

PRINCIPALES VENTAJAS

Permite un despliegue rápido y amplio de certificados digitales

Al aprovechar a un servicio gestionado muy adaptable, basado en estándares abiertos, las empresas pueden emitir y gestionar certificados de forma fácil para miles de usuarios finales y dispositivos de red.

Minimiza los costes de PKI

El servicio MPKI ofrece un bajo coste de propiedad al compararlo con las implementaciones de software de PKI independientes.

Ayuda al cumplimiento de la legislación vigente

Las empresas pueden aprovechar los servicios de certificados digitales como autenticación, codificación, firma digital y no rechazo para promover el cumplimiento de la normativa específica del sector en materia de protección de datos.

Reduce la exposición a los riesgos

Al delegar las tareas y procesos de seguridad clave a un reconocido líder del sector, la empresa minimiza los riesgos y las multas asociados a la elección o el funcionamiento de PKI interno.

Servicio Managed Public Key Infrastructure (MPKI) de VeriSign®

A medida que el comercio, la comunicación y la colaboración en línea se convierten en la forma esperada, y a menudo preferida, de hacer negocios, la seguridad de la red consiste tanto en dejar pasar a los “chicos buenos” como en dejar fuera a los “chicos malos”. Para integrarse con los socios comerciales, proporcionar acceso seguro a los usuarios, asegurar la continuidad de los negocios, y cumplir con la normativa gubernamental, las empresas deben ser capaces de autenticar a los usuarios internos y externos y asegurar los intercambios de datos seguros en línea, las transacciones y las comunicaciones.

El servicio MPKI de VeriSign® es una solución de empresa completamente integrada, diseñada para asegurar las aplicaciones de intranet, extranet e Internet a la vez que permite una interacción fluida con los socios comerciales, los comerciales, los dispositivos de servicios web, y otros usuarios. Este servicio completamente adaptable permite a las empresas establecer rápidamente una sólida infraestructura de clave pública (Public Key Infrastructure, PKI) y un sistema de entidades emisoras de certificados (Certificate Authority, CA), al mismo tiempo que se reduce la carga del desarrollo, del mantenimiento y de la supervisión de PKI. Las empresas conservan el control total de la política de seguridad, los modelos de autenticación, y la gestión de la vida útil del certificado. Construido sobre estándares abiertos para asegurar la máxima flexibilidad, el servicio MPKI permite la interoperabilidad con casi cualquier aplicación o dispositivo y está integrado previamente con las soluciones líderes listas para su uso, incluyendo las aplicaciones de Microsoft® y los sistemas operativos Windows®. Al aprovechar el servicio MPKI para desarrollar servicios de certificados digitales, las empresas pueden reducir el coste y la complejidad de las implementaciones PKI a la vez que proporcionan servicios avanzados y de confianza en todo el mundo de la autenticación, la codificación, la firma digital y el no rechazo, dentro y fuera de la empresa.

+ Funcionalidad completa

El servicio MPKI permite a las empresas emitir certificados digitales de forma rápida, segura y económica no sólo para los empleados, clientes y socios comerciales, sino también para las aplicaciones de servicios web y los dispositivos de red, como los servidores, enrutadores, y cortafuegos. La generación de claves de raíz auditables y centralizadas, la custodia de las claves y la recuperación de claves distribuidas certifican la máxima seguridad y la protección de las claves privadas. También se admite la generación de pares de claves duales, permitiendo la emisión por separado de los pares



Abre la empresa para socios comerciales de forma segura

Los certificados digitales permiten a los usuarios de la empresa llevar a cabo transacciones y comunicaciones seguras con prácticamente todo el mundo, en cualquier lugar.

Promueve la adopción por parte de socios, clientes y proveedores

La plataforma de probada eficacia de VeriSign goza de gran prestigio e inspira confianza en todo el mundo, lo que alienta la rápida adopción de los servicios facilitados por PKI, tanto dentro como fuera de la empresa.

de claves de firma y codificación. Las funciones de internacionalización incluyen la compatibilidad para la codificación del formato de transformación Unicode (UTF)-8, lo que permite a los usuarios de la empresa inscribirse y mostrar ID digitales en idiomas que necesitan caracteres que no son ASCII (como japonés, chino y la mayoría de los idiomas europeos).

+ Implementación rápida, adaptable

Los conjuntos de herramientas y la integración previa con las aplicaciones y plataformas líderes aseguran un rápido desarrollo del servicio MPKI en casi cualquier sistema, red o dispositivo, tanto si se encuentra ubicado dentro de la empresa, como fuera de ella. El servicio MPKI se ha probado en situaciones reales para adaptarse sin problemas tanto a cientos como a millones de usuarios, permitiendo a las empresas desarrollar certificados digitales en función de sus necesidades. Además, puesto que todos los servicios están albergados en la infraestructura existente, la puesta en marcha se puede completar en cuestión de semanas.

+ Acceso remoto fácil y seguro

El servicio MPKI, que está integrado previamente con soluciones de red privada virtual (Virtual Private Network, VPN) líderes en el mercado (Check Point®, Cisco®, Nortel Networks™) y con redes de área local (Local Area Networks, LAN) inalámbricas compatibles mediante protocolos de autenticación extensible (Extensible Authentication Protocol, EAP), y de seguridad de niveles de transporte (Transport Layer Security, TLS), ofrece la posibilidad de utilizar certificados digitales de forma transparente para facilitar una autenticación segura en entornos de acceso inalámbricos y de línea fija. Las capacidades de roaming permiten a los usuarios móviles finales, que trabajen desde cualquier equipo o dispositivo con acceso a Internet, utilizar los certificados digitales sin ningún tipo de problema al acceder a intranets, extranets, aplicaciones y portales web. En función de los requisitos comerciales, las empresas pueden elegir un servicio de roaming de un sólo servidor, a nivel de entrada, o un servicio más sólido, de múltiples servidores. Finalmente, la integración con tarjetas inteligentes, token USB y módulos de plataformas de confianza en equipos basados en Intel® Centrino™ permite la utilización de una variedad de soluciones de autenticación de dos factores para un acceso remoto.

+ Flexibilidad de largo alcance

El compromiso de VeriSign con los estándares abiertos, la tecnología innovadora y las colaboraciones estratégicas asegura la flexibilidad y facilidad de uso que las empresas necesitan no sólo para operar libremente en diferentes entornos, sino también para maximizar los beneficios en las inversiones existentes. MPKI es compatible con diferentes tipos de certificados estándar, incluyendo los protocolos Secure Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL), e Internet Protocol Security (IPSec), así como los estándares del sector, como X.509v3, Lightweight Directory Access Protocol (LDAP), y Public-Key Cryptography Standards (PKCS) 7, 10, y 12. MPKI opera en versiones actuales de los navegadores más extendidos, como Internet Explorer y Netscape® y en sistemas operativos, incluyendo Windows, Solaris™ y AIX®. El complemento basado en Java™ o ActiveX®, Personal Trust Agent (PTA) de VeriSign®, permite a las empresas presentar una interfaz de usuario común e identificable para los servicios de certificados digitales, incluso en entornos de plataforma de suscriptor heterogéneos.

+ Integración completa con las aplicaciones de Microsoft

VeriSign se ha aliado con Microsoft para ofrecer servicios de seguridad basados en Microsoft Windows Server™ 2003. Construida sobre Microsoft Windows Server 2003 y los servicios MPKI de VeriSign, esta plataforma PKI de última generación permite a las empresas desarrollar rápidamente soluciones de gestión de identidad

digital para miles de usuarios finales y permite una interoperabilidad perfecta entre sistemas heterogéneos y redes de empresas. La nueva plataforma utiliza las capacidades de autoinscripción en Windows Server 2003 y Windows XP para permitir un rápido desarrollo de las aplicaciones, como correo electrónico seguro, protección de archivos y firmas digitales. Además, las soluciones están particularmente bien diseñadas para proporcionar acceso seguro a las redes de empresas a través de LAN inalámbrico, VPN y otras aplicaciones.

+ Conformidad con los requisitos del sector

MPKI es el primer servicio de Managed PKI que consigue la aprobación de la entidad emisora de certificados Federal Bridge Certification Authority (FBCA), lo que permite a las empresas interoperar fácilmente con los PKI de las agencias gubernamentales. Además, la infraestructura MPKI ayuda a las empresas a cumplir con la legislación específica vigente para el sector, acerca de la protección, la disponibilidad y la posibilidad de realizar auditorías de datos confidenciales. Al utilizar el servicio MPKI, los proveedores de servicios sanitarios, las instituciones financieras, las agencias gubernamentales, las compañías de seguros y otras organizaciones pueden autenticar, codificar, firmar y auditar intercambios de datos para cumplir con la normativa federal, como la Ley de portabilidad y responsabilidad de la seguridad social (Health Insurance Portability and Accountability Act, HIPAA), la Ley 1386 del Senado de California (California Senate Bill 1386), la Ley Gramm-Leach-Bliley (Gramm-Leach-Bliley Act), y el Título 21 del Código de normativas federales (Code of Federal Regulations, CFR), Parte 11.

+ Programa de modernización de PKI de VeriSign®

En respuesta a la creciente tendencia de las empresas de abandonar los sistemas de software de PKI propios, VeriSign ofrece un programa para permitir a las empresas y a las agencias gubernamentales la utilización de software de desarrollador PKI para migrar de forma rápida, fácil y económica a los servicios MPKI de última generación de VeriSign. Los incentivos de precios especiales y la asistencia técnica están disponibles para los clientes que desean actualizar su software propio para las soluciones del servicio PKI de última generación.

+ Características de MPKI

Características principales

Mecanismo de autenticación común para múltiples aplicaciones:

- mensajería de confianza (Microsoft Exchange, IBM® Lotus Notes®, AOL® Instant Messenger™)
- VPN segura (Check Point, Cisco y Nortel Networks)
- autenticación de dos factores (Aladdin™, Authenex™, ActivCard®, Schlumberger™)
- formularios seguros (Adobe®, Evincible™)
- servicios web (servicio Trust Gateway de VeriSign®)

Host local:

- el cliente puede localizar, identificar y albergar páginas de inscripción de usuarios finales.

Gestión completa de la vida útil del certificado:

- el centro de control de VeriSign® proporciona a los administradores de la empresa el control completo para inscribir, aprobar, revocar y renovar los certificados digitales.

Métodos de autenticación flexibles:

- autenticación manual
- autenticación mediante passcode
- administración automatizada

Entidad emisora de certificados integrada:

- infraestructura de entidad emisora de certificados integrada y operada por VeriSign en nombre del cliente
- funcionamiento continuo del centro de datos de VeriSign®
- recuperación de desastres

Programa de asistencia Gold Support de VeriSign®:

- contratos de prestación de servicios con el programa opcional de garantía NetSure® de VeriSign®

+ VeriSign Trust NetworkSM

- Los clientes que tienen una entidad emisora de certificados pública pueden sacar partido de VeriSign Trust Network, que se rige por la política de certificados y la referencia normativa de certificación VeriSign® (Certificate Policy and Certification Practices Statement, CP/CPS).

Características de valor añadido

Servicios de gestión clave:

- depósito seguro y recuperación de las claves privadas

Servicios de roaming:

- modelo de servidor único o servidores múltiples, enteramente albergado en un sitio de cliente, dividido entre un sitio de cliente y el centro de datos de VeriSign, o completamente albergado en el centro de datos de VeriSign
- compatibilidad para la validación de total confianza del directorio LDAP (modelo albergado por el cliente)
- lista de revocación de certificados (Certificate revocation lists, CRL) actualizada cada hora
- protocolo Online Certificate Status Protocol (OCSP) para validación de certificados a tiempo real

Programa de asistencia Platinum Support de VeriSign®:

- servicio de asistencia al cliente continuo
- sistema de preproducción para pruebas y desarrollo
- administrador de asistencia asignado

Si desea más información visítenos en www.verisign.es