

CC-50

DESIGNED AND BUILT IN THE USA WITH FIPS 140-2
LEVEL 4 PHYSICAL SECURITY INCLUDED



CC-50

50 Ops/Sec

**Based on RSA-2048
signing operations*

CyberCog's hardware security modules (HSM) defend information systems from cybersecurity attacks with tamper-protected separation of sensitive keys, data, and operations. Multiple card choices and robust suite of cryptographic services supports standard security protocols to simplify development and provide a security solution for every system.

PRODUCT DETAILS



TECHNICAL SPECIFICATIONS

- Symmetric: AES 128, 192, 256 (CBC, ECB, CTR, CMAC, GCM, GMAC, XTS, XEX)
- Asymmetric: RSA (1024, 2048, 3072, 4096), ECC (P-224, P-254, P-384, P-521), ECDSA (224, 283, 256, 384, 521)
- Hashing: HMAC-SHA-1, HMAC-SHA-256, HMAC SHA-384, HMAC-SHA-512, SHA-1, SHA-256, SHA384, SHA-512
- Key Derivation: PBKDF2 (SP 800 132)
- Key Wrapping: SP800-38F
- Key Agreement / Transport: DH, ECDH, RSA
- Random Number Generation: HW based true noise source alongside NIST 800-90A compliant CTR DRBG CNSA Suite Support
- PKI Certificate Management: PEM & DER x509v3, PKCS #7, CRL, PKCS#1, PKCS#8, PKCS#12
- API Support: PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI, and CNG
- Assurance: FIPS 140-2 Level3 and Level 4. Meet compliance needs for GDPR, HIPAA, PCI-DSS, eIDAS
- Compliance: UL, CSA, CE, FCC, CE, VCCI, C-TICK, KC MARK, RoHS2, WEEE, TAA
- Dimensions: Low Profile PCIe card, 2.74" x 6.57" x .074"
- Power: 18W maximum, 14W typical
- Temperature Range: Operating 0° to 50°C
- American designed and manufactured

USER APPLICATIONS

- PKI Certificate Signing & Validation
- Secure Communication: SSL & TLS
- Storage (online CA keys & offline CA keys)
- Smart Card Issuance & Management
- Code & Document Signing
- Database & File Encryption
- Email Encryption
- Infrastructure Security
- Identity & Rights Management
- Key Management
- Cryptographic Acceleration
- Secure Manufacturing

FEATURES

- Tamper protected generation, storage, and management of cryptographic keys
- Cryptographic operations isolated from potentially compromised software
- Loadable software modules for execution of custom modules in a trusted environment
- Out-of-the-box integration with open source security protocols and stacks
- Role based access control and management
- Audit logging
- M of N Backup, Restore, and Decommission

About CyberCogs

As gears turn big wheels with less energy, making the work easier, CyberCogs offers system developers with the highest grade security building blocks to make cybersecurity easy