innovation & performance

HARDWARE SECURITY MODULES

We provide the best solutions for protecting your cryptographic materials from unauthorized use and potential adversaries. Go beyond software-only solutions and get unbeatable performance and security from our highly qualified team.

Best price and performance in industry

Crypto Agility: Supports Post Quantum Cryptography

Full-Featured HSM includes:

- Life-cycle management of keys
- User authentication: password and smartcard based
- Onboard secure cryptographic key generation, storage, and management
- Offloading execution of crypto-enabled application servers for complete asymmetric and symmetric cryptography
- Managing transparent data encryption keys for databases

Prototypes shipping now!

PERFORMANCE

RSA-2048:	20,000 transactions per second
ECC P-256:	13,000 transactions per second
ECC P-384:	8,000 transactions per second
ECC P-521:	5,000 transactions per second

NEXT GEN CRYPTO

Post Quantum Cryptography

Quantum Safe Key Exchange and Signature Algorithms
• Hash Based Signatures

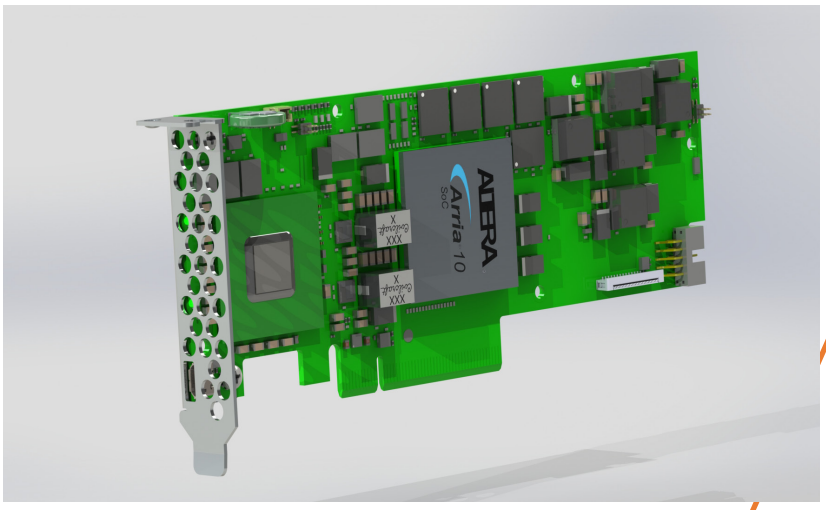
FEATURES

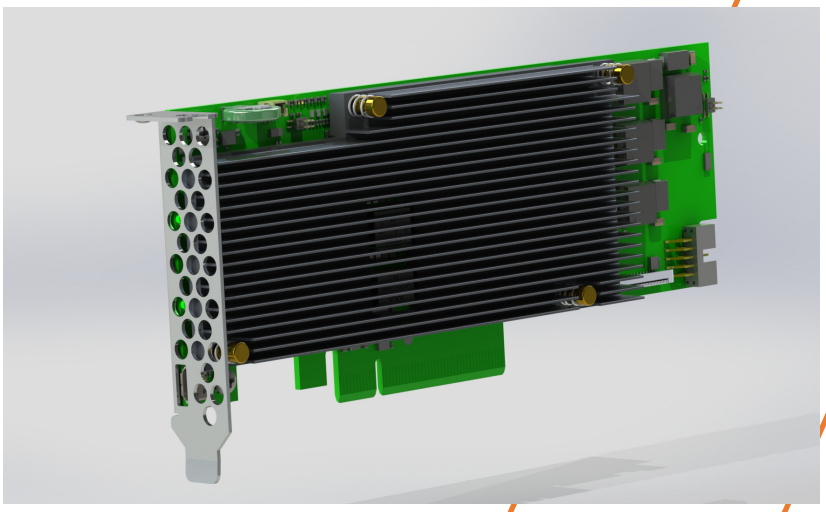
- CNSA Suite Support
- Symmetric: AES (CBC, GCM, CTR, ECB, F8), Triple DES, DES, RC4
- Hashing: MD5, SHA-1, SHA-2
- Authentication: HMAC-MD5, HMAC-SHA-1, HMAC-SHA-2, GMAC (AES), XCBC MAC, CMAC, SSL 3.0 MAC
- Asymmetric: RSA and DH (up to 4K bits), DSA, ECDH and ECDSA (P-192 to P-521), X25519
- Random Number Generator: SP800-90 DRBG
- FPGA Reprogrammability
- Key Storage: 128 MB
- Supported Operating Systems: Linux
- API Support: PKCS #11, Java, OpenSSL

Software designed in USA
Hardware manufactured in USA

HSM

Hardware Security Modules





ENVIETA™

7175 Columbia Gateway Dr., Ste. T, Columbia, MD 21046 | T: 410.290.1136 | F: 410.290.1168 | info@envieta.com