Ensuring Confidentiality (and trust)

Encryption, Data Retrieval, and Key Management Technologies

Jerry Smith, US Department of Defense

Anthony Rutkowski, Yaana Technologies

Bob Griffin, RSA, the Security Division of EMC
Ensuring confidentiality and trust ...

... is not easy

- Information growth
- Mobility, virtualization & cloud

- Evolving threat landscape
- Collaboration / Exchange
Ensuring Confidentiality (and trust):

the Extended Validation Certificate Platform

Tony Rutkowski
SVP for Regulatory Affairs and Standards, Yaana Technologies
ITU-T Rapporteur for Cybersecurity
Editor, Rec. ITU-T X.evcert
Liaison, CA/Browser Forum
EVcerts: critical for IdM and cybersecurity

- Trust in network sites and providers is critical to achieving effective Identity Management and cybersecurity
  - adverse effects include harm to users, other providers, and the infrastructure; loss of assurance
- The Extended Validation Certificate platform bundles together a proven set of technologies and practices to
  - significantly enhance trust assurance in the site/provider
  - create an encrypted path with the site
  - sign software
Some of what the EVcert platform provides

- Visible EVcert trust indication in user browser
- Extensive initial and continuing identity proofing of service provider; signing software
- Real-time Online Certificate Status Protocol (OCSP) checking
- Extensive process and auditing requirements for issuing EVcert authorities
- SSL (Secure Sockets Layer) encryption for end-to-end confidentiality
Additional value proposition

- CA/Browser Forum: developed and initially implemented by the most prominent software and digital certificate vendors worldwide over the past several years
- The platform has been included as a core capability in security standards by ETSI, Liberty Alliance, and ISO
- The platform is completely “open” and promotes a competitive environment
- ITU-T is importing and promulgating the platform for adoption in early 2011 as the X.evcert Framework to enhance global ubiquity and further its development
- Version 1.3 includes features to enhance use for cloud computing
How browsers display EVcert information

**Google Chrome**

**Microsoft Explorer 8.0**

**Mozilla Firefox 3.1 pre**

**Opera 10.51**

**Apple Safari 4.0.5**
Comprehensive specification and continuing examination/evolution

Enrollment
- Enrollment Registrant Requirements
  - Required Information
- Initial Verification Methods
- Enrollment Legal Requirements
- Continuing Verification & Renewal

Credentials
- Trust Model
- Issuer Approval
- Validity Period
- Credential Strength & Weakness

Status Checking
- Revocation Capabilities
  - Technical Ability to Check Status
- Reporting Investigation Response

Employee & Third Party
- Trustworthiness & Competence
  - Trusted Delegation of Functions

Data and Record
- Data Security
- Audit Trail

Compliance
- Audit Requirements

Transport Security
- SSL
Extensible roadmap

- New kinds of organizations
- New applications
- Expanded geographical coverage and assurance schemas
- Expanded Cloud IdM use
- Enhanced user visual indicators
Ensuring Confidentiality (and trust):

Extending Enterprise Key Management to Infrastructure Entity Authentication

Bob Griffin

Technical Director, RSA, the Security Division of EMC

Co-chair, OASIS Key Management Interoperability Protocol TC
Data Encryption using Symmetric Keys

Enterprise Key Manager

Key Management Interoperability Protocol

Application
Server
SAN
Tape Library
Storage Array
KMIP: Single Protocol Supporting Enterprise Cryptographic Environments

Key Management Interoperability Protocol

Enterprise Key Management
User Identity with Asymmetric Keys
Infrastructure Entity Identification

- KMIP to Commercial Meter
- KMIP to low-end Residential Meter
- KMIP to Industrial Meter
KMIP Request / Response Model

Enterprise Key Manager

Request Header | Get | Unique Identifier

Response Header | Symmetric Key | Unique Identifier | Key Value

Encrypted data

Commercial Meter

Utility

Name: XYZ
SSN: 1234567890
Acct No: 45YT-658
Status: Gold

Unencrypted data
Transport-Level Encoding

Key Client
- API
- Internal representation
- KMIP Encode
- KMIP Decode
- Transport

Key Server
- API
- Internal representation
- KMIP Encode
- KMIP Decode
- Transport

KMIP

- Encode
- Decode
Objects, Operations and Attributes

**Protocol Operations**
- Create
- Create Key Pair
- Register
- Re-key
- Derive Key
- Certify
- Re-certify
- Locate
- Check
- Get
- Get Attributes
- Get Attribute List
- Add Attribute
- Modify Attribute
- Delete Attribute
- Obtain Lease
- Get Usage Allocation
- Activate
- Revoke
- Destroy
- Archive
- Recover
- Validate
- Query
- Cancel
- Poll
- Notify
- Put

**Managed Objects**
- Certificate
- Symmetric Key
- Public Key
- Private Key
- Split Key
- Template
- Secret Data
- Opaque Object

**Object Attributes**
- Unique Identifier
- Name
- Object Type
- Cryptographic Algorithm
- Cryptographic Length
- Cryptographic Parameters
- Cryptographic Domain
- Certificate Type
- Certificate Identifier
- Certificate Issuer
- Certificate Subject
- Digest
- Operation Policy Name
- Cryptographic Usage Mask
- Lease Time
- Usage Limits
- State
- Initial Date
- Activation Date
- Process Start Date
- Protect Stop Date
- Deactivation Date
- Destroy Date
- Compromise Occurrence Date
- Compromise Date
- Revocation Reason
- Archive Date
- Object Group
- Link
- Application Specific Information
- Contact Information
- Last Change Date
- Custom Attribute
Secure multi-tenancy, verifiable chain of trust.

Information-centric security, risk-driven policies, IT and security operations in alignment, information compliance

Visibility into virtualization infrastructure, privileged user monitoring, access management, network security, infrastructure compliance
Security as a System

Business Strategy and Risk

EVIDENCE

- DLP
- SIEM
- Fraud Prevention
- Configuration Management
- Patch and Vulnerability Management

CONTROLS and CAPABILITIES

- Firewalls
- Anti-Virus
- Anti-Malware
- Authentication
- Access Management
- Encryption
- Key Management

IT INFRASTRUCTURE

- Physical
- Virtual
- Cloud

CONTEXT | POLICY

BUSINESS PROCESS

BUSINESS VIEWS
The Need to Extend Enterprise Key Management

End to end chain of trust

End to end visibility

Trusted zone

End to end visibility

DMZ

Virtual Infrastructure
(including hypervisor)

APP
OS

APP
OS

APP
OS

Compute

Network

Storage
Establishing the Web of Trust

End to end chain of trust

Virtual Infrastructure (including hypervisor)

Compute
Network
Storage

Trusted zone
DMZ

APP
OS
APP
OS
APP
OS

Services

End to end visibility