ULTRA SAFE KEYPER*PLUS* HARDWARE SECURITY MODULE

KEY BUSINESS BENEFITS

- ASSURANCE - THE ONLY STAND-ALONE HSM WITH FIPS 140-2 LEVEL 4
- 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

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.

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

"Security is a critical factor for ICANN's DNSSEC deployment, AEP's Keyper HSM & FIPS Level 4 was an easy choice" - Richard Lamb,

APPLICABLE MARKETS

- ENTERPRISE PKI, AUTHENTICATION & VPN
- REGISTRATION, CERTIFICATION & VALIDATION AUTHORITIES
- DIGITAL SIGNATURE - EMAIL, DOC, CODE (SOFTWARE), FIRMWARE
- INTERNET DOMAIN NAME ORGANISATIONS, DNSSEC
- ONLINE CONTENT PROVIDERS
- ELECTRONIC GAMING COMPANIES

KEYPER*PLUS*: THE ULTIMATE PROTECTION OF KEY MATERIAL

Ultra Electronics AEP has designed the Keyper*Plus* range of HSMs to provide the ultimate level of protection for the most sensitive data and information systems. At the heart of Keyper*Plus* 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*Plus* HSM is ideally suited to businesses deploying a cryptographic system where the protection of cryptographic keys is a priority, for example, in organisations requiring certificate signing, code or document signing, bulk generation or ciphering of keys or data.

The Keyper*Plus* HSM is available in three models to suit differing requirements:

- Keyper*Plus*
- Keyper*Plus* 10 Key Licence
- Keyper*Plus* Without ECC

KEYPER*PLUS* 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
- Availability - Optional Redundant Power Module
- Scalability - Load balancing of multiple HSMs across multiple hosts
- Choice of Interfaces - PKCS#11, Microsoft CAPI/CNG, Java JCE/ JCA
- Connectivity - Ethernet connectivity offering greater scalability and flexibility
- Manageability - Local or remote management using Keyper Management Centre
- Field Upgradable – Upgrade firmware and algorithms in the field
- Authenticated Use of Keys - Optionally PIN activated
- Operating Systems - Linux, FreeBSD, Solaris and Windows

ORDERING INFORMATION

Product	Ordering Part Number
Keyper*Plus*	KEY-PLS
Keyper*Plus* 10 Key Licence [1]	KEY-PLS-10
Keyper*Plus* Without ECC [2]	KEY-PLS-NE

[1] Licensed for applications requiring a maximum of 10 private keys
[2] ECDSA and ECDH algorithms not included (can be subequently soft-upgraded via license key)

OPTIONS & ACCESSORIES

- Keyper Load Balancer
- Rack Mount Shelf
- Redundant Power Module
- Smart Cards
- Training
- Professional Services

TECHNICAL SPECIFICATIONS

Product Dimensions	223 x 51 x 244 mm
Power Requirements	100 – 240VAC, 47-63 Hz (65VA) Optional Redundant Power Module Clean power feed required to avoid triggering tamper protection
Batteries	• Built-in batteries for tamper protection when unpowered • Minimum life-expectancy 5 years at room temperature
Cryptographic Functions and Services (firmware v3.0)	• ECDSA curves: - P192 – P521 - brainpoolP224r1 - P512r1 - brainpoolP224t1- P512t1 - secp256k1 • ECDH curves: - P192 – P521 - brainpoolP224r1 - P512r1 - brainpoolP224t1- P512t1 • RSA: 1024 - 4096 bit key length • DSA: 1024 bit key modulus • AES: 128 - 256 bit key length • 3DES: 168 bit key length • SEED: 128 bit key length • Hash: SHA-2, RIPEMD-160
Performance (key signing, using up to 8 connections)	• >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 • Crypto Officer • Operator
Key Management	• Storage Master Key (SMK) import/export via smart cards in M of N components • Application Key import/export via smart card or USB protected with an internal Master Key
Key Protection	• Red Key Store: keys actively erased when a tamper is detected • Black Key Store: large key store encrypted under the SMK
Key Storage	• 15,000 keys (any size)
Connectivity	• TCP/IPv4 and IPv6 over Ethernet at 10/100/1000 Mbps full/half duplex with auto-negotiation • Up to 256 concurrent connections
Device Management	• Local or remote using Keyper Management Centre (remote management requires firmware v3.0 or later)
Crypto Module Certification	• FIPS 140-2 Level 4 (cert. #2298) firmware v2.4
Tamper Protection	• Sensitive data is encrypted under a master key that is zeroised if physical tampering, anomalous voltages or unexpected temperature variations are detected, or if the batteries fail when the unit is unpowered • Units have tamper-evident seals and are supplied in serialised, tamper-evident packaging
Operating Environment	• Operating temp: 5 to 40 °C (25 to 90% humidity, non-condensing) • Storage temp: -15 to 65 °C • Exceeding these limits will trigger the tamper protection
Host Software	• PKCS#11 Provider • MS-CAPI Provider • MS-CNG Provider • Keyper Load Balancer (optional)

making a difference

Ultra Electronics
AEP
419 Bridport Rd,
Greenford,
Middlesex UB6 8UA
Main Switchboard: +44 (0)1628 642 600
Email: info@ultra-aep.com
www.ultra-aep.com
www.ultra-electronics.com

IDGP

20416 Bashan Drive
Suite 201
Ashburn, VA 20147

Phone: 424.285.0015
Email: sales@id-gp.com
Web: id-gp.com