Microsec ayuda a los bancos a aprovechar el PSD2 con HSMs nShield de Entrust

Los beneficios potenciales de la banca abierta, donde la información financiera se comparte de forma segura con la aprobación del cliente, incluyen una mejor experiencia del cliente y nuevas fuentes de ingresos. Microsec desarrolló una solución basada en su experiencia técnica y en la industria, utilizando módulos de seguridad de hardware (HSMs) nShield® de Entrust, que hace que los bancos y los servicios financieros cumplan y sean competitivos. Microsec es uno de los líderes en el mercado de TI de Hungría y opera la Autoridad de Certificación e-Szignó, una de las primeras Autoridades de Certificación (CA) en Europa en proporcionar certificados calificados que cumplen con la Directiva de Servicios de Pago (UE) 2015/2366 revisada (PSD2).

Las principales actividades de Microsec incluyen:

- Mantenimiento y desarrollo del registro de sociedades de Hungría y el sistema de información de sociedades
- Proporcionar una gama completa de servicios de infraestructura de clave pública (PKI) y soluciones comerciales, incluida la formación y la consultoría profesional en Hungría, Europa central y oriental
- Prestación de servicios de confianza calificados de conformidad con el Reglamento (UE) No. 910/2014 sobre identificación electrónica y servicios de confianza para transacciones electrónicas (eIDAS)

DESAFÍO DEL NEGOCIO

PSD2 es una directiva de la UE para regular los servicios de pago y los proveedores de servicios de pago. Es un requisito de cumplimiento que busca otorgar mayor autonomía al consumidor para acceder y controlar sus datos financieros y aumenta la responsabilidad de los bancos para proteger esos datos. PSD2 también les permite a terceros crear servicios financieros nuevos e innovadores a través de APIs abiertas para las cuentas bancarias de los clientes.

PSD2 trae dos cambios importantes a la industria de pagos. Exige requisitos de seguridad más estrictos para las transacciones en línea a través de una sólida autenticación del cliente y obliga a los bancos y otras instituciones financieras a dar acceso a los proveedores de servicios de pago de terceros a las cuentas bancarias de los consumidores, si los titulares de las cuentas dan su consentimiento.

Antes de PSD2, los proveedores de servicios financieros realizaban transacciones en nombre de sus clientes utilizando su propia información de identificación. Este fue un grave riesgo de seguridad para el cliente.

Microsec

Según la PSD2, los proveedores de servicios de pago deben interactuar con los bancos utilizando sus propias identidades en lugar de las de sus clientes. Esto requiere que los bancos publiquen APIs abiertas para hacer que la información de la cuenta del cliente sea accesible para los proveedores de servicios financieros externos. Para hacer esto, los bancos necesitan implementar nuevas infraestructuras que incorporen el uso de certificados digitales para identificar y autenticar tanto al proveedor de servicios de pago externo como al banco.

CERTIFICADOS DIGITALES CUALIFICADOS

Los estándares técnicos regulatorios PSD2 requieren el uso de certificados digitales calificados, que atestiguan de manera segura la identidad del proveedor de servicios de pago (PSP) y su clave pública. Los certificados calificados permiten a los PSP, incluidos los proveedores externos (TPP) y los proveedores de servicios de pago de servicio de cuentas (ASPSP), así como a los bancos, cumplir con PSD2. Estos certificados aseguran la autenticidad, confidencialidad e integridad de la comunicación, así como también proporcionan evidencia legalmente vinculante sobre transacciones y contenidos.

Los certificados digitales calificados PSD2 deben crearse de acuerdo con eIDAS, que requiere que los proveedores de servicios de confianza (TSP) utilicen sistemas confiables y HSMs certificados para proteger su infraestructura de emisión de certificados. Los HSMs nShield están certificados según Common Criteria EAL4+ AVA_VAN.5 y ALC_FLR.2 según el perfil de protección EN 419 221-5, según el esquema NSCIB holandés. Con esta certificación Common Criteria, los TSPs de eIDAS que emiten certificados digitales, sellos de tiempo o firmas digitales pueden lograr soluciones compatibles con eIDAS.

El proveedor de servicios de confianza calificado (QTSP) emisor debe verificar todos los datos incluidos en un certificado calificado y realizar una verificación de identidad cara a cara o equivalente del PSP. Los certificados calificados deben validarse según las Listas de confianza de la UE, que contienen la lista de proveedores de servicios de confianza calificados (QTSP) en cada Estado miembro de la UE.

OPORTUNIDAD DE NEGOCIO

El requisito para el uso de certificados digitales calificados representó una oportunidad comercial para Microsec y el potencial para abrir una nueva fuente de ingresos. Microsec ya apoyaba numerosos bancos con herramientas de autenticación de clientes sólidas PSD2. El requisito PSD2 para que los bancos publiquen APIs abiertas para hacer que las cuentas de usuario sean accesibles para los TPP, significa que Microsec también puede ayudar a los bancos y a los proveedores de servicios de pago (TPP) de terceros a proteger sus comunicaciones y cumplir con los requisitos de identificación.

DESAFÍO TÉCNICO

Entrar en esta nueva línea de negocio requería que Microsec adaptara y escalara su infraestructura de clave pública (PKI) existente para satisfacer la mayor demanda requerida para respaldar a los bancos y los TPP. Microsec necesitaba crear nuevos perfiles de certificado para los certificados específicos de PSD2, desarrollar su software de AC para respaldarlos, así como especificar los procedimientos y prácticas para la emisión y gestión del nuevo tipo de certificado. También necesitaba completar la evaluación de conformidad de su nuevo servicio de confianza: emisión de certificados calificados para la autenticación de sitios web.

INFRAESTRUCTURA DE CLAVE PÚBLICA

A medida que los modelos comerciales en evolución se vuelven más dependientes de las interacciones electrónicas, que requieren de la autenticación en línea y del más estricto cumplimiento de las regulaciones de seguridad de datos, las aplicaciones comerciales de próxima generación se han vuelto más dependientes de la infraestructura de clave pública (PKI) para garantizar una alta seguridad.

Microsec

PSD2 requiere que los proveedores de servicios de pago utilicen certificados calificados como se define en la regulación eIDAS y, en la práctica, estos certificados son certificados de clave pública basados en PKI que siguen el estándar X.509. Aunque la regulación eIDAS es neutral desde el punto de vista tecnológico, actualmente PKI es la única tecnología en uso que proporciona el nivel requerido de seguridad y usabilidad.

MÓDULOS DE SEGURIDAD DE HARDWARE (HSMs)

Los HSMs son dispositivos de hardware reforzados y a prueba de manipulaciones indebidas que aseguran los procesos criptográficos al generar, proteger y gestionar claves que se utilizan para cifrar y descifrar datos y crear firmas y certificados digitales. Los HSMs se ponen a prueba, validan y certifican con los más altos estándares de seguridad, incluidos FIPS 140-2 y Common Criteria. Los HSMs les permiten a las organizaciones:

- Cumplir y superar los estándares regulatorios establecidos y emergentes para la ciberseguridad, que incluyen eIDAS, PSD2, GDPR, PCI DSS, HIPAA, etc.
- Lograr altos niveles de seguridad y confianza de datos
- Mantener altos niveles de servicio y agilidad empresarial

La regulación eIDAS exige que los TSP utilicen sistemas confiables y los estándares técnicos aplicables requieren específicamente el uso de HSMs certificados para proteger las claves privadas utilizadas para emitir los certificados digitales.

SOLUCIÓN

Microsec enfocó sus esfuerzos en desarrollar el software de la autoridad de certificación que incorporaría los nuevos atributos necesarios en los certificados digitales requeridos para las transacciones TPP y ASPSP.

El uso de HSMs nShield de Entrust para proteger las claves privadas utilizadas para emitir los certificados digitales, le permitió a Microsec cumplir con los requisitos para emitir certificados eIDAS calificados y lograr el estatus calificado que lo reconoce como QTSP en todos los estados miembros de la UE.

Debido a que Microsec ya contaba con un patrimonio sustancial de HSMs nShield de Entrust, en dos centros de datos separados geográficamente, tenía la capacidad y la agilidad para satisfacer el aumento anticipado de la demanda.

Además, Security World, el marco de gestión de claves de nShield, proporciona el control total, el respaldo sencillo, la escalabilidad y la flexibilidad que requieren los proveedores de servicios para ayudarlos a mantener una infraestructura de servicio calificada y confiable.

Microsec también implementó los procedimientos y protocolos necesarios, que incluyen:

- Verificar toda la información personal y organizativa necesaria cuando un banco, proveedor de servicios de pago o una empresa FinTech solicita un certificado
- Consultar el registro público de la autoridad nacional competente para verificar que el proveedor de servicios de pago posee la autorización necesaria de dicha autoridad competente
- Identificar el número de autorización único de la entidad solicitante, que actúa como un número de referencia o identificador único global dentro del certificado.
- Verificar para cuáles funciones está autorizada la entidad

RESULTADOS

Microsec emite certificados calificados eIDAS para autenticación de sitios web (QWAC) y sellos electrónicos (QSealC) de acuerdo con ETSI TS 119 495, que especifica un formato estándar y gestión de datos específicos de PSD2. El servicio se ofrece en todo el Espacio Económico Europeo (EEE) y Microsec ya ha emitido certificados específicos de PSD2 a solicitantes de 10 estados miembros de la UE.

Microsec

Necesidades del negocio

- Crear un servicio para ayudar a los bancos y TPP a operar dentro de las regulaciones del PSD2

Necesidades tecnológicas

- Desarrollar un nuevo negocio utilizando la infraestructura existente, desarrollando el software y los procesos necesarios para la emisión de certificados específicos del PSD2.

Soluciones

- HSMs nShield Solo de Entrust
- Procesos y software de AC personalizados
- nShield Security World de Entrust

Resultados

- Infraestructura existente, adaptada rápida y sin esfuerzo para ofrecer un nuevo servicio que aprovecha las nuevas regulaciones a nivel de la UE, lo que aumenta los ingresos generales.
- Solución HSM comprobada y confiable
- Cumplimiento de los mandatos regulatorios

Los servicios fiduciarios, el correspondiente desarrollo de software y la consultoría representan actualmente dos tercios de los ingresos de Microsec. Con la incorporación del nuevo servicio para PSP, se espera que la proporción de ingresos internacionales aumente en los próximos años.

Desde 2007 Microsec ha sido miembro de pleno derecho del Instituto Europeo de Normas de Telecomunicaciones (ETSI), reconocido mundialmente. ETSI proporciona estándares aplicables en todo el mundo para tecnologías de TI que pueden ser la base de futuros procesos económicos. Microsec participa activamente en los trabajos del Comité Técnico de Firmas e Infraestructuras Electrónicas (TC ESI) del ETSI y ha contribuido con el desarrollo de la especificación del certificado PSD2 TS 119 495.

Los productos y servicios de alto nivel de Microsec tienen el respaldo de su sistema de garantía de calidad basado en ISO 9001:2008 y un sistema de gestión de seguridad de la información aprobado por Lloyd's de acuerdo con ISO/IEC 27001:2013.

Para obtener más información sobre Microsec y sus soluciones y servicios, visite: www.microsec.com

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Hoy más que nunca, las personas exigen experiencias seguras y sin problemas, ya sea que crucen fronteras, realicen una compra, accedan a servicios de gobierno electrónico o inicien 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 en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.

Aprenda más en
entrust.com/HSM

ENTRUST

Contacte con nosotros:
HSMinfo@entrust.com