KeyOne

Autoridad de Registro

Descripción

Componente de la solución de KeyOne para Infraestructuras de Clave Pública (PKI) que aporta las funciones de una Autoridad de Registro (RA). KeyOne XRA está diseñado para:

- Aportar un sistema de registro de usuarios y gestionar el ciclo de vida de sus certificados digitales interactuando con KeyOne CA.
- Gestionar todo el ciclo de vida de los certificados para servicios y aplicaciones de la PKI que requieren autenticación, firma y/o cifrado de datos.
- Soportar la gestión de certificados digitales de un conjunto amplio de dispositivos y plataformas de usuario.
- Soportar un conjunto completo de mecanismos de registro, tanto presenciales como remotos, simplificando el despliegue de la PKI.
- Permitir la integración del sistema de registro en los procesos corporativos mediante interfaces estándares REST/JSON y SOAP/XML.

Beneficios

Entornos de usuario y movilidad

La gestión de los usuarios que aporta KeyOne XRA es independiente de su entorno, habilitando el despliegue de mecanismos de autenticación PKI, firma electrónica y/o cifrado de para un amplio conjunto de aplicaciones y plataformas compatibles con PKI: soporta entornos de escritorio Windows, Mac y Linux, así como los dispositivos móviles con sistemas operativos Google Android y Apple iOS.

Certificados para aplicaciones

KeyOne XRA gestiona igualmente aplicaciones que requieran certificados digitales: interactúa con KeyOne CA para provisionar los certificados digitales para diferentes propósitos tales como certificados SSL, SSL EV, VPN y específicos de servicios de la PKI que requieren autenticación, firma electrónica y cifrado de datos basado en certificados digitales X.509.

Flujos de trabajo y registro

KeyOne XRA destaca por su capacidad de adaptación a las necesidades de negocio, tanto en los procesos de registro de usuario como en la entrega de certificados digitales. Su gestor de flujos de trabajo permite configurar el sistema de forma sencilla y fiable para establecer qué acciones de procesado de datos conformarán el proceso de registro y qué datos deberá intercambiar el sistema con usuarios, operadores y aplicaciones.

Integración y ahorro de costes

KeyOne XRA es un producto especialmente adecuado para su integración del registro de la PKI en los procesos corporativos: las funciones del sistema pueden usarse como servicio Web gracias a los interfaces REST o SOAP que incorpora el producto. Asimismo, el sistema de gestión de flujos de trabajo permite determinar de forma sencilla cuáles son las funciones que deben expondrán como servicio web y cuáles serán accesibles desde el propio GUI.

Máxima seguridad y control

KeyOne XRA dispone de los mecanismos de gestión de roles, auditoría y reporting recomendados en los sistemas de gestión de certificados digitales para firma electrónica CEN TS 419 261 (reemplaza a CWA 14167-1). Facilita la adecuación a las recomendaciones de la regulación eIDAS (ETSI EN 319 411-2) y de ETSI TS 101 456 sobre las políticas de autoridades de certificación que emiten certificados digitales reconocidos.

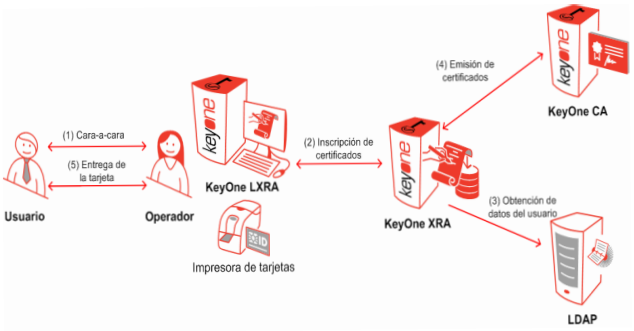
KeyOne

Autoridad de Registro

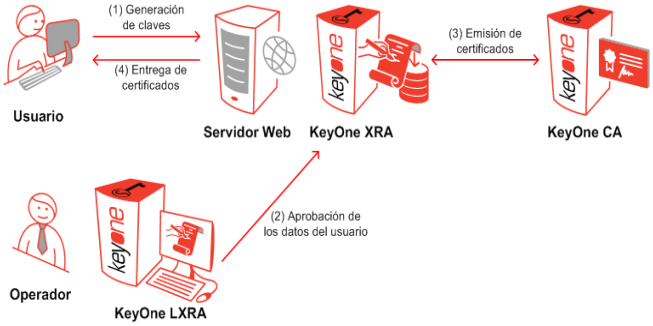
Funcionamiento

KeyOne XRA funciona como servicio de registro de usuarios o aplicaciones (RA) para solicitar la generación o revocación de certificados digitales (en conexión con el producto KeyOne CA). El sistema puede combinar los siguientes procedimientos de registro:

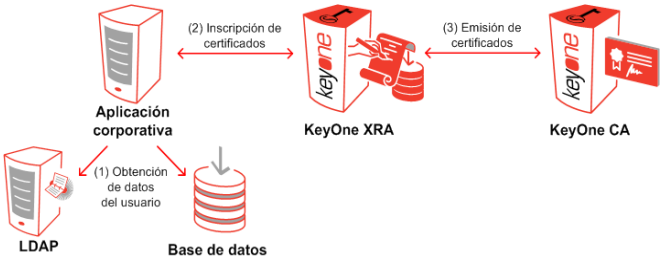
- Procedimiento **cara-a-cara**. El solicitante debe acreditarse de forma presencial para obtener sus certificados digitales. Una vez el operador de registro aprueba la solicitud, el sistema inicia proceso de generación de claves completándose en una tarjeta criptográfica, un dispositivo móvil o en el propio PC del usuario según defina la política de registro. Para desplegar puestos de registro cercanos al solicitante, el operador dispone de la aplicación cliente de KeyOne XRA denominada KeyOne LXRA.



- Procedimiento **remoto**. En un modelo de registro Web, el sistema de registro permite al usuario entregar sus peticiones de certificado remotamente, típicamente desde un navegador web. Los solicitantes pueden disponer de un PC para certificados software o en tarjeta criptográficas, o bien de un dispositivo móvil para certificados y claves destinadas a sistemas operativos móviles. Los certificados para dispositivos y aplicaciones también se solicitan vía web y/o en con protocolos estándar como SCEP o Windows Enrollment. Las solicitudes pueden ser preautorizadas (en este caso, el solicitante debe autenticarse habitualmente mediante una contraseña), o bien, deberán ser aprobadas posteriormente por el operador de registro un vez éste valide los datos del registro proporcionados por el solicitante.



- Procedimiento **automático**. Este procedimiento permite la carga de los datos de los solicitantes de una fuente fiable: base de datos de RRHH, directorio o aportados por una aplicación corporativa que interactúa con KeyOne XRA. La conexión con KeyOne XRA se realiza usando sus interfaces REST/JSON o SOAP/XML para invocar de forma remota las funciones del sistema de registro de aprobación, renovación o revocaciones de certificados digitales, o bien ser la propia RA quien se conecta a la base de datos o directorio corporativo para obtener los datos de los solicitantes.



Características técnicas

- **Formatos de solicitudes de certificación:** PKIX-CRMF, RSA PKCS #10, ITU-T X.509v3 y Firefox.
- **Formatos de entrega de certificados y cadenas de certificación:** RSA PKCS #7, PKCS #12 y ITU-T X.509v3.
- **Protocolos de inscripción de certificados:** REST/JSON, SOAP/XML, SCEP, Windows Enrollment y OTA Enrollment de Apple.
- **Perfiles de certificación:** Todas las extensiones estándar definidas por ITU-T X.509v3, Firefox y Microsoft.
- **Conectividad:** SQL, LDAP/SLDAP, Microsoft Active Directory, HTTP/HTTPS, Servicios web REST y SOAP, POP3 y SMTP
- **Dispositivos criptográficos:** RSA PKCS #11
- **Monitorización de eventos:** SNMP v1, v2c y v3.
- **Auditoría e integración con SIEM:** Syslog o Windows Event Log
- **Certificación:** CC EAL4+. (*)

Requisitos del sistema

- **Sistemas operativos:** Windows o Solaris SPARC
- **Sistemas de base de datos:** Oracle, Microsoft SQL Server, My SQL o Maria DB.
- **HSM opcional:** Fabricantes Thales nCipher o SafeNet. Consultar para modelos homologados.
- **Servidor LDAP:** Recomendado para la publicación de certificados y/o CRL en directorio.
- **Servidor de correo SMTP:** Recomendado para la generación de notificaciones automáticas.
- **Impresoras de tarjetas inteligentes:** Fabricante Datacard. Consultar para modelos homologados.
- **Tarjetas inteligentes:** Fabricantes G&D, SafeNet o Gemalto. Consultar para modelos homologados.

(*) KeyOne RA con un nivel de garantía CC-EAL4+ - ISO/IEC 15408 (ALC_FLR.2) (http://www.oc.ccn.cni.es/) y conforme con el Perfil de Protección CIMC Security Level 3 “Certificate Issuing and Management Component” del NIST.

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