



AEP SureWare Keyper Professional

e-Security hardware for enhanced security
and performance

In any PKI environment, security is the cornerstone on which the trust and integrity of the certification service is built. Trust and integrity in a PKI are derived from the security of the underlying signing/encryption keys, therefore the protection of this material is critical to the overall trust and integrity of the system. Key material can be stored and protected in many ways on a variety of mediums, such as in software on a hard drive, protected on a smart card or USB token, or for ultimate protection, on a hardware security module (HSM) designed to protect key material independently of the PKI or cryptographic system.

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 manufacturer?

Ultimate Protection of key material

AEP Systems has designed a range of hardware security modules capable of protecting the most sensitive data or system, SureWare.

AEP SureWare Keyper Professional is a hardware security module offering the highest level of security and performance in PKI environments, where the management and storage of cryptographic keys is essential. AEP SureWare Keyper offers protected key storage, high-speed signature and hardware key generation.



KEY 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 a single or multiple hosts

ARCHITECTURE

Built on ACCE giving tamper protection to FIPS 140-1, Level 4 & ITSEC E3

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

ACCE

(Advanced Configurable
Crypto Environment)

All AEP SureWare products incorporate ACCE technology - the most advanced crypto hardware environment available.

AEP Systems' leading hardware and crypto engineers have combined over 100 years of experience to bring new levels of security, speed and manageability to a range of hardware security devices.

All critical security functions are housed within the tamper detection envelope, which is accredited to FIPS 140-1 Level 4 and ITSEC E3.

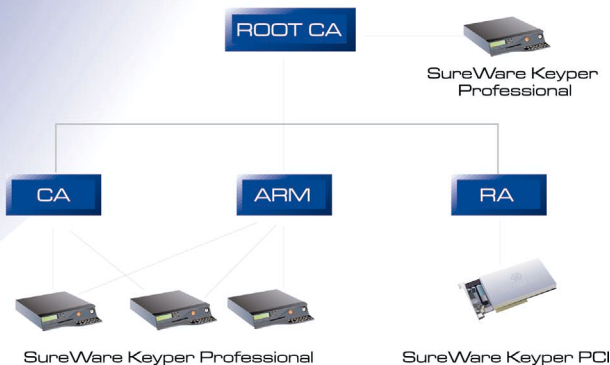
ACCE supports a range of Key Management options, with protected internal key store for over 1,000 keys, backed by secure key export and transport options.

All AEP SureWare modules can be upgraded with new software and algorithms, and configured remotely. Standard algorithms include 3-DES, RSA, DSA, Diffie-Hellman, MD5 and SHA-1.

ACCE's low power, highly integrated design leads to increased reliability and savings in overall lifecycle costs.



**EXAMPLE INSTALLATION :
CERTIFICATE AUTHORITIES**



SureWare Keyper Professional is a FIPS 140 - 1, Level 4 & ITSEC E3 certified module capable of generating, securing and managing cryptographic data. SureWare Keyper Professional has an Ethernet interface for complete flexibility enabling multiple hosts and systems to share a single Keyper concurrently. It employs tamper detection to FIPS 140-1, Level 4 and ITSEC E3; the highest assurance of any hardware module worldwide and each module is capable of storing up to 1000 keys inside the module and can be securely upgraded in the field.

The SureWare Keyper Professional has an integrated keypad, LCD display, smart card reader and physical key switch enabling operators to backup key material from the module, reconfigure the security settings and enable/ disable the cryptographic services.

AEP SureWare Keyper is ideally suited to businesses deploying a PKI or cryptographic system where the protection of cryptographic keys is a priority, for example PKI Signing, Commercial CAs, transaction, code or document signing or bulk generation or ciphering of keys or data.

CRYPTOGRAPHIC FUNCTIONS AND SERVICES

RSA: 512 to 2,048 bit key length
DSA: 512 to 1,024 bit key length
Des/3DES: 56, 112, 168 bit key lengths
DIFFIE HELLMAN: Up to 2,048 bit key length
HASH: SHA-1, MD5

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: Runner personality keys and application keys encrypted under a key from the Secure Key Store.

CONNECTIVITY

TCP/IP over Ethernet at 10/100 Mbps full/half duplex, with auto-negotiation.
 Up to 4 concurrent TCP/IP connections

STANDARDS CERTIFICATION

FIPS PUB 140-1, Level 4
 ITSEC E3 Certified
 FCC part 15 Class B
 BSEN60950 Safety
 BSEN61000 Susceptibility, performance B
 BSEN55022 Level B Emissions

OPERATING ENVIRONMENT

+5 degrees C to 40 degrees 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

USA
 AEP Systems Inc.
 30 Rowes Wharf
 Boston, MA 02110

Tel: 1.800.383.7716
 Fax: (+1) 617.443.0160
 E-mail: info@aepsystems.com

Europe
 AEP Systems Ltd.
 Bray Business Park
 Southern Cross Route
 Bray, Co. Wicklow
 Ireland

Tel: (+353 1) 204 1300
 Fax: (+353 1) 204 1301
 E-mail: info@aepsystems.com

Asia-Pacific
 AEP Systems Co., Ltd.
 2107 Tower 2, Lippo Centre
 89 Queensway
 Hong Kong

Tel: (+852) 2845 1118
 Fax: (+852) 2845 9240
 E-mail: info@aepsystems.com

For more information,
 visit www.aepsystems.com

www.aepsystems.com