

Where cryptographic services are used to protect an information system, trust and integrity are derived from the security of the underlying signing and encryption keys. This makes protection of these keys critical to the overall trust and integrity of a system.

Cryptographic key material can be stored and protected in a variety of ways and on a variety of media including software, smart cards and USB tokens. However, where protection is critical, the level of security offered by these solutions may not always be enough. Storing and protecting key material on a physically separate Hardware Security Module (HSM) is the only viable option.

A critical element in the architecture and deployment of a cryptographic system is the design and flexibility that a HSM can afford the system. In choosing a HSM, a range of options need to be considered:

- What connectivity does the HSM offer?
- What key storage capability does the HSM offer?
- What tamper detection does it provide?
- How many hosts can be connected to a single HSM?
- Can multiple hosts share the same HSM?
- Can the HSM be upgraded at a future point without requiring a return to the manufacturer?

AEP Series K: The Ultimate Protection of Key Material

AEP Networks has designed the Series K range of HSMs which offer the ultimate level of protection for the most sensitive data and information systems. At the heart of AEP Series K is AEP Networks' revolutionary ACCE technology.

ACCE is the next generation flexible crypto platform that provides the highest level of assurance – FIPS 140-2, Level 4. Based on this core technology, AEP Networks has built a comprehensive product range to cater to the PKI, VPN and Web markets.

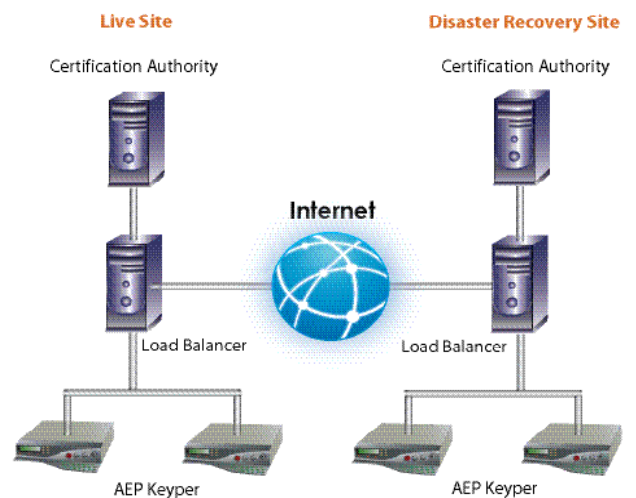
The AEP Series E is ideally suited to businesses deploying a cryptographic system where the protection of cryptographic keys is a priority, for example, in organizations requiring certificate signing, code or document signing, bulk generation or ciphering of keys or data. Series K is available in two models that offer two levels of storage capacity, Enterprise and Professional.

Series K Features and Benefits



- Connectivity – Ethernet connectivity offering greater scalability and flexibility
- Manageability – Small footprint allows desktop use or rack mounting
- Design – Fully integrated module with smart card reader, PIN entry and cryptographic processing within a single device
- Performance – Increases the number of crypto operations achievable
- Fault Tolerance – Extended reliability through automated switch-over to live module
- Load Sharing – Software available to load balance multiple modules with one or multiple hosts
- Architecture – Built on ACCE giving tamper protection to FIPS 140-2, Level 4
- Scalability – Up to 16 modules can be connected to a single host
- Choice of Interfaces – On host PKCS#11 and Microsoft CSP interfaces
- Field Upgradable – Ability to upgrade firmware and algorithms in the field
- Support for latest algorithms
- Authenticated use of keys that are optionally PIN activated
- Drivers for Windows, Linux and Solaris

Configuration Diagram



Technical Specifications

Series K Enterprise	Series K Professional
Cryptographic Functions and Services	
<ul style="list-style-type: none"> ▶ RSA: 512 to 4096 bit key length ▶ DSA: 512 to 1024 bit key modulus ▶ AES: 128, 192 & 256 bit key length ▶ DES/3DES: 56,112,168 bit key lengths ▶ Diffie Hellman: Up to 2,048 bit key length ▶ Hash: SHA-1, SHA-2, MD-5 ▶ Performance: In excess of 1,200 tps (1024 bit signature) 	<ul style="list-style-type: none"> ▶ RSA: 512 to 4096 bit key length ▶ DSA: 512 to 1024 bit key modulus ▶ AES: 128, 192 & 256 bit key length ▶ DES/3DES: 56,112,168 bit key lengths ▶ Diffie Hellman: Up to 2,048 bit key length ▶ Hash: SHA-1, SHA-2, MD-5 ▶ Performance: In excess of 300 tps (1024 bit signature)
Operator Interface	
<ul style="list-style-type: none"> ▶ Key entry from the smart card is possible under dual control (four eye-principle) using the key switch and access control via smart card 	
Random Number Generation	
<ul style="list-style-type: none"> ▶ Hardware random number generator with full entropy ▶ FIPS 186-2 compliant 	
Key Management	
<ul style="list-style-type: none"> ▶ Storage Master Key (SMK) import/export via smart cards in M of N components ▶ Application Key import/export via smart cards protected with SMK 	
Key Storage	
<ul style="list-style-type: none"> ▶ Red Key Store: Keys temporarily in clear text, actively erased when a tamper is detected ▶ Black Key Store: large key store encrypted under the SMK 	
Connectivity	
<ul style="list-style-type: none"> ▶ TCP/IP over Ethernet at 10/100 Mbps full/half duplex with auto-negotiation ▶ Up to 32 concurrent TCP/IP connection 	
Standards Certification	
<ul style="list-style-type: none"> ▶ FIPS 140-2, Level 4 ▶ FCC part 15 Class B ▶ BSEN60950 Safety ▶ BSEN61000 Susceptibility, Performance B ▶ BSEN55022 Level B Emissions 	
Operating Environment	
+5°C to 40°C	
Operating Humidity Range	
25% to 90%, non-condensing	
Power Requirements	
100-240 VAC, 47-63Hz	
Product Dimensions	
223 x 45 x 244 mm	
Maximum Battery Lifetime	
10 Years	
ACCE (Advanced Configurable Crypto Environment)	
<ul style="list-style-type: none"> ▶ All AEP HSMs incorporate ACCE technology – the most advanced crypto hardware environment available ▶ AEP Networks' leading hardware and crypto engineers have over 100 years of combined experience to bring new levels of security, speed and manageability to a range of hardware security devices ▶ ACCE supports a range of authorized Key Management options with protected internal key store for over 8000 keys, backed by secure key export and transport options ▶ All AEP modules can be upgraded with new software and algorithms. Standard algorithms include RSA, DSA, AES, 3 DES, Diffie-Hellman, MD-5, SHA-1 and SHA-2 ▶ ACCE's low power, highly integrated design leads to increased reliability and savings in overall lifecycle costs 	

Accreditation



United States

Toll-Free: +1-877-638-4552
Tel: +1-732-652-5200

Email: sales@aepnetworks.com Web: www.aepnetworks.com

Europe

Tel: +44 1344 637 300

Greater China

Tel: +8621 5116 7120

SE Asia, Singapore

Tel: +852 2961 4566

Australia/New Zealand

Tel: +61 2 9413 2282

Japan

Tel: +8180 5645 4503

Malaysia

Tel: +60 32166 2260