Operational and Organizational Models for Certificate Management Entities

April 19, 2012
Washington, DC
Table of Contents

- Overview of Project
- CME Functions
- Security Baselining
- Organizational Models
- Connected Vehicle Environment
- Comparative Analysis
- Oversight Options
- Cost Approach
- Summary of Outstanding Questions
- Next Steps
Project Description

- Analyze alternative approaches and models for Certificate Management Entities (CMEs) for the Connected Vehicle Program

- All approaches balance the security of communications with protection of the system’s users’ privacy

- CMEs perform the back-end processes to ensure the security of communications and protect the privacy of system users

- User trust is built by system users receiving valid messages from other system users

- Any viable CME structure must be cost-effective, efficient, and scalable
Project Goals

**Original Goals**
- Analyze organizational and operational models
- Define roles and responsibilities of CME
- Develop implementation plan for operating CME
- Develop cost estimates of resources/operation

**Additional Goals**
- Identify baseline to analyze security risks
- Identify policies needed to drive decisions
- Identify ways to integrate into existing organizations
- Identify missing technical specifications
Project Approach

Overview of Project

Review and Integrate Feedback
- Reviewed all documentation
- Documented the perspectives of multiple stakeholder groups:
  - Researched comparative industry practices and organizations
    - Federal PKI Policy Authority
    - International Registration Plan
    - E-ZPass toll system
    - Smart Grid

Additional Research and Analyses
- Analyzed sub-functions and activities
- Narrowed list of acceptable models
- Built in requisite elements to models:
  - Analyzed different oversight structures
  - Developed policy and technical assumptions
  - Defined outstanding questions and decisions

Evaluate and Refine
- Detailed development of three models
- Analyzed security baseline and privacy protections for:
  - Electronic Health Records
  - Electronic Voting
  - Standard PKI systems
- Detailed all implications of outstanding questions
- Evaluated each model against DOT criteria
Principles of Certificate Management

- A CME is an organization responsible for some of the functions and activities of certificate management.
- A Public Key Infrastructure (PKI) scheme was selected for communications security.
- The Activation system is the only part of the system that may collect PII, if that decision is made.

**Functions: The high level CME functions**

<table>
<thead>
<tr>
<th>Certificate Authority (CA)</th>
<th>Registration Authority (RA)</th>
<th>Linkage Authority (LA)</th>
<th>Misbehavior Detection &amp; Mgmt (MDM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central signing authority for all certificates</td>
<td>Communicates directly with On Board Equipment (OBE)</td>
<td>Creates linkage values</td>
<td>Reviews misbehavior reports to identify malfeasance and malfunction</td>
</tr>
<tr>
<td>Distributes certificates to RA</td>
<td>Coordinates with CA and LA to distribute certificates to OBE</td>
<td>Encrypts and sends linkage values to RA</td>
<td>Reviews Certificate Revocation Lists (CRLs)</td>
</tr>
</tbody>
</table>
CME Process Flow (Certificate Batch Development)

1. **OBE**
   - Requests annual batch of certificates

2. **RA**
   - Receives request
   - Approves request (checks that CSR is OK)
   - Shuffles with other OBE requests & sends to CA

2.a. **LA1**
   - Creates 105,120 linkage values

2.b. **LA2**
   - Creates 105,120 linkage values

3. **CA**
   - Signs and encrypts certificates

4. **CA**
   - Sends encrypted certificates to RA

5. **RA**
   - Receives encrypted certificates, boxes them into 12 sets, and sends annual batch to the OBE

6. **OBE**
   - Receives annual batch of encrypted certificates
CME Process Flow (Certificate Decryption)

7. OBE
   Requests monthly decryption key

8. RA
   Receives requests, checks against CSR CRL and assigns decryption key

9. RA
   Sends monthly decryption key

10. OBE
    - Receives monthly decryption key
    - Decrypts box and uses certificates
Security Baselining for CME

- **PKI Design Baseline**
  - CMEs feature a separated CA and RA function and the LA functions.
  - This adds complexity to traditional PKI design.

- **Vulnerability Baseline**
  - PKI design indicates that no level of vulnerability is acceptable.
  - Comparative industries protect against vulnerabilities in different ways.

**ICAO (ePassports)**
- The International Civil Aviation Organization.
- Passive Authentication is the Baseline Security Method.
- Advanced Security Methods include Extended Access Control, Data Encryption.

**Payment Card Industry (PCI)**
- The PCI Data Security Standard (PCI DSS).
  - Routine audits, external vulnerability scans, and specific SW/HW controls.
  - Merchants with high transaction rates require more security measures.

**Department of Defense**
- The Dept. of Defense certificate policy (CP).
  - Subscribers have certification practice statements (CPS).
  - Can trust outside participants by cross certifying with Federal PKI Policy Authority.
Model 1: Registration Authority/Misbehavior Integrated

- Registration and Misbehavior Organization
  - RA
  - MDM

- Certification Organization
  - CA

- Linkage Organization
  - LA1
  - LA2
Model 2: Certificate Authority/Misbehavior Integrated

- **CA**
- **MDM**
- **RA**
- **LA1**
- **LA2**

**CA** and **RA** combined form **CAACT** and **RAACT**

**Linkage Organization**

**Registration Organization**

**Certification and Misbehavior Organization**
Model 3: Registration/Misbehavior/Linkage Integrated

Registration, Misbehavior and Linkage Organization

Certification Organization

RA
MDM
LA1
LA2
CA

CME Models
Connected Vehicle Environments

- **V2V** communication represents the base level environment
- **V2I / I2V** communication involve both safety messages and exchanges of data
- **V2X** communication involve the incorporation of devices such as cell phones into the communication system
Personal Privacy Protection and Auditing

- Each industry has standards for security systems that participants are required to abide by
- Audits determine what levels of security breaches are unacceptable
- Some industries require extra security levels based on affiliation

Electronic Voting Systems
- Generally required that ex-convicts are screened to be able to vote
- Real time audit logs ensure vote count accuracy by producing a printout of individual votes without PII for recounts

Electronic Health Records
- Protections such as Wireless Intrusion and Prevention Systems (WIPS) and file integrity monitoring identify and prevent unauthorized data access
- Compliance audits can lead to license revocation/fines

Payment Card Industry
- Payment Card Industry Data Security Standards calls for routine audits, external vulnerability scans, and specific software and hardware controls
- Merchants with high transactions require more security measures and face greater penalties for non-compliance
## Physical, Technical, and Procedural Controls

- Controls are implemented in PKI systems to address risk associated with both internal and external threats

### Physical Controls
- Address the physical design elements of PKI equipment and security of facilities and stored data
  - Department of Defense

### Procedural Controls
- Address the methods by which processes are carried out by the PKI. Other controls (such as personnel controls) were rolled into this category during analysis
  - Federal Bridge Certification Authority

### Technical Controls
- Address the specific hardware and software security specifications as well as how certain technical processes, such as those associated with public and private keys, are carried out
  - SAFE-BioPharma
  - CertiPath
Large Scale Implementations

Analog to Digital TV
- Estimated 70-80 million TVs
- Customers who did not switch to DTV would no longer receive channels
- Authorized list of coupon-eligible converter boxes provided by the National Telecommunications Information Administration (NTIA) for DTV transition

Seatbelts
- Mandatory for all vehicles since the mid 1960’s
- Drivers who do not participate by using a seatbelt are usually fined
- DOT "Safety incentive grants" for use of seat belts are available to states for having a higher rate of seatbelt usage than the national average and for engaging in innovative projects related to seatbelt safety

Emissions
- Mandatory for all vehicles beginning in 1967
- Drivers without valid emissions inspection stickers can be fined or have their licenses revoked (applies to states that require frequent emission checks)
- Tax credits for drivers of hybrid cars were created by the Energy Policy Act of 2005
CME Oversight Options

**Public (Federal) Oversight**
- Increased costs
- Increased approvals
- Possible streamlined coordination among dispersed
- Increased resistance
- Difficult to leverage commercial industry and opportunities

**Hybrid Oversight**
- Combination of public and private standards, regulations, policies, and oversight
- Can leverage the most effective models and funding sources
- Can also be leveraged with state and local options and systems
- May not imply same standards across entire system

**Private Oversight**
- Must still comply with federal regulations and policies
- More flexibility
- Independent organizations develop standards and practices
- Extensive opportunities for developing commercial applications
- Additional possibilities for investment and funding
- May spur independent economic activity

U.S. Department of Transportation
Research and Innovative Technology Administration
Approach to Cost Estimation

Challenges and Constraints in Cost Estimation for CMEs

- Size and scope of the program
  - 250 million vehicles at full implementation, five-minute certificates
  - Largest PKI set in the world today is ~6.5 million users
  - Longest running commercial PKI platform to date has issued 103 million certificates
- Additional security and technical requirements
  - Certificate lifespans require thousands of Hardware Security Modules (HSM) and potentially several hundred thousand servers
- The proposed organizational structures differ largely from current PKI organizations
Cost Elements

**Major Cost Elements**

- Start-up (design, development, and implementation)
- Annual operation and maintenance
- Auditing security and privacy procedures across all functions and resources
- Software acquisition and maintenance
- Hardware and networking infrastructure
- Secure facilities
- Creation and auditing of policies and procedures
- Management of the certificate lifecycle
CME Organizational Models

CA_{\text{ACT}} \quad RA_{\text{ACT}}

- Registration and Misbehavior Organization
  - RA
  - MDM

- Certification Organization
  - CA

- Linkage Organization
  - LA1
  - LA2

CA_{\text{ACT}} \quad RA_{\text{ACT}}

- Certification and Misbehavior Organization
  - CA
  - MDM

- Registration Organization
  - RA

- Linkage Organization
  - LA1
  - LA2

CA_{\text{ACT}} \quad RA_{\text{ACT}}

- Registration, Misbehavior and Linkage Organization
  - RA
  - MDM
  - LA1
  - LA2

- Certification Organization
  - CA
Impact of Organizational Models on Cost

- Organizational models may have a limited impact on cost
  - Technical requirements drive software and hardware procurement
  - Combined functions can lead to the sharing of facilities and human resources
  - Cross-training of personnel across functions may be possible within policy, technical, and procedural controls needed

**Model 1: RA/MDM Integrated**
- RA and MDM could share personnel and facilities costs
- CA and LAs would not realize cost savings

**Model 2: CA/MDM Integrated**
- CA and MDM would be able to leverage shared personnel
- RA would not realize cost saving efficiencies under this model

**Model 3: RA/MDM/LA Integrated**
- CA may be able to operate in a virtual environment
Outstanding Issues and Decisions to be Made

Credentialing
Where and how much PII to collect:
- No PII (policy)
- PII during Activation (new or existing system) (policy)
- PII connected to certificates (policy)

Misbehavior
- How malfeasance is identified (global processing) (technical)
- Penalties (policy)
- What behavior requires suspension vs. revocation (policy)

Oversight and Ownership
What will the industry oversight structure be:
- Public (policy)
- Private (policy)
- Hybrid (policy)
Outstanding Issues and Decisions to be Made

Implementation Planning
- Policy decisions over time (policy)
- Built in versus after market devices (policy)
- Technological requirements (technical)
- Roll out strategy – coverage prioritization (policy/technical)

Certificate Policy
- What the policy will say regarding roles, rules governing obtaining certificates, technical and audit requirements (policy)

Certificate Length and Download
- Lifespan of certificates is five minutes (technical)
- Certificates are downloaded annually (technical)
Next Steps

**Updating and Reporting**
- Incorporate DOT feedback into March 2012 Report
- Develop proceedings of April workshops
- Additional analysis of outstanding questions and topics
- Additional cost model scenarios and analysis

**Phased Development Approach**
- Collaborate with technical teams developing the approach
- Build in requisite elements to phased roll out model:
  - Security baseline
  - Implementation scenarios
  - Governance models
  - Cost estimates
  - Roles and responsibilities

**Present and Communicate**
- Update analyses and reports based on feedback
- Evaluate all models and updated scenarios against criteria
- Develop public meeting materials for presentation to stakeholders
- Present findings and analyses to USDOT and external stakeholders