Hardening BIND using DNSSEC with HSMs

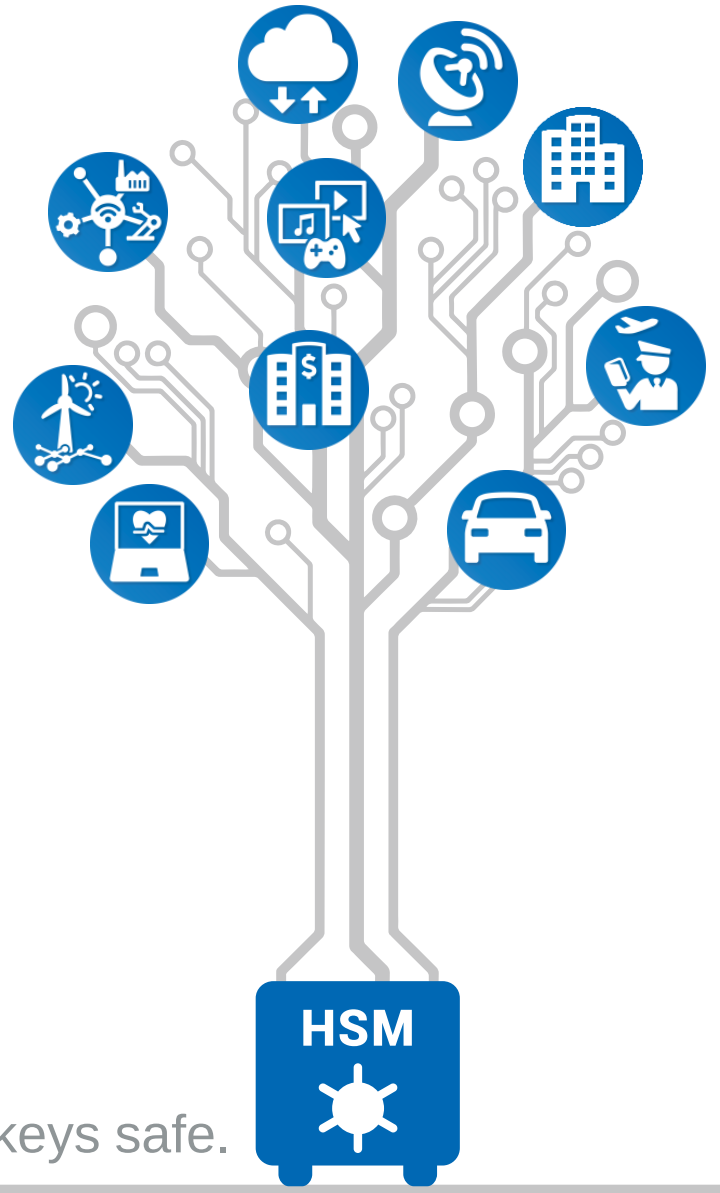
Viktor Wiebe

21st March 2019

utimaco®

Agenda

- What is an HSM
- BIND
- DNSSEC
- Live Demo
  - Initialize an PKCS#11 Slot
  - Generate Keypair in HSM
  - Generate Keypair referencing to a Key in the HSM
  - Sign a Zonefile



We keep your cryptographic keys safe.

What is an HSM?

What is an HSM?

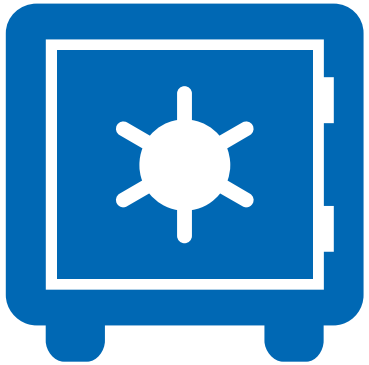
An HSM is a
Hardware Security Module.

What is an HSM?

A device to generate,
store and manage
cryptographic keys safely.

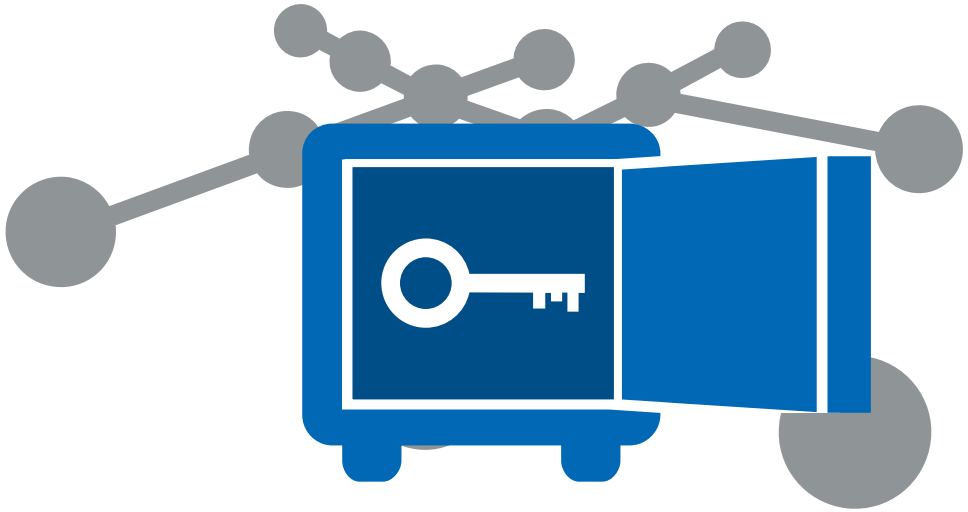
What is an HSM?

An HSM is like a safe
deep inside your network…



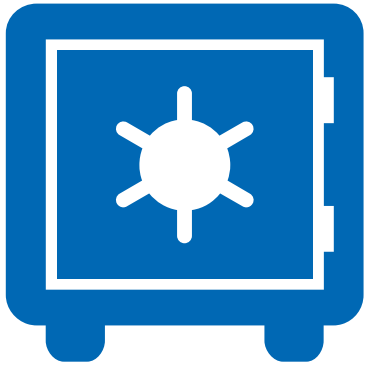
What is an HSM?

… that store the key
to unlock your data.



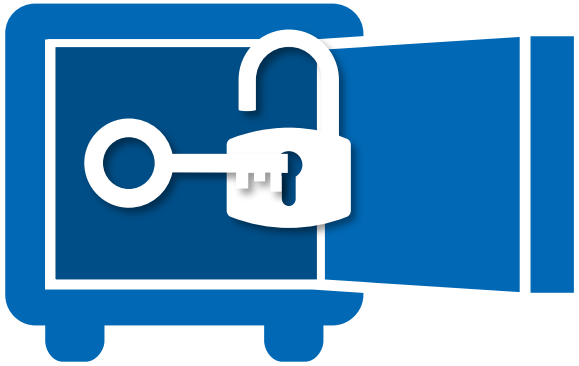
What is an HSM?

Your data is encrypted
when you don’t need it.



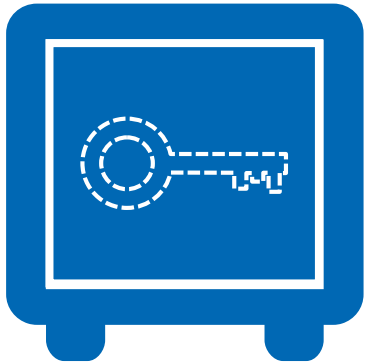
What is an HSM?

When you need access,
the key unlocks the encryption
and your data is usable.



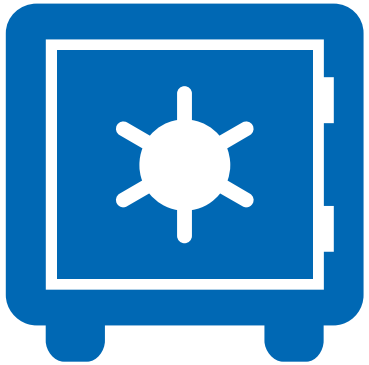
What is an HSM?

The key and sensitive data
never leave the safe
so the are always secure!



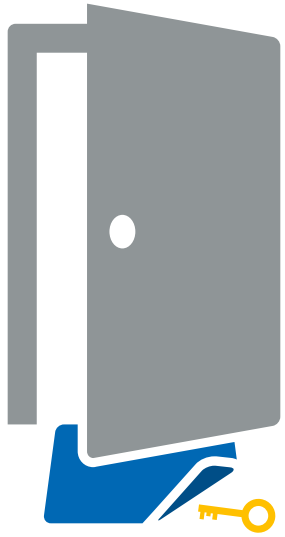
What is an HSM?

All done?
End your session
and your data gets locked up.



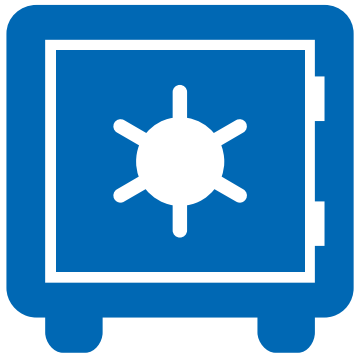
What is an HSM?

The weak link?
Your security is only as good
as your key's hiding place.



What is an HSM?

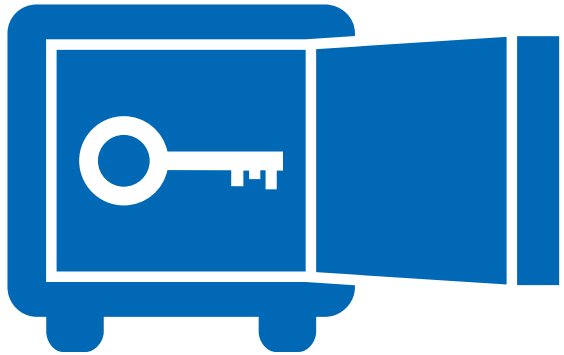
- Secure Memory device to store vital data objects - Cryptographic Private/Secret Keys
- Hardware designed to detect attack and respond by deleting keys
- Dedicated hardware provides highly specialized Cryptographic processing engine
- FIPS 140-2 Level 3/4, CC
- Hardware device (as opposed to software service) enforces Separation of Duties away from Admin/System/Ops/IT personnel to dedicated Security team



Why are they used?

- HSMs provide secure store, and highly specialized processing environment for keys
- HSMs can hold 1000s keys and secure many applications on many servers
- HSMs often hold “Master Keys” that secure unlimited number of externally held keys
- User Application keys never “in clear” in HSM memory – secured by hierarchy of keys
- Regulations over holding of data often now mandate security (e.g. PCI DSS, GDPR)
- HSMs provide:

  Increased Security
  Dedicated Cryptographic Engine
  Compliance with Security Regulations



How do they work?

- Provides security around keys – “innermost layer of an onion” (physical access, MofN, hierarchy of keys, attack detection)
- HSMs perform functions for applications:

  Key generation, encryption and decryption, signing, hashing……
- Application Server sends instruction to HSM to process data using specific key that never leaves HSM (apart from backup/clustering)
- Application integrated with HSM via client API running on server – crypto function calls/instructions forwarded by client to HSM for execution
- 3 main Crypto APIs – libraries of functions for programming language used by application:

  PKCS#11 (C), Microsoft (CSP/CNG), Java/JCE

Who buys them?

- Governments – National, Local, Regional orgs (EU, NATO)
- Banks and Financial Institutions (Stock Exchanges, Payments Processors)
- Utilities (Electricity, Telco's, ISPs)
- Transportation (Airlines)
- Healthcare (Hospitals)
- Education (Universities)
- Retail (Physical Stores and Online)
- Manufacturing (Automotive, Pharmaceutical, Oil/Mining)
- Official Agencies (Police)
- CAs (PKI – Trusted Root and Corporate)
- Internet/technology-related industries
- Gaming Industry
- And others …

What applications are they used for?

- PKI
- Webservers - SSL
- DNSSec
- Time Stamping
- Document Signing
- Database encryption
- Code Signing

- ePassports
- ID Cards
- Manufacturing
- Smart Meters
- SIM Cards
- Bitcoin mining
- And many more…

BIND.

BIND

- BIND is by far the most popular and widely used DNS software on the Internet. It provides a robust and stable platform on top of which organizations can build distributed computing systems with the knowledge that those systems are fully compliant with published DNS standards.
- BIND supports the full DNSSEC standard.
- BIND 9.14rc3

DNSSEC.

What is DNSSEC

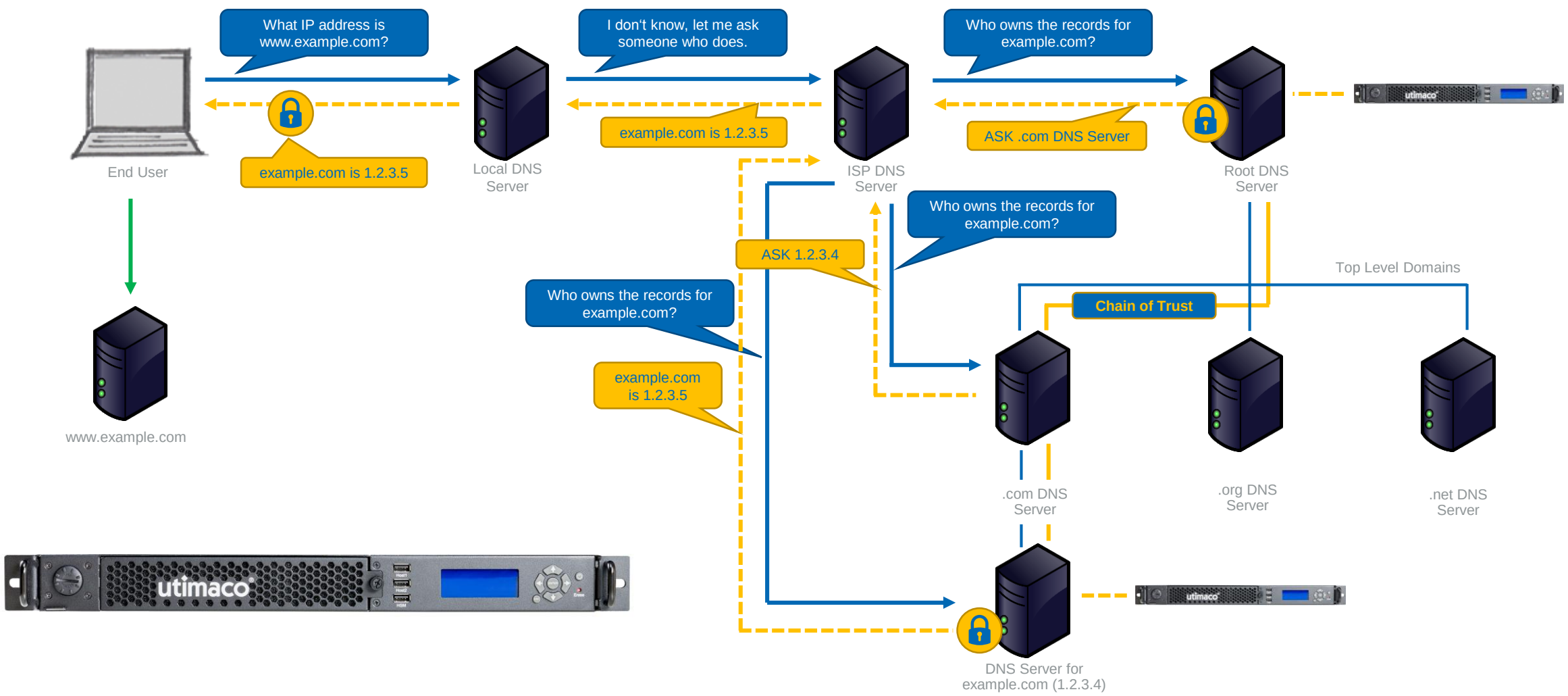
- DNSSEC is a suite of Internet Engineering Task Force (IETF)
- A set of extensions to DNS which provide to DNS clients (resolvers)
  - origin authentication of DNS data
  - authenticated denial of existence
  - data integrity
- but not availability or confidentiality.

DNSSEC and HSM

What role does a HSM play in DNSSEC

- It is imperative that private DNSSEC signing keys are kept secure.
- The public key can be made widely available
- If the private key is compromised, a rogue DNS server can masquerade as the real authoritative server for a signed zone.

- HSMs secure the DNS server
  - Generation of keys
  - Storing of the private key
- signing of zones is performed on a DNS server that is physically secure and whose access is restricted to essential personnel only.


What IP address is www.example.com?
I don't know, let me ask someone who does.
Who owns the records for example.com?
example.com is 1.2.3.5
ASK .com DNS Server
example.com is 1.2.3.5
End User
Local DNS Server
ISP DNS Server
Root DNS Server
Who owns the records for example.com?
ASK 1.2.3.4
Top Level Domains
Chain of Trust
Who owns the records for example.com?
example.com is 1.2.3.5
www.example.com
.com DNS Server
.org DNS Server
.net DNS Server
DNS Server for example.com (1.2.3.4)

Why using DNSSec in combination with HSMs

Benefits

- Ensure integrity of the DNSSEC validation process with independently certified HSMs (FIPS 140-2 Level 3 and Common Criteria EAL4+).
- Maintain a robust tamper-resistant hardware boundary and a proven, auditable mechanism to protect valuable signing keys.
- Enforce separation of duties through robust access controls to mitigate the threat of single “super users” and facilitate regulatory compliance.
- Achieve high availability and improved DNS server performance with secure key storage, backup and recovery, and powerful cryptographic acceleration.

Demo.

- Install requiered packages
  - gcc, python, libssl-dev, libcap-dev, make
- copy utimaco PKCS#11 Library and config file
- Configure, compile and install Bind 9.14rc2
  - ./configure --enable-native-pkcs11 --with-pkcs11=/usr/local/utimaco/libcs_pkcs11_R2.so --with-python=no

- Initialize PKCS#11 Slot
- Generate Keypair in HSM
- Generate KeyPair referencing to key in HSM
- Sign Zonefile

Initialize PKCS#11 Slot

utimaco®

>_Console

```
# ./p11tool2 Slot=0 Login=ADMIN,/path2file/ADMIN.key InitToken=1234

# ./p11tool2 Slot=0 LoginSO=1234 InitPin=5678
```

Generate Keypair in HSM

utimaco®

>_Console

```
# pkcs11-keygen -a RSASHA256 -b 2048 -l midgard-ksk

# pkcs11-keygen -a RSASHA256 -b 1024 -l midgard-zsk
```

Create PIN File for PKCS#11 Slot

>_Console

```
# echo -n "1234" > /usr/local/utimaco/slot0
```

Generate KeyPair referencing to key in HSM

utimaco®

>_Console

```
# dnssec-keyfromlabel -a RSASHA256 -l 'pkcs11:pin-
source=/usr/local/utimaco/slot0;object=midgard-ksk' -f KSK midgard.com

# dnssec-keyfromlabel -a RSASHA256 -l 'pkcs11:pin-
source=/usr/local/utimaco/slot0;object=midgard-zsk' midgard.com
```

Edit Zonefile

and add created public key at the end

>_Console

```
...
$include Kmidgard.com.+008+59459.key
$include Kmidgard.com.+008+20280.key
...
```

Sign Zonefile

utimaco®

>_Console

```
# dnssec-signzone -S -o midgard.com midgard.zone
```

Curious what you can do with our HSM?

Wanne try to integrate into your application?

Ready to take off?

Download our HSM simulator!

Register for free

Thank you for your attention

Viktor Wiebe

Sales Engineer HSM

Utimaco IS GmbH

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

Utimaco Inc.

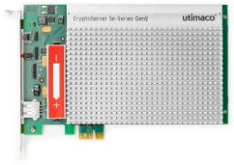
Suite 150
910 E Hamilton Ave
Campbell, CA 95008
United States of America
Tel +1 844 884 6226
Email hsm@utimaco.com

Utimaco Technical Overview.

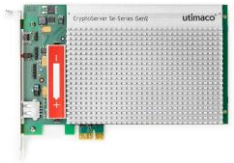
CryptoServer LAN v5

1U form factor
40% less power consumption
40% less heat dissipation
Hot-Plug fan & power supply replacement

CryptoServer Hardware Platforms

	CryptoServer Se-Series Gen2		CryptoServer CSe-Series	
				
Physical Interface	PCIe plug-in	Network attached	PCIe plug-in	Network attached
Cryptographic Support	3DES, AES, RSA, DSA, DH, ECDSA, ECDH, ECIES, SHA-1, SHA-2 family, …			
RSA 2048 signature generation per second	Between 16 and 3400		Between 17 and 90	
Certifications	FIPS 140-2 Level 3 / CC EAL 4+		FIPS 140-2 Level 3 w/ Physical Security Level 4, “DK” Approval, PCI-HSM	

CryptoServer Product Packages

	CryptoServer Se-Series Gen2	CryptoServer CSe-Series
	 	 
SecurityServer	PKCS#11, JCE, MS CSP/CNG/SQL EKM, CXI	
CryptoServer SDK	Development Kit for CryptoServer Firmware Development	
CryptoScript SDK	Development Kit for Scripting HSM Extensions	
TimestampServer	RFC 3161, CTS API	RFC 3161, CTS API
PaymentServer	EFTPOS	
eIDAS	QSCD compliant firmware	