate integration with corporate information systems
- Reduce installation and maintenance costs

Benefits

Maximum security

KeyOne products support defining the roles and events required to operate in compliance with the CEN TS 419 261 “Security Requirements for Trustworthy Systems Managing Certificates and Time-stamps” (replaces CWA14167-1). KeyOne VA supports the roles of security operator, system administrator and system auditor.

Reliability and control

The event system guarantees the integrity of the registered data and that no information is lost. This is possible thanks to an emergency mechanism that is activated when connection to the database is lost. KeyOne also supports selecting automatic events (which are assigned different levels of severity) and defining manual events (for registering actions that occur outside the application).

Efficiency for large infrastructures

KeyOne VA facilitates managing large volumes of certificates via the KeyOne CA certificate database connection. As certificate status updating is optimized, the response efficiency is guaranteed. KeyOne VA supports high availability and scalable architectures.

Easy to integrate and accounting

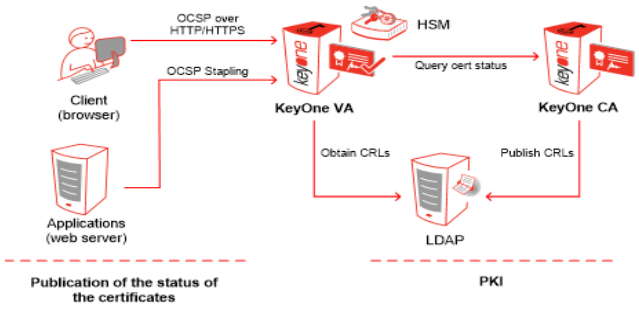
KeyOne VA includes a workflow engine to define the interaction with information systems. It is possible to customize the system, incorporate new functions, connect to access-control systems and access internal information systems (to complement the response generated).

KeyOne
Validation Authority

Architecture

The following figure illustrates the general architecture of KeyOne VA and how it interacts with network components (applications or users) under the IETF OCSP standard. KeyOne VA can operate with a HSM (network or internal) and requires access to a database and a network time source (not shown in the figure).

Depending on the configuration of the certificate status update system, KeyOne VA connects regularly to the KeyOne CA certificate database or downloads CRLs from an LDAP directory or a Web server. If it connects to KeyOne CA, KeyOne VA can obtain information on the status of certificates and the certificate transparency information.



Functions

The main functions of KeyOne VA are to:

- Store information on the status of certificates generated by one or more certification authorities.
- Respond to the requests for information on the status of digital certificates used in the signing of electronic transactions. These requests can come from users or service providers.
- Respond to the requests for information on the status of digital certificates used when a Web server protects the communication via SSL/TLS. These requests can come from either the user's browser or the Web server if OCSP stapling is used.
- Guarantee the non-repudiation of the responses. These responses are digitally-signed by the Validation Authority and specify the date and status (valid, revoked, suspended or unknown) of the certificate.
- Redirect, if necessary, the requests to an external OCSP responder that can provide an authoritative response for certain certificates.
- Generate event logs so operators can monitor the system status, its security and to what extent the corporate specifications are being met.
- Optionally, keep track of and limit each client's use of the OCSP service. To do this, KeyOne VA, assign a service usage quota or restrict use for a specific time period (i.e., billing).

Technical Specifications

- **Online validation protocol:** OCSP as per IETF RFC2560 and RFC 6960. Support of OCSP Stapling (IETF RFC 6066 and RFC 6961).
- **Certificate Transparency:** IETF RFC 6962.
- **Cryptographic devices:** RSA PKCS #11.
- **Connectivity:** SQL, LDAP/SLDAP, Microsoft Active Directory, HTTP/HTTPS, REST and SOAP Web Services, POP3 and SMTP.
- **Update mechanism:** ITU-T X509v3 CRL, quieries to KeyOne CA and/or external OCSP Responder. Supports multiple CAs.
- **Event monitoring:** SNMP v1, v2c and v3.
- **SIEM integration and audit:** Syslog protocol or Windows Event Log.
- **Certification:** CC EAL4+ (*)

System Requirements

- **Operating systems:** Windows or Solaris SPARC.
- **SMTP mail server:** Recommended for implementing customized event notification.
- **Database systems:** Oracle, Microsoft SQL Server, MySQL or Maria DB.
- **Optional HSM:** Thales nCipher and SafeNet. Contact Safelayer to find out which models are homologated.
- **Time source:** Operating system time synchronized with an external source.

(*) KeyOne VA has achieved the ISO/IEC 15408 EAL4+(ALC_FLR.2) guarantee level (http://www.oc.ccn.cni.es/) and complies with the CIMC security level 3 Protection Profile Certificate Issuing and Management Component, NIST, version 1.0.

Safelayer Secure Communications S.A.
Basauri, 17 Edif. Valrealty Edif. B Pl. Baja Izquierda Ofi. B
28023 Madrid (Spain)
Tel. +34 917 080 480 Fax +34 913 076 652

www.safelayer.com
World Trade Center (Edif. Sud- 4ª Planta). Moll de Barcelona s/n
08039 Barcelona (Spain)
Tel. +34 935 088 090 Fax +34 935 088 091

SAFELAYER