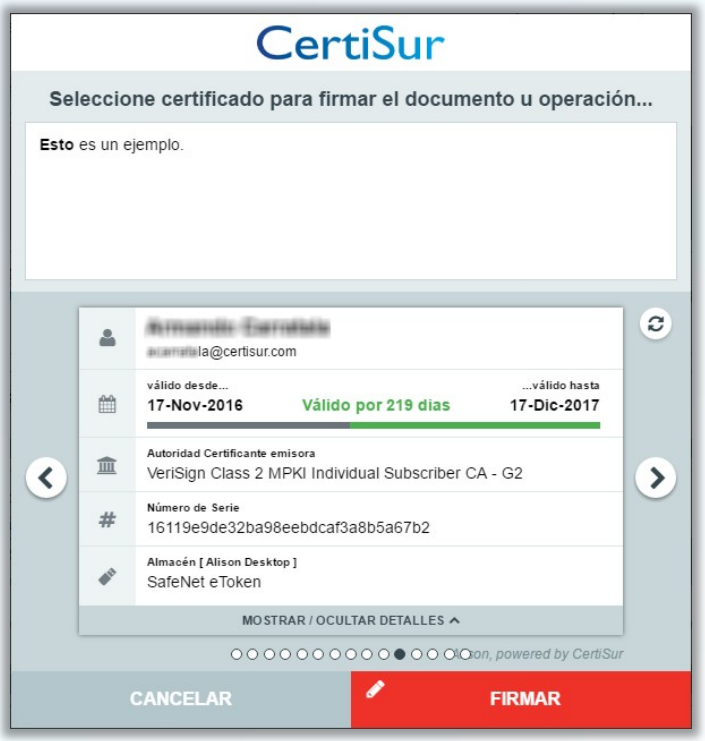
CertiSur

Alison

Desktop

Alison Desktop es la solución que facilita la integración de funcionalidades de firma digital y autenticación segura para todos aquellos usuarios de navegadores (Internet Explorer, Firefox, Chrome, Opera, Safari) que tienen instalados sus certificados en diversos repositorios seguros (Microsoft CSP, Firefox NSS, Dispositivos PKCS#11, Smartcards, eTokens) y sobre diversas plataformas (Windows, Mac OS, Linux).



Esta solución ha sido diseñada para ofrecer a los usuarios una interfaz homogénea en todos los navegadores y minimizar los cambios necesarios para la integración de las soluciones de firma y autenticación.

Alison Desktop cuenta con un asistente de instalación (Alison Wizard) de sus componentes que permite guiar al usuario dependiendo del tipo de navegador. Asimismo, detecta las condiciones mínimas bajo las cuales la misma se debe realizar y sugiere los pasos correctivos necesarios. Permite que el usuario pueda verificar si un certificado se encuentra correctamente instalado.

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

Arquitectura

Alison cuenta con una arquitectura modular que permite reutilizar los componente ya instalados en las estaciones de los usuarios y utilizar la misma librería de desarrollo (100% javascript) para todas las plataformas.

Entre los componentes principales de la solución podemos mencionar:

- *Alison Desktop*: la aplicación es ejecutada en la estación del usuario, no requiriendo permisos de administrador para su instalación.
  Todos los certificados instalados en el equipo pueden ser accedidos por el usuario a los fines de realizar la firma de un documento o frase, sin importar el dispositivo criptográfico o repositorio en donde se encuentre almacenada su clave privada.
  Cada operación de firma es controlada por el usuario solicitando el acceso al dispositivo.

  La solución es multiplataforma y se puede ejecutar en plataformas Windows, MacOS y Linux.

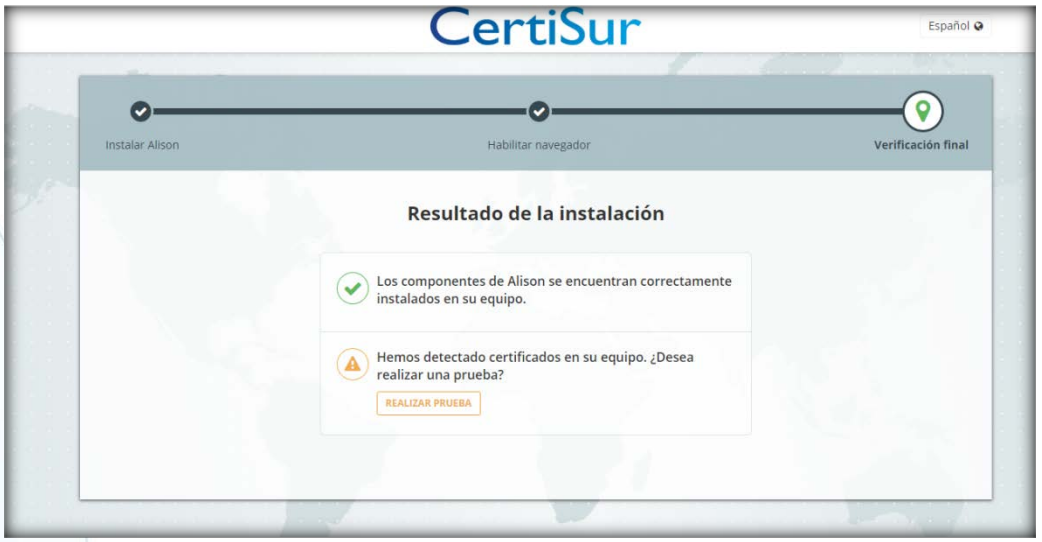
  Soporta repositorios de certificados estándar de cada plataforma tales como Windows CAPI (y cualquier dispositivo que cuente con integración con Windows), MacOS Keychain y Mozilla Firefox.

  Alternativamente, también cuenta con un repositorio propio (CSK) que permite asociar el certificado a varios elementos de hardware del equipo, lo que garantiza que el mismo no pueda ser exportado y utilizado indebidamente en otro equipo.

- *Alison Wizard*: para facilitar el despliegue de la solución en las estaciones de los usuarios, un asistente web permite determinar si los componentes

se encuentran correctamente instalados y sugerir su instalación o actualización. Entre las tareas que se realizan podemos citar:

- Llevar adelante la descarga de los componentes mediante asistentes propios,
- Verificar la correcta instalación de los mismos,
- Validar su correcto funcionamiento y la firma de una transacción de prueba (si el usuario cuenta con un certificado)



- *Alison SDK*: los programadores hacen uso de un SDK, 100% Javascript, que permite acceder a las funciones de firma y autenticación de la solución. Cada una de las funciones cuenta con parámetros que permiten definir el comportamiento de la solución, como por ejemplo, permitir firmas múltiples con una única intervención del usuario o que la misma haga uso de su interfaz web para la selección de los certificados a utilizar.

  Estas librerías también son utilizadas para solicitar la generación e instalación de certificados en algunas plataformas específicas.

- *Alison Extensions*: este componente opcional puede ser instalado sobre algunos navegadores (Firefox, Chrome, Internet Explorer) para permitir una comunicación de manera indirecta entre el navegador y Alison Desktop.

Integración y uso

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

Un archivo de configuración permite definir todo el comportamiento de la librería para sus distintas funciones, tales como: seleccionar certificados, verificar un certificado, autenticarse, firmar una transacción, firmar un archivo, etc. De esta manera es fácil realizar cambios en el funcionamiento de la aplicación. Estos cambios se realizan por medio de su configuración solamente, sin tener que afectar los desarrollos ya realizados.

Los certificados instalados pueden ser filtrados según diversos criterios tales como: autoridad certificante emisora, fecha de vencimiento, titular del certificado, número de serie, etc. Al momento de firmar o autenticarse, el usuario debe seleccionar el certificado que desea utilizar. Los datos disponibles en pantalla le permiten distinguir entre todos los certificados disponibles.

Si un certificado se encuentra próximo a expirar, el usuario es alertado para que pueda tomar la acción de renovación correspondiente.

En ocasiones, si el usuario debe firmar múltiples documentos, es posible instruir al módulo Alison Desktop para que solicite solamente una vez la confirmación de la operación, mejorando de esta forma la experiencia del mismo.

El resultado de la operación de firmar, dependiendo del formato y tipo de documento, es enviado hacia el servidor para determinar la validez de la firma y su posterior almacenamiento.

Ventajas y Beneficios

- Alison Desktop integra una visión uniforme de todos los certificados con los que cuenta el usuario en su equipo permitiendo que los mismos puedan ser utilizados por Alison SDK desde cualquier navegador.
- La solución es multiplataforma y puede operar en ambientes Windows, MacOS y Linux. Su distribución, instalación y diagnóstico es realizada por un asistente (Alison Wizard) que permite al usuario instalar cada uno de los componentes y habilitarlo en el navegador apropiadamente.
- Alison Desktop controla el uso de los certificados y notifica al usuario cuando alguna aplicación se ha comunicado para solicitar una firma. El usuario puede configurar ésta y otras características de la aplicación instalada.
- Alison Desktop facilita la instalación de nuevos certificados ya que se encuentra totalmente integrado con el portal de administración CoLT.
- Para ambientes donde el certificado deba ser utilizado de manera segura solamente en ambientes web es posible hacer uso de su repositorio seguro de claves. En este repositorio se define una

política de seguridad que controla, entre otras características, la cantidad de intentos de uso de clave, el tipo de clave, si la misma puede ser exportada, etc.

- Este repositorio de certificados se encuentra vinculado de manera segura a diversos elementos de hardware del equipo del usuario, garantizando de esta forma que el mismo no pueda ser utilizado en otro equipo de manera indebida y sin el control del usuario.