



www.safelayer.com

KeyOne VA

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 (in contrast to the conventional mechanism which are based in revocation lists).

KeyOne VA is designed to:

- Provide reliable information on the status of a digital certificate
- Facilitate integration with corporate information systems
- Reduce installation and maintenance costs

Benefits

• Maximum security

KeyOne version 3.0 products comply with the security requirements for digital certificate management systems for electronic signatures (CWA 14167-1). These products are Common Criteria EAL4+ certified under the CIMC security level 3 Protection Profile. Their configuration system supports defining the roles and events required to operate in CWA 14167-1 mode, in CIMC NSA/NIST mode and in customized security levels.

• 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 CertStatus Server publication service. As certificate status updating is optimized, the response efficiency is guaranteed. KeyOne VA supports high availability and scalable architectures.

• Easy to integrate and customize

KeyOne VA features an interpreter for the high-level Safelayer Scriptor language. Scriptor can be used to customize the system, incorporate new functions, connect to access-control systems and access internal information systems (to complement the information generated).





www.safelayer.com

KeyOne VA

VALIDATION AUTHORITY

Functions

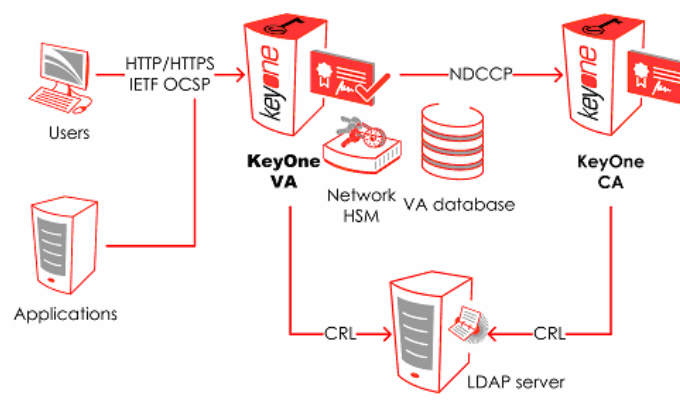
The main functions of KeyOne VA are to:

- Store information on the status of the certificates generated by one or more Certification Authorities. The status of a digital certificate is updated by downloading the revocation lists or the information provided by Certification Authorities (CA) that have the KeyOne publication service (KeyOne CertStatus Server) installed. In both cases, updating is performed remotely.
- Receive user or service-provider requests on the status of the digital certificates used in the signing of electronic transactions.
- Guarantee the non-repudiation of the responses. These responses are digitally-signed by the Validation Authority and specify the date and status (valid, revoked, cancelled or unknown) of a certificate.
- Generate event logs so operators can monitor the system status, its security and to what extent the corporate specifications are being met.
- Customize the system to tailor response delivery and content to the identity of the requester.

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 a CA or an LDAP directory. If it connects to a CA, the information on the status of the digital certificates comes from the KeyOne CA databases (which are accessed via the CertStatus service and the Safelayer's NDCCP protocol). If it connects to an LDAP directory, the CRL published in the directory (or in a Web server not shown in the figure) is downloaded.



Publication of the status of the certificates

PKI

Specifications subject to change without notice. All brand names are registered trademarks of their respective owners. Updated May 2009.

Technical Specifications

- * **Online validation protocol:** IETF RFC2560.
- * **Database access:** Oracle, Microsoft SQL Server.
- * **Cryptographic devices:** RSA PKCS #11.
- * **Connectivity:** LDAP, Microsoft Active Directory for Windows versions, HTTP or secure HTTP (SSL).
- * **Update mechanism:** ITU-T X509.v3 CRL and/or the KeyOne CertStatus Server module. Supports multiple CAs.
- * **Certification:** CC EAL4+ (*).

System Requirements

- * **Operating systems:** Windows or Solaris with Java JRE 6. Minimum architecture requirements: Intel 1x Dual Core with 4 GB RAM for Windows; UltraSPARC IIIi with 8 GB RAM for Solaris.
- * **SMTP mail server:** Recommended for implementing customized event notification.
- * **Database systems:** Oracle or Microsoft SQL Server.
- * **Optional HSM:** PKCS #11 (currently homologated nCipher and SafeNET models).
- * **Time source:** Operating system time synchronized with an external source.

(*) KeyOne 3.0 has achieved the ISO/IEC 15408 EAL4+(ALC_FLR.2) guarantee level (www.oc.ccn.cni.es/certificacion_en.html) and complies with the CIMC security level 3 Protection Profile (Certificate Issuing and Management Component, NIST, 31 October 2001)



SAFELAYER SECURE COMMUNICATIONS S.A.

c/Basauri, 17 Edif. Valreality Edif. B Pl. Baja Izquierda Ofi. B 28023 Madrid (SPAIN) Tel.: +34 917 080 480 Fax: +34 913 076 652
World Trade Center (Edif. Sud- 4º Planta). Moll de Barcelona s/n 08039 Barcelona (SPAIN) Tel.: +34 935 088 090 Fax: +34 935 088 091