FUTUREX

Excrypt **SSP Enterprise** V.2

Hardware Security Module

The World's Most Advanced Financial Hardware Security Module

Protect Sensitive Payment Data at Rest, in Use, and in Motion

Electronic payment networks need data security solutions that scale in speed and expand over time to support emerging payment types and algorithms. The Excrypt SSP Enterprise v.2 is the world's fastest hardware security module (HSM) for financial transaction processing. It offers robust functionality and full backward compatibility with the Excrypt SSP Series of HSMs. It has a high degree of scalability, offering speeds in excess of 50,000 transactions per second. All in a tamper-resistant, 1U rackmount chassis.

Integrated disaster recovery and redundancy features ensure rock-solid reliability. The device complies with key management best practices and contains some of the industry's most advanced security features.

The Excrypt SSP Enterprise v.2 excels in high throughput environments. Not only does this device provide increased redundancy, physical and logical security, and platform virtualization, it's the fastest payment HSM in the world, capable of processing over 50,000 transactions per second.

Payment Security Functionality

- ✔ Card/PIN Issuance
- ✔ Mobile Payments
- ✔ P2PE and Tokenization
- ✔ ATM Remote Key Loading
- ✔ Card/PIN Validation
- ✔ EMV Issuance/Validation
- ✔ MAC and Hashing
- ✔ General Purpose Functionality

HSM Virtualization and Application Partitioning

- The Excrypt SSP Enterprise v.2 offers HSM virtualization and application partitioning. This allows multiple logically separated environments to be created within a single FIPS 140-2 Level 3 validated HSM boundary.

HSM Virtualization

The Excrypt SSP Enterprise v.2 can create multiple logically independent HSMs inside a single host device for separate transaction processing environments.

- Increase the ROI of your HSM infrastructure
- Multiple methods of access including a web portal, API, the Guardian Series 3, and VirtuCrypt
- Test new firmware on an independent virtual instance
- Unique firmware versions, users, key storage space, and security policies on each virtual HSM
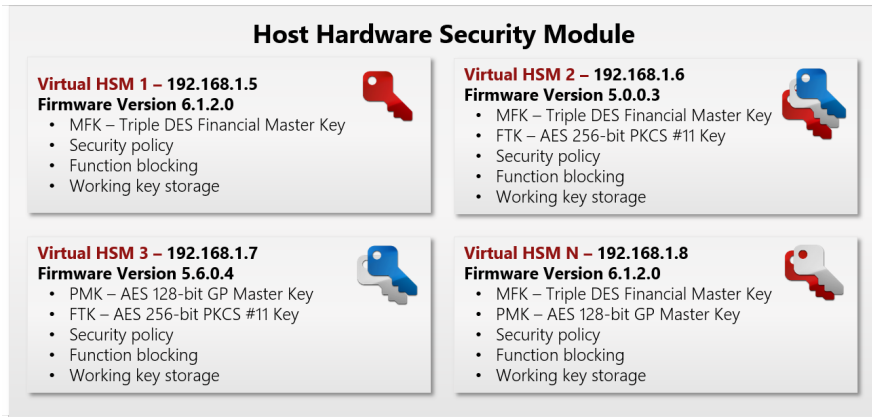
Universal Compatibility

- Turnkey compatibility with all major financial host application software, as well as support for standards-based interfaces like PKCS #11 and Java for general purpose cryptographic processing.

Product Overview: Excrypt SSP Enterprise V.2

The Excrypt SSP Enterprise v.2 provides virtualization capabilities that allow users to host logically separated virtual HSMs from within a single physical device. A sample configuration for these independent devices is pictured below.

Host Hardware Security Module

Virtual HSM 1 – 192.168.1.5
Firmware Version 6.1.2.0
• MFK – Triple DES Financial Master Key
• Security policy
• Function blocking
• Working key storage

Virtual HSM 2 – 192.168.1.6
Firmware Version 5.0.0.3
• MFK – Triple DES Financial Master Key
• FTK – AES 256-bit PKCS #11 Key
• Security policy
• Function blocking
• Working key storage

Virtual HSM 3 – 192.168.1.7
Firmware Version 5.6.0.4
• PMK – AES 128-bit GP Master Key
• FTK – AES 256-bit PKCS #11 Key
• Security policy
• Function blocking
• Working key storage

Virtual HSM N – 192.168.1.8
Firmware Version 6.1.2.0
• MFK – Triple DES Financial Master Key
• PMK – AES 128-bit GP Master Key
• Security policy
• Function blocking
• Working key storage

Wide-Ranging Cryptograhic Functionality

• Magnetic Stripe and EMV Card Issuance and Verification
• MAC and Hashing
• Point-to-Point Encryption (P2PE)
• Format-Preserving Encryption
• ATM Remote Key Loading
• HCE and Cloud Payments
• Digital Signing
• General-Purpose Cryptography
• Mobile Payments
• PIN Management and Printing
• Tokenization
• Contactless/NFC
• 3-D Secure
• PCI Data Protection
• On Behalf Key Management (OBKM)
• Custom Functionality

HSM Virtualization, Application Partitioning, and Custom Command Extentions

• A single Excrypt SSP Enterprise v.2 HSM can be divided into multiple logically separated, completely independent virtual HSMs
• Design and deploy custom extensions within the HSM's cryptographic boundary to add functionality to existing API commands
• Use application partitioning to segregate key storage locations, giving individual applications control over their own keys and security policies through API function blocking

Native Integration with Futurex Solutions

• The Excrypt SSP Enterprise v.2 integrates directly with other Futurex solutions for centralized configuration, management, monitoring, alerting, load balancing, cloud services, and more.

Disaster Recovery and High Availability

• Contains hot-swappable power supplies and dual Ethernet ports
• Integrates with VirtuCrypt for increased infrastructure visibility and uptime

Product Specifications

Dimension and Weight

Weight: 36 pounds (16.33 kg)
Width: 19 inches (48.3 cm)
Height: 1U - 1.7 inches (4.37 cm)
Depth: 19.44 inches (49.38 cm)

Industry Compliance Standards

• FIPS 140-2 Level 3 validated
• PCI HSM
• RoHS
• FCC Part 15 - Class B
• ANSI X9.24 Part 1 and Part 2—TR-39

Guardian Series 3

Create a centrally managed network of devices communicating over encrypted TLS. The Guardian can manage groups of client Futurex devices from any location.

Guardian
HSM #1   HSM #2
Host HSM

Functionality and Interfaces

Algorithms

• 3DES DUKPT
• RSA
• AES
• ECC

Interfaces

• RESTful API
• Java JCA/JCE
• PKCS #11
• And more

Key Block Formats

• TR-31
• Cryptograms
• AKB

Remote Management

Combine the Excrypt SSP Enterprise v.2 & the Excrypt Touch for remote access and management.

Available Configurations

Scalable as processing needs grow

Starting from
1,000 TPS

50,000+ TPS
and beyond

Base Config