Microsec helps banks take advantage of PSD2 with Entrust nShield HSMs

The potential benefits of open banking, where financial information is shared securely with approval of the customer, include improved customer experience and new revenue streams. Microsec developed a solution based on its industry and technical expertise, using Entrust nShield® hardware security modules (HSMs), that makes banks and financial services both compliant and competitive. Microsec is a leading player in the Hungarian IT market and operates the e-Szignó Certificate Authority, one of the first Certificate Authorities (CAs) in Europe to provide qualified certificates that comply with the revised Payment Services Directive (EU) 2015/2366 (PSD2).

Microsec's main activities include:

- Maintenance and development of the Hungarian company registry and company information system
- Providing a full range of public key infrastructure (PKI) services and business solutions, including training and professional consultancy in Hungary, Central and Eastern Europe
- Providing qualified trust services in accordance with Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions (eIDAS)

BUSINESS CHALLENGE

PSD2 is an EU directive to regulate payment services and payment service providers. It is a compliance requirement that seeks to give greater autonomy to the consumer in accessing and controlling their financial data and increases the liability of banks to protect that data. PSD2 also enables third parties to create new and innovative financial services through open APIs to customers' bank accounts.

PSD2 brings two major changes to the payments industry. It mandates stronger security requirements for online transactions through strong customer authentication and it forces banks and other financial institutions to give third-party payment services providers access to consumer bank accounts, if account holders give their consent.

Before PSD2 financial services providers made transactions on behalf of their customers using the customers' own identifying information. This was a serious security risk for the customer.

Microsec

Under PSD2 payment service providers are required to interact with banks using their own identities rather than those of their customers. This requires the banks to publish open APIs to make customer account information accessible to third-party financial services providers. In order to do this, banks need to deploy new infrastructures that incorporate the use of digital certificates to identify and authenticate both the third-party payment service provider and the bank.

QUALIFIED DIGITAL CERTIFICATES

The PSD2 regulatory technical standards require the use of qualified digital certificates, which securely attest the identity of the payment service provider (PSP) and its public key. The qualified certificates allow PSPs, including third-party providers (TPPs) and account servicing payment service providers (ASPSPs), such as banks, to comply with PSD2. These certificates ensure the authenticity, confidentiality, and integrity of the communication, as well as provide legally binding evidence about transactions and contents.

The PSD2 qualified digital certificates need to be created in accordance with eIDAS, which requires Trust Service Providers (TSPs) to use trustworthy systems and certified HSMs to protect their certificate issuing infrastructure. nShield HSMs are certified to Common Criteria EAL4 + AVA_VAN.5 and ALC_FLR.2 against EN 419 221-5 Protection Profile, under the Dutch NSCIB scheme. With this Common Criteria certification, eIDAS TSPs who issue digital certificates, time stamps, or digital signatures are able to achieve eIDAS compliant solutions.

The issuing Qualified Trust Service Provider (QTSP) must verify all data included in a qualified certificate and perform face-to-face or equivalent identity verification of the PSP. Qualified certificates must be validated based on the EU Trusted Lists, which contain the list of qualified trust service providers (QTSPs) in each EU Member State.

BUSINESS OPPORTUNITY

The requirement for the use of qualified digital certificates represented a business opportunity for Microsec and the potential to open up a new revenue stream. Microsec already supported numerous banks with PSD2 strong customer authentication tools. The PSD2 requirement for banks to publish open APIs to make user accounts accessible to TPPs, meant Microsec can also support banks and third-party payment service providers (TPPs) in securing their communications and complying with the identification requirements.

TECHNICAL CHALLENGE

Entering this new line of business would require Microsec to adapt and scale its existing public key infrastructure (PKI) to meet the increased demand required to support the banks and TPPs. Microsec needed to create new certificate profiles for the PSD2-specific certificates, develop its CA software to support these as well as specify the procedures and practices for the issuance and management of the new certificate type, It would also need to complete the conformity assessment of its new trust service: issuing qualified certificates for website authentication.

PUBLIC KEY INFRASTRUCTURE

Next generation business applications are becoming increasingly reliant on PKI technology to guarantee high assurance as evolving business models become more dependent on electronic interaction requiring online authentication and compliance with stricter data security regulations.

Microsec

PSD2 requires payment service providers to use qualified certificates as defined in the eIDAS regulation, and in practice these certificates are PKI-based public key certificates following the X.509 standard. Although the eIDAS regulation is technology-neutral, currently PKI is the only technology in use which provides the required level of security and usability.

HARDWARE SECURITY MODULES (HSMs)

HSMs are hardened, tamper-resistant hardware devices that secure cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates. HSMs are tested, validated and certified to the highest security standards including FIPS 140-2 and Common Criteria. HSMs enable organizations to:

- Meet and exceed established and emerging regulatory standards for cybersecurity, including eIDAS, PSD2, GDPR, PCI DSS, HIPAA, etc.
- Achieve higher levels of data security and trust
- Maintain high service levels and business agility

The eIDAS regulation mandates TSPs use trustworthy systems, and the applicable technical standards specifically require the use of certified HSMs to protect the private keys used to issue the digital certificates.

SOLUTION

Microsec focused its efforts on developing the certificate authority software that would incorporate the necessary new attributes into the digital certificates required for the TPP and ASPSP transactions.

Using Entrust nShield HSMs to protect the private keys used to issue the digital certificates enabled Microsec to meet the requirements to issue qualified eIDAS certificates and achieve the qualified status that sees it recognized as a QTSP in all EU member states.

Because Microsec already had in place a substantial estate of Entrust nShield HSMs, in two geographically separated data centers, it had the capacity and agility to meet the anticipated increase in demand.

In addition, Security World, the nShield key management framework, provides the full control, easy back-up, scalability and flexibility required by service providers to help them maintain a qualified and reliable service infrastructure.

Microsec also implemented the necessary procedures and protocols, including:

- Checking all the personal and organizational information needed when a bank, payment service provider, or a FinTech company applies for a certificate
- Consulting the public register of the national competent authority to verify that the payment service provider holds the necessary authorization from that competent authority
- Identifying the applying entity's unique authorization number, which acts as a globally unique reference number or identifier within the certificate
- Verifying which roles the entity is authorized to have

RESULTS

Microsec issues eIDAS qualified certificates for website authentication (QWAC) and electronic seals (QSealC) according to ETSI TS 119 495, which specifies a standard format and management of PSD2-specific data. The service is offered throughout the European Economic Area (EEA), and Microsec has already issued PSD2-specific certificates to applicants from 10 EU member states.

Microsec

Business need

- Create a service to help banks and TPPs operate within PSD2 regulations

Technology need

- Create a new business using existing infrastructure, by developing the software and processes needed for the PSD2-specific certificate issuance

Solutions

- Entrust nShield Solo HSMs
- Custom CA software and processes
- Entrust nShield Security World

Results

- Existing infrastructure, quickly and effortlessly adapted to offer a new service that takes advantage of new EU-wide regulations, adding to overall revenues.
- Proven, trusted and dependable HSM solution
- Compliance with regulatory mandates

Trust services, the corresponding software development, and consultancy currently represent two-thirds of Microsec's revenue. With the addition of the new service for PSPs, it is expected that the proportion of international revenue will increase over the coming years.

Since 2007 Microsec has been a full member of the globally recognized European Telecommunications Standards Institute (ETSI). ETSI provides worldwide applicable standards for IT technologies which can be the basis for future economic processes. Microsec actively participates in the work of the ETSI Technical Committee for Electronic Signatures and Infrastructures (TC ESI), and has contributed to the development of the PSD2 certificate specification TS 119 495.

Microsec's high standards products and services are backed by its quality assurance system based on ISO 9001:2008 and an information security management system approved by Lloyd's in line with ISO/IEC 27001:2013.

To learn more about Microsec and its solutions and services visit: www.microsec.com

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com