Entrust nShield HSM, Verifone의 VeriShield Total Protect 솔루션에 보안 제공

까다로운 환경에서의 승인부터 처리 과정까지, 안전한 전자 POS 솔루션의 선도 기업이 카드 소지자 정보를 보호하는 방법

도전 과제: 성능 저하 없이 신용카드 거래 보안 극대화

신뢰할 수 있는 결제 보안 솔루션의 선도 기업인 Verifone은 소매업체가 더 나은 방법으로 신용카드 거래를 보호하고 고객 데이터 침해 위험을 줄일 수 있어야 한다는 점을 파악했습니다. 대중에게 잘 알려진 주요 데이터 유출로 소매업체의 평판과 매출이 저하되며 매년 수백만 달러의 손실이 발생했습니다. 그러나 어느 솔루션이든지 카드 소지자 데이터에 강화된 보안을 제공할 수 있을 뿐만 아니라, 처리업체나 소매업체 같은 사용자가 최고 수준의 성능(하루 최대 수백만 건 처리)을 누릴 수 있도록 해야 했습니다.

솔루션: ENTRUST NSHIELD HSM 으로 종단간 암호화

Verifone은 고보장성 암호화와 키 관리 기능을 제공할 VeriShield Total Protect 솔루션의 핵심 구성 요소로 Entrust nShield® 하드웨어 보안 모듈(HSM)을 고려했습니다. VeriShield는 정확한 승인 시점부터 처리 시점까지 카드 소지자 정보를 암호화하며, 처리 시점에 거래를 복호화하여 결제 네트워크로 전송합니다. Entrust nShield HSM으로 보안 키 교환과 파생 작업을 수행하여 모든 결제 거래를 보호하는 고유한 키를 생성합니다.

Verifone은 Entrust nShield 시큐리티 월드 아키텍처의 고유 기능을 활용하여 중복성을 구축했습니다. 여러 데이터 센터에 배포된 다수의 서버와 HSM을 원활히 결합하여, 자동화된 로드 밸런싱과 장애 조치뿐만 아니라 대용량 처리가 가능하도록 하기 위해서였습니다. 또한 Entrust는 Verifone이 고객에게 호스팅 옵션을 제공할 수 있도록 지원했습니다. Verifone 고객은 일반적으로 선호하는 현장 호스팅 HSM 옵션이나 Verifone에서 호스팅하는 관리 서비스 옵션 중에서 선택할 수 있습니다.

Verifone

이 솔루션을 통해 Verifone은 악의적인 카드 소지자 데이터 수집 행위에 맞서 강력한 보안과 위험 완화라는 독특한 서비스 조합을 제공하는 동시에, 거래 성능과 가용성을 보장하여 소매업체에 일석이조의 이점을 제공합니다. 또한 Point-to-Point Encryption(P2PE)라고도 불리는 종단간 암호화를 배포하면, 승인 지점인 POS와 처리업체의 복호화 지점 사이에 있는 중간 시스템이 대부분의 PCI DSS 규정 준수 요건 범위에서 제외됩니다. 중간 시스템을 지나는 데이터는 암호화된 상태이기 때문입니다. Verifone 솔루션은 소매업체가 PCI DSS 요건을 훨씬 뛰어넘는 수준의 보안을 제공할 수 있도록 특별히 설계되었습니다.

솔루션 소개

Entrust nShield HSM

Entrust nShield HSM은 암호화 처리, 키 보안 및 관리를 안전하게 이행할 수 있도록 강화된 조작 방지 환경을 제공합니다. 이 제품으로는 암호 시스템과 모범 사례에 관련하여 널리 인정받는 표준과 새로운 표준 모두를 충족하고, 고도로 정밀한 보안 솔루션을 배포할 수 있을 뿐만 아니라 고도로 효율적인 운영 수준을 유지할 수 있습니다.

Entrust nShield Connect HSM은 기업 핵심 애플리케이션의 암호화 작업과 관련 키를 분리, 보호합니다. 또한 PKI(공개 키 기반 구조), 신원 관리 시스템, 애플리케이션 수준 암호화 및 토큰화, SSL/TLS, 코드 서명을 비롯한 여러 상업용 애플리케이션과 주문형 애플리케이션을 대상으로 암호화와 디지털 서명, 키 관리를 수행합니다. 소프트웨어 기반 암호화 라이브러리를 대체하는 고보장성 Entrust nShield Connect HSM은 세계에서 가장 빠른 ECC 성능뿐 아니라 모든 주요 알고리즘을 인증받은 방식으로 구현하는 이점을 제공합니다.

Entrust nShield HSM을 사용하면 다음과 같은 장점을 누릴 수 있습니다.

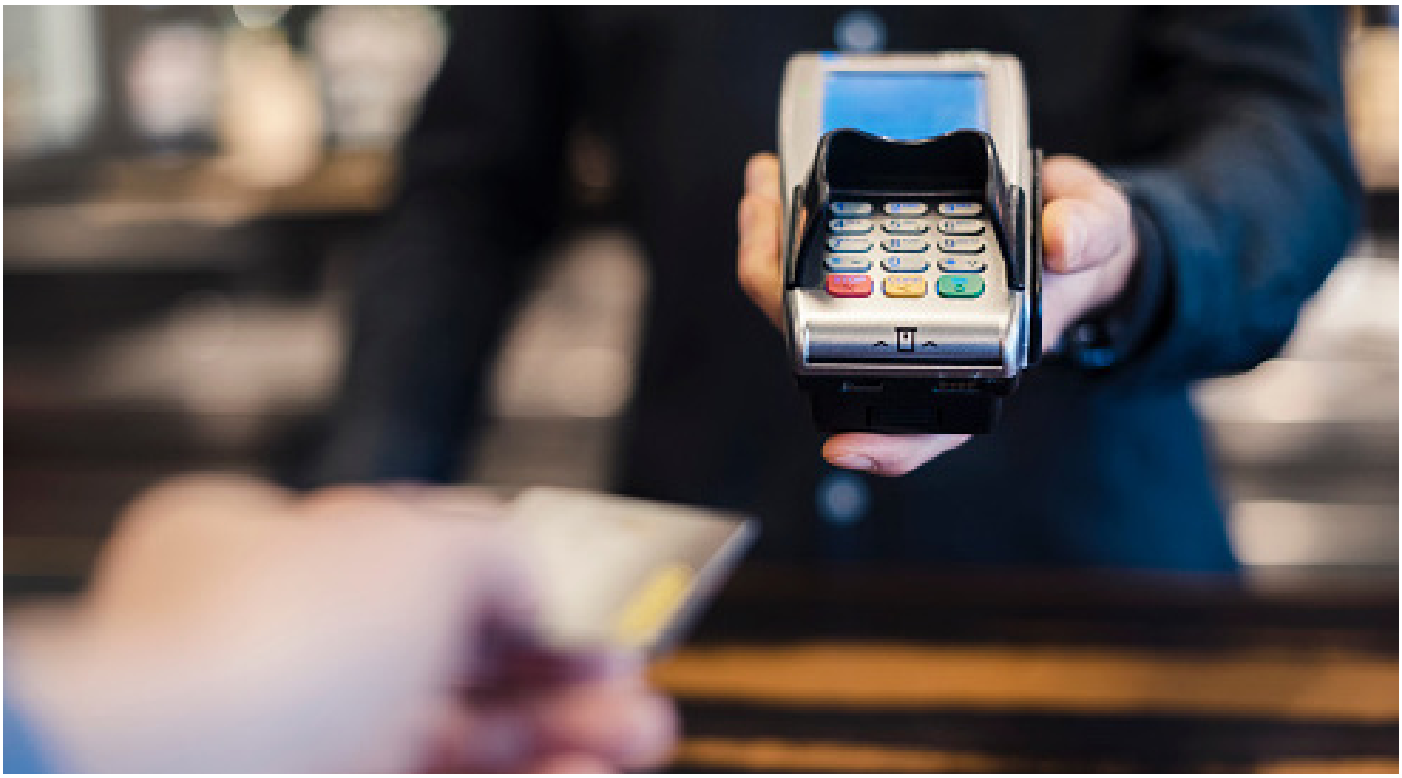
- 변조 방지 하드웨어 내에서 암호키 및 암호화 작업에 인증받은 보안을 제공하여 중요한 애플리케이션에 한층 강화된 안전성 제공
- 암호화를 비용 효율적으로 가속화하고, 기존 데이터센터나 클라우드 환경과는 비교할 수 없는 운영 유연성 확보
- 소프트웨어 한정 암호화의 보안 취약성과 성능 문제 극복
- 규제 준수 관련 비용 절감, 백업 및 원격 관리 등을 비롯한 일상적인 키 관리 업무 축소 Entrust nShield HSM을 사용하면 필요한 용량만 구매하고 요건 변화에 맞추어 손쉽게 솔루션을 확장할 수 있습니다

Verifone

ENTRUST를 선택해야 하는 이유

Verifone은 다른 공급업체 3곳에서 제공하는 6가지 HSM 모델을 평가한 후 Entrust nShield Connect HSM을 선택했습니다. 선택의 이유는 다음과 같습니다.

- **상호 운용성과 통합**. Entrust는 다양한 인터페이스(표준 PKCS #11 및 하위 수준 인터페이스)를 제공하여 Verifone 개발자가 VeriShield 아키텍처를 최대한 활용하며 유연성 있게 HSM을 통합하도록 지원했습니다.
- **간편한 사용**. Verifone은 성능을 최대화하고 키 지속성을 최소화하는 방식으로 시스템을 설계할 때 Entrust nShield HSM가 다른 HSM보다 사용하기 쉽고 훨씬 유연하다는 점을 발견했습니다.
- **성능**. Entrust nShield HSM은 경쟁사 제품보다 훨씬 많은 처리량을 다룰 수 있어 Verifone은 VeriShield 솔루션이 성능에 악영향을 미치지 않으리라는 점을 소매업체에 보장할 수 있었습니다.
- **지원**. Verifone은 Entrust 전문가가 nShield HSM 통합 작업 시 개발자에게 제공한 서비스 지원과 Entrust와의 긴밀한 협력 관계를 높이 평가했습니다.
- **Entrust nShield 시큐리티 월드**. Entrust nShield 시큐리티 월드 아키텍처를 통해 Verifone은 적절한 로드 밸런싱과 고가용성, 안정성을 제공하는 시스템을 설치할 수 있었습니다. 이를 통해 VeriShield 보안 트랜잭션을 여러 사이트와 HSM에서 동기화 서비스 형태로 제공할 수 있습니다.



ENTRUST.COM/HSM에서 자세히 보기

Verifone

주요 이점

- 핵심 데이터에 고보장성 암호화 제공, 성능이나 가용성 저하 없이 전체 수명주기간 키 관리 보장
- 자동화된 밸런싱 및 장애 조치로 대용량 처리 가능
- PCI DSS 요건을 뛰어넘는 수준의 보안 제공
- 강력한 키 관리 아키텍처로 운영 비용 및 규제 관련 보고 비용 절감
- 과중하고 위험할 수 있는 관리 작업을 자동화하고, 단일 장애 지점과 값비싸고 수동 집약적인 백업 프로세스 제거

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