



Key business benefits

- Assurance against loss of cryptographic keys
- Future proofed scalability without initial over specification. HSMs deployed as required will scale to the demand of the highest-performance applications
- Automated fault tolerant service continuity
- Allows for flexibility of Load Balancer placement within the system architecture
- Graceful handling of loads that could otherwise exceed an HSM's capacity
- Enables project to select OS to suit application
- Centralised source for audit across HSM estate, configurable to four levels of detail and three categorisations of events
- Session open, request timeouts and retry timers can be configured to match application requirements for optimal performance across widest range of architectures
- Service continuity in case of unexpected Load Balancer process termination

Keyper HSM Load Balancer Datasheet

The Keyper Load Balancer is a highly flexible piece of software that sits between the Keyper Hardware Security Module (HSM) and its Providers (PKCS#11, Microsoft CAPI/CNG Providers). It allows:

- Scalability - Aggregated performance of multiple HSMs acting in parallel
- Resilience - Active-active high availability HSM configurations
- Automatic Key Backup - key replication over a secured channel
- Geographic DR - Architectures supporting service continuity

All of these services are transparent to the Application and the Provider, without either being 'aware' that any of these services are being performed. Up to 16 Keyper HSMs can be handled, appearing as one logical Keyper to the application accessing those Keyper HSMs via an AEP Provider.

The Keyper Load Balancer itself can be installed on the same host as the application and Provider or can be installed on dedicated hosts.

Keyper Load Balancer supports a wide variety of architectures, including:

- Load Balancer on Application Server(s)
- Load Balancer per Application Server(s)
- Dedicated Load Balancer server(s)
- Application Servers clustered with Load Balancer server(s)
- Geographically distributed Disaster Recovery Load Balancer server(s)

Features

Feature	Benefit
Automatic key distribution amongst load balanced Keyper	Assurance against loss of cryptographic keys
Aggregated performance of multiple HSMs, added on demand	Future proofed scalability without initial over specification. HSMs deployed as required will scale to the demand of the highest-performance applications
Active-active High Availability HSM Architectures, with HSM failure handling	Automated fault tolerant service continuity
Standards based TCP/IP application	Allows for flexibility of Load Balancer placement within the system architecture
Peak load handling	Graceful handling of loads that could otherwise exceed an HSM's capacity
Cross Platform	Enables project to select OS to suit application
Centralised audit collection	Centralised source for audit across HSM estate, configurable to four levels of detail and three categorisations of events
Highly configurable	Session open, request timeouts and retry timers can be configured to match application requirements for optimal performance across widest range of architectures
Process watchdog	Service continuity in case of unexpected Load Balancer process termination

Specifications

- All calls are distributed to the Keyper under least load
- Keys generated or imported are distributed amongst all Keyper being balanced/distributed
- If a Keyper is added after a key has been distributed, the Load Balancer will import that key into that Keyper when that Keyper first receives a call that requires it – where PKCS#11 'no export' attribute is not set
- If a call to a Keyper fails for whatever reason Load Balancer redirects it to another Keyper
- Load Balancer maintains a queue of calls awaiting a free Keyper to become free to process the call. This queue varies in size and response time depending upon a time-out parameter.
- Load Balancer can be allocated a maximum number of calls (tasks) per Keyper
- Load Balancer can reside on a machine other than the Provider
- MS CAPI/CNG Provider and PKCS#11 Providers can share Keyper and their Load Balancer seamlessly but not their keys

Supported Operating Systems

Supported Operating Systems	Architecture
Microsoft Windows	
2008 Server R2	x86_64
2003 Server	x86
Linux	
CentOS 6 (RHEL 6)	x86, x86_64
FreeBSD	
FreeBSD 8.1	x86_64
Sun/Oracle	
Sun Solaris 10	SPARC (64-bit)

Typical Applications

- PKI Certificate Authority
- DNSSEC
- Code, Application and Download Signing
- User- and card-based authentication systems

Product Compatibility

- Keyper Professional
- Keyper Enterprise
- Keyper ^{Plus}

Ordering information

Product	Ordering Part Number
Keyper Load Balancer software (licensed for single server, single Keyper)	KEY-LB
Keyper Load Balancer software (licensed for single server, unlimited Keyper)	KEY-LB1



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

