



Revolutionizing Cryptographic Management for Secure Payment Processing

Customer Overview

As a major European payment processor, this leading financial services organization supports over 250 million users, facilitating over five billion transactions annually, and providing the foundation for secure and reliable payment solutions across Europe.

Key Challenges in Cryptographic Management

Faced with a need to consolidate its cryptographic infrastructure, the company launched a two-year IT transformation project to migrate from a monolithic mainframe to a more efficient distributed systems architecture.

The Goals

The company sought to reduce processing costs (MIPS) and accelerate time-to-market for payment solutions, while building an efficient and scalable cryptographic infrastructure backed by HSM deployments to guarantee security and compliance.

Other important solution requirements included:

Acquirer Processing

- Processing EMV transactions (ATM and POS networks)
- 13,000 ATMs and 400,000 POS systems supporting over 3 million cryptographic symmetric keys
- Key storage for all the cryptographic keys (both symmetric and asymmetric)
- Active-active cryptographic architecture to support two processing sites (2 data centers) and key synchronization between the two sites
- Key synchronization between the two data centers

Issuer Processing

- Card data preparation (EMV Cards: MCI, VISA, AMEX)
- National card scheme (Manage EMV CA)
- Generation of bulk EMV card keys (RSA)

90%
reduction in infrastructure support cost

► Industry Compliance

- FIPS 140-2 level 3 compliant
- PCI-certified HSMs

► Solution Specification Requirements

- Key migration from IBM mainframes
- Remote device management
- Remote key management capabilities

► Key Takeaways

- **90%** reduction in support costs
30% reduction in infrastructure
90 million transactions/day
5x greater scalability in TPS
- Enabled high-availability and disaster recovery, reduced processing costs (MIPS), and accelerated time-to-market for payment solutions
- Leveraged Futurex's advanced orchestration and management capabilities for payment processing, cryptographic operations, and PIN mailing

The Solution

Futurex delivered a comprehensive HSM deployment for all cryptographic commands (both financial and general purpose).

- The Futurex **KMES Series 3** manages key storage, key insertion, modification, and deletion operations
- The **Guardian Series 3** processes application requests, load balancing between the different HSMs and key storage devices, and event monitoring
- The **Excrypt Touch** device, a tablet-based HSM provides remote management, orchestration, and remote key management

Deployment and Implementation

The project implementation included key migration and synchronization. Leveraging Futurex's Excrypt API, the company developed its own security manager application that encompasses load balancing between the local and remote crypto infrastructure, controls different application response errors, and enables the controlled removal of Futurex crypto clusters without downtime: for example, during the Futurex firmware upgrade processes.

The Results

The company successfully consolidated its HSMs, leveraging Futurex's advanced orchestration and management capabilities to manage payment processing, cryptographic operations, and PIN mailing. With the latest Guardian Series 3 and KMES Series 3, the company achieved cryptographic processing of 20,000 TPS, scalable to 100,000 TPS with a simple license upgrade.

The Future

The company is acquiring new disaster recovery hardware to future-proof its infrastructure, elevating HSM resilience, and supporting over 90 million cryptographic transactions daily. It is also advancing its crypto agility program to prepare for post-quantum cryptography, leveraging Futurex's VirtuCrypt platform to test PQC algorithms per new NIST standards.

The KMES Series 3

- PKI and CA for automatic key rotation and digital signing use cases
- Generates, encrypts, and manages an organization's encryption keys
- Single, unified platform deployed on-premises or in the cloud

The Guardian Series 3

- Streamlines cryptographic management for both cloud and on-premises HSMs
- Customizable settings, seamless peering, and centralized auditing
- Simplified enterprise HSM management

The Excrypt Touch

- Remotely configures and manages enterprise data security technology
- Orchestrates, manages, and monitors the entire HSM network
- Ensures robust data protection



*Futurex reduced our crypto infrastructure **by over 30%** while enabling us to support **90M transactions per day.***

*The transformation has been **exceptional.***

*— Director of Cryptography,
Leading Payment Processor*



For over 40 years, Futurex has been an award-winning leader and innovator in the encryption market, delivering uncompromising enterprise-grade data security solutions. Over 15,000 organizations worldwide trust Futurex to provide groundbreaking hardware security modules, key management servers, and cloud HSM solutions.

Futurex is headquartered outside of San Antonio, Texas, with regional offices worldwide and over a dozen data centers across five continents, Futurex delivers unmatched support for its clients' mission-critical data encryption and key management requirements.

FUTUREX.COM

864 Old Boerne Road,
Bulverde, Texas 78163

