Key business benefits

- Assurance - the only FIPS 140-2 Level 4 HSM
- Capability - broad range of algorithms including AES, ECDSA
- Compatibility - supports numerous third-party security applications, operating systems
- Scalability - load-sharing across multiple devices
- Reliability - resilience and disaster recovery configurations
- Pedigree - long history of use in blue chip companies

Applicable markets

- Enterprise PKI, Authentication & DNSSEC
- Registration, certification & validation authorities
- Digital Signature - Email, Doc, Code (Software), Firmware
- Internet domain name organisations
- Online content providers
- Electronic gaming companies

Keyper HSM

Datasheet

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, making the HSM a critical element in the architecture of any security system.

"Security is a critical factor for ICANN's DNSSEC deployment...

...so Keyper & FIPS Level 4 was an easy choice"

Richard Lamb, ICANN

Choosing the right HSM

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 the HSM be upgraded at a future point without requiring a return to the manufacturer?

AEP | Ultra ELECTRONICS

Keyper: The ultimate protection of key material

Ultra Electronics AEP has designed the Keyper range of HSMs to provide the ultimate level of protection for the most sensitive data and information systems. At the heart of Keyper is AEP'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 has built a product range to cater to the PKI, VPN and Internet security markets. The Keyper HSM 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.

The Keyper HSM is available in three models offering various levels of scale and performance:

- Keyper Professional
- Keyper Enterprise
- Keyper *Plus*

Keyper Features and Benefits

- Architecture - Built using ACCE giving tamper protection to FIPS 140-2 Level 4
- Design - Integrated smart card reader, PIN entry and cryptographic processing
- Fault Tolerance - Supports resilient configurations
- Scalability - Load balancing of multiple HSMs across multiple hosts
- Choice of Interfaces - PKCS#11, Microsoft CAPI, Java JCE/JCA
- Connectivity - Ethernet connectivity offering greater scalability and flexibility
- Manageability - Small footprint allows desktop use or rack mounting
- Field Upgradable – Upgrade firmware and algorithms in the field
- Authenticated Use of Keys - Optionally PIN activated
- Operating Systems - Linux, Free BSD, Solaris and Windows

AEP | Ultra ELECTRONICS

Technical Specifications

	Keyper Professional Keyper Enterprise	Keyper *Plus*
Product Dimensions	223 x 51 x 244 mm	
Power Requirements	100 – 240VAC, 47-63 Hz (42VA)	100 – 240VAC, 47-63 Hz (65VA)
Cryptographic Functions and Services	• RSA: 1024-4096 bit key length • DSA: 1024 bit key modulus • AES: 128-256 bit key length • DES/3DES: 112/168 bit key length • Hash: SHA-1, SHA-2, MD5	• ECDSA: P192-P521 curves • ECDH: P192-P521 curves • RSA: 1024-4096 bit key length • DSA: 1024 bit key modulus • AES: 128-256 bit key length • 3DES: 168 bit key length • Hash: SHA-2
Performance (key signing, using up to 8 connections)	• Keyper Professional: 300 tps (RSA 1024) • Keyper Enterprise: 1,200 tps (RSA 1024)	• >3,500 tps (RSA 1024) • >2,000 tps (RSA 2048) • >950 tps (ECDSA 256)
Random number generation	Hardware random number generator with full entropy (FIPS 186-2 compliant)	
Administrator Roles	• Security Officer • Operator	• Security Officer • Crypto Officer • Operator
Key management	• Storage Master Key (SMK) import/export via smart cards in M of N componens • Application Key import/export via smart cards protected with an internal Master Key (also via USB on Keyper *Plus*)	
Key storage	• Red Key Store: keys actively erased when a tamper is detected • Black Key Store: large key store encrypted under the SMK	
Connectivity	• TCP/IPv4 over Ethernet at 10/100 Mbps full/half duplex with auto-negotiation • Up to 32 concurrent connections	• TCP/IPv4 and IPv6 over Ethernet at 10/100/1000 Mbps full/half duplex with auto-negotiation • Up to 256 concurrent connections
Certification	• FIPS 140-2 Level 4 (cert. #1340) • Common Criteria EAL4+	• FIPS 140-2 Level 4 (expected 2013) • FIPS 140-3 Level 4 (expected 2014)
Operating Environment	• Operating temp: 5 to 40 °C (25 to 90% humidity, non-condensing) • Storage temp: -15 to 65 °C	
Host Software	• Keyper Management Centre • PKCS#11 Provider • MS-CAPI Provider • CNG Provider • Load Balancer (optional)	• Keyper Management Centre • PKCS#11 Provider • MS-CAPI Provider • CNG Provider • Load Balancer (optional)

Ordering information

Product	Ordering Part Number
Keyper Professional	KEY-PRO
Keyper Enterprise	KEY-ENT
Keyper *Plus*	KEY-PLS

AEP | Ultra ELECTRONICS

Ultra Electronics
AEP
Knaves Beech Business Centre
Loudwater
High Wycombe
Buckinghamshire, HP10 9UT
Main Switchboard: +44 (0)1628 642 600
Email: info@ultra-aep.com
www.ultra-aep.com
www.ultra-electronics.com

ISO 27001