U.S. Department of Transportation
Intelligent Transportation Systems Joint Program Office

Vehicle-to-Everything (V2X) Security

Images courtesy of iStock

V2X and the USDOT

Vehicle-to-everything (V2X) technologies can save lives by enabling vehicles to communicate with each other, with infrastructure, and with other road users such as pedestrians and cyclists. As V2X safety applications exchange information, a security system is needed to ensure that users can trust in the validity of information received from other system users. The U.S. Department of Transportation (USDOT) is dedicated to integrating security and trust capabilities into V2X communications on the 5.9 GHz band to ensure message integrity and authenticity and to prevent possible interference and misbehavior.

Source: Getty / Olemedia

Security by Design

V2X communications rely on clear, reliable, and trustworthy messages to deliver safety warnings, potentially reducing crashes. The USDOT has applied "security by design" principles from the start of V2X concept development. Working with industry, it has built a multilayered security approach that provides trust in messages, provides privacy to roadway users, and incorporates policies, processes, and capabilities that are able to adapt to new and emerging cybersecurity threats.

These layers of security include:

V2X message protections

V2X system policies and procedures

V2X misbehavior detection

Establishing Trusted Data Exchanges Through the Security Credential Management System

The Security Credential Management System (SCMS) serves as a message security solution for V2X, employing a Public Key Infrastructure (PKI)-based approach along with innovative privacy and certificate management techniques to ensure trust in communication. Collaborating with the automotive industry and security experts through the Crash Avoidance Metrics Partnership (CAMP), the USDOT designed and developed a proof-of-concept security system, fostering confidence among users and the system itself. Building upon the initial SCMS, multiple commercial SCMS vendors are now operational, providing certificates for real-world connected vehicle deployments.[1]

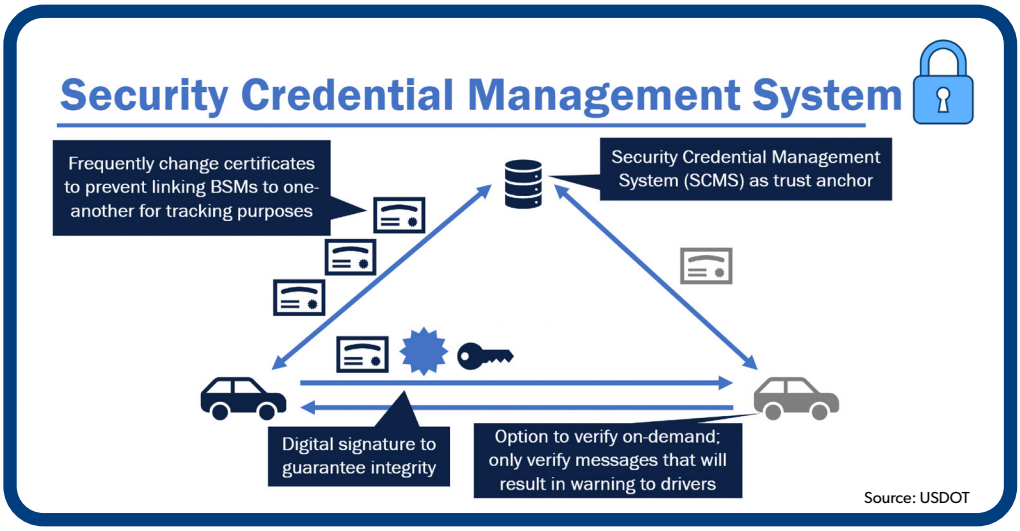
1 See "Security Credential Management System" at https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf

Continued on Reverse Side

FAQs

How does the SCMS work?

V2X devices sending messages need to digitally sign their messages, and the receiving devices need to verify the signature before acting on it. The SCMS distributes security certificates to V2X devices, which use these certificates to sign their messages. Upon receiving a V2X message, the device checks if it is signed with a valid certificate; if not, the message is ignored. Device certificates rotate regularly to enhance privacy and prevent vehicle tracking.



What are the benefits of the SCMS?

The SCMS provides several benefits, including:

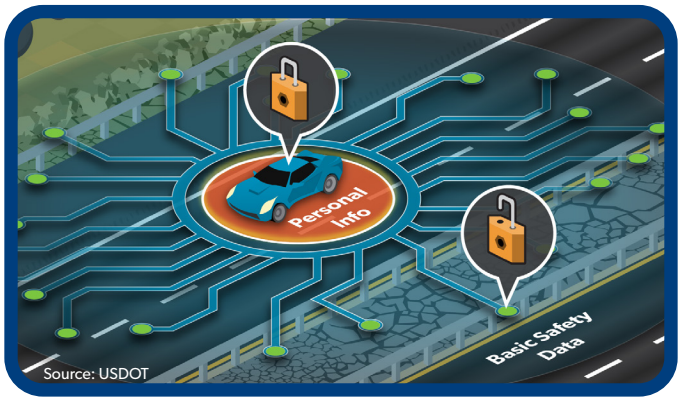
- Ensuring authenticity—so users can trust that the message originates from a trustworthy and legitimate source.
- Ensuring privacy—so users can trust that the message appropriately protects their privacy.
- Helping achieve interoperability—so different vehicle makes and models will be able to talk to each other and exchange trusted data without specifying pre-existing agreements or altering vehicle designs.

Who is eligible to enroll in the SCMS?

Vendors are eligible to enroll their devices in the SCMS if they meet the strict security requirements set by the industry consortium that oversees policy for V2X device security. Enrollment requirements involve device certification with specific security testing to ensure compliance. The V2X industry has developed the Certificate Trust List (CTL), which enables devices to trust certificates from approved SCMS vendors meeting stringent security requirements. The USDOT is collaborating with the industry to foster the development of these policies.

How is V2X misbehavior detection managed?

The Misbehavior Detection (MBD) system analyzes the contents of the messages generated by vehicles to determine if any specific element seems abnormal and could reflect either intentional or unintentional misbehavior. The SCMS maintains a Certificate Revocation List (CRL), which tracks devices that have crossed a specific misbehavior threshold. When a V2X device validates a message, it checks the message's certificate against the CRL and ignores messages from devices on the list.



What is the future for V2X security?

V2X connectivity beyond the 5.9 GHz band continues to evolve, and the USDOT is ensuring that other wireless technologies provide safe and secure communications for intelligent transportation systems (ITS). To facilitate that, the Intelligent Transportation Systems Joint Program Office (ITS JPO) has an Interagency Agreement (IAA) with the National Telecommunications and Information Administration (NTIA) to analyze fifth-generation cellular (5G) technology to identify if there are any cybersecurity-related risks for vehicles and ITS infrastructure systems.

For more information about this initiative, please contact:
Justin Anderson, PMP, CSEP, CISSP, Next Generation Wireless Communications and SCMS Program Manager
Intelligent Transportation Systems Joint Program Office | 202-366-9198
Justin.Anderson@dot.gov | www.its.dot.gov

5802-20240404