Entrust nShield HSM으로 은행의 PSD2 활용을 지원하는 Microsec

고객의 승인을 받아 재무 정보를 안전하게 공유하는 오픈 뱅킹의 잠재적인 장점으로는 향상된 고객 경험과 새로운 수익 흐름이 있습니다. Microsec은 Entrust nShield®HSM(하드웨어 보안 모듈)을 사용하여 업계 및 기술 전문 지식을 기반으로 하는 솔루션을 개발하여 은행과 금융 서비스가 규정을 준수하고 경쟁력을 갖출 수 있도록 했습니다. Microsec은 헝가리 IT 시장의 선두 주자이며 개정된 결제서비스지침(EU) 2015/2366(PSD2)을 준수하는 적격 인증서를 제공하는 유럽 최초의 CA(인증 기관) 중 하나인 e-Szignó CA를 운영합니다.

Microsec의 주요 활동은 다음과 같습니다.

- 헝가리 회사 등록 및 회사 정보 시스템의 유지 관리 및 개발
- 헝가리, 중유럽 및 동유럽의 교육 및 전문 컨설팅을 포함, 모든 범위의 PKI(공개 키 인프라) 서비스 및 비즈니스 솔루션 제공
- eIDAS(전자 거래를 위한 전자 식별 및 신뢰 서비스)에 대한 규정(EU) No 910/2014에 따라 적격 신뢰 서비스 제공

비즈니스적 난관

PSD2는 결제 서비스 및 결제 서비스 제공 업체를 규제하는 EU 지침입니다. 소비자가 금융 데이터를 이용하고 제어하는 데 대해 더 큰 자율성을 부여하고 해당 데이터를 보호해야 하는 은행의 책임을 높이는 것이 규정 준수 요구 사항입니다. 또한 PSD2는 제3자가 고객의 은행 계좌에 대한 개방형 API를 통해 새롭고 혁신적인 금융 서비스를 만들 수 있도록 합니다.

PSD2는 결제 산업에 두 가지 주요 변화를 가져왔습니다. 온라인 거래를 위한 보안 요구 사항이 강력한 고객 인증을 통해 의무적으로 강화되어야 하며, 은행 및 기타 금융 기관은 계좌 소유자가 동의하는 경우 제3자 결제 서비스 제공업체가 소비자 은행 계좌에 액세스할 수 있게 해야 합니다.

PSD2 금융 서비스 시행 전에는 제공업체가 고객을 대신해 고객 자신의 식별 정보를 사용하여 거래를 했습니다. 이것은 고객에게 심각한 보안 위험이었습니다.

Microsec

PSD2 결제 서비스 시행 후 제공업체는 고객이 아닌 자신의 ID를 사용하여 은행과 상호 작용해야 합니다. 이를 위해서는 은행이 개방형 API를 게시하여 타사 금융 서비스 제공업체가 고객 계정 정보에 액세스할 수 있도록 해야 합니다. 이를 위해 은행은 디지털 인증서 사용을 통합하는 새로운 인프라를 구축하여 제3자 결제 서비스 제공업체와 은행을 모두 식별하고 인증해야 합니다.

공인 디지털 인증서

PSD2 규제 기술 표준은 결제 서비스 제공업체(PSP) 및 공개 키의 신원을 안전하게 증명하는 적격 디지털 인증서를 사용해야 합니다. PSP는 적격 인증서를 통해 PSD2를 준수할 수 있습니다. PSP는 타사 공급자(TPP) 및 은행과 같은 계정 서비스 결제 서비스 공급자(ASPSP)를 포함합니다. 이러한 인증서는 통신의 신뢰성, 기밀성 및 무결성을 보장할 뿐만 아니라 트랜잭션 및 그 내용에 대한 법적 구속력이 있는 증거가 됩니다.

PSD2 인증 디지털 인증서는 eIDAS에 따라 생성되어야 하며, TSP(신뢰 서비스 제공자)는 인증서 발급 인프라를 보호하기 위해 신뢰할 수 있는 시스템과 인증된 HSM을 사용해야 합니다. nShield HSM은 네덜란드 NSCIB 체계에 따라 EN 419 221-5 보호 프로필에 대해 CC(Common Criteria) EAL4 + AVA_VAN.5 및 ALC_FLR.2 인증을 받았습니다. 이 CC 인증을 통해 디지털 인증서, 타임스탬프 또는 디지털 서명을 발급하는 eIDAS TSP는 eIDAS 준수 솔루션을 얻을 수 있습니다.

발급하는 QTSP(적격 신뢰 서비스 공급자)는 적격 인증서에 포함된 모든 데이터를 확인하고 PSP의 대면 또는 동등한 신원 확인을 수행해야 합니다. 적격 인증서는 각 EU 회원국의 QTSP 목록이 포함된 EU 신뢰 목록을 기반으로 검증되어야 합니다.

비즈니스 기회

적격 디지털 인증서 사용에 대한 요구 사항은 Microsec의 비즈니스 기회와 새로운 수익 흐름을 열 수 있는 가능성이 되었습니다. Microsec은 이미 강력한 PSD2 고객 인증 도구로 수많은 은행을 지원한 바 있습니다. 은행이 TPP에 액세스할 수 있는 사용자 계정을 만들기 위해 개방형 API를 게시해야 한다는 PSD2 요구 사항에 따라, Microsec 역시 은행 및 TPP(제3자 결제 서비스 공급자)가 통신을 보호하고 식별 요구 사항을 준수하는 것을 지원할 수 있게 되었습니다.

기술적 난관

이 새로운 비즈니스 라인에 진입하기 위해 Microsec은 은행 및 TPP를 지원하는 데 필요한 증가하는 수요를 충족할 수 있도록 기존의 PKI(공개 키 인프라)를 조정하고 확장해야 했습니다. Microsec은 PSD2 준수 인증서에 대한 새 인증서 프로필을 만들고 이를 지원하기 위한 CA 소프트웨어를 개발하고 새 인증서 유형의 발급 및 관리를 위한 절차와 관행을 지정해야 했습니다. 또한 자사의 새 신뢰 서비스인 웹사이트 인증용 적격 인증서 발급에 대한 적합성 평가를 완료해야 했습니다.

공개 키 인프라

진화 중인 비즈니스 모델이 온라인 인증 및 더 엄격한 데이터 보안 규정 준수를 요구하는 전자 상호 작용에 점점 더 많이 의존함에 따라 차세대 비즈니스 애플리케이션은 높은 보증을 보장하기 위해 PKI(공개 키 인프라)에 더욱 의존하게 되었습니다.

Microsec

PSD2는 결제 서비스 제공업체가 eIDAS 규정에 정의된 적격 인증서를 사용할 것을 요구하며, 실제로 이러한 인증서는 X.509 표준을 따르는 PKI 기반 공개 키 인증서입니다. eIDAS 규정은 기술 중립적이지만 현재 PKI는 필요한 수준의 보안과 유용성을 제공하는 유일한 기술입니다.

HSM(하드웨어 보안 모듈)

HSM은 데이터를 암호화 및 해독하고 디지털 서명 및 인증서를 생성하는 데 사용되는 키를 생성, 보호 및 관리하여 암호화 프로세스를 보호하는 강화된 변조 방지 하드웨어 장치입니다. HSM은 FIPS 140-2 및 CC(Common Criteria)를 포함한 가장 높은 보안 기준에 맞추어 테스트, 검증 및 인증되었습니다. HSM을 통해 조직은 다음과 같은 것을 할 수 있습니다.

- eIDAS, PSD2, GDPR, PCI DSS, HIPAA 등 사이버 보안에 대한 기존 및 새로운 규제 기준을 충족 및 능가
- 더 높은 수준의 데이터 보안 및 신뢰 달성
- 높은 수준의 서비스 및 비즈니스 민첩성 유지

eIDAS 규정에 따라 TSP는 신뢰할 수 있는 시스템을 사용해야 하며, 해당 기술 표준은 특히 디지털 인증서 발급에 사용되는 개인 키를 보호하기 위해 인증되는 HSM을 사용해야 합니다.

솔루션

Microsec은 TPP 및 ASPSP 트랜잭션에 필요한 디지털 인증서에 필요한 새 속성을 통합하는 인증 기관 소프트웨어 개발에 집중했습니다.

Microsec은 Entrust nShield HSM을 사용하여 디지털 인증서를 발급하는 데 사용되는 개인 키를 보호함으로써 적격 eIDAS 인증서 발급에 필요한 요구 사항을 충족하고 모든 EU 회원국에서 QTSP로 인정되는 적격 상태를 달성할 수 있었습니다.

Microsec은 이미 지리적으로 분리된 두 데이터 센터에 Entrust nShield HSM의 상당한 자산을 보유하고 있었기 때문에, 예상되는 수요 증가를 충족할 수 있는 용량과 민첩성을 갖추고 있었습니다.

또한 nShield 키 관리 프레임워크인 Security World는 서비스 제공업체가 적격하고 신뢰할 수 있는 서비스 인프라를 유지하는 데 필요한 완전한 제어, 간편한 백업, 확장 성 및 유연성을 제공합니다.

Microsec은 다음을 포함하여 필요한 절차 및 프로토콜도 구현했습니다.

- 은행, 결제 서비스 제공업체, 핀테크 회사에서 인증서 신청시 필요한 모든 개인 및 조직 정보 확인
- 지불 서비스 제공자가 해당 관할 기관으로부터 필요한 권한을 보유하고 있는지 확인하기 위해 국가 관할 기관의 공적 등록부에 문의
- 인증서 내에서 전역적으로 고유한 참조 번호 또는 식별자 역할을 하는 신청 실체의 고유 인증 번호 식별
- 그 실체에게 보유 권한이 있는 역할이 무엇인지 확인

결과

Microsec은 PSD2 관련 데이터의 표준 형식 및 관리를 지정하는 ETSI TS 119 495에 따라 eIDAS QWAC(웹사이트 인증용 적격 인증서) 및 QSealC(전자 씰)를 발급합니다. 이 서비스는 유럽경제지역(EEA) 전역에서 제공되며 Microsec은 이미 10개 EU 회원국의 신청자에게 PSD2 관련 인증서를 발급했습니다.

Microsec

비즈니스적 요구

- 은행 및 TPP가 PSD2 규정을 충족하며 운영할 수 있는 서비스 제작

기술적 요구

- PSD2 관련 인증서 발급에 필요한 소프트웨어 및 프로세스를 개발하여 기존 인프라를 사용하는 새로운 비즈니스 생성

솔루션

- Entrust nShield Solo HSM
- 맞춤형 CA 소프트웨어 및 프로세스
- Entrust nShield Security World

결과

- 기존 인프라를 빠르고 손쉽게 조정하여 새로운 EU 규정을 활용하는 새로운 서비스를 제공하고, 전체 수익 상승에도 기여합니다.
- 믿고 맡길 수 있는 검증된 HSM 솔루션
- 규제 의무 준수

신뢰 서비스, 해당 소프트웨어 개발 및 컨설팅은 현재 Microsec 수익의 2/3를 차지합니다. PSP에 대한 새로운 서비스가 추가됨에 따라 향후 몇 년 동안 해외 수익의 비율이 증가할 것으로 예상됩니다.

2007년부터 Microsec은 세계적으로 인정받는 ETSI(유럽전기통신표준협회)의 정회원입니다. ETSI는 미래 경제 프로세스의 기반이 될 수있는 IT 기술에 대한 전 세계적으로 적용 가능한 표준을 제공합니다. Microsec은 ETSI의 전자 서명 및 인프라를 위한 기술 위원회(TC ESI) 작업에 적극적으로 참여하고 있으며 PSD2 인증서 사양 TS 119 495의 개발에 기여하고 있습니다.

Microsec의 높은 표준 제품 및 서비스는 ISO 9001 : 2008에 기반한 품질 보증 시스템과 ISO / IEC 27001 : 2013에 따라 Lloyd 's에서 승인한 정보 보안 관리 시스템에 의해 뒷받침됩니다.

Microsec과 자사의 솔루션 및 서비스에 대한 자세한 내용은 www.microsec.com을 참조하십시오.

ENTRUST 소개

Entrust는 믿을 수 있는 신원, 결제 및 데이터 보호를 가능케 함으로써 안전한 세상을 유지합니다. 사람들은 국경을 넘고, 구매를 하고, 전자 정부 서비스에 접속하고 기업 네트워크에 로그인하는 것이 원활하고 안전한 경험이기를 오늘날, 그 어느 때보다도 더 요구합니다. Entrust는 이와 같은 모든 상호작용의 핵심에 있는 디지털 보안 및 자격 증명 발급 솔루션에 있어 견줄 데 없는 다양성을 자랑합니다. 2,500명이 넘는 동료 및 글로벌 파트너로 구성된 네트워크, 그리고 150개국 이상의 고객을 보유한 당사는 세계에서 가장 신뢰 받는 기관들의 신뢰를 받고 있습니다.

에서 자세히 보기
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com