

DATASHEET

Entrust nShield HSMi 2

HIGHLIGHTS

Built and optimized for secure issuance

The nShield HSMi 2 is FIPS 140-3 Level 3-certified hardware designed to deliver cryptographic services enabling Entrust's secure issuance software. These tamper-resistant HSMs perform vital functions for financial and identification issuance, including EMV data preparation, key generation, and data protection.

- Maximizes performance and availability with high cryptographic transaction rates and flexible scaling
- Supports issuance data preparation and personalization for both central and instant issuance applications
- Facilitates secure remote access for administration functions with nShield Remote Administration kit

The Entrust nShield HSMi 2 works with existing Entrust software, hardware, service, and supply offerings to create an integrated ecosystem that delivers unparalleled security, simplicity, and serviceability. Our unique Security World architecture is closely integrated with Entrust Key Manager Software (KMS), ensuring seamless failover and load balancing for maximum program availability.

Operationally efficient and IT friendly

Installation and ongoing maintenance are accessible and straightforward.

- Comes with a quick-fit slide rail kit for easy installation
- Includes a remote administration kit featuring an nShield Trusted Verification Device to facilitate the remote presentation of smart cards for HSM administration, remote firmware updates, Security World creation, and administration

Faster processing

High cryptographic capacity ensures your investment can handle the constantly evolving EMV and ICAO security standards, as well as key and certificate requirements of the industry, including contactless card profiles.

- Updated CPU (HSMi: 3 core CPU – HSMi 2: 4 core CPU)
- New FPGA-based crypto processor positions for potential PQ use cases in issuance
- Updated analog RNG

Highly integrated, highly secure

Have peace of mind knowing you have a highly integrated, highly secure solution designed specifically for your issuance program.

Ideal for:

- Instant issuance (banks and credit unions)
- Central issuance (card bureaus, banks, and other payment card issuers)

TECHNICAL SPECIFICATIONS

Supported cryptographic applications

- Symmetric Key Mechanisms: AES (Advanced Encryption Standard), DES (Data Encryption Standard), Triple DES (3DES)
- Asymmetric Key Mechanisms: RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), ECDSA (Elliptic Curve Digital Signature Algorithm)
- Hashing Mechanisms: SHA-1 (Secure Hash Algorithm 1), SHA-256, SHA-384, SHA-512
- MAC (Message Authentication Code) Mechanisms: HMAC (Hash-Based Message Authentication Code) CMAC (Cipher-Based Message Authentication Code)
- Random Number Generation: RNG (Random Number Generator)

Supported issuer EMV certificates

- American Express®
- Discover®
- Elo
- Interac
- Japan Credit Bureau (JCB)
- JETCO
- Mastercard®

- NSICCS Indonesia
- RuPay
- UnionPay
- Visa®
- VCCS Vietnam

Related software

- Secure KLD for key loading
- Key Manager 8.5.0 and higher
- Instant Financial Issuance Software 6.11 and higher
- Security World (Please see the Adaptive Issuance Key Manager Software datasheet for the latest version)

Security compliance

- FIPS 140-3 Level 3 certified hardware

Host connectivity

- Dual-gigabit ethernet ports (two network segments with network bonding option)

Safety and environmental standards compliance

- UL, CE, FCC, UKCA, RCM, Canada ICES
- RoHS, WEEE, REACH

High availability

- All solid-state storage
- Field-serviceable fan tray
- Dual hot-swap power supply
- HSM load balancing/failover with Key Manager
- Network bonding supporting active backup mode and 802.3ad mode



ENTRUST
SECURING A WORLD IN MOTION

Management and monitoring

- nShield Remote Administration – includes nShield Trusted Verification Device and remote administration smart cards

Physical characteristics

- Standard 1U 19in. rack mount dimensions: 43.4 x 430 x 705mm (1.7 x 16.9 x 27.8in)
- Weight: 11.5kg (25.4lb)
- Input voltage: 100-240V AC auto switching 50-60Hz
- Power consumption: 220W maximum
- Heat dissipation: 445 BTU/hr (typical load)
- Reliability - MTBF: 107,845 hours

Available Configurations:

nShield HSMi 2 is available in 2 versions:

- nShield HSMi 2 8000 (Product Code: 535052-001): Low-speed, intended mainly for test/development and with low-volume environments
- nShield HSMi 2 16000 (Product Code: 535052-002): High-speed, intended for high-volume production environments