Photo Source: USDOT

SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS) PROOF OF CONCEPT (POC)

LIMIT 35 SAFETY | MOBILITY | ENVIRONMENT

What Is the SCMS?


Photo Source: USDOT

The U.S. Department of Transportation (USDOT) is committed to ensuring that connected vehicle technologies operate in a safe, secure, and privacy-protective manner. As connected vehicle applications exchange information among vehicles, roadway infrastructure, traffic management centers, and wireless mobile devices, a security system is needed to ensure that users can trust in the validity of information received from other system users—indistinct users whom they have never met and do not know personally. For this reason, the Department has partnered with the automotive industry and industry security experts through the Crash Avoidance Metrics Partnership (CAMP) to design and develop a state-of-the-art security system that enables users to have confidence in one another, and the system as a whole.

The SCMS is a POC message security solution for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. It uses a Public Key Infrastructure (PKI)-based approach that employs highly innovative methods of encryption and certificate management to facilitate trusted communication. Authorized system participants use digital certificates issued by the SCMS POC 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 POC also plays a key function in protecting the content of each message by identifying and removing misbehavior devices, while still maintaining privacy.

Why Do Connected Vehicles Need the SCMS?

Connected vehicle technology has the potential to transform the way Americans travel through the use of dedicated short-range communication (DSRC), GPS, and other wireless technologies to share safety, mobility, and environmental information. The SCMS is a critical component of this connected vehicle environment.

In contrast to other types of safety technologies currently found in the vehicle fleet, connected vehicle applications are cooperative—meaning, vehicles must exchange and analyze data in real time to realize the benefits of the system. This cooperative exchange of messages generates data that applications use to issue alerts and warnings to drivers about the driving situation around them. It also enables applications to determine mobility and environmental conditions. However, a cooperative system can only work when drivers are able to trust the alerts and warnings issued by their connected vehicle devices,

SCMS POC Eligibility Criteria

- Research deployment sites that derive funding from the USDOT are eligible to request enrollment in the USDOT SCMS POC. The SCMS POC will only support a select number of connected vehicle applications (mapped by Provider Service Identifier or PSID). Deployers are encouraged to review the list of supported applications by following this link: https://wiki.campllc.org/display/SCP/SCMS+PoC+Supported+V2X+Applications.
- Deployment sites that are not funded by the USDOT, research or otherwise, are currently not eligible to enroll in the USDOT SCMS.
- Deployments that support commercial activities, state/local maintenance and operations, and production rollout deployments are also not eligible to enroll in the USDOT SCMS. One major reason for this is that these commercial providers offer certificate services beyond the USDOT SCMS window of 5 years, which is the expected lifespan of the SCMS POC.

U.S. Department of Transportation

which are based, at least in part, on information received from other connected vehicle devices.

Thus, a primary requirement for a connected vehicle system is trust. To achieve that trust, received messages must have:

- **Integrity –** The message was not modified between sender and receiver.
- **Authenticity –** The message originates from a trustworthy and legitimate source.
- **Privacy –** The message appropriately protects the privacy of the sender.

The SCMS POC provides the mechanism for devices to exchange information in a trustworthy and private manner using digital certificates. It also provides a critical element in achieving interoperability—so different vehicle makes and models will be able to talk to each other and exchange trusted data without pre-existing agreements or altering vehicle designs.

The SCMS POC is being developed in conjunction with USDOT research activities that support the acceleration of connected vehicle technology deployment:

- **V2V Notice of Proposed Rulemaking –** Citing the enormous benefits associated with connected vehicle technologies, the National Highway Traffic Safety Administration issued a Notice of Proposed Rulemaking[1] that would enable V2V communication technology on all light vehicles. The proposed rule would require automakers to include V2V technologies in all new light-duty vehicles and require V2V devices to "speak the same language" through standardized messaging.
- **V2I Research –** As a complement to the proposed V2V rule, the Federal Highway Administration is conducting research into V2I communication, which will help transportation planners integrate technologies that allow vehicles to "talk" to roadway infrastructure such as traffic lights, stop signs, and work zones to improve mobility and safety.
- **Connected Vehicle Pilot Deployment Program –** The Intelligent Transportation Systems Joint Program Office (ITS JPO) Connected Vehicle Pilot Deployment Program seeks to combine connected vehicle and mobile device technologies in innovative and cost-effective ways to improve traveler mobility and system productivity. The SCMS POC is one of the technologies that will be integrated into early deployments (Connected Vehicle Pilot sites) to showcase how the system works in a realistic environment.

How Does the SCMS Work?

The SCMS provides the security infrastructure to issue and manage the security certificates that form the basis of trust for V2V and V2I communication. Connected vehicle devices enroll into the SCMS, obtain security certificates from certificate authorities (CAs), and attach those certificates to their messages as part of a digital signature. The certificates prove the device is a trusted actor in the system, while also maintaining privacy. Misbehavior detection and reporting allow the system to identify bad actors and revoke message privileges, when necessary.

Enrolling into the System

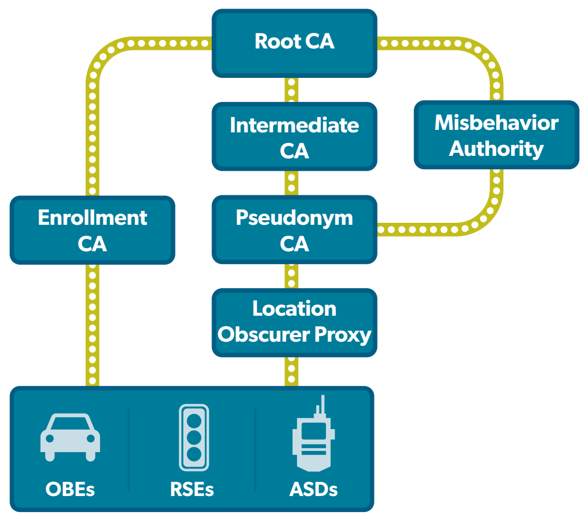
Devices enroll into the system by submitting an enrollment request to the USDOT. Criteria are being developed for authorizing devices to participate in the system. Once authorized, devices are considered trusted actors in the system. A certification process will ensure that devices meet program requirements and perform as intended.

Certificate Management

CAs within the SCMS POC ecosystem create, distribute, and revoke certificates. The CAs form a chain of trust, with each authority representing an individual link along the chain. The chain follows a hierarchy so that the signature on a certificate from any entity (CA) along the chain is validated as a validator climbs up a link of the chain, and if the last signature on the chain is verified and that entity is implicitly trusted (a trust anchor), then the whole chain is accepted and trust flows down to the entity at the bottom of the chain. This concept is called chain-validation of certificates, and is the fundamental concept of a PKI.

The SCMS makes use of several certificate types depending on whether the connected vehicle application is installed on a vehicle or roadside unit (RSU).

SIMPLIFIED SCMS ARCHITECTURE DESIGN



Onboard Equipment (OBE)

- **OBE Enrollment Certificate –** An enrollment certificate is like a passport for the OBE in that it uses the enrollment certificate to request other certificates—pseudonym and identification certificates. A certification process will provide authorization for OBEs to interface with the SCMS and request an enrollment certificate during the bootstrap process.
- **Pseudonym Certificate –** Pseudonym certificates are short term and used primarily for basic safety message authentication and misbehavior reporting. For privacy reasons, a device is given multiple certificates that are valid simultaneously, so that it can change them frequently.
- **Identification Certificate –** OBEs use identification certificates primarily for authorization in V2I applications. None of the current V2I applications require encryption by the OBE at the application level; however, there might be a need in the future. As there are no privacy constraints for identification certificates, an OBE has only one identification certificate valid at a time for a given application.

RSU

- **RSU Enrollment Certificate –** An enrollment certificate is like a passport for the RSU in that it uses the enrollment certificate to request application certificates. A certification process will provide authorization for RSUs to interface with the SCMS and request an enrollment certificate during the bootstrap process.
- **Application Certificate –** 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.

Misbehavior Reporting and Revocation

A key feature of the SCMS architecture is misbehavior detection and reporting. Beyond authenticating and validating basic safety messages, system users need to be able to detect and block messages that have been compromised—whether intentionally or erroneously. Since basic safety messages provide situational awareness for devices to issue safety warnings and alerts, accepting a false message with inaccurate data can be extremely dangerous. The SCMS will implement a misbehavior authority that will collect misbehavior reports generated locally by devices in the environment. Misbehavior reports provide the SCMS with information that can be used to determine whether a device is not performing at the appropriate level. If enough misbehavior reports are received by the SCMS, it will revoke a device from the environment. Once a device is revoked from the system, it is no longer considered a trusted source for sending and receiving messages.

The Road Ahead

The SCMS POC will be made available to early deployment sites in 2017. Connected Vehicle Pilot, Smart Cities, and other research deployments will be able to interact with the SCMS POC to ensure the security and privacy of their messages. The SCMS Quality Assurance environment is now available for devices to begin interacting and testing their local certificate management software. In September 2017, the SCMS Operational Environment (production-ready) will be available to coincide with the full-scale deployment of devices at the Connected Vehicle Pilot sites.

Several projects are underway in support of the SCMS and funded by the USDOT:

- Operations of the SCMS
- Technical Management of the SCMS
- Governmental Management of the SCMS
- Misbehavior Detection Development and Implementation
- National SCMS Development.

The policies, procedures, and lessons learned from the POC will eventually be shared with connected vehicle stakeholders to support the establishment of the National SCMS.

Eligible Deployments

Research deployment sites that derive funding from the USDOT are eligible to request enrollment into the USDOT SCMS POC. Since these deployment sites are research-focused and support USDOT connected vehicle research activities, they provide a suitable test environment for the USDOT SCMS.

Participating deployments understand that the USDOT SCMS is a POC system designed to educate policymakers and industry experts on the challenges associated with ensuring safe, secure, and privacy-protective V2V and V2I communications. Lessons learned from the implementation of the system will be used to facilitate the establishment of an eventual national system by private industry.

The USDOT SCMS POC will only support a select number of connected vehicle applications (mapped by PSID). Deployers are encouraged to review the list of supported applications by following this link: https://wiki.campllc.org/display/SCP/SCMS+PoC+Supported+V2X+Applications

The expected lifetime of this system is through December 2020.

Ineligible Deployments

Deployment sites that are not funded by the USDOT, research or otherwise, are currently not eligible to enroll in the USDOT SCMS. Deployments that support commercial activities, state/local maintenance and operations, and production rollout deployments are also not eligible to enroll in the USDOT SCMS POC. These deployments are encouraged to utilize security services from a commercial supplier. One major reason for this is that these commercial providers offer certificate services beyond the USDOT SCMS window of 5 years, which is the expected lifespan of the SCMS POC.

Any agency that plans to initiate a project to deploy connected vehicle technology may consider procuring turnkey connected vehicle devices that meet the following requirements:

1. Devices are provisioned with security credentials upon delivery
2. Security certificate services, including downloads of new certificates, are provided for the life of the device
3. Security credentials provided by the supplier are interoperable with credentials provided by the USDOT SCMS.

Additional Information

For documentation on the technical requirements for end-entities to interface with the SCMS POC, please visit: https://wiki.campllc.org/display/SCP/SCMS+CV+Pilots+Documentation.

For additional information on the Connected Vehicle Pilots, please visit: https://www.its.dot.gov/pilots/.

To understand the research and thinking leading up to the current V2V communication environment and SCMS development, please refer to: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/readiness-of-v2v-technology-for-application-812014.pdf.

For more information about this initiative, please contact:

Bob Kreeb, Chief, ITS Research Division
National Highway Traffic Safety Administration
(202) 366-0587 | robert.kreeb@dot.gov | www.its.dot.gov

Kevin Gay, Chief – ITS Policy, Architecture, and Knowledge Transfer
ITS Joint Program Office
(202) 493-0259 | kevin.gay@dot.gov | www.its.dot.gov

FHWA JPO-11-021