ULTRA

FIPS 140-2
Level 4 Certified

Keyper^{PLUS}

HARDWARE SECURITY MODULE

Key features

Assurance - The only stand-alone HSM with NIST FIPS 140-2 Level 4 certification

Capability - Provides for secure key generation and storage, encryption/decryption, digital signature generation/verification using a broad range of algorithms, including AES, RSA, DSA, ECC (various curves)

Flexibility - Software Development Kit supplied for bespoke security application development and technical support

Pedigree - Over 20 years history of trusted use worldwide by blue chip companies and market leaders in a range of sectors, including online retail, digital entertainment distribution, banking and internet infrastructure administration

Scalability - Load sharing across up to 16 devices.

Reliability - Resilience and disaster recovery configurations

Reactive anti-tamper mechanisms (even when unpowered)

Hardware cryptographic acceleration

Chip and PIN smartcard multi-operator authentication

Local and remote management facilities via included software

Customisable cryptographic mechanism configuration

Large internal key storage capacity

Compatible with Windows and Linux operating systems

Ability to remote backup cryptographic keys using Keyper Management Centre

ultra.group

Overview

The Keyper^{PLUS} Hardware Security Module (HSM) provides robust and reliable cryptographic technologies to give the ultimate layer of protection for your most sensitive key material, used to protect your most highly securely information. Going far beyond the layers of security offered by mediums including software, smart cards and USB tokens. Trust and integrity are derived from the security of the underlying signing and encryption keys, meaning that the protection of these keys is critical to the security of the system.

Storing and protecting key material on a physically separate HSM is the only viable option to ensure the highest levels of security and protection, making the HSM a critical element in the architecture of any security system.

FIPS 140-2 security levels explained

	General Requirements for all Embodiments	Multiple-Chip Standalone Cryptographic Modules	Keyper^{PLUS}
Security Level 4	Environmental Failure Protection or Environmental Failure Testing for temperature and voltage	Tamper detection/ response envelope with tamper response and zeroization circuitry.	✓
Security Level 3	Automatic zeroization when accessing the maintenance access interface. Tamper response and zeroization circuitry. Protected vents.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong enclosure with removal/ penetration attempts causing serious damage.	✓
Security Level 2	Evidence of tampering (e.g., cover, enclosure, or seal).	Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	✓
Security Level 1	Production-grade com-ponents (with standard passivation).	Production-grade enclosure.	✓

Source: NIST

ULTRA

Keyper^{PLUS} the ultimate protection of key material

Keyper^{PLUS} features and benefits

Architecture - Hardware tamper protection to FIPS-140-2 Level 4 certification

Design - Integrated smart card reader, PIN entry and cryptographic processing

Availability - Redundant power module option

Choice of interfaces - PKCS#11, Microsoft CAPI/CNG, Java PKCS#11 wrapper

Connectivity - Ethernet connectivity offering greater scalability and flexibility

Manageability - Local or remote management using keyper management centre

Field upgradable - Ability to upgrade firmware in the field

Ultra's Keyper^{PLUS} range of HSMs is the only module to be certified to FIPS 140-2 Level 4, ensuring the highest standards of security and protection available on the market. Keyper^{PLUS} secures the most sensitive data and information systems, employing the next generation flexible crypto platform that provides the highest level of assurance over the integrity of the information it holds.

Keyper^{PLUS} has been specifically designed to limit all potential points of access with a tamper-resistant design, ensuring only those with intended permission are able to access the sensitive data it protects. Through rigorous and careful management of any areas of physical or digital infiltration, Keyper^{PLUS} delivers a robust solution that meets the most stringent of security standards.

Based on this core technology, Ultra 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.

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

ULTRA

Technical Specification

Product Dimensions	223 x 51 x 244 mm
Power Requirements	100 – 240VAC, 47-63 Hz (65VA) Optional Redundant Power Module
Batteries	Built-in batteries for tamper protection when unpowered Minimum life-expectancy 5 years at room temperature
Cryptographic Functions and Services (firmware 3.4)	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 - 2048 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	Master key which encrypts all user keys, is erased when a tamper is detected.
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)
Firmware v2.3, v2.4, v3.2, v3.3, v3.4	FIPS 140-2 Level 4 (cert. #2793)
Tamper Protection	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
Host Software	Keyper PKCS#11 Provider Keyper Key Storage Provider (CNG) Keyper CSP Providers Keyper Load Balancer (extra cost option)

ULTRA

Ordering Information

Product	Ordering Part Number
Keyper[PLUS]	AEP-KEY-PLS

Options and Accessories:

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

Cyber
Ultra Intelligence & Communications
sales@ultra-us-gbs.com
ultra.group