KeyOne

Autoridad de sellado de tiempo

Descripción

La incorporación de la hora electrónica es la única forma de asegurar el momento en que se ha producido una transacción o se ha firmado un documento electrónico. KeyOne TSA, el servicio seguro de sellado de tiempo de Safelayer, está diseñado para:

- Garantizar de forma objetiva y precisa el momento en el que se ha producido una transacción.
- Proteger de forma segura los registros de sellado de tiempo.
- Facilitar la conexión segura con los sistemas de control corporativos, minimizando así los costes de instalación y mantenimiento.

Beneficios

Máxima seguridad

KeyOne TSA cumple con los estándares ETSI EN 319 421 “Protection Profile for trustworthy systems supporting time stamping” (reemplaza TS 102 023) y ETSI TS 319 422 “Time-stamping protocol and time-stamp profiles” (reemplaza TS 119 422 y TS 101 861) que definen los requisitos para los sellos de tiempo cualificados en la regulación eIDAS.

Los productos KeyOne disponen de los mecanismos de gestión de roles, auditoría y reporting recomendados para los sistemas de gestión de certificados digitales para firma electrónica (CEN TS 419 211, reemplaza a CWA 14167-1). KeyOne TSA admite los roles operador de seguridad, administrador del sistema y auditor del sistema.

Fiabilidad y Control

La fiabilidad del sistema de registro de una TSA (Time Stamping Authority) es clave para garantizar la trazabilidad de los sellos de tiempo emitidos y auditar su correcta operación. El mecanismo de registro de KeyOne incorpora tanto un sistema de protección de datos como un sistema de emergencia que evita la pérdida de logs. Además, permite seleccionar eventos automáticos (con asignación de diferentes grados de severidad) y definir eventos manuales (para registrar acciones que ocurren fuera de la aplicación).

Máximo rendimiento y escalabilidad

KeyOne TSA puede conectarse con aceleradores criptográficos para adaptarse a los más altos requisitos de carga, integrarse en arquitecturas de alta disponibilidad y garantizar la máxima rapidez de respuesta transaccional.

Facilidad de integración y accounting

KeyOne TSA 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

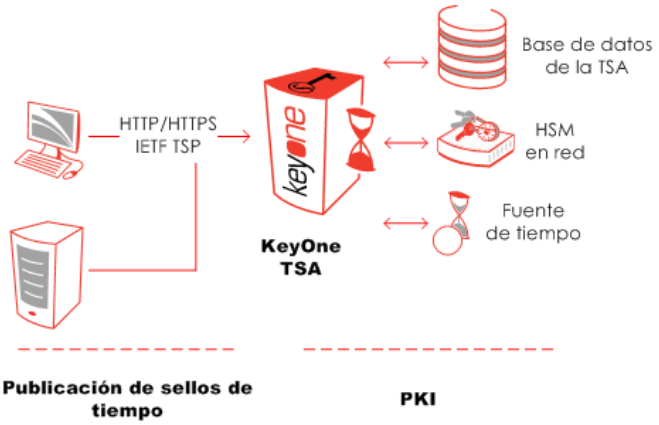
Autoridad de sellado de tiempo

Funcionamiento

- Recibir a través de Internet peticiones de sellado de tiempo (procedentes de usuarios o proveedores de servicios) que soliciten incorporar un sello de tiempo a documentos o transacciones electrónicas.
- Generar un sello de tiempo firmado electrónicamente que incluya lo siguiente: hora de solicitud, información que vincule de forma segura el sello con el documento electrónico sellado, número de registro único para posteriores auditorías.
- Generar logs de auditoría para que los operadores realicen seguimientos periódicos sobre el estado del sistema, su seguridad y el cumplimiento de las especificaciones corporativas.
- Opcionalmente, contabilizar y limitar el uso del servicio de sellado de tiempo 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 TSA y su interrelación con los componentes de red (mediante el protocolo de sellado de tiempo de IETF). KeyOne TSA 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 (accesible por ejemplo mediante NTP).



Características técnicas

- **Protocolos de sello de tiempo:** IETF RFC 3161 y RFC 5816.
- **Perfiles de sellado y políticas:** ETSI TS 102 023 y ETSI TS 101 861.
- **Dispositivos criptográficos:** RSA PKCS #11.
- **Conectividad:** SQL, LDAP/SLDAP, Microsoft Active Directory, HTTP/HTTPS, Servicios web REST y SOAP, POP3 y SMTP.
- **Monitorización de eventos:** SNMP v1, v2c y v3.
- **Auditoría e integración con SIEM:** Syslog o Windows Event Log.

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 bases de datos:** Oracle, Microsoft SQL Server, My SQL, 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.

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