USDOT Guidance Summary for Connected Vehicle Deployments

Security Operational Concept

www.its.dot.gov/index.htm
Final Report — July 2016
Publication Number: FHWA-JPO-16-338

U.S. Department of Transportation

Produced by Noblis, Inc.
U.S. Department of Transportation
Intelligent Transportation Systems (ITS) Joint Program Office

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.
The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Cover photo courtesy of ITS JPO Module 13 ePrimer Presentation (Connected Vehicles)

Technical Report Documentation Page

1. Report No. **FHWA-JPO-16-338**	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle **USDOT Guidance Summary for Connected Vehicle Pilot Site Deployments: Security Operational Concept**		**5. Report Date** **July 2016**
		6. Performing Organization Code
7. Author(s) **Michael McGurrin (Noblis)** **Kevin Gay (ITS JPO)**		**8. Performing Organization Report No.**
9. Performing Organization Name And Address Noblis 600 Maryland Ave., SW, Suite 755 Washington, DC 20024		**10. Work Unit No. (TRAIS)**
		11. Contract or Grant No. DTFH61-11-D-00018
12. Sponsoring Agency Name and Address ITS-Joint Program Office 1200 New Jersey Avenue, S.E. Washington, DC 20590		**13. Type of Report and Period Covered** Final Report
		14. Sponsoring Agency Code **HOIT-1**
15. Supplementary Notes Work performed for: Kate Hartman (ITS JPO, CV Pilots Program Manager)		
16. Abstract This document provides guidance material in regards to security for the CV Pilots Deployment Concept Development Phase. An approach for developing the security operational concept is presented based on identifying the impacts of security breaches regarding confidentiality, integrity, and availability along with the potential threats. Additional references for security analyses, V2V security, the Security Credential Management System, and connected vehicle application security needs are included. Major challenges such as SCMS integration, security for a complex system of systems, and, if applicable, payments system security are described. The document concludes with summary of USDOT technical support events.		

17. Key Words Data Privacy, Personally Identifiable Information, DSRC, BSM	**18. Distribution Statement**		
19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 16	**22. Price**

Table of Contents

List of Tables

1 Introduction

1.1 Purpose of the Report

The purpose of this report is to assist CV Pilot Deployers in the timely and successful completion of Concept Development Phase deliverables. This includes a synthesis of considerations in key topic areas, such as security. This report provides additional information and guidance to assist in the development of the Security Operational Concept deliverable. The approach recommended in this guidance is the one documented in FIPS PUB 199 and FIPS PUB 200, which is also being used in a separate study of connected vehicle applications security project funded by USDOT. Use of this approach is not mandatory. It is recommended as a widely used and accepted practice that is also being used in related connected vehicle projects.

Security is closely linked with privacy. Additional guidance on privacy issues is provided in a companion report.

This document does not replace or alter the work statement defined in the Broad Agency Announcement; it only provides technical assistance to the CV Pilot Deployers in completing the tasks and deliverables described in the statement of work.

1.2 Organization of the Report

This report contains four additional sections and a references section. Section 2 provides a general background to several key security concepts as well as several useful references. Section 3 walks through the relevant deliverables and how each of these must incorporate security considerations. Section 4 summarizes several of the key challenges that may arise when dealing with security in the CV Pilots, including methods that can be used to overcome them. Section 5 identifies several voluntary events that USDOT will provide to support the security elements of the Concept Development Phase of the CV Pilots. Finally, the Reference section identifies references that may be useful in conducting the work, including those listed in Section 2.

2 Background

The USDOT does not require the use of any specific methodology or standards, however the overall approach described in FIPS PUB 199 and FIPS PUB 200 is recommended as a starting point, as they provide a widely-used, well documented approach. A similar approach is being used in related V2I security analyses, which may make it easier to leverage this other work and reduce the effort required to develop the Security Operational Concept.

The Security Credential Management System (SCMS) Proof-of-Concept (POC) is under development by U.S. DOT, and one of the objectives of this system is to support a subset of security needs for the CV Pilots Program. Therefore, each Pilot site must interface with and use the SCMS as part of their approach to address at least a subset of the Pilot's security requirements.

2.1 Key Concepts

2.1.1 Security Assessment

The information, information systems, and communications systems that form components of the Pilot project must be assessed in order to determine the security requirements for the various components. The approach used by the Federal Government for classifying potential impacts and resulting security requirements, as defined in FIPS PUBS 199 and 200 are recommended. Regardless of the approach, the assessment must examine confidentiality, integrity and availability impacts. FIPS PUBS 199 defines these as:

- CONFIDENTIALITY: “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information.
- INTEGRITY: “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…” [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information. Non-repudiation is: preventing users from denying their actions, e.g., the ability to prove a given user took a given action, such as sending a message. Authentication is verifying the user's identity or authorization, e.g., that the message sender is authorized to send that message.
- AVAILABILITY: “Ensuring timely and reliable access to and use of information…” [44 U.S.C., SEC. 3542] A loss of availability is the disruption of access to or use of information or an information system.

The impact assessment must look at multiple types of security threats:

- Intentional threats: both internal and external
- Accidental threats: both internal and external
- Acts of nature

The approach defined in FIPS PUBS 199 then assigns a low, medium, or high impact assessment rating for each set of information in each of the three impact areas. An impact of “not applicable” may also apply for confidentiality. For example, basic safety messages (BSMs) are designed to be received by any and all neighboring vehicles as well as by roadside equipment. There is no confidentiality requirement for BSM messages. The definitions of these impact levels are provided in FIPS PUBS 199.

The impact assessment for a system is then the highest impact for any information handled by the system, scored separately for each impact area. Because some confidentiality of internal information is needed to provide integrity and availability, a system, unlike information, cannot have a confidentiality assessment of "not applicable." So, for example, a server used as part of the Pilot might have a rating of confidentiality: low, integrity: medium, and availability: medium. In theory, this means that a system could fall into one of 27 different combinations of security levels. The *Threat Definition of V2I Architecture: Confidentiality, Integrity, Availability Analysis of Sample CVRIA Information Flows* report proposes a smaller subset to reduce the need to develop security requirements for 27 different combinations. This approach is NOT required for the Pilots, but is provided as information.

2.1.2 Security Requirements

FIPS PUBS 200 defines an approach for identifying the appropriate types of security controls (high level requirements) for each security level in the three impact areas defined in FIPS PUBS 199. The document defines *minimum* requirements for *Federal* information and information processing systems. Neither the overall approach nor the specific guidance is mandatory for the CV Pilots, as they are not Federal systems. However this approach provides a well-established guide for determining the security requirements that can be used by the Pilot sites. If this approach is used, CV Pilot designers might still determine that certain controls are not needed for a specific application or system even if it would be required for a Federal system with the same security impact level. Similarly, the Pilot developer may determine that a specific application or system requires one or more security controls beyond those in the minimum required Federal requirements.

If a Pilot program utilizes the Federal approach as a model, the next step is to identify the specific security and privacy controls of each type that the system will require. These are defined in *Security and Privacy Controls for Federal Information Systems and Organizations*. Appendix J of this document addresses the closely related topic of privacy controls.

2.1.3 Public Key Infrastructure (PKI)

The Security Credential Management System (SCMS) utilizes a Public Key Infrastructure (PKI) approach to support trusted and secure communications. Public key systems use what are called *asymmetric key systems.* There are two separate but mathematically related keys. The private key is kept secret by its owner, while the public key may be distributed to anyone (hence the name public key). Knowledge of the public key does not enable anyone to derive the private key. Use of a public key system simplifies issues of key management and distribution, since public keys require no security. However an infrastructure device will be required to generate and manage its private and public keys, i.e., a *Public Key Infrastructure.*

Users can encrypt data intended for a particular recipient by encrypting it using the recipient's public key. The data can only be unencrypted by someone who possesses the corresponding private key, i.e., the intended recipient. Messages can also be digitally signed by computing a digest of the message (a mathematically computed *hash*) and using the sender's private key as input to the digital signature algorithm (RSA, ECDSA, etc). Recipients will use the message digest (computed independently from message body), the sender's public key and the digital signature attached to the message as inputs to the signature verification function. The signature verification function will compare two separate mathematical values to verify the authenticity of the signature. If the mathematical values match, then the message must have been sent by the claimed sender, as only they have their private key, and the message was not altered during transmission (since if it had been changed, the hashes would not match).

The proof-of-concept SCMS provides the public key infrastructure via elliptical curve cryptography for use by the CV Pilots. It *must* be used for at least one application in each Pilot, and can be used for as many other elements of each Pilot as is desired by the Pilot team. It is an important element of the solution for meeting the security requirements for each Pilot.

2.1.4 The Security Credential Management System

NHTSA is drafting a proposed rule that will require that all future light vehicles be equipped with V2V technology capable of transmitting BSMs which include vehicle data such as position, speed, and heading. In order for the system to be trusted, it is important to be able to verify that these messages are authentic. At the same time, privacy is very important, and the security system is being developed in such a way that prevents individual vehicles or drivers from being identified by the messages they transmit. The SCMS is a critical element of this approach. The SCMS design calls for the use of a Public Key Infrastructure (PKI) where a central authority issues credentials in the form of short-lived pseudonym certificates to certified devices (e.g., On-Board Equipment on vehicles) that possess a valid enrollment certificate. These short-lived certificates are used to sign BSMs prior to transmission. The device changes these pseudonym certificates on a regular basis over the course of each trip in order to protect the end user privacy. The purpose of attaching certificates and signing each BSM is to allow the receiver to determine if the transmitter is authorized and to ensure the integrity of the signed message. This is accomplished by verifying the digital signature on the message and verifying transmitter's short-lived certificate by following the chain of trust, verifying the transmitter has adequate credentials to send the message contents, as well as verifying that the credentials have not expired. The receiving device must also verify that the credentials of the transmitter have not been placed on a global revocation list that is managed and distributed by the SCMS.

The process for obtaining an enrollment certificate was developed in such a way that no single organization has sufficient information to re-identify a device. It will take the cooperation of two entities, e.g., in response to a court order, to re-identify a device.

The SCMS is also capable of providing Vehicle-to-Infrastructure (V2I) enrollment and application certificates to roadside units (RSUs). Application certificates are required in order for the RSU to digitally sign any messages that it transmits, such as Traveler Information Message (TIM), Signal Phase and Timing (SPAT), and MAP messages. This ensures that any device receiving these messages can verify that they were transmitted by an authorized device in the connected vehicle environment. These V2I certificates are distinct from the certificates issues to vehicles (V2V certificates) because privacy is not a requirement for roadside units as they are typically owned by a public agency or toll authority.

CAMP, LLC, as part of a cooperative agreement with USDOT, is developing the proof-of-concept SCMS. Once development is completed, this system will be set up and operated on behalf of the USDOT to support the CV Pilots and other research, field testing, and early deployment users. It is this SCMS that the CV Pilots will interface with and use. The knowledge gained through the operation and management of the SCMS POC will lead to the eventual establishment of the National SCMS. The plan for establishing the National SCMS is beyond the scope of the CV Pilots Program.

The details on the functions performed by the SCMS as well as the interface definitions are documented in several of the reference documents.

2.1.5 IEEE 1609.2: IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages

Dedicated Short Range Communications (DSRC) in the 5.9 GHz band is used for both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications (although some applications may use alternative V2I media, such as cellular communications). DSRC is defined by a set of standards, including IEEE 802.11p and the IEEE 1609 family of standards. These standards refer to DSRC communications as Wireless Access in Vehicular Environments (WAVE).

IEEE 1609.2 is a standard for the security techniques that will be used for DSRC communications.

IEEE 1609.2 specifies a set of security services available to applications and processes running on WAVE devices. WAVE Security Services include a secure data service (SDS) that transforms unsecured Protocol Data Units (PDUs) into secured Protocol Data Units (SPDUs) to be transferred between entities, and processing SPDUs on reception, including transforming SPDUs into unsecured PDUs. It also includes security management for managing information about certificates.

IEEE 1609.2-2013 is currently being updated. The latest draft is P1609.2™/D9: Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. This draft is in the sponsor ballot process and is expected to be published in spring, 2016. Two notable additions in this new version of this standard include a Certificate Revocation List (CRL) Verification Service which validates incoming CRLs and passes related revocation information for storage on the device and a Peer to Peer Certificate Distribution (P2PCD) Service that enables peer-to-peer certificate distribution.

IEEE 1609.2-2013 is available at http://standards.ieee.org/findstds/standard/1609.2-2013.html. IEEE 1609.2/D9 is currently available to IEEE 1609 Working Group members only. After publication, it will be available from the IEEE SA website.

2.1.6 Privacy

Privacy, including the protection of Personally Identifiable Information (PII), is closely linked to security. See the Privacy guidance document for additional information on privacy concepts and requirements.

2.2 Key References:

The seven key references referred to in this report are:

- *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUBS 199, February 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf. This document provides a standardized, widely used approach for assigning security categories to information and information systems. Impact categories of high, medium, and low are assigned in each of the three major security objectives for major information flows. A system’s impact categories would be the highest level found for any information flows handled by the system. The three security objectives are confidentiality, integrity, including non-repudiation and authenticity, and availability.

- Use of this approach is not mandated for the CV Pilots, however it is recommended for consideration as it is a widely used and well-documented approach that is used by the Federal government for federal systems. In addition, as noted below, this same approach is being used by USDOT to assess V2I applications, and results of that analysis can be most easily leveraged by Pilot sites if they choose to use a similar approach.
- *Minimum Security Requirements for Federal Information and Information Systems*, FIPS PUBS 200, March 2006, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf. This document builds upon FIPS PUBS 199 by defining security controls and mapping appropriate security controls to the impact levels defined in FIPS PUBS 199. The document defines minimum requirements for *Federal* information and information processing systems. These are not mandatory requirements for the CV Pilots, however they provide a well-established guide for determining the security requirements that can be used by the Pilot sites.
- *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 Revision 4, April 2013 includes updates as of 01-22-2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. This document defines specific security and privacy controls to address the security requirements identified in accordance with FIPS PUBS 200. Appendix J of this document addresses the closely related topic of privacy controls. As with the other NIST documents, use of this approach is encouraged but not required. This document will be most useful for determining specific security approaches (controls) needed in CV Pilot systems. Identification of the full set of specific controls is beyond the scope of the Security Operational Concept but this level of detail should be included in the security section of the System Requirements Specification.
- *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*, Chapter IX, V2V Security, DOT HS 812 014, August 2014, http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf. This chapter of this report provides an extensive overview and analysis of the planned security approach to be implemented for V2V communications. The same approach and the same systems, e.g., the SCMS, will be used for V2I DSRC-based communications, as well as for elements of communications using other media. Technical, institutional, and policy issues and approaches are presented and analyzed. This document provides the essential background information for understanding V2V and V2I security.
- *Vehicle Safety Communications Security Studies: Technical Design of the Security Credential Management System*, July 2013. [USDOT will provide to the CV Pilot Deployers]
- *Security Credential Management System Proof-of-Concept: Interface Protocols*, October 2015. [USDOT will provide to the CV Pilot Deployers]
- *Threat Definition of V2I Architecture: Confidentiality, Integrity, Availability Analysis of Sample CVRIA Information Flows,* This is a forthcoming USDOT report authored by Iteris, expected on or before 31 November 2015. This report utilizes the approach described in FIPS-PUB-199 to assess the security needs for five sample V2I applications and proposes four “device security classes” to simplify device development.
- This document provides a useful model for applying the approach described in FIPS-PUB-199 to V2I applications, and the specific results may also be directly useful if the Pilot project includes one or more of the five applications that were analyzed for the study.
- IEEE 1609.2-2013: IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages. This standard is available from the IEEE SA Website at https://standards.ieee.org/findstds/standard/1609.2-2013.html. The not-yet approved draft update, IEEE 1609.2/D9, is currently available to IEEE 1609 Working Group members only. After publication, it will be available from the IEEE SA website.

Additional references can be found in the References section at the end of this report.

3 Deliverables

This section describes each individual security-related deliverable by task as explained in the CV Pilots Broad Agency Announcement. While the main deliverable dealing with security is the *Privacy and Security Management Operating Concept* of task 3, elements of security need to be addressed in several of the other deliverables prepared as part of other tasks. Below are each of the tasks which could include security considerations or which drive security requirements. Security may play a minor role in other deliverables as well.

3.1 Task 2: Pilot Deployment Concept of Operations (ConOps)

The Pilot Deployment ConOps will, among other things, "describe the specific combination of applications to be deployed in the Pilot Deployment, and how operational practice will be altered based on the introduction of these applications." These security needs for the pilot systems depend upon the set of applications being provided, hence this work will be a key input to the Privacy and Security Management Operating Concept..

3.2 Task 3: Privacy and Security Management Operating Concept

The *Privacy and Security Management Operating Concept* describes, at a high level, the concepts to be implemented to meet system security and privacy needs. As stated in the BAA, "This document shall describe the underlying needs of the Pilot Deployment to protect the privacy of users, ensure secure operations, and outline a concept that addresses these needs." As described above, FIPS PUBS 199 and 200 provide a recommended (but not required) approach.

3.3 Task 5: Performance Measurement and Evaluation Support Plan

The Performance Measurement and Evaluation Support Plan is primarily a task dealing with technical aspects of the deployment. With these technical aspects such as performance measures, action logs, field data collection, and ultimately modelling and simulation, there may very well be personal information about participants. Privacy should be an active considerations in these deliverables when recording participant's location via GPS, or personal information for contact purposes (name, home address, etc…). Any personal data collected in relation to task 5 shall be planned in accordance with the *Privacy and Security Management Operating Concept* document.

3.4 Task 6: System Requirements

The System Requirements document is to include "Functional requirements: including communications, *security*, and safety requirements." (emphasis added). It provides the next level of detail on the system requirements, beyond the high level requirements that were identified in the *Privacy and Security Management Operating Concept* developed under Task 3. As described above, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 Revision 4, which documents security and privacy controls for Federal systems is an approach that can be used to document the more specific requirements that will be implemented to meet the previously identified high-level requirements. Note that this document defines minimum requirements for Federal systems, and is not binding on the Pilot sites. Each pilot site is responsible for determining their own security requirements, which will likely differ from the minimum set of requirements for Federal IT systems.

The SCMS is required to be used as part of the approach to meeting the security requirements. The SCMS will provide security certificates and related security services that can be used as part of the solution for meeting the security and privacy requirements. The proposed pilot shall utilize the SCMS for at least one of the proposed applications. As stated in the BAA, the COR will supply technical supply information on the SCMS' capabilities and interfaces.

3.5 Task 8: Human Use Approval Summary

IRB approval is a vital aspect in the CV Pilots Deployment (when necessary). Private data is often necessary when dealing with human subjects in scientific trials. For all data recorded, a plan for its use, and safe keeping should be considered. A privacy portion of the Human Use Approval Task helps to validate that private data is being managed appropriately.

3.6 Task 9: Participant Training and Stakeholder Education Plan

Similar to Task 5, private data can often be collected from individuals when training participants on technical aspects of the deployment. Private data may include name, address, role and activities of participants, and description of their activities. A plan for the participant data shall be delivered to manage privacy concerns.

3.7 Task 12: Comprehensive Pilot Deployment Plan

The final Comprehensive Pilot Deployment plan is the culmination of the material prepared from tasks 2-11 and includes "the steps to be taken to ensure the safety and privacy of participants and steps to be taken to ensure system security." Therefore the security operational concept should be summarized in this deliverable.

4 Key Challenges

The major challenges for security include:

- Balancing security needs, usability, and costs
- Security in a complex system of systems
- SCMS integration
- Payment processing (if applicable to the pilot)

This section of the orientation material will touch upon just the top few major challenges that may arise during the CV pilots, and what can be done to ensure an appropriately secure deployment.

4.1 Balancing Security Needs, Usability, and Costs

No system is totally secure. Security requires making tradeoffs among multiple factors, including security, usability, and cost. Excess security can reduce system usability while raising costs. At the same time, inadequate security can result in breaches that result in financial losses, loss of privacy, identity theft, and lack of trust in the system. For this reason, a risk-based approach that examines the types of security needed as well as the likelihood and impact of security breaches is recommended as the starting point for determining security requirements.

4.2 Complex System of Systems

The Pilots involve multiple interconnected IT systems, some of which are outside of the control of the CV Pilot team. This makes security a greater challenge, since these systems and communications links may or may not adequately address the security needs of the pilot applications. The Pilot team needs to understand the security controls put in place by these systems, coordinate with these system managers and operators, and, where needed, implement appropriate boundary security at the boundaries between systems under Pilot control and those that are not. In addition, internal security audits should be considered as a security control to pro-actively identify security breaches.

4.3 SCMS Integration

The SCMS proof-of-concept system is an external system provided by the Federal government. Each pilot must interface with the SCMS and use it as part of the security solution for at least one application. Each pilot is encouraged to use it wherever it is appropriate.

The SCMS proof-of-concept currently being developed in parallel with the CV Pilot planning phase under a cooperative agreement between the USDOT and CAMP, LLC. This increases the challenges associated with incorporating it into each pilot and adds risk. However, the interface protocols for interfacing with the SCMS are currently being documented and are expected to be available, in draft form, in the late fall of 2015. This is the key document that the pilots will need in order to interface to and use SCMS services. In addition, as described in Section 5, the USDOT is willing to conduct multiple webinars to provide additional information on the SCMS and address questions. Additional documentation on the SCMS will also be made available as it becomes available.

4.4 Payment Processing (if applicable)

Payment processing, if part of the pilot, introduces additional complexities and security needs. By nature, payment processing requires collection of personally identifiable information by some party, user authentication, and non-repudiation at some level (i.e., the ability to prove a user actually conducted the transaction). In addition, the payment card processing industry has their own standards that must be followed if applications may involve payment (e.g. credit) card transactions.

The privacy guidelines, Appendix J of *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 Revision 4 (which addresses privacy controls), and the standards put in place by the payment card industry each provide useful guides for ensuring adequate protection of personally identifiable and payment information.

5 Technical Support Summary

A series of USDOT-sponsored webinars were developed to assist early deployers of connected vehicle technologies with Concept Development activities. The webinars described below provide support for the development of the Security Operational Concept.

1. ***Preparing a Security Operational Concept for Connected Vehicle Deployments***

   This webinar presents the USDOT perspective on the development of a Security Operational Concept, a key step in the concept development phase for deployment planning. Kevin Gay of the National Highway Traffic Safety Administration describes the design concept and the requirements of a Security Operational Concept, which will address the underlying needs of the connected vehicle deployments to ensure secure operations and to protect the privacy of vehicle and device owners.

2. ***SCMS Proof-of-Concept Interface Requirements for Connected Vehicle Deployments***

   The Security Credential Management System Proof-of-Concept (SCMS PoC) is expected to provide security credential management services for USDOT Intelligent Transportation Systems Joint Program Office Connected Vehicle Pilot deployment sites. The SCMS PoC is planned to be completed and become operational in the Fall of 2016. The USDOT has released the initial version of the SCMS POC interface requirements which describes how devices will interact with the system and receive security credential materials. Kevin Gay of the National Highway Traffic Safety Administration, Benedikt Brecht of Volkswagen and Dean Therriault of General Motors describe the interface requirements documentation and provide a high level walkthrough specifically focusing on the planned enrollment and provisioning processes

To access the presentation slides and audio recordings for these webinars, please visit the technical assistance page of the CV Pilots website:
http://www.its.dot.gov/pilots/technical_assistance_events.htm.

Additionally, the *EE Requirements and Specifications Supporting SCMS Software Release 1.0* document detailing requirements and specifications for SCMS PoC protocols and components can be found on the CV Pilots website: http://www.its.dot.gov/pilots/technical_assistance_events.htm.

References

1. Connected Vehicle Pilot Deployments: Phase 1 Concept Development, Broad Agency Announcement No. DTFH6115R00003, Federal Highway Administration, January 2015.

   https://www.fbo.gov/index?s=opportunity&mode=form&id=36ac05d6be6db2c92dd77bda3965e245&tab=documents&tabmode=form&tabid=7c71a2c57d27b4c1185c15f069d80180&subtab=core&subtabmode=list&=

2. Standards for Security Categorization of Federal Information and Information Systems, FIPS PUBS 199, February 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

3. Minimum Security Requirements for Federal Information and Information Systems, FIPS PUBS 200, March 2006, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

4. Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 4, April 2013 includes updates as of 01-22-2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

5. Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application, Chapter IX, V2V Security, DOT HS 812 014, August 2014, http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf.

6. Vehicle Safety Communications Security Studies: Technical Design of the Security Credential Management System, July 2013.

7. Security Credential Management System Proof-of-Concept: Interface Protocols, expected October 2015.

8. Threat Definition of V2I Architecture:Confidentiality, Integrity, Availability Analysis of Sample CVRIA Information Flows. Forthcoming USDOT report authored by Iteris, expected on or before 31 November 2015.

9. Dedicated Short-range Communications Factsheet (USDOT) , FHWA JPO-11-034 http://www.its.dot.gov/factsheets/pdf/JPO-034_DSRC.pdf

10. Whyte et al., A Security Credential Management System for V2V Communications, 2013 IEEE Vehicular Networking Conference. http://www.cvt-project.ir/Admin/Files/eventAttachments/A%20Security%20Creential%20Management%20System%20for%20V2V%20Communications%20-%20VNC%20Conference%202013_514.pdf

11. A Security Credential Management System for V2V Communications, CAMP Vehicle Safety Communications 3, December 2013. http://www.ieee-vnc.org/2013/media/ieee_vnc_scms.pdf

12. PCI SSC Data Security Standards Overview, https://www.pcisecuritystandards.org/security_standards/, accessed Sept. 15, 2015.

13. Linke and Integrated, Using the Elliptic Curve Digital Signature Algorithm effectively, Embeded, Feb. 2, 2014, http://www.embedded.com/design/safety-and-security/4427811/Using-the-Elliptic-Curve-Digital-Signature-Algorithm-effectively, accessed Sept. 25, 2015.

14. IEEE 1609.2-2013: IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages. This standard is available from the IEEE SA Website at https://standards.ieee.org/findstds/standard/1609.2-2013.html. The not-yet approved draft update, IEEE 1609.2/D9, is currently available to IEEE 1609 Working Group members only. After publication, it will be available from the IEEE SA website.

Appendix: List of Acronyms

Table A-1: List of Acronyms

Acronym	Meaning
BAA	Broad Agency Announcement
BSM	Basic Safety Message
COR	Contracting Officer's Representative
CRL	Certificate Revocation List
CV	Connected Vehicles
CVRIA	Connected Vehicle Reference Implementation Architecture
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
DSRC	Dedicated Short Range Communications
FHWA	Federal Highway Administration
IT	Information Technology
ITS	Intelligent Transportation Systems
JPO	Joint Program Office
NHTSA	National Highway Traffic Safety Administration
PCI	Payment Card Industry
PDU	Protocol Data Unit
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POC	Proof of Concept
RSA	A public key cryptosystem named for its developers: Ron Rivest, Adi Shamir, and Leonard Adleman
RSU	Roadside Unit
SCMS	Security Credential Management System
SDS	Secure Data Service
SPaT	Signal Phase and Timing
SPDU	Secure Protocol Data Unit
SSC	Security Standards Council
TIM	Traveler Information Message
USDOT	United States Department of Transportation
WAVE	Wireless Access in Vehicular Environments

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

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

FHWA-JPO-16-338

U.S. Department of Transportation