Title
Month Year

Panel Discussion on Enterprise Key Management

June 9, 2009

Chii-Ren Tsai (Citigroup)
Matt Ball (Sun Microsystems)
Matthew Fanto (Aegis Data Security)
Robert Griffin (RSA/EMC)
Steven Wierenga (HP)

Agenda

- Perspectives on enterprise key management
- Questions from the chair
- Q & A

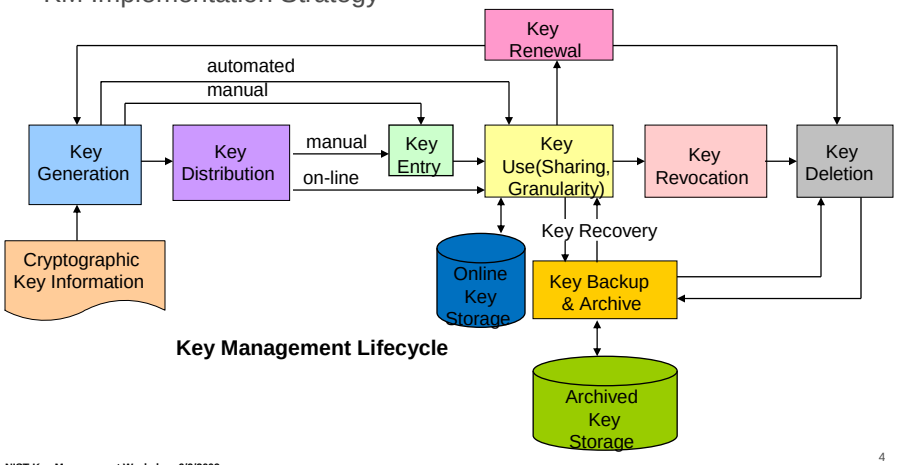
Title
Month Year

Perspectives on Enterprise Key Management

Chii-Ren Tsai
Citigroup O&T Risk Management
chiiren.tsai@citi.com

Citi Key Management Initiative

- KM Guidelines for all aspects of key management lifecycle
- KM Checklist with a risk-based assessment method
- KM Reference Processes
- KM Implementation Strategy



Key Management Lifecycle

Title
Month Year

Key Management Issues & Future Directions

- Common technical KM Issues
  - Weak pseudo-random generators for key generation
  - Cryptographic keys hard-coded in the application
  - Approved CAs, cryptographic algorithms and key lengths not used
  - Cryptographic keys not renewed periodically
  - Cryptographic keys or passwords not encrypted/protected in storage or in transit
- Future directions
  - Central KM solutions for managing keys in HSMs or software
  - Crypto implementation framework to simplify KM
    - Segregate key management from key use
    - Key attributes & KM policy, especially for symmetric keys
    - KM policy mapping for interoperability

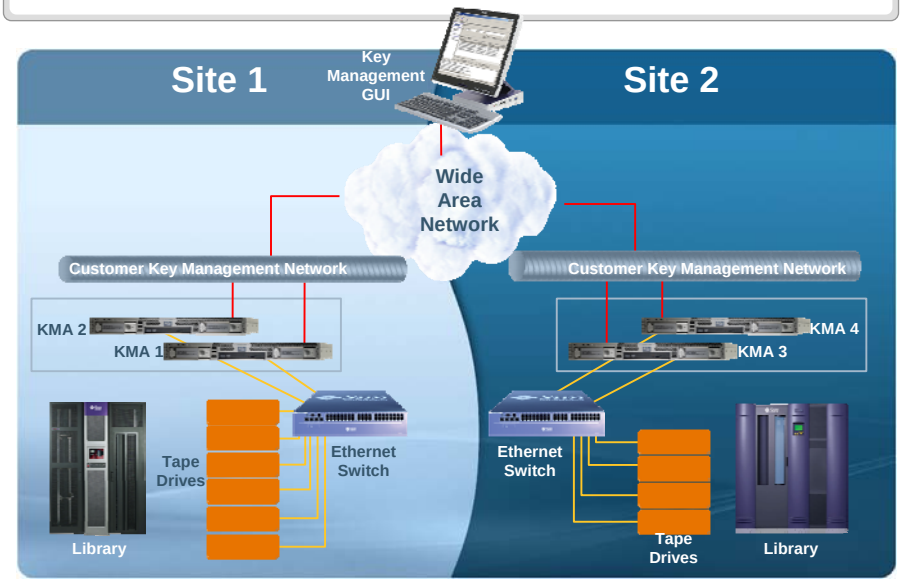
Perspectives on Enterprise Key Management

Matt Ball
Sun Microsystems
matthew.ball@sun.com

What is in Enterprise Key Management?

- Secure creation of cryptographic keys
- Automatic replication of keys
- Policy management for the keys
- Secure Audit Logging
- Role-based management / Quorum requirements
- Scalability across the entire enterprise
  - High availability
  - Large number of keys and appliances
- Interoperability, Standards Compliance:
  - IEEE P1619.3
  - OASIS Key Management Interoperability Protocol (KMIP)
- Key export to trusted partners

Example Enterprise Key Management Configuration for Tape Encryption



Title
Month Year

Perspectives on Enterprise Key Management

Matthew Fanto
Aegis Data Security
mfanto@gmail.com

Overview of Key Management

- Key Management within the auto industry
  - Issues within the organization – Multiple divisions worldwide, each with different legislative and technical needs.
  - In-Vehicle access to crypto keys – Embedded platforms with limited connectivity need to obtain crypto keys and verify signatures.
- Key management vs. credentialing
  - Our approach – support any credential provider. This allows flexibility in the organization to deploy immediately, adopt new standards, without having to overhaul any existing infrastructure.

Issues with Enterprise Key Management

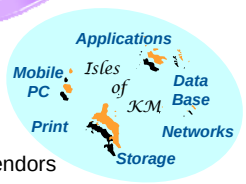
- Single point of failure
  - Systems without support for redundancy, distributed key management, or solid backups are at risk of catastrophic loss
- Immediate need vs. cost
  - Many organizations already locked into their credentialing system. EKM that leverages existing policies and authentication methods more flexible, with less cost, and quicker deployment
- "Offline" availability of keys

Perspectives on Enterprise Key Management

Steve Wierenga
HP
Steve.wierenga@hp.com

HP and Key Management

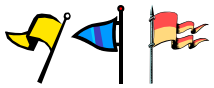
- HP – Global IT Products/Services Provider
  - #1 in desktops, notebooks, servers, disk storage, printers, infrastructure services…
  - 30+ years managing keys securely for the worldwide debit/payments network
- Recent Market Drivers for Encryption, Key Management
  - Breach Notice legislation, PCI-DSS mandates
  - Large-scale hacks/attacks/breaches, fines, remediation
- Interoperable Enterprise Key Management (EKM)
  - Customer need and market requirement
  - Proprietary/partial/point solutions are inadequate
  - Lack of KM interoperability is a barrier to encryption adoption
  - Fragmented KM increases cost, risk, complexity for users, vendors



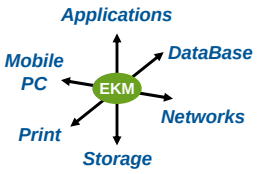
- HP Key Management Vision
  - Pervasive, Integrated, Transparent, Enterprise Data Protection
  - Desktop to Datacenter, Mobile to Print, Devices to Applications
  - Heterogeneous, multi-vendor, multi-partner environments
  - Reduce IT Costs, Risk, and Complexity
    - Protect IT Resources, Protect Data, Provide Compliance Validation

HP EKM standards and interoperability

- HP supports and contributes to KM standards efforts
  - OASIS KMIP founder, sponsor, contributor
  - IEEE P1619.3, ANSI X9F, TCG storage TCs…



- Enabling HP and partner product interoperability
  - HP Enterprise Key Management Client SDK
    - No-cost SDK license agreement
    - Developer support, HP EKM server access
  - HP Secure Advantage Alliance
    - Pan-HP, strategic security partners
    - EKM interoperability is a partner requirement
  - Sponsoring broader EKM standardization
    - KMIP founder, co-author, contributor
    - KMIP client/server PoC implementation, interop testing
    - OASIS KMIP submittal and member recruitment
  - NIST Key Management Workshop and other venues



Questions?

- For those viewing via webcast, please submit questions to:

kmwquestions@nist.gov