Ultra Safe

Product line overview

Cryptographic keys are now used to protect a variety of digital assets including online music, software, electronic gaming machines and DNSSEC records. It is critical that the underlying infrastructure supporting the generation, management and use of the encryption keys is protected to provide trust and integrity of the overall system.

The Ultra Safe product line stores and protects cryptographic keying material on a purpose built and physically separate Hardware Security Module (HSM) called Keyper.

The Ultra Electronics AEP Keyper HSM is designed to ensure that the generation, storage and management of cryptographic keys meets the high level of security demanded by organisations.

Available in the following versions:
- Professional
- Enterprise (Enhanced throughput)
- Plus (Support for Elliptic Curve)

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

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

Richard Lamb, ICANN

Key benefits to business

- The only FIPS 140-2 level 4 Hardware Security Module
- Tamper reactive key management
- The HSM's high assurance tamper reactive mechanisms are aimed at defending assets, IPR and reputation through strengthened security keys, processes and role management.

Applicable markets

- Online content providers
- Electronic gaming companies
- Registration, certification & validation authorities
- Internet domain name organisations

AEP | Ultra ELECTRONICS

High quality key generation

In order to ensure the security and integrity of the cryptographic system, it is important to have keys which are derived from a truly random seed. The random seed is fed into a pseudo random number generator and the result is passed into the key generator. The Keyper uses the highest quality random seed generator which results in the highest quality keys being generated.

Key protection

Once keys have been generated, they need to be stored securely in order to maintain the integrity of the entire cryptographic system. To achieve this, the associated hardware has to be reactive to attack.

The AEP Keyper hardware and firmware have been purpose built to meet these strict requirements.

The proprietary hardware is validated to US Government NIST FIPS-140-2 level 4 which means that in the event of it being subject to power, temperature, chemical or physical attack, the unit positively destroys the private and secret keys to ensure that they are not stolen.

As well as the physical protection of cryptographic keys, AEP's Keyper software is not based on a standard operating system such as Windows or Linux and is therefore not exposed to the vulnerabilities present in these environments. The code is separated from the data which prevents buffer overrun attacks and all firmware downloads are AEP signed and encrypted to ensure the integrity of all new upgrades.

Advanced architecture – security and reliability

Cryptographic systems need to be available at all times to successfully support the applications that are protecting digital assets. The AEP Keyper architecture has been designed with high availability in mind; it is based on solid state technology which means there are no moving parts that can fail.

Load balancing capabilities mean that up to 16 Keyper HSMs can be deployed in parallel to ensure that there is both enough capacity to deal with abnormally high workloads and a high degree of fault tolerance in the event of device failure.

Keyper HSMs are hot swappable which means it is easy to replace a defective device without impacting the operation of the rest of the cryptographic infrastructure.

If a Keyper is not available to handle a transaction then the load balancer automatically re-routes the transaction to another available Keyper.

This load balancing functionality is completely transparent to the requesting application.

Security during operations is enforced by the following measures:

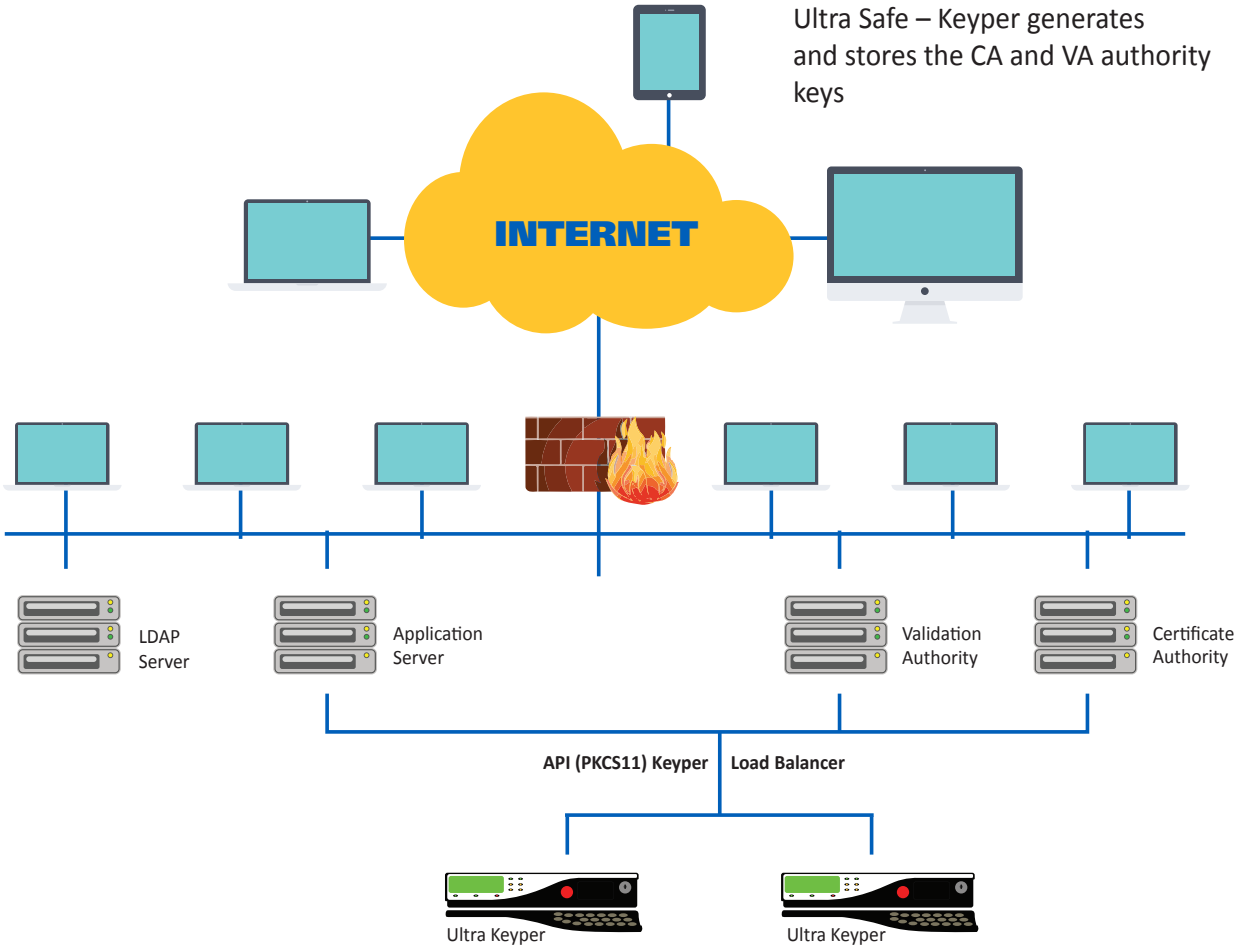
- A PIN is required to authorise key access by applications (PKCS11)
- M of n operator smart cards are required to authorise HSM use by applications
- Multiple layers of key policy restrict what each key can be used for
- M of n security officer smart cards are required for HSM and key management
- Internal firmware is cryptographically authenticated before it is installed or run
- Physical tamper reaction layers prevent key theft

Key management

Unlike other HSMs, the Keyper does not require another device to be connected in order to carry out key management tasks. All management activity is carried out using the built-in LCD, keypad and smart card reader. All key management requires two security officers to be present each with their own smart card and PIN number.

AEP's load balancing functionality allows keys to be automatically and securely distributed between Keyper's regardless of whether they are local to each other or are distributed across multiple sites, this distribution of keys is transparent to the application using the keys.

Ultra Safe - Keyper PKI example:



Model	Distinguishing Features	Certification
Keyper Professional	Low Price	• FIPS 140-2 Level 4 • Common Criteria EAL4+
Keyper Enterprise	Enhanced throughput	
Keyper *Plus*	Elliptic curve algorithm supported	• FIPS 140-2 Level 4 (expected 2014)
Keyper DNSSEC	Instant DNS signing server	• FIPS 140-2 Level 4 (expected 2014)

Typical uses

AEP Keyper's are used by many different organisations including government, finance, telecommunications companies, PKI applications, content providers, electronic gaming machine companies, payment card industry compliance, supply chain, and healthcare electronic patient record security. The table below shows some examples of how:

Customer type	Application	Benefits
Online content provider	Digital signing of online music, software and media	Scalable, secure digital signing of assets to ensure integrity of products being purchased
Electronic gaming companies	Digital signing of slot machine firmware	Ensures that companies comply with regulatory requirements to verify gaming machine software integrity
Registration, certification and validation authorities	Issuing, maintaining, validating PKI identities and certificates	Secure, scalable and reliable infrastructure
Internet domain name organisations	Signing of DNS records (DNSSEC)	Prevents DNS cache poisoning
Enterprise	Digital signing also used for email, documents and software/code	Non-repudiation and authenticity for any transaction

Services

AEP has a wide range of professional services and support packages available to help install, configure and maintain a secure application access infrastructure. For more details please see the Service product sheet.

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