

SmartID® OCSP Client para DNI-e

SmartID OCSP Client para DNI-e extiende las capacidades de la plataforma Windows, permitiendo a las aplicaciones comprobar online el estado de revocación de los certificados digitales mediante el protocolo OCSP, especialmente para ellos certificados digitales contenidos en el nuevo DNI electrónico español.



Introducción

El imparable avance de la firma digital en el desarrollo de la sociedad de la información, hace que cada día existan más aplicaciones dentro de nuestra empresa u organismo público que deben gestionar certificados digitales.

Cuando recibimos un correo electrónico o una factura electrónica firmada digitalmente, cuando algún usuario utiliza su DNI electrónico (u otro certificado digital) para obtener acceso a información confidencial o firmar una transacción a través de la web es probable que necesitemos verificar que los certificados digitales involucrados son válidos y no han sido revocados por sus propietarios.

Comprobar el estado de los certificados.

Esta comprobación requiere que las aplicaciones que gestionan los certificados digitales, se conecten con la autoridad de certificación que emitió el certificado (**habitualmente a través de Internet**) y compruebe que el certificado o certificados no se encuentran publicados en una lista negra denominada **“lista de revocación”** (en inglés, Certificate Revocation List o CRL).

Hasta hace relativamente poco tiempo, durante esta conexión la aplicación descargaba la lista de revocación del servidor donde la autoridad de certificación la publicaba firmada, bien de forma completa o bien particionada, y una vez descargada se comprueba la inclusión o no del certificado. Estas conexiones emplean protocolos comunes como HTTP o LDAP, pero requieren un alto coste de comunicaciones y de rendimiento, por lo que es habitual almacenar estas listas en un caché para reducir la necesidad de descargas continuas de la misma lista.

El uso de un caché, mejora el rendimiento de las aplicaciones evitando alargar el tiempo de la transacción de comprobación de la revocación, aunque puede añadir un retardo (habitualmente de algunas horas) desde que un certificado es publicado en la lista de revocación y la aplicación lo detecta.

La comprobación online.

Con el objetivo de mejorar el rendimiento de las aplicaciones sin renunciar a la inmediatez de detección de la revocación de un certificado, se desarrolló el protocolo OCSP que permite una consulta online a la lista de

revocación por parte de la aplicación.

La aplicación realiza una consulta directamente a un servidor OCSP sobre el certificado del cual quiere conocer su estado y el servidor le responde indicando el estado actual del certificado, sin necesidad de descargar la lista de revocación.

SmartID® OCSP Client para DNI-e, **añade a** la plataforma Windows el protocolo OCSP integrado con el API de criptografía de Windows denominado CryptoAPI.

Al instalar SmartID® OCSP Client para DNI-e todas sus aplicaciones comerciales y propias que utilizan el API de Windows se benefician del protocolo OCSP y de sus mejoras de rendimiento y seguridad, sin necesidad de modificar las aplicaciones en la mayoría de los casos, dado que el propio sistema operativo se encarga de la verificación.



Son compatibles con SmartID® OCSP Client para DNI-e, las aplicaciones de servidor (como Microsoft Exchange, Microsoft SharePoint, Microsoft Internet Information Server,

Microsoft Forms Server, etc.), aplicaciones de puesto cliente (como Microsoft Office y Microsoft Outlook) y aplicaciones desarrolladas con Microsoft .NET.

Instalación y administración

La instalación de SmartID® OCSP Client para DNI-e es sencilla y no requiere de cambios en la estructura de la red o en los componentes críticos de los sistemas. Soporta la tecnología MSI (Microsoft Installer) que permite la instalación desatendida del software empleando políticas del Directorio Activo u otras herramientas de distribución de software.

La administración del producto se realiza de forma muy sencilla desde la consola de gestión del Directorio Activo y la gestión de los puestos mediante el uso de políticas de directorio que permiten la



la configuración centralizada y granular de cada equipo.

Licenciamiento

SmartID® OCSP Client para DNI-e se licencia por cada puesto cliente o servidor que utilice su funcionalidad. Es necesario instalar un agente en cada puesto y realizar su activación mediante una sencilla operación que requiere conectividad con Internet.

Soporte y Mantenimiento

El producto dispone de un servicio de mantenimiento correspondiente a un periodo anual y que le permite disponer de las actualizaciones y nuevas versiones que se publiquen durante dicho periodo, así como el derecho a la resolución de incidencias y consultas ilimitadas sobre el producto.

Configuración mínima:

- Pentium II 233Mhz o superior
- 256 Mb de RAM
- 60 Mb de espacio en disco
- Certificados digitales X509v3
- DNI electrónico y software asociado
- Lector de tarjetas PC/SC
- Windows 2000, XP, 2003 o Vista