RITA Intelligent Transportation Systems Joint Program Office

Certificate Management Entities for a Connected Vehicle Environment

Public Workshop Read-Ahead Document

April 5, 2012

U.S. Department of Transportation
Research and Innovative Technology Administration

Produced by **Booz Allen Hamilton** for
ITS Joint Program Office
Research and Innovative Technology Administration
U.S. Department of Transportation

Notice

Technical Report Documentation Page

1. Report No. **FHWA-JPO-**	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Certificate Management Entities for Connected Vehicle Environment Public Workshop Read-Ahead Document		**5. Report Date** 04/06/2012 **6. Performing Organization Code**
7. Author(s) Dominie Garcia, Andrea Waite, Richard Walsh, Blake Sheppard, Larry Frank, Dan Jeffers		**8. Performing Organization Report No.**
9. Performing Organization Name And Address Booz Allen Hamilton 8283 Greensboro Drive McLean, VA 22102		**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.** **DTFH61-11-D-00019**
12. Sponsoring Agency Name and Address Research and Innovative Technology Administration Intelligent Transportation System, Joint Program Office 1200 New Jersey Ave SE Washington, DC 20590		**13. Type of Report and Period Covered** Public workshop background document **14. Sponsoring Agency Code**
15. Supplementary Notes		

16. Abstract

This document presents an overview of work conducted to date around development and analysis of organizational and operational models for certificate management in the connected vehicle environment. Functions, organizational models, technical background, and approach to cost estimation are all included. This work is being conducted on behalf of the US Department of Transportation, with collaboration from multiple agencies within the department.

17. Key Words	18. Distribution Statement		
19. Security Classif. (of this report)	**20. Security Classif. (of this page)**	**21. No. of Pages** 15	**22. Price**

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Certificate Management Entities for a Connected Vehicle Environment

Introduction

As part of the research and preparation work for an eventual nationwide deployment of vehicle-to-vehicle and vehicle-to-infrastructure systems capable of supporting crash imminent safety and other applications, the US Department of Transportation (USDOT) Research and Innovative Technology Administration's (RITA's) Intelligent Transportation Systems Joint Program Office (ITS JPO) has contracted Booz Allen Hamilton (Booz Allen) to analyze alternative approaches and models for Certificate Management Entities (CMEs), with collaboration from multiple agencies within the department. CMEs perform the back-end processes to ensure the security of communications and protect the privacy of system users, thereby building user trust. Any viable CME structure must be cost-effective, efficient, and scalable.

The purpose of this project is to analyze the ability of alternative potential organizational structures for CMEs to address these goals and functional requirements, and to balance the security of communications with protection of the system's users' privacy. A total of 15 models were considered although only seven were deemed acceptable based on privacy and security needs. These seven models were then pared down to three for detailed development and analysis, based on several system criteria.

The project unfolded in phases, with different levels of detail on the various elements of organizational designs for CMEs addressed along the way. The first phase of the project presented a description of all the potential organizational models that could be implemented to execute certificate management, with a discussion of initial findings to distill trade-offs and advantages and disadvantages of various organizational models and approaches. A second phase of the project included detailed build out of three models, as well as development of security baseline and credentialing approaches. All these were evaluated against a set of criteria developed by USDOT, included in Table 4 below.

Project Approach

Booz Allen followed a systematic methodology in collecting and analyzing data in order to understand the various elements to be included and designed into the organizational models for Certificate Management Entities. This methodology included interviews with key stakeholders, a full document review, discussions with Subject Matter Experts in related fields, and frequent discussions with the USDOT internal working group members to validate and revise the approach and findings.

The project team engaged in discussions with several key stakeholder groups, both internal and external to USDOT. Some of these groups, such as the Vehicle Infrastructure Integration Consortium (VIIC), Crash Avoidance Metrics Partnership (CAMP), and American Association of State Highway and Transportation Officials (AASHTO), have been involved in developing the connected vehicle paradigm. However, other

stakeholder groups had not previously been involved and discussions with them provided an opportunity to introduce the concept and begin the process of soliciting feedback. Table 1 below includes a full list of the stakeholder groups involved in discussions to date.

Table 1: List of Stakeholder Groups

Stakeholder Group	Areas of Interest
Vehicle Infrastructure Integration Coalition (VIIC) and Crash Avoidance Metrics Partnership (CAMP)	▸ Multiple separate entities with different governance structures ▸ Backwards compatibility of system technology ▸ Accounting for and managing jurisdictional boundaries/barriers
American Association of State Highway and Transportation Officials (AASHTO)	▸ Functional responsibilities ▸ Sources of funding ▸ CMEs integrated into and built on existing standards
Volpe	▸ Levels of privacy and security of system ▸ Sustainable financing/cost implications of system
Trucking Industry Representatives and FMCSA	▸ Type and amount of PII collected ▸ Potential differences in trucking involvement versus light vehicle ▸ Sources of funding
National Highway Traffic Safety Administration (NHTSA)	▸ Integrating security credentials with existing organization (e.g. vehicle registration/VIN) ▸ Privacy frameworks
Transit Industry Representatives and FTA	▸ Certificate revocation ▸ Accounting for and managing jurisdictional boundaries/barriers ▸ Sources of funding

Booz Allen also reviewed and synthesized the perspectives and technical guidance provided in a series of documents developed by some of the stakeholder groups included above as well as internal USDOT working groups and affiliate organizations. The documents explain the current thinking around technical requirements, policy considerations, and decisions that must be made, and how various functions and processes should be designed in order to protect both security of communications and privacy of users within the system.

Iterative development of organizational models and configurations was conducted in parallel with deep research into security and privacy baseline techniques and standards, as well as into exploration of multiple methods of device credentialing. Cost estimates were developed based on as much relevant data as are available, keeping in mind the unique needs of a connected vehicle environment, capable of supporting crash-imminent safety warnings.

CME Functions

Public Key Infrastructure (PKI) is the communications security foundation upon which the proposed security system models and functions are based. For the PKI to meet the security needs of the Connected Vehicle

Environment, four necessary functions were identified: Registration Authority (RA), Certificate Authority (CA), Linkage Authority (LA), and Misbehavior Detection and Management (MDM). The LA is a unique function introduced in the connected vehicle environment to facilitate efficient revocation of groups of certificates issued to a single On Board Equipment (OBE). Short descriptions of all functions follow.

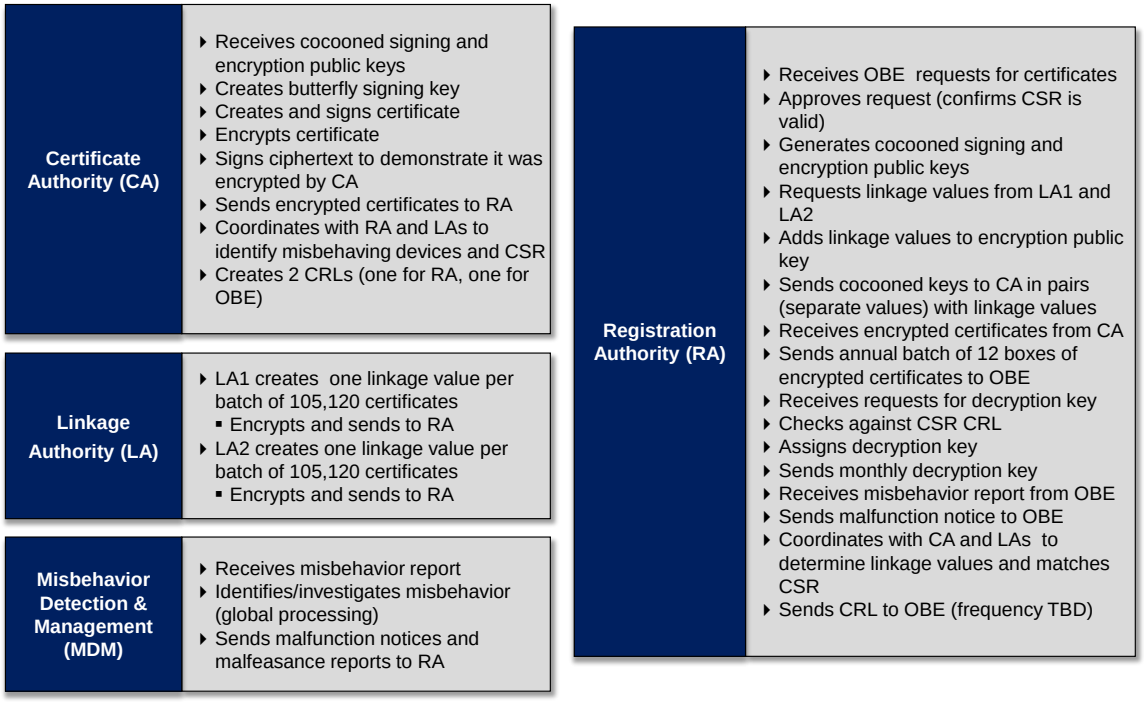
Registration Authority (RA) communicates directly with the OBE and interfaces with each of the other CME functions. The RA receives OBE certificate requests, which include a signing and encryption public key. The RA expands each OBE public key into a set of intermediate keys for each OBE for 1 year of certificates, each valid for 5.5 minutes, that is 105,120 pairs of keys. The RA communicates with each LA to obtain encrypted linkage values. The RA creates a complete certificate request which consists of a single signing key, an encryption key and one linkage value from each LA. The RA collects sets of request data from multiple OBEs and shuffles the requests to ensure that complete certificate requests are not sent to the CA in a sequentially identifiable order. The RA sends the certificate request to the CA for certificate issuance. The RA receives the OBE certificates back from the CA, batches them into groups that are encrypted, and forwards them to the OBE for use.

Linkage Authority (LA) communicates only with the RA and provides linkage values in response to a request by the RA. The linkage values provide the CA a means to calculate a certificate ID and a mechanism to connect all 105,120 certificates for ease of revocation. At least two LAs are required to split formation of the certificate ID and improve the privacy of the system.

Certificate Authority (CA) issues the Basic Safety Message (BSM) certificates and other Wave Short Messages (WSMs). It receives the certificate request from the RA. It does a final transformation of the intermediate keys, calculates a certificate serial number using the linkage values, and generates and signs the BSM certificates. It encrypts the BSM certificate with the associated OBE's encryption key and sends the encrypted data back to the RA for distribution to the OBE. In addition to certificate issuance, the CA collaborates with the LAs and RA to identify OBE values to place on the Certificate Revocation List (CRL). Once identified, the CA will place the value on the CRL which it generates, signs, and sends to the RA for distribution.

Misbehavior Detection and Management (MDM) receives misbehavior reports from the OBE and performs investigations or other processes to figure out levels of misbehavior. This is not an external law enforcement type function, but rather a function that represents the internal CME work to detect when messages are not plausible or when there is potential malfeasance within the system. Any connection to law enforcement is addressed by policy directives. Figure 1 represents a functional hierarchy with a detailed listing of responsibilities within each function.

Figure 1: Certificate Management Functions and Responsibilities

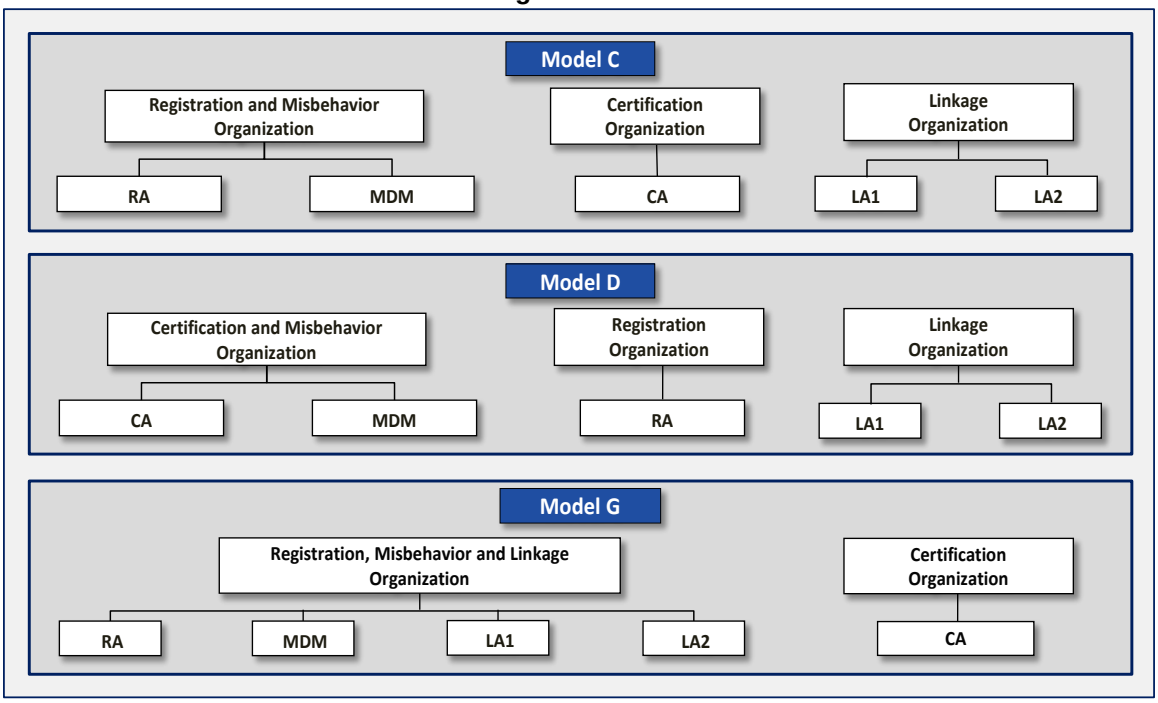


A key conclusion about the CME functions is related to the separation of the two LA functions. External stakeholder groups have suggested that these need to be within legally/administratively separate entities. This team's research and analyses suggest that this separation is not necessary, as it would negligibly improve security safeguards and significantly increase costs and organizational complexity.

CME Models

Following an initial presentation to USDOT and the public in December 2011, a few approaches to organizing CME functions in different operational and organizational models were chosen for further exploration. This paper presents additional analyses on multiple topics that affect CME functions and thus the organizational models. We present here in Figure 2 the three high-level organizational models that are subsequently modified based on the additional analyses presented.

Figure 2: CME Models



The basis of the different models is grouping of functions into different entities. To clarify – when functions are represented to be in one entity by a single box in a model, it implies that the operations, governance, administration, and legal definition/boundaries of an organization are distinct and independent of those for another organization or entity represented by a different box. As mentioned previously, there is an assumption that separating functions into distinct administrative/legal entities provides the highest levels of security and protection against data and information crossing functional lines. Individuals would have to collude across organizational boundaries in order to breach security protocols and controls in place.

In developing the models, the team took input from stakeholder groups that suggested that the two LAs be separated into distinct legal entities. It is our understanding, as noted previously in the discussion on LAs, that there is not sufficient evidence to date that organizational separation of the LAs is necessary, and that robust technical and procedural controls exist to segment data from one LA function to another. Furthermore, some of the models proposed would not have been acceptable because CA and LA functions cannot be in the same organization – a condition that this team believes requires a greater level of security than the organizational separation of LAs.

An additional note is that the existence of an organization to house a particular function does not imply the number of physical locations or machines that may be required to administer that particular function. For example, depending on processing needs and capabilities, and estimates of scale and possible geographical structure, there may need to be several locations and/or organizations across the nation that operate the functions within a legal/administrative entity, based on the model chosen. If Model G were selected, for example, there could be several locations or geographic centers for operating the Certificate Organization. The decisions about numbers and locations of physical entities will be predicated on scale of the system, and policy guidance.

Baselining

The process of establishing a security baseline, in terms of vulnerability and risk thresholds was completed by analyzing existing PKI systems in other industries and organizations, and by examining audit thresholds and protocols, when available. Industry protections against potential risks and vulnerabilities were examined. The primary findings are that PKI as a choice of security system is the fundamental protection against threats and vulnerabilities. Other industries protect against threats to IT systems by implementing procedural, technical, and physical controls to hardware and software access. In addition, auditing procedures and protocols specify acceptable levels of security breaches for some industries, though exact numbers are not available.

Certificate policies within all industries specify how organizations are to protect against hardware and software vulnerabilities, though almost all to date are based on X.509 certificates (those most commonly used in PKI systems today), while the connected vehicle environment will use IEEE 1609.2 certificates (recently standardized certificates that provide added security and encryption levels expressly for connected vehicles), for which new certificate policies and controls will need to be specified. Technical and policy direction about how to monitor, audit, and enforce standards will guide implementation of security standards within the CME PKI.

The nature of a PKI trust model, with the CA serving as a single body that must sign all certificates, implies that *any* level of vulnerability would be unacceptable. PKI experts have asserted that there may be some level of risk expected for end users or trusted agents, but any known vulnerability in the system used by the RA or CA should be prevented or mitigated as soon as possible. In attempting to understand how existing security systems approach the issue of vulnerability, the team uncovered information on several organizations and systems that use PKI to protect the security and privacy of users. Table 2 summarizes the examples reviewed.

Table 2: Examples of Addressing Security Vulnerability

Organization – Topic	Method of addressing security vulnerability
International Civil Aviation Organization (ICAO) – ePassports	▸ Defines 'Baseline Security Method' that countries must follow for the processing of machine readable travel documents, and additional 'Advanced Security Methods' that countries may elect to follow ▸ This approach names a specific security measure that participants must take instead of defining a numerable factor that is acceptable for breaches, identity theft crimes, etc.
Payment Card Industry Security Standards Council – PCI DSS	▸ Requires regular system scans to identify IT vulnerabilities in merchant computer systems. Any IT vulnerabilities with a CVSS score of 4.0 or above are unacceptable ▸ The approach identifies a threshold above which existing IT vulnerabilities are not acceptable. However, it does not account for non-IT vulnerabilities, such as internal malfeasance or physical tampering
Department of Defense, Policy Management Authority – PKI for Identity Management	▸ Specifies general requirements for compliance auditing and maintenance of audit logs for participating PKI systems. Audits are designed to evaluate adherence to each participant's certification practice statement ▸ This approach relies on auditing to identify instances of non-compliance with the security measures that participating PKIs claim to follow. This general requirement for auditing is common among large scale PKI systems such as that of the Department of Defense and Federal PKI Policy Authority (FPKIPA) that are essentially collections of smaller PKI systems

*CVSS = Common Vulnerability Scoring System, which uses a Base Score derived from an algorithm that measures a vulnerability's exploitability and impact to the system.

Fundamentally, the differences between organizational models are not anticipated to change levels of security or privacy protection due to the common application of a PKI approach in all.

Personal Privacy Protection

Protection of users' privacy within the connected vehicle environment is of utmost importance to all stakeholders. Certain conceptualizations of the certificate management approach include a credentialing function, in order to authenticating a device, thereby ensuring its acceptable participation in the system. The notion of credentialing describes a process by which to connect a device to a user in order to ensure that non-allowed devices (as dictated by policy guidance) are not part of the system. For the connected vehicle system, this process (credentialing of devices) would also provide a mechanism through which to follow up on misbehavior and malfeasance issues as they arise, thereby keeping the system secure and trusted. Currently, several options of how to collect users' personally identifiable information (PII) within the CME system have been evaluated.[1] The team presented and evaluated these credentialing options in terms of their impact on privacy protection and CME operations. The various ways of credentialing explored are:

- Total anonymity – no collection of any PII, thus no credentialing process, and no ability to trace malfeasance or misbehavior back to an individual

[1] Fair Information Practice Principles (FIPPS) (NIST SP 800-53 Draft, Appendix J) will provide the framework for analysis of privacy protection

- Collection of PII during device activation. This can in happen in a number of ways:
    - Leveraging existing systems that collect vehicle-based PII, such as VIN
    - Collecting new PII
- Collection of PII within the system that produces and manages short term daily use certificates

A thorough evaluation and description of how each of these credentialing approaches would operate in the connected vehicle system included an analysis of the impacts on the CMEs, summarized below in Table 3.

- **Table 3: Device Credentialing Types**

Type of Credentialing	Implications to CMEs
No PII is Collected	▸ Increases participation of system users ▸ Unable to track back to prosecute malfeasance/bad actors
Direct Linking of Credentials to Certificates	▸ Increases opportunity for collusion or hacking of PII since PII will be included in each certificate ▸ Eliminates the need for the Activation system* (CA_{ACT})
Create New PII Collection System	▸ Increases costs and organizational complexity ▸ Duplicates information already collected by other systems ▸ Requires new policies and regulations for protection of PII ▸ Increases resistance of non participation in the system ▸ Requires the need for a separate database of PII to be maintained
Leverage Existing PII Collection System	▸ Reduces costs and organizational complexity since the Activation system will not be needed ▸ Requires centralized system that is used across jurisdictions ▸ Decreases ability to collect any other PII ▸ Increases trust of system participants since no additional PII is collected

* The Activation system is separate from the one that manages the short term, daily use certificates and the only part of the system that would collect PII, if that decision is made.

Each of these methods of credentialing for various users and communications environments (V2V, V2I, and Vehicle to nomadic devices, V2X) is compared against a set of criteria provided by USDOT, included below in Table 4. The most feasible option, in terms of technical viability, cost, and security protections is integrating credentialing of users within existing systems, such as vehicle registration and USDOT registration for heavy commercial vehicles.

Table 4: Evaluation Criteria

Criteria	Specific Considerations
Technical Feasibility	Impact to security system
	Back office policy choice
	Possible from technical standpoint
	Technical implications that would make option impossible/unfeasible/inadvisable
	Technical implications that would make option desirable
Ability to Leverage Existing System	Leverage existing motor vehicle or driver registration systems
	Reduce scale of RA functions
Security	Pose any special risk to security of PKI design
	RAs choice for identifying system users impact security
	Which poses the least risk to security and why
	Impact to extra-system enforcement as through law enforcement/state/Federal agencies
Privacy	Pose any special risk to privacy of PKI design
	RAs choice for identifying system users impact privacy
	Which poses the least risk to privacy and why
Scope of Data Collection	Scope of data collected and maintained by the RA
Number of Transactions	Estimated number of transactions for the RA annually
Ease of System Use/Implementation	Will the options have an impact on participation in V2V

Expansion of Users to Infrastructure and Mobile Devices

As the connected vehicle environment evolves and expands in scope, it is expected that additional applications and types of users will need to be authenticated and provided with the security credentials to participate in the system. Infrastructure nodes as both conduits of communications between CMEs and OBE, as well as originators of messages will need to be authenticated as trusted members of the system. Nomadic and other non-vehicle-based devices are also addressed in the team's work. The fundamental finding is that the CMEs will need to add levels of functional breadth to existing operations. Additional specification of technical needs and types of applications will determine the kinds of authentication practices that will be added to CME functions.

Misbehavior

A critical component of the CME system is the methods by which misbehavior will be detected and followed up on based on policy direction by regulatory agencies. To date, some conceptual ideas about how misbehavior will be detected and how it will be differentiated between technical malfunction and human malfeasance have been developed. However, technical architecture and processes for executing these conceptual ideas have not yet been developed, and so there remains a high degree of uncertainty in terms of feasibility. Some critical issues related to misbehavior processes and their implications to CME operations are outlined:

- Technical malfunction and human malfeasance within the system – how the differences between these types of misbehavior are detected and what policies are in place to deal with consequences of each are yet to be specified
- Certificate Revocation List (CRL) – exact technical specification of how the CRLs are constructed and distributed is yet to be specified
- Regaining access to the system after placement on CRL – whether this happens through replacement of OBE (as suggested by one stakeholder group), or by reactivation of existing CSR, or by rekeying with new CSR are all decisions that have yet to be made, and will impact how CMEs operate and communicate between each other
- Suspension vs. revocation – decisions about what offenses would require suspension of certificates versus revocation are yet to be made and will also impact the above-point about how to regain access to the system once either suspension or revocation is reversed

Costs

An initial approach to cost estimation has been developed, based on research into existing PKI systems and anticipated needs of all CMEs at different levels of deployment. High level estimates are being developed for all functions, including hardware, software, facilities, redundancy needs, and personnel. Up front and annual costs will be considered. Sensitivity analyses of roll out phases (penetration percentage), regional needs, public versus private ownership, and cost savings realizable per model will represent attempts at providing a range of estimates and considerations.

While there are no one-to-one comparisons from existing PKI systems, certain hardware and software needs, based on current CME process flows and operations can be specified. Additional data about new functions, such as those performed by the LAs, and the process of differentiating between technical malfunction and human malfeasance for the MDM function will have to be further developed and described before applicable cost estimates can be made.

Implementation Planning

Initial high-level discussion of implementation planning and additional considerations required for successful roll out of the CMEs has been part of the work on this project, with particular focus on:

- Communication and training – what kinds of plans and training will be needed to effectively inform and educate users and technical specialists related to CME functions and operations
- Phased roll out – what are the expectations for roll out of the system across different geographic boundaries and areas, and what is needed to support this phased roll out

- Technical and policy support for users and CMEs – what kinds of technical support functions and organizations will be needed over time
- Performance measurement and metrics (see Table 5 below)

Table 5: Initial Performance Measures

Vehicles and linked infrastructure need to trust each other when they exchange information	▸ How is trust determined? ▸ How is trust lost or gained? ▸ What makes the CME reliable?	▸ Accuracy of data being exchanged ▸ Security audits ▸ Signing and encrypting certificates ▸ Disaster recovery ▸ Separation of PII ▸ CRL suspensions, revocations, and reinstatements
Vehicles and linked infrastructure need to exchange meaningful data to facilitate safety, traffic, and environmental messages	▸ What defines meaningful data in this context?	▸ Type of information collected ▸ Where the information is stored and how it is retrieved ▸ How the information is distributed ▸ How the information is used
The CMEs need to allow for operation, maintenance, and system updates over time	▸ How do we tell when an update is needed? ▸ How do we tell if the update was successful?	▸ CSR and certificate lifespans ▸ OBE and CSR CRL content ▸ V2V, V2I, and V2X technology compatibilities ▸ CMEs' process quality management
The CMEs need to have requisite roles and tasks to maintain operations	▸ What is the job of the RAs, LAs, CAs, and MDMs? ▸ How well do they do their job?	▸ Frequency of certificate requests sent and received ▸ Ability to fill certificate requests ▸ Critical certificate component and time requirements ▸ Misbehavior criteria
The CMEs should be cost effective without sacrificing security	▸ What are the explicit and implicit costs of each CME function? ▸ How do they relate to security?	▸ ROI (Return on Investment) ▸ Benefits to costs of CMEs

Several examples of nationwide changes in key policy and systems, such as seat belt laws, emission standards and digital to analog television transition were examined to provide direction and lessons learned. All of the implementation discussions are predicated on the knowledge that key technical and policy decisions are yet to be made.

Conclusion

For the CMEs for a connected vehicle environment to be successfully implemented, at initial roll out and over time, several outstanding issues must be addressed from the policy and technical perspectives. Decisions in these areas will allow for development of actual organizations and their functions to deliver certificate management operations within the constraints and goals established.

Technical and policy decisions still outstanding include:

- Phases of Roll Out – urban versus rural roll out, timing for implementation of CMEs across the country
- Misbehavior – how it is detected, how malfunction is differentiated from malfeasance (technical questions), and what are the consequences and enforcement policies (policy questions)
- Credentialing – what, if any, PII will be collected at what point in the system and what are the rules governing access to data
- LAs – for current analysis, they are presented as one entity with technical, procedural, and physical controls to separate them. Decisions about what those controls should be need to be specified. Also, what the actual mathematical and algorithmic processes are still under development
- CSR – what is the lifespan of the CSR and how it is rekeyed or renewed
- Back Up Certificates – if they exist and how they are used
- Certificate Policy – what the policy will say regarding the roles and responsibilities, the rules governing obtaining certificates, the technical requirements for generation and protection of private keys and certificates, and the requirements for audit records and periodic compliance audits
- End of Life – how end of life is determined and defined and what the policies are that govern disposal of OBE and removal from the system
- Frequency of Certificate Download – currently assumed to be once a year, but may need to be revisited based on problematic sixe of downloads
- Number of RAs – determined by amount of hardware needed and communications delivery network decisions to communicate with OBE
- Number of CAs – determined by decisions about virtual or physical environment and how to distribute and produce redundancy around the system
- PKI Hierarchy – root CA and hierarchy decision based on options and security determination