AEP Series K
Hardware Security Module
Product Information

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 Keyper is AEP Networks' revolutionary ACCE technology.

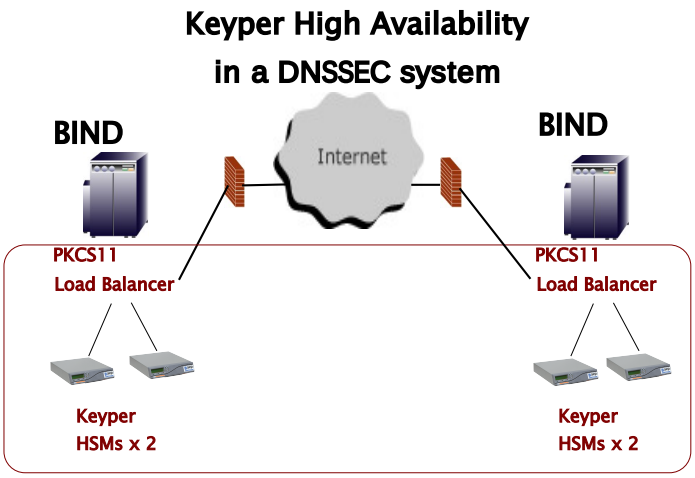
ACCE is the next generation flexible crypto platform that provides the highest level of assurance – FIPS 140-2, Level 4. Based on this core technology, AEP Networks has built a comprehensive product range to cater to the PKI, VPN and Web markets.

The AEP Series K 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 four models offering various levels of scale: Professional, Enterprise, Professional High Availability, Enterprise High Availability.

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
- Scaleable performance – Increases the number of crypto operations achievable
- Fault Tolerance
- Load Sharing – Software available to load balance multiple modules with one or multiple hosts
- Architecture – Built on ACCE giving tamper reaction to FIPS 140-2, Level 4 (certificate1340)
- Scalability – Up to 16 modules can be connected to multiple hosts
- Choice of Interfaces – On host PKCS#11 and Microsoft CSP interfaces
- Field Upgradable – Ability to upgrade firmware and algorithms in the field
- Support for the latest algorithms
- Authenticated use of keys that are optionally PIN activated
- Drivers for Windows, Solaris, Free BSD, GNU Linux and MAC OSX

Configuration Diagram



AEP Series K
Hardware Security Module
Product Information

Technical Specifications

Series K

Cryptographic Functions and Services

- RSA: 1024 to 4096 bit key length
- DSA: 1024 bit key modulus
- AES: 128, 192 & 256 bit key length
- DES/3DES: 112,168 bit key lengths
- Hash: SHA-1, SHA-2, MD-5
- Performance: From 300 tps to 4800 tps depending upon the product

Random Number Generation

- Hardware random number generator with full entropy
- FIPS 186-2 compliant (certificate 699)

Key Management

- Storage Master Key (SMK) import/export via smart cards in M of N components
- Application Key import/export via smart cards protected with an internal Master Key

Key Storage

- 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

- TCP/IP over Ethernet at 10/100 Mbps full/half duplex with auto-negotiation
- Up to 32 concurrent TCP/IP connection

Standards Certification

- 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

5 Years minimum

ACCE (Advanced Configurable Crypto Environment)

- 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, 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

FIPS VALIDATED 140-2

GSA FIPS 201 APPROVED

United States
Toll-Free: +1-877-638-4552
Tel: +1-732-652-5200
Email: sales@aepnetworks.com

Europe
Tel: +44 1344 637 300
Web: www.aepnetworks.com

Greater China
Tel: +8621 5116 7120

SE Asia, Singapore
Tel: +852 2961 4566

Japan
Tel: +81 3 5979 2149

Australia/New Zealand
Tel: +61 2 9413 2282

Malaysia
Tel: +60 32166 2260