SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS)

Photo Source: U.S. DOT

What Is an SCMS?

The U.S. Department of Transportation (U.S. DOT) 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 partnered with the automotive industry and industry security experts through the Crash Avoidance Metrics Partnership (CAMP) to design and develop a proof-of-concept (POC) security system that enables users to have confidence in one another and the system as a whole.

Subsequently, the POC SCMS has been retired and multiple commercial SCMS vendors are operating and providing certificates for real-world connected vehicle deployments.

The SCMS is a 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 an 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 and operators, 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.


Photo Source: U.S. DOT

The Need for a National SCMS

The U.S DOT is supporting the creation of a National SCMS for several reasons:

New Environment: The U.S. DOT has been supporting connected vehicle research, development, testing, and deployment for more than a decade. V2V and V2I communications are creating a new environment that allows vehicles and transportation infrastructure to communicate with each other.

New Deployments: The U.S. DOT has transitioned its research efforts to activities around adoption and eventual deployment of connected vehicle systems. A National SCMS must be established to govern and manage the security credentials needed for the gradual national roll-out of connected vehicles.

New Technologies: The vehicles of the future will use V2X wireless technologies. A National SCMS can consider how various technologies and communications services will interact and operate within the anticipated connected vehicle environment, supporting safety and other types of applications and messages. https://rosap.ntl.bts.gov/view/dot/36397

Intelligent Transportation Systems
Joint Program Office

U.S. Department of Transportation

SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS)

Why Do Connected Vehicles Need the SCMS?

Connected vehicle technology has the potential to transform the way Americans travel using advanced wireless communications between vehicles and infrastructure and other vehicles and transportation system users (collectively referred to as "V2X"), GPS, and other 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, 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 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.

How Does an SCMS Work?

An 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 an 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 contracting with an SCMS provider. The SCMS provider will provide the security criteria that devices must meet to operate within their system. Once authorized, devices are considered trusted actors in the system. A certification process will ensure that devices meet performance requirements identified across multiple connected vehicle standards and perform as intended.

Certificate Management

CAs within the SCMS 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 system.

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

SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS)

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

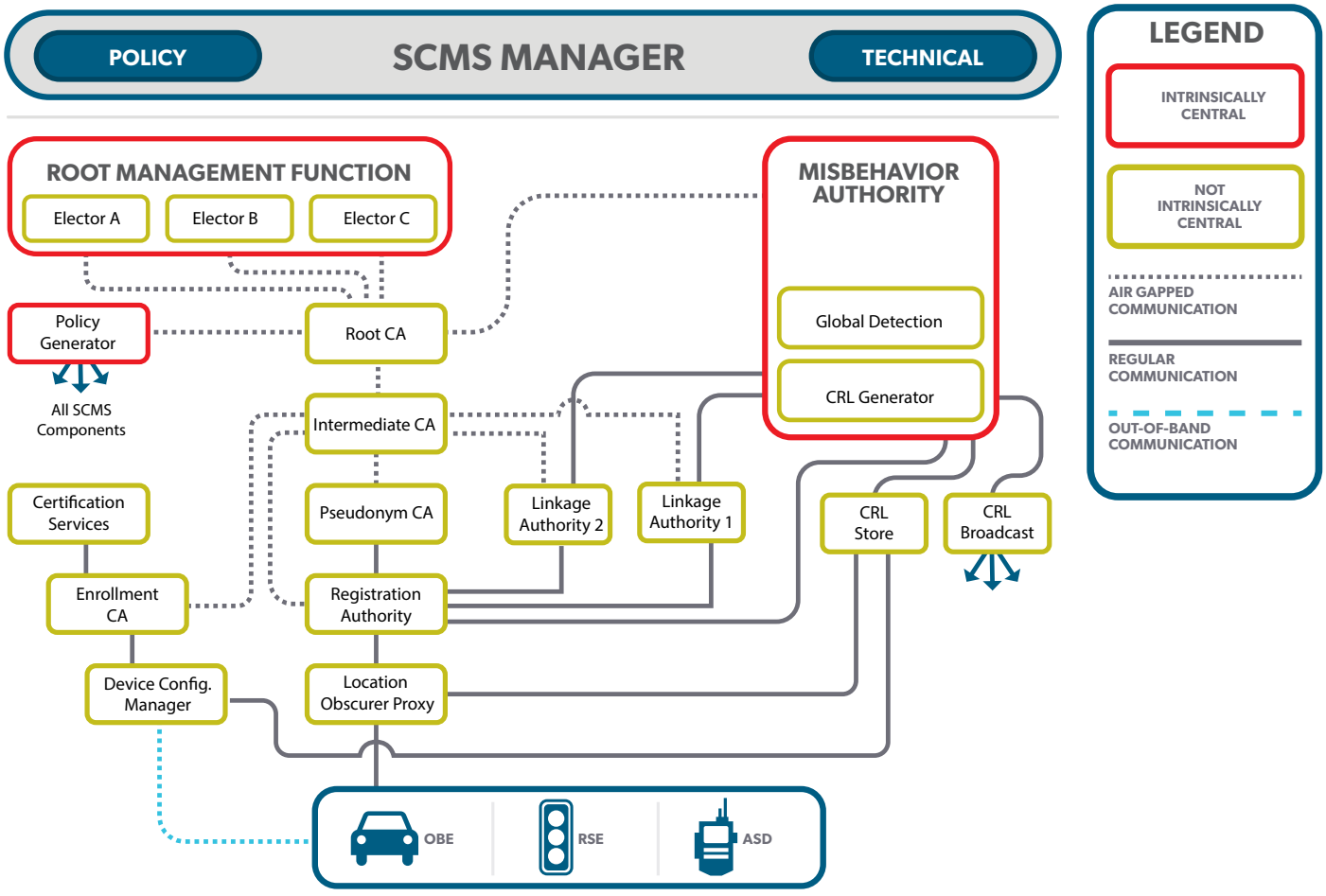
A key feature of the SCMS architecture is misbehavior detection and reporting. Beyond authenticating and validating basic safety messages, system users need to be able to detect and block messages that have been compromised—whether intentionally or erroneously. Since basic safety messages provide situational 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 add a device's certificates to the certificate revocation list (CRL) and distribute the updated CRL to other devices in the environment. Once another device identifies that a message came from a device on the CRL, it will no longer consider that a trusted source for sending and receiving messages.

The Road Ahead

The Connected Vehicle Pilots, Smart Cities, and other early deployments are currently interacting with commercial SCMS providers to ensure the security and privacy of their messages. These providers have supported the deployment of devices at the Connected Vehicle Pilot sites since 2017.

SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS)

SCMS ARCHITECTURE DESIGN



Additional Information

For documentation on the SCMS, please visit: https://rosap.ntl.bts.gov/view/dot/43635.

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/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf.

For more information about this initiative, please contact:

Steve Sill, P.E., PMP, Intelligent Transportation Systems Architecture, Standards, and Cybersecurity Program Manager

Intelligent Transportation Systems Joint Program Office
(202) 366-1603 | steve.sill@dot.gov