Enterprise Key Management Infrastructure (EKMI)

Arshad Noor
StrongAuth, Inc.
Chair, EKMI TC
arshad.noor@strongauth.com
Business Challenges

- **Regulatory Compliance**
  - PCI-DSS, HIPAA, SB-1386, FISMA, PCSA (MN), EU Directive, PIPEDA, etc.

- **Avoiding fines** - ChoicePoint $15M, Nationwide Building Society $2M

- **Avoiding lawsuits** – BofA, TJX

- **Avoiding negative publicity**
  - VA, IRS, TJX, E&Y, BofA, Wells Fargo, UC, IBM, Nieman-Marcus, Citibank, etc.
Technical Challenges

- Enabling business while
  - Protecting the end-point
  - Protecting the data
  - Keeping barriers (for attackers) high
  - Keeping it simple for employees, partners & software developers
  - Keeping costs lows
Asymmetric Key Management

- Public Key Infrastructure (PKI)
  - SSL/TLS
  - IPSec
  - S/MIME
  - Digital Signatures
  - Identity Cards
  - E-Passports
Asymmetric Key Management

PKI

OCSP  RA  LDAP

CA  TSA
Symmetric Key Management

- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy

- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy

- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy

- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy

- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy

- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy

- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy

- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy

- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy

- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy

........and on and on
The EKMI Problem

Application A
Application B
Application C
Application D
Application E

Database A
Database B
Database C
Database D

LAN

PKI
OCSP
RA
LDAP
CA
TSA
Without EKMI

- **Higher TCO**
  - Multiple Key-Management solutions
  - Lack of coherency & standards (in symmetric key management)
  - More training & administration
  - More Audits

- Increased potential for a security breach
The EKMI Solution
The Encryption Solution

- Generate
- Protect
- Escrow
- Authorize
- Recover
- Destroy

- Encrypt
- Decrypt

WAN

SKS Server

- Encrypt
- Decrypt

SKS Server

- Encrypt
- Decrypt

SKS Server

- Encrypt
- Decrypt

SKS Server

- Encrypt
- Decrypt

SKS Server

- Encrypt
- Decrypt

SKS Server

- Encrypt
- Decrypt
What is an EKMI?

- An **Enterprise Key Management Infrastructure** is:

  “A collection of technologies, policies and procedures for managing *all* cryptographic keys in the enterprise.”
EKMI Characteristics

- A single place to define policy
- A single place to manage all keys
- Standard protocols for KM services
- Platform & application independent
- Scalable (for millions of clients)
- Available even when network fails
- Extremely secure
EKMI Components

- **Public Key Infrastructure (PKI)**
  - For digital certificate management; for strong-authentication, secure storage & transport of symmetric encryption keys

- **Symmetric Key Management System**
  - **SKS Server** for key management
  - **SKCL** for client interaction with SKS Server

- **EKMI = PKI + SKMS**
1. Client Application makes a request for a symmetric key
2. SKCL makes a digitally signed request to the SKS
3. SKS verifies SKCL request, generates, encrypts, digitally signs & escrows key in DB
4. Crypto HSM provides security for RSA Signing & Encryption keys of SKS
5. SKS responds to SKCL with signed and encrypted symmetric key
6. SKCL verifies response, decrypts key and hands it to the Client Application
7. Native (non-Java) applications make requests through Java Native Interface
The Sharing Problem - (DHS-PCII)

Private Sector PCI Data

Key shared out-of-band

DHS Personnel

Encryption Key

PCI Ciphertext

Internet

First Responder

Encryption Key shared out-of-band
The Sharing Problem - Multiplied

Private Sector PCI Data
(Tens of thousands?)

Encryption Keys

DHS Personnel
(180,000+)

First Responders
(50 States,
3000+ Counties,
20,000+ Cities)
The Sharing Problem - Solved

Private Sector PCI Data
(Tens of thousands?)

First Responders
(50 States,
3000+ Counties,
20,000+ Cities)

DHS Personnel
(180,000+)

Internet

SKS Server

PCII Database
EKMI TC Goals

- Standardize **Symmetric Key Services Markup Language (SKSML)**
- Create Implementation & Operations Guidelines
- Create Audit Guidelines (with ISACA)
- Create Interoperability Test-Suite
EKMI TC Members/Observers

- FundServ, PA Consulting, PrimeKey, Red Hat, StrongAuth, US DoD, Visa, Wave Systems
- Many large companies as Observers
  - Security, Database, Consulting, Non-US Government Agency
- Individuals representing Audit and Security backgrounds
The Burton Group on EKMI

- "The life cycle of encryption keys is incredibly important. As enterprises deploy ever-increasing numbers of encryption solutions, they often find themselves managing silos with inconsistent policies, availability, and strength of protection. Enterprises need to maintain keys in a consistent way across various applications and business units," said Trent Henry, senior analyst, Burton Group. "EKMI will be an important step in addressing this problem in an open, cross-vendor manner."
Potential Encryption Layers

- **Data-in-Use**
- **Data-in-Motion**
- **Data-at-Rest**

### Potential Layers:
- Inside Application
- Network (Typically, already encrypted with SSL or IPSec)
- Database Driver
- Inside Database
- File-system Driver in OS
- Device Driver in OS
- Disk/Tape Firmware
Exposure Spread

- Application
- Network
- Database or DB Driver
- Operating System and its Drivers
- Disk

The further away from the Application layer you encrypt data (in the stack), the greater the probability of you having to encrypt it again!

Vulnerability due to exposure of unencrypted data
Conclusion

- “Securing the core” should have been Plan A from the start – yet, it's not too late for most companies.
- OASIS EKMI TC is already making significant strides in advancing this concept.
- Get involved!
EKMI Around the World

- ISACA International
  - Singapore, July 22-25, 2007
  - www.isaca.org

- ISSA
  - Chennai (Madras) India, August 3, 2007
  - mp.badrinath@in.ey.com

- ISSE/SECURE 2007
  - Warsaw, Poland, September 25-27, 2007
  - www.isse.eu.com
EKMI Resources

- www.oasis-open.org
  - Policy template, Use Cases, SKSML Schema, Presentations, White Papers, Implementation Guidelines, etc.

- www.strongkey.org - Open Source SKMS implementation

- www.issa.org - Article on SKMS in February 2007 issue of ISSA Journal