HYPERPKI™
HYP2003-J

DATASHEET

OVERVIEW

- Built-in high performance secure smart card chip
- Onboard RSA, AES, DES/3DES, SHA-256 algorithms approved by NIST's Cryptographic Algorithm Validation Program (CAVP) for FIPS 140-2 Level 2 and Level 3 certification
- Reliable middleware supports multiple operating systems
- Tamper-evident hardware

Dimensions (mm): 53 x 16.5 x 8.5

Weight (g): 6

OPERATING INFO

Supported OS

- Windows XP/Vista/7/8/8.1 x64/x86
- Windows Server 2003/2008 x64/x86
- Linux x64/x86
- Mac OS X
- Other platforms such as Java 3.0 or higher, .NET, Sun Solaris, etc.
- 32 and 64-bit systems supported

Storage Temperatures

- -20 - 85°C

Operating Temperatures

- 0 - 70°C

Hardware Interface

- PC/SC
- USB 2.0 (CCID 1.0 compatible)

Middleware

- PKCS#11 v2.01, v2.11, X.509 v3 certificate storage

SPECIFICATIONS

PHYSICAL PARAMETERS

User Memory

- 64 KB secure memory for storing multiple digital signature certificates

Data Retention

- More than 10 years

CRYPTOGRAPHIC ALGORITHMS

- SHA-256
- RSA up to 2048-bit keys
- DES, 3DES, ECC curves

STANDARDS

- True Random Number Generator (TRNG) as per NIST SP 800 or ANSI X9.31 PRNG

CERTIFICATIONS

- FIPS 140-2 Level 2/3
- Common Criteria CC 4/4+ (chip-level)

OTHER FEATURES

- Hard tamper-proof body as one unit
- No method to extract, view, nor access the private key
- SDK and API available with user guide
- Crypto-related operations performed on-board only
- Unique serial number available

CANADA: 200-6191 Westminster Hwy, Richmond BC V7C 4V4
USA: 2219 Rimland Drive, Suite 301 #341, Bellingham, WA 98226
hypersecu.com | 1 (604) 279-2000