

SmartCard-HSM Data Sheet



Order No	510050000 SmartCard-HSM Mini USB-Token (4.1-P7)														
Purpose	The SmartCard-HSM is a light-weight hardware security module for secure key generation, storage and use. 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 BSI TR-03110 (Extended Access Control) makes a SmartCard-HSM the perfect choice for storing key material in a distributed Public Key Infrastructure. A trusted channel and public key attestation allow remote key generation and certificate issuance. Advanced key management functions provide for key backup and device clustering in key domains.														
Authentication	User-PIN / Transport-PIN Public Key Authentication with CV-Certificates Chip Authentication V2.0 based on BSI TR-03110 with Secure Messaging (AES, TDES) Peer authentication in key domains														
Key Types	RSA 1024, 1536, 2048, 3072 and 4096 bit ECC 192, 224, 256, 320, 384, 512 and 521 bit on GF(p) AES 128, 192 and 256 bit														
Algorithms	Generate key (RSA, ECC, AES) RSA Sign (Raw, PKCS#1 V1.5, PSS, +SHA-1/256/384/512) ECDSA Sign (Raw, SHA-1, SHA-256, SHA-384 and SHA-512) Key Agreement (RSA OAEP, ECDH Raw and ECDH Authenticated) AES Key Derivation with Export (CBC, CMAC, NIST SP 800-56C) Wrap / Unwrap Key under AES-256 Key Encryption Key														
Random Number	Class DRG.3 as defined in AIS 20														
Memory Size	179Kb Flash RSA 4096 key typically 4000 byte ECC 521 key typically 2500 byte AES 256 key typically 250 byte All key sizes plus memory space for meta-data (e.g. certificates)														
Performance	<table> <tr> <td>RSA 1024: 40 ms</td> <td>ECDSA/ 256: 50 ms</td> </tr> <tr> <td>RSA 1536: 60 ms</td> <td>ECDH 256: 50ms</td> </tr> <tr> <td>RSA 2048: 120 ms</td> <td>ECDSA 512: 90 ms</td> </tr> <tr> <td>RSA 3074: 290 ms</td> <td>ECDH 512: 90 ms</td> </tr> <tr> <td>RSA 4096: 1150 ms</td> <td></td> </tr> <tr> <td>RSAGEN 2048: 10 sec</td> <td>ECGEN 256: 1 sec</td> </tr> <tr> <td>RSAGEN 4096: 25 sec</td> <td>ECGEN 512: 2 sec</td> </tr> </table>	RSA 1024: 40 ms	ECDSA/ 256: 50 ms	RSA 1536: 60 ms	ECDH 256: 50ms	RSA 2048: 120 ms	ECDSA 512: 90 ms	RSA 3074: 290 ms	ECDH 512: 90 ms	RSA 4096: 1150 ms		RSAGEN 2048: 10 sec	ECGEN 256: 1 sec	RSAGEN 4096: 25 sec	ECGEN 512: 2 sec
RSA 1024: 40 ms	ECDSA/ 256: 50 ms														
RSA 1536: 60 ms	ECDH 256: 50ms														
RSA 2048: 120 ms	ECDSA 512: 90 ms														
RSA 3074: 290 ms	ECDH 512: 90 ms														
RSA 4096: 1150 ms															
RSAGEN 2048: 10 sec	ECGEN 256: 1 sec														
RSAGEN 4096: 25 sec	ECGEN 512: 2 sec														
Data Retention Endurance	25 years 500.000 write cycles														
Platform Certification	Common Criteria EAL 6+ (NSCIB-CC-0313985-CR) No composite applet certification performed														