Bit4ID mejora el sistema de tarjeta de identificación electrónica de Oriente Medio con un sistema de identificación digital en línea compatible con eIDAS, utilizando HSMs de Entrust

Bit4ID desarrolla tecnologías de autenticación, firmas digitales y criptografía fáciles, seguras y estándar. Con su sede central en Italia, la empresa tiene oficinas en Ecuador, India, Macao, Perú, Portugal, España y el Reino Unido.

La filosofía de Bit4ID es que, de la misma forma en que la identidad física de una persona es única y se reconoce a nivel universal, la identidad digital de esa persona debería ser singular y capaz de representarle de forma segura en redes informáticas e Internet. Además, opinan que, a fin de que los programas de identidad digital tengan éxito, deben ser simples y seguros, así como fáciles y naturales de usar, tanto para las empresas que los gestionan como para quienes los utilizan.

> **«Los HSMs nShield de Entrust son el estándar en todo el mundo. Desarrollamos proyectos basándonos en la extraordinaria fiabilidad y responsabilidad que ofrecen los HSMs nShield de Entrust, y los integramos en todos nuestros productos. Confiamos implícitamente en la marca Entrust y en sus productos.»**
>
> – Pierluigi Pilla, director la unidad de sistemas de identificación y PKI en Bit4ID

APRENDA MÁS EN ENTRUST.COM/HSM

Bit4ID

DESAFÍO EMPRESARIAL

Como parte de una empresa conjunta de integradores de sistemas, Bit4ID recibió un contrato con el Ministerio de Información de un país de Oriente Medio para ofrecer una solución de identidad digital para toda su población, que incluye tanto a los ciudadanos como a los no ciudadanos del país. Dicho país ya tenía un sistema de documentos de identidad electrónicos (microchip), pero el Ministerio de Información quería complementar el sistema con una infraestructura informática para generar y gestionar los documentos de identidad digitales en el ciberespacio (de acuerdo con el reglamento de Identificación Electrónica y los Servicios de confianza (eIDAS) de la Unión Europea). Usar el modelo eIDAS no solo asegura un enfoque de prácticas recomendadas, sino que su cumplimiento también permite el comercio con la UE y con otros países que se adhieren a dicho estándar.

DESAFÍO TÉCNICO

PKIs, certificados digitales e identidades digitales

Las infraestructuras de claves públicas (PKI) ayuda a establecer la identidad de las personas, los dispositivos y los servicios, permitiendo el acceso controlado a sistemas y recursos, protección de datos y contabilidad de transacciones en línea. Las PKI son la base que permite el uso de tecnologías como las firmas electrónicas y el cifrado en poblaciones con muchos usuarios. Por consiguiente, las PKI son esenciales para las transacciones gubernamentales y el comercio electrónico seguro y fiable.

Certificados digitales

Los certificados digitales son las credenciales que facilitan la verificación de identidades entre los usuarios y una transacción. Así como un pasaporte certifica la identidad de alguien como ciudadano de un país, el certificado digital establece la identidad de los usuarios dentro de un ecosistema. Puesto que los certificados digitales se usan para verificar la identidad de quien firma la información, es de vital importancia proteger la autenticidad y la integridad del certificado para mantener la confianza del sistema.

Autoridades certificadoras

Una Autoridad Certificadora (CA) es el componente central de una PKI responsable de establecer una cadena de confianza jerárquica. Las CA emiten credenciales digitales que se usan para certificar la identidad de los usuarios y sustentan la seguridad de una PKI y de los servicios que respalda. Los controles físicos y lógicos, así como los mecanismos reforzados de los módulos de seguridad de hardware (HSM) garantizan la integridad de una PKI y mitigan el riesgo de sufrir ataques.

eIDAS

eIDAS es un reglamento de la UE que establece estándares para identidades, autenticación y firmas electrónicas. Esto aplica para los organismos gubernamentales y las empresas que ofrecen servicios en línea para ciudadanos europeos y que reconocen o utilizan identidades, autenticación o firmas. eIDAS también requiere el uso de HSMs certificados con Common Criteria EAL4+ (AVA_VAN.5) para emitir certificados digitales, firmas digitales, marcas de tiempo y otros datos de transacción.

Requisitos del sistema

El Ministerio de Información ya tenía una PKI para emitir documentos de identidad electrónicos para los ciudadanos. Bit4ID necesitaba integrar capacidades adicionales en la PKI que:

- Permitan a los residentes firmar transacciones y documentos de forma digital usando tanto dispositivos móviles como de escritorio, tal es el caso de computadoras portátiles, tablets o teléfonos inteligentes

Bit4ID

- Puedan crecer fácilmente
- Generen certificados para millones de usuarios
- Procese miles de transacciones por segundo

SOLUCIÓN

Una de las razones por las que el Ministerio de Información asignó este proyecto a Bit4ID, fue su propuesta de que los certificados móviles se guardaran en un HSM nShield ® de Entrust, certificado con Common Criteria EAL4+, en vez de guardarlos en el mismo dispositivo; por ejemplo, un teléfono móvil. Esto cumpliría con el reglamento eIDAS con respecto a las credenciales digitales remotas. Bit4ID, una empresa experta en el cumplimiento con eIDAS, sabía cómo hacer que el sistema funcionara.

La empresa diseñó un sistema de identidad digital personalizado que facilitaría el tráfico entre la PKI nacional, los HSMs nShield de Entrust, y los residentes del país del Medio Oriente que utilizaran el sistema. El sistema administra de forma segura la emisión de certificados de la PKI nacional al HSM, regula el uso de los certificados desde el HSM hasta los usuarios y controla la gestión del ciclo de vida de los certificados (suspensión, revocación, renovación). Los usuarios necesitan los certificados para identificarse y autenticarse en el sistema y así, firmar documentos de las varias solicitudes del gobierno, como abrir un negocio, rellenar electrónicamente el formulario para el impuesto sobre la renta y firmar o subir documentos de correspondencia legal.

Actualmente, la instalación utiliza la solución SignCloud de Bit4ID junto con aplicación de middleware complementaria, Universal Key Chain, además de un total de cuatro HSMs nShield Connect XC: uno para el desarrollo, uno para las pruebas y dos para la producción, que incluye un mecanismo de conmutación por error. Lo que ofrece una alta disponibilidad y equilibrio de carga para un funcionamiento sin complicaciones. Bit4ID también sacó partido a la arquitectura única de Entrust, Security World, que permite almacenar claves como archivos cifrados y protegidos fuera de los límites físicos de los HSMs, ofreciendo almacenamiento virtual ilimitado para las claves.

El sistema de identificación actual se utiliza principalmente para solicitudes del gobierno a los ciudadanos. Sin embargo, existen planes para replicar la implementación actual para habilitar más casos de uso que utilicen las firmas digitales en solicitudes entre el gobierno y los negocios, así como entre varios gobiernos.

"Bit4ID ha trabajado con Entrust y ha utilizado sus HSMs de nShield durante muchos años", comenta Pierluigi Pilla, director la unidad de sistemas de identificación y PKI en Bit4ID. "Los HSMs de Entrust son el estándar en todo el mundo. Desarrollamos proyectos basándonos en la extraordinaria fiabilidad y responsabilidad que ofrecen los HSMs nShield de Entrust, y los integramos en todos nuestros productos. Confiamos implícitamente en la marca Entrust y en sus productos".

Bit4ID

Necesidades del negocio

Crear un sistema de identificación digital en línea que complemente un sistema electrónico de tarjetas de identificación ya existente y que cumpla con eIDAS

Necesidades tecnológicas

Integrarlo en una infraestructura PKI adicional ya existente que:

- Permita a los residentes firmar de forma digital usando tanto un ordenador de escritorio como un dispositivo móvil, así como ordenadores portátiles, tablets o smartphones
- Puedan crecer fácilmente
- Generen certificados para millones de usuarios
- Procesen miles de transacciones por segundo

Soluciones

Diseñar un sistema de identificación digital personalizado usando:

- SignCloud de Bit4ID
- Universal Key Chain de Bit4ID
- HSMs Entrust nShield Connect
- Arquitectura nShield Security World

Resultados

- Creación de un sistema de identificación digital móvil a nivel nacional
- Cumplimiento con las necesidades tecnológicas y de seguridad de los negocios de los clientes
- Sistema sólido que se duplicará y ampliará a otros casos de uso

RESULTADOS

Bit4ID creó un sistema de identificación digital móvil de acuerdo con eIDAS que complementa el sistema de tarjetas de identificación electrónicas actuales del país del Medio Oriente. El sistema:

- Permite que los residentes firmen digitalmente tanto desde dispositivos móviles como de escritorio
- Puede crecer fácilmente
- Genera certificados para millones de usuarios
- Procesa miles de transacciones por segundo
- Se duplicará y se ampliará a solicitudes entre el gobierno y los negocios, así como entre varios gobiernos

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Ahora más que nunca, la gente necesita experiencias seguras impecables, mientras cruzan fronteras, realizan compras, acceden digitalmente a servicios del gobierno o inician sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes de más de 150 países, no es una sorpresa que la mayoría de organizaciones autorizadas del mundo confíen en nosotros.

Aprenda más en
entrust.com/HSM

ENTRUST

Contacte con nosotros:
HSMinfo@entrust.com