

Communications Data Delivery System Analysis

Task 2 Report: High-Level Options for Secure Communications Data Delivery Systems

June 21, 2012



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

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

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

Technical Report Documentation Page

1. Report No. FHWA-JPO-12-061		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle Communications Data Delivery System Analysis Task 2 Report: High-Level Options for Secure Communications Data Delivery Systems				5. Report Date May 16, 2012 - DRAFT	
				6. Performing Organization Code	
7. Author(s) James Misener, Scott Andrews, Peter Cannistra, Tori Adams, John Collins, Dominie Garcia, Andrea Waite, Richard Walsh, Blake Sheppard				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 Intelligent Transportation System Joint Program Office Research and Innovative Technology Administration 1200 New Jersey Ave SE, HOIT-1 Washington, DC 20590				13. Type of Report and Period Covered Formal Deliverable 1/8/2012 – 3/30/2012	
				14. Sponsoring Agency Code	
15. Supplementary Notes					
16. Abstract <p>This Communications Data Delivery System Analysis Task 2 report describes and analyzes options for Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications data delivery systems using various communication media (Dedicated Short Range Communications (DSRC), cellular, Wi-Fi, potential hybrid approaches and others), with security credentials management as a primary purpose. This task consisted of two subtasks. The first subtask was to gather and perform an initial level of analysis on the available communications options and methods to analyze deployment technology and business cases. Up to four options were to be considered during Task 2 – DSRC and cellular, and up to two more were to be selected by USDOT. The second subtask was to take the documented results of the Task 2 analysis, distribute to multiple groups of interested stakeholders for their review, and collect their feedback during a public workshop, for consideration and inclusion in a follow-up iteration of the report. This report is the result of both subtasks.</p>					
17. Key Words			18. Distribution Statement		
19. Security Classif. (of this report)		20. Security Classif. (of this page)		21. No. of Pages 90	22. Price

Form DOT F 1700.7 (8-72)

Reproduction of completed page authorized

Intelligent Transportation Systems Joint Program Office
U.S. Department of Transportation, Research and Innovative Technology Administration

Table of Contents

Executive Summary	1
Introduction	12
Chapter 1. Summary of Proposed Certificate Management Approach.	13
1.1 SUMMARY OF CERTIFICATE MANAGEMENT APPROACH	13
1.2 CERTIFICATE UPDATES.....	14
1.3 MISBEHAVIOR DETECTION AND REPORTING	16
Chapter 2. CDDS Technical Review	20
2.1 SUMMARY OF COMMUNICATIONS NEEDS.....	20
2.2 TECHNOLOGY OVERVIEW	27
2.2.1 Cellular/Long Term Evolution	27
2.2.2 WiFi	28
2.2.3 Dedicated Short Range Communications	29
2.2.4 Additional Technologies	30
2.2.5 Technology Summary	30
2.3 DATA COMMUNICATIONS ANALYSIS.....	32
2.3.1 V2V Communications	36
2.3.2 V2I Communications.....	38
2.3.3 Security Management Communications	39
2.4 TECHNOLOGY ANALYSES FINDINGS.....	39
2.4.1 Cellular Communications.....	40
2.4.2 WiFi Communications.....	43
2.4.3 DSRC Technology.....	45
Chapter 3. Commercial/Finance Review	48
3.1 COMMERCIAL ANALYSIS APPROACH.....	48
3.2 SCENARIO ANALYSIS	49
3.3 ANALYSIS OF OUTCOMES	57
3.4 NETWORK ANALYSIS	57
3.5 NETWORK MODELING ISSUES	58
3.6 NETWORK DEPLOYMENT CHALLENGES	59
3.7 REVENUE AND COST MITIGATION OPPORTUNITIES	60
3.8 ADDING SERVICES OR APPLICATIONS.....	61
3.9 ECONOMIC AND BUSINESS MODELS	63
Chapter 4. Summary and Next Steps	65
Appendix A. Data Transfer Dynamics	68
DATA TRANSFER DYNAMICS	68
Stationary Updates.....	68
On-The-Fly Updates.....	69
TECHNICAL REQUIREMENTS SUMMARY	72
Appendix B. State Vehicle Inspection Requirements	75
Glossary of Terms	78
Acronyms and Abbreviations	81
Bibliography	83

List of Tables

Table 1: Wireless Technology Summary 4

Table 2: Key Takeaways from Stakeholders Related to CDDS 9

Table 3: Misbehavior Reports and CRL Entries vs. Penetration Level (per day) 18

Table 4: General Technical Characteristics for Mobile Communications 21

Table 5: Communications Needs by Application Category 23

Table 6: Wireless Technology Summary 31

Table 7: Basic Signed Message Sizes..... 33

Table 8: Vehicles in Footprint Based on Different Road Situations..... 37

Table 9: V2V Data Transfer Load (Kbit/Sec) in Footprint Based on Different Road Situations..... 37

Table 10: V2I Data Transfer Load (Kbit/Sec) in Footprint Based on Different Road Situations (1500 Byte messages)..... 38

Table 11: Cellular Strengths and Weaknesses for Connected Vehicle Applications..... 40

Table 12: Cellular System Performance for Security Updates..... 42

Table 13: WiFi Strengths and Weaknesses for Connected Vehicle Applications..... 43

Table 14: WiFi Performance for Security Updates 45

Table 15: DSRC Strengths and Weaknesses for Connected Vehicle Applications..... 46

Table 16: Possible CDDS Scenarios 52

Table 17: Commercial Issues..... 58

Table 18: Areas Allowing Reasonable Assumptions 59

Table 19: USDOT DMA and NCHRP 3-101 Applications..... 62

Table 20: Key Takeaways from Stakeholders Related to CDDS 66

Table 21: On-The-Fly Update Demand vs. Population 69

Table 22: Number of Vehicles in Footprint vs Speed 70

Table 23: Probability of More than One Vehicle Updating vs Speed and Footprint Size 70

Table 24: Technical Requirements..... 72

Table 25: State Vehicle Inspection Requirements..... 75

List of Figures

Figure 1: Connected Vehicle Messaging Data Volumes 3

Figure 2: Cost Analysis Process 6

Figure 3: Certificate Update Flow 15

Figure 4: Certificate Revocation Flow..... 17

Figure 5: Lower Bound Misbehavior Report Volume vs. Penetration 19

Figure 6: Typical Cellular System Arrangement 27

Figure 7: Mobile Data Projection 28

Figure 8: WiFi Hot Spot Distribution 29

Figure 9: Connected Vehicle Messaging Data Volumes 35

Figure 10: Cost/Benefit Analysis..... 48
Figure 11: Rate of Adoption Model 54
Figure 12: Cost Elements Definitions 55
Figure 13: Cost Elements 56
Figure 14: Costs/Requirements and Technical Options..... 57
Figure 15: Encounter Time vs. Vehicle Speed and RF Footprint Diameter.. 71

Executive Summary

This report is the Communications Data Delivery System (CDDS) Analysis project Task 2 deliverable documenting High-Level Options for Secure Communications Data Delivery Systems aimed at providing the communication links to enable the necessary, trusted communications functions of the Connected Vehicle system, described below.

Task 2 of the CDDS project consisted of two subtasks. The first subtask was to gather and perform an initial analysis on the available options for delivering secure communications within the Connected Vehicle Environment and to begin the analysis of possible business cases for deploying the communications options. Up to four options were considered during Task 2 – including Dedicated Short Range Communication (DSRC) and cellular, and two more selected by U.S. Department of Transportation (USDOT). The second subtask was to take the documented results of the first analysis, distribute to multiple groups of interested stakeholders for their review, and collect their feedback during a public workshop for consideration and inclusion in a follow-up iteration of the report. This report is the result of both subtasks.

The Connected Vehicle concept depends on participants that operate in a system of trusted communication to exchange safety, mobility and environmental data. In particular, the concept relies on a Public Key Infrastructure (PKI) system to provide assurance to all participants that messages are legitimate. PKI is a security system that ensures authentication and validity of participants and their messages and uses encrypted and signed certificates as that validation check. The messages and the underlying certificates that ensure this level of trust within a PKI must be exchanged across data communications systems or networks. Identifying and analyzing the needs and options associated with this communication system and the business proposition to set up such a system are the primary subjects of this project.

This report presents analyses and research conducted to date on the exploration of various networks and systems that can be implemented for communications related to the Connected Vehicle System as it is deployed. Included is a thorough discussion of the technical implications of several network options, with multiple levels of analyses that highlight the potential needs of the CDDS under various operating scenarios. While working in close coordination with the development of organizational and operational models for Certificate Management Entities (CMEs), those organizations that operate the back-end PKI system that ensures trust throughout the communications and exchanges of messages, the team examining CDDS options has identified a comprehensive list of considerations to account for in choosing and implementing a network.

To attain a basic understanding of the communication needs, the currently envisioned certificate management approach anticipated for the CME project is summarized here. The communications requirements of the CMEs are a primary driver of the CDDS requirements.

For the Public Key Infrastructure (PKI) under consideration for certificate management in the Connected Vehicle Environment, the functions identified include:

- Registration Authority (RA), which maintains a trusted relationship with the vehicles. All vehicle communications related to certificate management is carried out between the vehicle and the RA

- Certificate Authority (CA), which generates and manages the certificates, based on assurances from the RA
- Misbehavior Detection and Management (MDM), which, based on reports of observed misbehavior determines when a terminal is malfunctioning or otherwise behaving improperly
- Linkage Authority (LA), which is able to generate a (linkage) value that can be used to determine that certificates provided with other (future) messages are associated with a misbehaving unit and should be ignored

A detailed process flow for certificate management is described in Chapter 1 of this report.

Of direct applicability to understanding the options available to provide the CDDS for CMEs are several implications of the current design and working assumptions:

- Sizes of the certificate bundle that will be downloaded to the On Board Equipment (OBE)
 - The current working assumption is that OBE will receive annual bundles of certificates (105,120 certificates)
- The volume of misbehavior reports from OBEs
- The size and distribution approach for the Certificate Revocation List (CRL)
 - The size of the CRL depends on the lifetime of the certificates and how frequently they are updated, and the expected rate of misbehavior. It is important to note that a 1% rate of malfunction and misbehavior at full deployment will comprise 2.5 million units, so even at low rates of revocation, the CRL may be quite large
 - The distribution of the CRL determines how much data must be communicated. If the CRL is updated in its entirety, then the volume of data may be large. If the CRL is updated incrementally, then the CRL updates are presumably much smaller

Misbehavior reporting and detection, and the processes associated with the CRL, are still very much under development. As a result, there are still many questions to be answered about the specifics of which organization and function may be responsible for which of the sub functions and activities associated with managing misbehavior and distributing the CRL. For the purposes of the CDDS options and approaches, the team specifies assumptions used to detail the needs of the communications networks without delving into the split between organizations, functions, higher level processes, or other nuances of the CMEs.

The core communications that will need to be covered by a choice of CDDS include all communications between OBE and CMEs:

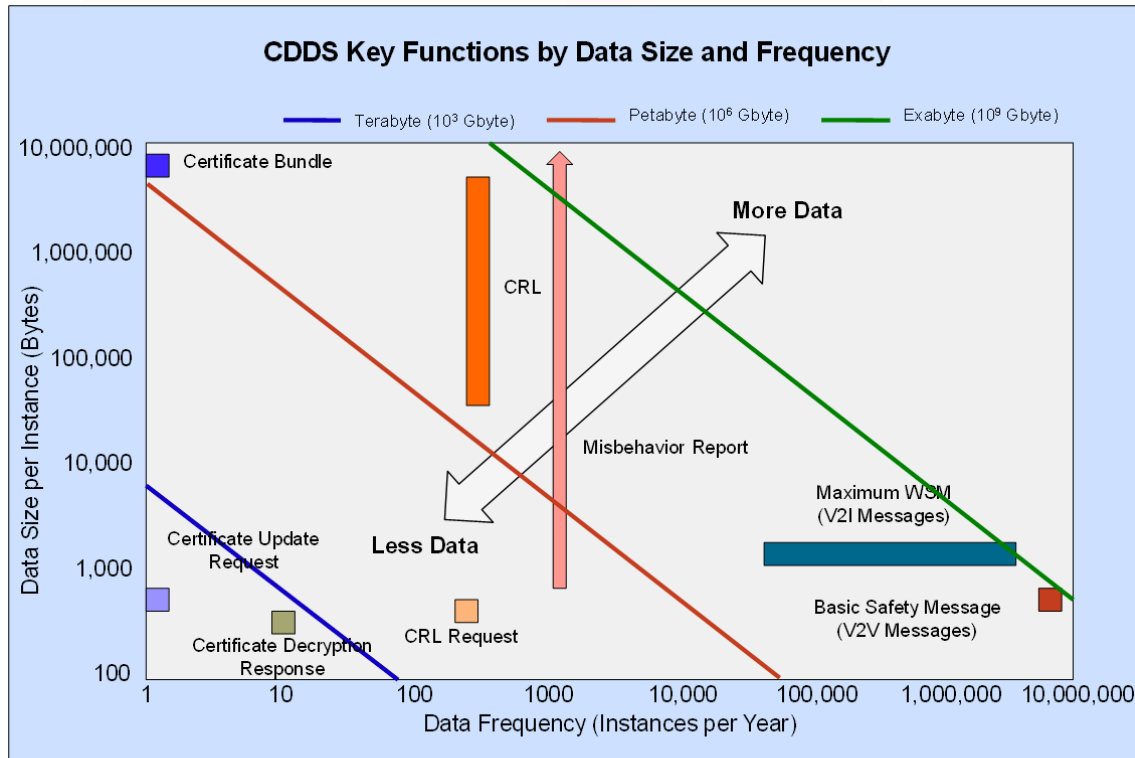
- Requests for and distribution of annual certificates
- Requests for and distribution of monthly decryption keys
- Misbehavior reports from OBE to CMEs
- CRLs from CMEs to OBE

In addition, in the interest of efficiency, the CDDS should also support other forms of connected vehicle communications, with focus on communication from Roadside Equipment (RSE) and other devices with the OBE, in what is referred to as the “edge” of the over-the-air network. Communications between the CME and the RSE or other devices is often referred to as the “backhaul” and while not inconsequential to operating a security system the technical and business considerations, are relatively straightforward relative to the focus of this project’s research, which focuses on the over-the-air portions. Additional communications needs may evolve to include various

non-safety applications, many of which are discussed in this report. It may be that build out and operations of the communications network to provide exchange of certificates and thus safety messages may benefit also from investment in the (same) communications system that will support additional, optional applications, due to revenue and commercial opportunities for the latter.

The overall volume of data that the CDDS must support depends on the size of the messages and the how often they are sent. A detailed analysis of the message types, sizes and frequencies is provided in Chapter 2 (Section 2.3). Figure 1 below summarizes the overall data volumes represented by various types of connected vehicle messages. As can be appreciated from the figure, the annual certificate bundle represents a delivery challenge simply because it is rather large (20-30 Mbytes), although since it is only sent annually, the overall aggregate data volume is relatively small. In contrast, the CRL payload is smaller, but the current model is that it is sent approximately daily, so on an annual basis it represents nearly 1000 times as much aggregate data as provisioning certificate bundles. The annual payload from other certificate management-related messages is also shown. These generally represent substantially lower overall data volumes, although the misbehavior reports could rival the annual certificate bundle if the rate of misbehavior is high.

Figure 1: Connected Vehicle Messaging Data Volumes



Assumptions: 250 M vehicles and 50% Adoption; BSM and Max WAVE short message operate only while vehicles are operating and communicating, ~54 minutes per day

While the CDDS is not the network upon which V2V messages are exchanged, the Basic Safety Message (BSM) is also indicated on Figure 1 above for reference. The Maximum WAVE Short Message (WSM) represents typical V2I messaging. This is the maximum size WSM that can be sent. The overall volume of this type of message depends heavily on the number of alert or warning sites (i.e., the density of on-road events or conditions that must be communicated). In the worst case such as an urban grid, this density could be as high as every 100 meters.

From a CDDS perspective, the annual certificate bundle, the CRL delivery, and V2I messaging represent significantly different communications challenges. The certificate bundle requires substantial system bandwidth in order to quickly transfer certificates, but this bandwidth is only needed once per year for each car (i.e., for a few seconds or minutes each year). This means that the certificate update could conceivably be supported with a low bandwidth system while the vehicle is stationary (e.g., at a fueling/charging station, or at the user's home, parking lot, etc.). Encountering such a stationary access point once per year does not seem unreasonable, allowing use of WiFi for example. On the other hand, if the certificate update is conducted with the vehicle in motion the CDDS must be connected long enough to allow the transfer of this large volume of data. This may be difficult for small radio footprint systems like DSRC and WiFi, since the vehicle may pass through the coverage zone before the data transfer is complete.

In contrast, the delivery of CRLs is currently envisioned to be performed approximately daily. This means that the vehicle must encounter an access point once per day, and it must be in range of that access point long enough to transfer the CRL. If the CRL is large, this may be problematic. V2I messaging represents a similar challenge to the CRL, except that the dynamics are more extreme. The per message data volume for V2I is very low, but, in order to assure that important V2I messages are received, the vehicle must encounter access points with high regularity. If the vehicle is not in operation (i.e., it is parked in a garage for days or months) it will not receive any updates.

In short, the certificate update requires access to high bandwidth for relatively long intervals (tens of seconds to minutes) but only once per year. The CRL requires access to high bandwidth for somewhat shorter intervals (e.g., 1-30 seconds), but on at least a daily basis. V2I messaging requires access to relatively low bandwidth for very short intervals (milliseconds), but with sufficient frequency or geographic density that the car always has up to date roadway condition and hazard information as it moves.

As part of the Task 2 effort wireless technologies to accommodate the data loads were subsequently analyzed, with results summarized in Table 1.

Table 1: Wireless Technology Summary

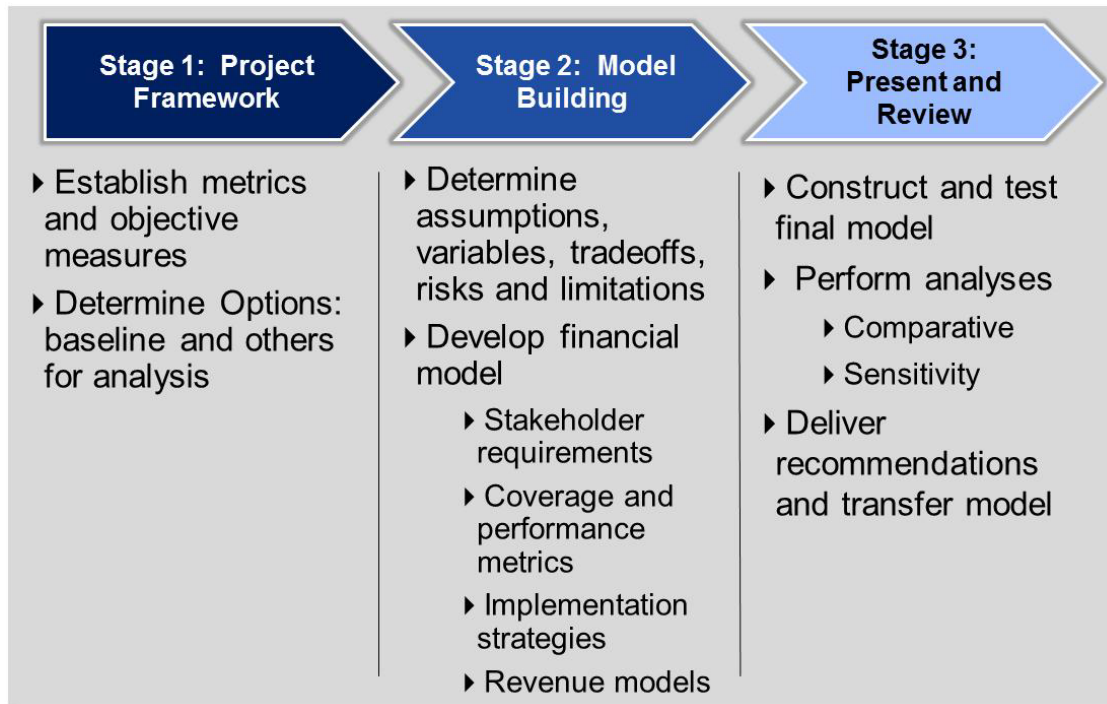
Technology	Advantages	Disadvantages	Comment
Cellular	<ul style="list-style-type: none"> Nationwide coverage Universal equipment available 	<ul style="list-style-type: none"> Partnerships required with wireless carriers V2I Broadcast is problematic since system is point to point. Vehicles must join the network and request data for their location); inefficient and not anonymous 	<ul style="list-style-type: none"> Key element in analysis
WiFi	<ul style="list-style-type: none"> Universal standard Many hotspots available High Bandwidth 	<ul style="list-style-type: none"> Small coverage footprint of hotspots requires vehicles to be nearly stationary for most transactions Disparate control and 	<ul style="list-style-type: none"> Considered with limited use while in stationary mode (for example in provisioning)

Technology	Advantages	Disadvantages	Comment
		<p>ownership of hotspots</p> <ul style="list-style-type: none"> • V2I Broadcast is problematic since system is point to point. Vehicles must join the network and request data for their location; inefficient, but could be anonymous • Joining the network takes longer than moving vehicle is in hot spot (3-5 seconds in hot spot vs. 10 seconds to join) 	<p>annual certificate bundle) in final scenario analysis</p>
DSRC	<ul style="list-style-type: none"> • WiFi-like standardization • Broadcast capability; does not require IP addressing • Nearly instantaneous network attach time • High bandwidth 	<ul style="list-style-type: none"> • Not deployed • Small RF footprint limits size of data exchanges at higher speeds • Potential for channel congestion from high density V2V messaging 	<ul style="list-style-type: none"> • Key element in analysis
WiMAX	<ul style="list-style-type: none"> • High bandwidth • Low cost from wireless carriers 	<ul style="list-style-type: none"> • No nationwide deployment • LTE technology selection by most carriers • Broadcast is problematic • V2I Broadcast is problematic since system is point to point (i.e., addressed). Vehicles must join the network and request data for their location; inefficient, but could be anonymous 	<ul style="list-style-type: none"> • Not considered in this analysis • Provides no substantial benefit over cellular, and has lower level of deployment
Satellite Radio (SDARS)	<ul style="list-style-type: none"> • Nationwide coverage • Equipment is widely available 	<ul style="list-style-type: none"> • Broadcast only • Huge footprint may result in high latency since there may be millions of location specific V2I 	<ul style="list-style-type: none"> • One-way communications possible, e.g., CRL distribution. As the volume of data grows so

Technology	Advantages	Disadvantages	Comment
		messages (a takes time to send all messages and start from the beginning) <ul style="list-style-type: none"> • Current system has about 30-60 seconds of built-in latency 	does latency (up to several hours delay). <ul style="list-style-type: none"> • Latency may make this communication means impractical
Hybrid Digital (HD) Radio	<ul style="list-style-type: none"> • Widespread urban coverage • Widely available in automotive equipment 	<ul style="list-style-type: none"> • Broadcast only • Large footprint and resulting low bandwidth may result in high latency 	<ul style="list-style-type: none"> • Not considered in this analysis

In parallel to identifying the various technical needs, standards, estimates, and scenarios, we have begun the process of developing robust cost analytic models. The overall plan of the cost analysis effort has been designed as a three-step approach, with the tools and prime output being a commercial analysis based upon comparing a baseline or status quo system, calculating the incremental requirements of deploying a CDDS, and then outlining and comparing the network options on cost and effectiveness in fulfilling the requirements. The approach to this analysis is shown in Figure 2 below.

Figure 2: Cost Analysis Process



The approach to analyzing costs is applied to the following scenarios:

Scenario One (Hybrid One)

- Certificate Management—Cellular
- V2I Safety and Mobility Data—Cellular
- V2V Safety Data—DSRC

This scenario uses cellular for certificate management and V2I mobility communications and uses DSRC for V2I and V2V safety communications. Fulfillment of requirements to the system will depend on the costs of using two different networks for data delivery.

Scenario Two (Hybrid Two)

- Certificate Management—Cellular, WiFi, DSRC
- V2I Mobility Data—Cellular, DSRC
- V2V Safety Data—DSRC

This scenario uses the “wireless ecosystem” (cellular, WiFi, or DSRC) for certificate management depending on certificate management function and V2I mobility communications. The scenario uses cellular or DSRC for V2I mobility communications, DSRC for V2I mobility communications, and DSRC for V2V safety communications. Wireless carrier costs will likely be on a data usage basis and particular attention will be paid to the technologies in the wireless networks today.

Scenario Three (All DSRC)

- Certificate Management—DSRC
- V2I Safety and Mobility Data—DSRC
- V2V Safety Data—DSRC

This scenario will rely on DSRC to provide the wireless data communications needed for each of the operational functions of the CDDS. The security benefits of having a “secure”, all DSRC systems will be weighed against the costs of building a new 5.9GHz network.

Scenario Four (Phased Deployment) - *Under Development*

This emerging scenario, referred to as the Phased Deployment option, describes at least as an initial deployment with more reliance on stored certificates within the vehicle and less frequent communications with other entities, including CMEs and RSE. The basic communication links would remain the same as the above three scenarios, although the frequency of the delivery of the CRL and decryption keys would be different. As more detail emerges, the communication needs will be more accurately determined.

The four scenarios were selected from a variety of possible options. A key driver for local area communications is the state of the vehicle (in motion or stationary). This is because a vehicle in motion may pass through and out of the relatively small communication zone before the data transaction is completed. Another key is the nature of the information being communicated. Specifically, information that is valid or used over a large geographic area, such as what is contained on the CRL, may need to be accessed anywhere over that area. Information that pertains only to a single place is most relevant when delivered at or near that place. Using a wide area communications system for locally relevant data generally means that the system must send data for all possible local points of concern (hazards, road areas, etc.) to any vehicle in the larger area. Alternatively the vehicle can contact the system and request information for the local area they are in, but this means the vehicle must continually contact the system and ask if there is new data for the local area they have just entered.

Wireless carriers continually look for new revenue sources to exploit the wireless networks. This is where some of the costs and challenges may be offset by the potential for additional revenue. Hence, there are revenue and cost mitigation opportunities, where commercial organizations such as wireless carriers could potentially provide some network access for little or no cost in exchange for opt-in access to the large numbers (up to 250 million) of users in order to provide additional, optional commercial services.

Below are three major areas where value to third parties (such as wireless carriers) may be present:

1. Making location data available to third parties in a way that protects consumers appropriately from unwanted privacy risks.
2. Monetizing any excess capacity that is delivered in the wireless network. There are examples of value to third parties of safely delivering content to new customers in connected automobiles
3. There are specialized services beyond the V2V “safety of life” services that could be delivered to vehicles that the users could potentially find valuable

Critical parts of these models will include the network, user and additional requirements that would arise from full deployment of the connected vehicle system. It is important to realize the difficulty of separating the costs of a “certificate only” use of the communications system and a mixed use approach where the certificate management use would be realized as a requirement, and the non-certificate use (i.e. additional optional applications) could be provided on some other semi-commercial basis. Any excess wireless capacity, in addition to that used during the delivery of certificate management, might be viewed as a business opportunity for the public and private sectors alike. This is the view in constructing an analysis of the entire set of costs associated with the wireless delivery of certificate management, to include V2V and V2I networks. Outcomes facilitated from the entire system (crash reduction, traffic reduction and emissions reduction) are examined.

Key Findings

The scenarios presented resulted from the analysis of a number of wireless technologies available for the three communications methods, all involving a number of implications, limitations, and risks that impact technology options. Based on the outcomes of the technical considerations of this report, cellular and DSRC are both viable for certain aspects of connected vehicle applications. Based on analyses to date, other technologies appear to be too limited to continue considering. Detailed size estimates of data loads for different functions are essential to this analysis and are included throughout the report.

The major advantage of cellular technology is the wide area, relatively high bandwidth communications capability. These capabilities make the technology most appropriate for both V2I applications and CME functions, although the technology appears to be lacking for V2V applications. V2V requires a peer-to-peer communications capability, which would be a challenge at higher levels of deployment. Additional cellular weaknesses include the requirement that the device be registered with a cellular carrier, which usually requires a user agreement, contract, and payment, which may conflict with USDOT principles and requirements. Alternative models exist, but adaptability will need to be further studied.

DSRC is well suited to V2V and most V2I applications, though it is not as appropriate for security management if the data volumes are large and infrequent. DSRC has equivalent performance to cellular for security management if updates are performed at least monthly and CRLs are updated incrementally.

In general, none of the options using a single communications system are suitable since the nature of the communications varies widely, based on data load sizes and how often messages are exchanged, as described above. Similarly, options that do not limit the choices are problematic since one has no knowledge of which communications system may be used. If vehicles are free to choose any of the three communications technologies (setting aside the fact that some are not appropriate for some types of data), then the infrastructure must support all three types in order to serve all of the vehicles. Neither of these approaches is economically viable.

It is also important to determine the required baseline, since it is always possible for a user or a carmaker to establish additional services. For example Hybrid 2 differs from Hybrid 1 only in that the car can optionally use WiFi instead of cellular in some stationary settings. So, under Hybrid 2, cellular and DSRC would be required, but one could add WiFi if it were desired. Hybrid 2 provides an additional link that the user may choose to use, but it does not allow a choice between the implementation of one link over another. The vehicle is still required to have a cellular or some other connection for the initial wireless connection. Similarly, Scenario 3 assumes sufficient DSRC coverage to support all transactions, but the user can also choose to use cellular for some of these. However they still need to have the ability to use DSRC in order to establish the initial wireless connection.

Examination of costs reveals not only the network and infrastructure costs associated with expansion or implementation of any large-scale network, but also additional costs to users, government, and other organizations that may be involved in network operations. Ways to fund and provide revenue opportunities to cover these costs and thus realize requirements are also under examination.

Stakeholder Feedback

On April 19th and 20th, 2012, USDOT hosted a public workshop in Washington, DC to collect feedback from key stakeholders and gain insights to support this CDDS effort and the related CME project. Table 2 below highlights some of the topic areas that concerned stakeholders and lists key takeaways from their comments and inputs.

Table 2: Key Takeaways from Stakeholders Related to CDDS

Topic Area	Key Takeaways from Stakeholders
Technical Specifications	<ul style="list-style-type: none"> ▶ The level of bandwidth available for non-safety applications when the system reaches full deployment will shape the competitive landscape for potential applications providers ▶ There is a need for risk identification and mitigation during the planning process, and for precautions such as system redundancy ▶ Many technical specifications are still outstanding, some of which include: certificate revocation policies, distribution of architecture for communications system, and certificate life span decisions (see discussion below)
Privacy	<ul style="list-style-type: none"> ▶ Privacy for users can be assured in different ways and at different levels, but regardless it is critical that the system adheres to such policy guidelines as Fair Information Practice Principles (FIPPS)

Topic Area	Key Takeaways from Stakeholders
Implementation	<ul style="list-style-type: none"> ▶ Industry estimates for implementation of the system range from 15 to 20 years; one estimate is 20 years to reach 95% of automobiles ▶ It has not yet been determined whether a vehicle-only system or a system that includes V2I communication will be deployed initially ▶ The specific details of the roll-out process will likely be determined in large part by the owner(s) of the system
Ownership Structure	<ul style="list-style-type: none"> ▶ A strong emphasis was placed on the concept of a public-private partnership ▶ Subgroups of stakeholders felt that the government should take a lead in the stand-up of the system initially, and also that the details of any public-private partnership that develops should be transparent to all parties involved
Future Policy Decisions	<ul style="list-style-type: none"> ▶ NHTSA must ensure privacy for users and outline an economic benefit for any mandates issued to the public ▶ A decision on the potential next steps for implementation of the Connected Vehicle Program will be made by NHTSA in 2013 at the earliest.

Two important points related to policy brought forward by stakeholders are issues of privacy and certificate life times. These issues will be further explored during Task 3, but they are briefly discussed here.

With regard to privacy, PII and location or trip traceability are the key policy concerns. The certificates used for BSM authentication do not contain any PII (i.e. information linking them to an individual user or vehicle through a requesting certificate signing request (CSR)). PII is restricted to a back-end system for registering users behind two separate layers of certificates, making it close to a non-issue. Location or trip traceability concerns relate to vehicle positioning based on BSMs sent by OBE. Therefore, policy research in Task 3 will concern the extent to which location traceability is a reasonable concern, based on public acceptability and technological feasibility, especially as it affects investment decisions to deploy the envisioned Connected Vehicle and security environment.

The second takeaway relates to certificate life times. The certificate life time is one of the cost drivers of the connected vehicle system, with shorter life spans requiring more certificates. The tradeoff means easier location traceability for a longer life span. More difficult location traceability is the implication for a shorter certificate life span. This comes at a higher cost of certificate issuance infrastructure. CRL size is an additional concern with short certificate life spans, although it is mitigated by the use of the LA. Longer certificate life times could eliminate the need for this additional infrastructure component. Where an LA type construct is not used, longer certificate life would cause larger CRLs. It is also important to understand that revoking certificates from a single vehicle will require greater CRL bandwidth when shorter life span certificates are used. Certificate life time will be viewed as a major policy implication, especially with regards to the tradeoffs.

We summarize the next steps, to be conducted in Task 3:

- Examine the four scenarios going forward and determine exact technical description for each scenario in order to provide input to cost model
- Complete Cost Analysis. This will be the “baseline” case, by which the other scenario outcomes/advantages and costs will be judged

- Determine detailed objective measures and assumptions consistent with CDDS technical and policy issues, with particular focus on PII and traceability as well as certificate life time issues.
- Fully investigate potential revenue models in all scenarios
- Complete a report on the tradeoffs and compromises in each scenario, from technical and commercial analysis points of view

The work conducted in this task enables those next steps as it has defined technical options for delivery of certificate management, provides consideration of the value of this wireless network, not only for certificate management but also for other Connected Vehicle Environment functions. It also resulted in down selection of four scenarios for consideration going forward. The work conducted in this task included input from a public workshop, which has given us additional input to consider policy implications of PII and traceability, and the impact certificate lifetimes on technical and business solutions for CDDS. As the project progresses, these will be incorporated into the business analysis on establishing and maintaining a CDDS to enable a secure and trusted Connected Vehicle Environment.

Introduction

This report documents an initial set of technical and finance requirements for a CDDS to deliver a secure and private PKI system for the Connected Vehicle Environment, based upon the emerging organizational structures concurrently under consideration by the companion project to develop alternative CME organizational and operational models. While there are potentially other uses of the CDDS in a Connected Vehicle Environment, the focus of the CDDS analyses presented here is the technical means and business models to deliver communication from the roadside or back office to vehicles. The mobile and large-scale consumer (or traveler) component of the entire trust network is a difficult and important communication issue for reasons of potential scale, complexity, and mobility.

At this point, promising options are presented, along with high-level technical and financial analyses of those options. While various wireless connectivity links are considered and presented, for reasons of viability described in this report, there is deeper focus on DSRC and cellular approaches. The high-level analysis of DSRC and cellular-based options reported here will support the process defined in subsequent Subtasks 3.A and 3.B: “Development and Evaluation of Promising Options”.

Therefore in this report, we review and present research, analyses and integration of both technical and commercial/economic considerations. The report is organized according to these chapters:

Chapter 1: Summary of Proposed Certificate Management Approach

Chapter 2: CDDS Technical Review

Chapter 3: Commercial/Finance Review

Chapter 4: Summary and Next Steps

Chapter 1. Summary of Proposed Certificate Management Approach

1.1 Summary of Certificate Management Approach

As noted in the Introduction, a parallel project is tasked with developing alternative approaches of organizational and operational models of the CME that will manage, oversee, and perform all “back-office” functions related to the authentication, creation, batching, and distribution of the certificates that are part of the PKI. The currently envisioned certificate management approach anticipated for the CME project is summarized here because it is important to understand the foundation of the system that will need to be supported by the networks described in this document.

For the PKI under consideration for certificate management functions in connected vehicle environments, the functions identified include RA, CA, and MDM. The LA is an additional function that has been identified as necessary for full nationwide deployment of CMEs for the Connected Vehicle Environment. A detailed process flow is described below, and then included below in Figure 3.

Of direct applicability to understanding the options available to provide the CDDS for CMEs are several implications of the current design and working assumptions:

- Sizes of data packets that are made up of the certificates that will be downloaded to the OBE. The current working assumption is that OBE will receive annual batches of certificates (105,120) with monthly decryption keys being sent. This implies that CDDS options need to account for:
 - Annual batches of certificates – requests from OBE and distribution of certificates from CMEs
 - Requests from OBE to CMEs for monthly decryption keys
 - Distribution of monthly decryption keys to OBE from CMEs
- Misbehavior process and distribution of the CRL. This process is still very much under development. Of most significance to the CDDS options is the anticipated size of the CRL and how it will be distributed

There are still many questions to be answered about the specifics of which organization and function may be responsible for which of the sub functions and activities associated with authorizing users, creating and distributing certificates, creating and distributing keys, and managing misbehavior and distributing the CRL. For the purposes of the CDDS options and approaches we specify assumptions used to detail the needs of the communications networks without delving into the split between organizations, functions, higher level processes, or other nuances of the CMEs.

1.2 Certificate Updates

The current proposed approach, as noted above, is that certificates will be updated and sent to an OBE once per year in batches of 105,120, with monthly sub-batches being encrypted together so they can be “opened” with a decryption key provided to the OBE from one of the CMEs. The OBE has an identified and trusted relationship with the necessary CME in order to communicate and send requests, as well as receive updates, certificates, and decryption keys. Requests for certificates are communicated wirelessly from the OBE to one of the CMEs (RA), and include specific values that are generated by the OBE, after which the RA verifies the identity and legitimacy of the OBE. Another CME (CA) then generates certificates, and encrypts them so that the RA cannot examine them. These are sent to the RA which then further encrypts the keys in batches, and communicates the batches to the requesting OBE. The requesting OBE then periodically and again via wireless communication requests decryption keys from the RA to unlock a batch of keys, and once unlocked, uses its internal private keys to decrypt the certificates for usage.

The current certificate management design describes providing the vehicles with one full year of certificates, and updating this set of certificates once per year. With a five minute lifetime, and a 30 second time overlap, each vehicle will thus obtain 105,120 certificates at activation, and each year it will engage in a transaction to acquire the same number of new certificates. The expected certificate size is about 132 bytes, so the total set of certificates will sum to about 13.9 Mbytes in size. This volume of data, combined with the fact that most network access points are likely to be used by more than one vehicle at a time means that the access times, while infrequent, will be somewhat long. This is problematic for moving vehicles in smaller radio frequency (RF) footprints. This is discussed below.

For access to certificates, the vehicle must also obtain an access key each month. The volume of this transaction is very small in comparison to the certificate update process, but the need to access the network to conduct the transaction demands that the vehicle connect to the network at least monthly.

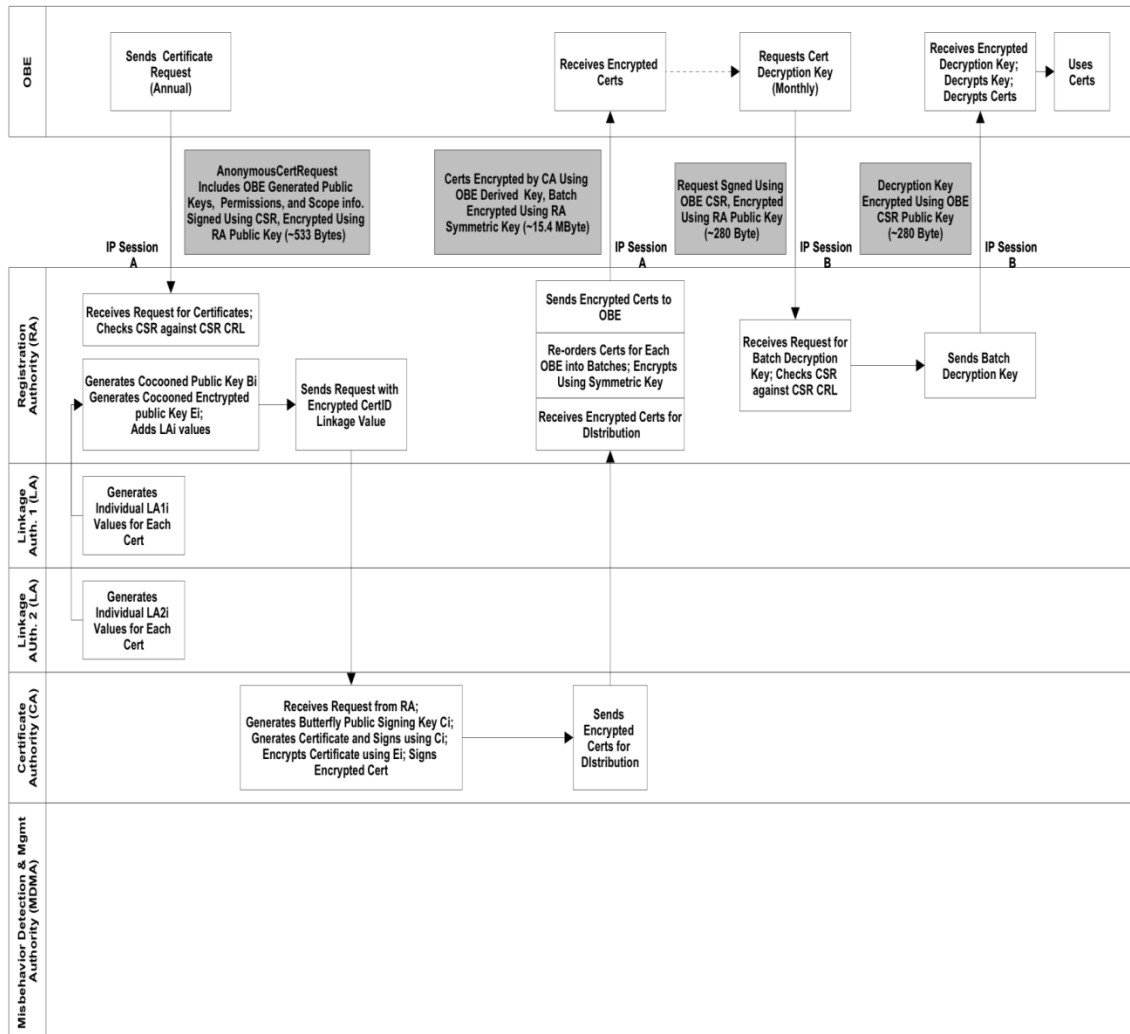
Since there is no way to predict exactly where any given vehicle will drive, it is difficult to specify requirements for annual connectivity. Clearly a ubiquitous system such as cellular would allow any vehicle to connect at the time of its annual update. Smaller footprint connection points, however, will need to be located in areas that vehicles have a high probability of traveling through at least once per year. This approach can be separated into two basic classes:

- Stationary access points would be located at places where vehicles are likely to visit at least monthly, and where those vehicles may stop and remain stopped for some period of time. Access at these locations is straightforward since the vehicle has sufficient time to connect and execute the transaction. The connection can be dedicated to this task, so competition for bandwidth can be easily managed (see Appendix A)
- On-The-Fly access points would be placed in locations that any given vehicle is likely to pass on a regular basis. In this situation the access is complex since the vehicle must connect to the network, and execute the transaction while moving. Because the vehicle is moving, the time available for the transaction is limited. Because the access point is placed in a location where many vehicles are likely to pass regularly, the system will also need to serve multiple vehicles at the same time (especially at high levels of deployment). Because the dynamics are different, these two approaches to small footprint access points result in substantially different communications requirements

The current development of operational and organizational approaches for the CME include several layers of security and privacy protection to ensure a trusted relationship, the cornerstone of an effective CME system. Since the information from and about the OBE is not passed to the CA, the CA has no information about which OBE is being certified. Since the CA encrypts the certificates and keys it generates, the RA does not know which certificates were provided to any specific OBE. In this way the OBE identity is shielded from the CA, and the certificates are shielded from the RA.

The basic certificate updating process flow is illustrated together with the over the air data elements highlighted in grey in Figure 3 below.

Figure 3: Certificate Update Flow



1.3 Misbehavior Detection and Reporting

There must be a process and responsible CMEs for detecting misbehavior – either as generated by malfunctioning equipment or by human malfeasance. This area has yet to be developed in detail, though there have been certain assumptions made that affect the network and options presented for CDDS. Key assumptions include:

- The OBEs will be programmed to run plausibility checks of incoming messages. In addition, when “bad” messages are not caught by OBE plausibility checks, there must be a mechanism for identifying them. Although at a very nascent stage of development, the current vision for this process is that reports would be sent from OBE to CMEs in order to help identify misbehaving devices. For the purposes of the CDDS project, the important point to note is that there will need to be communications between OBE and CMEs to send misbehavior reports
- There is also a working assumption that the CMEs will create CRLs, which would be updated frequently (perhaps daily) and then sent to the OBE. This is another communications that the CDDS will have to facilitate. Assumptions about sizes of the CRL are detailed below

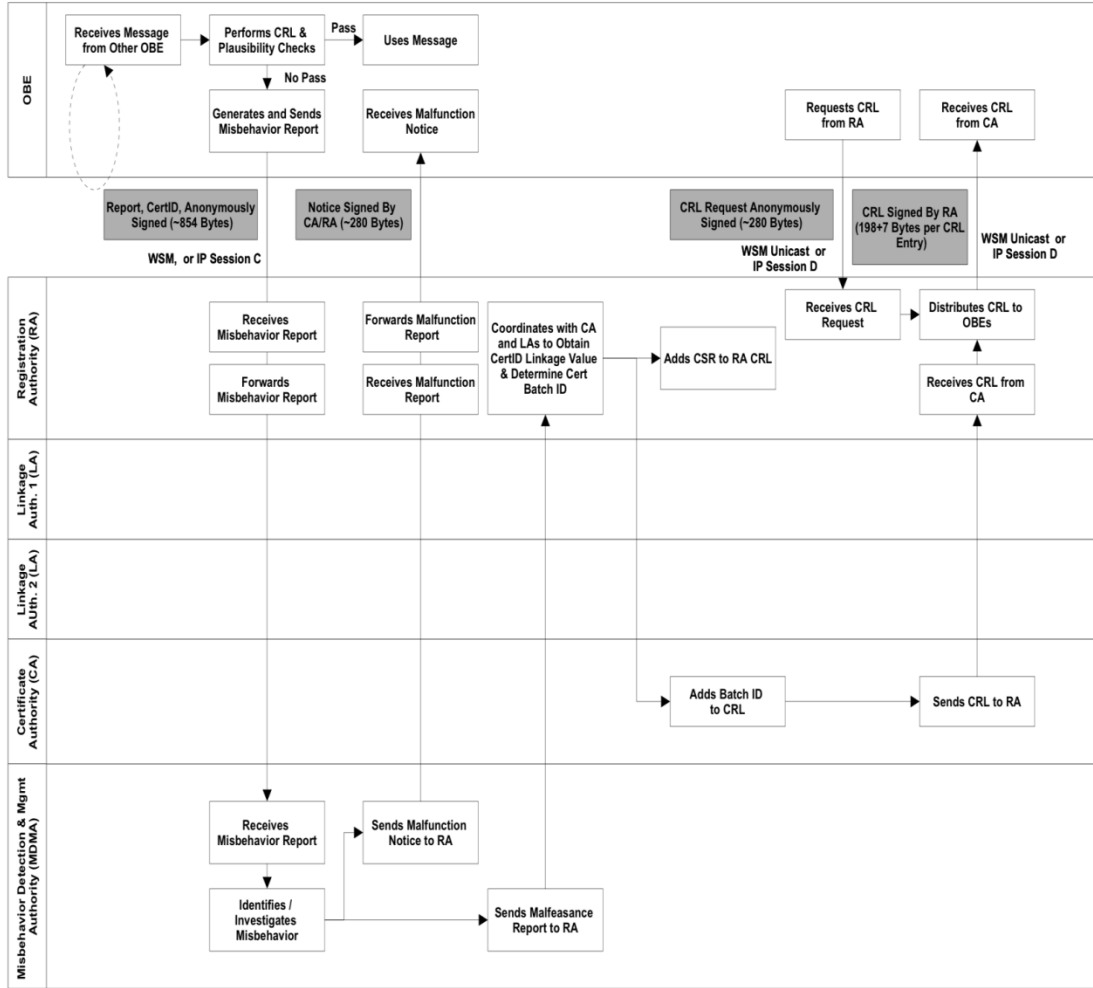
The misbehavior reporting process flow (at its nascent stage of development) is illustrated below as part of Figure 4, with the communications needs highlighted in grey.

In general, each vehicle must regularly visit a location where it can wirelessly access the network to update the CRL and submit misbehavior reports. These two transactions represent the highest temporal load on the system, since they must be done daily.

The data volumes for these transactions depend entirely on the level of misbehavior detected in the system. In situations where the misbehavior level is low, the number of misbehavior reports will also be low; furthermore, the size of the CRL will be correspondingly low. Since it is impossible to know these levels in advance we must estimate an expected value and identify a worst case value. If the level of misbehavior is higher than some still indeterminate worst case level, then it is likely that users will simply disable the systems, since the overall connected vehicle system will be effectively inoperable since it would effectively comprise a nuisance.

The background and generally continuous low level of misbehavior is defined to include failed vehicles, deliberately tampered vehicles, and those that have acquired some form of malware. It is important to also note that multiple OBEs are likely to report any other misbehaving OBE. The number of reports can thus be assumed to be equal to the number of equipped vehicles the misbehaving OBE encounters in any given day. For purposes of this analysis, it is estimated that the average vehicle encounters about 1000 other vehicles each day. Obviously, commuting vehicles may encounter many more than this, but other vehicles may encounter many less. However, at the nominal encounter rate, the misbehavior reporting rate is the number of misbehaving vehicles times 1000 times the penetration rate. In order to set working parameters for the calculations, we examine a scenario where if 1% of the vehicles are equipped, then the average misbehaving vehicle will encounter 10 other equipped vehicles (1% of 1000) in any given day, and each of those vehicles will issue a misbehavior report.

Figure 4: Certificate Revocation Flow



There are other methods for reporting misbehavior that can change these estimates. For example a random reporting scheme, while probably ineffective at identifying misbehavior, would result in far lower (and controllable) volumes of data transfer associated with misbehavior. These models have not yet been refined, so for purposes of this analysis, the most effective reporting scheme – each OBE reports any misbehavior it observes – will be analyzed.

Table 3 below shows the upper and lower bounds on data loads associated with misbehavior reports and CRLs at various levels of system deployment. As can be seen in the table, the fact that multiple vehicles are likely to report the same misbehaving vehicle causes the volume of misbehavior data to rise rapidly as the equipped population rises. This is also plotted in Figure 5 below.

The protocol for reporting misbehavior has not yet been defined, but presumably, vehicles could report all misbehaving vehicles observed since the last time they made a report, assuming they could identify misbehavior. In the worst case situation this would be once per day. Under the worst-case assumption of 50% of vehicles having misbehaviors, each vehicle would report 500 vehicles per day for a total data volume of 427 Kbyte per vehicle per day for the misbehavior report from OBE to CME. In contrast, under more modest background misbehavior levels of 1%, each vehicle would send about

8 Kbytes per day of misbehavior reports. These levels assume that at least one misbehaving message of 500 bytes is included in each report.

We note that since misbehavior can be induced as an attack, the introduction of the misbehavior report concept actually creates a new attack vector. Specifically by creating some mechanism, a substantial rate of misbehavior (or even a substantial *perception* of misbehavior within the OBEs), the rate of misbehavior reporting may grow without bound, resulting in an effective denial of service attack.

Unless other provisions are made to remove them, the entries in the CRL will remain for one year, since this is the lifetime for the full set of certificates. Other mechanisms are certainly possible, but unless the certificates are revoked in timed batches, or the CMEs acquire additional information about removed/repaired vehicles, the only way to assure that a user does not accept a bad certificate is to keep it on the CRL until it expires.

CRLs represent a substantial data load on the system. At any nominal level of misbehavior, the CRL represents about the same data load as the data transfer required to update certificates. In other words, at a nominal level of revocation, estimated at 1%, the CRL will be as large as the entire annual certificate update package. Since it is unlikely that any vehicle will be stationary at a connection point every day, updating CRLs must be performed as vehicles are traveling, a so-called On-The-Fly transaction. Alternatively some form of incremental updating may be possible, since each vehicle that has previously updated the CRL will presumably be current except for the most recent additions, which would significantly reduce the size of the daily CRL downloads. It is important to note, however, that the CRL approach is not yet finalized. For small scale model deployments the CRL is unlikely to represent a significant data load, so a single CRL update is easily feasible; however, going forward to full deployment, it is almost certain that an incremental approach would be used. Because this seems most practicable, in the remaining analyses we assume that CRLs will be incrementally updated and thus do not represent a substantial data load.

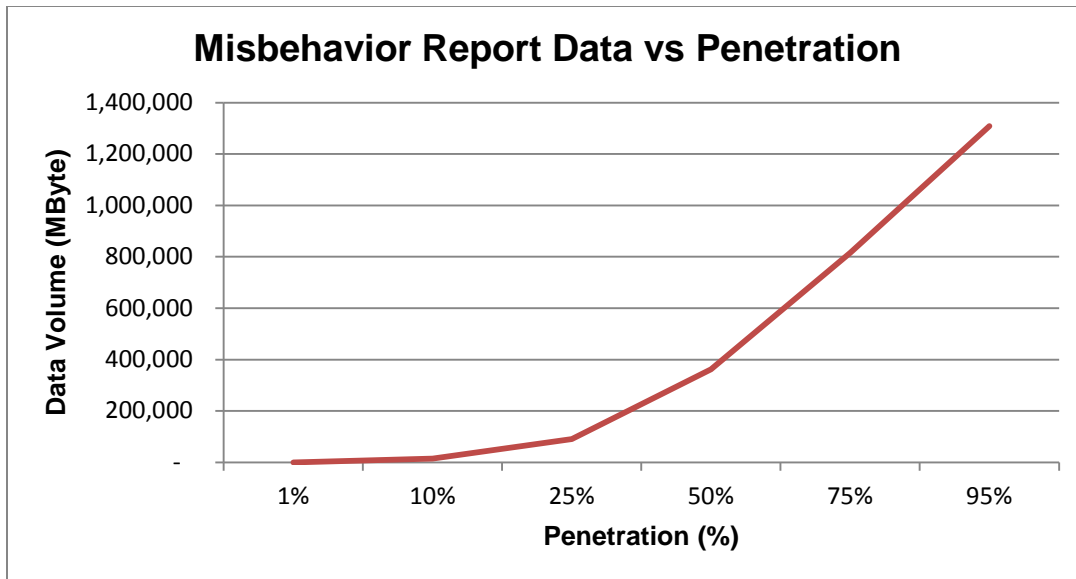
Table 3: Misbehavior Reports and CRL Entries vs. Penetration Level (per day)

Deployed Penetration	1%	10%	25%	50%	75%	95%
Deployed Population	2,500,000	25,000,000	62,500,000	125,000,000	187,500,000	237,500,000
Upper Bound Misbehaving Units	1,250,000	12,500,000	31,250,000	62,500,000	93,750,000	118,750,000
Lower Bound Misbehaving Units	25,000	250,000	625,000	1,250,000	1,875,000	2,375,000
Upper Bound Misbehavior Reports	12,500,000	125,000,000	312,500,000	625,000,000	937,500,000	1,187,500,000
Lower Bound Misbehavior Reports	250,000	2,500,000	6,250,000	12,500,000	18,750,000	23,750,000
Upper Bound CRL Entries	1,250,000	12,500,000	31,250,000	62,500,000	93,750,000	118,750,000
Lower Bound CRL Entries	25,000	250,000	625,000	1,250,000	1,875,000	2,375,000

Intelligent Transportation Systems Joint Program Office
 U.S. Department of Transportation, Research and Innovative Technology Administration

Upper Bound Misbehavior Report Signed Message Size (MB)	10,675	1,067,500	6,671,875	26,687,500	60,046,875	96,341,875
Upper Bound Misbehavior Report Demand per Vehicle (Byte)	427,000	427,000	427,000	427,000	427,000	427,000
Upper Bound Signed CRL Size (MB)	9	88	219	438	656	831
Lower End Misbehavior Report Signed Message Size (MB)	214	21,350	133,438	533,750	1,200,938	1,926,838
Lower End Misbehavior Report Demand per Vehicle (Byte)	8,540	8,540	8,540	8,540	8,540	8,540
Lower Bound Signed CRL Size (MB)	0.2	1.8	4.4	8.8	13.1	16.6

Figure 5: Lower Bound Misbehavior Report Volume vs. Penetration



Chapter 2. CDDS Technical Review

This Chapter presents a summary of the technical review of data transfer needs and specifications in order to provide background information about subsequent discussions of commercial and business models. A full discussion of data transfer needs and other CDDS technical requirements is included in Appendix A.

2.1 Summary of Communications Needs

There are a variety of connected vehicle applications that will be intended to provide safety, mobility and environmental messages to drivers and to road authorities. They fall into three broad categories:

- Vehicle-to-Vehicle (V2V) – In which vehicles broadcast messages to provide improved situational awareness to nearby vehicles, enabling collision warnings to be provided to drivers
- Vehicle-to-Infrastructure (V2I) – In which messages from roadway systems provide safety and mobility information to nearby vehicles (or nearby users, in the broadest set of applications), and where vehicles provide information to service providers or road authorities to allow them to either understand the traffic situation, or to better manage the roadway
- Security Management – In which the security credentials for mobile terminals (typically vehicles) are updated and managed. This is a unique form of V2I in which the information is not generally location oriented, and in which the volume of data may be substantially larger

Mobile communications systems can be characterized by a set of architectural and performance characteristics. The basic technical points of these systems are summarized in Table 4.

Table 4: General Technical Characteristics for Mobile Communications

Characteristic	Description
Radio Footprint	All conventional wireless radio communication systems have a maximum range. This is caused by the fact that radio waves spread out as they propagate, so the farther one is from the transmitter, the lower the signal level. Eventually, the communications signal falls below the noise floor, and communications reliability suffers and then communications ceases. For connected vehicles the communications generally occurs in all directions, so the area in which communications can be reliably conducted is known as the radio or RF footprint. The transmitter power, the receiver sensitivity, the size and design of the transmit and receive antennas, and various coding techniques can affect the size of the footprint.
Overall /Data Rate	<p>The Bandwidth of a wireless communications system determines how much data can be sent in any given time interval. In general, the wider the bandwidth the more data can be carried per second.</p> <p>The bandwidth can also affect the number of users that the system can serve, since higher bandwidth means any given message is sent more quickly, so the system has more time to devote to other users.</p>
Maximum User Demand	<p>The maximum terminal demand is the total number of terminals that can physically fit inside the RF footprint for the communications system. If the footprint is large, it can contain many users, and it must potentially support all of these users. If it is small, it will obviously include fewer users.</p> <p>User demand is essentially inversely proportional to coverage. A small footprint system has poor coverage, but it has low user demand. Conversely, a large footprint has good coverage, but this means it must also serve more users.</p>
User Data Rate	The maximum data bandwidth of a system must typically be shared among some or all of the users in the RF footprint. In the best case, the system has sufficient data bandwidth to serve the needs of all users in the footprint. However, as this demand increases (either by the introduction of more users or by users sending more data) the bandwidth available to any given user will decline. Depending on how the system manages user demand, this may result in slower overall data rates for all users, or longer latency (while each user waits for other users to complete their transactions. Typically the user data rate is decreased.
Connection Duration vs. Vehicle Speed	<p>The terminal must be able to connect for a period of time sufficient to allow the transaction to complete within a single transaction session. The available connection duration is a function of the local radio footprint size (the size of the area that is in range of the radio) and the vehicle speed.</p> <p>For any given vehicle speed, the size of the footprint will determine how long the vehicle will be in range and able to communicate, and the bandwidth of the communications channel will determine how much data can be transferred during the connection interval.</p> <p>Obviously if the vehicle is stationary or moving slowly in the footprint, it will be able to transfer more data than if it passes through the footprint at high speed.</p>

Characteristic	Description
Internet Protocol Addressing	<p>Unless they are constrained by physical limitations on the radio beam (e.g., point to point laser communications), most point to point communications systems require internet protocol addressing. Including this identifier informs any intermediary communications system elements about where the message is to go, and, in wireless networks, allows a terminal to filter out only those messages addressed to it (ignoring the others).</p> <p>For broadcast communications systems addressing represents a barrier, since the sender would like to send one message and have everyone in range receive it. Trying to broadcast a message in an addressed system typically requires learning the addresses of all intended recipients and then sending the message separately.</p>
Trip Anonymity	<p>A key concern in the connected vehicle area is maintaining privacy or obviating tracking of individual trips. In general one-to-one transactions are not anonymous, although there are cases where this may be desirable.</p>
Latency	<p>Latency is the time delay between when a message is sent, and when it is received. In most communications systems protocol processes take time, and this introduces a delay. In some cases the system must wait for other communications traffic before it can transmit, and this introduces other delays.</p>
Network Attach Time	<p>Network attach time is similar to latency, but it has a different nature. Many wireless systems create a network where each node in the network becomes aware of one or more nodes in the network. In office LANs, for example, the addition of a printer to the network will result in the printer acquiring a network address, and each device on the network being informed of this address. The printer also learns the addresses of all other nodes on the network. In a WiFi network this process includes the device discovering the network (the SSID) and then the process of joining the network. In some cases the network attach process also requires authentication transactions.</p> <p>This process takes time, and it must be completed before a device can send or receive messages on the network.</p>
Overall Coverage	<p>If the RF footprint is not larger than the road network, then there will be areas of the road network that are not within a footprint. For smaller footprints this means that the mobile terminal will pass in and out of footprints as it drives. The coverage of a communications system is a measure of how much of the road network falls within radio footprints for the communications system under consideration.</p> <p>Some footprints (e.g., satellite) are very large, while others (e.g., WiFi) are very small.</p>

Characteristic	Description
Security	<p>To avoid eavesdropping (listening in) and spoofing (masquerading as someone else) the communications technology must be able to support secure communications.</p> <p>For broadcast messages, the messages must be able to be authenticated. Encrypting them makes no sense since they are intended for all recipients, however it is valuable to be sure that the sender is legitimate. Authenticating a message while maintaining the anonymity of the sender is a key technical challenge.</p> <p>For one-to-one communications it is useful to also encrypt the messages.</p> <p>The degree of security depends on the type of application.</p>

Table 4 illustrates the subtle distinctions between various communication systems that need to be accounted for in planning for CDDS implementation. In general the three categories of connected vehicle applications described above (V2V, V2I and Security Management) impose substantially different needs or demands relative to the overall communication system capabilities. These needs are summarized in Table 5.

Table 5: Communications Needs by Application Category

Characteristic	V2V	V2I	Security Management
Radio Footprint	<p>Generally best served by small footprint located around vehicle. Size of footprint depends on range of potential hazards. Typically footprint is less than 100 meter radius.</p>	<p>For V2I safety warning and/or tolling applications this is generally best served by small footprint located around the roadway point of interest (hazard or tolling point). The infrastructure installations may need to network with each other locally to provide “upstream” advisories to allow users to take countermeasures.</p> <p>For wide area mobility information collection or distribution footprint is not particularly important other than how it affects coverage.</p>	<p>Security Management requires substantial data transfer volumes. As a result the RF footprint must be sufficiently large that the data transaction can be completed while the vehicle is inside the footprint. For stationary vehicles, this footprint can be quite small. For moving vehicles it needs to grow, but not so large that there are many other vehicles competing for high bandwidth security updates.</p>
Overall Data Rate	<p>Generally best served by high data rate that allows messages to be sent quickly to minimize bandwidth congestion.</p>	<p>Generally low data rates are acceptable, with the exception of data collection applications which benefit from higher rates to avoid bandwidth congestion.</p>	<p>Requires relatively high data rates to transfer large volumes of data. Changing credential update frequency can reduce this requirement.</p>

Characteristic	V2V	V2I	Security Management
Maximum User Demand	Typically limited to about 100 users in immediate vicinity of vehicle.	Typically limited to about 100 users in immediate vicinity of vehicle who are likely to be conducting the same transactions. For safety systems this is effectively the same as for V2V.	Typically limited to only a small subset of the users in the immediate vicinity. However, in larger footprints, user demand can become relatively large.
User Data Rate	For Basic Safety Messages, the user data rate must be sufficient to allow each user to send their messages every 100 msec.	For V2I the user data rate must be sufficient to allow users to deliver collected probe data to the system/service provider. Other V2I applications generally impose lower demand.	Must be sufficient to allow user to complete transactions while in the RF footprint. Generally limited by certificate updates and non-incremental CRL delivery (entire CRL).
Connection Duration vs. Vehicle Speed	This is not an issue for V2V communications since it is assumed that any vehicles outside the footprint do not represent hazards.	This is generally not an issue for V2I communications since the messages are short enough that it is not likely the vehicle will leave the footprint before receiving them.	This is a serious issue for certificate management since the data volumes can be rather large. For small footprint technologies the speed must be low enough to allow the data transfer to complete.

Characteristic	V2V	V2I	Security Management
Overall Coverage	This is not an issue for V2V communications since only the vehicles in the immediate vicinity are important. It does raise the question that sparse vehicle penetration is effectively the same and poor coverage.	V2I coverage is primarily related to specific locations. It is possible to broadcast messages in one location (where there is coverage) and have the message activate a warning when the vehicle reaches or approaches a hazard in another location. The vehicle might, for example pass an RSE, or contact a service provider over cellular, and obtain general road hazard information.. These messages would be stored for some time, and if the vehicle approached the area where they were relevant, they would be presented to the driver. As a result local coverage is not critically important since messages can be delivered when there is coverage and presented when and if the vehicle reaches the place where the messages are relevant.	Coverage is important for security management since the vehicle is assumed to be connected daily (to obtain CRLs). So the coverage must be sufficient that the vehicle regularly passes a connection footprint. Since all vehicles must be managed by the CME, this imposes a significant requirement.
Latency	Latency is critical for close proximity safety applications that are used in the V2V category.	Latency is important for some time critical V2I applications. If the delay is too long and the data in the message changes, then the vehicle must be updated promptly.	Latency is not generally critical for security management transactions.
Network Attach Time	V2V transactions are highly time critical. If there is any network attach time it must be less than about 50 msec.	Network attach time is less critical for V2I transactions than V2V transactions. However, the network attach time can detract from the duration in the RF footprint. For moving vehicles and small footprints network attach time cannot be more than about 2 seconds, preferably less.	Network attach time can detract from the duration in the RF footprint. For moving vehicles and small footprints network attach time can severely limit the ability of a moving vehicle to complete a security update.

Characteristic	V2V	V2I	Security Management
Anonymity	All V2V transactions must be anonymous.	V2I transactions that originate from the vehicle may need to be anonymous unless the receiver has a trusted relationship with the vehicle. Broadcast roadside messages are not anonymous since they are from the system.	Security transactions do not need to be anonymous (between the vehicle and the RA). They must however be encrypted to prevent others from capturing them and violating the vehicle owner's privacy or stealing security information.
Security	Requires message authentication.	Requires message authentication. May require encryption.	Requires authentication and encryption.
Addressing	Not required or desired since the sender vehicle would need to learn the network addresses of all surrounding vehicles, and these change rapidly.	Not generally required or desired since the messages are meant for many vehicles and the sender would need to learn the network addresses of all surrounding vehicles. May be used for vehicle to roadside transactions such as tolling and probe data collection where the system can provide the address, and there is only a single address.	Generally required since all communication is point to point.

Based on the number of messages and communications that may be developed within the context of connected vehicle system, we must analyze the applicability of various network options to be the carriers of these communications. To summarize, the communications that will need to be covered (at a minimum) by a choice of CDDS involve the wireless or over-the-air transactions to enable the CME to work with wireless terminals:

- All communications between OBE and CMEs. These include:
 - Requests for and distribution of annual certificates
 - Requests for and distribution of monthly decryption keys
 - Misbehavior reports from OBE to CMEs (unless an onboard means of diagnosing other misbehaving participants is developed)
 - CRLs from CMEs to OBE (unless an onboard means of diagnosing other misbehaving participants is developed)
- Communications between RSE and OBE

Following we discuss several network solutions or options in turn and then examine their advantages and disadvantages based on current working assumptions about the sizes and kinds of communications that will fall into the above categories.

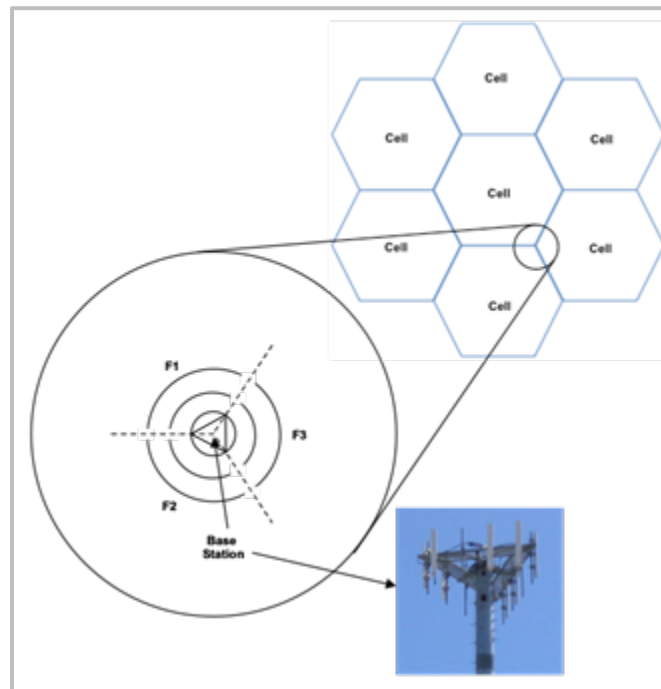
2.2 Technology Overview

In order to examine the options available for networks upon which to send and receive the messages from OBE to CMEs, as well as the messages from OBE to Infrastructure, in the case of V2I configuration, several existing networks are analyzed in order to draw conclusions about advantages and disadvantages of each. Cellular, DSRC, and WiFi are the candidate technologies for supporting connected vehicle applications, however other technologies were considered. All these are discussed in this section.

2.2.1 Cellular/Long Term Evolution

Cellular communications uses a series of base stations to provide voice and data communications services over relatively large areas. Typically each base station serves several sectors that are arranged to use slightly different frequencies to minimize interference. This also assures that reasonable channel bandwidth is available to the users in any given sector. A typical cellular arrangement is shown in Figure 6 below.

Figure 6: Typical Cellular System Arrangement



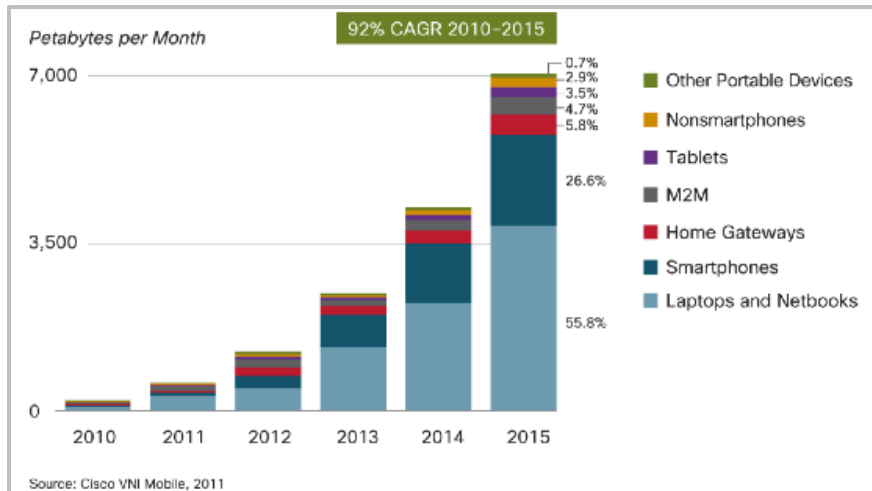
In this arrangement each base serves some number of sectors. The base stations are linked within the system to enable a mobile terminal operating in one sector to be “handed off” to an adjacent base station when it passes from one cell or sector to another.

Because of the popularity of mobile telephones, cellular technologies have advanced rapidly. The recent rise of “smart phones” and other connected consumer devices has further fueled this growth. The technologies are still evolving but the latest Long Term Evolution (LTE) cellular technologies are able to provide very high speed data transfer rates to a large number of subscribers simultaneously.

Nearly all new applications available on connected tablets and smartphones are based on services provided through the internet, so backhaul connectivity to any internet connected server is a given.

As shown in Figure 7 below, Cisco anticipates about a tenfold increase in mobile data traffic over the next five years. (For reference, one Petabyte is 1M gigabytes.)

Figure 7: Mobile Data Projection



(Ref: Cisco Visual Networking Index: *Global Mobile Data Traffic Forecast Update, 2010–2015*)

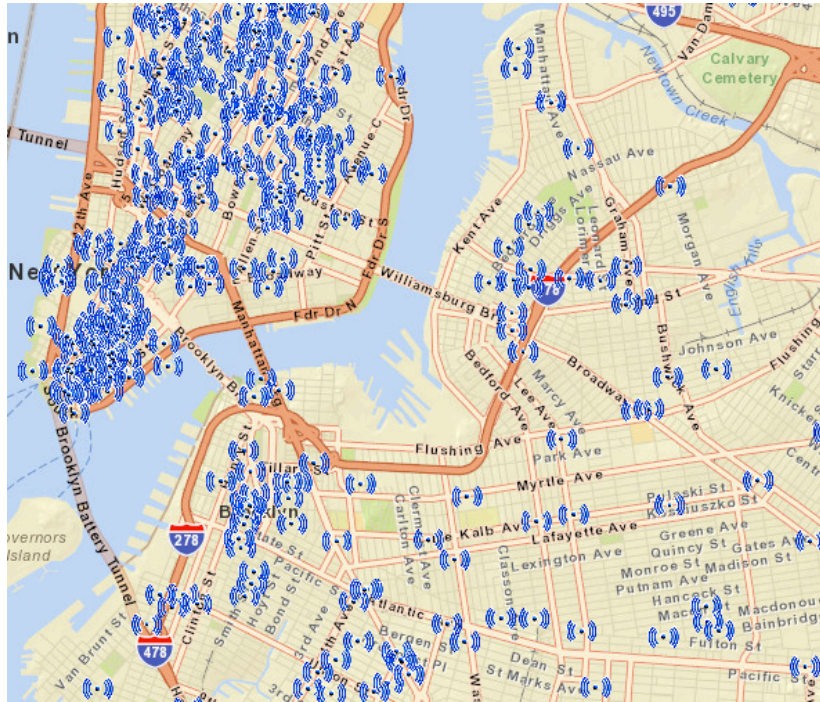
Generally, cellular systems are commercially operated, so all data transactions involve some form of fee. There is, however, substantial flexibility in these commercial arrangements. While most users simply support a service subscription, other models are also used. For example, the Amazon Kindle electronic reader uses a 3G cellular service provided by Sprint. Known as Whispernet, the service supports the over-the-air download of books purchased on the Amazon web site. Each Kindle device is registered with the network, and the data fees paid to Sprint by Amazon are recovered as a portion of the purchase price for the electronic book, rather than as a separate charge to the individual user. Such an approach could presumably be applied to an infrequent, relatively low volume transaction such as updating security credentials.

Because they are intended to serve mobile users, cellular systems are designed to provide high data bandwidth to users in motion. They are also widely deployed so that customers can enjoy the services regardless of where they go. As popularity has grown all urban areas generally have cellular coverage provided by multiple carriers. While not ubiquitous, most major highways also have coverage.

2.2.2 WiFi

WiFi is a wireless internet technology typically used to provide mobile internet access to devices that stay within the footprint of the WiFi device. WiFi networks are typically found in home and office environments, and more recently in cafes, public areas, and transit vehicles such as buses, trains, and airliners.

Figure 8 below shows a typical geographic distribution of WiFi hot spots, in this case in lower Manhattan and Brooklyn, NY. A hot spot is the area in which the WiFi signal is active and able to be picked up by a WiFi terminal.

Figure 8: WiFi Hot Spot Distribution

(Ref: NYC Open Data)

WiFi is governed by one of several versions of the IEEE 802.11 standard. Typical WiFi operates at 2.4 GHz and conforms to the 802.11b/g. Higher performance systems often conform to the 802.11a standard which operates in the 5.15-5.25 GHz band. These systems typically offer ranges up to about 100 feet, although some advanced antenna technologies (MIMO) can substantially increase this for stationary users. Nearly all WiFi systems use the Internet Protocol (IP), enabling a mobile terminal within range of a WiFi base station to request to join the network, and if permission is granted, receive an IP address for the local subnet. The base station will typically also provide all network nodes with an updated network table. In this way, new members of the network will become aware of the other nodes on the network, and those nodes will learn of the new member. This process, known as “association” takes about 10 seconds to complete. Once a terminal is attached to the network, it can then send IP packets to other members of the network, or, if the base station is connected to the Internet, to any server on the Internet.

The relatively long association time, coupled with disparate and sometimes unknown ownership of hotspots and small coverage footprint, render WiFi problematic for purposes of certificate management. The small coverage and long association are sufficient to rule out WiFi, as these require vehicles to be nearly stationary for most transactions.

2.2.3 Dedicated Short Range Communications

Dedicated Short Range Communications (DSRC) is a communications protocol developed specifically to address the technical issues associated with sending and receiving data between vehicles and between moving vehicles and fixed roadside access points. DSRC is a specialized form of WiFi. As with WiFi it is a derivative of the basic IEEE 802.11 standard. DSRC is governed by the IEEE 802.11p and 1609 standards. DSRC uses a dedicated 75 MHz frequency band in the 5.9 GHz range. This

frequency is usable by most WiFi chipsets, so typically DSRC radios are based on modified WiFi radios.

The two primary differences between WiFi and DSRC are the fact that DSRC does not use a network association process, and it provides a mechanism for simple application specific message addressing, including broadcasting. Instead of the conventional association process, DSRC uses IPv6, an internet protocol used to direct internet traffic, to allow each new terminal to generate its own IP address using the Link Local address of the base station, and its own Media Access Control (MAC) address, a unique identifier assigned to network interfaces. This effectively eliminates the network attach time. To preserve anonymity, each OBE generates a random MAC address, and to prevent “bridging between certificates (e.g. linking certificates by matching the corresponding MAC address), the OBE creates a new random MAC address whenever the security certificate is changed.

DSRC also includes the WAVE Short Message (WSM) protocol that allows terminals to broadcast messages to all other devices in radio range. This is highly efficient because any given terminal does not need to learn the network identities of each other terminal. For security management this is inconsequential since all of the transactions (with the possible exception of broadcasting a CRL) are between a vehicle and a remote server (the RA).

At a conservative estimate, the typical range of a DSRC access point is about 300 meters. Ranges up to about 1Km have been observed. Typical installations are expected to be at intersections, fueling and charging stations and other roadside locations.

2.2.4 Additional Technologies

Other technologies, including WiMAX, satellite and HD radio were examined but eliminated from more detailed analysis because they were considered unsuitable. WiMAX technology is rapidly being eclipsed, since most carriers are using or building LTE systems. Satellite and HD radio are broadcast only and are infrastructure based, so they cannot support V2V or V2I applications (where data is collected from the vehicle), and they cannot support two-way transactions.

Satellite Digital Audio Radio Service (SDARS) is a communications method to deliver digital audio to subscribers over a nationwide satellite link. The standard is open to anyone who can obtain spectrum, but the only current operator is Sirius/XM. The only practical purpose for SDARS is broadcasting messages to vehicles; however, the national footprint inhibits regional use.

It is possible that some roadside warning applications could be supported by SDARS and HD Radio, but these systems have relatively low bandwidth, and as the volume of data grows the latency of these two means of communications grows substantially. It is possible under some models that latencies could rise into tens of hours with these systems, especially SDARS which has a half-nationwide footprint (which means that a warning message for a road in Virginia would also be sent to vehicles in Detroit, and vice versa).

2.2.5 Technology Summary

Table 6 below summarizes the high level advantages and disadvantages of all technologies described above, highlighting how the various options would influence the effectiveness and efficiency of the Connected Vehicle Environment. From the table, and at this juncture of the report based on technical considerations alone, cellular and DSRC are both viable for certain aspects of connected vehicle applications. However, based on our analyses to date, the conclusion is that other technologies reviewed are generally very limited in their utility. Cellular offers a good solution for most V2I

applications and it is well suited to security management. It is not appropriate for V2V applications. DSRC is well suited to V2V and most V2I applications. It is slightly less well suited for security management if the data volumes are large and infrequent. If updates are performed at least monthly, and CRLs are updated incrementally, then DSRC has equivalent performance to cellular for security management.

Table 6: Wireless Technology Summary

Technology	Advantages	Disadvantages	Comment
Cellular	<ul style="list-style-type: none"> Nationwide coverage Universal equipment available 	<ul style="list-style-type: none"> Partnerships required with wireless carriers Broadcast is problematic Requires IP addressing 	<ul style="list-style-type: none"> Key element in analysis
WiFi	<ul style="list-style-type: none"> Universal standard Many hotspots available High Bandwidth 	<ul style="list-style-type: none"> Small coverage footprint of hotspots requires vehicles to be nearly stationary for most transactions Disparate control and ownership of hotspots Requires IP addressing and network setup (long attach delay) 	<ul style="list-style-type: none"> Considered with limited use while in stationary mode (for example in provisioning annual certificate bundle) in final scenario analysis
DSRC	<ul style="list-style-type: none"> WiFi-like standardization Broadcast capability; does not require IP addressing Nearly instantaneous network attach time High bandwidth 	<ul style="list-style-type: none"> Not deployed Small RF footprint limits size of data exchanges at higher speeds Potential for channel congestion from high density V2V messaging 	<ul style="list-style-type: none"> Key element in analysis
WiMAX	<ul style="list-style-type: none"> High bandwidth Low cost from wireless carriers 	<ul style="list-style-type: none"> No nationwide deployment LTE technology selection by most carriers Broadcast is problematic Requires IP addressing 	<ul style="list-style-type: none"> Not considered in this analysis Provides no substantial benefit over cellular, and has lower level of deployment
SDARS	<ul style="list-style-type: none"> Nationwide coverage Equipment is widely available 	<ul style="list-style-type: none"> Broadcast only Huge footprint may result in high latency 	<ul style="list-style-type: none"> Not considered in this analysis

Technology	Advantages	Disadvantages	Comment
HD Radio	<ul style="list-style-type: none"> Widespread urban coverage Widely available in automotive equipment 	<ul style="list-style-type: none"> Broadcast only Large footprint and low bandwidth may result in high latency 	<ul style="list-style-type: none"> Not considered in this analysis

2.3 Data Communications Analysis

As described in the prior section and Table 6, connected vehicle applications require substantially different basic characteristics from a communications system. This section explores the specific data communications loads imposed by these different applications, based on current assumption of the technical architecture and specifications. A theme which we take into the analysis of the business case is the difficulty of separating the technology (and subsequently, the costs and values) of a “certificate only” use of the system and a commercial use of the system non-essential to safety. We view these two parts as holistic, with the certificate management portion realized as a requirement. Given this, the technologies used for delivering certificate management might also be viewed as the same wireless means to deliver the set of considered V2V and V2I applications. As such, a top-level communications analysis which takes into account not only the data load from certificate management functions but also the concurrent and therefore additive data load from the applications is presented below and is used as we size the requirements of the system *in toto*.

Nearly all V2V and V2I messages from DSRC are sent in a special single packet form known as a WAVE Short Message (WSM). The maximum size of a WSM is fixed by the 802.11 Maximum Transmission Unit (MTU) which is typically limited to 1500 bytes total, including all protocol headers and the message payload.

The following sections describe the various messages used in these application categories. To obtain these values we have made the following assumptions:

- IEEE 1609.2 security based on elliptic curve cryptography will be used. This generally results in certificates of about 132 bytes
- Encryption does not increase file size (other than by the addition of certificates)
- Signing increases file size by the size of the signature and associated certificates appended to the message

The specific message sizes were developed from examination of the 1609.2 standard, and the various system description, security and SAE J2735 (DSRC Technical Committee) standards documents. The actual messages in an implementation may have slightly different sizes, so the sections below represent the general scale of the messages. Table 7 below describes the data element sizes for different types of messages, referred to during the more detailed discussion about various loads and implications on the CDDS of the different messaging schemes.

Table 7: Basic Signed Message Sizes

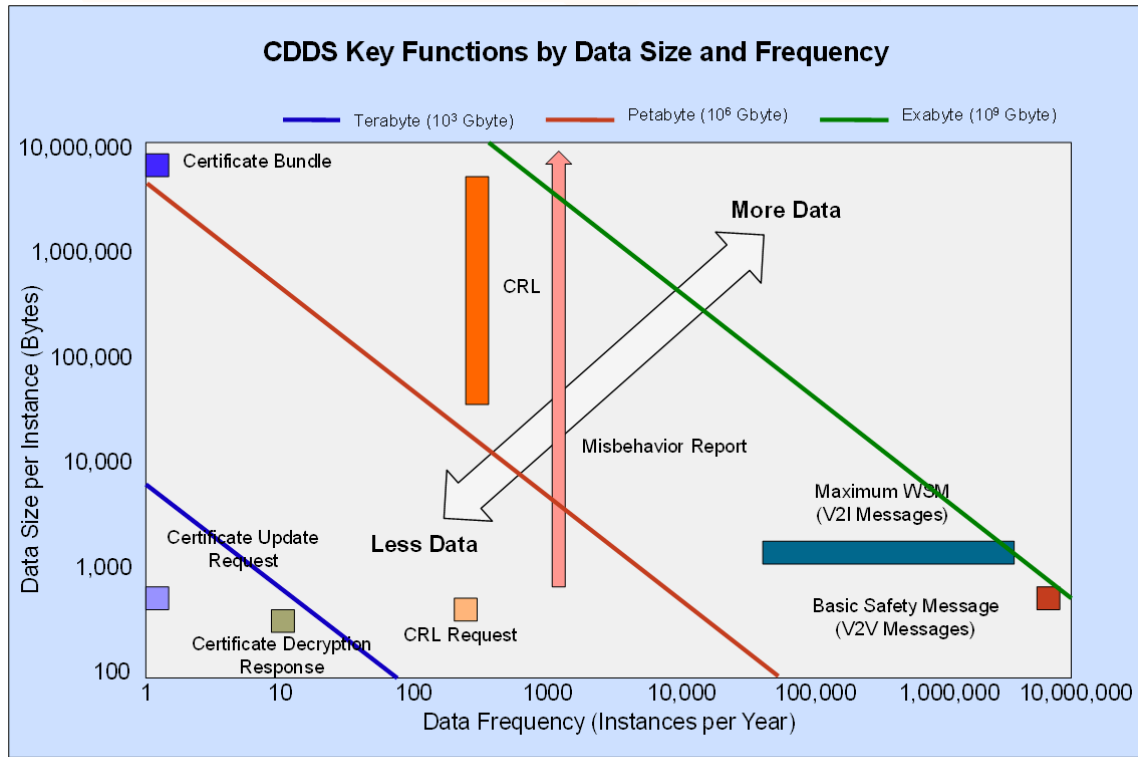
Message Transaction	Data Elements	Element Size (Byte)	Overall Size (Byte)	Send	Receive	Freq
Basic Safety Message			528	OBE	OBE	10 Hz
	Payload	330				
	OBE Signature	66				
	OBE Cert	132				
Max WSM			1500	I/V	V/I	~10 Hz
	Payload	1302				
	OBE Signature	66				
	OBE Cert	132				
Certificate Update Request			533	OBE	RA	Annual
	Request	203				
	OBE CSR Cert	132				
	CA Cert	132				
	OBE CSR Signature	66				
Certificate Bundle			15,572,400	RA	OBE	Annual
	Certificates	13,875,840				
	CA Signature	154,176				
	CA Cert	132				
	RA Cert	132				
Certificate Decryption Request			362	OBE	RA	Monthly
	Request	32				
	OBE CSR Signature	66				
	OBE CSR Cert	132				
	CA Cert	132				
Certificate Decryption Reply			378	RA	OBE	Monthly
	Decryption Key	32				
	Misc. Info	16				
	RA Signature	66				
	RA Cert	132				
	CA Cert	132				
Misbehavior Report			854	OBE	MDMA	Variable
	Report	24				
	Message Sample	500				
	OBE Anon. Sig	66				
	OBE Anon. Cert	132				
	CA Cert	132				
CRL Request			336	OBE	CA/RA	Daily
	Request	6				
	OBE Anonymous Sig	66				
	OBE Anonymous Cert	132				
	CA Cert	132				

Message Transaction	Data Elements	Element Size (Byte)	Overall Size (Byte)	Send	Receive	Freq
CRL			Variable	CA/RA	OBE	Daily
	CRL	7 Byte per CRL Entry				
	CA Signature	66				
CA Cert	132					

While the V2V, V2I and certificate management applications are not expected to change appreciably as the number of equipped vehicles grows, the growing number of vehicles will increase the demand on communications since the total volume of data communicated will grow as the population grows. This means that either the communications capacity needs to increase or the existing capacity will need to be spread among an increasing number of users. We include below an examination of the additional communications demand imposed by each of the application categories.

The overall volume of data that the CDDS must support depends on the size of the messages and the frequency over which they are sent. A detailed analysis of the message types, sizes and frequencies is provided in Chapter 2 (Section 2.3). Figure 9 below summarizes the overall data volumes represented by various types of connected vehicle messages. As can be appreciated from the figure, the annual certificate bundle represents a delivery challenge simply because it is rather large (20-30 Mbytes), although since it is only sent annually, the overall data volume is relatively small. In contrast, the CRL payload is smaller, but in the current model it is sent approximately daily, so on an annual basis it represents nearly 1000 times as much data as provisioning certificate bundles. The annual payload from other certificate management-related messages is also shown. These generally represent substantially lower overall data volumes, although the misbehavior reports could rival the annual certificate bundle if the rate of misbehavior is high.

Figure 9: Connected Vehicle Messaging Data Volumes



Assumptions: 250 M vehicles and 50% Adoption; BSM and Max WAVE short message operate only while vehicles are operating and communicating, ~54 minutes per day

While the CDDS is not the network upon which V2V messages are exchanged, the Basic Safety Message (BSM) is also indicated on Figure 1 above for reference. The Maximum WAVE Short Message (WSM) represents typical V2I messaging. This is the maximum size WSM that can be sent. The overall volume of this type of message depends heavily on the number of alert or warning sites (i.e., the density of on-road events or conditions that must be communicated). In the worst case this density could be as high as every 100 meters or so (e.g., in an urban grid).

From a CDDS perspective, the annual certificate bundle, the CRL delivery, and V2I messaging represent significantly different communications challenges. The certificate bundle requires substantial system bandwidth in order to quickly transfer certificates, but this bandwidth is only needed once per year for each car (i.e., for a few seconds or minutes each year). This means that the certificate update could conceivably be supported with a low bandwidth system while the vehicle is stationary. Encountering such a stationary access point once per year does not seem unreasonable. On the other hand, if the certificate update is to be done with the vehicle in motion the CDDS must be connected long enough to allow the transfer of this large volume of data. This may be difficult for small radio footprint systems like DSRC and WiFi, since the vehicle may pass through the coverage zone before the data transfer is complete.

In contrast, the delivery of CRLs is currently envisioned to be performed approximately daily. This means that the vehicle must encounter an access point at least once per day, and it must be in range of that access point long enough to transfer the CRL. If the CRL is large, this may be problematic. V2I messaging represents a similar challenge to the CRL, except that the dynamics are more extreme.

The per message data volume for V2I is very low, but, in order to assure that important V2I messages are received, the vehicle must encounter access points with high regularity.

In short, the certificate update requires access to high bandwidth for relatively long intervals (tens of seconds to minutes) but only once per year. The CRL requires access to high bandwidth for somewhat shorter intervals (e.g. 1-30 seconds), but on at least a daily basis. V2I messaging requires access to relatively low bandwidth for very short intervals (milliseconds), but with sufficient frequency or geographic density that the car always has up to date roadway condition and hazard information as it moves.

2.3.1 V2V Communications

V2V communications are dominated by the BSM, which is defined in SAE J2735. This message provides basic vehicle position and state information to other surrounding vehicles. The current standard defines Part 1 of the BSM to about 330 bytes. When signed this message is about 528 bytes. BSMs are always sent in broadcast mode, so they are one way from vehicles to other vehicles.

Each message is small, since they are sent from all vehicles and they are sent every 100 msec. This creates a rather large communications demand.

V2V messaging involves broadcasting BSMs every 100 msec from each vehicle. In general, because of the safety focus of the BSM, the only vehicles of relevance to any given vehicle are those within about 100 meters. DSRC (within the vehicle, broadcast from DSRC radio on each OBE) is the obvious choice for this application. However, for completeness, we have analyzed the message traffic parametrically, so other technologies can also be assessed.

Passenger vehicles range from about three to five meters in length. Assuming an average of 4 meters, and a minimum spacing of one car length, maximum lane density is one vehicle every 8 meters, or 125 vehicles per lane per kilometer. The number of vehicles as a function of different physical situations is provided in Table 8 below. These values represent the highest possible vehicle density (i.e., gridlock), but they do illustrate the effect of increasing RF footprint size. Note that since trucks and buses are normally a relatively smaller fraction of the traffic volume, not including them in this analysis does not significantly alter the results. Note also that these numbers assume only one message per vehicle every 100 msec. If some form of addressing scheme was used, the data volumes would increase by the number of vehicles (so, for example, the data volume for a 100 meter radius footprint on a two lane road would increase by a factor of 25).

Table 8: Vehicles in Footprint Based on Different Road Situations

Situation	Footprint Radius (meters)					
	10	50	100	500	1000	5000
2 Lane Road	2.5	12.5	25	125	250	1250
4 Lane Road	5	25	50	250	500	2500
2 Lane Intersection	5	25	50	250	500	2500
4 Lane Intersection	5	50	100	500	1000	5000
8 Lane Intersection	5	100	200	1000	2000	10000
2 Lane Grid, (100 Meter Spacing)	5	25	50	2,250	9,500	190,000
Mixed 2 & 4 Lane Grid (50%) (100 Meter Spacing)	5	38	75	3,375	14,250	285,000

The corresponding data load (in Kbits/sec) from BSMS for these footprints is provided in Table 9 below.

Table 9: V2V Data Transfer Load (Kbit/Sec) in Footprint Based on Different Road Situations

Situation	Footprint Radius (meters)					
	10	50	100	500	1000	5000
2 Lane Road	106	528	1,056	5,280	10,560	52,800
4 Lane Road	211	1,056	2,112	10,560	21,120	105,600
2 Lane Intersection	211	1,056	2,112	10,560	21,120	105,600
4 Lane Intersection	211	2,112	4,224	21,120	42,240	211,200
8 Lane Intersection	211	4,224	8,448	42,240	84,480	422,400
2 Lane Grid, (100 Meter Spacing)	211	1,056	2,112	95,040	401,280	8,025,600
Mixed 2 & 4 Lane Grid (50%) 2 Lane Grid, (100 Meter Spacing)	211	1,605	3,168	142,560	31,680	12,038,400

(Note: 100K Kbits/sec equals 100 Mbits/sec)

As can be appreciated from the tables 8 and 9 above, the V2V data load increases dramatically as the footprint grows beyond about 500 meters in radius. This is driven by the frequency of the BSM transmissions and the number of vehicles in the footprint. This illustrates why DSRC is best suited for

V2V applications since the V2V range is typically limited to about 100 meters. Using wider area (larger footprint) communications systems is clearly not appropriate for V2V applications.

2.3.2 V2I Communications

V2I applications can cover a wide range of approaches. Generally these applications will be focused on providing information about the roadway or the roadway state within a region. In many applications this region can be rather small. For example a curve speed warning message only applies in the roadway region approaching the curve, and a Signal Phase and Timing (SPaT) message only applies in the roadway region approaching a signalized intersection. The repeat rate of these messages can also vary significantly. While the SAE J2735 standard assumes a 10 Hz rate for most messages, this may not be optimal or necessary.

V2I messages are also generally one way (from the RSE to the OBE), but since they may originate from the vehicle or the roadside, they require a bi-directional data link, or a pair of unidirectional data links.

For purposes of analysis we have assumed that a typical signed V2I message is about 500 bytes long and is repeated at a 10 Hz rate. Some messages may be longer, and some may be repeated less frequently, but these assumptions appear to be realistic for the average V2I application. (Refer to Table 9 above for a summary of V2I message sizes.)

V2I messaging involves a much lower data load than V2V. In general V2I messages are sent at the same basic rate (about 10 Hz) as V2V messages, but they typically originate from only one location on the roadway and are relevant for only the region around a potential hazard. In most cases any given segment of roadway will have no hazards. To model the data load for V2I we can assume a worst case hazard density of one hazard per 100 meters of roadway. In an urban grid environment, this would equate to every intersection being signalized and sending out SPaT messages. In a single road segment, this might equate to some form of road issue every 100 meters (which is clearly higher density than most roads).

Following the same processes as for V2V above, the data loads for various RF footprints are provided in Table 10 below. Here we have assumed that however the messages are broadcast, the message density is one message for every region 100 meters across. The message size is assumed to be 1500 bytes and the repeat rate is 10 Hz. V2I messages can be in a number of forms, some small (500 bytes) and others larger. We used a conservative estimate in order to ensure planning for sufficient coverage.

Table 10: V2I Data Transfer Load (Kbit/Sec) in Footprint Based on Different Road Situations (1500 Byte messages)

Situation	Footprint Radius (meters)			
	100	500	1000	5000
Single Road	120	600	1,200	6,000
Crossing Road	120	1,200	2,400	12,000
Urban Grid (100 Meter Spacing)	120	9,720	43,320	866,400

For smaller, 500 byte messages the values would be 30% of those in the Table 10.

As with V2V messaging, the data volume grows rapidly as the footprint area served by the communications system grows.

2.3.3 Security Management Communications

The security management process is described in Chapter 1. The process as currently conceived requires a two-way secure link between the vehicle OBE and the RA.

As described in Chapter 1, each OBE must engage in transactions to update certificates, to obtain regular certificate bundle decryption keys, and to obtain updated CRLs. The data elements included in these transactions, together with estimates for the size of the data for each element, are summarized earlier in Table 3. By far, the largest data transactions are the provision of certificates from the RA to the OBEs, and the provision of the CRL to the OBEs.

Security management can be separated into two basic processes: Certificate Updating and Misbehavior Management. Certificate updating involves requesting new certificates, receiving the certificates and then regularly requesting and receiving keys to decrypt batches of certificates. Misbehavior management involves OBEs reporting observed potential misbehavior, and then requesting and receiving certificate revocation information (to know what certificates to ignore). These operations are dealt with separately in the sections below.

In general the security operations differ from V2V and V2I messaging in that they are not dependent on the RF footprint size. If a vehicle is in a footprint, and it requires security transactions it performs them, but, generally, increasing the size of the footprint has only a small effect on the overall bandwidth requirement.

2.4 Technology Analyses Findings

Based on the literature review and industry research and feedback from the Policy Workshop, the primary candidates for security credential management were found to be cellular, WiFi and DSRC. Other technologies considered were satellite (SDARS), WiMAX, and HD Radio.

V2V communications requires a radio transceiver in each vehicle, so this limits the possible choices of technology to Cellular, WiFi, DSRC and WiMAX.

V2I communications can be supported by any of the candidate systems, although review of the general literature indicates that using satellite or HD radio would result in very long latencies at high levels of message traffic. For this work, our team performed an updated review of the advantages and disadvantages of using all four technologies for CDDS as described below to arrive at these findings.

In general, while it is possible to conceive of a security management scheme that does not require a two-way communications link, these systems are very inefficient since they effectively require sending information for each vehicle to all areas of the country. Since one cannot know specifically when a given vehicle is operating, or if it has received the updates, these messages must be transmitted multiple times.

While WiMAX is a potential candidate, this technology has not seen widespread deployment, and it appears to be fading in favor of other higher capability LTE cellular technologies.

There has also been consideration of using combinations of technologies, for example broadcasting some data but using direct links for other data. An example of this approach is an internet service provided by Direct TV. In this system the user's PC is connected to a conventional low speed DSL line, and to a higher speed satellite link. Outbound data from the PC is sent over the relatively low bandwidth DSL link, and inbound data is delivered at higher speed over the satellite link. The primary motivation for this service is to serve areas that do not already have high speed landline connections.

While these schemes could potentially be made to work, they appear to be much more complex and much less well suited to the applications under analysis. If one were to use any of the candidate technologies, these schemes would be unnecessary, and the other alternative communication technologies do not appear to offer any advantage over the current candidates.

2.4.1 Cellular Communications

Cellular technology can provide wide area relatively high bandwidth communications capability. It is conceptually appropriate for V2I applications and for security management functions, however I2V messaging is problematic because the system can grow rapidly, placing a heavy burden on bandwidth. Moreover, because IP addressing, where the receiving terminal is identified, is an integral part of cellular networks, vehicles could potentially be identified, limiting anonymity. It is less effective for V2V applications because it does not provide any sort of convenient peer to peer communications capability; creating a virtual peer to peer capability would be very challenging at higher levels of deployment.

Table 11 below summarizes the strengths and weaknesses of cellular for the three categories of applications.

Table 11: Cellular Strengths and Weaknesses for Connected Vehicle Applications

Application	Strengths	Weaknesses	Comments
V2V	None	Only provides addressed point to point communications; limited broadcast capability and this is seldom implemented by carriers.	To send a message, it is thus necessary to include the IP address of the recipient along with the message. Using cellular for V2V requires that any given OBE learn the IP address of the vehicles nearby before it can send them a message. Since the vehicles around any given OBE are moving and changing all the time, the task of somehow maintaining an active IP address list for each OBE is overwhelming.

Application	Strengths	Weaknesses	Comments
<p>V2I</p>	<p>Wide area coverage means existing infrastructure can be used for many situations.</p>	<p>Requires vehicles to request V2I data based on location. This increases the overall data load because of many requests that result in null data responses. Also, messages must be sent uniquely to each vehicle on request.</p>	<p>This approach was used in the SafeTrip 21 Connected Traveler project with good results. It is unclear how well it can scale to large numbers of users.</p>
<p>Security Management</p>	<p>The widespread availability of cellular service means that most vehicles are highly likely to be in a cell coverage zone at any given time, certainly on any given day. As a result concerns about availability are minimal.</p> <p>The cellular system is intended to serve mobile users with high data transfer rates. At full 250 M unit penetration (a deployment level which is unlikely to be reached before 2030) would require 0.3 petabytes per month, less than .005% of the available system, data capacity.</p> <p>The current encryption system used for cellular service may not be sufficient to assure that data exchanges cannot be intercepted. However, this issue can be easily overcome by applying more rigorous encryption at the application layers.</p>		

Application	Strengths	Weaknesses	Comments
General	Highly available and low cost.	Requires payment for data usage.	The greatest weakness of a cellular system 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 (e.g., the Whispernet model described above), but it is unclear how this may or may not be adaptable in the context of a mandated system. Agency guidance and decision on the program is set to be made by 2013 and will guide this issue.

Because of the high transaction size requirements, we have provided a separate performance assessment for the use of cellular technology for security credential management in Table 12 below.

Table 12: Cellular System Performance for Security Updates

Requirement	Comments
Connection Duration vs. Vehicle Speed	The connection duration for cellular is impacted by the number of other users competing for use of the channel. This reduces the available user to about 2.0 Kbit/sec/user in dense environments. Under normal usage situations the system should be capable of delivering about 1 Mbit/sec user data rate. At these data rates a certificate update will take between 123 seconds and 17 hours. To avoid competition for data bandwidth it may be necessary to implement off hours certificate update protocols to use the cellular system, at off-peak usage hours.
Latency	The latency of the cellular system is about 200 msec, which does not pose any significant problem for completing any of the security management processes. It may limit the ability to support highly time sensitive applications, but, in general these applications are V2V.
Overall Coverage/Footprint	Cellular system coverage is effectively ubiquitous, so coverage is not a limiting characteristic.
Security	The existing cellular security is insufficient to secure the key and certificate transactions because it is not based on PKI, nor does it have the underlying protections needed to ensure against tracking and other security breaches.

2.4.2 WiFi Communications

WiFi technology can provide local area relatively high bandwidth communications capability. It is conceptually appropriate for security management functions and possibly V2I functions in areas where the vehicle is stationary or moving very slowly. It is not appropriate for V2V communications because it has no broadcast mechanism and it relies on the formation of a conventional network.

Table 13 below summarizes the strengths and weaknesses of WiFi for the three categories of applications.

Table 13: WiFi Strengths and Weaknesses for Connected Vehicle Applications

Application	Strengths	Weaknesses
V2V	None	<p>Requires network setup which, in a constantly changing roadway environment is infeasible.</p> <p>Also requires addressed communications which would require learning the address of all local vehicles.</p>
V2I	<p>The typical WiFi Hot Spot footprint is at most about 100 feet radius, making it "footprint-limited." For moving vehicle applications this severely limits the amount of time that the vehicle is in the hot spot. This limited access time correspondingly limits the total volume of data that can be exchanged. A hot spot is the area in which the WiFi signal is active and able to be picked up by a terminal.</p>	<p>The typical WiFi Hot Spot footprint is at most about 100 feet radius. For vehicle applications this significantly limits the number of user vehicles that will fit in the hot spot, and this thus assures a relatively high level of user bandwidth.</p> <p>WiFi involves a relatively long network attach (association) process. This limits the effectiveness of this technology since the vehicle is not in the hot spot for very long. In many situations at highway speeds, the vehicle may never complete the association process before it has exited the RF footprint. As a result, WiFi is only realistically usable in areas where the vehicle is stationary. It is thus not effective for V2I applications.</p>

Application	Strengths	Weaknesses
<p>Security Management</p>	<p>The typical WiFi Hot Spot footprint is at most about 100 feet radius. For vehicle applications this significantly limits the number of user vehicles that will fit in the hot spot, and this thus assures a relatively high level of user bandwidth. On the other hand, for moving vehicle applications this severely limits the amount of time that the vehicle is in the hot spot. This limited access time correspondingly limits the total volume of data that can be exchanged.</p> <p>Because the RF footprint is relatively small, any connected vehicle system based on WiFi would require a very large number of terminals (to assure that any given vehicle will regularly encounter an access point). Generally these access points will need to be located in areas where vehicles travel regularly and are traveling at low speeds (or are stationary). This attribute limits the effectiveness of WiFi for daily security operations.</p>	<p>WiFi involves a relatively long network attach (association) process. This limits the effectiveness of this technology since, as described immediately above, the vehicle is not in the hot spot for very long. In many situations at highway speeds, the vehicle may never complete the association process before it has exited the RF footprint. As a result, WiFi is only realistically usable in areas where the vehicle is stationary. It is thus inappropriate for on-the-fly certificate updating, and it is not effective for V2I applications.</p>
<p>General</p>	<p>The cost of a WiFi network is very low (typically about \$10 per node) although each base station typically also requires an Internet Service Provider subscription that can cost between \$50/month and several hundred dollars per month, depending on the bandwidth required.</p>	<p>Data bandwidth is generally limited by the capacity of the backhaul. Typical low cost installations will exhibit about 1.5 Mbits/sec data rate, but substantially higher rates can be achieved.</p>

The performance of the WiFi technology for security credential management is summarized in Table 14 below.

Table 14: WiFi Performance for Security Updates

Requirement	Comments
Connection Duration vs. Vehicle Speed	<p>The connection duration for WiFi is impacted by the number of other users competing for use of the channel. This reduces the available user to about 16.7 Kbit/sec/user in dense environments. Under sparse usage situations the system should be capable of delivering about 10 Mbit/sec user data rate, depending on the speed of the backhaul network.</p> <p>At these data rates a certificate update will take between 11 seconds and 2 hours, depending on the number of other network users. It may also be possible to limit use of the system to only security update transactions based on some form of network access control. This may be especially effective at fueling and charging stations since it is unlikely that many other users present will be using the network.</p>
Overall Coverage/Footprint	<p>The typical WiFi footprint is only about 30 meter radius. This small footprint, combined with the relatively long association time requires that vehicles be stationary, or nearly stationary to support the security certificate update transactions.</p> <p>The small size of the WiFi footprint means that vehicles have intermittent connectivity. It is thus necessary to distribute connection points in a way that any given vehicle will encounter at least one hot spot each day (to support misbehavior reports and CRLs) and where any given vehicle may be stationary for some time, at least once per year.</p>
Latency	The latency of any WiFi system is about 200 msec, which does not pose any significant problem for completing any of the security management processes.
Security	Existing standards for WiFi encryption are presumably sufficient to support the security management applications. Additional security protections can be easily added.

2.4.3 DSRC Technology

DSRC technology was specifically developed to support vehicular communications in a mobile environment. As a result it is well suited for most location-based messaging, both point to point and broadcast.

Table 15 below summarizes the strengths and weaknesses of DSRC for the various categories of connected vehicle applications.

Table 15: DSRC Strengths and Weaknesses for Connected Vehicle Applications

Application	Strengths	Weaknesses
V2V	N/A	N/A
V2I	<p>The relative range of DSRC means that the RF footprint is large enough to transfer most expected V2I messages. The lack of any association process also means that essentially all of the RF footprint can be used to send and receive data, and there is lower risk that the vehicle will exit the footprint before completing the association.</p>	<p>No existing infrastructure of DSRC terminals currently in the field (current installations are for experimental purposes).</p>
Security Management	<p>The relative range of DSRC means that the RF footprint is reasonably large. This means that the vehicle will be in the radio footprint for a relatively long time, and thus it can transfer a significant volume of data. The lack of any association process also means that essentially all of the RF footprint can be used to send and receive data, and there is lower risk that the vehicle will exit the footprint before completing the association.</p> <p>Because it has substantial bandwidth per channel, and multiple channels, DSRC is well suited to the large data transfers required in certificate management. This is especially the case for stationary updates where the system is expected to be highly effective.</p>	<p>Because the RF footprint is not huge, any certificate management system based on DSRC would require a very large number of terminals (to assure that any give vehicle will regularly encounter an access point). These access points can be located along the roadway so that vehicles are more likely to encounter them regularly, but the numbers required to assure regular encounters are still considered to be relatively large (>55K).</p> <p>DSRC is barely adequate to support annual certificate updates on-the-fly. This is because at road speeds over 60 km/h, the entire certificate update process is unlikely to be completed before the vehicle exits the RF footprint. More frequent updates can mitigate this weakness.</p>

Application	Strengths	Weaknesses
<p>General</p>	<p>Because DSRC can limit the use of a channel to specific applications it is possible to further dedicate an access point so that it only serves specific transactions (e.g., security, V2I, V2V, etc.). This substantially increases the available data bandwidth, and results in shorter update transactions.</p> <p>DSRC is also assumed to be used for V2V communications. Given the assumption that each device (OBE) will have a DSRC transmitter, the cost of the radio equipment on the vehicle to support security and/or V2I transactions is effectively nil. This may also limit the impact of antenna real estate on the vehicle and other related systems. If the vehicle already has DSRC for V2V, then using DSRC for certificate updates and/or V2I applications seems highly efficient.</p>	<p>DSRC is not widely deployed. Any roadside deployment would need to be funded through some mechanism; presumably either enabled by regulatory guidance, or a business arrangement</p>

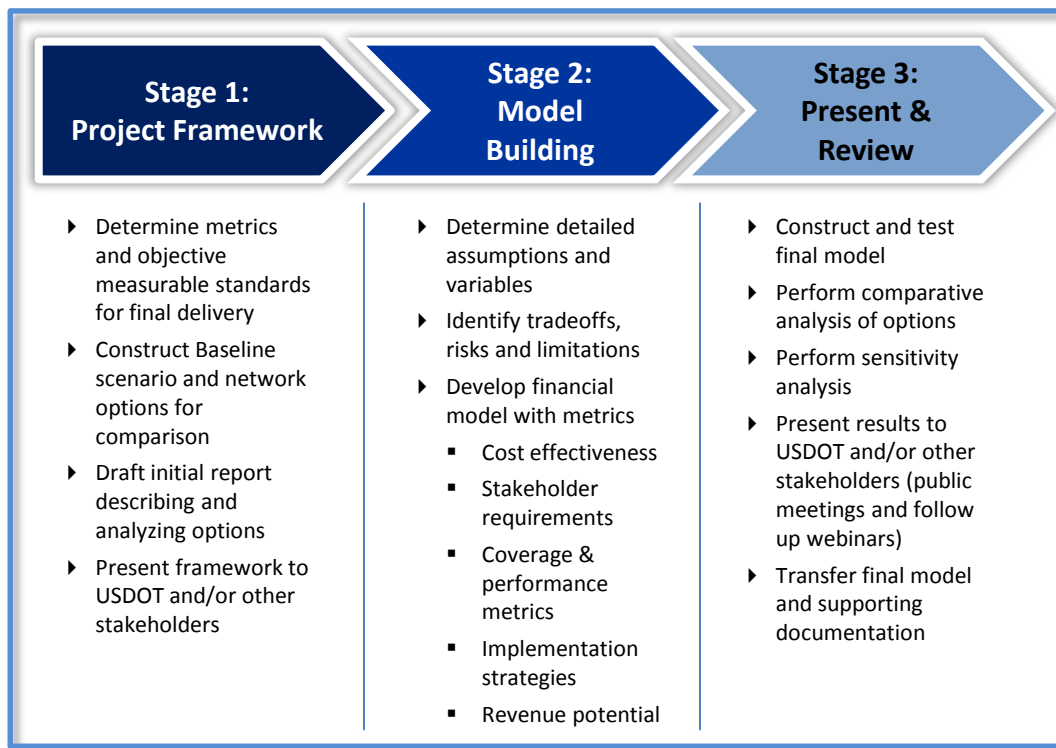
Chapter 3. Commercial/Finance Review

The commercial analysis of the CDDS is being conducted in tandem with the technical analysis in order to understand the relevant economic issues that will impact decision-making. While economic analysis itself is rarely the sole driver of decision making, it will provide valuable insight and a perspective on the relative effectiveness of the network options to deploy the CDDS. In Task 3, an examination of potential revenue sources and other cost mitigation strategies will be conducted.

3.1 Commercial Analysis Approach

The overall plan of the commercial analysis team will consist of a three-step approach, with the tools and prime output being a commercial analysis based upon comparing a baseline or status quo system, calculating the incremental advantages and outcomes of deploying a CDDS, and then outlining and comparing the network options on cost and effectiveness in attaining the system. The process flow is shown below in Figure 10.

Figure 10: Cost/Benefit Analysis



As noted in this approach diagram above, while examining the various technical options of networks that may be considered for CDDS, analyses of the various results and requirements of the overall messaging system and the costs, based on different scenarios, will be performed.

A self-supporting CDDS must have a clear value proposition for constituent stakeholders in order to be successful. For this reason, specific costs and advantages of individual potential CDDS will be assigned to participating entities, so that the sources of value in the system will be clear.

This perspective is important to highlight. We realize the difficulty of separating the costs and outcomes of a “certificate only” and a non-certificate part of the program; the two parts of the system could be viewed as symbiotic, with the certificate management portion realized as a requirement. Given this, there is a possibility of realizing a collateral benefit from the ability to use capacity beyond that needed for certificate management as a business opportunity for the public and private sectors alike. This is the view we take in constructing an analysis of the entire set of costs and values associated with the wireless delivery of certificate management, to include V2V and V2I networks. We plan to examine the possibility of other revenue sources and cost mitigation strategies from location data and the promising business opportunity offered by the concept of leveraging capacity for mobility applications on a network aimed at certificate management, justified in its build by the sum of the advantages of the Connected Vehicle Environment.

The metric of Net Present Value will be used to conduct the basic financial analysis and estimated total predicted costs and outcomes over a period of time. This concept discounts back all of the values and costs to today’s present value. This weighs costs in the short term heavily, and “discounts” future benefits to account for time value of money (essentially the ability to earn interest on money today) as well as the uncertainty of attaining future outcomes. The discount rate suggested by the OMB is 7%. As part of the total Net Present Value analysis, several assumptions and estimates have to be derived and used as the foundation for the estimates for present and future costs and benefits. Explicit articulation and explanation of those assumptions will be included in the subsequent analyses and reports.

In addition, a sensitivity analysis will be conducted. This will test each major variable for its overall impact upon the model and final results. If a small collection of variables (i.e., device costs, amount of emission of CO₂ reduced) is found to have an over-indexed impact on the Net Present Value of the model, these assumptions must be scrutinized at a higher level to ensure accuracy.

We will focus on comparing the current state of the environment, with no connected vehicle system, and thus no need for CDDS, to a vision of the various ways in which the CDDS can support a connected vehicle system. The financial trade-offs associated with those approaches from perspectives of society and the participating entities will form the foundation of the commercial analysis.

3.2 Scenario Analysis

To complete the overall analysis, several scenarios for the deployment of the CDDS have to be considered and compared to a baseline. The components of the network will be Certificate Management (the annual and monthly data loads that are delivered to vehicles), the V2I Safety and Mobility Data (vehicle communication with the infrastructure) and V2V Safety Data (vehicle communication with other vehicles).

The cellular network will rely on current wireless carriers providing capacity to be used in-vehicle. Costs will be on a data usage basis, with a per-MB or per-GB cost. This will not require heavy up-front investment to be made. Alternatively, a DSRC network would require up-front capital to build out coverage and capacity. Operating under the assumption that it is a public network, there will likely be minimal data usage costs (on a per-MB basis). However, this does not preclude the possibility of a private DSRC roadside network.

With the different components of the network (CM, V2I, V2V), there are a number of options for using the different technologies. Given the technical characteristics of the network technologies being considered, as well as reasonable commercial deployment abilities, the following scenarios will be analyzed as options to be considered by the technical and commercial teams:

Scenario One (Hybrid One)

- Certificate Management—Cellular
- V2I Safety and Mobility Data—Cellular, DSRC
- V2V Safety Data—DSRC

This scenario uses cellular for certificate management and V2I mobility communications and uses DSRC for V2I and V2V safety communications. Meeting of requirements of the system will depend on the costs of using two different networks for data delivery.

Scenario Two (Hybrid Two)

- Certificate Management—Cellular, WiFi, DSRC
- V2I Safety and Mobility Data—Cellular, DSRC
- V2V Safety Data—DSRC

This scenario uses the “wireless ecosystem” (cellular, WiFi, or DSRC) for certificate management depending on certificate management function. V2I mobility communications would use cellular and DSRC but no WiFi. The scenario uses DSRC for V2V and V2I safety communications. Wireless carrier costs will likely be on a data usage basis and particular attention will be paid to the technologies in the wireless networks today.

Scenario Three (All DSRC)

- Certificate Management—DSRC
- V2I Safety and Mobility Data—DSRC
- V2V Safety Data—DSRC

This scenario will rely on DSRC to provide the wireless data communications needed for each of the operational functions of the CDDS. The security advantages of having a “secure” system will be weighed against the costs of building a new 5.9GHz network.

***Under Development* – Scenario Four (Phased Deployment)**

This emerging scenario, referred to as the Phased Deployment option, describes at least as an initial deployment more reliance with stored certificates within the vehicle and less frequent communications. The basic communication links would remain the same as the above three scenarios, although the frequency of the delivery of the CRL and decryption keys would be different. As more detail emerges, the communication needs will be more accurately determined.

These scenarios were selected from a variety of possible options. A key driver for local area communications is the state of the vehicle (in motion or stationary). This is because a vehicle in motion may pass through and out of the relatively small communication zone before the data transaction is completed. Another key is the nature of the information being communicated. Specifically, information that is valid or used over a large geographic area may need to be accessed

anywhere over that area. Information that pertains only to a single place is most relevant when delivered at or near that place. Using a wide area communications system for locally relevant data generally means that the system must send data for all possible local points of concern (hazards, road areas, etc.) to any vehicle in the larger area. Alternatively the vehicle can contact the system and request information for the local area they are in, but this means the vehicle must continually contact the system and ask if there is new data for the local area they have just entered.

Table 16 below outlines several possible scenarios involving WiFi, DSRC and Cellular. In general none of the options using a single communications system are suitable since the nature of the communications varies widely, as described above. Similarly, options that do not limit the choices (the any and all options) are problematic since one has no knowledge of which communications systems may be used. On the one hand, if vehicles are free to choose any of the three communications systems (setting aside the fact that some are not appropriate for some types of data), then the infrastructure must support all three types in order to serve all of the vehicles. If, on the other hand, different system implementations choose different communications systems, then the vehicle must support all of the possible communication systems so that it can be assured that it will not miss any data. Neither of these approaches is economically viable.

It is also important to determine the required baseline, since it is always possible for a user, or a carmaker to establish additional services. For example Hybrid 2 differs from Hybrid 1 only in that the car can optionally use WiFi instead of cellular in some stationary settings. So, under Hybrid 2, Cellular and DSRC would be required, but one could add WiFi if it were desired. Hybrid 2 provides an additional link that the user may choose to use, but it does not allow a choice between the implementation of one link over another. The vehicle is still required to have a cellular connection. Similarly Scenario 3 assumes sufficient DSRC coverage to support all transactions, but the user can also choose to use cellular for some of these, however they still need to have the ability to use DSRC for any. Thus, these options are of the type “A and B”, not “A or B”.

Table 16 also reflects a wide area type of communication needed that has significant data volume demands. Using DSRC for certificate management also imposes substantial backhaul bandwidth limitations. To support certificate management, the RSE must be connected to the CME through some communications link. Since the data volumes for certificate update are large and the radio footprint is small, the RSE must provide high bandwidth over this backhaul link, otherwise the backhaul becomes the data bottleneck. If the number of RSEs is not large, then it is also likely that multiple vehicles will be seeking to do updates at the RSE, so the backhaul bandwidth must be multiplied to support this demand. As a result, options that assume DSRC for certificate management will require a large rollout of DSRC roadside equipment (to assure that vehicles will encounter RSEs regularly enough to get the security data they need), and these RSEs must support relatively high bandwidth (and consequently expensive) backhaul links.

Of these options Scenario 3 is the most viable. It matches the wide area need applications (remote V2I, including certificate management) with a wide area system (cellular), and it applies a local area system (DSRC) to local area applications (V2V and local V2I, such as provision of SPaT).

Other options are possible, but each has technical limitations and/or economic and scalability issues.

Table 16: Possible CDDS Scenarios

Scenario	Technologies	On-Road In-Motion			Stationary	Strengths	Weaknesses
		V2V	Localized V2I/I2V	Certificate Mgmt	V2I/I2V		
Hybrid 1 <ul style="list-style-type: none"> Cellular or DSRC for All V2I/I2V DSRC for all V2V Cellular for Cert Mgmt 	Cellular		●	●	●	<p>Can support security management for V2V, no concerns about geographic access or update periods.</p> <p>Inexpensive.</p>	<p>Requires addressing cellular access issue.</p> <p>Cellular support for localized and time critical applications may be problematic (requires relatively high bandwidth and large location server base to support billions of requests – not necessarily an issue in today’s Big Data world).</p>
	WiFi						
	DSRC	●					
Hybrid 2 <ul style="list-style-type: none"> DSRC or Cellular for V2I/I2V DSRC for all V2V Cellular, WiFi or DSRC for Cert Mgmt 	Cellular		●	●	●	<p>Same strengths as Hybrid 1.</p> <p>Adds flexibility of low cost WiFi access for stationary transactions to Hybrid 1.</p>	<p>Same weaknesses as Hybrid 1.</p> <p>Requires addressing WiFi access issue.</p> <p>May require regulations governing public WiFi access points.</p>
	WiFi			●	●		
	DSRC	●					

Scenario 3 <ul style="list-style-type: none"> • DSRC for all V2I/I2V • DSRC for V2V • DSRC for Cert Mgmt 	Cellular					Removes concern about cellular support for localized and time critical applications.	Requires addressing cellular access issue.
	WiFi						
	DSRC	•	•	•	•	Can support security management for V2V, no concerns about geographic access or update periods. DSRC RSEs do not require high bandwidth backhaul communications.	Requires DSRC facilities at localized points. Requires all vehicles to be equipped with cellular and DSRC to get both safety and mobility services.

Costs of the system, dependent on the various CDDS approaches, will be detailed, and will change based on estimated scenarios for deployment. The framework used for considering the Connected Vehicle Environment is the result of extensive modeling of future trends that will be performed as an extension of the work presented in this report. That analysis will include travel demand and fleet assumptions to include changes in GDP and constituent elements such as Total Vehicle Miles Traveled and anticipated fuel prices. These estimates will be made over several time periods (Near Term: now-2020; Medium Term: 2020-2030; and Long Term: 2030+). In conducting these sensitivity analyses, we will coordinate with USDOT to ensure that assumptions are consistent with others used in assessing the Connected Vehicle Environment.

Based on the framework and the estimates of needs of the system, network options will be analyzed for detailed costs, as well as the ability to meet the technological requirements and efficiently attain the requirements needed. One of the most important issues to consider in the planning for the deployment of a CDDS will be the total and ongoing costs of the network. Depending on the technical option selected for the network, there could be substantial upfront capital costs to build a network, and/or significant per-MB data and backhaul costs.

For analytic purposes, all four scenarios will be compared to a common baseline. This “status quo” baseline will be a view of the world without the CDDS being implemented. We can then compare the benefits and costs in each scenario to get a true picture of the incremental impact of the project. This result will be the net benefit (or net cost) of each scenario.

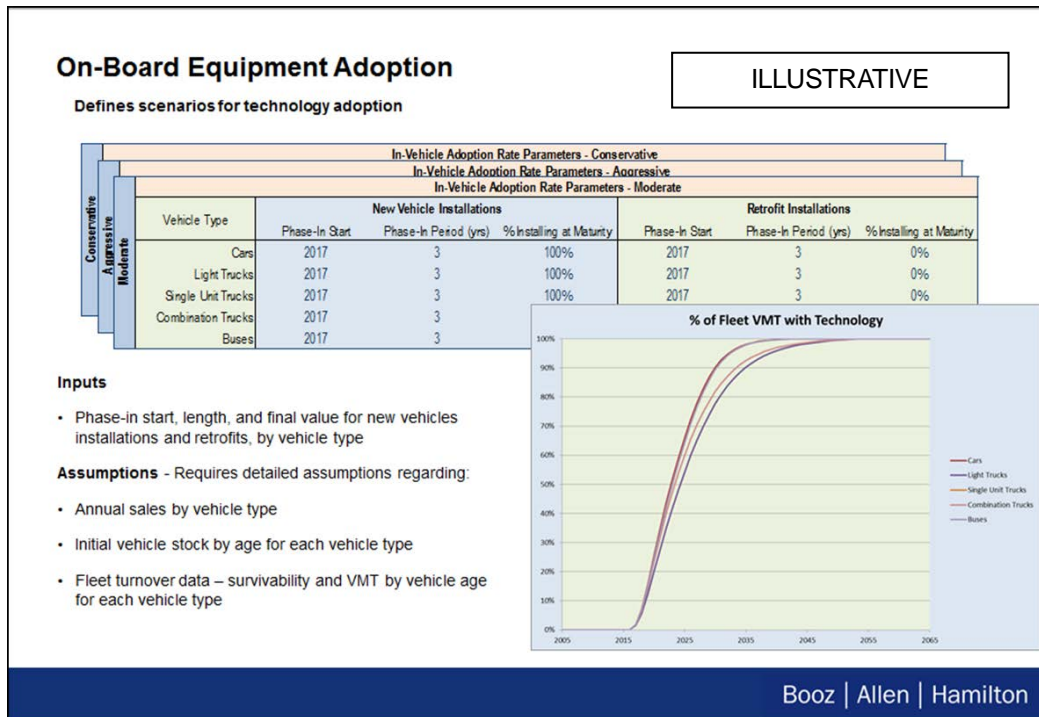
The cost assumptions from the modeling currently conducted for the AERIS (Applications for the Environment: Real-Time Information Synthesis) project for FHWA will provide the framework for the baseline scenario. The model looks at the time period from 2005 – 2055, and takes into account trends for vehicle types, roadway types, representative geographic density areas and other assumptions that impact the roadway and vehicular system. It determines the baseline and measures

the impact to the environment under a variety of scenarios. Again, the team will coordinate with representatives from USDOT to ensure that the assumptions used are consistent with other analyses conducted in association with the Connected Vehicle Environment.

The model structure and machinations will be used for the scenario analysis for the CDDS project. Key assumptions for equipment adoption, technology and cost trends as well as data usage can be input and manipulated. Sensitivities will be easily obtained by testing assumptions.

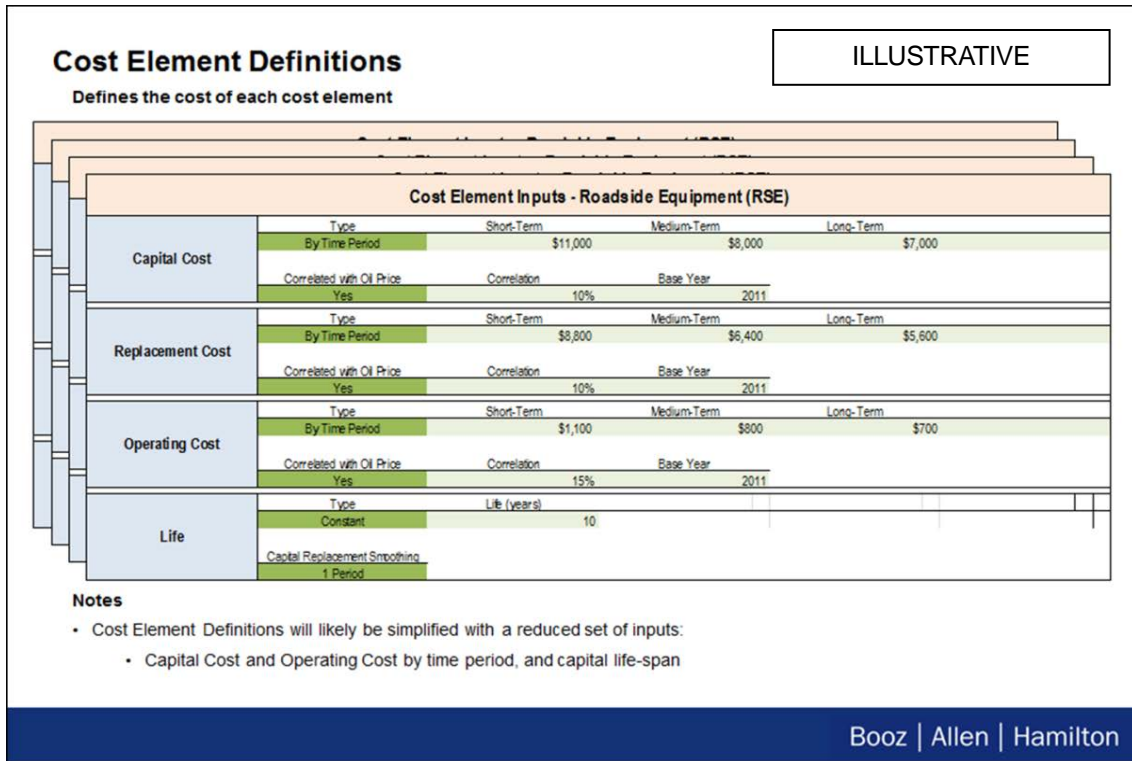
As an example, the rate of adoption and the point when a critical mass of equipped vehicles will be in place are important assumptions in the model. It not only indicates how rapidly the deployment will be attained, but also has direct cost implications. In addition, the different network solutions will have varied assumptions on how rapidly the network and devices will be implemented. The model allows different assumptions to easily be input and examined, and an illustrative example can be seen in Figure 11 below:

Figure 11: Rate of Adoption Model



In addition, the assumptions that are in the baseline AERIS model are detailed and wide in scope. These assumptions will all have impacts on the final output of the CDDS model. Specifically in the cost areas, the different network scenarios will have vastly differing assumptions that have impacts to the initial capital outlay, ongoing operating costs, device costs, technology change risk and other impacts. The model allows analysis and investigation to these areas efficiently, as seen below in Figure 12.

Figure 12: Cost Elements Definitions



Other general assumptions that will be used in the model will include all aspects of the incremental elements to effectuate the new network. The model will account for sensitivities and high/low/medium assumptions. A great amount of research has been done, and will continue, to ensure that the most accurate estimates are used in the model.

Figure 13 below lists some of the illustrative cost elements and their associated types and descriptions that are included in the model.

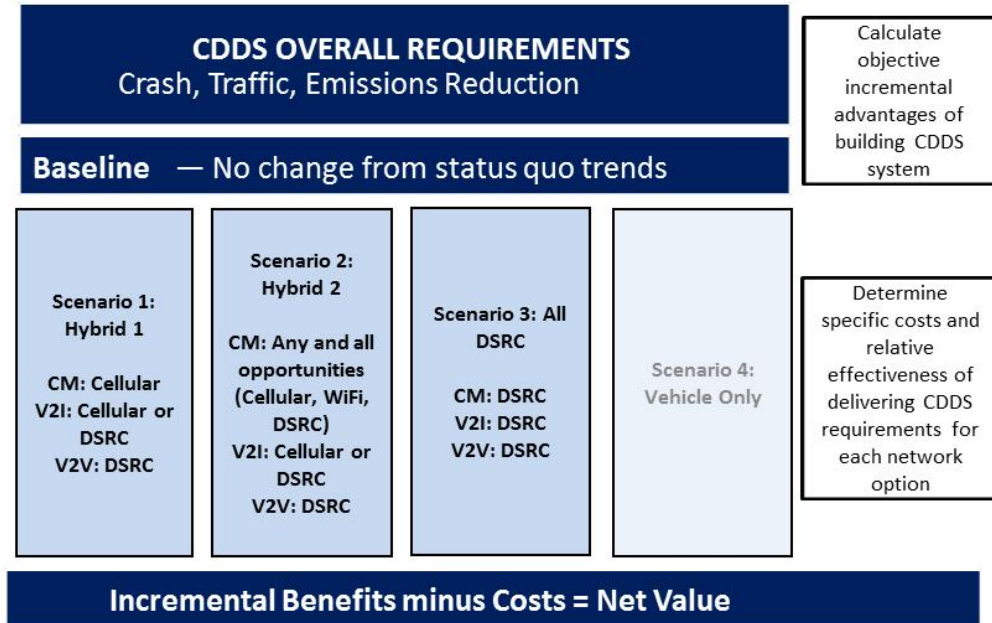
Figure 13: Cost Elements

Cost Element	Type	Description
Bill Processing	Operations	The cost of electronically processing payments and credit card "interchange fees".
Parking Enforcement	Operations	The cost of parking enforcement operations
Violation Processing	Operations	The cost of processing a violation.
Vehicle Control Computer	In-Vehicle	Any on-board computer making critical high-speed decisions about vehicle control.
Display Interface	In-Vehicle	A display with minor processing capabilities and a touch-based user interface, similar to a GPS unit.
Braking Actuator	In-Vehicle	The additional actuators and sensors required for an adaptive cruise control system compared to traditional cruise control.
Throttle Actuator	In-Vehicle	The actuator and sensors required for controlling the vehicle's throttle, as used in traditional cruise control systems.
Steering Actuator	In-Vehicle	The actuator required for lateral vehicle control.
Radar Unit	In-Vehicle	A unit for detecting the presence of vehicles ahead (and possibly around) for adaptive cruise control applications.
Real-Time Emissions Unit	In-Vehicle	This is a unit that calculates vehicle emissions in real-time based on vehicle operating information.
In-Vehicle CVN Unit	In-Vehicle	This could be an active DSRC unit installed into vehicles capable of medium/long range two-way communications.
GPS Unit, High Precision	In-Vehicle	A GPS unit capable of determining vehicle position on road.
Remote Emissions Sensor	Infrastructure	A fixed remote emissions sensor capable of detecting pollutant emissions levels by passing vehicles in real-time.
Environmental Sensor Station	Infrastructure	A station for sensing environmental conditions such as temperature, humidity, precipitation, fog, etc.
Signal Priority Installation	Infrastructure	This is the cost of installing a signal priority system on top of an existing signal controller.
Signal Controller Installation	Infrastructure	This is the cost of installing a signal controller and software at an intersection.
Dynamic Message Sign, Parking	Infrastructure	A dynamic sign used for parking space reservations, large enough to be seen from a car before pulling into a space.
Dynamic Message Sign, Transit Stop	Infrastructure	A DMS used at transit stops to provide information to passengers awaiting boarding.
Dynamic Message Sign, Freeway	Infrastructure	A DMS with a full matrix, LED, three-line, walk-in pixelated display for freeway use.
Online Presence	Infrastructure	The cost of building and operating an agency online presence dedicated to a specific purpose, such as smart parking.
Police Enforcement	Operations	The cost of additional police enforcement required for a given application.
Camera Enforcement	Infrastructure	The cost of camera-based systems for enforcement purposes, using ANPR or other techniques.
Roadside Message Sign	Infrastructure	A small to medium highway sign, including installation costs. Similar to speed limit or HOV signs.
Variable Speed Display	Infrastructure	A variable speed display sign for freeway use, using two 7-segment displays.
Dynamic Message Sign, Small Freeway	Infrastructure	A small Dynamic Message Sign (DMS) for freeway use, similar in size to an arterial DMS.
Back Office Costs	Infrastructure	The back-office costs to manage the daily operations for an application. May also be implemented as an expansion to a regional TMC.
Vehicle Presence Sensor	Infrastructure	This is the cost of a sensor for smart parking systems, as well as any power and communications equipment required.
CVN RSE	Infrastructure	This could be a roadside DSRC unit with wireless communications and a processing computer.
CVN Solar Power Unit	Infrastructure	This is a solar power unit used for remote CVN RSEs.
CVN Satellite Connection	Infrastructure	This is a satellite backhaul unit for very remote CVN RSEs.
CVN Telecom Backhaul	Operations	This is the cost of data backhaul for CVN RSEs.
CVN Network Governance	Infrastructure	This is the cost of governing the CVN network, including startup costs.
Ramp Metering Installation	Infrastructure	The cost of a ramp meter, including basic sensors, etc. Assumes upstream sensors are included in baseline.

ILLUSTRATIVE

Figure 14 below presents an illustration of the connection between benefit and cost analysis and the technical options being considered, although it is noted that to determine benefits is not a focus of the commercial analysis. Nominal values from existing literature or work will simply be plugged in.

Figure 14: Costs/Requirements and Technical Options



3.3 Analysis of Outcomes

The outcomes and value of CDDS will be translated into objective measures and discounted back to present values. Revenue and cost mitigation opportunities are discussed in the next section. For the purpose of this analysis, the team will primarily draw upon the work of the Volpe National Transportation Systems Center in the VII Benefit-Cost Analysis conducted for the ITS JPO in 2008, but with the variables updated to the latest values available via the aforementioned AERIS work. In addition, the team will incorporate the work being conducted in NCHRP 03-101, *Costs and Benefits of Public Sector Connected Vehicle Deployments* to ensure that we are consistent in approach and in the selection of values for travel time savings, injuries and fatalities, and emissions reductions.

3.4 Network Analysis

Once the monetary advantages are clearly defined, the network delivery system and the specific ability for each network option to effectuate these advantages have to be analyzed. In addition to the pure economic analysis, an examination of the implications, limitations, and risks of each option will be completed.

We have identified some of the preliminary commercial trade-off issues inherent in the various technical approaches, presented below in Table 17. These commercial issues and trade-offs build off the technical requirements and specification for each network option presented above.

Table 17: Commercial Issues

Network Strategy	Commercial Issues
DSRC	<ul style="list-style-type: none"> ▶ Building network requires intensive initial capital outlay ▶ Questions about ownership and operation of DSRC infrastructure nodes ▶ 5.9 GHz spectrum has limited coverage per distribution point ▶ Network equipment, cell towers, backhaul, maintenance and engineering are time and capital intensive, not least because of the need for right of way for placement of equipment and ongoing costs to maintain access to that land ▶ Would provide most flexibility for coverage, excess capacity revenue
WiFi Network	<ul style="list-style-type: none"> ▶ No initial capital investment required ▶ Uniform standards will lead to low per-unit pricing for devices ▶ Many different lease arrangements to be completed for nationwide coverage ▶ Spotty coverage, especially around highways, will require supplemental network
Cellular	<ul style="list-style-type: none"> ▶ Existing model of “wholesaling” capacity on a \$/MB or \$/GB basis could be used ▶ Contracts with national carriers (ATT, Verizon, Sprint) are commonplace ▶ Uniform technology allows lower-cost devices ▶ Most rapid path to nationwide coverage, networks designed for automobile coverage ▶ Ability to upgrade to 4G technology over time, as coverage improves
WiMAX	<ul style="list-style-type: none"> ▶ 4G technology with lowest per-MB cost ▶ 130MM people covered by current Clearwire/Sprint network, only major metro areas ▶ Limited ecosystem for devices ▶ Technology shift to LTE imminent

3.5 Network Modeling Issues

Conducting commercial analysis and building a financial framework by estimating the size, cost and benefit of a network is a complicated task, given the customization and specificity of building networks to meet technical requirements. Several factors limit broad assumption-making including individual market terrain, spectrum propagation characteristics, technological change, changing market pricing, and other factors.

Some major assumptions that have to be investigated and calculated will have a major impact on the results of the analysis. We can make reasonable and transparent assumptions about the areas presented in Table 18 below.

Table 18: Areas Allowing Reasonable Assumptions

Issue	Comment
Bandwidth Requirements	<ul style="list-style-type: none"> ▶ Precise calculations regarding packet size, delivery mechanism, payload and frequency to determine total amount of bandwidth are required per network option ▶ Network costs are determined by total number of MB/GB/TBs that are delivered through the system
Devices	<ul style="list-style-type: none"> ▶ Device cost will be determined by technical requirements, network technology, safety measures, installation procedures, scale, upgrade requirements, volume and total lifetime ▶ Other Policy, Legal and Technical team issues will impact device costs
Coverage	<ul style="list-style-type: none"> ▶ Total coverage requirements (ranging from ubiquitous national coverage to metro coverage) will inform technology and network selection ▶ Costs and benefits also impacted by coverage (i.e., less benefit if some locations not covered)
Time to Implement	<ul style="list-style-type: none"> ▶ Costs and benefits are impacted by roll-out schedule and how long it takes to get all cars and locations equipped for data delivery ▶ Schedule of implementation will be key assumption in benefits and costs
Network Management	<ul style="list-style-type: none"> ▶ Depending on technology and network selection, active network management costs (maintenance, backhaul, upgrade, etc.) will have to be managed and controlled

3.6 Network Deployment Challenges

Recognizing that a data communications delivery system must be employed in order for the connected vehicle system to operate, consideration of various networking options imply various challenges. It is important to recognize that beyond the value of providing a system/network upon which to distribute needed messages and certificates, there will be additional value in the data collected, and/or in the excess capacity that the system will be able to generate, and ways to leverage those data and the system could potentially be used to offset the costs. We begin with a discussion of the two major costs and obstacles in deploying a robust network: the network build and the device/user deployment.

Any original network build, generally, is incredibly capital intensive. Wireless operators have to invest billions of dollars in network infrastructure and spectrum before any revenue is realized. A wireless network has to be built out to a sufficient coverage level in order for the network to have value, and often virtually the entire network must be built before the wireless operator will launch services. An operator generally cannot launch an “almost ready” or spotty network, because customers would immediately see the deficiencies. Empirically, it has been shown to be very difficult to regain customers’ trust following a disappointing network deployment.

The second major challenge in launching wireless networks is the ability to obtain wide scale adoption of devices. One indirect measure of a network’s value is the number of participants in that network. To realize this value, it is important to get as many users on the network as quickly as possible. The high

device cost (usually subsidized by the wireless carriers in commercial markets) dampens the rapid, widespread proliferation of new users.

For these reasons, it is imperative for wireless operators to generate as much revenue as possible out of wireless networks. Whether new services are introduced to current customers, new markets are discovered (e.g., machine to machine traffic, SmartGrid services) or new devices are introduced (e.g., wireless connectivity to laptops and tablets, personal hotspots), **wireless carriers continually look for new revenue sources to exploit the wireless networks. Some of the costs and challenges may be offset by the potential for additional revenue or opportunities to connect to users based on the entire Connected Vehicle Environment.**

3.7 Revenue and Cost Mitigation Opportunities

If a network solution is deployed for the delivery of CDDS data, regardless of the technology used to deliver the data, there will be the potential to realize additional advantages from that network. While the network system will first have to deliver CDDS data effectively to garner the safety, traffic reduction, and emission reduction benefits, the existence of the network will provide the potential for external benefits as well.

Several potential business models exist that would assist in defraying costs of the network. Wireless carriers could potentially provide some network access for little or no cost (i.e., the carriers could provide 50MB per year for safety and certificate purposes). In exchange, the carriers would have access to the 250 million embedded cars in order to provide commercial services.

There are three major areas where value to third parties may be present:

- 1. Making location data available to third parties in a way that protects consumers appropriately from unwarranted privacy risks***
- 2. Monetizing any capacity that is delivered in the CDDS network which can be used for commercial applications***
- 3. There are specialized services beyond the V2V “safety of life” services that could be delivered to vehicles that the users could potentially find valuable***

Data collected or delivered to vehicles would be especially valuable. Overall penetration of wireless voice handsets is rapidly approaching 100% of the addressable market (i.e., everyone that would logically be in the market to use a mobile phone already has a mobile phone). This means that to get new sources of revenue, wireless carriers are desperately looking for new customers for new services. The connected automobile market presents a wealth of opportunities to reach new customers and potentially leverage the data that will be collected within the system.

The role of the USDOT is important to conceptualize in this framework. While the Department provides technical assistance, creates standards, develops guidance, and promulgates policies, it is likely not going to be an owner or operator of a CME system or its communication components. As such we consider opportunities for other parties, stakeholders or commercial entities as potential operators and/or owners of parts of the system.

3.8 Adding Services or Applications

A key challenge in thinking about how to monetize or leverage location data involves privacy issues. The most likely scenarios include additional (i.e., non-safety messages) opt-in or pay-for messages and services that build off the location data that are collected as part of the underlying safety system. Any commercialization or monetization of these data and other sensitive information would be dictated by customer desires and policies governing collection of personally identifiable information (PII). The market to date has shown that when connected to services that have clear value, customers seem to be willing to opt in to such services and provide vendors with PII and other sensitive information, such as credit data. Customers would have to be aware of the capabilities of data being shared, and be notified when it is happening. There would have to be a robust awareness and “opt-in” and “opt-out” systems in place to ensure that data was only being shared with consumer consent. Any use of the data would need to be consistent with the Fair Information Practice Principles (FIPPs) (NIST Special Publication 800-53, DRAFT APPENDIX J, July 2011). In addition, any additional messages sent to vehicles would have to conform to the USDOT Principles for a Connected Vehicle Environment, in which guarding against driver distraction is a key goal.

There are several ways to envision how location data may be leveraged or shared in order to provide additional value-added services or applications. For example, if data were generated that show that a high number of cars that were owned by a certain market segment traveled through a certain intersection or part of town at the same time every weekend, that data could be used to tailor broadcasted advertising messages in that area. Nonetheless, policies around awareness, acceptance and opt-in/opt-out procedures would need to be developed and validated. Regardless, there is significant potential value in linking location data with several monetize-able applications, which would imply a desire on the part of commercial organizations to at least partially invest in infrastructure and other costs associated with building and maintaining the communications network for connected vehicle programs.

Some initial examples of applications that could be provided using this data for consumers include:

- Alerting and recommending social events in a metro area
- User requests of the nearest business or service, such as an ATM, or restaurant
- Turn-by-turn navigation to any location
- Where tolls vary by time, telling users the expected cost to travel over a route at a particular time
- Reducing insurance costs by linking coverage to the user’s travel characteristics
- Locating selected people on a map displayed on the mobile phone or in-vehicle device
- Receiving alerts, such as notification of a sale in a store or warning of upcoming traffic
- Location-based mobile advertising by local establishments
- Asset recovery combined with active RF to find, for example, stolen autos
- Real-time Q&A revolving around restaurants, services, and other venues

For the carrier, location-based services could provide value by enabling services such as:

- Resource tracking with dynamic distribution
- Resource tracking for objects without privacy controls, using passive sensors or RF tags, such as packages and train boxcars
- Finding someone or something
- Proximity-based notification (push or pull)

- Proximity-based actuation (push or pull)

It is important to realize that the CDDS provides the enabling wireless network for security, and therefore, enables essential safety applications. However, there are various complementary motivations to build and operate this network. The public use cases and the potential value they hold to state, regional and local agencies and also to commercial entities may be of importance since, similar to the aforementioned use cases, they may drive the creation of a communications network that fulfills CDDS objectives, but are also supported by the CDDS.

Table 19 below lists the several USDOT Dynamic Mobility Application (DMA) and NCHRP 3-101 (Costs and Benefits of Public Sector Connected Vehicle Deployment) applications, notionally split into those requiring short range communications (such as DSRC) and others requiring longer range communications (such as cellular systems).

Table 19: USDOT DMA and NCHRP 3-101 Applications

Concept: Incremental Benefit to CDDS or Vice Versa	Short Range Communication Applications	Longer Range Communication Applications
Safety NCHRP 3-101	Cooperative Intersection Collision Avoidance (CICAS): Signalized Left Turn Assist, Traffic Signal Violation, Traffic Signal Adaptation	
Safety NCHRP 3-101	Cooperative Curve Speed Warning	Cooperative Curve Speed Warning
AERIS - Eco-Signal Operations	Eco-Traffic Signal System (ECO)	Eco-Traffic Signal System (ECO)
NCHRP 3-101	Traffic-responsive Adaptive Signal Control	Traffic-responsive Adaptive Signal Control
NCHRP 3-101	Weather-responsive Adaptive Signal Control	Weather-responsive Adaptive Signal Control
NCHRP 3-101		Arterial Network Signal Coordination
AERIS - Eco-Traveler Information	Eco-Approach to Signalized Intersections (ECO)	Eco-Approach to Signalized Intersections (ECO)
Arterial Data Environments	Intelligent Traffic Signal Systems (ISIG)	Intelligent Traffic Signal Systems (ISIG)
Arterial Data Environments	Mobile Accessible Pedestrian Signal System (PED SIG)	
Arterial Data Environments	Emergency Vehicle Preemption with Proximity Warning (PREEMPT)	
Other DMA (Regional, Corridor, Freeway)	Electronic Toll Collection System	Electronic Toll Collection System
Other DMA (Regional, Corridor, Freeway) NCHRP 3-101	Incident Scene Work Zone Alerts for Drivers and Workers (INC-ZONE) Cooperative Work Zone Speed Warning	

Concept: Incremental Benefit to CDDS or Vice Versa	Short Range Communication Applications	Longer Range Communication Applications
Other DMA (Regional, Corridor, Freeway) NCHRP 3-101	NxGen Ramp Metering System (RAMP) Adaptive Ramp Metering	
Other DMA (Regional, Corridor, Freeway)	Smart Park and Ride (S-PARK)	Smart Park and Ride (S-PARK)
Other DMA (Regional, Corridor, Freeway) NCHRP 3-101	Mileage Based User Fees (VMT) VMT-based User Fees	Mileage Based User Fees (VMT) VMT-based User Fees
Other DMA (Regional, Corridor, Freeway)		Multi-modal Real-time Traveler Information (ATIS)
Other DMA (Regional, Corridor, Freeway)		Drayage Optimization (DR-OPT)
Other DMA (Regional, Corridor, Freeway)		Emergency Communications and Evacuation (EVAC)
Other DMA (Regional, Corridor, Freeway)		Freight Real-Time Traveler Information with Performance Monitoring (FRATIS)
Other DMA (Regional, Corridor, Freeway)		NxGen Integrated Corridor Management (ICM)
Other DMA (Regional, Corridor, Freeway)	Mayday Relay (MAYDAY)	Mayday Relay (MAYDAY)
NCHRP 3-101	Real-Time Commercial Vehicle Data Exchange	Real-Time Commercial Vehicle Data Exchange
NCHRP 3-101	Real-Time Emissions Reporting	Real-Time Emissions Reporting
NCHRP 3-101		Agency App: Trip-based Traffic Studies

3.9 Economic and Business Models

In order to begin the process of understanding the possible business models to implement the CDDS, we have begun to develop approaches to resolving competing interests, in addition to identifying possible revenue opportunities. The cost of the network and device enablement has to be borne by the system. Costs should generally be borne by the entities in the system that benefit the most from the network. The ability—and appetite—for the government to take responsibility for the majority of these costs is minimal. Likewise, consumers will not respond favorably to a new tax or higher price of automobiles without seeing direct and obvious value.

Interested parties include companies that are making investments and inroads into this market space. These companies include all of the wireless carriers (Verizon, AT&T, and Sprint are all seeking new revenue sources and rely in location based services), Google (heavily vested in location-based advertising), Microsoft (location based advertising and services) and others.

By leveraging network location data or excess capacity to third parties, costs could possibly be offset and incentives for commercial investment can be developed. There are several potential models that would make this possible. First, there could be a traditional model of making anonymous location data

available to third parties that would estimate a value of the location data that is collected. Valuations of that data would have to be established, and then that data would be made available to third parties.

Another model that could potentially induce wireless carriers and other companies to build and maintain the network in exchange for access to new customers is based on excess capacity and the ability of commercial organizations to exchange messages through this capacity. An agreement with wireless network operators may be possible that would benefit all parties.

It is possible that wireless network companies may agree to maintain a network that met the government standards to provide the CDDS at no cost under certain circumstances. In exchange for this network operation, the wireless carriers may ask for access to market wireless data products to the customers with equipped automobiles. This access would be very valuable to the wireless carriers, who then could monetize that relationship with the excess data capacity that remained in the network. The team will fully analyze the current market opportunity and provide quantification of the potential value of this type of arrangement, as well implications to policy and other regulatory or oversight issues that would stem from an idea such as this one.

Device companies could potentially benefit as well. The cost of devices is expected to be very high, especially for the ultimate goal of 250 million equipped cars. As such, various models need to be established to keep this cost as low as possible. Allowing the device companies to collect data and provide services to customers with that data would be potentially very valuable.

It is important to note that to realize and implement any of the potential business models, private companies and non-government organizations would have to conform to any NHTSA guidance and the USDOT Principles for a Connected Vehicle Environment. Several requirements and guiding principles will impact the implementation and feasibility of the models and ideas outlined above, including: minimal driver distraction, safety priorities that may be impacted by leveraging and usage of excess capacity, and various other privacy, tracking and security concerns of multiple stakeholder groups.

Going forward, the team will perform a robust and detailed analysis of the various realistic options of realizing the commercial and revenue models outlined here, based on data and research into industry perspectives, technological feasibility, and costs. These parameters will be balanced by an analysis of how each model may impact the list of requirements, guidance, and stakeholder demands.

Chapter 4. Summary and Next Steps

This interim report presents analyses and research conducted to date on the exploration of various networks and systems that can be implemented for communications related to the Connected Vehicle Environment as it is deployed. We have included a thorough discussion of the technical implications of several network options, with multiple levels of analyses that highlight the potential needs of the CDDS under various operating scenarios. While working in close coordination with the development of organizational and operational models for Certificate Management Entities, the team examining CDDS options has identified a comprehensive list of considerations to account for in choosing and implementing a network.

In parallel to identifying the various technical needs, standards, estimates, and scenarios, we have begun the process of developing robust benefit-cost analytic models. Critical parts of these models will include the network and external benefits that would arise from full deployment of the connected vehicle system. Examination of costs reveals not only the network and infrastructure costs associated with expansion or implementation of any large-scale network, but also additional costs to users, the government, other organizations that may be involved in network operations, and potentially broader communities. Ways to fund and provide revenue opportunities to cover these costs and thus realize needed benefits are also under examination.

At this point in the CDDS project, we have presented initial findings on the following elements:

- Description of tradeoffs, limitations, and risks associated with each option
- Consideration of the financial viability of each option in terms of a business model that would be capable of funding deployment and ongoing operational costs – this work will continue and be more fully detailed in the subsequent tasks for this project
- Description of the initial understanding of the level of effort and challenges from organizational and institutional perspectives of the deployment – these levels of effort estimates at this point are presented as descriptive, but efforts to monetize or estimate costs associated with various inputs and levels of effort will continue during the remainder of the project
- Assessment of the feasibility of such approaches based on past practices within the telecom industry
- Inclusion of a profile of each CDDS option that enumerates the strengths, limitations, risks, and opportunities in relation to security requirements; these will be used in the subsequent models implemented and analyzed in Task 3

Recent Stakeholder Input

On April 19th and 20th, 2012, USDOT hosted a public workshop in Washington, DC to collect feedback from key stakeholders and gain insights to support this CDDS effort and the related CME project. The various discussions and sessions yielded excellent inputs from individuals representing both the public and private sectors. Table 20 below highlights some of the topic areas that stakeholders were most concerned about, and lists key takeaways from their comments and inputs.

Table 20: Key Takeaways from Stakeholders Related to CDDS

Topic Area	Key Takeaways from Stakeholders
Technical Specifications	<ul style="list-style-type: none"> ▶ The level of bandwidth available for non-safety applications when the system reaches full deployment will shape the competitive landscape for potential applications providers ▶ There is a need for risk identification and mitigation during the planning process, and for precautions such as system redundancy ▶ Many technical specifications are still outstanding, some of which include: certificate revocation policies, distribution of architecture for communications system, and certificate life span decisions (see discussion below)
Privacy	<ul style="list-style-type: none"> ▶ Privacy for users can be assured in different ways and at different levels, but regardless it is critical that the system adheres to such policy guidelines as FIPPs (see discussion below)
Implementation	<ul style="list-style-type: none"> ▶ Industry estimates for implementation of the system range from 15 to 20 years; one estimate is 20 years to reach 95% of automobiles ▶ It has not yet been determined whether a vehicle-only system or a system that includes V2I communication will be deployed initially ▶ The specific details of the roll-out process will likely be determined in large part by the owner(s) of the system
Ownership Structure	<ul style="list-style-type: none"> ▶ A strong emphasis was placed on the concept of a public-private partnership ▶ Subgroups of stakeholders felt that the government should take a lead in the stand-up of the system initially, and also that the details of any public-private partnership that develops should be transparent to all parties involved
Future Policy Decisions	<ul style="list-style-type: none"> ▶ NHTSA must ensure privacy for users and outline an economic benefit for any mandates issued to the public ▶ A decision on the potential next steps for implementation of the Connected Vehicle Program will be made by NHTSA in 2013 at the earliest.

In addition to the items listed in the table above, there are certain policy issues related to the CDDS that represent some of the most pressing matters to resolve as this project moves into its next phase. Two important points related to policy are issues of privacy and certificate life times. These issues will be further explored during Task 3, but they are briefly discussed here.

With regard to privacy, PII and location or trip traceability are the key policy concerns. The certificates used for BSM authentication do not contain any PII (i.e. information linking them to an individual user or vehicle through a requesting certificate signing request (CSR)). PII is restricted to a back-end system for registering users behind two separate layers of certificates, making it close to a non-issue. Location or trip traceability concerns relate to vehicle positioning based on BSMs sent by OBE. Policy research in Task 3 will concern the extent to which location traceability is a reasonable concern, based on public acceptability and technological feasibility, especially as it affects investment decisions to deploy the envisioned Connected Vehicle and security environment.

The second takeaway relates to certificate life times. As described in the communications system analysis of Section 2.3, the certificate life time is one of the cost drivers of the connected vehicle system, with shorter life spans requiring more certificates. The tradeoff means easier location traceability for a longer life span. More difficult location traceability is the implication for a shorter certificate life span. This comes at a higher cost of certificate issuance infrastructure. CRL size is an additional concern with short certificate life spans, although it is mitigated by the use of the LA. Longer certificate life times could eliminate the need for this additional infrastructure component. Where an LA type construct is not used, longer certificate life would cause larger CRLs. It is also important to understand that revoking certificates from a single vehicle will require greater CRL bandwidth when shorter life span certificates are used. Certificate life time will be viewed as a major policy implication, especially with regards to the tradeoffs.

Next steps for the CDDS project include:

- Examine the four scenarios going forward and determine exact technical description for each scenario in order to provide input to cost model
- Complete Cost Analysis. This will be the “baseline” case, by which the other scenario advantages and costs will be judged
- Determine detailed objective measures and assumptions consistent with CDDS technical and policy issues
- Fully investigate revenue potential models in all scenarios
- Complete a report on the tradeoffs and compromises in each scenario, from technical and commercial analysis points of view

Appendix A. Data Transfer Dynamics

Data Transfer Dynamics

Moving large files, even with reasonably high data rates, requires time. At 3 Mbps, a 10 MB file requires 25 seconds, and this is assuming no network or packet delays. Attaching to a network can sometimes take as much a 10 to 15 seconds. In a very large footprint system, such a cellular, these delays may not represent a problem, and in a stationary environment, where the vehicle is not moving relative to the network access point, these delay times are not significant, even for small footprint systems such as WiFi.

For connected vehicle applications, security management represents the single largest data transfer operation. Certificate updates and CRL updates require about 16 Mbytes of data transfer; far more than any other connected vehicle application. This section examines the characteristics of stationary and moving, or on-the-fly approaches to security management related data transfers.

As described in Chapter 1, the current security management approach requires that vehicles update certificates once per year, and update CRLs daily. We have assumed that the CRL update is typically incremental, so only the changes to the CRL are provided. If this is not the case all of the data transfer assumptions become much more challenging.

The issues for small footprint systems are:

- 1) Is the vehicle in the RF footprint for a sufficiently long time to begin and complete the data transfer?
- 2) Does the vehicle encounter a location where it can execute the transfer on a sufficiently frequent basis?

Stationary Updates

For stationary data transfers, the time in the footprint is not a significant factor other than the data transfer must be completed during a period of time that the vehicle can reasonably be expected to be either stationary, or moving (slowly) within the footprint. There are a variety of locations that vehicles visit regularly and where they are stopped during their visit.

One approach that has been suggested is to perform annual certificate updates concurrent with vehicle inspections. Unfortunately some states do not require vehicle inspections, and of the thirty five states that do, sixteen only require a biennial inspection (See Appendix B). In many cases the inspections are limited only to certain urban counties as well.

Another approach is to locate network connection point at charging stations or at shopping centers, since most vehicles will visit one of these locales at least once or twice per month, often more frequently (a singular exception being all electric vehicles that are charged only at home, which could be addressed using a home internet connection). A further analysis of how long it would take for these updates and any implications to the CDDS would need to be completed.

On-The-Fly Updates

On-the-fly updates, where the vehicle carries out the certificate update and/or access key transaction while in motion, are much more challenging. A variety of analyses carried out by the VSC indicate that a distribution of about 55K access points, placed at key locations should be sufficient to support the certificate update process while driving. It is important to point out that none of the analyses performed to date have fully addressed the non-uniform geographic vehicle distribution, so there remains the question of effectively distributing these access points so that both urban vehicles and rural vehicles will experience the same (or at least adequate) visit frequency. Urban vehicles travel in higher density corridors, so this makes it easier to predict where they are likely to travel, however, they generally travel shorter distances, so there are fewer road miles on which they may encounter an access point, and there are more road options, so assuring that all vehicles are served may require substantial density. Rural vehicles travel longer distances, and typically have fewer road choices, so identifying highly frequented locations may be easier, however, the rural environment covers a substantially larger geographic area, so the number of access point, while less dense, is still likely to be high. Further modeling and analysis is required to firmly establish the number and distribution of these access points. However, based on the 55K estimate, we can determine the basic communications parameters associated with this certificate update approach.

As with stationary updates, cellular communications will also work while the vehicle is in motion. In general, the achievable bandwidth will be slightly lower, but since the RF footprint is large (a typical cell sector is between 1 Km and 5 Km in extent), there will be more vehicles updating certificates in any given cell at any given time. WiFi and DSRC have substantially smaller RF footprints, and this significantly limits their ability to support on-the-fly updates of the scale proposed in the annual update model.

As shown in Table 21 below, at full deployment (250 M vehicles) the system will need to update 650K vehicles per day. With 55K access points distributed in a way that they are uniformly available to all vehicles, the maximum number of vehicles served by any given access point is 11.8 per day. While it is unlikely that any given access point would need to serve 11 vehicles simultaneously, it is possible that this situation could occur. If the distribution of access points is optimal, then it may be that this would be the only time that each of those 11 vehicles could update their certificates on that particular day, so 11 vehicles represents a reasonable upper bound on the average demand. It would be prudent to allow vehicles an update period spanning several days to assure that they encounter an available access point, to overcome this issue.

Table 21: On-The-Fly Update Demand vs. Population

Deployed Penetration	1%	10%	25%	50%	75%	95%
Deployed Population (M)	2.5	25.0	62.5	125.0	187.5	237.5
Vehicles Updated Per Day	6,849	68,493	171,232	342,465	513,698	650,684
Updates Per Station (55K stations)	0.12	1.25	3.11	6.23	9.34	11.83

Alternatively one can determine the likelihood that more than one vehicle will be updating at any given encounter. This depends on the number of vehicles in the RF footprint, and thus on the size of the RF footprint.

Table 22 below provides the number of vehicles within a given RF footprint diameter as a function of vehicle speed at a 1.5 second headway and assuming a nominal vehicle length of 4 meters. This obviously assumes uniform vehicle flow. It is likely that in congested situations there may be more vehicles packed more densely, but they will be moving more slowly.

**Table 22: Number of Vehicles in Footprint vs Speed
(1.5 second spacing, 4 lane road)**

RF Footprint Size (m)	Speed (km/h)				
	40	60	80	100	120
20	3.87	2.76	2.14	1.75	1.48
40	7.74	5.52	4.29	3.50	2.96
80	15.48	11.03	8.57	7.01	5.93
160	30.97	22.07	17.14	14.01	11.85
320	61.94	44.14	34.29	28.03	23.70
640	123.87	88.28	68.57	56.06	47.41

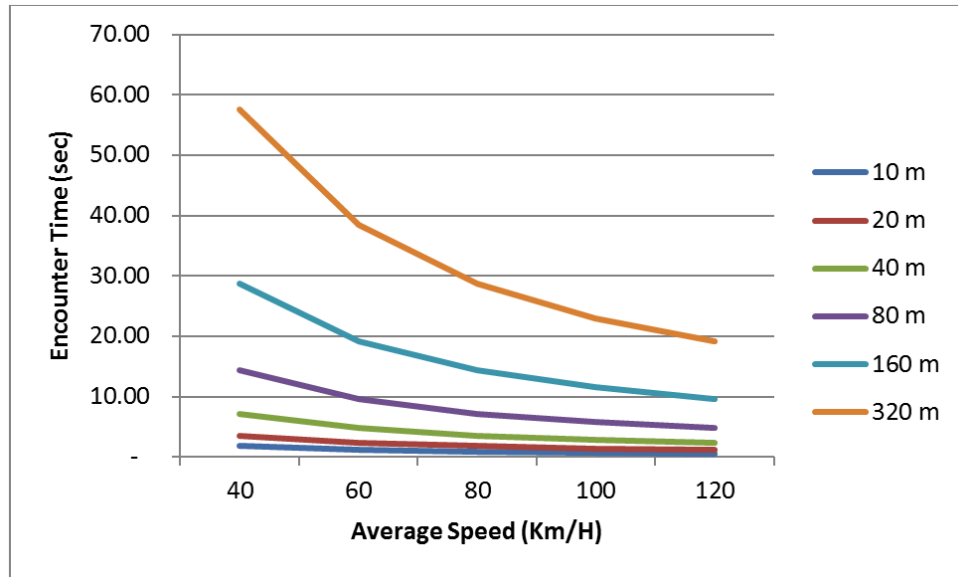
Table 23 below provides the probability that more than one vehicle will need to update at the same time within an RF footprint, as a function of the RF footprint diameter for a 4-lane road at various vehicle speeds (which impact their spacing).

Table 23: Probability of More than One Vehicle Updating vs Speed and Footprint Size

RF Footprint Radius (m)	Speed (km/h)				
	40	60	80	100	120
10	1%	1%	<1%	<1%	<1%
20	3%	2%	1%	1%	1%
40	7%	5%	4%	3%	2%
80	16%	11%	8%	7%	5%
160	30%	22%	17%	14%	12%
320	56%	43%	34%	28%	23%

Figure 15 below illustrates the encounter time, which is the period of time the vehicle is inside the RF footprint, as a function of the size of the RF footprint and the average speed of the vehicle.

Figure 15: Encounter Time vs. Vehicle Speed and RF Footprint Diameter



If only one vehicle is updating within an RF footprint, then, to transfer a 13.9 MB file at 6 Mbit/second will require an encounter time of 20.8 seconds, assuming zero network attach time (the time to connect to the network and start transferring data). From the figure above, this requires an RF footprint of at least 320 meters radius for most typical road speeds. However, as shown in Table 23 above, there is a substantial probability that, with this large footprint, at least one other vehicle will also be attempting to update. This limits the allowable speed, and thus restricts the locations at which access point should be placed. For example, if access points are located along a road with an average speed less than 60 km/h, and the access points have a 320 meter radius, then a passing vehicle has about 38 seconds to complete the update transaction. However, the probability that another vehicle will also be updating is 47%. This situation will effectively reduce the available bandwidth and will thus increase the time required to complete the update. If only one other vehicle is competing for the RF bandwidth, and both vehicles begin the transaction at exactly the same time, they will leave the RF footprint three seconds before completing the transaction. If, they are staggered by this amount of time, then they will complete the transaction just as they exit the footprint.

What this means is that if updates are performed once per year (which drives the volume of the data transaction) then on-the-fly updates must be supported by placement of access point on roads with four or fewer lanes, and travel speeds less than 60 km/h (37.5 mph). Higher speed roads and larger roads will result in more vehicles seeking to update and less overall time to complete the transaction.

It is also useful to examine the impact of more frequent updates. For example, if the certificate update is performed monthly instead of annually, the overall transaction can be completed for a single vehicle in 1.7 seconds. Examination of Figure 15 above, indicates that RF footprints as small as 80 meters will support this transaction at all legal road speeds. With an 80 meter radius footprint, the probability of more than one vehicle updating is less than 20%. At 120 km/h, the time available in the footprint is 2.9 seconds, so two vehicles could overlap their updates for about one third of the transaction time. The

probability of this occurring is less than 10%. Interestingly, at lower speeds the available time in the footprint is sufficiently high that several vehicles can update at the same time.

Increasing the frequency of certificate updates substantially improves the practicability of on-the-fly updates.

Technical Requirements Summary

There are a variety of technical requirements that affect the performance of the certificate update process. The key performance parameters are described in Table 24 below.

Table 24: Technical Requirements

Requirement	Comments
<p style="text-align: center;">Connection Duration vs. Vehicle Speed</p>	<p>The terminal must be able to connect for a period of time sufficient to allow the transaction to complete within a single transaction session. The available connection duration is a function of the local radio frequency footprint size and the vehicle speed. The allowable value is a function of the data size, the network attach time, and the channel bandwidth. If the footprint diameter is denoted by D_R, and the vehicle speed is S, then the available connect time is D_R/S. If the data load is P (bits/user), the User Data Rate is R_U (bits/user-sec), and the network attach time is T_N, the following relation can be used to bound this combination of parameters:</p> $D_R/S > P/R_U + T_N$ <p>These parameters vary depending on the approach used (e.g., stationary vs. on-the-fly, and controlled access vs. open access. See notes below)</p>
<p style="text-align: center;">Overall Coverage/Footprint</p>	<p>As described above (User Capacity/User Demand), it is assumed that the overall footprint is sufficient to allow any given terminal to encounter at least two radio frequency footprints per day (i.e., the average encounter rate is 2-3 per day) in order to provide for updating the CRL and for issuing misbehavior reports.</p> <p>Some terminals only encounter one footprint, and others may encounter more.</p> <p>The distribution of access points must be arranged to provide as nearly equal probability of access to all users across the country in rural and urban areas.</p>
<p style="text-align: center;">Latency</p>	<p>Latency must be sufficiently low to allow the terminal to connect and execute the CA transaction during the connection duration. Message latencies resulting from network routing (typically in the tens to hundreds of milliseconds) is not generally a concern for CA transactions.</p> <p>The network attach time is a form of latency, but this has been considered above in the context of allowable speed to travel through a given RF footprint.</p>

Requirement	Comments
Security	The communications technology must be able to support encrypted secure communications. As described in the various CME design documents, all communications is between parties that share a trusted relationship (the terminal and the RA), so there is no need for this data link to be secured in anonymous manner. Within the application layer, the overall message exchanges between the terminal, the RA and the CA must maintain anonymity between the terminal and the CA, but this is not a communications link issue.
CA Address Redirection	In general it is not thought to be required that the destination IP address be hidden, but this could be an added requirement.
Anonymity	Since all of the security transactions with the vehicle are between the vehicle and the RA, which includes a trusted and identified relationship, there is no requirement that the data link be anonymous.

Notes:

The requirements above depend on many factors that may be technology dependent. As noted in the table, the key requirement is that the communication system allow the vehicle to perform the transaction with the necessary frequency (which depends on the distribution of access points), and that the vehicle be able to complete the transaction during the time it is within the communications zone (which depends on a complex relationship between the number of users seeking to use the channel, the speed of the vehicle, the channel data rate, the time required to connect, and the size of the communications zone). These lower order performance parameters are described below.

Network Attach Time

The network attach time is the time required for a terminal to discover a network, obtain access information, and begin transferring data. In many cases the network management function must obtain addressing information from the terminal (e.g., a MAC address), provide supplemental addressing information (e.g., serve an IP address) and then update all members of the local network so that they can communicate with the newly attached terminal.

The allowable value for network attach time depends on the approach used (e.g., stationary vs. on-the-fly certificate updates), and on the speed of the terminal relative to the available channel data rate and the size of the communications footprint.

Channel Data Rate

The channel data rate is related to the bandwidth of the radio channel. It is a measure of how much data can be moved through the channel, assuming that the entire channel is devoted to only a single user (i.e., the maximum data rate a user can expect).

Typical channel data rates for Cellular, DSRC, and WiFi are currently about 3 to 10 Mbits/sec, although these rates are generally increasing over time as technology matures.

User Capacity and User Demand

User capacity is the maximum number of users that may access the channel at any given time. This may be limited by the nature of the channel itself, or by the physical constraints of the RF footprint, or it may be limited by dedicating a channel to the certificate update process. In this case, the number of simultaneous uses falls sharply.

Examples:

- About 250 vehicles can realistically fit inside a 600-meter diameter DSRC footprint
- About 60 vehicles can fit inside a typical WiFi footprint
- About 5,000-10,000 vehicles will typically be found in a cellular footprint

WiFi and cellular systems are used for a wide variety of applications, and neither system has any mechanism for constraining users to any particular application. This means that the available channel capacity must be shared between all possible users in the communications footprint, that is, the maximum user demand is equal to the user capacity.

DSRC has the ability to dedicate channels to particular applications (denoted by the WAVE Service Advertisement, WSA), so with DSRC it is possible to limit access to the communications footprint to only those vehicles needing to perform a security transaction. As described in Chapter 3 above, this can substantially reduce the number of users competing for the channel, thus effectively increasing the available channel bandwidth, as described below. For annual certificate updates, the maximum user demand is about two users. For monthly certificate updates it is about 1.1.

User Data Rate

User data rate is the channel data rate divided by the user demand. It is a measure of the minimum data rate that a user can expect. This value must be sufficient to allow the CA transaction to complete within the connection duration.

Determining the user data rate is complex, since generally not all users demand the channel at the same time, and in some cases the system will sequentially allocate resources to serve each user quickly but not all at the same time. However, a simple bound on user data rate can be determined by dividing the channel data rate by the user capacity. In this case we obtain the following values:

- Cellular: 2.0 Kbits/sec-user (=10 Mbit/sec/5K users) (obviously the cellular model would allocate more data bandwidth to each user for a shorter period of time, so this represents the average data rate per user)
- WiFi: 16.7 Kbits/sec-user (=10 Mbit/sec/60 users)
- DSRC Open Access: 24 Kbits/sec-user (=6 Mbit/sec/250 users)
- DSRC Restricted to Security: 3.0 Mbits/sec-user (=6 Mbit/sec/2 users)

Appendix B. State Vehicle Inspection Requirements

Table 25: State Vehicle Inspection Requirements

State	Emissions Inspection		Vehicle Inspection	
	Frequency	Requirement	Frequency	Requirement
Alaska	Biennial	Not in all areas		
Arizona	Annual	Phoenix and Tucson metro areas only		
California	Biennial			
Colorado	Annual			
Connecticut	Biennial			
District of Columbia	Biennial			
Delaware	Biennial		Annual	5 year exemption for new cars
Georgia	Annual	Metropolitan Atlanta area only		
Idaho	Biennial	Ada County (Boise) only		
	Biennial	4 year old and greater vehicles in Chicago area only		
Indiana	Biennial	Lake and Porter counties (Chicago metropolitan area) only.		
Hawaii	None		Annual	
Louisiana	Annual	Only in the Baton Rouge metropolitan area parishes of Ascension, East Baton Rouge, Iberville, Livingston, and West Baton Rouge.	Annual	
Maine	Annual	Cumberland County (Portland) only.	Annual	
Maryland	Biennial	Required in 13 (out of 18) counties and the independent city of Baltimore		
Massachusetts	Annual		Annual	
Mississippi	None		Annual	

State	Emissions Inspection		Vehicle Inspection	
	Frequency	Requirement	Frequency	Requirement
Missouri	Biennial	Required only in St. Louis City, and St. Louis, St. Charles, Franklin, and Jefferson counties	Biennial	
Nevada	Annual	Required only in Clark (Las Vegas) and Washoe (Reno) counties		
New Hampshire	Annual		Annual	
New Jersey	Biennial		Annual	Commercial Only
New Mexico	Biennial	Required only for vehicles registered in Bernalillo County		
New York	Annual		Annual	
North Carolina	Annual		Annual	
Ohio	Annual	Required only in the Cleveland metropolitan area (Cuyahoga, Geauga, Lake, Lorain, Medina, Portage, and Summit counties)		
Oregon	Annual	Required only in the Portland and Medford metro areas		
Pennsylvania	Annual		Annual	
Rhode Island	Biennial		Biennial	
Tennessee	Annual	Required only in Davidson Hamilton Rutherford Sumner Williamson, and Wilson counties, and the city of Memphis		
Texas	Annual	Required only in Houston, Dallas, Austin, San Antonio, and El Paso.	Annual	
Utah	Annual	Required Only in Weber, Davis, Salt Lake, and Utah counties	Biennial	
Vermont	Annual		Annual	

State	Emissions Inspection		Vehicle Inspection	
	Frequency	Requirement	Frequency	Requirement
Virginia	Biennial	Required only in urban and suburban jurisdictions in Northern Virginia	Annual	
Washington	Biennial	Required only in urban areas of Clark, King, Pierce, Snohomish and Spokane counties		
West Virginia	None		Annual	
Wisconsin	Biennial	Required only in Kenosha, Milwaukee, Ozaukee, Racine, Sheboygan, Washington and Waukesha counties		

Glossary of Terms

Asymmetric Key

A key that is used in an asymmetrical encryption/decryption algorithm, such that the key and algorithm used to encrypt data cannot be used to decrypt it. Asymmetric keys are generated in pairs, wherein one key decrypts what the other key encrypts. Either key can be used to encrypt or decrypt.

Broadcast Transmission

Transmitting a radio message such that anyone that can receive it can use the content. Broadcasting is typically intended to be a one-to-many mode of communication.

Butterfly Key

A pair of public and private key sets generated by the CA from the cocoon keys passed from the RA. One pair is used for signing and the other is used for encrypting.

Certificate (cert)

A digital file that contains information related to the authorized scope of activity (i.e., message type, area of operation, etc.) for the user of the certificate. A certificate includes the signature of the issuer to allow validation back to a known trusted entity.

Certificate Authority (CA)

The issuer of certificates. The CA is an entity within the PKI that established a general trusted (but not necessarily mutually identified) relationship with all other entities and users such that a message that has been certified by a CA, and which passes various authenticity and validity tests can be trusted.

Certificate Revocation List

A list of certificate identifiers, or information that can be used with a certificate identifier that corresponds to certificate that have been cancelled or revoked by the Certificate Authority. This is effectively a list of certificates that are no longer valid and that should be refused.

Channel Bandwidth

The difference between the upper frequency limit of a channel carrier and the lower frequency limit of that carrier; for example, DSRC channel 172 starts at 5.86GHz and stops at 5.87GHz making its Bandwidth 10 MHz.

Channel Data Rate

The data rate in a channel is related to the bandwidth of the radio channel It is a measure of how much data can be moved through the channel per second (nits per second), assuming that the entire channel is devoted to only a single user; i.e., the maximum data rate a user can expect.

Ciphertext

Plaintext that has been converted from a readable form into an unreadable form.

Cocoon Key

A pair of public and private key sets generated by the RA from the caterpillar keys passed from the OBE. One pair is used for signing and the other is used for encrypting.

Decryption

The process of converting ciphertext into plaintext; the inverse of encryption.

Encryption

The process of converting plaintext into ciphertext

Hash

A systematic reduction of one data set to a smaller data set using a specific algorithm. Hash values are typically independent of the size of the hashed file, and there is no way to determine the original file from the hash of that file.

Hash Algorithm

An algorithm or step by step systematic process that converts a file to fixed size bit stream.

Key

Information (typically a numerical value) that is used by an algorithm to convert plaintext into ciphertext and vice versa.

Linkage Authority

An entity in the PKI that issues linkage values such that multiple certificates issued by the CA to a particular terminal device/user can all be revoked by publishing a single revocation entry.

Misbehavior Detection

Identifying misbehaving or malfunctioning terminals based on a plurality of misbehavior reports.

Misbehavior Report

A message generated by the receiver of a message that fails a plausibility check. Such a message typically contains information about the event, and may include a copy of the message itself.

Network Attach Time

The network attach time is the time required for a terminal to discover a network, obtain access information, and begin transferring data. In many cases the network management function must obtain addressing information from the terminal (e.g., a MAC address), provide supplemental addressing information (e.g., serve an IP address) and then update all members of the local network so that they can communicate with the newly attached terminal.

On-The-Fly

Carrying out a process while the other activities are in progress. In this document it is used in conjunction with communications that are carried out while the vehicle is moving in relation to a fixed access point.

Plaintext

Human readable information, typically in numerical or text form.

Plausibility Check

A set of tests performed on a received message to determine if it is consistent with the physical world.

Point-to-Point Transmission

Transmitting a radio message such that the receiver is limited to a unique terminal; such a message is typically sent from one terminal (a point) to another terminal (point) specified by a terminal address.

Private Key

The portion of an asymmetric key pair that is maintained in secret by a user. The user's private key may be used to decrypt data that has been encrypted using the user's public key, or it may be used to encrypt data that can then only be decrypted by the user's public key.

Public Key

The portion of an asymmetric key pair that is publicly disclosed. Anyone using a user's public key can encrypt data, and that data can only be decrypted by the other portion of the asymmetric key pair; conversely anyone using a user's public key can decrypt data that has been encrypted by the other portion of the asymmetric key pair.

Public Key Infrastructure (PKI)

The aggregate of entities responsible for generating, maintaining and managing trust relationships.

Registration Authority (RA)

An entity within the PKI that has an identified and trusted relationship with the user. In this system, the RA has both identifying information as well as information that can be used to determine or verify that the user's terminal has not been tampered with or modified without authorization.

Signature

An encrypted digest (i.e., a short subset of the data in the message) of the message that is attached to a small portion of the message itself using a key that can be traced. A signature includes a certificate bearing the public key that can be used to decrypt it. This public key also has a certificate that attests to the authenticity of the public key.

Symmetric Key

A key that is used in a symmetrical encryption/decryption algorithm, such that the same (symmetric) key used to encrypt data can be used to decrypt it.

User Capacity and User Demand

User capacity is the maximum number of users that may access the channel at any given time. This may be limited by the nature of the channel itself, or by the physical constraints of the RF footprint, or it may be limited by dedicating a channel to a given operational use.

User Data Rate

User Data Rate is the data rate experienced by a single user when the channel is at full capacity. It is approximately (i.e., on average) the channel data rate divided by the Channel Capacity.

V2V Communications

The process of broadcasting messages from vehicles to other nearby vehicles.

V2I Communications

The process of broadcasting messages from roadway based systems to nearby vehicles.

Verification

The process of decrypting the digest in a signature, and comparing the decrypted digest to a digest of the actual message (generated using the same hash algorithm used to create the digest sent with the message). If the digests match, and the certificate chain can be verified to lead to a trusted entity (i.e., the CA), then the message can be considered valid (sent by the supposed sender, and unchanged from the originally sent version).

Acronyms and Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard
API	Application Program Interface
Apps	Applications
BER	Bit Error Rate
BICM	Binary Interleaved Coded Modulation
bps	Bits per Second
BPSK	Binary Phase Shift Keying
BS	Base Station
BSM	Basic Safety Message
BW	Bandwidth
CA	Certificate Authority
CAMP	Crash Avoidance Metrics Partnership
CDMA	Code-Division Multiple Access
Cert.	Certificate
CH	Channel
CICAS	Cooperative Intersection Collision Avoidance Systems
CRL	Certificate Revocation List
dB	Decibels
dBm	Decibels relative to 1 Milliwatt
dBW	Decibels relative to 1 Watt
DL	Downlink
DMA	Dynamic Mobility Applications
DOT	Department of Transportation
DSRC	Dedicated Short Range Communications
FCC	Federal Communications Commission
GHz	Gigahertz
HD Radio	Hybrid Digital Radio
Hz	Hertz (Cycles per Second)
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPsec	Internet Security Protocol
ISM	Industrial, Scientific and Medical (radio spectrum band)
ITS	Intelligent Transportation Systems
JPO	Joint Program Office
KB	Kilobytes
Kbit	Kilo Bits
Kbps	Kilobits per Second
KHz	Kilohertz
Km	kilometer
KW	Kilowatt
LAN	Local Area Network
LA	Linkage Authority

Abbreviation	Description
LTE	Long Term Evolution
M	Meters
MAC	Media Access Control
MB	Megabyte
Mb	Megabit
Mbps	Megabits per Second
MDM	Misbehavior Detection and Management
MHz	Megahertz
msec	Millisecond
nsec	Nanosecond (also ns)
OBE	On Board Equipment
OTA	Over The Air
PER	Packet Error Rate
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
psec	Picoseconds (also ps)
PTP	Point to Point
RA	Registration Authority
RF	Radio Frequency
RFC	Request for Coordination (Comments)
RFI	Radio Frequency Interference
RFID	Radio Frequency Identification
RSE	Roadside Equipment
Rx	Receiver
SAE	Society of Automotive Engineers
SAT	Satellite
SDARS	Satellite Digital Audio Radio Service
SPAT	Signal Phase and Timing
UL	Uplink
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VII	Vehicle Infrastructure Integration
WAN	Wide Area Network
WAP	Wireless Application Protocol
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Networks
WSM	WAVE Short Message
WSMP	Short Message Protocol
WSP	Wireless Session Protocol
WWAN	Wireless Wide Area Network

Bibliography

- Andrews, Scott. "Private Mobile User Security Plan". Cogenia Partners, LLC. Jan 25, 2008. Print.
- Barker, Branstad. et al. "A Framework for Designing Cryptographic Key Management Systems". National Institute of Standards and Technology. United States Government, Jun 15, 2010. Print.
- Barker, Roginsky. et al. "Transitions: Validation of Transitioning Cryptographic Algorithm and Key Lengths". National Institute of Standards and Technology. NIST Special Publication 800-131B. United States Government, Feb 2011. Print.
- Barker, Roginsky. et al. "Transitions: Validating the Transition from FIPS 1862 to FIPS 1863". National Institute of Standards and Technology. NIST Special Publication 800-131C. United States Government, Feb 2011. Print.
- Booz Allen Hamilton. "Task 2: Organizational Models for Certificate Management". Dec 9, 2011. Public Webinar Presentation.
- Booz Allen Hamilton. "Operational and Organizational Models for Certificate Management Entities as Part of the Connected Vehicle Program Draft Report (v2)". Dec 13, 2011. Report.
- CAMP – Vehicle Safety Communications 3 Consortium. "Summary of Research Results, Security Recommendations and Critical Security Inputs". VSC3 Interim Report. Dec 31, 2010. Print.
- Coulter, Ferrer. et al. "Architecture Specification for the Vehicle and Certificate Authority Certificate Management Subsystems". Telcordia Technologies, Inc. Apr 6, 2007. Print.
- Di Crescenzo, Pietrowicz. et al. "VII Vehicle Communications - Intrusion and Malicious Behavior Detection SEC 022-03". Telcordia Technologies, Inc. May 29, 2007. Print.
- Economic and Industry Analysis Division, RTV-3A. "Vehicle-Infrastructure Integration (VII) Initiative Benefit-Cost Analysis Version 2.3 (Draft)". John A. Volpe National Transportation Systems Center. United States Government. United States Department of Transportation. Research and Innovative Technology Administration. May 8, 2008. Print.
- Economic and Industry Analysis Division, RTV-3A. "Connected Vehicle Environment: Governance Roundtable Proceedings from June 20, 2011". John A. Volpe National Transportation Systems Center. United States Government. United States Department of Transportation. Research and Innovative Technology Administration. Aug, 2011. Print
- Gifford, Jonathan L., and Carlisle, W. Homer. "Data Retentions & Access Regimes for Wireless Message Logs in the U.S.: Exploratory Analysis". Transportation Research Record, No. 1879. 2004:114-119. Print.
- Mai, Andreas, and Schlesinger, Dirk. "A Business Case for Connecting Vehicles". Cisco Systems, Inc. April 2011. Report.
- McAllister, Grance. et al. "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)". National Institute of Standards and Technology. NIST Special Publication 800-122. United States Government, Apr 2010. Print.
- Narain, Burnette. et al. "Vehicle Segment Certificate Management Concept of Operations". Telcordia Technologies, Inc. Jan, 2007. Print.

- National Institute of Standards and Technology. "Security and Privacy Controls for Federal Information Systems and Organizations". NIST Special Publication 800-53 Draft Appendix J. United States Government, Jul 2011. Print.
- Oracle Corporation. "Oracle for the Connected Vehicle: Turning Data into Business". Oracle White Paper, Mar 2010. White Paper
- Peirce, Sean, and Ronald Mauri. "Vehicle-Infrastructure Integration (VII) Initiative Benefit-Cost Analysis: Pre-Testing Estimates Draft Report". Economic and Industry Analysis Division, RTV-3A. John A. Volpe National Transportation Systems Center. United States Department of Transportation. Mar 7,2007. Print.
- Pietrowicz, Di Crescenzo. et al. "VII Vehicle Segment Threat and Risk Analysis SEC 022-02". Telcordia Technologies, Inc. Jan, 2007. Print.
- Pincus, Marcia. "Intelligent Transportation Systems Benefits, Costs, Deployment, and Lessons Learned Desk Reference: 2011 Update". U.S. Government. U.S. Department of Transportation. Research and Innovative Technology Administration. Final Report. Sep 2011
- Research and Innovative Technology Administration. "Core System: Standards Recommendations Report". U.S. Department of Transportation. United States Government, Oct 28, 2011. Print.
- Research and Innovative Technology Administration. "Core System: Risk Assessment Report (RAR)". U.S. Department of Transportation. United States Government, Oct 28, 2011. Print.
- Research and Innovative Technology Administration. "Core System: System Requirements Specification (SyRS)". U.S. Department of Transportation. United States Government, Oct 28, 2011. Print.
- Research and Innovative Technology Administration. "Core System: System Architecture Document (SAD)". U.S. Department of Transportation. United States Government, Oct 14, 2011. Print.
- Research and Innovative Technology Administration. "Core System: Concept of Operations (ConOps)". U.S. Department of Transportation. United States Government, Oct 24, 2011. Print.
- Research and Innovative Technology Administration. "An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues" White Paper. U.S. Department of Transportation. United States Government, Nov, 2011. Print.
- Research and Innovative Technology Administration. "AASHTO Connected Vehicle Infrastructure Deployment Analysis" Final Report. U.S. Department of Transportation. United States Government, Jun 17, 2011. Print.
- The VII Consortium. "Final Report: Vehicle Infrastructure Integration Proof of Concept Technical Description – Vehicle". May 19, 2009. Print.
- VIIC Policy Committee. "Wireless Communications Assessment to support security requirements between Certificate Authority and Motor Vehicles for 5.9 GHz DSRC Cooperative Safety Applications". VIIC Consortium. Aug 25, 2010. Print.
- White, Mok. et al. "VII Vehicle Segment Certificate Management Scalability Analysis SEC 022-01". Telcordia Technologies, Inc. Jan, 2007. Print