nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

Microsec implementa una identificación móvil confiable compatible con eIDAS y los HSMs de nCipher Security

Con sede en Budapest, Hungría, Microsec es la mayor autoridad de certificación húngara y un proveedor de servicios de confianza (TSP) para firmas electrónicas y soluciones certificadas por eIDAS. Fundada en 1984, Microsec ofrece una amplia gama de soluciones y servicios de Infraestructura de clave pública (PKI) de próxima generación que incluyen el pasaporte electrónico, tecnología de seguridad de tarjetas de identificación electrónica (e-ID), autorización de transacciones y PKI móvil.

Una solución muy popular es Microsec PassBy[ME] Mobile ID, un sistema de identificación móvil basado en PKI que proporciona autenticación de usuario a prueba de futuro, firma de transacciones y firmas electrónicas móviles, creando un proceso digital de extremo a extremo para los usuarios. La solución está diseñada para equipar a los usuarios de teléfonos inteligentes con una identidad móvil segura que se puede utilizar para el acceso a la banca en línea, retiros de efectivo en cajeros automáticos, servicios de gobierno electrónico tales como servicios de salud electrónica o impuestos, o por proveedores de servicios en la nube para el acceso remoto seguro. La identificación móvil PassBy[ME] patentada aprovecha los certificados que cumplen con eIDAS para ofrecer una autenticación de cliente sólida a prueba de futuro; trazabilidad legal y no repudio; así como mensajes confiables con recibos de mensajes firmados como prueba de entrega.

DESAFÍO DEL NEGOCIO

Un objetivo de diseño fundamental de la identificación móvil por parte de Microsec PassBy[ME] era establecer las mismas garantías que existen en el mundo físico, igual que en una sucursal bancaria, replicadas en un modelo en línea para facilitar la autorización de transacciones y firmas legalmente vinculantes de cualquier tipo de dispositivo móvil.

El sistema europeo de reconocimiento de identidades electrónicas (eIDAS) es una regulación europea diseñada para crear consistencia y estándares en toda la Unión Europea (UE) para identidades electrónicas y servicios de confianza que respalden la autenticación y las firmas. eIDAS garantiza que las transacciones electrónicas sean seguras, sin importar dónde se realicen.

El Dr. Sándor Szőke, subdirector de Microsec de eIDAS Trust Services, explicó los principales casos de uso de PassBy[ME] Mobile ID: "Para el sector financiero, nuestra solución facilita la banca en línea y el comercio electrónico, las transacciones en cajeros automáticos y el uso en el punto de venta. Para las entidades gubernamentales, puede ofrecer servicios de salud electrónica, impuestos y una variedad de servicios para los ciudadanos. Los departamentos gubernamentales también pueden usar la solución para acceder de forma segura a información y datos confidenciales. También proporciona servicios de acceso remoto para entornos en la nube."

DESAFÍO TÉCNICO

El principal requisito relacionado con la tecnología para PassBy[ME] Mobile ID fue el uso de la PKI con las llaves correspondientes y los certificados compatibles con eIDAS. “Con la naturaleza crítica de las transacciones que apoyamos, necesitamos implementar tecnología de vanguardia con los componentes de solución de seguridad más altos disponibles para proteger las llaves de firma privadas utilizadas en el sistema. Estos requisitos solo pueden cumplirse aprovechando los Módulos de Seguridad de Hardware certificados,” describió el Dr. Szőke.

MICROSEC
PASS BY ME

"Con nuestra amplia experiencia de confiar en nCipher para las soluciones de HSM, cuando se trataba de seleccionar el componente adecuado para PassBy[ME] Mobile ID no necesitábamos buscar otros proveedores; los HSMs de nCipher siempre ofrecen el más alto nivel de confianza".

"Elegimos nShield Solo de nCipher porque permite transacciones de alto volumen a nivel empresarial con tasas de transacción aceleradas."

– Dr. Sándor Szöke, subdirector de eIDAS Trust Services, Microsec

SOLUCIÓN

Microsec cuenta con más de una década de experiencia utilizando Módulos de Seguridad de Hardware (HSMs) de nCipher, descubriendo que los dispositivos ofrecen un entorno reforzado para el procesamiento criptográfico seguro, la protección y la administración de llaves, al tiempo que permiten una eficiencia operativa óptima.

El Dr. Szőke informó: “Seleccionamos los HSMs nShield Solo de nCipher para integrarlos en la identificación móvil de Microsec PassBy[ME] para proporcionar una protección integral de las llaves privadas de la PKI. La integración les permite a clientes y proveedores de servicios cumplir con los estándares transfronterizos de la UE; generar y administrar llaves criptográficas confidenciales en un entorno de hardware certificado y resistente a las manipulaciones indebidas; además de facilitar una fuente de confianza para todos los servicios digitales derivados".

Específicamente, nShield Solo de nCipher se usa para asegurar llaves dentro de un límite criptográfico cuidadosamente diseñado, que aprovecha un mecanismo de control de acceso robusto, asegurando que las llaves solo se utilicen para su propósito autorizado. Los HSMs de nCipher certifican la disponibilidad de llaves mediante el uso de funciones sofisticadas de administración, almacenamiento y redundancia para garantizar que siempre estén accesibles cuando los necesite. La información clave, tales como registros de servicio y recibos de mensajes, como prueba de entrega, se almacenan en el HSM de nCipher.

Los HSMs nShield de nCipher están certificados con el Nivel de Garantía de Evaluación de Common Criteria (EAL) 4+ y, a través de esta certificación, son reconocidos como Dispositivos de Creación de Firma Segura (SSCD) que les garantiza el cumplimiento de eIDAS (Artículo 51, Medidas Transitorias). También están certificados para FIPS 140-2 Nivel 3, el punto de referencia de seguridad más ampliamente adoptado para soluciones criptográficas en empresas gubernamentales y comerciales. Además, los HSM nShield admiten opciones de interfaz con aplicaciones que utilizan API estándar de la industria, tales como PKCS#11, OpenSSL, JCE, CAPI y CNG.

RESULTADOS

"Si bien el concepto actual se dirige específicamente al mercado europeo, creemos que es aplicable fuera de la Unión Europea debido a sus características de seguridad inherentes y al cumplimiento de los estándares globales", señaló el Dr. Szőke.

LO MEJOR DE LO MEJOR

"Las llaves criptográficas privadas que se manejan fuera del límite protegido de un HSM certificado son significativamente más vulnerables a los ataques, por lo tanto nuestra selección de nShield Solo de nCipher nos da la tranquilidad de saber que tenemos la mejor solución de hardware integrada en PassBy[ME] Mobile ID", resumió el Dr. Szőke.

INCORPORAR EL MEJOR HSM EN SU CLASE

Necesidad del negocio

- Facilitar la autorización y firma de transacciones en línea legalmente vinculantes
- Replicar el proceso de garantía física dentro de un entorno digital protegido

Necesidad tecnológica

- Proteja las llaves de firma privadas utilizadas en la solución PassBy[ME] Mobile ID
- Identificar un método para ofrecer procesamiento criptográfico reforzado
- Garantizar el cumplimiento de rigurosos estándares industriales y gubernamentales.

Solución

- HSM nShield Solo de nCipher para la administración de llaves criptográficas confidenciales en un entorno de hardware certificado y resistente a las manipulaciones indebidas

Resultado

- Brindar una fuente de confianza en una amplia gama de servicios digitales móviles
- Capacidad para llevar al mercado una solución segura de identificación móvil compatible con eIDAS
- Cumplimiento de las normas FIPS y Common Criteria
- Compatibilidad total con la API estándar de la industria

ACERCA DE NCIPHER SECURITY

nCipher Security, una empresa de Entrust Datacard, lidera el mercado de Módulos de Seguridad de Hardware (HSMs) de propósito general y con ello fortalece a las organizaciones líderes en el mundo al brindarles confianza, integridad y control sobre la información y las aplicaciones críticas de sus negocios. El rápido entorno digital de hoy en día mejora la satisfacción del cliente, proporciona una ventaja competitiva y mejora la eficiencia operativa. Y también multiplica los riesgos en seguridad. Nuestras soluciones criptográficas protegen las tecnologías emergentes, tales como la nube, el IoT, el blockchain, los pagos digitales y ayudan a cumplir con las nuevas exigencias en materia de cumplimiento. Esto lo llevamos a cabo utilizando la misma tecnología comprobada de la que dependen las organizaciones globales en la actualidad para protegerse contra las amenazas a sus datos confidenciales, las comunicaciones de red y la infraestructura empresarial. Le ofrecemos confianza para las aplicaciones críticas de su negocio, aseguramos la integridad de sus datos y le damos el control completo, hoy, mañana y en todo momento. **www.ncipher.com**