Connected Vehicle Deployment Technical Assistance

Security Credential Management System (SCMS) Technical Primer

www.its.dot.gov/index.htm

Report – November 2019
FHWA-JPO-19-775

U.S. Department of Transportation

Introduction

Connected vehicle technologies enable vehicles, roadside infrastructure, and personal portable devices to communicate and share information through wireless communication technology. Onboard units (OBUs) installed on vehicles will continually broadcast information on the vehicle's position, direction, and speed in the form of a Basic Safety Message (BSM). These messages are received by other vehicles and used by applications to improve safety. Roadside units (RSUs) installed along the roadway will also receive and broadcast messages to further improve safety and enhance mobility.

The correctness and reliability of messages being transmitted between devices is of critical importance as it impacts the outcomes and effectiveness of safety applications based on them. Connected vehicle devices sending messages need to digitally sign their messages, and the receiving devices need to verify the signature before acting on it. To enable security in V2X systems, it is important to ensure:

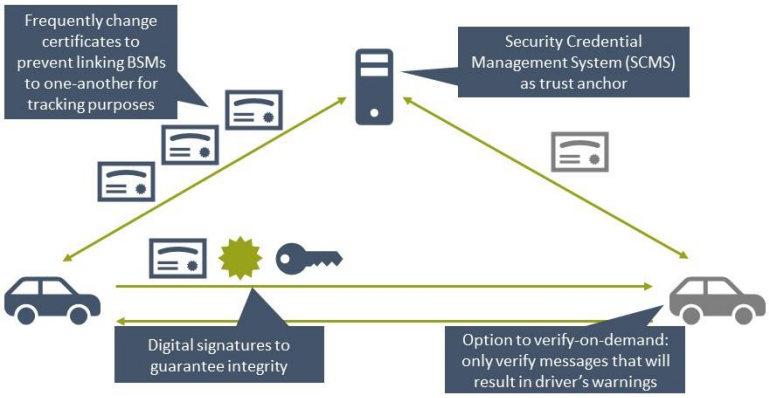

Figure 1. The SCMS Ecosystem (Source: USDOT)

1. A message originates from a trustworthy and legitimate device;
2. A message was not modified between sender and receiver; and
3. Misbehaving units are detected and removed from the system.

SCMS Overview

The Security Credential Management System (SCMS) is a critical component of this connected vehicle environment serving as a message security solution for V2X. It uses a Public Key Infrastructure (PKI)-based approach that employs specialized methods of encryption and certificate management optimized for anonymization to facilitate *trusted* communication. V2X devices enroll into the SCMS after completing device certification processes that validate the devices as trusted players in the system; obtain security certificates from certificate authorities (CAs); and attach those certificates to their transmitted messages as part of a digital signature. Authorized system participants use digital certificates issued by the SCMS to authenticate and validate the safety and mobility messages that form the foundation for connected vehicle technologies. To protect the privacy of vehicle owners, these certificates contain no personal or equipment-identifying information but serve as system credentials so that other users in the system can trust the source of each message. The SCMS also plays a key function in protecting the content of each message by identifying and removing misbehaving devices, while still maintaining privacy.

The Basics: Cryptography and PKI

Cryptography is the practice and study of techniques for secure communication in the presence of third parties, called adversaries. There are two primary types of cryptography – symmetrical and asymmetrical.

- **Symmetrical Cryptography:** This encryption technique uses the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption.
- **Asymmetrical Cryptography:** This encryption technique uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. By using a different key, this prevents someone from creating a decryption key from the encryption key and helps the encrypted data stay even more secure. In such a system, any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

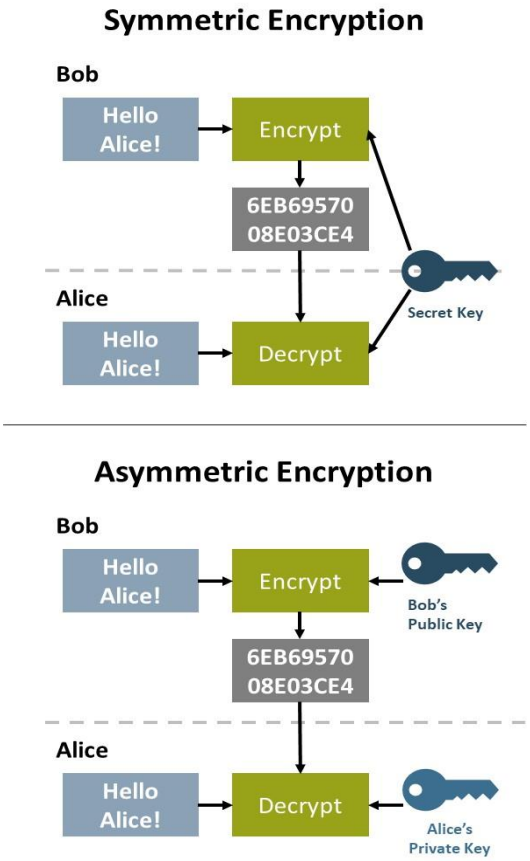

Figure 2. Symmetric and Asymmetric Encryption (Source: USDOT)

In cryptography, an important issue is confidence/proof that a particular public key is authentic, i.e., that it is correct and belongs to the person or entity claimed and has not been tampered with or replaced by a malicious third party. There are several possible approaches to ensuring confidence including the use of PKI, in which one or more third parties – known as certificate authorities (CAs) – certify ownership of key pairs. PKI encompasses a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption.

The certificate authority issuing the certificate must be trusted to have properly checked the identity of the key-holder, must ensure the correctness of the public key when it issues a certificate, must be secure from computer piracy, and must have made arrangements with all participants to check all their certificates before protected communications can begin. Aside from the resistance to attack a particular key pair, the security of the certification hierarchy must be considered when deploying public key systems. A certificate authority vouches for the identities assigned to specific private keys by producing a digital certificate.

SCMS Security and Design Considerations

The SCMS is distinguished from traditional PKI in several aspects – its size (i.e., a connected vehicle PKI-system would be the largest deployed to support over 300 million vehicles) and the balance among security, privacy, and efficiency. Besides its standard functionality as a PKI system, the SCMS is designed to handle the following types of attacks:

1. Attacks on end users' privacy from SCMS outsiders;
2. Attacks on end users' privacy from SCMS insiders; and
3. Authenticated messages leading to false warnings.

The first two items are addressed by "Privacy by Design". The third item is addressed by "Revocation", which uses misbehavior detection and a reporting scheme to identify devices to revoke.

- **"Privacy by Design":** A key goal of the SCMS is to protect the privacy of end users. To maintain privacy against attackers from outside the SCMS, certificates need to change (e.g., every X minutes). Another key requirement is that attacks should be difficult to mount for SCMS insiders. Thus, the SCMS operations are divided among different components, and those components are required to have organizational separation between them.
- **Misbehavior Detection and Revocation:** Misbehavior Detection is the process for identifying devices that send messages that could cause malicious events within the connected vehicle environment. There is a current minimum viable misbehavior detection capability that exists and utilizes basic algorithms to analyze Basic Safety Messages (BSM) to determine misbehavior. Devices that support misbehavior detection would then send a misbehavior report to the SCMS, where SCMS operators can act on those reports and potentially add a misbehaving device's certificates to the certificate revocation list (CRL). The CRL is used by connected vehicle devices to reject certificates from a misbehaving device. A CRL is a list of digital certificates that have been revoked by the issuing https://en.wikipedia.org/wiki/Certificate_authorityCertificate Authority before their scheduled expiration date and should no longer be trusted. A certificate is irreversibly revoked if, for example, it is discovered that the Certificate Authority had improperly issued a certificate, or if a private key is thought to have been compromised. Certificates may also be revoked for failure of the identified entity to adhere to policy requirements, such as publication of false documents, misrepresentation of software behavior, or violation of any other policy specified by the Certificate Authority operator or its customer.

SCMS Structure

The SCMS structure (see page 4) features the following components depicted by their logical roles. An implementation of the system may combine multiple roles within a single organization with proper separation of the logical roles.

- **Certification Services:** Provides information on which types of devices are certified to receive digital certificates and specifies the certification process.
- **CRL Store:** Stores and distributes CRLs. This is a simple pass-through function since CRLs are signed by the CRL Generator.

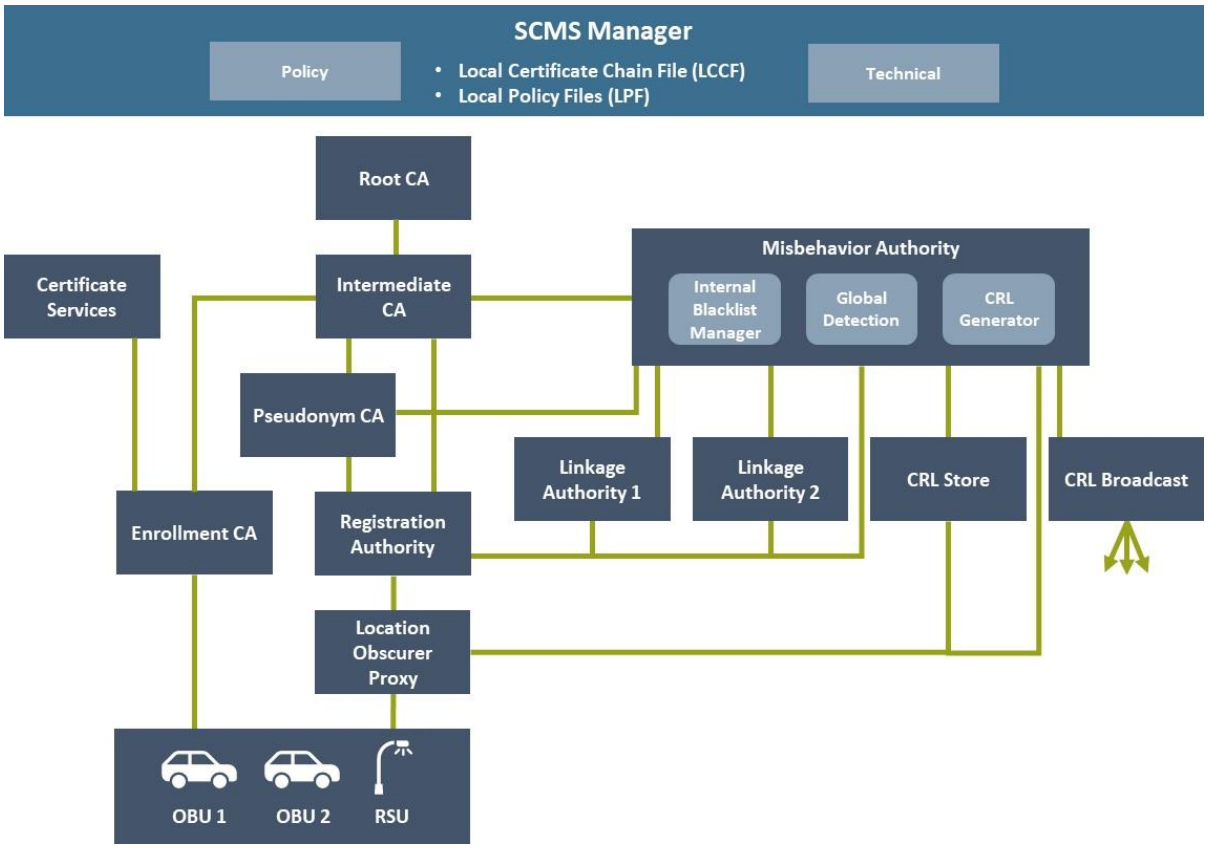

Figure 3. SCMS Structure (Source: USDOT)

- **CRL Broadcast:** Broadcasts the current CRL, may be done through roadside unit (RSUs) or satellite radio system, etc. This is a pass-through function. Devices download new CRLs through the Registration Authority every time they connect to the SCMS.
- **Enrollment CA (ECA):** Issues enrollment certificates, which act as a passport for the device and can be used to request pseudonym certificates. Different ECAs may issue enrollment certificates for different geographic regions, manufacturers, or device types. The ECA is only utilized during the enrollment of a device. After enrollment, devices will not need to connect to the ECA.
- **Linkage Authority (LA):** Generates linkage values, which are used in the certificates and support efficient revocation. There are two LAs in the SCMS, referred to as LA_1 and LA_2. The splitting prevents the operator of an LA from linking certificates belonging to a particular device. The linkage authorities are internal devices that a connected vehicle device will never need to interact with.
- **Location Obscurer Proxy:** Hides the location of the requesting device by changing source addresses, and thus prevents linking of network addresses to locations. Additionally, when forwarding information to the Misbehavior Authority, the Location Observer Proxy shuffles the reports to prevent the Misbehavior Authority from determining the reporters' routes.
- **Misbehavior Authority (MA):** Processes misbehavior reports to identify potential misbehavior by devices, and if necessary, revokes and adds devices to the CRL. It also initiates the process of linking a certificate identifier to the corresponding enrollment certificates and adding the

enrollment certificate to an internal blacklist. The Misbehavior Authority contains three subcomponents: Internal Blacklist Manager, which sends information required for updating the internal blacklist to the Registration Authority; Global Detection, which determines which devices are misbehaving; and CRL Generator, which issues certificate revocation lists to the outside world. Connected vehicle devices that have a misbehavior detection capability will send their misbehavior reports to the MA through the Registration Authority (RA) whenever they are in range of an RSU that supports SCMS connections.

- **Pseudonym CA (PCA):** Issues short-term (pseudonym) certificates to devices. Individual PCAs may, for example, be limited to a particular geographic region, a particular manufacturer, or a type of devices. The PCA will provide pseudonym certificates to connected vehicle devices when requested, through the Registration Authority. The PCA will generate 3 years' worth of pseudonym certificates for each connected vehicle device, and then add a new weeks' worth of certificates every week to ensure there are always 3 years of certificates available.
- **Registration Authority (RA):** Validates, processes, and forwards requests for pseudonym certificates to the Pseudonym CA. This is the part of the SCMS that all connected vehicle devices will interact on a regular basis. All requests for certificates as well as certificate and file downloads occur at the RA.

Types of Certificates

The SCMS is responsible for issuing certificates to devices through the RA to connected vehicle devices. The SCMS makes use of several certificate types depending on whether the connected vehicle application is installed on a vehicle or RSU. There are three types of operational certificates:

- **OBU Pseudonym Certificates:** Pseudonym certificates are short term and used primarily to sign Basic Safety Messages (BSMs). They are downloaded in batches, are valid for one week and rotate on a set basis (e.g., distance traveled, time since last certificate change). For privacy reasons, a device is given multiple certificates that are valid simultaneously, so that it can change them frequently. The SCMS generates and keeps 3 years' worth of pseudonym certificates available for devices to download. Some security profiles are configured for downloading a varying number of weeks' worth of these certificates to a vehicle at a time, typically based on how often an OBU is likely to communicate with an RSU that can provide the updated certificates. At this time, batch frequency and size is universal.
- **OBU Identification Certificates:** These certificates are used in the same way as pseudonym certificates, but for vehicles with special privileges that don't require anonymity (e.g., police vehicles, ambulances, fire trucks, transit vehicles, etc.). OBUs use identification certificates primarily for authorization in V2I applications, such as signal pre-emption for emergency vehicles. As there are no privacy constraints for identification certificates, an OBU has only one identification certificate valid at a time for a given application.
- **RSU Application Certificates:** Application certificates are used by an RSU to sign any over-the-air messages transmitted, such as signal phase and timing or traveler information message. As there are no privacy constraints for RSUs, an RSU has only one application certificate valid at a time for a given application. These certificates are used to sign the different types of messages an RSU may broadcast including: Signal Phase and Timing (SPAT), MAP and Traveler Information

Message (TIM). Devices typically have an active, valid certificate for one week and have another week in reserve. Application Certificates are tied to a Provider Service Identifier (PSID).

For connected vehicle devices to receive and use certificates, each device must have: (i) software associated with signing, authenticating, encrypting and decrypting (governed by IEEE 1609); (ii) software to generate public-private key pairs and create the requests for the SCMS to generate enrollment, pseudonym, application and identification certificates to be used by the first software block; and (iii) a *Hardware Security Module (HSM)* to securely store private keys. A HSM is a specialized, physical computing component or device that safeguards and manages digital keys for strong authentication and provides crypto-processing.

In addition to certificates, there are other files associated with the SCMS that devices will use. These files are updated whenever a device communicates with the SCMS Registration Authority (RA). These files serve as administrative/policy files that are defined by the SCMS Manager (see graphic on page 4).

- **Local Certificate Chain File (LCCF):** Provides the chain of trust for certificate authorities to trust. This allows devices to trust certificates generated from other certificate authorities.
- **Local Policy Files (LPF):** This file provides key configuration items associated with the SCMS and include: (i) number of pseudonym certificates granted per week and (ii) certificate validity periods. These are generally negotiable with the SCMS provider.

The SCMS Process

The SCMS process can be summarized in three parts: (i) enrollment, (ii) normal operations, and (iii) misbehavior detection. More details of each part are described below.

Enrollment

The enrollment process, also referred to as bootstrapping, is the first step in getting a device connected to the SCMS. During enrollment, a device will create a public or private key pair and produce an enrollment request that includes its public key. The public key is signed with its private key, which will be sent to the SCMS and await the enrollment request response. The SCMS will respond with an enrollment private key reconstruction file, so the device can create its enrollment public-private key pair. This process requires a secure physical environment, because keys are being exchanged. Device vendors generally conduct the enrollment or bootstrapping process themselves to ensure it is done securely.

Normal Operations

Once a device has valid enrollment credentials it can start requesting operational certificates. Devices will connect through a normal network connection to an SCMS Registration Authority (RA) to request new certificates. The RA is an intrinsically, non-central component of the SCMS. There may be multiple RAs active at any given time in the SCMS. Requesting new certificates is done via normal HTTPS protocols. For OBUs, they will need to connect to the SCMS via an RSU that advertises either the SCMS service or an IP service. The SCMS generates and stores three years' worth of pseudonym/identification certificates. Each week, a new weeks' worth of certificates is generated and added. (*Note:* OBUs can download however many weeks' worth of certificates the device vendor configures, up to 3 years.) The

SCMS generates application certificates only up to a week in advance, so RSUs will be required to connect to the SCMS on a more regular basis to request new application certificates.

Certification Revocation

There is currently an effort to develop a Minimum Viable Product (MVP) version of a Misbehavior Detection system to support the CV Pilot programs. This system utilizes simple algorithms to analyzed received BSMs to determine misbehavior. If a device detects misbehavior, it will generate a misbehavior report that is sent to the Misbehavior Authority (MA). An MA operator will then review those reports, and in accordance with processes and procedures agreed to by the CV Pilots and USDOT, add misbehaving devices to the CRL. CRLs identify those certificates from devices that are no longer considered trustworthy. Devices will download CRLs from the SCMS, via RSUs, and will check received message certificates against the CRL to determine validity. CRL updates are downloaded whenever a device connects to the SCMS. The SCMS, utilizing the linkage authorities, can identify all of the certificates generated for a device based on a pseudonym certificate. This is a process that will only occur if a device has been identified as misbehaving, through an automated misbehavior detection system, or a device is manually reported by the agency that owns that device (e.g. – if the device were stolen or ownership is being transferred, the device produces erroneous data.).

Lessons Learned from Early Deployers

Lessons learned from the Connected Vehicle Pilots – New York City, Tampa Hillsborough Expressway Authority (THEA), Wyoming DOT – related to SCMS activities are summarized below:

- **Number of Certificates per Validity Period:** A good starting point for the number of pseudonym certificates granted per validity period is approximately 20. This was determined based on an average of two hours of driving per vehicle per day. Through initial SCMS efforts, this number was determined to be sufficient to maintain anonymity of vehicles that travel this number of hours per day. Some other use cases include vehicles that travel more than two hours a day. For example, the NYC CV Pilot includes equipped taxi cabs that drive for an average of 12 hours per day. As a result, the NYC CV Pilot negotiated with their SCMS vendor to get 60 certificates per validity period for their vehicles. With the participation of professional drivers, such as the trucking and taxi industries, who drive for several more hours per day than the average commuter, considerations for protecting the privacy of these operators must be considered by the deploying agency, and the number of certificates needed for each weekly rotation may need to be increased.
- **Implement Proper Vehicle Certificate Change Requirements:** During development, the NYC CV Pilot Deployment team identified an issue with the SAE J2945/1 Standard's Certificate Change (CERTCHG) requirement criteria that was potentially putting the privacy of their participants at risk. The CERTCHG requirement calls for certificates to be changed every five minutes but contains an exception involving the "absolute distance" from the previous certificate change location. The exception states that a certificate change does not occur should the System be "separated by less than 2 kilometers in absolute distance from the location at which the last certificate change occurred." Under the current absolute distance assumption, a vehicle traveling within an urban grid network (such as a taxi in NYC) may not trigger the certificate change mechanism. The team concluded that the "absolute distance" was not the proper criteria for an exception for their Pilot, as it was still possible for a vehicle to operate in a large

area for an extended time period and not be required to change its certificate. The NYC team decided to implement a change mechanism that required certificates to change every 2 KM traveled or every 5 minutes – whichever comes first.

- **Validity Period of RSU Application Certificates:** The validity period for RSU application certificates is generally one week, which required RSUs to contact the SCMS on a weekly basis. Some entities have equipment installed in the field that does not have access to the internet – making it more difficult to support certificate refresh. It is important to consider how many devices will be installed in locations without cellular connection or access to backhaul. Another consideration is whether the RSUs can directly communicate with the SCMS, or if these communications must be proxied through the TMC.
- **Certificates in Rural (and Less Dense) Areas:** Rural locations – or deployments with limited RSU installations – will result in the situation where OBUs may not encounter RSUs often enough to receive certificate updates. The Wyoming CV Pilot Site was unable to use the Application or Identification Certificates for their distress notification application as trucks may not be encountering RSUs in a rural setting as often as necessary to keep those certificates valid. Based on conversations with the SCMS vendor, the Wyoming CV Pilot Sites learned that they would not be able to change the lifespan of the application certificates. As a result, the team decided to use pseudonym certificates for their distress notification application, which allowed them to secure certificates for a 3-year lifespan.
- **Have a Rough Estimate of the Number of Devices that Need to be Enrolled in the SCMS:** Before an agency procures services for a private SCMS, they should complete their project planning and have a rough idea of the number of OBUs, RSUs, and Traffic Management Center (TMC)/Backend Systems that will need to be enrolled with the SCMS. This will be necessary to get an accurate quote.
- **Topping Off Certificates for Installations and Reboots:** As entities set-up their devices, it is possible that the devices could run out of valid certificates because the certificates expire during transport from the device vendor to the deployer. For devices that only store a small number of weeks of certificates, it will stop transmitting should the device run out of valid certificates. The current solution is that the device must be restarted to enable the download of new certificates. As device vendors gain more experience with connecting to the SCMS, it is likely that this will no longer be an issue.
- **Understand What Applications Devices Will Be Supported Early in the Process:** Prior to procuring a SCMS vendor, entities should know what applications their devices will be supporting. When deploying secure connected vehicle devices that are signing messages with certificates from a SCMS, knowing the applications the devices will support, and the messages utilized by those applications is extremely important. As part of the initialization/set-up process for these connected vehicle devices, they will need to enroll with the SCMS for specific PSIDs as well as specific SSPs (if necessary). If these devices are deployed without enrolling with the proper PSIDs and SSPs, you may be required to re-initialize those devices, which could entail pulling RSUs off mast arms or removing OBUs from vehicles and bringing them back to a depot.
- **Ensure that Device Vendors Can Support Enrollment/Bootstrapping:** It is highly recommended that agencies have their connected vehicle device vendor conduct the enrollment/bootstrapping process. Agencies should work with your device vendors to understand if they have experience

enrolling devices with an SCMS and include appropriate requirements in the device vendors' contracts to enroll the devices with their SCMS.

- **Re-enroll Devices in Secure Environment:** While certificates can be downloaded while a vehicle is on the go, devices must be returned to a secure environment for re-enrollment in the SCMS infrastructure. Ideally enrollment should occur in the same environment where maintenance is being performed. Another option is to have a process in place to have the removed devices for suspected improper operation sent back to the vendor for repair and validation or replacement of the enrollment certificates.
- **Implement Misbehavior Detection Functionality:** It is necessary to implement a credential management misbehavior detection feature to address vulnerabilities to cyber-attacks, spoofing and malfunctioning equipment. These can be performed with misbehavior detection software and the use of a Certificate Revocation List (CRL) distribution mechanism–both of which are essential to maintain the security of the CV infrastructures.
- **Ensure that Devices have Sufficient Computing Power:** To support SCMS functionality, connected vehicle devices require processing signatures and validations of certificates. Early deployers need to ensure that their device hardware can support the load to handle the number of signatures and validations that need to be processed every tenth of a second (the rate at which BSMs are broadcast). Deployers should have a good understanding of the load requirements on their connected vehicle devices and ensure that their hardware is not under-powered.

References

Several documents and presentations were used to develop this Primer. These documents are listed below:

1. *A Security Credential Management System for V2V Communication*. Whyte, William; Weimerskirch, Andre; and Hehn, Thorsten. 2013 IEEE Vehicular Networking Conference.
2. CAMP SCMS Wiki (https://wiki.campllc.org/display/SCP/SCMS+CV+Pilots+Documentation) – a wiki page developed by the Crash Avoidance Metric Partners (CAMP) for the SCMS Proof of Concept. The work was sponsored by the National Highway Traffic Safety Administration (NHTSA).

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-19-775

U.S. Department of Transportation