CertiSur

Alison

Server

Alison Server es la solución para aquellas organizaciones que desean que sus usuarios hagan uso de certificados digitales para firmar sus documentos pero no desean o no tienen la capacidad de distribuir los mismos en cada una de las estaciones de trabajo.

Para aplicaciones 100% basadas en web, el uso de certificados instalados en las estaciones de los usuarios se ha convertido en un inconveniente que puede ser solucionado de esta manera sin sacrificar funcionalidad por parte de la integración.

Alison Server se comporta como un repositorio de certificados centralizados que pueden ser accedidos por medio de la librería Alison-SDK. Esta librería permite al usuario seleccionar el certificado apropiado e ingresar el challenge asociado (contraseña o código OTP) que garantiza que el usuario es el legítimo ticular del certificado.

Durante el proceso de emisión del certificado el usuario debe seleccionar el mecanismo de challenge deseado entre aquellos que hayan sido habilitados para su usuario. Entre los mecanismos disponibles se pueden mencionar:

- Contraseña: el usuario crea e ingresa una contraseña que debe cumplir con los criterios de fortaleza adecuados,
- Contraseña de único uso (OTP): utilizado Google Authenticator desde su dispositivo móvil el usuario genera una clave de único uso para cada una de las operaciones.

Otros mecanismos de acceso, tales como claves OTP por SMS o correo electrónico, o mensajes PUSH sobre el dispositivo móvil del titular del certificado se irán incorporados en el modelo en futuras versiones.

Alison Server genera firmas en los diversos formatos más utilizados tales como CAdES, XAdES, XML-DSign, PAdES.

Arquitectura

Alison Server se encuentra desarrollado en Java de manera modular y hace uso de varios componentes para lograr integrar una solución robusta y segura.

Su interfaz, desarrollada como servicios sobre un protocolo HTTP, recibe peticiones invocadas desde la librería Alison SDK. Cuenta con un motor Jetty, que permite desplegar varios hilos de ejecución para lograr un alta performance.

Cada una de las peticiones es mantenida en una sesión independiente tal como se encuentra descripto en la librería adjunta.

Dos componentes acompañan la solución y aportan seguridad a las claves de los usuarios:

- Challenge Server

  Este servicio, incluido en la distribución, es el encargado de mantener la relación entre usuarios y certificados, utilizando el challenge definido para poder acceder a cada uno de los certificados de un titular.

- HSM

  Las claves privadas de los usuarios y otros datos sensibles (tales como claves simétricas de cifrado) son resguardadas en el HSM que acompaña a la solución.

Cuando la cantidad de claves estimadas para los usuarios excede la cantidad de objetos que el HSM puede administrar nativamente, un árbol de directorio de claves cifradas es utilizado como repositorio seguro de almacenamiento.

Estas claves solamente son accesibles una vez que son retornadas al HSM para su uso[1].

[1] Ver detalles sobre almacenamiento, warp y unwrap de claves en HSM.

Challenge Server

Este componente es la puerta de entrada para cualquier tipo de operación que desee ser hecha sobre la clave del certificado de un usuario.

Un Challenge representa un desafío que se debe cumplir antes que sea permitida una operación y puede ser de alguno de los siguientes tipos:

- Contraseña
  Una contraseña ingresada por el usuario al momento de solicitar su certificado
- OTP
  Una clave de único uso, generada por Google Authenticator instalada en el dispositivo móvil, debe ser ingresada por el usuario cada vez que su clave requiere ser utilizada para firmar.

En ocasiones es posible que el acceso al certificado pueda ser utilizado sin contraseña alguna. Esta condición es soportada por el componente, aunque representa un riesgo de seguridad para el usuario. En este caso el acceso a Alison Server solamente debe res realizada desde un sistema (tal como Alison S3bp) que garantice un mecanismo de autenticación previo.

El challenge solicitado no puede ser reemplazado por otro distinto de menor nivel porque el mismo es el definido por el emisor del certificado. De esta manera se garantiza que el nivel de seguridad se conversa desde el origen de emisión del certificado y que ningún tercero puede degradar esta condición.

HSM

Alison Server hace uso de un HSM, externo a la solución, para proteger cada una de las claves privadas de los titulares de certificados.

Existen diversos tipos de HSM, algunos de ellos como tarjetas PCI instalables en el equipo y otros como dispositivos de red, pero cada uno de ellos cuanta con una interfaz PKCS#11 para el acceso homogéneo de claves.

Otra condición importante de los HSM es el manejo de objetos concurrentes internos que puede administrar. Algunos de ellos (tal como Utimaco), cuentan con una arquitectura y capacidad ilimitada de manejo de claves ya que las mismas pueden ser almacenadas de manera externa y solo pueden ser utilizadas a través del acceso al HSM.

Por otro lado, otras marcas de HSM (tal como Gemalto LUNA), cuentan con una cantidad limitadas de objetos internos, pero con mecanismos de alta disponibilidad y redundancia nativa definible en la granja de HSM pertenecientes

a la solución. En este caso es necesario hacer uso del mecanismo de exportación e importación de claves de manera dinámica (mecanismo de wrap/unwrap nativo dentro del dispositivo) para poder extender la cantidad de claves utilizables más allá de la limitación interna del HSM.

Aunque es conveniente el primero de los mecanismos, Alison Server también puede hacer uso del mecanismo de Wrap/Unwarp de claves desde y hacia el HSM para extender el volumen de usuarios[2].

Integración y uso

La integración de las capacidades de firma y autenticación debe ser hecha por medio de llamadas a las funciones definidas en el SDK.

El archivo de configuración de la librería permite acceder a los certificados almacenados en Alison Server utilizando la clave de identificación única definida durante el proceso de emisión del mismo. Habitualmente es utilizado el correo electrónico del titular del certificado como clave única ya que la misma puede ser rescatada también de otros sistemas de autenticación (tal como servicios LDAP de la propia organización o proveedores de identidad tal como Google o Facebook) de una manera sencilla y homogénea.

Una vez que el certificado es seleccionado para su uso y dependiendo del tipo de challenge que lo protege, el usuario debe completar los datos necesarios para hacer uso del mismo.

La interfaz del usuario es la misma que cuando hace uso de los certificados instalados en su propio equipo y accedidos por medio de Alison Desktop, lo cual facilita la integración con otros sistemas y tipos de certificados.

Configuración y distribución

Con el objetivo de lograr una solución robusta y segura, Alison Server es distribuido como un virtual appliance con todos los elementos preconfigurados y un equipo cerrado a servicios externos.

[2] Es necesario considerar las condiciones de la política de seguridad definida en el HSM y sus funcionalidades para determinar si la capacidad de exporta e importación claves privadas con un mecanismo de wrap/unwrap se encuentran disponibles entre sus funciones. En caso contrario, un mecanismo equivalente de protección es utilizado para derivar la contraseña de cifrado de la clave privada del usuario.

Solamente accesible por medio del servicio de publicación del servicio que puede ser consumido por la librería Alison SDK, y un puerto de administración para su consola de comandos. Desde dicha consola es posible completar la configuración necesaria y solicitar los elementos adicionales, tales como la solicitud del certificado SSL para ser instalado.

Para un correcto funcionamiento es necesario contar con algunos servicios que el servidor requiere tales como: servicio de DNS y servicio de NTP. En el caso que otros servicios deban ser configurados, tales como el acceso a la Autoridad Certificante para la descarar de CRL, o la Autoridad de Timestamp, la instalación debe considerar que estos servicios deben ser accesibles desde el mismo.

Ventajas y Beneficios

- Alison Server es un componente fundamentar en la suite de componentes de Alison. Se encuentra integrado en el proceso de emisión de certificados como un dispositivo más seleccionable por el usuario.
- La integración para su uso debe ser realizada por medio de la librería Alison SDK o respetando los servicios provistos por su interfaz sobre protocolo HTTP/HTTPS.
- Un módulo independiente de manera de Challenge por parte del usuario controla el acceso a los certificados del usuario. Este mecanismo de challenge a utilizar puede ser fijado por el emisor del certificado para garantizar que el usuario conserve el control de su clave privada respetando la política definida por la Autoridad Certificante.
- La protección de cada clave privada se encuentra garantizada por el HSM correspondiente asociado a la solución. El mecanismo de protección de la clave dependerá de las características del HSM en función de la política de seguridad que tenga definida.