RITA Intelligent Transportation Systems Joint Program Office

Communications Data Delivery System Analysis

Public Workshop Read-Ahead Document

April 9, 2012

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

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

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-12-039		

4. Title and Subtitle	5. Report Date
Communications Data Delivery System Analysis Public Workshop Read-Ahead Document	04/09/2012
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
James Misener, Scott Andrews, Peter Cannistra, Dominie Garcia	

9. Performing Organization Name And Address	10. Work Unit No. (TRAIS)
Booz Allen Hamilton 8283 Greensboro Drive McLean, VA 22102	11. Contract or Grant No. DTFH61-11-D-00019

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Research and Innovative Technology Administration Intelligent Transportation System, Joint Program Office 1200 New Jersey Ave SE Washington, DC 20590	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 communications data delivery systems for supporting transactions in the connected vehicle environment. It presents the results of technical analysis of communications needs and the ability of alternative communications media to support these needs. It also describes the next stage of analysis planned, which will include additional technical and commercial analysis around specific scenarios. The project is being conducted on behalf of multiple agencies within the U.S. DOT.

17. Key Words	18. Distribution Statement

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
		20	

Workshop Read Ahead

Introduction

The United States Department of Transportation (USDOT) is assessing options for a communications data delivery system (CDDS) to support security functions and other envisioned applications within a connected vehicle environment. This environment is envisioned first and foremost to support safety warnings in imminent crash situations, which requires a process of legitimizing messages sent across the system to a high degree of certainty. The USDOT and partners have focused on a Public Key Infrastructure (PKI) strategy, which relies on the exchange of digital certificates, for establishing the trust mechanism among users. At full deployment, the CDDS will need to support the communications needs with all legitimate devices on the system for security processes. Ideally the same system will also be able to support the applications envisioned for the system. The purpose of this project is to analyze both the technical implication of various communications options for the CDDS and implications for associated business models. Because there is no assumption of a government run system, the assessment of CDDS options takes on a distinctly commercial form: deployed communications data delivery systems that support certificate management functions must not only be technically viable, they must also be operationally sustainable.

The effort to develop and assess scenarios for a CDDS is approximately a year-long, with the effort reported here representing about a third of the project work to date. This work has thus far been focused on developing high level design and operational concepts that support the transport/delivery functions of a certificate management system. Three alternative data delivery communication links are now the focus: cellular systems, WiFi and Dedicated Short Range Communications (DSRC). The combinations of communication links to be used depend on the functions needed to operate and maintain the security approach, and on the companion institutional, technical and economic viability of the communications data delivery system.

This document is a summary of the results to date. As USDOT enters into further detail in analysis of the communications data delivery system to support the CMEs, obtaining a common understanding with and additional input from stakeholders are critical components to ensuring a robust and comprehensive analysis of CDDS options.

Certificate Management Entity (CME) Approach

As a starting point, a PKI approach depends on a certificate management entity (CME) to manage necessary transactions and back end processes. A separate effort is analyzing organizational models to support the functions needed to deliver trusted certificates to all users. This approach informs the determination of communication needs within the certificate management system and defines the entities involved in communication. A parallel effort to develop configurations to deliver PKI functions has defined the need for several functions: linkage authorities, a certificate authority, a registration authority, and misbehavior detection and management functions, all of which interact with a vehicle's on-board equipment (OBE). These elements and how they communicate are the focus of the data delivery analyses efforts. They dictate need to communicate and to encrypt and decrypt data in order to ensure the security of users through every aspect of the connected vehicle system. This project and analysis are focused on the set of options to deliver communications between these functions and the OBE.

Data Delivery Communication Links

It is easiest to understand the alternative data delivery systems by considering the wireless communications links needed within the set of CMEs and OBE. The landside backhaul system, or what is commonly called Center-to-Field communications, is not explicitly considered with the current analysis. The expectation is that these long-range communication systems may – and in many cases already – exist to perform operations functions. In other words, the communications between the various CMEs are not an explicit part of this analysis as they are assumed to exist already and will most likely be performed over landline networks.

The analysis examines:

- Communications between OBE and Certificate Management Entities (CMEs). The functions provided by this type of communications include:
    - Requests for and distribution of annual certificates
    - Requests for and distribution of monthly decryption keys
    - Misbehavior reports from On-Board Equipment (OBE) to CMEs (unless an onboard means of diagnosing other misbehaving participants is developed)
    - Certificate Revocation Lists (CRLs) from CMEs to OBE(unless an onboard means of diagnosing other misbehaving participants is developed)
- Communications between Roadside Equipment (RSE) and OBE
- Communications between RSE and CMEs
- Communications between RSE and other devices
- Communications between other devices and OBE
- Communications between CMEs and other devices

Six over-the-air communication modes were analyzed for their abilities to provide the needed communications between functions and devices, including for three essential connected vehicle environments: Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Security Management. The six modes examined are:

- Cellular
- WiFi
- Dedicated Short Range Communications (DSRC)
- WiMAX
- Satellite Digital Audio Radio Service (SDARS)
- High Definition (HD)Radio

The communication data delivery technical analysis has explored the general communication requirements for managing security credentials. This examination has identified several possible communications technologies that can support this objective. Three of these modes (WiMAX, SDARS, and HD Radio) were eliminated due to initial analysis that revealed they would not be technically sufficient or practicable to provide the needed support and network availability for the scale of the CMEs and their communications with OBE. The remaining three, (Cellular, WiFi, and DSRC) were developed in more detail in order to begin the process of understanding the business and institutional arrangements that may underpin delivery of certificate data.

The USDOT has also sought to understand how these technologies might support other applications envisioned by the system. So, while the primary objective is to support security related communications, it is important to also understand how any given technology also supports these other applications. These include the suite of V2I safety, mobility and environmental applications envisioned as part of the connected vehicle environment.

This overview is intended to outline the basic operational approach that may be used to support security credential management (or CME functions) using various types and combinations of communications technologies.

Technical Considerations

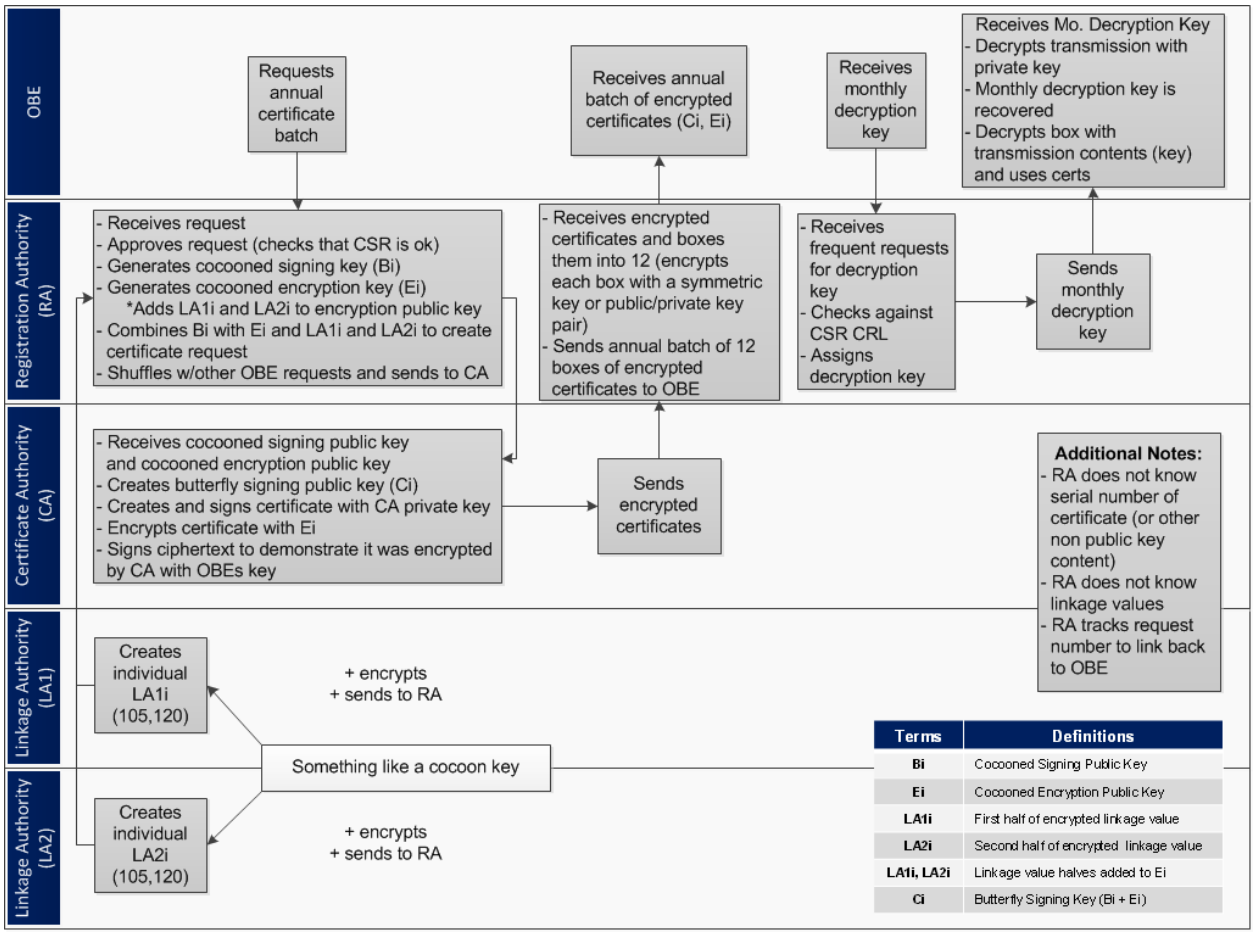
Basic Concepts

In general the CME security system can be modeled as shown in Figure 1 (page 4). Here the mobile terminal (typically a vehicle system) contacts the Registration Authority (RA) to request and obtain security certificates. The mobile terminal and the registration authority have a trusted and identified relationship. This means that the registration authority knows the identity of the mobile terminal, and has sufficient knowledge of the state of the terminal that it can determine that the certificate request originated from a legitimate device.

In order to preserve the privacy and anonymity of the mobile terminal, the registration authority does not issue the certificates directly. Instead, the registration authority, having determined that the mobile terminal is legitimate, request certificates from a certificate authority, on behalf of the mobile terminal. The certificate authority provides these certificates in an encrypted form, so that while the registration authority knows that the terminal is receiving certificates, it cannot read these certificates. Using this approach, the certificate authority knows what certificates were issued, but it does not know the identity of mobile terminal to which they were issued. The registration authority knows the identity of the mobile terminal, but it does not know which certificates were issued to it. Using this mechanism, the mobile terminal can then use the certificates to sign messages, and the receiver of the message can verify that the message came from a legitimate terminal, yet the certificates provide no identifying information about the sending terminal. The messages can thus be validated as authentic, but the privacy and anonymity of the sender is preserved.

It is important to note that since the mobile terminal and the registration authority have an identified relationship, the communications between them does not need to be anonymous. This communications link must be secure (i.e., encrypted) to avoid eavesdroppers from gaining access to the information exchanged between the RA and the mobile terminal. Any communications link capable of providing this security and also capable of providing sufficient data rates to allow the transaction to be completed in a timely manner will suffice.

Figure 1: Certificate Management Entity Process Flow



It is also useful to define a communications system. In the context of this analysis, it is typically a wireless mechanism through which data are transmitted. In most systems the wireless transmission is transmitted in all directions. The transmission can then be received by any terminal configured to receive the radio waves associated with that particular communication technology.
For a broadcast system, all receivers configured to receive messages from the system (i.e. of the corresponding technology type) can receive any transmitted messages. This is similar to FM radio or broadcast television.

In many cases the transmissions are meant to be sent to a specific terminal. Since the transmitter does not necessarily know the location of the terminal, it broadcasts the message as described above, but it includes an address with the message. As with a broadcast system, all terminals receive the message but since it is addressed, if the address does not match their own address they discard the message. In general in these systems the addressed message may also be encrypted to prevent all of the receivers to whom it is not addressed from reading the information in the message. Systems of this type are known as wireless "networks". In many network systems, when a new terminal "arrives" (i.e. comes into range of the other terminals), it must attach to, or join the network (sometimes also called "network association"). This joining process may require that the terminal validate itself as being authorized to join the network, and it generally also involves an exchange of addresses, so that each member of the network (often called "nodes") knows the network addresses of all other members of

the network. Large networks like the Internet are composed on millions of smaller local networks that are linked by routers. In this way a terminal can join a local network, learn the addresses of all of the nodes (e.g. the office printer and the local server), abut it does not need to learn the addresses of each of the billions of terminals that can access the Internet.

In this way, all wireless communication systems “broadcast”, but only some are networks. Connected vehicle applications include both types of communications. Some applications need to attach to a network so that they can exchange messages with specific devices, while others simply need to broadcast information to other terminals in local proximity. The communication technologies under consideration for CME include both types.

Key Technical Needs

The communications link between the mobile terminal and the RA must meet several technical requirements. Some of these requirements derive from the nature of the data exchange, and others arise from the nature of the communications system itself. That is, some characteristics of the communications system may impose other limitations or requirements given the needs of the application.

The core need for the communications system is to provide for communication of data associated with the applications that the system is intended to serve. Since the range of applications imposes a wide range of communications needs, and since not all communications technologies can meet all of the different needs, some technologies are suited for only a subset of the applications. In addition, various non-technical but still constraining characteristics of the potential technologies may impose practical or policy-related limitations that may render them unusable for some or all of the expected connected vehicle applications

Table 1 (page 6) outlines the basic data transfer needs of the various applications. The first two applications, Basic Safety Message (BSM) and WAVE Short Message (WSM), are generic descriptions of the messages (and bandwidth or size requirements) for connected vehicle safety, mobility and environmental applications. They are given in bold and italics to differentiate them from the balance of the application message types and sizes. Nearly all V2V and V2I messages, based on current technical specifications of data elements defined by the Society of Automotive Engineers J2735 (DSRC Technical Committee) have been structured to be sent as a special single packet message known as a WSM, which is specifically intended to support transmission using DSRC. The maximum size of a WSM is fixed by the 802.11 Maximum Transmission Unit (MTU) which is typically limited to 1500 bytes total. The actual messages in an implementation may have slightly different sizes, but the sections below represent the general scale of the messages.
Note that all the other message types and data needs are for CME functions.

Table 1: Basic Signed Message Sizes

Message	Overall Size (Byte)	Sender	Receiver	Sender Transmit Frequency	Security
Basic Safety Message	***528***	***OBE***	***OBE***	***10 per second***	***Anonymously Signed***
Maximum Size Wave Short Message, WSM (many applications)	***1500***	***I/V***	***V/I***	***~10 per second***	***Anonymously Signed (from OBE) Non-Anonymously Signed (from RSE)***
Certificate Update Request	533	OBE	RA	Annual	Encrypted Not Anonymous
Certificate Bundle (Annual)	15,572,040*	RA	OBE	Annual	Encrypted Not Anonymous
Certificate Decryption Request	362	OBE	RA	Monthly	Encrypted Not Anonymous
Certificate Decryption Reply	378	RA	OBE	Monthly	Encrypted Not Anonymous
Misbehavior Report	854	OBE	MDMA	Variable	Anonymously Signed
CRL Request	336	OBE	CA/RA	Daily	Anonymously or Non-Anonymously Signed

**Note, this value id based on available data. Depending on assumptions made, the actual volume may be twice this value (~30 MB).*

Other ways that messages can be sent is using the Internet Protocol (IP), in which the message is contained in a data payload section of the general purpose IP "datagram", or in specialized message formats defined specifically for the communications system.

Using IP communications it is possible to send arbitrary sized messages. In practice, messages larger than 1500 bytes are broken into smaller blocks, and sent in packets. These packets are then reassembled at the receiver end to provide the original large message.

Communications Technology Options

In the analysis conducted to date, cellular, DSRC and WiFi are identified as potential candidate technologies for supporting connected vehicle applications. As described above, the emphasis was on supporting security functions, but the ability of the technology to support other applications was also considered. In general each of these technologies is capable of supporting security transactions, although some can only do so in limited or constrained situations. A vehicle fitted with all three technologies could use whichever was available at the time, although such an implementation could be redundant and expensive. It is also possible that some terminals could use one system while others could use another, although in this situation the system operator would need to resolve the access, business model (payment), and policy issues for each of the technologies. Such an approach would be highly flexible from a terminal perspective, but would; be highly complex from an implementation, policy, and management perspective.

As shown in the next sections, cellular and WiFi technologies do not support the full range of other (non-security) connected vehicle applications. Because there is general interest in other broadcast

technologies, included in this document is a summary of SDARS in the following descriptions, although this technology is understood to be substantially more limited than the three core technologies (cellular, WiFi and DSRC).

The following are descriptions of the processes that would be used by each identified technology to support the application message transactions described above.

Cellular. Cellular communications is a wide area wireless system capable of providing high bandwidth two-way communications. Cellular systems are generally operated by large carriers who provide a variety of cellular voice and data services for a fee. These services range from high speed "unlimited" data (typically limited to between 2 and 5 GB of data transfer per month), to low cost low rate data transfer services that operate on an "as available" basis. These services provide background communications for low cost devices with minimal data transfer requirements, such as "smart" utility meters, alarm systems, and e-readers (to deliver digital books).

In most commercial implementations, cellular does not provide a broadcast function. Instead, all communications are point to point, typically addressed using the Internet Protocol (IP). Because of this, cellular communications are not anonymous to the extent that they are traceable to specific IP addresses, and while these addresses may be dynamically assigned, the carrier (cellular provider) could theoretically link the IP address of a message to a specific individual mobile terminal.

Table 2 below summarizes how the various application messages under consideration would be treated in a cellular system.

Table 2: Cellular Messaging Descriptions

Message	Approach	Security
Basic Safety Message	Not supported because OBE does not know IP addresses of surrounding vehicles	N/A
Maximum Size WSM (V2I)	OBE sends message to intended known recipient IP address	Non-Anonymous: Can be Encrypted
Maximum Size WSM (I2V)	Not directly supported because system does not know IP addresses of vehicles in region where message applies. Can be implemented by having vehicles request messages for specific regions	Non-Anonymous: Sender can link identity of terminal to locations
Certificate Update Request	OBE sends message to RA IP address; RA sends responses back to IP address of sender (which is contained in each incoming message)	Non-Anonymous: Encrypted
Certificate Bundle (Annual)		
Certificate Decryption Request		
Certificate Decryption Reply		
Misbehavior Report	OBE sends message to intended known recipient IP address (presumably RA)	Non-Anonymous Can be Encrypted
CRL Request/Provision	OBE sends message to RA IP address; RA sends responses back to IP address of sender (which is contained in each incoming message)	Encrypted Non-Anonymous Request Non-Encrypted Response

There are a host of technical issues and limitations to using an IP-based system. Underlying this is that in order to send a message in an IP-based system requires that the IP address of the recipient be known. This imposes severe constraints on the use of cellular communications to support many connected vehicle applications, described below in the context of existing cellular systems. In addition, alternative approaches that simplify the process are described where applicable. These alternative systems may require additional functionality beyond the current cellular system.

The use of IP based communications works well for most security transactions. It is problematic for V2V because the IP addresses of the surrounding vehicles are not generally known to all senders. While the IP addresses of all terminals in a given cell may be known, the cells are generally rather large; a given cell may include thousands of terminals. Arguments that the cell size can be reduced to offset this issue are problematic. For V2V each vehicle needs to communicate with other vehicles within about 100 meters range. This 100 meter radius zone moves with the vehicle. Unfortunately the cellular system is fixed. It is possible that alternative approaches to this issue might be developed, but no practical solutions that can scale to 250 million vehicles exist today.

Messages from the vehicle to the infrastructure (V2I) are well supported under a cellular system because the vehicle either knows the IP address of the recipient system or infrastructure (which is fixed) or it can easily learn this address either through an announcement, or by a simple query to a server that knows these addresses. As the vehicle moves the address of the fixed part of the system may change, but changes, if they occur, are infrequent.

Messages from the infrastructure to the vehicle (I2V) are somewhat problematic. The issue is that the fixed system cannot broadcast messages to terminals in a given region as described above. The vehicle also does not necessarily know the IP addresses of vehicles in any particular area where a message is to be distributed. If it were to send all messages for a cell region to all active terminals in the cell, each terminal would receive numerous messages that were geographically irrelevant. The typical solution to this is that each terminal individually requests information corresponding to their current location. The number of messages in this system can grow rapidly, and the bandwidth is not used efficiently since the same basic information is sent individually to all vehicles in any given area. In addition, since the vehicle/terminal is identified, the information provider can theoretically link the identity of the vehicle/terminal to the location of the vehicle at each request.

It is possible that this issue could be resolved by providing a clearinghouse system where the cellular carrier acted as a proxy, making requests on behalf of the information provider. In this way a generic information provider can provide location based information to the cellular carrier without knowing what terminals are requesting it, and the cellular carrier can then provide it over a secure link. This approach has not been completely vetted with carriers, and it would obviously require more involvement from them than simply moving packets.

WiFi. WiFi communications are handled by a local area wireless system capable of providing high bandwidth two-way communications. WiFi installations are numerous and may be operated by individuals or by commercial enterprises. A few municipalities have provided nearly seamless free WiFi coverage in their cities, although this trend appears to be in decline. Enterprise implementations are generally specific to a business or office. In large public areas such as airports and rail/transit terminals, commercial services provide WiFi-based internet access for a fee.

WiFi is a networked system, which means that all communications are point to point, and packets are addressed using the IP. Because of this, WiFi communications are not anonymous to the extent that they are traceable to specific IP addresses, and while these addresses may be dynamically assigned, the service provider who runs the access points, could theoretically link the IP address of a message to a specific individual mobile terminal.

WiFi systems typically are low power and they have a very small communications footprint, typically on the order of about 20 meters (~60 feet). The approach for WiFi to support different connected vehicle messages is described in Table 3 below. It is important to note that for many of the messaging situations that WiFi can support, the mobile terminal must be effectively stationary, since the association time, defined as the time for the terminal to join the network, is longer than the time the vehicle will be in the communications footprint. This is referenced below by the term “footprint-limited”.

Table 3: WiFi Messaging Descriptions

Message	Approach	Security
Basic Safety Message	Not supported because OBE does not know IP addresses of surrounding vehicles	N/A
Maximum Size WSM (V2I)	OBE sends message to intended known recipient IP address; (Footprint Limited)	Non-Anonymous: Can be Encrypted
Maximum Size WSM (I2V)	Not directly supported because system does not know IP addresses of vehicles in region where message applies. Can be implemented by having vehicles request messages for specific regions; (Footprint Limited)	Non-Anonymous: Sender can link identity of terminal to locations
Certificate Update Request	OBE sends message to RA IP address; RA sends responses back to IP address of sender which is contained in each incoming message; (Footprint Limited; certificate bundle transaction requires terminal to be in Hot Spot for several minutes)	Encrypted Not Anonymous
Certificate Bundle (Annual)		
Certificate Decryption Request		
Certificate Decryption Reply		
Misbehavior Report	OBE sends message to intended known recipient IP address (presumably RA); (Footprint Limited)	Non-Anonymous Can be Encrypted
CRL Request	OBE sends message to RA IP address;	Encrypted Non-Anonymous Request
CRL Provision	On request, RA sends responses back to IP address of sender (which is contained in each incoming message); (Footprint Limited for large CRLs)	Non-Encrypted Response

WiFi suffers from many of the same technical limitations as cellular. Specifically, since it is an IP based network without broadcast capability, all of the issues described above for cellular relative to addressing are also present for WiFi, although there are some differences in the mechanisms.

WiFi cannot easily support V2V transactions because vehicles must join the network; that is, they must associate and share IP addresses. This is problematic for several reasons: First, WiFi generally relies on an access point (base station) to set up and manage the network. The base station typically also provides a DHCP service which serves IP addresses to new terminals. There is no reasonable way to have a base station/DHCP server if the terminals are moving. If this is not done, then each terminal will need to have its own IP address, and this will create privacy issues. New technological developments may be able to resolve this issue in the same manner as DSRC does, but are still in development and not commonly available.

Because the set of vehicles in range is constantly changing, the network members are also changing. This will significantly increase network management overhead since the network will be in constant flux. In addition, WiFi has no mechanism for a terminal to be part of multiple networks, but unless vehicles are clumped into isolated groups, a vehicle physically between two other vehicles may need

to be in at least two networks simultaneously. Managing a real network with the combined issues of membership flux and uncertain geographic extent and multiple network membership is well outside the capability of existing WiFi standards.

Messages from the vehicle to the infrastructure (V2I) transactions are supported in the same way cellular V2I is supported. However, the small communications footprint size and the relatively long network association time delay of WiFi means that if the vehicle is moving at any significant speed (e.g. more than a few mph) it will exit the footprint before it can execute any data transactions. This means the vehicle must be essentially stationary in order to send messages to the infrastructure.

Messages from the infrastructure to the vehicle (I2V) transactions are also problematic. Unlike cellular, where the footprint is so large that sending messages for the entire region would be highly inefficient, WiFi footprints are so small that one must try to determine what data in the surrounding area would be useful to terminals in any given footprint. While this is certainly possible, it is not currently a well-understood problem. More importantly, as described above, the footprint is so small that the vehicle must be effectively stationary to join the network and then receive messages.

The limitations on V2I and I2V transactions using WiFi are especially problematic for security transactions because the volume of data to be exchanged (the annual certificate bundle) is large. It is possible that these transactions could be carried out by placing WiFi base stations at gas stations and charging facilities. This approach would generally assure that the vehicles were stationary for a sufficient time to complete transactions. In addition, most vehicles visit fueling and charging stations regularly, so updating certificates at these locations would be a natural fit. The only remaining issue if this approach is used is that the vehicles do not visit these locations daily, and the delivery of the Certificate Revocation List (CRL) is expected to occur on a daily basis. So, with a specialized deployment at fueling/charging stations a WiFi based system would probably support certificate updating, but would not necessarily assure that the vehicle had an up to date CRL.

DSRC. DSRC communications is a local area wireless system capable of providing high bandwidth two-way communications for vehicles in motion. DSRC provides for both broadcast operation, where messages are “addressed” to an application type, and for networked (point to point) operation, where messages use IP addresses. DSRC can operate in these two modes on a message by message basis, so one message might be broadcast, and the next might be sent to a specific IP address.

DSRC has no network association process. In broadcast mode, the terminal simply transmits messages and any terminal in range can receive that message. In IP mode, it uses the IP address of the RSE to create its own IP address dynamically via a process called “stateless address auto-configuration”. Essentially, the mobile terminal can operate in network mode when it is in range of a network node (i.e. an RSE), and it can operate in broadcast mode any time.

DSRC systems typically are medium power and they have a communications footprint of about 300 meters, specifically designed to support the roadway environment. The approach for DSRC to support different connected vehicle messages is described in Table 4 below. As with WiFi, where the transaction is limited by the size of the RF footprint and the volume of data (or where the maximum vehicle speed may be limited in order to support the transaction), the term “footprint-limited” is used.

Table 4. DSRC Messaging Descriptions

Message	Approach	Security
Basic Safety Message	Supported. Mobile terminals can broadcast BSMs to all terminals in range	Broadcast messages signed using anonymous certificates
Maximum Size WSM (V2I)	Mobile terminal either broadcasts message and terminals in range receive it, or it sends message to intended known recipient address (MAC address) for local terminal	Messages signed using anonymous certificates
Maximum Size WSM (I2V)	RSE broadcasts messages that can be received by all mobile terminals in range; Typically messages are sent in location where they are likely to be relevant	Broadcast messages signed using non-anonymous certificates (RSE does not need to be anonymous)
Certificate Update Request	Mobile terminal sends message to RA IP address via RSE; RA sends responses back to IP address of sender (which is contained in each incoming message); (Footprint Limited; Certificate bundle transaction requires terminal to be in range of RSE for about 1 minute; limits speed to 5 m/sec, 11 mph)	Encrypted non-anonymous IP messages
Certificate Bundle (Annual)		
Certificate Decryption Request		
Certificate Decryption Reply		
Misbehavior Report	Mobile terminal sends message to intended known recipient IP address (presumably RA) while in presence of RSE;	Non-Anonymous Can be Encrypted
CRL Request	Mobile Terminal sends message to RA IP address via RSE;	Encrypted Non-Anonymous Request
CRL Provision	On request, RA sends responses back to IP address of sender (which is contained in each incoming message); (Footprint Limited for large CRLs)	Non-Encrypted Response

DSRC was designed specifically to support V2V and V2I/I2V data exchanges, so it does not exhibit any severe limitations for most applications. However, under the current CME security design it is somewhat limited for operations related to certificate updating and CRL distribution. This is because the current design specifies annual certificate updates, and the volume of data for this transaction will fall between 15 MByte and 30 MByte. To remain in radio range of an RSE for a sufficient time period to complete this data exchange will require that the vehicle be traveling no faster than about 11 mph and possibly as slowly as 5 mph. Changing the CME security design to less frequent CRL distribution would substantially mitigate this issue.

SDARS. Satellite Digital Audio Radio Service (SDARS) is a communications standard used to deliver CD quality digital audio to subscribers over a nationwide satellite link. The standard is technically open to anyone who can obtain spectrum, but from a practical perspective, Sirius/XM, a product of the recent merger between Sirius Satellite Radio and XM Radio, is the only operator

SDARS is a one-way broadcast system, so terminals on the ground can receive data, but they cannot send data. Since the system is subscription based, the data is encoded in a way that requires an active receiver to decode. The receivers can be activated and de-activated (based on the status of the subscription) using messages sent over the satellite link. A new user can buy a receiver and subscribe over the phone or via the internet. At the time of subscription, the user provides the ID number of the receiver and the operator (Sirius/XM) sends an activation message addressed to that particular receiver. This activates the receiver so it can then receive various channels.

While originally conceived for audio delivery, the system can support delivery of a variety of low bandwidth data. For example, Sirius/XM currently provides traffic data for 60 metropolitan regions in the U.S. and can provide other car maker specific data. Acura uses the system to send service notices and recall data to equipped Acura vehicles over a service known as AcuraLink.

Attributes from SDARS that would be necessary to support different connected vehicle messages is described in Table 5.

Table 5: SDARS Messaging Descriptions

Message	Approach	Security
Basic Safety Message	Not supported. System can send data to vehicles, but vehicles cannot use system to send messages	N/A
Maximum Size WSM (V2I)	Not supported. System can send data to vehicles, but vehicles cannot use system to send messages	N/A
Maximum Size WSM (I2V)	Supported; System can send messages to all vehicles operating in the continental US. Messages can be geographically coded	Embedded in message encoding. No explicit message authentication
Certificate Update Request	Not supported. System can send data to vehicles, but vehicles cannot use system to send messages	N/A
Certificate Bundle (Annual)	Not directly supported since vehicle cannot make request for certificates. System can send message to specific vehicle however the cost of this for certificate updates would be exorbitant.	Embedded in message encoding. No explicit message authentication
Certificate Decryption Request	Not supported. System can send data to vehicles, but vehicles cannot use system to send messages	N/A
Certificate Decryption Reply	Not directly supported since vehicle cannot make request for certificates. System can send message to specific vehicle however, so if key provision were automatic, then this would work.	Embedded in message encoding. No explicit message authentication
Misbehavior Report	Not supported. System can send data to vehicles, but vehicles cannot use system to send messages	N/A
CRL Request	Not supported. System can send data to vehicles, but vehicles cannot use system to send messages; Can be avoided with automatic broadcast of CRL.	N/A
CRL Provision	System broadcasts CRL to vehicles nationwide	Embedded in message encoding. No explicit message authentication

SDARS is only useful for broadcasting messages to vehicles. Since the radio footprint is nationwide, every vehicle can technically receive every broadcast. If the broadcast is universally useful, this approach may be efficient. However, it is highly inefficient for regional information since the system must sequentially transmit information region by region. As long as the volume of regional; information is small, the revisit time (latency) is low. However, as the volume of regional information grows, the time required to cycle through all of the regions grows excessively long. Depending on how many channels are used, covering all roads would result in a revisit time of about 1 week.

Since it was designed primarily to support audio, the SDARS link is relatively narrow band. This means that sending large volumes of data is slow. While audio files can also be large, they are not downloaded, but instead are streamed, so the user can listen to the audio as it is received. Using this approach, a file that might actually be several Mbytes, can be received over a period of several minutes. While this link could also be used to broadcast the CRL, the cost of this approach would need to be examined as it would probably be prohibitive. Since not all vehicles are operating at the same time, the CRL would need to be re-broadcast more or less continuously. In addition, since the

broadcast is likely to be slow, provision would need to be made for the vehicle to receive different parts of the CRL at different times, and then to assemble the CRL as each component was received.

Models/Scenarios

In order to model the ways in which the three compunctions modes (WiFi, cellular, and DSRC) may be implemented to facilitate communications in the connected vehicle environment, three scenarios are developed and presented for more detailed analysis:

- Scenario 1 (Hybrid 1: "Short Term"): This scenario uses cellular for certificate management and V2I mobility communications and uses DSRC for V2V and V2I safety communications.
- Scenario 2 (Hybrid 2: "End State"): This scenario uses the wireless ecosystem (cellular, WiFi or DSRC) for certificate management depending on certificate management function and V2I mobility communications, and uses DSRC for V2V and V2I safety communications
- Scenario 3 (All DSRC): The all DSRC scenario relies on DSRC to provide the wireless data communications needed for the operational functions of the CDDS system

Salient features of these three scenarios summarized in the pages 16 and 17.

There is also an emerging scenario referred to as the vehicle-based option, which may require at least at initial stages of deployment less frequent communications and more "vehicle-only" reliance. The basic communication links would remain the same as the three possible scenarios above, although the frequency of the delivery of the CRL and decryption keys would be different. As more detail around this option emerges, we will further consider the communications needs for that type of system. This is not yet easily summarized as USDOT is currently developing the details.

SCENARIO 1: Hybrid "Short Term"

Certificate Management	**Cellular**
V2I Safety and Mobility Data	**Cellular**
V2V Safety Data	**DSRC**

- Will examine the hybrid approach of using cellular data delivery for Certificate Management and V2I communications, and the DSRC network for the V2V communications
- Will examine potential efficiencies and costs of using two different networks for data delivery, and its ability to deliver the benefits of the system

SCENARIO 2: Hybrid "End State"

Certificate Management	**Any and all opportunities; Cellular, WiFi, and DSRC**
V2I Safety and Mobility Data	**Cellular**
V2V Safety Data	**DSRC**

- Will rely on the wireless ecosystem: network carrier or WiFi as available to provide wireless data communications needed for each of the operational functions of the CDDS system
- Costs from the wireless carrier will likely be on a data usage basis, with a per-MB or per-GB cost
- Particular attention will be paid to the technologies in the wireless networks today, the impact on the device ecosystem, the cost per GB and the ability for ceullar technologies to fulfill requirements of safety and privacy

SCENARIO 3: All DSRC	
Certificate Management	**DSRC**
V2I Safety and Mobility Data	**DSRC**
V2V Safety Data	**DSRC**
• Will rely on DSRC to provide the wireless data communications needed for each of the operational functions of the CDDS system • Security benefits of having a "secure" system will be weighed against the costs of building a new 5.9GHz network.	

Implications/Opportunities

The communication links described in the scenarios highlight a need for third party involvement in communications delivery. Some of the communications may come from current networks and others from prospective networks. Moreover, commercial opportunities may be existent or may lie in prospects of a communication data delivery system to the scale envisioned. Certainly, third party involvement will include wireless carriers, but there may be others who contribute to and derive benefit from the overall system.

It is important to understand the role of USDOT in this context: the Department provides technical assistance, creates standards, develops guidance, and promulgates policies to influence the adoption of innovations which affect our transportation system, and in this role USDOT is an important stakeholder but not an owner or operator of a CME system or its communication components.

Hence, it is imperative that stakeholders – parties who can derive operational and in some cases business or commercial benefit – and their motivations are understood and considered, along with their manifold operational and other interests. Total costs and commercial benefits of providing the communications capability or capacity to underpin a CME are important to capture, from perspectives that include state and local (roadway) agency needs, wireless carriers and other parties to whom communicating to travelers is important.

Commercial/Financial Considerations

This upcoming commercial review therefore considers multiple components, including costs of the system needs for various technical options, and potential revenue and funding sources. Additional considerations include benefits analysis, network analysis, network modeling issues, network

deployment challenges, adding services or applications, and excess capacity implications. Network limitations largely concern the infrastructure required to support the systems. The latter considerations have significant business implications. Next steps for the commercial and financial analyses begin with considering inputs and expertise from this stakeholder community, and will then include actual cost estimates at different levels of deployment as well as modeling of alternative sources of revenue from the private-industry perspective.

Preliminary Conclusion

In conclusion, delivery of communications data delivery systems involves a number of tradeoffs, limitations, and risks that impact technology options. Key functions for which each of these communication technology options are to be applied are listed below (with calculated size in bytes provided parenthetically):

- Safety and mobility *to include delivery of the Basic Safety Message (BSM) and a calculated "maximum WAVE short message" or additional message* at 10 Hz, maximum (528 + 1500 byte)
- Certificate update request, ~ annually (533 byte)
- Certificate bundle, ~ annually (15,572,400 or more byte)
- Certificate decryption request, ~ monthly (362 byte)
- Certificate decryption reply, ~ monthly (378 byte)
- Misbehavior report, intermittent (854 byte)
- Certificate Revocation List (CRL) request, ~ daily (376 byte)
- CRL, ~ daily (variable)

Detailed estimates of sizes of data loads for different functions, as well as a range of wireless communications coverage areas and requirements, have all been considered to determine the best options for delivering on the needed communications throughout the system. The technologies are evaluated based on characteristics such as radio footprint, data rate, user demand, anonymity, and security.

The approximately annual certificate bundle delivery stands out, as it is almost 30,000 times larger than the BSM. Provision of this carries with it significant requirements; if done via low bandwidth and/or small footprint communication link, the bundle can only be provisioned within certain scenarios, e.g., a stationary or slow-moving vehicle.

Cellular technology can provide wide area and relatively high bandwidth communication capability. This technology is conceptually appropriate for the V2I applications and for the security management function. However, the connection duration for cellular is impacted by the number of other users competing for use of the channel. This is problematic in dense environments. Depending on demand, the delivery of a certificate update will take between 123 seconds and 17 hours. To avoid competition for data bandwidth, it may be necessary to implement off-hour certificate update protocols to use the cellular system at off-peak usage hours. The greatest weakness of cellular systems is that to access the cellular system the device must be registered with a cellular carrier. This typically requires some form of user agreement, contract and payment. Alternative models exist, but it is unclear how this may be adaptable in the context of a government-mandated system. It is, however, strictly a policy issue and not a technical one.

More detailed analysis of an all DSRC scenario as well as one that combines various technologies, such as WiFi, cellular and DSRC will explore in more the technical and financial considerations, including potential sources of revenue and investment. This is particularly important, since a host of stakeholders can derive operational and in some cases business or commercial benefit. The operating model, total costs, and commercial benefits of providing the communications capability or capacity to underpin the CMEs are important to capture, from perspectives that include state and local (roadway) agency needs, wireless carriers and other parties to whom communicate to travelers.

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487
www.its.dot.gov

FHWA-JPO-12-039

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