KeyOne

Registration Authority

Description

KeyOne XRA is part of Safelayer's public key infrastructure (PKI) solution. It provides the registration authority (RA) functions:

- User registration and digital certificate life-cycle management through interaction with KeyOne CA.
- Certificate life-cycle management for PKI services and applications that require authentication, signature and data encryption.
- Digital certificate management for a wide range of user platforms and devices.
- Simplified PKI deployment thanks to a complete range of face-to-face and remote registration mechanisms.
- Registration system integration in corporate processes using the REST/JSON and SOAP/ XML standard interfaces.

Benefits

User and mobility environments

KeyOne XRA's user management is independent of its environment. This enables deploying PKI authentication, e-signing and encryption for a wide range of PKI-compatible applications and platforms: Windows, Mac and Linux desktop environments and mobile devices with Google Android and Apple iOS operating systems are supported.

Certificates for applications

KeyOne XRA also manages applications that require digital certificates. It interacts with KeyOne CA to provide digital certificates for different purposes, including SSL, SSL EV, VPN certificates and certificates for PKI services requiring authentication, e-signature and data encryption based on X.509 digital certificates

Workflows and registration

KeyOne XRA is extremely adaptable to business needs: for user registration processes and for the delivery of digital certificates to users. Its workflow manager provides simple and reliable system configuration for defining what data processing actions are to be included in the registration process and what data the system is to exchange with users, operators and applications.

Integration and cost saving

KeyOne XRA is ideal for integrating PKI registration in corporate processes. System functions can be used as Web services via the product's REST and SOAP interfaces. The workflow management system supports easily defining which functions are provided as Web services and which are accessible from the GUI.

Maximum security and control

KeyOne XRA includes the role management, auditing and reporting mechanisms recommended for digital certificate management systems for CEN TS 419 261 (replaces CWA 14167-1) e-signature. It facilitates adaptation to the eIDAS Regulation (ETSI EN 319 411-2) and ETSI TS 101 456 recommendations for the policies of certification authority policies that issue recognized digital certificates.

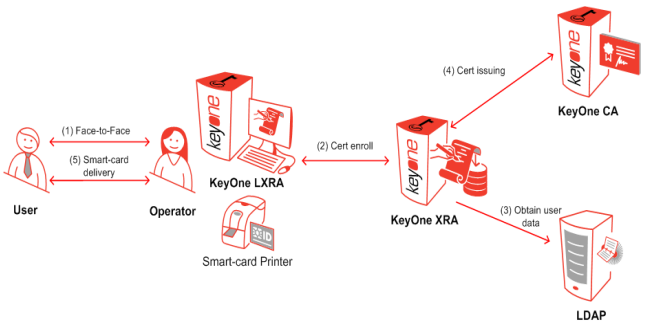
KeyOne

Registration Authority

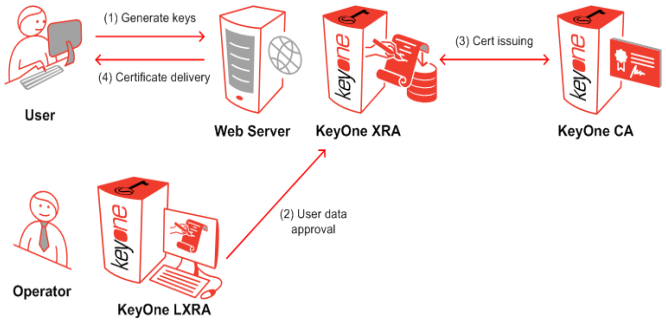
Functions

KeyOne XRA operates as a user/application registration service (RA) for requesting the issuing and revocation of digital certificates (in conjunction with KeyOne CA). The system can combine the following registration procedures:

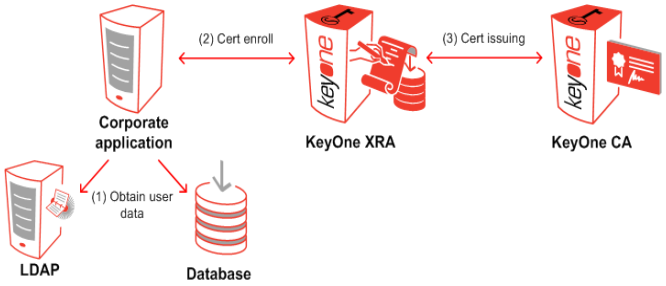
- **Face-to-face.** Requesters verify their identity face-to-face to obtain their digital certificates. Once the registration agent approves the request, the keys are generated on the user's cryptographic card, mobile device or PC, depending on the registration policy. For deploying the registration station close to requesters, the agent can use KeyOne LXRA connected to a smart card printer, the KeyOne XRA client application.



- **Remote.** In the Web registration model, the registration system lets the end user deliver their certification requests remotely, usually by Web browser. Requesters either have PCs for software certificates or certificates on cryptographic cards, or mobile devices for certificates and keys for mobile operating systems. Application and device certificates are also requested via Web and/or standard protocols like SCEP and Windows Enrollment protocols. Requests can be pre-authorized (in this case, the requester usually authenticates by password), or the registration agent can approve them after validating the registration details provided by the requester.



- **Automatic**. Supports loading requester details from a trusted source, e.g., a HRM database or directory provided by a corporate application that interacts with KeyOne XRA. The connection with KeyOne XRA is performed using XRA's REST/JSON or SOAP/XML interfaces for remotely invoking the registration system's digital-certificate approval, renewal and revocation functions. The RA can also connect directly with the corporate database or directory to obtain requester details.



Technical Specifications

- **Certification request formats: :** PKIX-CRMF, RSA PKCS #10, ITU-T X.509v3 and Firefox.
- **Certificate delivery and certification chain formats:** RSA PKCS #7, PKCS #12 and ITU-T X.509v3.
- **Certificate enrollment protocols:** REST/JSON, SOAP/XML, SCEP, Windows Enrollment and Apple OTA Enrollment.
- **Certification profiles:** All the standard extensions defined by ITU-T X.509v3, Firefox and Microsoft.
- **Connectivity:** SQL, LDAP/SLDAP, Microsoft Active Directory, HTTP/HTTPS, REST and SOAP Web Services, POP3 and SMTP.
- **Cryptographic devices:** RSA PKCS #11.
- **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 Server and Maria DB.
- **Optional HSM:** Thales nCipher and SafeNet. Contact Safelayer to find out which models are homologated.
- **LDAP server:** Recommended for publishing certificates and CRLs in directory.
- **SMTP mail server:** Recommended for the generation of automatic notifications.
- **Smart card printers:** Datacard. Contact Safelayer to find out which models are homologated.
- **Smart cards:** G&D, SafeNet or Gemalto. Contact Safelayer to find out which models are homologated.

(*) KeyOne XRA 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, 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