Hardware Security Modules

What they are and why it's likely that you've (indirectly) used one today
What Am I Going to Talk About?

What Is A HSM?  Where Will I Find One?
A Hardware Security Module is...

...a dedicated crypto processor...

...designed for the protection of keys throughout their lifecycle...

...validated as secure by third parties...

...a Trust Anchor...
A Hardware Security Module is…

…a source of high quality random numbers…

…a vault for holding cryptographic keys…

…Cryptographic Acceleration Hardware…

…a hardware solution that implements the cryptographic algorithms you want to use…
How is a HSM deployed?

Application Servers

Multiple Partitions

Availability and Load Balancing

Role Separation

Application

Crypto Services

Offload

PKCS #11
Java CSP
CAPI / CNG
XML-DIGSIG

Key Vault Services

Tamper Resistance/Response
Separation of Duties
MFA with M of N Controls

FIPS 140-2 Level 3
Common Criteria EAL4+

Certifications

Key Management Services

Backup/Restore
Access Controls
Export Controls
EKM Interface
Policy Def’n and Enforcement

Security Officer
Application Owner
Auditor
IT Admin

SafeNet
Certifications

- Provide independent verification of the security of a HSM

FIPS

Common Criteria

PCI Security Standards Council
Physical Security Features
Features of a Validated HSM Appliance

- Intrusion detection
- Tamper Resistant Fasteners
- Protected Electronics
- Internal Baffles to Prevent Probing
- Tamper Resistant I/O Mounts
- Tamper Resistant Fan Mounts
- Serialised Tamper Evident Labelling
HSM Form Factors
So What Do HSMs Get Used For?
1. Secure Documents
HSMs secure passport issuance
HSMs secure documents for governments, hospitals, and the court system
Secure Manufacturing
HSMs secure entertainment devices, including videogame consoles and Personal Video Recorders.
HSMs secure Smart Metering Systems and the delivery of Meter messages in our homes to Head End Utility systems.
Banking and Payments
HSMs secure mobile money payments and verbal banking transactions made by telephone
HSMs secure card data and the delivery of Personal Identification Numbers (PINs)
HSMs secure the production of credit and debit cards and mobile phone SIM cards.
And Yet More Payments Use Cases...
HSMs secure SSL for the websites we use every day
Transport and Infrastructure
HSMs secure Device Manufacturing in the delivery of Trusted Device Identities we used Every Day
Railway signalling infrastructure is secured by Hardware Security Modules
HSMs are used to protect the communication protocols for large industrial equipment.
HSMs secure the software and physical components of safety critical systems
HSMs secure automated toll booth passes
HSMs secure the delivery of streaming media
Thank You!