CardContact
smart system architects

SmartCard-HSM is a light-weight hardware security module for secure key generation and storage. It has been designed for PKI and cryptographic systems with low to moderate load. The unique build in support for card verifiable certificates as defined in TR-03110 (Extended Access Control) makes a SmartCard-HSM the perfect choice for storing key material in an EAC-PKI. A trusted channel and public key attestation allow remote key generation and certificate issuance.

FEATURES

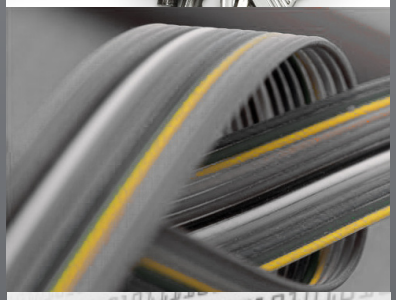
- Supports RSA and ECDSA
- Authenticated certificate signing requests as per TR-03110
- Chip authentication and secure channel as per TR-03110
- ISO 7816-4 command interface
- User PIN 6 – 16 bytes
- Standardized and proprietary domain parameters for ECC
- Common Criteria EAL 5+ certified operating system

ALGORITHMS

- RSA PKCS#1 V1.5/PSS with SHA-1/SHA-224/SHA-256
- ECDSA GF(p) with SHA-1/SHA-224/SHA-256

KEY SIZES

- RSA with 1024, 1536 and 2048 bits
- ECC with 192, 224, 256 and 320 bits



PERFORMANCE

Key Generation with authenticated public key export

	On-Card with Export per minute
RSA 1024	10
RSA 1536	5
RSA 2048	2
ECC GF(p) 256	10

Signature creation

	Off-Card Hash per minute	On-Card Hash per minute *)
RSA 1024	350	125
RSA 1536	200	100
RSA 2048	100	68
ECDSA GF(p) 256	360	125

**) SHA-256 with 1kb data*

MEMORY CAPACITY

- Up to 60 ECC GF(p) 256-bit keys or
- Up to 48 RSA 2048-bit keys or
- 55Kb in up to 50 elementary files

www.**smartcard-hsm**.com