KeyOne
Autoridad de Certificación

Descripción

Componente de la solución KeyOne para Infraestructuras de Clave Pública (PKI) que aporta las funciones de Autoridad de Certificación (CA). KeyOne CA está diseñada para:

- Despliegues de Infraestructuras de Clave Pública gubernamentales, prestadores de servicios de certificación y para entornos corporativos.
- Gestionar certificados digitales de usuario en dispositivos móviles, servidor centralizado o tarjetas inteligentes.
- Proporcionar certificados digitales para servidores, aplicaciones y dispositivos de comunicación que requieran autenticación, firma y cifrado de datos.
- Ofrecer las máximas garantías de seguridad y facilitar la adecuación de la CA a las recomendaciones CEN y ETSI.
- Soportar los estándares de integración incluyendo interfaces REST/JSON y SOAP/XML, simplificando los costes de integración y mantenimiento.

Beneficios

Solución completa y escalable

KeyOne CA está optimizado para la gestión de grandes volúmenes de certificados e incorpora la capacidad de gestión de CRL con múltiples puntos de distribución, apropiadas para infraestructuras gubernamentales y grandes infraestructuras. La solución KeyOne incluye componentes que aportan funciones avanzadas a la PKI, tales como el sistema de registro (KeyOne XRA), la validación de certificados (KeyOne VA) y el sellado de tiempo (KeyOne TSA).

Soporte de estándares y movilidad

KeyOne CA soporta certificados digitales X.509 interoperables para entornos de escritorio Windows, Mac y Linux, así como los sistemas operativos para móviles Google Android y Apple iOS. KeyOne habilita los mecanismos de autenticación PKI, firma electrónica y cifrado de datos sin necesidad del uso de aplicaciones propietarias, adaptándose a los mecanismos de seguridad de un amplio conjunto de aplicación y plataformas compatibles con PKI.

Mayor control y gestión de la PKI

KeyOne gestiona de forma automática las claves de la CA, aportando mayor facilidad de gestión y control de la Infraestructura de Clave Pública (PKI). Es posible definir qué eventos deben ejecutarse para la renovación de claves, incorpora mecanismos para adaptar la vigencia máxima de los certificados digitales y gestiona la coexistencia con las claves antiguas de la CA (usándolas de forma transparente para la revocación de los certificados vigentes generados con dichas claves).

Integración y ahorro de costes de mantenimiento

KeyOne CA opera como un componente se servicio especializado accesible por red. El sistema se puede operar desde su propio GUI y/o usando los interfaces JSON sobre REST ó XML sobre SOAP que aporta, simplificando los costes de integración y mantenimiento de las funciones de gestión de certificados digitales. El sistema soporta protocolos estándares de gestión de la información y eventos de seguridad así como de monitorización, facilitando su integración con los sistemas SIEM y monitorización corporativos.

Máxima seguridad y fiabilidad

KeyOne CA se ha diseñado para facilitar el cumplimiento de las recomendaciones de seguridad para sistemas de gestión de certificados digitales para firmas electrónicas (CEN TS 419 261, reemplaza a CWA 14167-1) en cuanto a roles y eventos. 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. El sistema soporta HSM FIPS 140-2 nivel 3 y está certificado ISO/IEC 15408 EAL4+ (ALC_FLR.2).

KeyOne

Autoridad de Certificación

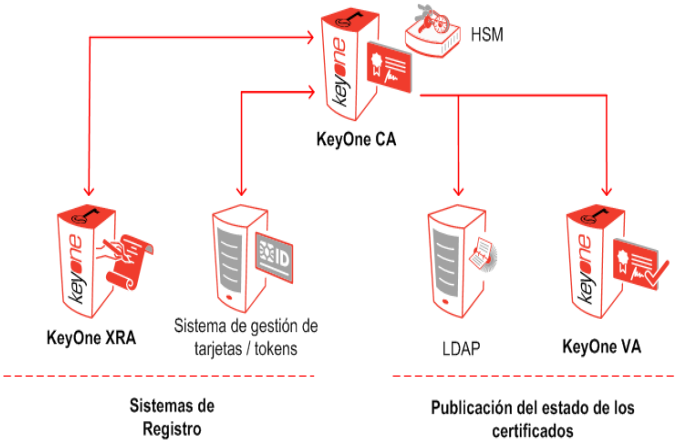
Funcionamiento

KeyOne CA puede funcionar como CA raíz, CA subordinada, CA cruzada o CA puente. En función del tipo de CA operará en conexión con el producto KeyOne XRA de Safelayer o con una aplicación que asume las funciones de registro de usuarios o aplicaciones. Opcionalmente, puede funcionar en conexión con el producto KeyOne VA para el servicio de validación de certificados digitales. Las funciones clave de KeyOne CA son las siguientes:

- Generar y custodiar las claves privadas mediante dispositivos criptográficos (HSM).
- Gestionar de forma automática el ciclo de vida y la coexistencia de las claves privadas de la CA.
- Gestionar las RA reconocidas y asignarles políticas de certificación.
- Generar los certificados digitales ITU-T.X509v3 para usuarios o aplicaciones, solicitados por las RA.
- Generar y publicar las listas de revocación (CRL) que incluyen los certificados revocados o suspendidos.
- Informar del estado de los certificados digitales al servicio de validación (VA) para su publicación mediante OCSP.
- Permitir la custodia y recuperación segura de las claves de cifrado, para supuestos de pérdida.
- Garantizar la auditoría segura de los eventos y acciones sobre el sistema.

Arquitectura

En la siguiente figura se muestra una Autoridad de Certificación (CA) operada por KeyOne CA y su interacción con los diferentes productos KeyOne o de terceros, agrupando diferentes opciones para los servicios de registro y de publicación del estado de certificados soportados. El sistema de registro se puede implementar mediante el producto KeyOne XRA y/o opcionalmente mediante un sistema de gestión de tarjetas / tokens (CMS / TMS) que asume el rol de RA. La publicación del estado de los certificados se podrá realizar mediante CRL y/o OCSP, usando un directorio o un servidor web (no representado en la figura) o el producto KeyOne VA. En la figura, también se ilustra un HSM que se usará para la protección de las claves privadas de la CA, que podrá ser en red o interno.



Características técnicas

- **Formatos de certificados:** ITU-T X.509v3, IETF RFC 5280 y RFC 6818.
- **Perfiles de certificación:** Todas las extensiones estándares definidas por ITU-T X.509v3, ETSI EN 319 412-5 (reemplaza TS 101 862) IETF RFC 5280, RFC 6818 y RFC 3739. Certificado SSL EV según las especificaciones del CA/Browser Forum.
- **Información de revocación:** ITU-T X.509v2 CRL con uno y múltiples puntos de distribución. Protocolo OCSP mediante el componente opcional KeyOne VA.
- **Generación de certificados:** RSA PKCS#10/PKCS#7. PKIX-CMP según RFC 4210. Soporte de Certificate Transparency (IETF RFC 6962) y DNS CAA (IETF RFC 6844).
- **Archivo de claves:** RSA PKCS#8 y PKCS#12 mediante el componente opcional KeyOne Archive.
- **Conectividad:** SQL, LDAP/SLDAP, Microsoft Active Directory, HTTP/HTTPS, Servicios web REST/JSON y SOAP/XML, POP3 y SMTP.
- **Dispositivos criptográficos:** RSA PKCS#11 con esquemas "N de M".
- **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 y SafeNet. Consultar para productos homologados.
- **Servidor LDAP:** Recomendado para la publicación de certificados y/o CRL en directorio.

(*) KeyOne CA 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