

ABOUT AEP NETWORKS

AEP Networks, the specialist in network and application access security, delivers infrastructure security solutions that are easy to use and manage while offering exceptional value and mission-critical reliability. The company provides a full range of innovative secure networking and application access products to meet the most demanding requirements of public-sector and commercial customers.



KEYPER ENTERPRISE



AEP KEYPER ENTERPRISE

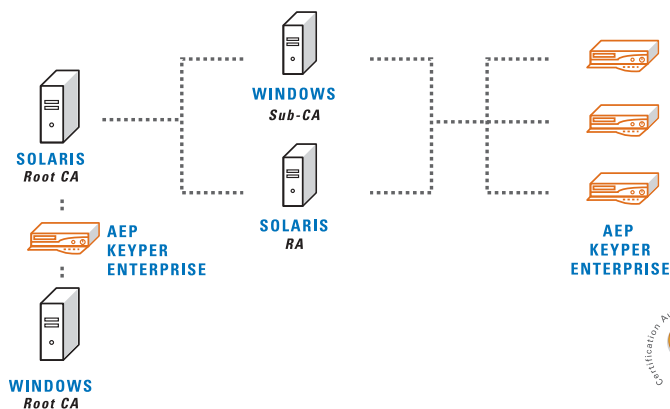
Where cryptographic services are used to protect an information system, trust and integrity are derived from the security of the underlying signing and encryption keys. This makes protection of these keys critical to the overall trust and integrity of a system.

Cryptographic key material can be stored and protected in a variety of ways and on a variety of media e.g. software, smart cards and USB tokens, to name but a few. However, where protection is paramount, 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 truly 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 needs 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 manufacturer?

Configuration Diagram



Ultimate Protection of Key Material

AEP Networks has designed the Keyper 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 Network's 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 for the PKI, VPN and Web markets.

AEP Keyper Enterprise 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.

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 Upgradeable – Ability to upgrade firmware and algorithms in the field
- Support for latest algorithms, AES
- Authenticated use of keys that are optionally PIN activated
- Drivers for Windows, Linux and Solaris



Technical Specifications

Cryptographic Functions and Services

RSA:	512 to 4096 bit key length
DSA:	512 to 1024 bit key modulus
AES:	128 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 (Q3 2005), MD-5
Performance:	In excess of 1,200 tps (1024 bit signature)

Operator Interface

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

Hardware random number generator with full entropy
FIPS 186-1 compliant.

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 SMK.

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 connections.

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

Battery Lifetime

10 years

ACCE (Advanced Configurable Crypto Environment)

- All AEP products 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, and configured remotely. Standard algorithms include RSA, DSA, AES, 3 DES, Diffie-Hellman, MD-5 and SHA-1
- ACCE's low power, highly integrated design leads to increased reliability and savings in overall lifecycle costs

Contact us:

CORPORATE HEADQUARTERS

347 ELIZABETH AVE., SUITE 100
SOMERSET NJ 08873
TOLL-FREE: 1 877 638 4552
TEL: (+1) 732 652 5200

ASIA-PACIFIC

2107 TOWER 2
LIPPO CENTRE 89 QUEENSWAY
HONG KONG
TEL: (+852) 2845 1118

GOVERNMENT SOLUTIONS GROUP

40 WEST GUDE DRIVE, SUITE 200
ROCKVILLE, MD 20850
TOLL-FREE: 1 800 495 8663
TEL: (+1) 240 399 1200

JAPAN

JOYO BLDG 6-22-6
SHIMBASHI MINATO-KU
TOKYO 105-0004
JAPAN
TEL: (+81) 3 3432 3336

EUROPE

FOCUS 31, WEST WING
CLEVELAND ROAD
HEMEL HEMPSTEAD
HERTS HP2 7BW U.K.
TEL: (+44) 1442 458 600

Accreditation

