

# Entrust Test and Development nShield HSMi

Lightweight, portable, USB-connected HSM that empowers your chip personalization test and development needs

## HIGHLIGHTS

The Entrust Test and Development nShield HSMi is a full-featured, USB-connected device that delivers vital functions for financial and identification issuance with convenience and value. The functions include data preparation, key generation, and data protection.

- Fully compatible with Adaptive Issuance™ Key Manager (version 8.2.3 or higher)
- Supports virtual machine environments for deployment flexibility
- Offers the same cryptographic features as the high-volume nShield HSMi production devices



## KEY FEATURES AND BENEFITS

### Highly portable

Its small, lightweight design with convenient USB connection supports a variety of platforms, including laptops and other portable devices.

### Cost-effective with productionlike features

The most economical HSM in the nShield HSMi family, the nShield HSMi Test and Development Kit gives you an entry-point HSM, which supports the same features as the production HSMs. It allows for full validation of your data preparation and smart card personalization applications prior to production deployment.

# TECHNICAL SPECIFICATIONS

## Supported cryptographic applications

- Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA (including NIST, Brainpool & secp256k1 curves), ECDH, Edwards (Ed25519, Ed25519ph)
- Symmetric algorithms: AES, Arcfour, ARIA, Camellia, CAST, DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224, HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, Triple DES
- Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160

## Supported issuer EMV certificates

- American Express
- Discover®
- Elo
- Interac
- Japan Credit Bureau (JCB)
- Jetco
- Mastercard®
- NSICCS Indonesia
- RuPay
- UnionPay
- Visa®
- VCCS Vietnam

## Related software

- Adaptive Issuance™ Chip Interface Software 8.2.3 or higher
- Adaptive Issuance™ Key Manager Software 8.2.3 or higher
- Adaptive Issuance™ EMV Data Prep and Perso Software 8.2.3 or higher
- Adaptive Issuance™ MULTOS Data Prep and Perso Software 8.2.3 or higher
- Instant Financial Issuance Software 6.9 or higher
- Security World software version compatible with your Key Manager Software version

## Security compliance

This product is intended for test and development use only, and is not suitable for production use. Do not use with non-test keys or with a DMK used to protect production keys. The Entrust Test and Development nShield HSMi offers all the security and key management features of the other nShield HSMs, but with reduced processing speed.

## Host connectivity

- USB port (1.x, 2.x compliant)

## Physical characteristics

- Portable desktop device with integrated smart card reader
- Dimensions with stand open 120 x 118 x 27mm (4.7 x 4.6 x 1in)
- Weight: 340g (0.8lb)
- Input voltage: 5v DC powered by USB host device
- Power consumption: 700mW

