



ENTRUST



# Entrust nShield HSM, Snapper의 대중교통 모바일 충전 솔루션에 보안 제공



한 혁신적인 기업이 통근자에게 편리함과 철통 보안을 동시에 제공한 방법

## 도전 과제: 성능 저하 없이 대중교통 모바일 충전 절차 보안 극대화

뉴질랜드에 소재한 진취적인 기업 Snapper는 아일랜드 더블린의 대중교통 이용자를 위해 대중교통 서비스를 개선하는 프로젝트에 착수했습니다. NTA(National Transport Authority of Ireland, 아일랜드 국립교통부)는 대중교통 이용자가 버스를 타기 직전에도 카드를 충전할 수 있을 만큼 비용 지불을 편리하게 만들기를 원했습니다. Snapper는 NTA 고객인 대중교통 이용자가 스마트폰으로 LEAP 교통 카드 잔액을 확인하고 바로 충전할 수 있는 솔루션을 제공해야 했습니다. 최대 500명의 동시 사용자가 서비스를 이용하는 동안에도 최고 수준의 보안을 유지하는 솔루션이어야 했습니다.

## 솔루션: ENTRUST NSHIELD HSM으로 스마트폰 결제 보안

Snapper는 고객이 대중교통 스마트카드인 LEAP을 휴대 전화에 대면 Snapper 앱을 통해 결제하여 대중교통 이용 계좌를 충전할 수 있는 솔루션을 설계했습니다. 카드에 내장된 비접촉식 칩을 인식한 휴대 전화가 Snapper 앱을 실행하면, Snapper 앱에서 카드 정보를 읽고 인증이 이루어져서 고객이 결제 카드 협회(PCI) 표준을 준수하는 신용 카드 거래를 진행합니다. 그리고 충전한 대중교통 카드로 더블린 버스나 트램, 전철을 이용합니다.



Snapper는 솔루션 보안을 위해 Entrust nShield® 하드웨어 보안 모듈(HSM)을 도입했습니다.

Snapper 앱은 고객 거래 데이터를 암호화하고 Entrust nShield HSM을 사용하여 데이터 보호에 핵심적인 암호키를 관리합니다. 암호화한 모든 데이터는 스마트카드의 비접촉식 칩에 저장되어 고도로 정교한 보안이 가능합니다.

## CODESAFE로 거래 보안

Snapper 솔루션 보안의 핵심은 암호화된 데이터와 키의 관리, 스마트카드와 HSM 간의 상호 인증으로 무결성을 보장하는 데 있습니다. 이 모든 작업은 Snapper의 업무 일과에 따라 처리됩니다. 민감한 작업 일과와 처리 대상인 민감 데이터는 폐쇄된 시스템 외부에 노출될 경우 위협에 취약합니다. Entrust nShield CodeSafe는 Entrust nShield HSM의 보안 경계 시스템 내에서 암호화 코드를 보호하는 방식으로 Snapper에 필수적인 보안을 제공했습니다.

## 고객 각자에게 키 통제권을 부여하는 ENTRUST NSHIELD HSM

NTA의 마스터키는 가장 중요한 기밀 요소로, NTA의 IT 관리자는 매우 엄격한 절차를 따라 마스터키를 보호합니다. Entrust nShield HSM과 이에 연계된 시큐리티 월드 아키텍처는 마스터키 취급 절차를 완벽하게 지원했으며 Snapper의 개입 없이도 NTA가 간편하게 모든 생성키 관련 기능을 안전하게 관리할 수 있도록 했습니다.

## ENTRUST 아키텍처로 엄격한 정책 준수

Entrust nShield 시큐리티 월드는 역할 기반 통제 기능으로 권한 없는 직원이 암호키를 통제할 위험을 크게 줄여주는 포괄적인 보안을 보장합니다.

## 솔루션 소개

### Entrust nShield HSM

Entrust nShield HSM은 암호화 처리, 키 관리를 안전하게 이행할 수 있도록 조작 방지 환경을 제공합니다. 인증받은 Entrust nShield HSM은 암호화 시스템 관련 기존 보안 표준과 새로운 보안 표준을 모두 충족하는 동시에 효율성을 잃지 않습니다.

Entrust nShield HSM은 기업 핵심 애플리케이션의 암호화 작업과 암호키를 분리, 보호합니다. 또한 PKI(공개 키 기반 구조), SSL/TLS, 코드 서명을 포함하는 다양한 애플리케이션의 암호화와 디지털 서명, 키 관리를 수행합니다. 소프트웨어 기반 암호화를 대체하는 고도로 정교한 솔루션인 Entrust nShield HSM은 모든 주요 알고리즘을 지원하고 세계적인 수준의 ECC 성능을 제공합니다.

Entrust nShield HSM과 고유 아키텍처를 이용하면, 필요 용량만 구매해도 추후 요건 변화에 따라 솔루션을 쉽게 확장할 수 있습니다.



## Entrust nShield CodeSafe

Entrust nShield CodeSafe는 민감한 맞춤형 애플리케이션을 nShield HSM 내에서 호스팅하고 실행합니다. 또한, 애플리케이션이 보안 환경 내에서 데이터를 복호화/암호화하고 처리하는 작업을 지원합니다. 그 결과, 스마트카드 인증용 Snapper 코드와 같은 애플리케이션을 외부 위협에서 안전하게 보호할 수 있습니다.

## Entrust 전문 서비스

Entrust 전문 서비스팀의 보안 컨설턴트는 비즈니스 고유의 요건에 따른 맞춤 서비스를 제공합니다. 다양한 애플리케이션에 대한 풍부한 경험을 바탕으로 배포 및 현장 테스트를 진행하여, 솔루션 통합 계획을 세우고 위험을 완화하며 빠르고 안전하게 프로젝트를 실행할 수 있도록 지원합니다.

## ENTRUST를 선택해야 하는 이유

Snapper는 해외 비즈니스 확장에 핵심적이었던 6개월 프로젝트를 다른 보안 솔루션 공급업체와 함께 시작했습니다. 하지만 프로젝트 중, 선택한 공급업체가 암호화 코드를 보호하거나 아일랜드 국립 교통부가 요구하는 성능 사양을 충족하지 못하리라는 점을 깨달았습니다.

3개월이 남은 시점에서 Snapper는 Entrust에 프로젝트 참여를 요청했습니다. Entrust 솔루션이 올바른 선택이었던 이유는 다음과 같습니다.

- **용이한 구현 방식** - Snapper는 자사의 설계 방식과 완벽하게 통합할 수 있는 간단한 솔루션이 필요했습니다. Entrust는 필요한 솔루션을 제공하여 고정된 예산만으로도 분초를 다투는 프로젝트를 달성할 수 있도록 지원했습니다.
- **성능** - Entrust nShield HSM은 프로젝트 요건보다 6배 더 빠르고 Snapper가 처음 선택한 보안 공급업체보다 훨씬 빠른 속도로 소비자 거래 동시 처리를 지원합니다. 이를 통해 Snapper와 국립 교통부는 앞으로 커질 소비자 요구도 충족할 수 있다는 확신을 얻었습니다.
- **수준 높은 지침** - Snapper의 표현에 따르면 Entrust 전문 서비스팀은 "전문 지식에 대한 문제 없는 접근"을 가능하게 했으며 Snapper와 효율적으로 협력하여 프로젝트 요건에 맞춰 팀을 운영함으로써 더블린 교통당국에 신속하고 자신 있게 솔루션을 제공하도록 했습니다.



## Entrust 솔루션의 주요 장점

- 변조 방지 하드웨어 내에서 암호키 및 암호화 작업에 보안을 제공하여 소프트웨어 한정 솔루션에 한층 강화된 안전성 제공
- Entrust nShield CodeSafe를 이용해 HSM 보안 경계 내에서 민감한 맞춤형 애플리케이션 실행
- Entrust nShield 시큐리티 월드만의 아키텍처를 이용하여 키에 대한 주도권을 유지하고 변화하는 요건에 따라 확장 가능한 HSM 자산 구축
- Entrust 전문 서비스팀의 수준 높은 지침에 따라 효율적이고 자신 있게 솔루션 개발 가능

## 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. 2,500 명이 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](https://www.entrust.com/HSM)



**ENTRUST**

연락처:

[HSMinfo@entrust.com](mailto:HSMinfo@entrust.com)