Enterprise Key Management Infrastructure (EKMI)

Securing data for e-Business and e-Government

Arshad Noor, Co-Chair, EKMI-TC
arshad.noor@strongauth.com

OASIS Symposium 2007, San Diego
Business Challenge

- **Regulatory Compliance**
  - PCI-DSS, HIPAA, FISMA, SB-1386, etc.
  - Impending Massachusetts H213 bill

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

- **Avoiding lawsuits – BofA, TJX (multiple)**

- **Avoiding negative publicity**
  - VA, IRS, TJX, E&Y, Citibank, BofA, WF, Ralph Lauren, UC, and 300+ others
e-Business/e-Government Challenges

- Sharing data while keeping it secure
  - Protected Critical Information Infrastructure (PCII) at the DHS
  - Medical, Taxpayer and Employee data
  - Credit Card Numbers
  - Other sensitive data

- Protecting data across the enterprise
  - Laptops, Desktops, Databases, PDAs, Servers, Storage devices, Partners, etc.
The Encryption Problem

- 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
Key Management Silos

Network

Key Management Connections

Application

Database or DB Driver

OS or its Drivers

PKI
What is an EKMI?

- An Enterprise Key Management Infrastructure is:

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

- A single place to define EKM policy
- A single place to manage all keys
- Standard protocols for EKM services
- Platform and Application-independent
- Scalable to service millions of clients
- Available even when network fails
- Extremely secure
EKMI Harmony

Network

Key Management Connections

Database or DB Driver

Database or DB Driver

Database or DB Driver

OS or its Drivers

OS or its Drivers

OS or its Drivers

Application

Application

Application

Application

Application

Application

EKMI

PKI

SKMS
The Encryption Solution

- SKS Server
  - Generate
  - Protect
  - Escrow
  - Authorize
  - Recover
  - Destroy

- PKI Server
  - Issue & Manage Credentials

- WAN
  - Encrypt
  - Decrypt

Encrypt
Decrypt
EKMI Components

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

- **Symmetric Key Management System**
  
  - SKS Server for symmetric key management
  - SKCL for client interactions 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 + Encryption Key = Internet

Key shared out-of-band

DHS Personnel

First Responder

PCI Ciphertext

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
The Healthcare Solution

- ER Application and Database
- Patient Registration
- ER Nurse
- SKS Server
- Wireless MAN
- EMT 1 Laptop
- EMT N Laptop
- AP
- Ambulance
The Financial Solution

Branch 1

WAN

Branch N

SKS Server

Central Database
## Solutions to Barriers

<table>
<thead>
<tr>
<th>Barrier</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slow</td>
<td>Multi-core CPUs</td>
</tr>
<tr>
<td>Complex</td>
<td>Higher-level APIs</td>
</tr>
<tr>
<td></td>
<td>Design standards</td>
</tr>
<tr>
<td></td>
<td>Education</td>
</tr>
<tr>
<td>Expensive</td>
<td>Open-source</td>
</tr>
<tr>
<td>Lack of standards</td>
<td>OASIS EKMI-TC</td>
</tr>
</tbody>
</table>
EKMI-TC Goals

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

- Booz Allen Hamilton, EMC (RSA), Entrust, Mitre Corporation, Oracle, Red Hat, Sigaba, Symantec
- Individuals representing Audit and Security backgrounds
Conclusion

- “Securing the Core” should have been Plan A from the beginning
  - But it’s not too late
- OASIS EKMI-TC is driving new key-management standards that cuts across platforms, applications and industries.
- Get involved!
Resources

- **OASIS EKMI-TC Resources**
  - Use Cases, SKSML Schema, Presentations, White Papers, Guidelines, etc.

- **www.strongkey.org** - Open Source SKMS implementation

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