Microsec unterstützt Banken mit nShield HSM von Entrust bei der Umsetzung von PSD2

Zu den möglichen Vorteilen von Open Banking, bei dem Finanzinformationen mit Erlaubnis des Kunden sicher weitergegeben werden, gehören die verbesserte Kundenerfahrung und das Erschließen neuer Einnahmequellen. Mithilfe der nShield®-Hardware-Sicherheitsmodule (HSM) von Entrust hat Microsec auf Grundlage seiner Branchenkenntnis und seines Fachwissens eine Lösung entwickelt, die die Wettbewerbsfähigkeit von Banken und Finanzdienstleistern fördert und sie bei der Einhaltung von Vorgaben unterstützt. Microsec ist ein führender Anbieter auf dem ungarischen IT-Markt und Betreiber von e-Szignó, einer der ersten Zertifizierungsstellen (Certificate Authorities, CAs) in Europa, die qualifizierte Zertifikate ausstellt, die der überarbeiteten Zahlungsdiensterichtlinie (EU) 2015/2366 (Payment Services Directive 2, PSD2) entsprechen.

Zu den hauptsächlichen Aktivitäten von Microsec gehören:

- Pflege und Entwicklung des ungarischen Unternehmensregisters und Unternehmensinformationssystems
- Bereitstellung umfassender Public-Key-Infrastructure-Dienste (PKI-Dienste) und Unternehmenslösungen einschließlich Schulung und Fachberatung in Ungarn sowie in Mittel- und Osteuropa.
- Bereitstellung qualifizierter Vertrauensdienste gemäß der Verordnung (EU) 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS)

GESCHÄFTLICHE HERAUSFORDERUNG

PSD2 ist eine Richtlinie der EU für Zahlungsdienste und Zahlungsdienstleister. Diese Vorgaben sollen dem Verbraucher mehr Eigenständigkeit beim Zugriff auf ihre Finanzdaten sowie bei deren Kontrolle gewährleisten und die Haftung der Banken für den Schutz dieser Daten erhöhen. Außerdem erlaubt PSD2 Dritten, mithilfe offener API zu den Bankkonten ihrer Kunden neue und innovative Finanzdienstleistungen zu entwickeln.

PSD2 bringt zwei große Veränderungen für die Zahlungsindustrie mit sich. Sie fordert strengere Sicherheitsauflagen für Online-Transaktionen durch stärkere Kundenauthentifizierung und zwingt Banken und andere Finanzinstitutionen, Drittanbietern von Zahlungsdiensten Zugang zu den Bankkonten von Verbrauchern zu gewähren – die Zustimmung des Kontoinhabers vorausgesetzt.

Bisher führten Anbieter von PSD2-Finanzdienstleistungen Transaktionen im Auftrag ihrer Kunden mit deren personenbezogenen Daten aus. Das stellte ein ernstes Sicherheitsrisiko für den Kunden dar.

Microsec

PSD2 schreibt vor, dass Anbieter von Zahlungsdiensten bei der Interaktion mit Banken statt der personenbezogenen Daten des Kunden ihre eigenen Identitäten verwenden. Dazu müssen die Banken offene API bereitstellen, damit die Kontodaten des Kunden für Drittanbieter von Zahlungsdiensten zugänglich sind. Zu diesem Zweck benötigt die Bank neue Infrastrukturen, die auch die Verwendung digitaler Zertifikate zur Identifizierung und Authentifizierung sowohl des Drittanbieters von Zahlungsdiensten als auch der Bank umfassen.

QUALIFIZIERTE DIGITALE ZERTIFIKATE

Die technischen Normen der PSD2 verlangen die Verwendung qualifizierter digitaler Zertifikate, die die Identität des Zahlungsdienstleisters (PSP) und seines öffentlichen Schlüssels sicher belegen. Diese qualifizierten Zertifikate ermöglichen es den PSPs, darunter auch Drittanbieter (TPPs) und kontoführende Zahlungsdienstleister (ASPSPs), die PSD2 einzuhalten. Sie garantieren die Authentizität, Vertraulichkeit und Integrität der Kommunikation und sind ein rechtlich bindender Nachweis der Transaktionen und der entsprechenden Inhalte.

Die qualifizierten digitalen Zertifikate gemäß PSD2 müssen entsprechend der eIDAS ausgestellt sein. Diese verlangt, dass Anbieter von Vertrauensdiensten (TSPs) zum Schutz ihrer Infrastruktur, in der die Zertifikate ausgestellt werden, vertrauenswürdige Systeme und zertifizierte HSM verwenden. nShield HSM sind laut Common Criteria EAL4 + AVA_VAN.5 und ALC_FLR.2 nach den Vorgaben des Schutzprofils EN 419 221-5 P gemäß dem niederländischen NSCIB-System zertifiziert. Dank dieser Zertifizierung laut Common Criteria können TSPs, die digitale Zertifikate, Zeitstempel oder digitale Signaturen ausstellen, eIDAS-konforme Lösungen anbieten.

Der ausgebende qualifizierte Vertrauensdienst (QTSP) muss alle Daten eines digitalen Zertifikats prüfen und eine persönliche oder gleichwertige Überprüfung der Identität des PSP vornehmen. Qualifizierte Zertifikate müssen mit den Vertrauenslisten der EU verglichen werden, die alle qualifizierten Anbieter von Vertrauensdiensten enthalten.

GESCHÄFTSMÖGLICHKEIT

Die verpflichtende Verwendung qualifizierter digitaler Zertifikate stellt eine Geschäftsmöglichkeit für Microsec dar und eröffnet den Zugang zu potenziellen neuen Einnahmequellen. Microsec hat bereits zahlreiche Banken mit starken Tools zur Authentifizierung von Kunden gemäß PSD2 unterstützt. PSD2 verlangt von den Banken, dass diese offene API bereitstellen, damit TPPs auf die Konten ihrer Kunden zugreifen können. Das bedeutet, dass Microsec auch Banken und Drittanbieter von Zahlungsdienstleistungen (TPPs) bei der Sicherung ihrer Kommunikation und bei der Einhaltung der Identifikationsanforderungen unterstützen kann.

TECHNISCHE PROBLEMSTELLUNG

Dieses neue Geschäftsfeld erfordert, dass Microsec seine bestehende Public-Key-Infrastructure (PKI) entsprechend der steigenden Nachfrage von Banken und TPPs anpasst und skaliert. Microsec musste neue Profile für PSD2-spezifische Zertifikate und eine entsprechende unterstützende CA-Software entwickeln sowie die Verfahren und Prozesse für die Ausgabe und Verwaltung des neuen Zertifikattyps festlegen. Außerdem mussten sie die Konformitätsprüfung ihres neuen Vertrauensdienstes abschließen: die Ausgabe qualifizierter Zertifikate für die Authentifizierung von Websites.

PUBLIC KEY INFRASTRUCTURE

Um höchste Sicherheit garantieren zu können, sind Geschäftsanwendungen der nächsten Generation verstärkt auf PKI-Technologie angewiesen, da zeitgemäße Geschäftsmodelle mehr und mehr von elektronischer Interaktion abhängig sind, die Online-Authentifizierung und die Einhaltung strenger Datensicherheitsvorschriften erfordern.

Microsec

PSD2 verlangt, dass Zahlungsdienstleister qualifizierte Zertifikate gemäß der eIDAS-Verordnung verwenden. In der Praxis handelt es sich hierbei um PKI-basierte Public-Key-Zertifikate laut der Norm X.509. Obwohl die eIDAS-Verordnung keine bestimmte Technologie vorschreibt, ist PKI derzeit die einzige verwendete Technologie, die das geforderte Maß an Sicherheit und Benutzerfreundlichkeit bietet.

HARDWARE-SICHERHEITSMODULE (HSM)

HSM sind robuste, manipulationssichere Hardware-Geräte, die kryptographische Prozesse sichern. Dies erfolgt durch die Erstellung, den Schutz und die Verwaltung von Schlüsseln, die zur Ver- und Entschlüsselung von Daten sowie zur Erstellung digitaler Signaturen und Zertifikate dienen. HSM werden getestet, validiert und zertifiziert, sodass sie den höchsten Sicherheitsstandards einschließlich FIPS 140-2 und Common Criteria entsprechen. Mithilfe von HSM können Unternehmen:

- bestehende und neue gesetzliche Normen für Cyber-Sicherheit wie eIDAS, PSD2, DSGVO, PCI DSS, HIPAA etc. einhalten und übertreffen.
- einen höheren Grad an Datensicherheit und Vertrauen erreichen
- ein hohes Serviceniveau und wirtschaftliche Agilität aufrechterhalten

Die eIDAS-Verordnung verlangt, dass TSPs vertrauenswürdige Systeme nutzen, und die geltenden technischen Normen schreiben insbesondere die Verwendung zertifizierter HSM vor, um private Schlüssel zu schützen, die zur Ausgabe von digitalen Zertifikaten verwendet werden.

LÖSUNG

Microsec konzentrierte seine Bemühungen auf die Entwicklung eine Software für Zertifizierungsstellen, welche die neuen, für TPP- und ASPSP-Transaktionen erforderlichen Attribute umfasst.

Zum Schutz der privaten Schlüssel für die Ausgabe digitaler Zertifikate setzte Microsec auf nShield HSM von Entrust. Dadurch waren sie in der Lage, die entsprechenden Vorgaben der eIDAS zu erfüllen und damit auch die Voraussetzungen, um in allen EU-Mitgliedsstaaten als QTSP anerkannt zu werden.

Da Microsec bereits eine beträchtliche Zahl an nShield HSM von Entrust in zwei geografisch getrennten Rechenzentren besaß, verfügten sie über die Kapazität und die Agilität, mit der erwarteten Steigerung der Nachfrage Schritt halten zu können.

Außerdem bietet Security World, die Schlüsselverwaltungsarchitektur von nShield, volle Kontrolle, einfaches Back-up, Skalierbarkeit und Flexibilität, damit Dienstanbieter eine qualifizierte und zuverlässige Dienstinfrastruktur aufrechterhalten können.

Microsec hat zudem die erforderlichen Verfahren und Protokolle eingeführt, darunter:

- Überprüfung der gesamten personen- und unternehmensbezogenen Informationen, die erforderlich sind, wenn eine Bank, ein Zahlungsdienstleister oder ein FinTech-Unternehmen ein Zertifikat beantragt.
- Prüfung im öffentlichen Register der zuständigen nationalen Behörde, ob der Zahlungsdienstleister die erforderlich Genehmigung dieser Behörde besitzt.
- Identifikation der individuellen Autorisierungsnummer, die weltweit als eindeutige Referenznummer oder ID innerhalb des Zertifikats dient.
- Überprüfung, für welche Rolle das Unternehmen autorisiert ist.

ERGEBNISSE

Microsec stellt qualifizierte Zertifikate gemäß eIDAS für die Authentifizierung von Websites (QWAC) und elektronische Siegel (QSealC) laut ETSI TS 119 495 aus, welche ein Standardformat und eine Standardverwaltung für PSD2-bezogene Daten festlegen. Diese Dienstleistung wird im gesamten Europäischen Wirtschaftsraum (EWG) angeboten, und Microsec hat bereits PSD2-bezogene Zertifikate an Antragsteller aus zehn EU-Mitgliedsstaaten ausgestellt.

Microsec

Geschäftliche Anforderungen

- Entwicklung eines Dienstes, der Banken und TPPs bei der Einhaltung der PSD2-Richtlinien unterstützt

Technische Anforderungen

- Aufbau eines neuen Geschäftsbereichs unter Verwendung bestehender Infrastruktur durch Entwicklung der für die Ausstellung von PSD2-bezogenen Zertifikaten erforderlichen Software und Prozesse

Lösungen

- nShield-Solo-HSM von Entrust
- Individuell anpassbare CA-Software und Prozesse
- nShield Security World von Entrust

Ergebnisse

- Eine bestehende Infrastruktur wurde schnell und problemlos angepasst. Das daraus entstehende neue Serviceangebot profitiert von neuen EU-weiten Verordnungen und trägt zum Gesamtumsatz bei.
- Erprobte, vertrauenswürdige und zuverlässige HSM-Lösung
- Einhaltung regulatorischer Vorgaben

Vertrauensdienste, die entsprechende Softwareentwicklung sowie Beratung machen derzeit zwei Drittel des Umsatzes von Microsec aus. Dank dieses neuen Dienstes für PSPs wird erwartet, dass der Anteil des internationalen Umsatzes in den kommenden Jahren steigen wird.

Seit 2007 ist Microsec vollwertiges Mitglied des global anerkannten European Telecommunications Standards Institute (ETSI). ETSI stellt weltweit geltende Normen für IT-Technologie bereit, die Grundlage für zukünftige Wirtschaftsprozesse sein können. Microsec ist aktiv an der Arbeit des Technical Committee for Electronic Signatures and Infrastructures (TC ETSI) beteiligt und hat an der Entwicklung der PSD2-Zertifizierungsnorm TS 119 495 mitgewirkt.

Die hochwertigen Produkte und Dienstleistungen von Microsec werden von ihrem Qualitätssicherungssystem auf Grundlage von ISO 9001:2008 und einem von Lloyd's anerkannten System zur Verwaltung der Informationssicherheit gemäß ISO/IEC 27001:2013 gestützt.

Weitere Informationen zu Microsec und seinen Lösungen finden sie auf www.microsec.com.

ÜBER ENTRUST

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com