TrustedX

Tarjeta Virtual

Descripción

Módulo de TrustedX para la gestión centralizada de claves y certificados:

- Las claves de los usuarios se custodian en un repositorio centralizado, que actúa de tarjeta virtual.
- El usuario únicamente precisa de un plug-in estándar que se integra en sus aplicaciones habituales (Explorer, Chrome, Acrobat, Office, etc..).
- Los certificados se pueden usar tanto para firma como cifrado (correo seguro con Outlook).
- Las claves se pueden compartir entre varios usuarios corporativos (i.e. certificados de persona jurídica).
- Aporta un sistema centralizado de auditoría y reporting.

Beneficios

Gestión centralizada y control

- Evita la necesidad de repositorios locales de claves y certificados, centralizando la custodia en un repositorio seguro y auditado.
- Control de acceso basado en políticas y roles. Cualquier uso de las claves quedará registrado.
- Varios usuarios pueden compartir un mismo certificado, quedando registrado qué usuario ha usado la clave en todo momento.

Orientación al usuario

- La complejidad de la firma/PKI queda enmascarada y el usuario sólo debe tratar con una contraseña.
- El usuario podrá disponer de uno o más certificados, o bien usar certificados compartidos.
- La experiencia de usuario es uniforme, perfectamente integrada en el escritorio e independientemente del puesto de trabajo.

Solución de fácil despliegue

- Los usuarios no deben provisionarse de nuevo, se puede usar el repositorio corporativo (LDAP/AD, etc.).
- No se tienen que desplegar tarjetas ni lectores. Los usuarios pueden utilizar su credencial corporativa para activar su tarjeta virtual.
- Al integrarse en el escritorio de forma estándar, los usuarios pueden utilizar sus certificados desde sus aplicaciones habituales.

Ahorro de costes

- Se disfruta de las ventajas de la PKI sin el coste de despliegue y gestión de tarjetas físicas o repositorios locales.
- Se eliminan los costes de administración de repositorios de claves y certificados distribuidos/duplicados en diferentes puestos de usuario.
- Se ahorran los posibles costes de pérdida de tarjetas y/o posible uso fraudulento sin detectar.

TrustedX

Tarjeta Virtual

Funcionamiento

La Tarjeta Virtual incluye un plug-in Microsoft CAPI y/o PKCS#11 que permite al usuario utilizar de forma remota las claves y certificados PKI custodiadas en TrustedX desde sus aplicaciones de escritorio y ofimática.

La Tarjeta Virtual también permite acometer los procesos de enrollment y renovación de las claves y los certificados por parte del propio usuario o de forma integrada con Microsoft Autoenrollment.

Uso basado en Políticas/Roles:

- Con una única credencial, los usuarios pueden acceder a una o varias Tarjetas Virtuales, dependiendo de la Política/Rol «autorizado» con el que puedan actuar.
- Una Tarjeta Virtual bajo una Política/Rol puede tener asociados múltiples usuarios autorizados. Por ejemplo, varios usuarios autorizados pueden usar un certificado de persona jurídica.

Movilidad y control de acceso:

- Al estar centralizada, la Tarjeta Virtual puede usarse desde cualquier puesto de trabajo activándola con una contraseña estática o de un solo uso (OTP) dependiendo de la Política/Rol.
- Sistema basado en políticas de autorización, incluyendo controles adicionales de acceso: dirección IP, franja horaria, fortaleza de la autenticación, etc.

Integración estándar

- Gracias al uso de plug-ins estándares Microsoft CAPI y PKCS #11 es compatible con los navegadores más populares, Microsoft Office y herramientas de desarrollo Java/.NET habituales.

Aprovisionamiento

- Los usuarios de la Tarjeta Virtual pueden existir previamente en repositorios corporativos LDAP/AD, o pueden crearse de forma independiente.
- El registro de la Tarjeta Virtual puede hacerse por el propio usuario, usando una página web de la CA.
- En entornos corporativos basados en Microsoft Windows es compatible con los servicios de Autoenrollment.

Seguridad y confianza

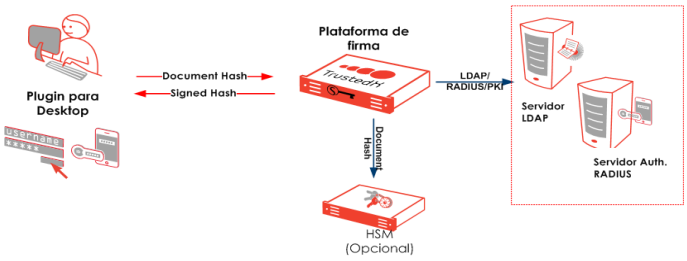
- El sistema permite, por Política/Rol, aumentar la seguridad de acceso a tarjetas virtuales: un password diferente al de sistema, obligar a un password robusto y/o passwords de un solo uso (OTP).
- El sistema centralizado con un HSM FIPS 140-2 Nivel 3 aporta mayor seguridad y protección a las claves.

Escalabilidad de la solución

- El módulo Tarjeta Virtual forma parte de la solución de TrustedX. En el siguiente diagrama se marca el módulo en relación a otros módulos de TrustedX.

Arquitectura

La siguiente figura muestra la extensión de Tarjeta Virtual dentro de la solución completa de TrustedX. El HSM que aparece en la figura es opcional.



Características técnicas

- **Formato:** Software appliance. Contact for more information about supported hardware or virtual machines.
- **Integración en aplicaciones de escritorio:** Compatible con Microsoft CAPI y/o PKCS #11 para entornos Windows.
- **Acceso a servicios de autenticación:** Autenticación basada en LDAP/AD y TMS compatibles con protocolo RADIUS.
- **Monitorización de eventos:** Simple Network Management Protocol (SNMP).
- **Acceso a base de datos y directorios:** Oracle, Microsoft SQL Server o MySQL. Protocolo de acceso a directorio LDAP.
- **Soporte de HSM:** Dispositivos PKCS #11 homologados por Safelayer.

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