Hardware Security Modules (HSMs) Benefits and Challenges

Mark Southam
Keyper HSM Product Manager
Security Layers

INTERNET

Perimeter Defense
Front End App Server (DMZ)
Internal Defense
Back End App Server
Users & Groups
Permissions (ACLs)
Data
HSM
Keys
Physical Separation
Hardware Random Number Generator
Level 4 Physical Security
Quorum of up to 9 People for Access to Cryptographic Services and Key Management
PIN Access for Applications

© 2014 Ultra Electronics: Proprietary Data
Certification

• Good Cryptography states that a cipher should only be used if it has been thoroughly Crypto Analysed

• Keyper HSM has 15 Years of FIPS140 Level 4 attacking and certification

• The only HSM to have undergone both this and Common Criteria testing and certification to EAL4+AVA_VAN.5 (Advanced Vulnerability Analysis)

• Has any form of cryptography performed using software undergone such analysis?
The heart would never have bled