Scalability of Utimaco HSMs

Info Webcast

Utimaco HSM Academy
Oliver Mueller
Product Trainer

Agenda

- Intro
- Upgrade
- Clustering
- Data Storage

Scalability of Utimaco HSMs

Easy to configure for Scalability

- Easily upgrade your device with a license file
- Set up your HSMs into cluster mode
- Extend the HSMs data storage

Scalability of Utimaco HSMs

Upgrade with a license file

- Se12 → Se52
- Se500 → Se1500 (model with crypto accelerator)
- CSe10 → CSe100




Product	CryptoServer Se-Series Gen 2		CryptoServer CSe-Series	
Form Factor	PCIe plug-in card	LAN	PCIe plug-in card	LAN
Performance (RSA signatures (2048bit) / sec.)	16 / 80 / 690 / 960	16 / 75 / 580 / 780	17 / 90	17 / 90
Models	Se12 / Se52 / Se500 / Se1500	Se12 / Se52 / Se500 / Se1500	CSe10 / CSe100	CSe10 / CSe100

Scalability of Utimaco HSMs

Upgrade with a license file

- Se12 → Se52
- Se500 → Se1500 (model with crypto accelerator)
- CSe10 → CSe100



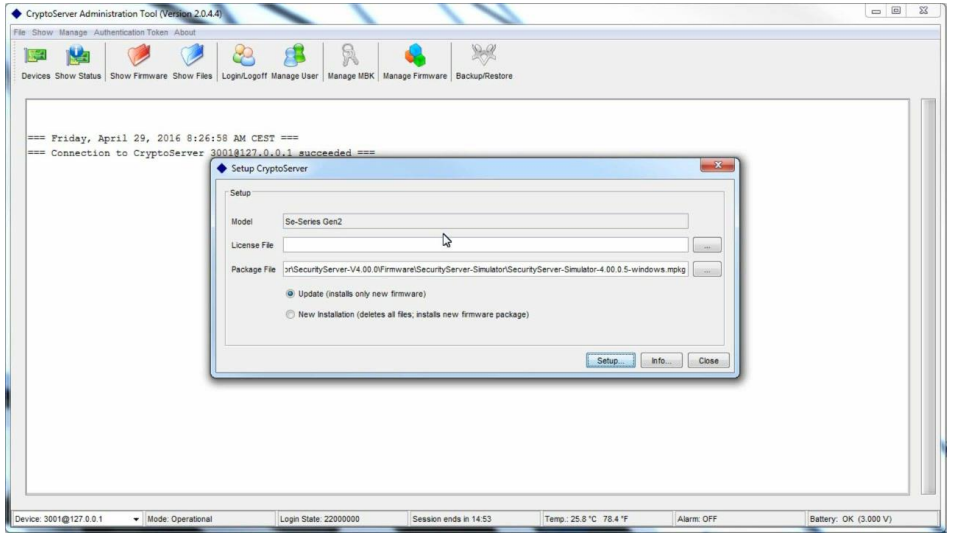

Product	CryptoServer Se-Series Gen 2		CryptoServer CSe-Series	
Form Factor	PCIe plug-in card	LAN	PCIe plug-in card	LAN
Performance (RSA signatures (2048bit) / sec.)	16 / 80 / 690 / 960	16 / 75 / 580 / 780	17 / 90	17 / 90
Models	Se12 / Se52 | Se500 / Se1500	Se12 / Se52 | Se500 / Se1500	CSe10 / CSe100	CSe10 / CSe100

The different HSM model pairs are based on the same hardware platform.

Scalability of Utimaco HSMs

Upgrade with a license file

- Upgrade is possible at anytime
- Without any modification
  - Easily load a license file into the CryptoServer
  - All settings will remain as configured



→For upgrade of the license file a special license file related to the Serial Number of the HSM must be issued by Utimaco.

Scalability of Utimaco HSMs

Upgrade with a license file

- Upgrade is possible at anytime
- Without any modification
  - Easily load a license file into the CryptoServer
  - All settings will remain as configured

→Preferably via CSADM:

```
csadm dev=... logonsign=ADMIN,... loadfile=<licensefile>.slf restart
```

Scalability of Utimaco HSMs

Clustering

- All Utimaco HSMs support clustering
  - Used via APIs

- Possible to use with

  →Load Balancing
  - natively supported by CXI and PKCS#11

  →Failover
  - natively supported by CXI, PKCS#11, CNG/CSP, JCE

Scalability of Utimaco HSMs

Clustering

- Configuration file “cs_pkcs11_R2.cfg”

  - Mode

```
# Configures load balancing mode ( == 0 ) or failover mode ( > 0 )
FallbackInterval = 0
```

  - Devices

```
#[CryptoServer]# Device specifier (here: CryptoServer is logical failover
device of CSLANs with IP address 192.168.0.2, 192.168.0.3 & 192.168.0.4)

Device = { 192.168.0.2 192.168.0.3 192.168.0.4 }
```

Scalability of Utimaco HSMs

Clustering

- Configuration file “cs_pkcs11_R2.cfg”

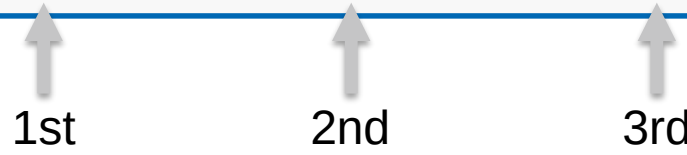
  - Mode

```
# Configures load balancing mode ( == 0 ) or failover mode ( > 0 )
FallbackInterval = 0
```

  - Devices

```
#[CryptoServer]# Device specifier (here: CryptoServer is logical failover
device of CSLANs with IP address 192.168.0.2, 192.168.0.3 & 192.168.0.4)

Device = { 192.168.0.2 192.168.0.3 192.168.0.4 }
```



Scalability of Utimaco HSMs

Clustering

- All CryptoServer have to be accessible for the client computer
  - The HSM has to be connectable via TCP

Scalability of Utimaco HSMs

Clustering

- All CryptoServer have to be accessible for the client computer
  - The HSM has to be connectable via TCP
- All CryproServer have exactly the same firmware versions

Scalability of Utimaco HSMs

Clustering

- All CryptoServer have to be accessible for the client computer
  - The HSM has to be connectable via TCP
- All CryproServer have exactly the same firmware versions
- All CryptoServer have to use exactly the same MBK

Scalability of Utimaco HSMs

Clustering

- All CryptoServer have to be accessible for the client computer
  - The HSM has to be connectable via TCP
- All CryproServer have exactly the same firmware versions
- All CryptoServer have to use exactly the same MBK
- All user databases of the used CryptoServer have to be synchronized
  - Same user accounts and user credentials (password, key file, attributes)

Scalability of Utimaco HSMs

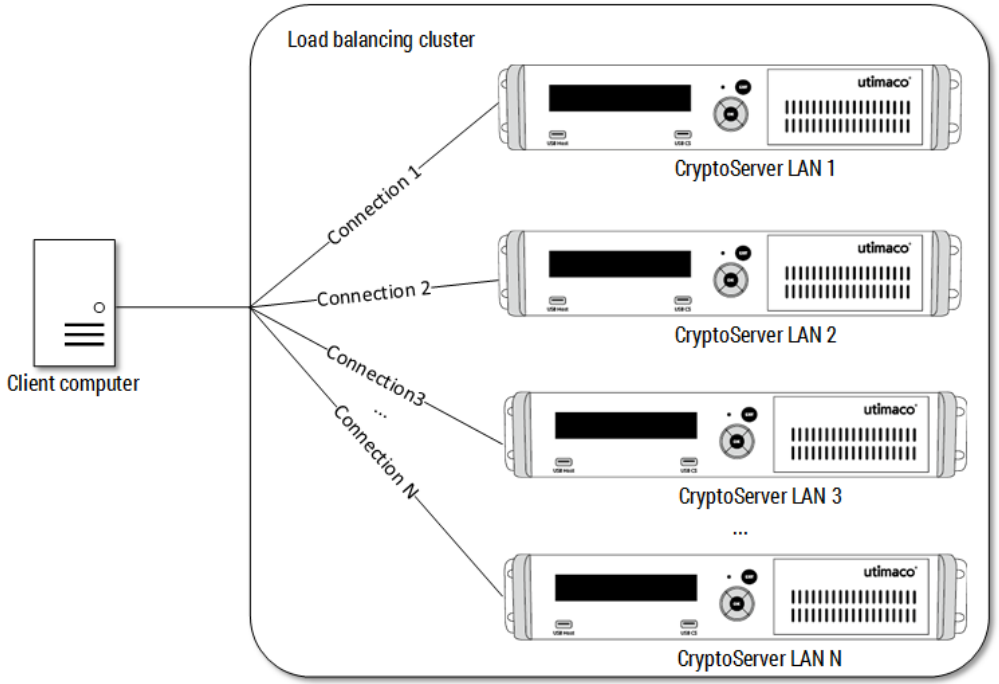
Clustering – Load Balancing

- If your are using load balancing
  - CryptoServer API handles session of Round Robin based connections
  - Reaching higher system performance
  - Even distribution of load on cluster members
  - High availability in case of a failure

Scalability of Utimaco HSMs

Clustering – Load Balancing

- CryptoServer in the cluster must be configured identically
- Connections are established by the client-side software based on the "Least Connections" principle
  - i.e. a new connection is opened on the CryptoServer with the least number of existing connections



Scalability of Utimaco HSMs

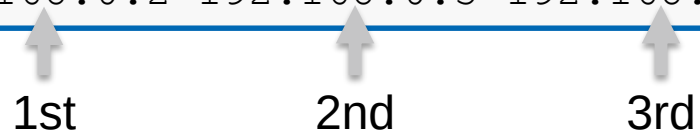
Clustering – Failover

- If your are using failover
  - Multiple CryptoServer can be configured in a cluster
  - The first CryptoServer is the primary CryptoServer device

→If the primary CryptoServer is not reachable, the next CryptoServer will be connected

→If the primary CryptoServer is active, the other cluster members stay passive

```
Device = { 192.168.0.2 192.168.0.3 192.168.0.4 }
```



→Failover mechanism tries to re-connect to the primary CryptoServer

→In regular time intervals (fallback interval) in seconds

```
# Configures load balancing mode ( == 0 ) or failover mode ( > 0 )
FallbackInterval = 60
```

Scalability of Utimaco HSMs

Data Storage

- All HSMs support internal and external key storage out of the box
  - The internal key store has a size of 4 MB for Se Gen1 & CSe Series
    →Corresponding RSA Keys (1024 bit) ~ 3350
  - The internal key store has a size of 8 MB for Se Gen2
    →Corresponding RSA Keys (1024 bit) ~ 6700

- Configure an external key storage
  - Unlimited storage size possible
  - Automatic key synchronization between cluster members
  - Master Backup Key (MBK) has to be installed on all cluster members
  - Path for external key storage has to be configured in the API configuration file

  →It can be stored anywhere (SAN, RAID,…)

→Switching from internal key storage to external key storage is possible at anytime

Scalability of Utimaco HSMs

Data Storage

- Using the HSM with different applications
  - The (internal/external) storage is logically partitioned
  - Applications can access only their dedicated key store
    - This implies that you can safely deploy multiple applications on a single HSM

Scalability of Utimaco HSMs

Data Storage

- Using the HSM with different applications
  - The (internal/external) storage is logically partitioned
  - Applications can access only their dedicated key store
    - This implies that you can safely deploy multiple applications on a single HSM

→Note: No licensing on algorithms and client connections

→All HSM series of Utimaco have the same functionalities & same firmware packages

Thanks for your attention!

Oliver Mueller

Product Trainer
oliver.mueller@utimaco.com

Utimaco IS GmbH

Germanusstraße 4
52080 Aachen
Germany
Tel +49 241 1696 200
Fax +49 241 1696 199
Email hsm@utimaco.com

Utimaco Inc.

Suite 150
910 E Hamilton Ave
Campbell, CA 95008
United States of America
Tel +1 844 884 6226
Email hsm@utimaco.com