Security Credential Management System (SCMS) Overview

Connected Intersections Program Brief

PURPOSE AND DESCRIPTION

A Vehicle-to-Everything (V2X) Security Credential Management System (SCMS) provides anonymous trust by issuing digital certificates, based on Institute of Electrical and Electronics Engineers (IEEE) 1609.2, to approved devices. Devices use these certificates to sign messages they broadcast, and receiving devices verify the signatures to ensure messages are from a trusted source. Messages are signed using certificates generated and provided from a known and trusted Certificate Authority (CA) (certificate issuer).

Background

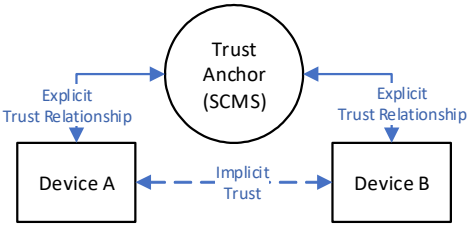
Security is a critical aspect of any communication system. Vehicle-to-Everything (V2X) systems are typically comprised of infrastructure roadside units (RSU) and vehicle-based on-board units (OBU), exchanging data using SAE J2735 messages. Additional infrastructure devices, such as traffic signal controllers (TSC), back office systems, such a transportation management centers (TMC), and the IT network that connects everything together, all play critical roles in securing the overall system.

A unique aspect of a V2X system is that most OBUs need to remain anonymous to protect the privacy of the vehicle operator and owner. Conventional IT security mechanisms require a pre-established trust relationship between the data sender and the data receiver. This is not practical for a V2X system, so for vehicles to securely exchange data with other unknowdn (anonymous) devices, a mechanism is required for RSUs, OBUs, and other V2X devices to verify received messages are from a "trusted" source; this helps prevent the broadcasting and use of malicious fake or misleading data. This mechanism enables vehicles to exchange data with each other and the infrastructure while remaining anonymous.

SCMS Certificates

The SCMS uses certificates for devices to sign messages they broadcast, and receiving devices verify the signatures to ensure messages are from a trusted source. Certificates are only valid for one week and devices top-off (request new certificates) every week. Three types of certificates are typically used:

1. ***Pseudonym certificates*** protect the privacy of the vehicle owner\operator. OBUs typically contain up to 20 certificates for a given week, rotating which certificate is used to sign messages during the week. When the OBU changes certificates, the device changes other identity data to prevent certificates and other Basic Safety Message (BSM) data from being used to track vehicles over long periods of time and distance. Note that OBUs may not top off pseudonym certificates for up to 18 months.
2. ***Identity certificates*** are used by OBUs when privacy is not required. For example, to request signal priority or preemption; the infrastructure needs to know who is requesting priority\preemption before it can be granted.
3. ***Application certificates*** are used by RSUs. RSU privacy is not required. RSUs sign signal phase and timing (SPaT) and RTCM messages with Application certificates. MAP messages may be signed at the RSU or elsewhere.



SCMS RESOURCES

Connected Intersections Program: V2X System Security 101

Collision Avoidance Metrics Partnership (CAMP) SCMS Proof-of-Concept Design https://wiki.campllc.org/display/SCP

Connected Transportation Interoperability (CTI) Standard 4501 v01

Connected Intersections Implementation Guide http://www.ite.org/pub/76270782-B7E4-7F75-BC72-D5E318B14C9A

SCMS CERTIFICATE PROVIDERS

Identified by the USDOT/ITE Connected Intersections Project for informational purposes:

- AutoCrypt, South Korea: Jungwook Kim, jwkim@autocrypt.io
- BlackBerry, Canada: William Lee, wlee@blackberry.com
- ESCRYPT, Canada: Omar Alshabibi, omar.alshabibi@escrypt.com
- INTEGRITY Security Services, US: Support, support@isscms.com
- Microsec, Hungary: Roland Kraudy, roland.kraudy@microsec.com

SCMS Function

Certificates contain Provider Service Identifiers (PSID) for services the device is "authorized" to provide. Service Specific Permissions (SSP), for a given PSID, are also contained in the certificate. If an OBU or RSU receive messages/data that are inconsistent, impossible, or improbable, they should report the transmitting device as "Misbehaving" to the SCMS provider. Some examples of misbehavior include: BSM containing a location (latitude\longitude) 100s of miles away from the receiving device, BSM containing a highly excessive speed (e.g. 150 MPH), or a SPaT message indicating conflicting phases or containing a time value in the past. Based on these "Misbehavior Reports" the SCMS will generate and distribute Certificate Revocation Lists (CRL), containing information about the offending devices indicating these devices should no longer be trusted. Devices that receive messages from a device listed in the CRL, will simply ignore the messages.

Other Security Needs

While the SCMS is critical for securing communications between V2X devices, other security measures and practices need to be in place to ensure the entire system is protected. The Institute of Transportation Engineers (ITE) *Connected Intersections Implementation Guide* provides IOOs with guidance in deploying a system to support V2X Red Light Violation Warning (RLVW) applications. It depicts high level components of a V2X system and the communication paths connecting the components together. There are four key areas in which security needs to be addressed:

- V2X devices, including RSUs and OBUs.
- Other roadside equipment, including traffic signal controllers and message handler.
- Back office systems, particularly the transportation management center (TMC).
- The general IT network, which connects RSUs to the signal controller, the message handler, and the TMC.

While back office systems and the general IT network should be protected using conventional IT data center and security practices, additional details on securing V2X devices and other roadside equipment can be found in the *Connected Intersections Implementation Guide. A*dditional details regarding the information provided in this fact sheet can be found in the CV PFS *Connected Intersections Program: V2X System Security 101* resource.

SCMS Manager is a standalone organization (SCMS Manager LLC) that develops and enforces security standards in the V2X ecosystem, primarily focused on end entities (RSU and OBU) and SCMSes and their subsystems. Membership is open to all organizations which operate or provide technology, products and services for vehicles, roadside infrastructure, and traffic management centers. Further, SCMS Manager provides ongoing operational oversight for the security elements of the V2X ecosystem to manage and verify their continued compliance with SCMS Manager best practices.

Relevance to CV PFS Members

- The SCMS is a required component of interoperable connected intersections, as defined by the USDOT/ITE Connected Intersections *Implementation Guide.*
- When considering a connected intersection deployment, agency staff should familiarize themselves with SCMS resources to understand requirements, costs, and available providers.
- Agencies may join SCMS Manager as an "Observer Member" at no cost; however, Observer Members cannot vote on work products or chair working groups.