

# SmartID<sup>®</sup> Corporate Logon

Reemplaza las contraseñas de acceso a sus equipos corporativos por el uso de tarjetas inteligentes con certificados digitales (PKI). Un sistema de acceso completamente compatible con el nuevo DNI electrónico español y que produce un mínimo impacto en su infraestructura de red actual. Fácil y seguro.

## Introducción

Hoy en día, las empresas y organismos públicos tienen la necesidad de garantizar un acceso seguro a sus redes e información corporativa.

Desafortunadamente, muchas de ellas todavía confían su seguridad de acceso a contraseñas estáticas y reutilizables, y con ello se exponen a que usuarios no autorizados accedan a su información empresarial.

SmartID<sup>®</sup> Corporate Logon proporciona a las empresas un sistema de autenticación robusta de dos ó tres factores, flexible y de bajo coste, para el inicio de sesión (logon) a puestos y servidores Windows mediante el uso de smartcard con certificados digitales, entre los que destacan el nuevo DNI Electrónico o la tarjeta CERES.

SmartID<sup>®</sup> Corporate Logon ha sido diseñado para su uso en puestos y servidores de una organización, funciona con cualquier modelo de smartcard o token USB que contenga al menos un certificado digital X509 en su interior y es independiente del emisor del certificado y del fabricante de la tarjeta, proporcionando a la



organización independencia y una completa integración con el sistema operativo.

La autenticación del usuario se realiza al insertar la smartcard en el lector y teclear su número personal (PIN), obteniendo acceso al equipo y a los servicios/aplicaciones asociados como ficheros, impresoras, aplicaciones web, correo electrónico, intranet, servidores de terminal o Citrix y en general todo tipo de aplicaciones con integración Kerberos sin que sea necesaria la introducción de nuevas contraseñas.

Es la propia organización quien decide, en que entidades de certificación confía y los administradores de la red pueden definir las relaciones entre los usuarios y sus certificados mediante la definición de reglas de asociación, empleando para ello una sencilla consola de administración. Es posible definir el uso de varias smartcard asociadas a una misma persona, bien para que disponga de diferentes niveles de acceso (diferentes usuarios) o bien para definir múltiples smartcard autorizadas (mismo usuario), incluso de diferentes emisores.

## Instalación y administración:

La instalación de SmartID<sup>®</sup> Corporate Lo-

gon no produce impacto en los sistemas, y al contrario que otras soluciones, evita la sustitución del proceso de inicio de sesión original de Windows **(GINA) y la modificación del esquema del Directorio Activo**, lo que facilita las actualizaciones del sistema, mejora la coexistencia con otras aplicaciones y elimina la necesidad de disponer de diferentes versiones para cada versión de sistema operativo.



### Soporte para usuarios móviles

Por otro lado, en el diseño del producto también se ha tenido presente a los usuarios móviles, disponiendo de la posibilidad de activar el caché de credenciales que permite a los usuarios de ordenadores portátiles el acceso a sus equipos con su smartcard aún cuando estos no se encuentran conectados a la red corporativa, así como la conexión externa mediante autenticación Web, a servidores Citrix o a redes privadas virtuales VPN mediante el uso de certificados digitales. Para estos usuarios, se contempla también la posibilidad de coexistencia con soluciones de cifrado de disco con el fin de proteger los datos en caso de pérdida o sustracción del equipo.

### Extensiones biométricas



La solución se complementa con diferentes extensiones, orientadas para aquellos entornos donde se considera crítico añadir un tercer factor para comprobar la identidad de quien accede a la información, extendiendo la autenticación de SmartID® Corporate Logon mediante la verificación biométrica del usuario. SmartID® Fingerprint realiza la

lectura, análisis y verificación de la huella dactilar con soporte para la mayoría de sensores y algoritmos de *matching* líderes del mercado, almacenando la información biométrica en el Directorio Activo.

### Gestión de la revocación

Durante el inicio de sesión el producto realiza la comprobación del estado de revocación de los certificados mediante la conexión a los servidores públicos de las entidades de certificación, siendo esta opción configurable por el administrador.

La familia de productos SmartID® se complementa con SmartID® Revoke Server que actúa como autoridad de validación central multi-PKI de todos los certificados que se manejan en la organización, mejorando la seguridad y rendimiento de las aplicaciones de firma electrónica con el uso de protocolo OCSP, funciones de caché, reglas de configuración y validación, descarga offline de CRL y capacidades avanzadas de auditoría. El producto dispone de un agente que al instalarse en equipos activa las funciones de comprobación de revocación, sin necesidad de más cambios, en todas las aplicaciones basadas en CryptoAPI, como son Microsoft Office, Microsoft Outlook, Internet Explorer y software de servidor de Microsoft.

#### Requisitos hardware

- Pentium II o superior
- 256 Mb de RAM
- Lector de smartcard PC/SC (CCID recomendable)
- Smartcard ISO-7816 1,2,3 y 4
- Certificado X509v3

#### Requisitos software

- Puesto con Windows 2000, XP Profesional o Windows Vista.
- Servidores Windows 2000 Server o Windows Server 2003 con Directorio Activo instalado.