A Microsec ajuda os bancos a tirar proveito do PSD2 com os HSMs Entrust nShield

Os benefícios potenciais do serviço bancário aberto, em que as informações financeiras são compartilhadas com segurança com a aprovação do cliente, incluem uma melhor experiência do cliente e novos fluxos de receita. A Microsec desenvolveu uma solução baseada em sua indústria e experiência técnica, usando módulos de segurança de hardware Entrust nShield® (HSMs), que torna os bancos e serviços financeiros compatíveis e competitivos. A Microsec é uma empresa líder no mercado de TI húngaro e opera a Autoridade de Certificação e-Szignó, uma das primeiras Autoridades de Certificação (CAs) na Europa a fornecer certificados qualificados em conformidade com a Diretiva de Serviços de Pagamento (UE) revisada 2015/2366 (PSD2)

As principais atividades da Microsec incluem:

- Manutenção e desenvolvimento do sistema de registro e informação empresarial húngaro
- Fornecimento de uma gama completa de serviços de infraestrutura de chave pública (PKI) e soluções de negócios, incluindo treinamento e consultoria profissional na Hungria, Europa Central e Oriental
- Prestar serviços de confiança qualificados de acordo com o Regulamento (UE) n.º 910/2014 sobre identificação eletrônica e serviços de confiança para transações eletrônicas (eIDAS)

DESAFIO DO NEGÓCIO

PSD2 é uma diretiva da UE para regular os serviços de pagamento e os provedores de serviços de pagamento. É um requisito de compliance que visa dar maior autonomia ao consumidor no acesso e controle de seus dados financeiros e aumenta a responsabilidade dos bancos na proteção desses dados. O PSD2 também permite que terceiros criem serviços financeiros novos e inovadores por meio de APIs abertas para contas bancárias de clientes.

O PSD2 traz duas mudanças importantes para o setor de pagamentos. Ele impõe requisitos de segurança mais rígidos para transações on-line por meio de sólida autenticação do cliente e força os bancos e outras instituições financeiras a fornecer aos provedores de serviços de pagamento a terceiros acesso às contas bancárias do consumidor, se os titulares das contas derem consentimento.

Antes do PSD2, os provedores de serviços financeiros faziam transações em nome de seus clientes usando as próprias informações de identificação dos clientes. Esse era um sério risco de segurança para o cliente.

Microsec

De acordo com o PSD2, os provedores de serviços de pagamento são obrigados a interagir com os bancos usando suas próprias identidades em vez das de seus clientes. Isso exige que os bancos públicos APIs abertos para tornar as informações da conta do cliente atendidos a provedores de serviços financeiros terceirizados. Para fazer isso, os bancos precisam implantar novas infraestruturas que incorporem o uso de certificados digitais para identificar e autenticar tanto o provedor de serviços de pagamento terceirizado quanto ao banco.

CERTIFICADOS DIGITAIS QUALIFICADOS

Os padrões técnicos regulatórios do PSD2 exigem o uso de certificados digitais qualificados, que atestam com segurança a identidade do provedor de serviços de pagamento (PSP) e sua chave pública. Os certificados qualificados permitem que PSPs, incluindo provedores terceirizados (TPPs) e provedores de serviços de pagamento de serviços de contas (ASPSPs), como bancos, cumpram o PSD2. Esses certificados garantem a autenticidade, confidencialidade e integridade da comunicação, bem como fornecem evidências legalmente vinculativas sobre transaçõese conteúdos.

Os certificados digitais qualificados PSD2 precisam ser criados de acordo com o eIDAS, o que exige que os provedores de serviços confiáveis (TSPs) usem sistemas confiáveis e HSMs certificados para proteger sua infraestrutura de emissão de certificados. Os HSMs nShield são certificados pelos Critérios Comuns EAL4 + AVA_VAN.5 e ALC_FLR.2 em relação ao Perfil de Proteção EN 419 221-5, sob o esquema NSCIB holandês. Com esta certificação Common Criteria, os eIDAS TSPs que emitem certificados digitais, time stamps ou assinaturas digitais podem obter soluções compatíveis com eIDAS.

O Provedor de Serviço de Confiança Qualificado (QTSP) emissor deve verificar todos os dados incluídos em um certificado qualificado e realizar uma verificação de identidade cara a cara ou equivalente do PSP. Os certificados qualificados devem ser validados com base nas listas de confiança da UE, que contêm a lista de fornecedores de serviços de confiança qualificados (QTSPs) em cada Estado-Membro da UE.

OPORTUNIDADE DE NEGÓCIOS

A exigência de uso de certificados digitais qualificados representou uma oportunidade de negócios para a Microsec e o potencial de abrir um novo fluxo de receita. A Microsec já apoiou vários bancos com ferramentas de autenticação de cliente PSD2 fortes. O requisito PSD2 para que os bancos publiquem APIs abertas para tornar as contas de usuário acessíveis aos TPPs, significa que a Microsec também pode oferecer suporte a bancos e provedores de serviços de pagamento (TPPs) terceirizados na proteção de suas comunicações e no cumprimento dos requisitos de identificação.

DESAFIO TÉCNICO

A entrada nessa nova linha de negócios exigiria que a Microsec adaptasse e escalasse sua infraestrutura de chave pública (PKI) existente para atender à crescente demanda necessária para dar suporte aos bancos e TPPs. A Microsec precisava criar novos perfis de certificado para os certificados específicos de PSD2, desenvolver seu software CA para apoiá-los, bem como especificar os procedimentos e práticas para a emissão e gestão do novo tipo de certificado. Também precisaria completar a avaliação de conformidade de seu novo serviço de confiança: emissão de certificados qualificados para autenticação de sites.

INFRAESTRUTURA DE CHAVE PÚBLICA

Os aplicativos de negócios da próxima geração estão se tornando cada vez mais dependentes da tecnologia PKI para garantir alta segurança, pois os modelos de negócios em evolução se tornam mais dependentes da interação eletrônica que exige autenticação online e conformidade com regulamentos de segurança de dadosmais rígidos.

Microsec

PSD2 exige que os provedores de serviços de pagamento usem certificados qualificados conforme definido no regulamento eIDAS e, na prática, esses certificados são certificados de chave pública baseados em PKI seguindo o padrão X.509. Embora a regulamentação eIDAS seja neutra em termos de tecnologia, atualmente a PKI é a única tecnologia em uso que oferece o nível necessário de segurança e usabilidade.

MÓDULOS DE SEGURANÇA DE HARDWARE (HSMs)

HSMs são dispositivos de hardware reforçados e resistentes a adulterações que protegem os processos criptográficos gerando, protegendo e gerenciando as chaves usadas para criptografar e descriptografar dados e criar assinaturas digitais e certificados. Os HSMs são testados, validados e certificados de acordo com os mais altos padrões de segurança, incluindo FIPS 140-2 e Common Criteria. HSMs permitem que as organizações:

- Atender e superar os padrões regulatórios estabelecidos e emergentes para segurança cibernética, incluindo eIDAS, PSD2, GDPR, PCI DSS, HIPAA, etc.
- Obter níveis mais altos de segurança de dados e confiança
- Manter serviços de alto nível e agilidade de negócios

O regulamento eIDAS exige que os TSPs usem sistemas confiáveis e os padrões técnicos aplicáveis exigem especificamente o uso de HSMs certificados para proteger as chaves privadas usadas para emitir os certificados digitais.

SOLUÇÃO

A Microsec concentrou seus esforços no desenvolvimento do software de autoridade de certificação que incorporaria os novos atributos necessários aos certificados digitais exigidos para as transações TPP e ASPSP.

O uso de HSMs Entrust nShield para proteger as chaves privadas usadas para emitir os certificados digitais permitiu que a Microsec atendesse aos requisitos para emitir certificados eIDAS qualificados e atingir o status de qualificado que o considera reconhecido como um QTSP em todos os estados membros da UE.

Como a Microsec já possuía um conjunto substancial de HSMs Entrust nShield, em dois data centers separados geograficamente, ela tinha capacidade e agilidade para atender ao aumento previsto da demanda.

Além disso, o Security World, a estrutura de gerenciamento de chaves do nShield, oferece controle total, backup fácil, escalabilidade e flexibilidade exigidas pelos provedores de serviço para ajudá-los a manter uma infraestrutura de serviço qualificada e confiável.

A Microsec também implementou os procedimentos e protocolos necessários, incluindo:

- Verificar todas as informações pessoais e organizacionais necessárias quando um banco, provedor de serviços de pagamento ou uma empresa FinTech solicita um certificado
- Consulta ao registo público da autoridade nacional competente para verificar se o prestador de serviços de pagamento possui a autorização necessária dessa autoridade competente
- Identificar o número de autorização exclusivo da entidade solicitante, que atua como um número de referência globalmente exclusivo ou identificador dentro do certificado
- Verificar quais funções a entidade está autorizada a ter

RESULTADOS

A Microsec emite certificados qualificados eIDAS para autenticação de sites (QWAC) e selos eletrônicos (QSealC) de acordo com ETSI TS 119 495, que especifica um formato padrão e gerenciamento de dados específicos do PSD2. O serviço é oferecido em todo o Espaço Econômico Europeu (EEE), e a Microsec já emitiu certificados específicos do PSD2 para candidatos de 10 estados membros da UE.

Microsec

Necessidade de negócios

- Crie um serviço para ajudar os bancos e TPPs a operar dentro dos regulamentos PSD2

Necessidade de tecnologia

- Crie um novo negócio usando a infraestrutura existente, desenvolvendo o software e os processos necessários para a emissão do certificado específico do PSD2

Soluções

- HSMs Entrust nShield Solo
- Software e processos CA personalizados
- Security World nShield da Entrust

Resultados

- Infraestrutura existente, adaptada com rapidez e sem esforço para oferecer um novo serviço que tira proveito de novas regulamentações em toda a UE, aumentando as receitas globais.
- Solução HSM comprovada, confiável e segura
- Conformidade com mandatos regulatórios

Os serviços de confiança, o desenvolvimento de software correspondente e a consultoria representam atualmente dois terços da receita da Microsec. Com a adição do novo serviço para PSPs, espera-se que a proporção da receita internacional aumente nos próximos anos.

Desde 2007, a Microsec é membro titular do Instituto Europeu de Normas de Telecomunicações (ETSI), reconhecido mundialmente. O ETSI fornece padrões aplicáveis em todo o mundo para tecnologias de TI que podem ser a base para processos econômicos futuros. A Microsec participa ativamente dos trabalhos do Comitê Técnico de Assinaturas Eletrônicas e Infraestruturas do ETSI (TC ESI) e contribuiu para o desenvolvimento da especificação do certificado PSD2 TS 119 495.

Os produtos e serviços de alto padrão da Microsec são respaldados por seu sistema de garantia de qualidade baseado na ISO 9001: 2008 e um sistema de gestão de segurança da informação aprovado pela Lloyd's em linha com a ISO / IEC 27001: 2013.

Para saber mais sobre a Microsec e suas soluções e serviços, visite: www.microsec.com

SOBRE A ENTRUST

A Entrust mantém o mundo movendo-se com segurança, permitindo identidades, pagamentos e proteção de dados confiáveis. Hoje, mais do que nunca, as pessoas exigem experiências seguras e contínuas, quer estejam cruzando fronteiras, fazendo uma compra, acessando serviços de governo eletrônico ou entrando em redes corporativas. A Entrust oferece uma gama incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiáveis do mundo confiem em nós.

Saiba mais em
entrust.com/HSM

ENTRUST

Entre em contato conosco:
HSMinfo@entrust.com