KeyOne

Certification Authority

Description

KeyOne public key infrastructure (PKI) solution component that provides certification authority (CA) functions.

KeyOne CA provides:

- Public key infrastructure deployment for governments, certification service providers and corporate environments.
- Management of user digital certificates in mobile devices, centralized servers and smart cards.
- Digital certificate provision for servers, applications and communication devices that require authentication, e-signing and data encryption.
- Maximum security guarantees and CA compliance with CEN and ETSI recommendations.
- Reduced integration and maintenance costs through support for integration standards including REST/JSON and SOAP/XML interfaces.

Benefits

Complete and scalable

KeyOne CA is optimized for managing large volumes of certificates. It can handle CRLs with multiple distribution points, ideal for government and large infrastructures. The KeyOne solution includes components that provide advanced functions to the PKI, including registration (KeyOne XRA), certificate validation (KeyOne VA) and time-stamping (KeyOne TSA).

Standard support and movility

KeyOne CA supports X.509 digital certificates interoperable with Windows, Mac and Linux desktop environments and mobile devices with Google Android and Apple iOS operating systems. KeyOne provides PKI authentication, e-signing and date encryption without requiring proprietary applications. It is adaptable to the security mechanisms of a wide range of PKI-compatible applications and platforms.

Greater PKI control and management

KeyOne automatically manages the CA keys, providing greater ease of management and control of the public key infrastructure (PKI). You can define the events executed when keys are renewed, incorporate mechanisms to adjust the maximum lifetime of the digital certificates and manage the coexistence of expired CA keys (used to transparently revoke certificates generated with these keys).

Integration and reduced maintenance costs

KeyOne CA operates as a network-accessible specialized service component. The system can be operated from the GUI or via the JSON on REST and XML on SOAP interfaces it incorporates. This reduces the cost of integrating and maintaining the digital certificate management functions. It supports standard protocols for information and security event management and monitoring, facilitating integration with SIEM and corporate monitoring systems.

Maximum security and trust

KeyOne CA is designed to facilitate compliance with the security requirements for trustworthy systems managing certificates for electronic signatures (CEN TS 419 261 replaces CWA 14167-1) in terms of roles and events. It facilitates adaptation to the eIDAS Regulation (ETSI EN 319 411-2)), PSD2 Directive and recommendations for certification authority policies that issue recognized digital certificates. The system supports FIPS 140-2 level 3 HSMs and is ISO/IEC 15408 EAL4+ (ALC_FLR.2) certified.

KeyOne

Certification Authority

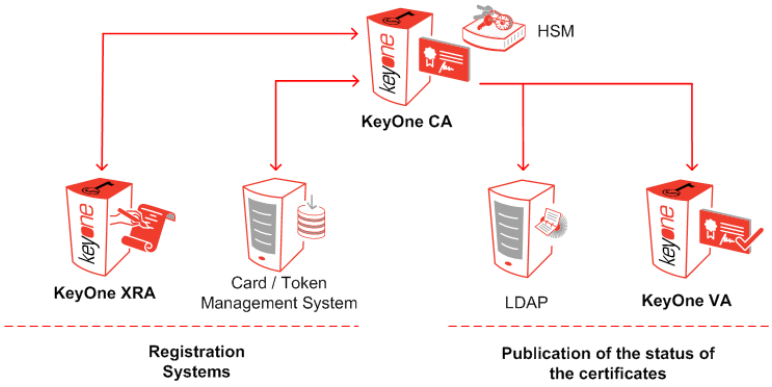
Functions

KeyOne CA can act as a Root CA, Subordinate CA, Cross CA and a Bridge CA. Depending on how it is used, the CA operates in conjunction with the Safelayer KeyOne XRA product or an application that assumes the entity registration functions. KeyOne CA can also operate in conjunction with the KeyOne VA product to provide the digital certificate validation service. The main functions of KeyOne CA are to:

- Generate and protect the private keys via the use of cryptographic devices (HSM).
- Automatically manage the life-cycle and the coexistence of the private keys of the CA.
- Manage recognized RAs and assign them certification policies.
- Generate the ITU-T X509v3 digital certificates (for users and applications) requested by the RAs.
- Generate and publish lists of revoked and suspended certificates (CRLs).
- Report on the status of the digital certificates so the validation service (VA) can publish it via OCSP.
- Allow the secure protection and retrieval of encryption keys (if they become lost).
- Guarantee the secure auditing of the events and actions carried out in the system.

Architecture

The following figure illustrates a Certification Authority (CA) operated by KeyOne CA and how it interacts with KeyOne (or third party) products to provide registration and publishing options for the status of the certificates. The registration system can be implemented with KeyOne XRA or a third party card token management system (CMS/TMS) that acts as the RA. A directory, a Web server (not shown in the figure) or KeyOne VA can be used to publish the status of the certificates (using CRLs or OCSP). The HSM (network or internal) used for protecting the private keys of the CA is also shown in the figure.



Technical Specifications

- **Certificate format:** ITU-T X.509v3, IETF RFC 5280 and RFC 6818.
- **Certification profiles:** All standard extensions defined by ITU-T X.509v3, IETF RFC 5280 and RFC 6818. Qualified certificates according to RFC 3739, eIDAS Regulation (ETSI EN 319 412-5, replaces TS 101 862) and PSD2 Directive. EV SSL certificates according to CA/Browser Forum guidelines.
- **Revocation information:** Single and multiple ITU-T X.509v2 CRL distribution points. OCSP via the optional KeyOne VA component.
- **Certificate generation:** RSA PKCS#10/PKCS#7. PKIX-CMP as per RFC 4210. Support of Certificate Transparency (IETF RFC 6962) and DNS CAA (IETF RFC 6844).
- **Key archiving:** RSA PKCS#8 and PKCS#12 via the optional KeyOne Archive component.
- **Connectivity:** SQL, LDAP/SLDAP, Microsoft Active Directory, HTTP/HTTPS, REST/JSON and SOAP/XML Web Services, POP3 and SMTP.
- **Cryptographic devices:** RSA PKCS #11 with M-out-of-N secret sharing schemes.
- **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.
- **Database systems:** Oracle, Microsoft SQL Server, MySQL or MariaDB.
- **Optional HSM:** Thales nCipher and SafeNet. Contact Safelayer to find out which models are homologated.
- **LDAP server:** Recommended for publishing certificates and CRLs to directory.

(*) KeyOne CA with ISO/IEC 15408 (ALC_FLR.2) level of assurance (https://www.commoncriteriaportal.org/products/) and compliant with NIST's CIMC ("Certificate Issuing and Management Component") Security level 3 Protection Profile, 31 October 2001.

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