CertiSur

Debbie

Validation Module

Debbie es una herramienta que facilita la validación de firmas digitales sobre distintos tipos de documentos por medio de una interfaz web sencilla y fácil de integrar en aplicaciones.

Ya sea accediendo por protocolo HTTP o HTTPS, el resultado en formato JSON puede ser fácilmente interpretado por cualquier tipo de lenguaje.

Debbie esa aplicación independiente que puede ser ejecutada como un servicio en diversas plataformas tales como Windows o Linux. Se encuentra desarrollada en Java y cuenta con un servidor Jetty embebido, lo que lo hace un módulo independiente de alta performance que puede ser desplegado en cualquier equipo de una manera sencilla y sin requerimientos adicionales tales como Applications Servers.

La distribución también viene integrada con su propia Java Runtime Enviroment para aportarle mayor independencia del equipo donde se instale. El motivo de esta solución es lograr la mayor estabilidad para un módulo que habitualmente trabaja de manera desatendida pero es altamente crítica para otros sistemas.

Debbie puede validar distintos tipos de firmas (CAdES, PAdES) asi como solamente certificados. También pueden definirse diversas políticas de validación donde en cada una de ellas condiciones exigidas pueden ser distintas tal como se describe más adelante.

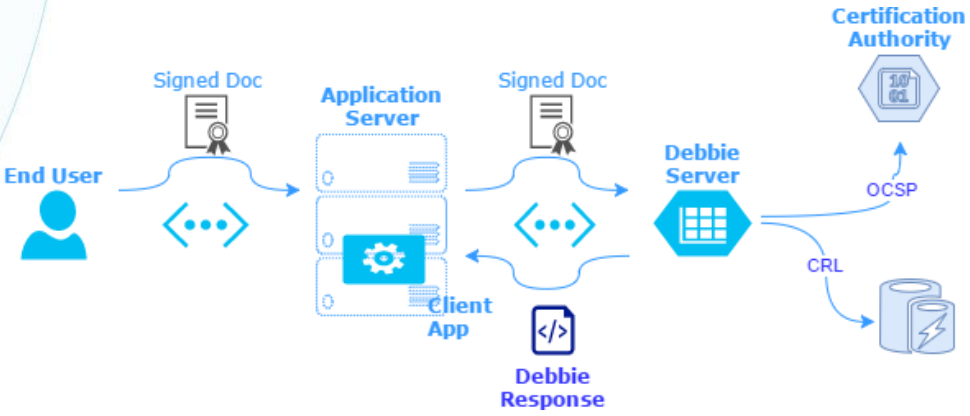
El servicio una vez instalado es iniciado y detenido siguiendo las comunicaciones propias de cada sistema operativo. Las funciones de start, stop y restart con las propias de cada tipo de servicio.

Flujo de datos para validar firma

Cada validación de una firma o un certificado es iniciada por medio de una petición POST en el protocolo HTTP/HTTPS. El resultado de la validación es un objeto JSON que el software que haya hecho la petición debe interpretar para determinar el resultado de la validación.

El siguiente flujo de datos se produce al validar una firma:

1. Un usuario o una aplicación ha generado la firma de un documento o de un texto. Esto pudo ocurrir en un navegador tal tanto como un servidor. Esta condición es previa a cualquier petición a Debbie y la firma puede ser realizada por cualquier herramienta de firma tal como Alison Desktop.
   La aplicación que recibe los datos de firma (texto o documento firmado) desea realizar la validación de la firma y envía los datos necesarios para realizar esta tarea a Debbie.
   Cada política de validación se encuentra definida con una URL propia dentro del servidor.
2. En proceso se debe comunicar con el servidor y puerto donde Debbie se encuentra instalado utilizando una llamada POST del protocolo HTTP/HTTPS.



Dependiendo del tipo de política de validación definida en Debbie el proceso de comunica con las Autoridades Certificantes emisoras del certificado para determinar su validez. Una consulta OCSP y la descarga de la última CRL emitida se producirá durante esta etapa. En el caso que no pueda cumplirse con alguno de estos requisitos, y si así está indicado

en la política de validación, el resultado es reflejado en la respuesta JSON que recibe el proceso que invocó el servicio.

3. La respuesta de Debbie es una estructura JSON con información sobre la validez de la firma, de los firmantes, y del cumplimiento de la política definida, tal como se muestra más adelante.
4. La aplicación cliente puede devolver la información necesaria al usuario final en función del tipo de resultado obtenido. En función de la respuesta, el proceso debe seguir su flujo de datos definidos.

Política de Validación

Debbie permite la configuración de diversas políticas de validación de manera independiente.

En cada una de ellas es posible definir, entre otros elementos:

- Listado de Autoridades Certificantes confiables para la política
- Listado de los repositorios de CRL o servicios OCSP que ofrecen cada una de dichas Autoridades Certificantes
- Frecuenta de actualización de CRL
- Filtro sobre el certificado del firmante (esto es importante cuando se desea restringir qué certificados deben ser considerados válidos cuando una Autoridad Certificante emite a comunidades heterogéneas).

El valor más importante en la política de validación es aquél que permite definir el nivel de validación que se desea aplicar. Este valor es representado por un rango que va desde 0 hasta 4 tal como se detalla en la siguiente tabla:

Valor		Descripción
0	NONE	No se valida el status del certificado del firmante. Solo se valida si el mismo se encuentra expirado.
1	TRUSTED	El certificado tiene que estar emitido por una de las Autoridades certificantes definidas en los Anchors. No se valida si el certificado es válido o no.
2	CRL	Se valida el firmante vía CRL[1]
3	OCSP_CRL	Se valida el firmante vía OSCP, si no responde se valida por CRL[2]. Si se encuentra activa esta opción, y alguno de los certificados es validado por medio de CRL, entonces el resultado final de la

[1] Utilizar este valor solamente si todas las validaciones se realizan solamente por CRL (no por OCSP). En el caso que la validación de un certificado haya sido realizada por OCSP, entonces se presentará como un error.

[2] Utilizar este valor cuando no se desea validar por OCSP y/o CRL indistintamente.

		validación será WARNING.
4	OCSP	Se valida el firmante vía OSCP. Si se encuentra activa esta opción, y alguno de los certificados no puede ser validado por OCSP, entonces el resultado final de la validación será ERROR.

Respuesta Debbie

La respuesta es una estructura JSON con el resultado de la validación de cada uno de los elementos de manera independiente, y un resultado final con la aplicación de cada uno de estos elementos contra el nivel de validación definido en la política de validación.

De esta manera el programador puede obtener el resultado de cada uno de los elementos, con sus datos desplegados para que puedan ser utilizados, pero al mismo tiempo no requiere hacer una validación de cuándo debe considerar si la firma es válida.

El criterio de validación se mantiene definido de manera centralizada evitando errores de interpretación por parte de los programadores, y con la posibilidad de ampliar o restringir dicha política de una manera sencilla y controlada.

La respuesta Debbie contiene información de valides de la firma (es decir, si la misma corresponde al texto firmado), así como el status del certificado de cada uno de los firmantes.

Una estructura WebCertificate acompaña el resultado de cada certificado validado.

Plataformas y requerimientos

Sistemas operativos soportados

- Windows Server 2012 (32-bit, 64-bit)
- Windows Server 2012 R2 (32-bit, 64-bit)
- Ubuntu Server 12 o superior (32-bit, 64-bit)
- Red Hat Enterprise 7 o superior (32-bit, 64-bit)
- CentOS 7 / 6 (32-bit, 64-bit)

Procesador: 2 cores (recomendado), 1 core (mínimo)

Memoria: 4GB (recomendado), 2GB (mínimo)

Disco rígido: 20GB (recomendado), 10GB (mínimo)

Conectividad

Para realizar la validación del status de los certificados de los firmantes, y dependiendo de los elementos y políticas que se configuren, Debbie requiere contar con el acceso a los servicios de las Autoridades Certificantes emisoras de los certificados del firmante.

Estos servicios son habitualmente accesibles por medio de HTTP, tanto para la publicación de la Lista de Certificados Revovados (CRL) como para los servicios de OCSP (Online Certificate Status Protocol).

Ventajas y Beneficios

- Debbie es un servicio fácil de instalar y actualizar, y altamente flexible para configurar diversas políticas de validación.
- Cada política de validación es mantenida de manera independiente pero utilizan los mismos elementos de validación en el caso que sean elementos compartidos.
- Es posible validar firmas como también certificados.
- Los criterios de validación son amplios y contemplan grados de contingencia, tal como el hecho de poder operar con la CRL en el caso que el servicio OCSP no se encuentre disponible para una consulta.
- Es posible definir la política de manera centralizada, evitando errores de programación e interpretación sobre la validez de una firma.