trustis®

HARDWARE SECURITY MODULES (HSMs)

Cryptography: The basics

- Protection of data by using keys – based on complex, randomly-generated, unique numbers
- Data is processed by using standard algorithms (mathematical formulae) – key length measure is bits (more bits = more variants)
- Symmetric encryption: one key to encrypt and decrypt data. E.g. AES256
- Asymmetric encryption: Public and Private key pair to sign and verify identity as well as to exchange keys securely. e.g. RSA 2048
- Hashing – checks authenticity/integrity – e.g. SHA2
- Longer keys and regular rekeying adopted to combat increasing strength of hackers
- Move to ECC (asymmetric) - enables shorter keys and less processing power for equivalent levels of security

Data security depends on keys.

These must be kept secure, hence the need for HSMs

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 high-performance cryptographic processing engine
- Built to comply with internationally-recognised security standards – e.g. FIPS 140-2 Levels 3 or 4
- Hardware device (as opposed to software service) enforces separation of duties away from Admin/Systems team to dedicated security team

Why are they used?

- HSMs provide a secure storage and processing environment for keys that protect data or signing transactions.
- They can hold 1000s of keys and secure many applications on many servers
- HSMs can also hold the Master Key that secures an unlimited number of external keys
- User application keys never “in clear” in HSM storage – secured by hierarchy of keys
- Growth in cloud services and increasing data breaches require more stringent security measures
- HSMs provide increased security, trusted crypto processing and compliance with security regulations

How do they work?

- Provides security around keys – “layers of an onion” (physical access, MofN, hierarchy of keys, electrical/physical tamper sensing)
- HSMs perform functions for applications - key generation, encryption and decryption, signing and verifying, hashing
- Application server sends instruction to HSM to process data using specific key that never leaves HSM
- Applications are integrated with HSMs via client 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 (CAPI/CNG), Java (JCE/JCA)

Who buys them?

- Governments – National, Local, Regional orgs
- Banks, Financial Institutions and Payments Processors
- Utilities
- Telcos and Hosting providers
- Transportation
- Healthcare
- Education
- Retail
- Manufacturing
- Official Agencies
- PKI Providers
- Etc.

Types of HSMs - Applications

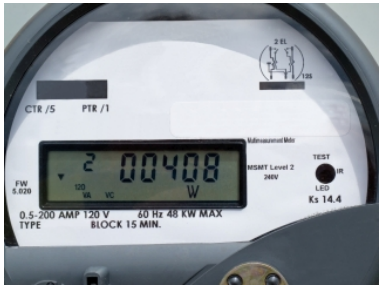
General purpose (PKI etc.) – optimised for asymmetric

Payments (Banking and retail - issuing/processing of credit and debit cards); industry-specific function sets – optimised for symmetric

[Note: A bank may buy a general-purpose HSM for PKI, and a payments HSM for ATM transactions]

Customisable (user can load their own functions, algorithms)

Applications that use HSMs

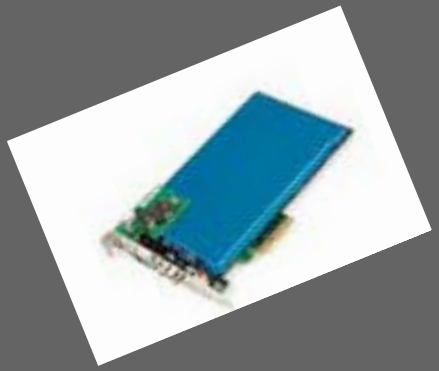


- PKI
- Webservers - SSL
- DNSSec
- Time stamping
- Document signing
- Database encryption
- Code signing
- ePassports
- ID Cards
- Manufacturing
- SIM cards
- Smart metering & IoT

trustis

Types of HSMs - Physical

PCI card



Network-attached, shared HSM

Stand-alone, dedicated HSMs for one application
(e.g. Root CA – can be taken offline)

Smart cards (origin of PKCS#11 standard)

USB tokens (smart card on USB form factor)

Features required in HSMs

- Certification
- Ease of use
- High availability/load balancing
- Monitoring
- Auditing (for regulations)
- Secure backup
- Secure link to app server client
- Full suite of algorithms and key lengths (inc ECC)
- Documented integrations
- Partitioning – separate virtual HSMs in one device for different users
- Ability to control key lifecycle according to corporate policy (creation / use / deletion)

Policies & procedures

More important than the HSM itself is how it is managed and controlled:

- Secure location
- Multiple people required to authenticate (M of N)
- Separation of duties
- Protection of smart cards/PINs/backup media
- Documentation and labelling
- Agreed roles and duties – Security Officer, Compliance Officer, Auditor

Security consultants often advise on best practices and develop policy documents.
All relevant parties to agree, understand and sign off on their duties.

Managed HSMs

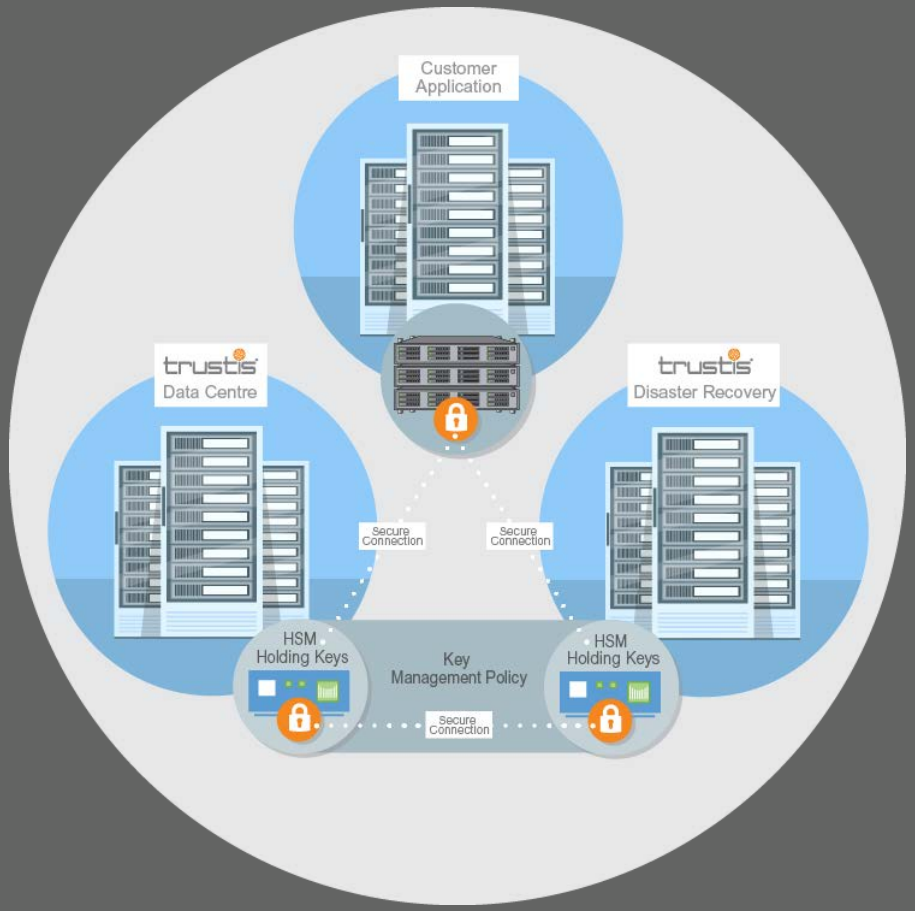
Cloud SaaS/IaaS/PaaS use is now commonplace

Challenge: should I trust my cloud provider to host my HSMs and manage my cryptographic keys?

Are they cryptography specialists? Can they properly separate and control key splits? Are multi-person controls or my specific Key Management Policies complied with? How and where will they host the HSMs? Can I be sure I still have control? Do they have access to my keys?

If they cannot offer you HSM services or their HSM services will not meet your requirements of security or management, then Trustis, through our “Cryptography-as-a-Service”, provides HSM hosting, HSMs on Demand and Key Management services

Cloud HSM architecture



About Trustis

- For over 15 years, Trustis has specialised in cryptographic solutions that include large-scale PKIs, managed HSMs, Identity Federation, as well as security policy and compliance.
- We serve both the public and private sectors in the UK and around the world and have been a G-Cloud supplier since its inception.
- Trustis' services comply with ISO 27001:2013 as well as tScheme and are ETSI Certified.
- A product-independent approach ensures that customers get the best solution to meet their requirements.
- Recent projects include public sector networks, 4G security in telecoms, smart grid and metering rollouts, payment systems in banking and ePassport PKIs.

Contact details

Trustis Commercial Contact:
Robert Hann
robert.hann@trustis.com
+44 (0) 7818 552411

Trustis Limited
Building 273, Greenham Business Park, Thatcham, RG19 6HN

+44 (0) 1635 231361
info@trustis.com
www.trustis.com