

Accredited Digital Signature Tools

1. Smart Tokens

| | Token | Specifications |
|---|-----------------------------|--|
| 1 | SafeNet eToken 5110 | <p>Supported operating systems: Windows Server 2008/R2, Windows Server 2012 and 2012 R2, Windows 7, Mac OS, Linux, Windows 8, Windows 10</p> <p>API & Standards Support: PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPsec/IKE, MS minidriver, CNG</p> <p>On Board Security Algorithms: Hash: SHA-256, RSA: 2048-bit, Elliptic curves: P-256, P-384, ECDH</p> <p>Security certifications: FIPS 140-2 level 3.</p> |
| 2 | ePass 2003 smart token | <p>Supported operating systems: Supports Windows, Linux and Mac OS</p> <p>API & Standards Support: Support PKCS #11 standard API, Microsoft CryptoAPI and Microsoft CryptoAPI: Next Generation (CNG)</p> <p>On-board security algorithms: On board RSA, AES, DES/3DES, SHA-1, SHA-256 algorithms approved by NIST FIPS CAVP</p> <p>Security certifications: Certified by Common Criteria EAL 5+</p> |
| 3 | G&D Star Design smart token | <p>Supported operating systems: Windows XP, Vista - Windows 7 – 32 and 64 bit - Linux and MAC OS 10.5 on request</p> <p>API & Standards Support: PKCS#11 - Microsoft CSP - USB 2.0 - PC/SC (CCID)</p> <p>On-board security algorithms: RSA 2048 bit, AES 256 bit, ECDSA up to 256 bit, SHA-224, SHA-256, SHA-384, SHA-512</p> <p>Security certifications: Chip: Common Criteria EAL 5+ Operating system: FIPS 140-2 level 3 Token: FIPS 140-2 level 3 CE, FCC, WEEE,</p> <p>RoHS</p> |

| | | |
|---|-----------------------------------|--|
| 4 | HYPERSECU® HyperPKI HYP2003 A3 | <p>API & Standards Support: Microsoft CAPI, CNG PKCS#11 V2.20 Microsoft Smart Card Minidriver PC/SC, CCID SSL v3 IPSec/IKE</p> <ul style="list-style-type: none"> On-board security algorithms: 3DES(192),RSA(2048),ECC(256),AES(128-256),SHA1,SHA256,SHA384,SHA512 <p>Security certifications: FIPS-140-2 Level 3 validation Cert #3602</p> |
|---|-----------------------------------|--|

2. Crypto SD Cards

| Crypto SD Card | Specifications |
|-------------------------------------|---|
| <p>Spyrus Rosetta® Micro SD</p> | <p>Supported operating systems: Compatible with support for Windows 7, 8, 8.1, 10 and Linux and more on request</p> <p>On-board security algorithms: RSA 2048 digital signature algorithm, Elliptic Curve Cryptography (P-256, P-384, P-521), SHA-1, SHA-224/256/384/512 Secure Hash Algorithms</p> <p>Security certifications: FIPS 140-2 Level 3 Certified</p> |

3. Smart Cards

| Crypto SD Card | Specifications |
|-----------------------|---|
| JCOP 4 P71 Smart Card | <p>Supported operating systems: Windows, Linux and Mac</p> <p>On-board security algorithms: RSA: 512 bits up to 2048 bits in 8-bit steps; optionally (via Order Entry Form) up to 4096 bits in 8-bit steps, ECC: 224 bits up to 521 bits, SHA: SHA_224, SHA_256, SHA_384, SHA_512</p> <p>Security certifications: Certified CC EAL+5</p> |

4. Hardware Security Modules (HSMs)

For digital signature creation and verification products and in trustworthy hardware devices used as secure signature creation devices, it is required to have concurrent acceptance and usage of FIPS 140-2 level 3 or higher, or CC EAL5+ or higher.