

Autenticación segura multi-factor con Athena IDProtect Client



A medida que las organizaciones toman conciencia de los beneficios que aportan los servicios digitales, se hace más importante fortalecer la autenticación del usuario para garantizar la integridad de los sistemas permitiendo el acceso sólo a aque-

llas personas con permisos.

La tecnología de autenticación multi-factor de Athena permite que las organizaciones utilicen 'algo que el usuario conoce', 'algo que el usuario tiene' y 'algo que el usuario es' con un único dispositivo criptográfico seguro que puede ser distribuido entre empleados o clientes de forma segura.

La tecnología de autenticación de Athena consta de dispositivos seguros (tarjetas o tokens), middleware y lectores de tarjetas – IDProtect Client es el middleware que proporciona el enlace entre usuarios, credenciales almacenadas en un dispositivo seguro y los sistemas de autenticación cliente.

Autenticación multi-factor y multi-plataforma

IDProtect Client tiene la flexibilidad de poder trabajar con soluciones de autenticación multi-factor en topologías de red mixtas – incluyendo Microsoft Windows, LINUX y Apple Mac OSX tanto en sistemas de 32 bits como de 64 bits. En Windows, IDProtect Client se puede instalar como CSP o Minidriver.

Estándares

IDProtect Client cumple con los estándares Microsoft CAPI/CAPI 2/CNG y PKCS#11 asegurando su interacción con el rango más amplio de hardware y software, como Microsoft Outlook, Adobe, Cisco, Checkpoint, Citrix, Lotus Notes, Novell y PGP entre otros.

Biometría Match-on-Card

A través de una extensión opcional, IDProtect

Client puede mejorar la autenticación de Windows Logon utilizando los más modernos algoritmos biométricos Match on Card. IDProtect Client junto con un dispositivo seguro puede almacenar varias plantillas de dedos para ser usadas en un proceso de autenticación en la propia tarjeta o token. Soporta biometría completa en máquinas 32 bits y 64 bits.

Seguridad es la base

Diseñado y construido primando la seguridad – IDProtect Client, en combinación con el dispositivo seguro, genera claves, comprueba datos biométricos y almacena políticas de PIN en el dispositivo; ofrece criptografía basada en curvas elípticas; la comunicación (claves & PINs) entre el host y el dispositivo viaja cifrada usando mensajería segura y se ofrecen diferentes opciones seguras de distribución como por ejemplo la inyección segura de claves entre otras..

Sistemas de Administración de Tarjetas y Tokens

Para soportar la distribución masiva de proyectos PKI, IDProtect Client se ha integrado con los sistemas líderes de CMS (Card Management System) para emitir y administrar el ciclo de vida de forma sencilla. Los usuarios pueden acceder a la administración del ciclo de vida, el desbloqueo remoto, los portales autoservicio y el soporte de múltiples CAs.

Dispositivo seguro e integración PC/SC

Para garantizar una integración y funcionamiento óptimos, IDProtect Client se ha diseñado, construido y probado con la gama de tokens USB, tarjetas con y sin contacto de Athena y tarjetas MicroSD. IDProtect Client también está disponible para algunas tarjetas y productos de terceras partes.

IDProtect Client es compatible con todos los lectores de tarjetas que sean PC/SC. Athena tiene sus propios lectores biométricos, lectores de tarjetas con o sin contacto y teclados que complementan IDProtect Client, ofreciendo unas prestaciones, calidad y flexibilidad únicas en proyectos de autenticación multi-factor.

Especificaciones Técnicas

Soporte de Especificaciones

- Windows Smart Card Minidriver Specification 7.06; con compatibilidad total con Windows 7 y Server 2008 R2.
- Microsoft CAPI y CNG (dependiendo de la instalación)
- Microsoft ILM/FIM (opcional)
- PKCS# 1, 7, 10 y 11 (2.20)
- Certificados X509 versión 3

Sistemas Operativos

- Soporte y certificación complete de todos los SOs de 32 bits y 64 bits. Incluye:
 - Windows XP x86 y x64
 - Server 2003 x86 y x64
 - Windows Vista x86 y x64
 - Server 2008 x86 y x64
 - Windows 7 x86 y x64
 - Server 2008 R2 x64
- Librería Mac OSX PKCS#11, TokenD y PIN Tool disponibles (incluye 10.5 y 10.6 TokenD para plataformas Intel y PPC)
- Librería LINUX PKCS#11 y PIN Tool.

Opciones de instalación

- Se puede instalar y usar diferentes componentes de Microsoft Smart Card dependiendo de la red y configuración de la tarjeta, como los interfaces MS CAPI, CAPI 2 o CNG.
- Se puede instalar el soporte de tarjeta en entornos Microsoft Windows utilizando Athena CSP o Minidriver
- API's accesibles desde el software cliente, por ejemplo Minidriver y/o PKCS#11.
- Versiones en diferentes idiomas.
- Instalador para Mac OSX
- Instalador para Linux

Características Generales

- Inyección segura de claves - funcionalidad avanzada que permite almacenar las claves en un servidor seguro centralizado en vez de en los clientes. Cuando se necesita, el minidriver de Athena crea un canal

seguro entre el servidor de claves y la tarjeta a través de una cadena de clientes para intercambiar los datos de la clave.

- Los certificados creados con Athena CSP también están disponibles en los interfaces Athena Minidriver y PKCS#11, es decir, los certificados y claves privadas creadas a través de MD, P11 o CSP, estarán disponibles en los otros dos interfaces.
- Soporte completo de desbloqueo remoto del PIN a través de mecanismos challenge response.
- Criptografía de Curvas Elípticas (ECC) soportada con minidriver y PKCS#11 sobre dispositivos con capacidad ECC

Características de Seguridad

- Todos los datos que circulan entre el middleware de Athena y la aplicación de la tarjeta viajan cifrados.
- La implementación PKCS#11 no permite la exportación de claves privadas.
- Política de PIN aplicada en la tarjeta, no en el host.
- Verificación segura del PIN. Protegido contra ataques de fuerza bruta añadiendo niveles adicionales de seguridad.
- Almacenamiento seguro de PIN y claves - ningún PIN o clave se guarda en texto plano.
- Historial de PINs en la tarjeta
- El PIN se puede configurar para que sea cambiado tras el primer uso o después de desbloquearlo. Se administra y se sigue en la tarjeta o token.
- Validación del PIN - el PIN puede definirse para que caduque tras cierto periodo (se administra dentro de la tarjeta o token).

Soporte biométrico opcional

- Ofrece soporte de autenticación sólo biométrico, biométrico y PIN (3 factores de autenticación) o biométrico o PIN. Verdadera autenticación multi-factor
- PIN externo - soporta autenticación biométrica a través de la tecnología de alta seguridad match on card.
- Soporte biométrico para XP con GINA (Graphical Identification and Authentication), para Vista y superiores a través del proveedor de credenciales del SO. Soporte completo de biometría con Athena CSP o Minidriver (Vista y superior).
- Soporte de logon con cualquier certificado apropiado, también en XP/2003 server, incluso sin GINA.

Aplicaciones Soportadas (lista parcial)

- Windows Smart Card Logon, firma y cifrado de correo en Outlook y Outlook Express (S/MIME), Microsoft VPN, IIS SSL, OpenSSL, corre en el almacén de certificados raíz de Microsoft CA, Adobe Acrobat, Checkpoint VPN, Cisco VPN, Citrix, Lotus Notes, Novell, PGP, Netscape, Firefox, Mozilla, SSH

Soporte de dispositivos seguros

- Plataformas Athena de tarjetas con y sin contacto, USB y MicroSD.
- Otras soluciones de terceras partes.

Soporte de Lectores de Tarjeta & Bio

- Soporta cualquier lector de tarjetas que cumpla la especificación PC/SC.
- Lectores Athena biométricos, con o sin contacto y teclados
- Todos los lectores biométricos principales. Soporta productos de terceras partes.

Asia

1-14-16, Motoyokoyama-cho
Hachioji-shi
Tokyo, 192-0063
Tel: +81-426-60-7555
Fax: +81-426-60-7106

North America

20380 Town Center Lane
Suite 240
Cupertino, CA 95014
Tel: +1 866 359 2273
Fax: +1 408 608 1818

LATAM & Iberia

CL. Padre Jesús Ordoñez, 5
1-B, 28002,
Madrid, Spain
Tel: +34 9 1564 4651
Fax: +34 9 1564 4651

EMEA & International

Westpoint
4 Redheughs Rigg
Edinburgh EH12 9DQ
Tel: +44 131 208 1202
Fax: +44 131 777 8150

athena
Smartcard