KeyOne

Autoridad de Validación

Descripción

KeyOne VA es el sistema adecuado para los procesos críticos de validación de firma electrónica. Frente al mecanismo convencional (basado en listas de revocación) ofrece valor probatorio y mayor eficiencia en la verificación del estado de los certificados digitales. KeyOne VA está diseñado para:

- Ofrecer información fiable sobre el estado de un certificado digital
- Facilitar la integración con los sistemas de información corporativos
- Minimizar los costes de instalación y mantenimiento

Beneficios

Máxima seguridad

Los productos KeyOne disponen de los mecanismos de gestión de roles, auditoría y reporting recomendados para sistemas de gestión de certificados digitales para firma electrónica (CEN TS 419 2161, reemplaza a CWA 14167-1). KeyOne VA admite los roles operador de seguridad, administrador del sistema y auditor del sistema.

Fiabilidad y control

El sistema de eventos garantiza tanto la integridad de los datos del registro como la no pérdida de información. Para ello, dispone de un mecanismo de emergencia que se activa cuando se pierde conectividad con la base de datos. Además, pueden seleccionarse eventos automáticos (a los que asignar diferentes grados de severidad) o definir eventos manuales (para registrar acciones que ocurren fuera de la aplicación).

Eficiencia para grandes infraestructuras

KeyOne VA facilita la gestión de grandes volúmenes de certificados mediante la conexión a la base de datos de KeyOne CA. Al optimizar la actualización del estado de los certificados, dicho servicio garantiza la máxima eficiencia en la respuesta para soportar arquitecturas escalables y en alta disponibilidad.

Facilidad de integración y accounting

KeyOne VA incluye un motor de flujo de trabajo que permite definir interacciones con los sistemas de información. Es posible incorporar nuevas funciones, conectarse a sistemas de control de acceso o acceder a sistemas de información internos (para complementar la información generada por el sistema) de forma rápida y sencilla.

KeyOne

Autoridad de Validación

Funcionamiento

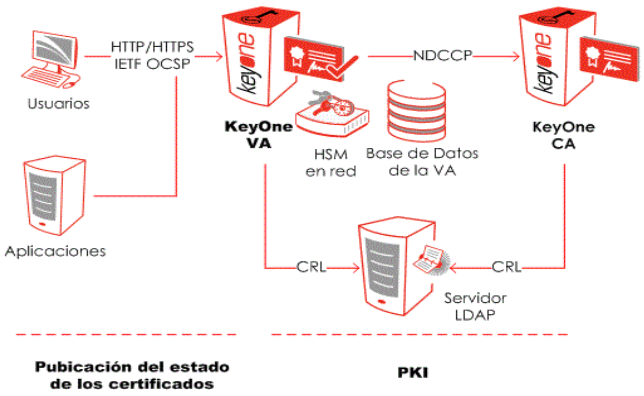
Las principales funciones de KeyOne VA son las siguientes:

- Mantener información sobre el estado de los certificados generados por una o varias Autoridades de Certificación.
- Atender peticiones de usuarios o proveedores de servicio que desean conocer el estado de los certificados digitales utilizados en la firma de transacciones electrónicas.
- Responder a peticiones de información sobre el estado de certificados digitales utilizados en la firma de transacciones electrónicas. Dichas peticiones pueden provenir tanto de usuarios como de proveedores de servicios.
- Responder a peticiones de información sobre el estado de certificados digitales utilizados cuando un servidor web protege la comunicación mediante SSL/TLS. Dichas peticiones pueden provenir tanto del navegador web del usuario como del propio servidor web si utiliza OCSP Stapling.
- Garantizar el no repudio de la respuesta. Dicha respuesta, firmada digitalmente por la Autoridad de Validación, indica tanto la fecha como el estado del certificado (válido, revocado, suspendido, desconocido).
- Si es necesario reencaminar las peticiones a un OCSP Responder que puedan proporcionar respuesta autoritativa para determinados certificados.
- Registrar eventos que permitan a los operadores auditar periódicamente el estado del sistema, su seguridad y el cumplimiento de las especificaciones corporativas.
- Opcionalmente, contabilizar y limitar el uso del servicio OCSP por parte de cada cliente, asignando una cuota de uso del servicio o restringiendo a un periodo de tiempo concreto (p.e. billing).

Arquitectura

La siguiente figura muestra la arquitectura general de KeyOne VA y su interrelación con los componentes de red (aplicaciones o usuarios) mediante el estándar OCSP de IETF. KeyOne VA puede operar con un HSM (en red o interno) y requiere acceso tanto a una base de datos como a una fuente de tiempo en red (no representada en la figura).

Según la configuración del sistema de actualización de estado de certificados, KeyOne VA se conectará de forma periódica a la base de datos de certificados de KeyOne CA o descargará las CRL de un directorio LDAP o de un servidor Web . Si se conecta a KeyOne CA, KeyOne VA puede obtener información sobre el estado de los certificados así como información de Certificate Transparency.



Características técnicas

- **Protocolo de validación en línea:** OCSP según IETF RFC 2560 y RFC 6960. Soporte de OCSP Stapling (IETF RFC 6066 y RFC 6961).
- **Dispositivos criptográficos:** RSA PKCS #11.
- **Conectividad:** SQL, LDAP/SLDAP, Microsoft Active Directory, HTTP/HTTPS, Servicios web REST y SOAP, POP3 y SMTP.
- **Mecanismo de actualización:** ITU-T X509v2 CRL, consultas a KeyOne CA y/o OCSP Responder externo. Soporta múltiples CA.
- **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.
- **Servidor de correo SMTP:** Recomendado para la implantación de personalizaciones específicas de notificación de eventos.
- **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.
- **Fuente de tiempo:** Sincronización del tiempo del sistema operativo mediante fuente externa.

(*) KeyOne VA 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