



La mejor aproximación a la firma digital basada en PKI

Autores:

Ramel Levin

Uri Resnitzky



Table of Contents

Introducción	1
CoSign	1
Introducción a la tecnología PKI	1
Por qué se utiliza la firma digital basada en PKI	2
Problemas en el despliegue de PKI	2
Gestión de claves	2
Integración	3
Solucionando los problemas de despliegue de PKI mediante el uso de CoSign	3
Arquitectura de CoSign y flujo de datos	3
Trabajando con otros directorios de gestión de usuarios	4
Almacenamiento centralizado de claves de firma	5
Firmas Gráficas ("húmedas")	5
Facilidad de uso – Firma con un click	5
CoSign Solución Certificada	5
Solución "llave en mano"	6
ROI mejorado	7
Resumen técnico de CoSign	8
Esta sección presenta los detalles técnicos detrás de la tecnología de CoSign, pendiente de patente.....	8
Componentes	8
Instalación	8
Operación de usuario final	8
Registro y actualización de Directorios (Active Directory o Novell/NDS)	9
Renovación de certificados	9
Administración	9
Seguridad	10
Alta disponibilidad	10
Soporte para autoridad certificadora subordinada (Subordinate CA Support)	10
Soporte de CA externa	10



Introducción

En los últimos años, se han aprobado en todo el mundo nuevas leyes que soportan las firmas digitales y electrónicas como medio de autenticar datos y transacciones electrónicas. La "US e-Sign Bill", firmada por el anterior presidente de los E.E.U.U. Bill Clinton y la directiva de la UE para firma electrónica son dos ejemplos de esta tendencia global.

Las organizaciones han sido reacias a saltar al carro de las firmas digitales debido al coste y a la complejidad asociados a las soluciones típicas de PKI. Aunque las firmas digitales ofrecen una reducción inmediata en papeleo, costes de manipulación y de archivo, la tecnología ha llegado a ser asociada con despliegues muy lentos, alto costo y dificultad de gestión para despliegues más allá de los 100 usuarios.

CoSign, herramienta innovadora de firma digital, ofrece una nueva aproximación para la implantación de soluciones de firma digital.

Esta aproximación soluciona la mayor parte de los problemas de despliegue y reduce dramáticamente el TCO (coste total de la propiedad) de la firma digital.

Este libro blanco trata los problemas de despliegue típicos de la tecnología tradicional de firma digital y explica cómo CoSign puede solucionar estos problemas, dando por resultado un ROI atractivo y un TCO muy bajo para los beneficios obtenidos.



CoSign

CoSign es un dispositivo que ofrece una solución llave en mano de firma digital para firmar documentos, formularios y mensajes con las aplicaciones más habituales como Microsoft-Word, Adobe-Acrobat, ERP y sistemas de Content Management. Se basa en la tecnología de infraestructura de clave pública (PKI) desarrollada al final de los 70 y que ha demostrado ser a fecha de hoy la única tecnología disponible que asegura firmas infalsificables (para más información sobre la tecnología PKI ver la "introducción a la tecnología de PKI" más adelante).

CoSign ofrece una solución total de firma digital con la que se pueden realizar todas las funciones relacionadas con la misma, incluyendo la gestión de credenciales de firma y permite firmar de cualquier tipo de datos o transacciones con o sin representación gráfica de la firma.

Introducción a la tecnología PKI

Para obtener información más profunda sobre la tecnología de PKI, se anima al lector que consulte la extensa literatura publicada sobre el tema. Un buen punto de partida es el foro de PKI en www.pkiforum.org.

En un sistema de PKI, cada usuario tiene dos claves: una clave pública y una clave privada. Estas claves se pueden utilizar para cifrar y descifrar información, firmar digitalmente información electrónica y para verificar la autenticidad del usuario. Este documento se centra únicamente en el uso de la tecnología PKI con respecto a las firmas digitales.

En un sistema de PKI, la clave pública se distribuye a todo el mundo, mientras que la clave privada correspondiente se almacena por su dueño en un lugar seguro. Mientras que ambas claves se relacionan matemáticamente, la clave pública no permite calcular la clave privada. Esto hace que la tecnología PKI sea adecuada para la firma digital. Por ejemplo, cuando Alicia desea firmar un documento y enviarlo a Bob, ella realiza una determinada función matemática utilizando su clave privada. Entonces envía el documento original, junto con su firma y su clave pública a Bob. Para que Bob se pueda asegurar que el documento viene realmente de Alicia, Bob aplica un cierto método de cálculo a la firma (conocido como verificación de la firma), utilizando la clave pública. Como resultado, se consigue una huella digital del documento. Si es la misma huella digital que la contenida en el documento que Alicia había enviado, la firma de Alicia queda verificada. Si no, Bob sabe que Alicia no es la que firma este documento, o que el documento se ha cambiado a partir del momento en que Alicia lo firmó.

Puesto que solamente Alicia conoce su clave privada, y que esta clave no se puede calcular a partir de la clave pública, quedan asegurados la integridad de los datos y el no repudio. Este proceso da lugar a la responsabilidad del firmante. Es decir en un eventual proceso judicial, el firmante no puede argumentar que él/ella no ha firmado el documento.

Todavía queda un tema pendiente. ¿Cómo puede saber Bob que "la Alicia" que había enviado el documento firmado es la misma Alicia con la que quiere hacer negocios? Bob necesita la certificación de una tercera parte de confianza que conoce a Alicia y puede verificar que ella es de hecho quien dice ser. Tales entidades se llaman Autoridades Certificadoras (CA); que emiten certificados que aseguran la autenticidad del firmante. Los



certificados se pueden comparar a los pasaportes emitidos por los países a sus ciudadanos para recorrer el mundo. Cuando un viajero llega a un país extranjero, no hay otra forma de autenticar la identidad del viajero que confiar en el emisor del pasaporte (en terminología de PKI: el CA) y se utiliza el pasaporte para autenticar al portador de la misma forma que Bob utiliza el certificado de la CA para autenticar la identidad de Alicia.

Por qué se utiliza la firma digital basada en PKI

En los procesos legales y de negocio utilizados hoy, las firmas sobre papel son la forma legal más común de asegurar la responsabilidad del firmante. A pesar de que la falsificación de la firma es frecuente, las firmas siguen siendo el método más popular (y más legal) usado en los negocios. A medida que las organizaciones y negocios migran del papel a las transacciones electrónicas, se necesita un método para definir la responsabilidad del firmante en el mundo electrónico. Las firmas electrónicas básicas se han definido y han llegado a ser legales en muchas partes del mundo durante los últimos años.

El "US e-Sign Bill" de los E.E.U.U. (efectivo a partir de 1 de octubre de 2001) y la directiva "EU Directive 1999/93/EC for Electronic Signatures" definen la firma electrónica básica como: cualquier tipo de datos electrónicos que se unen a la información electrónica original. Bajo esta definición, por ejemplo, una foto del firmante pegada a un documento de Word es suficiente. Esto es el equivalente, en los documentos de papel, a poner una "X" o una estampilla en el área de la firma. Obviamente, la debilidad más grande con una "X", nombre mecanografiado, foto o similar está en que no hay ninguna forma de evitar que otros usen el mismo método para falsificar documentos.

La directiva de la Unión Europea reconoce esta vulnerabilidad y ha definido en la misma un tipo de firma electrónica más fuerte, la firma electrónica avanzada. Aunque la directiva ha intentado ser neutra a la tecnología, sólo las firmas digitales basadas en PKI cumplen los requisitos definidos en la directiva. Las firmas electrónicas avanzadas proporcionan no sólo una autenticación más fuerte del usuario, sino también protegen la integridad de los datos firmados, asegurando así el no repudio de la transacción por el firmante.

Las firmas avanzadas son críticas a su organización. Las firmas electrónicas básicas que son firmas "no PKI" son soluciones vulnerables que añaden datos (texto, sonido, símbolo, cuadro etc.) a un documento y pueden servir solamente como método débil de autenticación del firmante. Solamente las firmas digitales basadas en PKI ofrecen la mejor tecnología para proteger contra la falsificación proporcionando integridad y el no repudio de los datos.

Pero según lo mencionado antes brevemente, el PKI ha tenido sus propios problemas que han evitado que se convierta en la principal tecnología utilizada en la firma digital. En la sección siguiente discutiremos los problemas del despliegue de sistemas basados PKI.

Problemas en el despliegue de PKI

En este capítulo discutimos los problemas de desplegar soluciones tradicionales de PKI.

Gestión de claves

Según lo mencionado previamente, en un entorno PKI, cada usuario tiene un par de claves que se utilizan para firmar y validar la información. El problema es que para guardar con seguridad las claves privadas se precisa de un método seguro para almacenarlas. Generalmente, las soluciones habituales de almacenaje se dividen en dos categorías: basadas en hardware o en software. Los dispositivos de hardware, a menudo llamados tokens de hardware, almacenan las claves en tarjetas inteligentes o en dispositivos de USB. Al utilizar un medio del software, las claves se almacenan en archivos cifrados en el ordenador (sobremesa o portátil) del usuario. Estos archivos cifrados se refieren a menudo como "tokens de software".

Aunque el concepto es simple, muchas compañías han encontrado que los tokens de hardware y software son muy difíciles de manejar desde un punto de vista técnico y operacional. Los usuarios tienen una acusada tendencia a perder y olvidar sus tokens de hardware, creando enorme cantidad de problemas administrativos para volver a emitir las claves y certificados en caso de pérdida, o emitir certificados y claves temporales y en caso de un usuario que se olvida su token de hardware en casa. Hay un aumento de llamadas al helpdesk de la organización; Es necesario asignar personal de IT para manejar continuamente la gestión y distribución de claves y certificados, resultando en un aumento en el número de empleados del departamento de IT o en una pérdida de tiempo y de eficacia.

Para la mayoría de las organizaciones, los tokens de software no es una solución conveniente. En una organización donde los trabajadores tienden a ser móviles cambiando de ordenador, tanto de sobremesa como portátil, el token de software es problemático ya que no hay una manera fácil para trasladar el token de software de un ordenador a otro. Por otra parte, los ordenadores experimentan la tendencia de fallar de vez en cuando, dando por resultado la pérdida de los datos, incluyendo el token de software. No hay una manera simple para prevenir la pérdida del token de software en tales situaciones.



Integración

Los sistemas estándares de PKI incluyen componentes múltiples: el CA (Autoridad Certificadora), dispositivo del almacenaje de claves (hardware o software), software para la gestión de claves, para gestión e incorporación de nuevos usuarios, y por supuesto, los componentes necesarios para firmar en aplicaciones de la vida real (aplicaciones de workflow, ERP, correo, o cualquier otra). La integración de todos estos componentes es compleja y dura de mantener en el día a día.

Hasta hace poco tiempo, ha habido muy pocas alternativas estándar de interconexión entre los diversos componentes, y aún poniendo estos interfaces en marcha, cada vendedor define su propia versión del interfaz. Esto ha creado procesos largos y costosos de integración donde los costes han aumentado, generando un alto TCO para el proyecto.

La integración de la infraestructura de firma digital con las aplicaciones es compleja e implica generalmente desarrollos utilizando API criptográficos a bajo nivel. Aunque la tecnología está madurando y los vendedores cada vez cumplen más los estándares de la industria, la única manera de interaccionar con tokens (hardware o software) y con la CA es a través de estos interfaces criptográficos de bajo nivel (tales como PKCS#11, y MS-CAPI) que requieren un profundo conocimiento de la tecnología PKI.

Solucionando los problemas de despliegue de PKI mediante el uso de CoSign

CoSign es una solución nueva e innovadora de firma digital basada en tecnología PKI. Al contrario que las soluciones tradicionales de PKI, CoSign soluciona el despliegue, la integración y los cotidianos problemas de gestión discutidos en la sección anterior, reduciendo dramáticamente los costes de despliegue y de mantenimiento de un sistema de firma digital basado en PKI.

CoSign está recomendado en los entornos en los cuales las organizaciones conocen las partes que firman. Éste podría ser el caso con una organización usando PKI para las firmas digitales de sus usuarios internos (es decir sus empleados), con los clientes de negocio o con proveedores.

Arquitectura de CoSign y flujo de datos

CoSign es un dispositivo hardware instalado en la red. El dispositivo incluye todos los ingredientes de un PKI incluyendo la Autoridad Certificadora y el repositorio de claves privadas de firma de usuario. CoSign se integra con el sistema existente de gestión de usuarios de la organización para reducir la complejidad y el coste de la incorporación y gestión de nuevos usuarios.

La autenticación del usuario se realiza bien por la aplicación o través del directorio de usuarios de la organización. CoSign utiliza "Single-Sign-ON" o autenticación por cada firma. Para firmar, y una vez que autentique al usuario, el hash del documento (es decir la huella digital del documento) se envía a CoSign y después se firma dentro del dispositivo con la clave privada del usuario.

A la hora del alta, los usuarios pueden introducir opcionalmente su firma ("húmeda") gráfica capturada mediante el uso de una tableta gráfica. La imagen gráfica de la firma se almacena dentro de CoSign. La combinación de la firma "húmeda" y de la firma digital proporciona un sensación visual a la que el usuario está acostumbrado, así como un método seguro de sellar documentos.



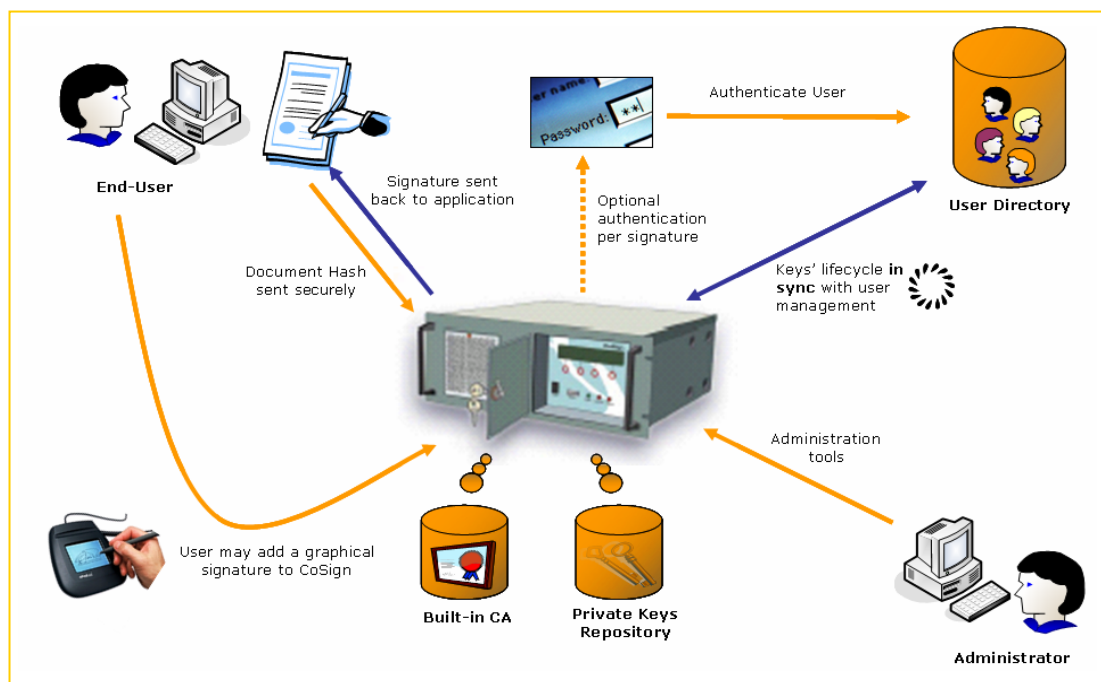


Figure 1: Arquitectura de CoSign

Alta automática usando el directorio de usuarios estándar de compañía

CoSign proporciona una sincronización automática con los directorios estándares de gestión de usuario tales como "Microsoft's Active Directory", Novell/NDS y otros LDAPs. Con CoSign, el alta y gestión de usuarios (es decir creación de claves, emisión y renovación de certificados) se realiza automáticamente una vez que un nuevo usuario entra en el sistema.

La lógica detrás de esta idea es simple. Si la organización agrega un nuevo usuario a su sistema de gestión de usuarios, y al mismo tiempo decide permitirle el acceso a determinados recursos de la red tales como correo electrónico, bases de datos y aplicaciones, puede también decidir si le permite el acceso a CoSign y crear automáticamente para él sus claves de firma únicas.

El alta de usuario en CoSign está ligada al sistema de la gestión de usuarios.

- ▶ **Añadir un nuevo usuario** - Puede crear automáticamente el par de claves y el certificado necesarios para firmar.
- ▶ **Renovación de certificado** - Los certificados de usuario se renuevan automáticamente antes de que expire el certificado, para aquellos usuarios que están dados de alta en el directorio.
- ▶ **Modificación de usuarios** – Al producirse cualquier cambio al perfil de usuario (ejemplo: empleado que cambia su apellido), se publica automáticamente un certificado actualizado.
- ▶ **Baja de usuario** - Una vez se da de baja al usuario de la lista de usuarios (en la mayoría de los casos por dejar la organización), el certificado se revoca y se agrega al CRL (lista de la revocación de los certificados). Las nuevas firmas de este usuario no se aceptan más aun cuando los documentos firmados anteriormente se pueden seguir validando.

Trabajando de forma sincronizada con el sistema de gestión de usuarios, los clientes de CoSign eliminan los costes asociados de manejar a usuarios en dos sistemas separados, uno para el sistema estándar de usuarios y el otro para el sistema de PKI. La gestión necesaria para CoSign se reduce virtualmente cero para el departamento de IT, y permite un TCO muy bajo.

Trabajando con otros directorios de gestión de usuarios

CoSign se puede también integrar con otros sistemas o entornos de gestión de usuario o funcionar en los casos en que no se utilizan dichos entornos. Por ejemplo, CoSign se puede integrar en un producto (ej. ERP) que tenga un sistema de gestión de usuarios propietario o cuando la gestión de usuario del producto/entorno no se basa en el "Microsoft Active Directory" o "Novell NDS", cuya integración con CoSign es automática.

Para estos casos, CoSign proporciona un API externo llamado SAPI ("API de firma") que permite al integrador gestionar a los usuarios (agregar, actualizar, dar de baja) dentro de CoSign o utilizar la GIU de la utilidad incluida en CoSign de gestión de usuarios.



Almacenamiento centralizado de claves de firma

Ya hemos comentado que en la arquitectura tradicional de PKI, las claves de firma de los usuarios se almacenan en tokens de software o hardware, creando problemas técnicos y logísticos y aumentando perceptiblemente el TCO del sistema. En CoSign, las claves de firma (claves privadas) se almacenan con los certificados del usuario en un repositorio central securizado.

Los usuarios pueden acceder con seguridad a sus claves de firma desde cualquier ordenador en que estén trabajando. No hay necesidad de distribuir claves o emitir claves temporales o de gestionar los tokens olvidados, puesto que todas las claves se manejan centralmente.

Se puede considerar a CoSign como una enorme tarjeta inteligente conectada a la red, combinada con el sistema de autenticación de usuario de la organización.

La autenticación de usuario para CoSign se realiza con el mismo método de autenticación utilizado por la organización antes del despliegue de CoSign. Las mismas medidas de seguridad utilizadas por la organización para el acceso a los servidores de ficheros, correo electrónico, etc. se utilizan también por CoSign. Si la organización ha decidido utilizar un determinado método de autenticación, este método se debe utilizar para todos los propósitos y usos. Sin embargo, se pueden utilizar otros métodos de autenticación, si procede, por ejemplo Smart Cards, Tokens USB, Biometría & OTP (Contraseñas de Un Solo Uso).

Firmas Gráficas ("húmedas")

Los usuarios pueden agregar su firma gráfica ("húmeda"), capturada mediante una tableta gráfica. La imagen gráfica de la firma se almacena dentro de CoSign. La combinación de la firma "húmeda" y de la firma digital proporciona una imagen visual, a la que el usuario está acostumbrado, así como una forma segura de sellar documentos.

Facilidad de uso – Firma con un click

El proceso de firma de CoSign para los usuarios finales es simple e intuitivo. Tomemos Microsoft Word como ejemplo, agregar una firma en Word es un proceso de dos etapas: Agregar un nuevo campo de firma haciendo "click" en el botón de "añadir firma" en la barra de tareas de CoSign y seleccionar "Firmar" en el menú correspondiente. Si queremos añadir el motivo por el que se firma, (por ejemplo, conformidad, autorización, etc.) se selecciona igualmente del menú.

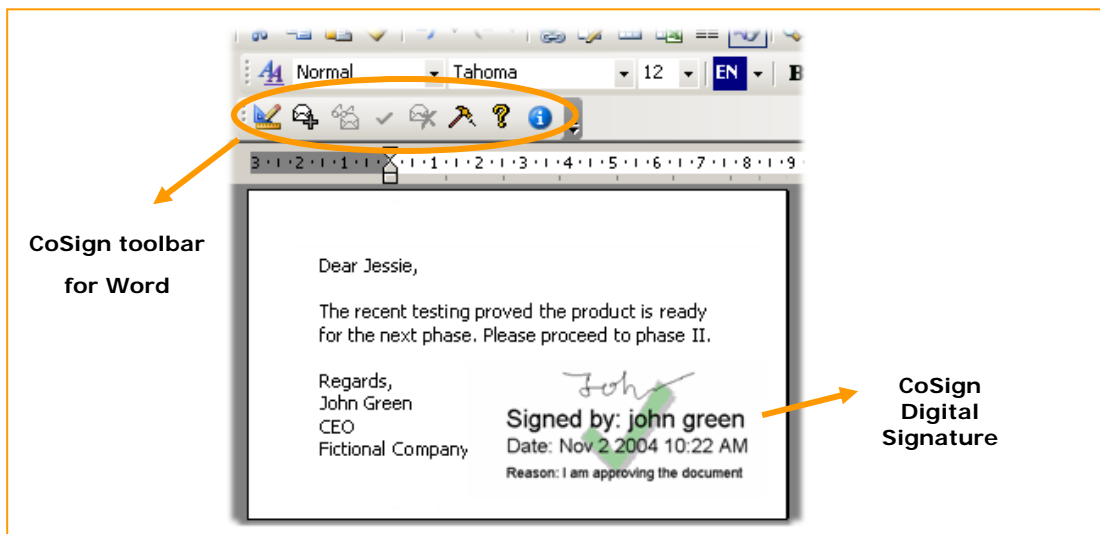


Figure 2: CoSign Digital Signature in Word

Cuando el usuario se autentifica, cada vez que él/ella firma un documento, la huella digital del documento se envía junto con las credenciales del usuario (recuperadas del directorio de usuarios de la organización) a CoSign. CoSign firma la huella digital del documento con la clave de firma del usuario.

CoSign Solución Certificada

CoSign se ha diseñado para satisfacer el "FIPS 140-2 Level 3". CoSign cumple los requisitos del "SSCD (Secure Signature Creation Device)" y los criterios de "firma digital avanzada" de acuerdo a la directiva para la firma electrónica de la Unión Europea. Adicionalmente, CoSign está en este momento en proceso de evaluación formal para obtener el "Common Criteria EAL 4+ (CWA 14169)".

Solución “llave en mano”

CoSign proporciona una solución completa e integrada de firma de Digital basada en la tecnología PKI, estándar de la industria. La solución CoSign incluye una autoridad certificadora (CA), un sistema de gestión de usuarios y un repositorio de claves y de certificados, proporcionando una solución completa basada en PKI. La solución se integra con las aplicaciones de firma usando uno de los dos métodos siguientes:

- ▶ Interfaces Criptográficas / Seguridad. CoSign soporta las principales interfaces criptográficas: Microsoft Cryptographic API (MS-CAPI), PKCS#11 y Java JCA. Las aplicaciones que utilizan llamadas PKI, y que soportan los anteriores APIs, trabajarán con CoSign sin mayor esfuerzo.
- ▶ SAPI (API de firma) - Este API de fácil uso, se utiliza para realizar llamadas a funcionalidades de alto nivel que necesitan interactuar con los diferentes APIs criptográficos descritos en el párrafo anterior de manera transparente al usuario y está diseñado para ser utilizado por aplicaciones convencionales ajenas a la tecnología PKI y que no pueden o no necesitan interactuar con los APIs criptográficos a bajo nivel. La integración con SAPI es simple e intuitiva y soporta firma, validación, funciones de gestión de usuario y las firmas manuscritas.



ROI mejorado

CoSign reduce el TCO del despliegue de una solución PKI a un nivel asequible eliminando todos los costes ocultos. La tabla siguiente compara los costes asociados a la puesta en marcha de CoSign con los de una solución tradicional PKI. El TCO incluye el coste de gestión de claves, integración con las aplicaciones, y las medidas de seguridad necesarias en una la solución de PKI. Obviamente, en un sistema basado PKI tradicional, hay muchos costes ocultos.

	PKI Tradicional	CoSign	Notas
Costo	Alto	Bajo	
Integración	50,000-100,000€	0€	CoSign es una solución "llave en mano" sin costes ocultos. Las PKI tradicionales requieren varios meses de esfuerzo de integración.
Costos de Certificados	30-100€ por usuario y año	0€	La solución CoSign lleva una CA embebida eliminando los costes de la compra de certificados y/o la funcionalidad de CA.
Costo de Tokens de Hardware	~30€por usuario	0€	CoSign no requiere el uso de tokens de hardware. Todas las claves se almacenan centralizadamente dentro de CoSign. PKI tradicionales: El costo depende del tipo de dispositivo.
Costos de seguridad de la CA	Alto	0€	CoSign es un dispositivo con protección antivandálica de acuerdo a C.C EAL4+ y está diseñado para cumplir FIPS 140-2 Level 3; la firma es no repudiable y los documentos están sellados y no se pueden alterar.

Figure 3: Costo total de propiedad de CoSign (TCO)



Resumen técnico de CoSign

Esta sección presenta los detalles técnicos detrás de la tecnología de CoSign, pendiente de patente.

Componentes

- » El sistema CoSign contiene tres componentes:
- » **El dispositivo CoSign** - Conectado con la red de la empresa en el centro de datos corporativo. Se puede instalar más de un dispositivo en configuraciones de alta disponibilidad.
- » **Cliente** – El software de cliente CoSign instalado en los servidores corporativos (Windows 2000 and siguientes) con conectores para soportar aplicaciones como Microsoft Word, Adobe Acrobat.
- » **Administrador** – La consola “Microsoft Management Console (MMC)” de CoSign se instala en los ordenadores de los administradores. También incluye una tableta gráfica para capturar y almacenar las imágenes gráficas de las firmas de los usuarios.

CoSign se puede integrar de forma transparente en la infraestructura IT del usuario interconectándose con los directorios de usuario existente. Los directorios soportados actualmente son Microsoft Active Directory y Novell/NDS estando prevista la integración con otros LDAP.

Instalación

El proceso de instalación incluye los siguientes pasos:

Directorio	Creación de un objeto en el Directorio para el dispositivo CoSign.
	Creación de objetos en el directorio donde se publicarán en certificado de CA y la CRL.
	Creación de un objeto “Service Connection Point” (SCP) en el directorio para el servicio CoSign, de forma que los clientes se puedan conectar automáticamente el dispositivo
Dispositivo CoSign	Activa una CA interna. Este paso incluye la generación de la clave de firma privada de la CA y el autocertificado ¹ de la CA
	Para cada usuario existente en el directorio, genera una clave privada y emite un certificado de usuario en la CA interna. Las claves privadas y los certificados se almacenan en la base de datos interna del dispositivo.

Operación de usuario final

Si el usuario está ejecutando una aplicación sensible a PKI (como Microsoft Word, Adobe Acrobat, etc.), la aplicación accede al cliente CSP (Cryptographic Service Provider) de CoSign que le presenta un contenedor de clave para la clave de usuario almacenada en el dispositivo CoSign. Entonces la aplicación es capaz de utilizar el contenedor de clave para ejecutar las operaciones de firma.

Los pasos a realizar son los siguientes:

- » El usuario hace “login” en la red corporativa.
- » El usuario ejecuta una aplicación CAPI sensible a PKI (ejemplo: Microsoft Word).
- » El subsistema CAPI activa los módulos CSP registrados y busca contenedores de claves.
- » El CSP de CoSign encuentra el dispositivo CoSign utilizando la entrada SCP en el Active Directory.
- » El CSP de CoSign establece una conexión SSL connection con el dispositivo, es decir autentifica el dispositivo².

¹ La clave privada del CA interno se almacena en la base de datos del dispositivo.

² La clave privada SSL utilizada para la identificación del dispositivo es única para cada unidad fabricada y se certifica por una AR (autoridad de registro) durante el proceso de fabricación.



- ▶ Single Sign On (SSO) en el Active Directory: El CSP ejecuta, sobre la conexión SSL, un intercambio de "Support Provider Interface" (SSPI) con el dispositivo utilizando las credenciales de "logon" del usuario en el "Windows Active Directory", para autenticar al usuario en el dispositivo³.
- ▶ En el "Novell/NDS" y "DII" (Directory Independent Installations), se solicita al usuario sus credenciales de "login", que se transfieren sobre un canal seguro SSL al dispositivo. En "Novell/NDS" las credenciales se verifican contra el directorio. En DII, el dispositivo verifica localmente las credenciales.
- ▶ En respuesta a una petición del CSP, el dispositivo recupera de la base de datos interna⁴ las propiedades de la clave privada del certificado de usuario (sin mandar la clave⁵) y la imagen gráfica de su firma (si está disponible) y las devuelve a través de la conexión SSL.
- ▶ El CSP presenta el certificado de usuario como parte del almacén local de certificados y presenta en contenedor de claves a la aplicación CAPI llamante.
- ▶ Cuando la aplicación realiza una petición de firma digital, el CSP dirige la petición al dispositivo utilizando la conexión SSL y entonces el dispositivo realiza la operación utilizando la clave privada de usuario, almacena el evento de firma en el registro de auditoría y devuelve la firma realizada.
- ▶ El dispositivo se puede configurar para que pida al usuario que se vuelva a autenticar cada vez que firma. En este caso, se pedirán las credenciales al usuario que se verificarán por el dispositivo contra el directorio, caso de AD/NDS o localmente cuando usamos DII.

La instalación del software de cliente de CoSign es rápida y simple. Puesto que la instalación se basa en la tecnología MSI, el software de cliente se puede desplegar y configurar fácilmente usando "Active Directory Group Policy" u otras aplicaciones de gestión de usuarios.

Además de CAPI, el software de cliente de CoSign también proporciona APIs para PKCS#11 y el token criptográfico JCA permitiendo la integración con otras aplicaciones que utilizan tecnología PKI.

Registro y actualización de Directorios (Active Directory o Novell/NDS)

El dispositivo detecta los cambios en el directorio y toma las medidas apropiadas para reflejarlos en la base de datos interna:

- ▶ Cuando se agrega un nuevo usuario al directorio, el dispositivo recupera la información del nuevo usuario, genera un nuevo certificado y clave privada y los da de alta en el CA interno. El nuevo certificado emitido se almacena, junto con la clave privada, en la base de datos interna. El nuevo usuario puede comenzar a utilizar la firma digital inmediatamente, después de darse de alta en la red corporativa, sin tener que pasar primero con un tedioso proceso de alta manual de certificados.
- ▶ Cuando se da de baja del directorio a un usuario, el dispositivo revoca el certificado del usuario en el CA interno y borra al usuario de la base de datos interna. Esto proporciona la inmediata revocación de la información, evitando el riesgo de falsificación de la firma.
- ▶ Cuando se actualiza la información de usuario (como nombre o dirección de correo) en el directorio, el dispositivo recupera la información actualizada, revoca el certificado existente y emite un certificado de usuario nuevo, basado en la información actualizada y la clave privada existente.
- ▶ El dispositivo sincroniza y guarda actualizados en el directorio, el certificado de la CA interna, las listas de revocación (CRL) y los certificados de usuario emitidos. Esto permite la fácil integración con las aplicaciones que utilizan el directorio.

Renovación de certificados

El dispositivo renueva automáticamente los certificados de usuario próximos a caducar volviendo a generar sus claves en la CA interna. Esto significa que los certificados de usuario se renuevan automáticamente de manera transparente al usuario.

Administración

La administración del sistema requiere una mínima atención y se limita a tareas generales:

- ▶ Copia de seguridad y restauración de la base de datos encriptada del dispositivo.
- ▶ Carga segura de actualizaciones de firmware firmadas digitalmente.
- ▶ Parametrización del sistema.

³ Permite el uso de mecanismos de autenticación avanzados de terceras partes, tales como contraseña de un solo uso, dispositivos de autenticación biométricos, que soporten la arquitectura de "logon" de Windows.

⁴ Todos los registros en la base de datos interna se referencian utilizando el GUID del directorio del usuario autenticado que se recupera mediante una autenticación positiva.

⁵ Las claves privadas de usuario nunca salen del dispositivo. Esta característica proporciona un nivel de seguridad similar al de las tarjetas inteligentes.



Estas tareas se realizan a través de la interfaz MMC. El menú MMC de CoSign se comunica con el dispositivo de la misma forma como el cliente CSP (sesión SSL con autenticación de usuario). Las funciones de administración, sólo pueden ser realizadas por usuarios autenticados con atributos de administrador del sistema.

Para los casos en que el cliente no utilice directorio de usuarios, se proporciona una herramienta de gestión de usuarios. Esta herramienta se puede utilizar para añadir, modificar o borrar usuarios y también para el manejo de sus contraseñas de acceso.

El registro de auditoría que se mantiene en el dispositivo se puede descargar y visualizar utilizando el visor de eventos estándar de Windows. Al contrario de otras soluciones, el registro de auditoría de CoSign permite al administrador el seguimiento del uso de las claves privadas (cuándo y quién firmó).

Seguridad

El dispositivo CoSign está diseñado para cumplir el "FIPS 140-2 Level 3" y la validación "Common Criteria EAL4+". Esto asegura que cumple los rigurosos estándares de la seguridad requeridos para los HSM, así como garantiza una seguridad total para todo el sistema (hardware, sistema operativo y aplicación):

- » Solamente se utilizan los algoritmos estándares aprobados para el cifrado simétrico, los cálculos digitales de la huella del documento (hash) y la generación de números aleatorios.
- » Se realizan chequeos automáticos para asegurar la operación apropiada de los algoritmos criptográficos y del generador de números aleatorios.
- » Se realizan pruebas para asegurar la integridad del firmware y de la base de datos de CoSign.
- » La base de datos interna de la aplicación está cifrada para prevenir cualquier exposición al exterior de las claves privadas de los usuarios.
- » El dispositivo está instalado dentro de una carcasa resistente con sensores anti vandálicos.
- » En caso de que el dispositivo es violado, todas las claves utilizadas para proteger el sistema (encriptación de la base de datos, etc..) se destruyen, borrando el contenido del dispositivo (resistente al vandalismo).
- » El sistema operativo del dispositivo se ha reforzado, quitando los componentes innecesarios, e instalando un filtro para los paquetes de la red.
- » Las validaciones incluyen la revisión de la política formal de seguridad del producto, del autómata de estados finito y la documentación del proceso de desarrollo del software (procedimientos de control del código fuente, diseño del producto, plan de pruebas, etc.). La funcionalidad, las especificaciones del interfaz y la implantación se verifican por un laboratorio externo independiente de acreditado prestigio.

Alta disponibilidad

Se pueden instalar concurrentemente varios dispositivos para construir arquitecturas con **Redundancia y Balanceo de carga**.

- » Redundancia - En caso de fallo de uno de los dispositivos CoSign, uno de los restantes dispositivos asumirá el control y realizará las operaciones de firma digital.
- » Balanceo de carga – Balanceo de carga entre varios dispositivos CoSign, permitiendo a las organizaciones realizar altos volúmenes de transacciones simultáneas confortablemente.

Solamente el dispositivo principal realizará operaciones de sincronización con los directorios de usuario, mientras que los otros dispositivos de CoSign instalados proporcionarán recursos para las firmas y no gestionarán nuevos usuarios.

Soporte para autoridad certificadora subordinada (Subordinate CA Support)

Si una compañía ha invertido ya en una infraestructura PKI, CoSign se puede configurar para ser utilizado en un entorno que incluya ya una CA, y puede actuar como CA subordinada. En este modo, CoSign genera certificados y sus claves públicas y privadas. Sin embargo, el CA de CoSign se firma con la clave del CA padre. Esto elimina la necesidad de distribuir la raíz de la CA de CoSign, pues el CA del padre (si se asume que lo se ha distribuido ya) se puede utilizar para validar los certificados. La cadena de certificados de cada certificado de usuario incluirá el CA de CoSign, el CA del padre, y el CA de cualquier otros padres que se pudieran definir.

Soporte de CA externa

CoSign soporta las organizaciones que utilizan certificados de un CA externo (ejemplo: la CA nacional que publica certificados cualificados). Al usar un CA externo, el dispositivo CoSign no genera claves privadas y certificados del usuario final durante la instalación. En este caso, hay que utilizar los mecanismos definidos por el CA externo para generar claves privadas y certificados de usuario final.



For more information please contact
sales@arx.com or visit www.arx.com

Your comments and feedback are welcome media@arx.com