Microsec Builds Trust in Smart Transportation and Logistic Communications with nShield HSMs

In a world of smart cities and communities, a wide range of personal, vehicle, roadside, and central devices need to be able to communicate effectively and securely. To accomplish this, vehicle manufacturers, road infrastructure providers, government authorities, and related organizations are working to standardize Cooperative Intelligent Transport Systems (C-ITS). This includes vehicle-to-everything (V2X) communication that enables trusted interactions between vehicles, people, and the digital road infrastructure, with the aim of increasing road safety, decreasing traffic congestion, and preparing the infrastructure for automated management. Such a complex network creates a wide range of potential attack vectors, so it is critical that these communications be protected, trusted, and managed.

Business challenge

The main goal for autonomous vehicles and smart community infrastructure is to improve safety, ease traffic congestion, and increase efficiency and mobility for vehicles, pedestrians, and goods. To make this a reality, the C-ITS needs to be standardized and secured across a wide range of manufacturers, governmental, regulatory bodies, communication, and hardware systems.

Furthermore, while various types of vehicle-to-everything (V2X) communication may be developed to meet the different use cases and scenarios, the security underpinning these communications needs to be consistent and effective across the full spectrum of V2X communications. Compliant digital certificates for connected devices and vehicles are a proven solution for delivering the higher trust levels outlined in the C-ITS trust model.

Microsec, a qualified service provider for the Hungarian IT market with international reach, is working with Entrust to create a Public Key Infrastructure (PKI) framework that provides a security infrastructure (V2X certificates) for car manufacturers, vendors, roadside and onboard unit developers, transportation and smart city infrastructure operators, as well as the secure management of the associated signing and encryption keys.

Microsec V2X Case Study

Technical challenge

V2X communication can cover a range of protocols that let vehicles exchange information with other vehicles, pedestrians, and traffic infrastructure in real time. Until recently, V2X communication has been based primarily on the ITS-G5 protocol, a dedicated short-range communication (DSRC) standard using WiFi signals. Now, data exchange is being accelerated rapidly and at wider range with the expansion of 4G and 5G networks.

During the data exchange, each party or device needs to verify their permissions. They do this using digital certificates that establish trusted identity for each party while maintaining anonymity, preventing unauthorized parties from interfering with the exchange of data. These certificates are created, managed, distributed, stored, and revoked via the PKI framework. However, with a single vehicle expected to use as many as 100 certificates a week (according to the latest published version of the European Certificate Policy in 2019), the number of cryptographic operations that need to be run and the many thousands of certificates that need to be created and managed in a secure environment necessitates using hardware security modules (HSMs).

Solution

Microsec's V2X PKI security framework has been developed to provide secure vehicle-to-everything communication. In such environments, public key infrastructures (PKIs) are used to secure the environment by verifying the participants' permissions with the use of certificates. V2X PKI does this with the most up-to-date cryptographic solutions, including Elliptic Curve Cryptography (ECC), which has more advantages than the widely used RSA algorithm, and using Entrust nShield® HSMs for encryption and signing operations, and key management at scale.

Entrust nShield HSMs are among the highest-performing, most secure, and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial, and government organizations. The purpose-built hardware devices are designed to generate, safeguard, and manage cryptographic keys on behalf of applications. The unique nShield Security World key management architecture enforces important separation of duties with dual controls that segregate security functions from administrative responsibilities.

The hierarchy and mechanism of V2X PKI is as follows: at the top there is a Root Certificate Authority (CA), an offline entity that acts as the anchor of trust. This organization issues certificates for two other authorities, the Enrollment Authority (EA) and the Authorization Authority (AA). The Enrollment Authority's main task is to authenticate the car's on-board unit unique ID or certificate. The need for Authorization Authorities originated from the need for anonymity when it became clear that someone could easily track a car's movement by following the unique identifiers which the car uses to communicate with. Based on the enrollment credentials, the Authorization Authority issues authorization tickets, which are pseudonymous (they cannot be linked to the enrollment credentials, except for the

Microsec V2X Case Study

issuing CAs) creating an entirely secure and untraceable flow of messages that can be sent to the surrounding environment.

The European Union's European Certificate Trust List (ECTL) currently has three levels of trust (L0/L1/L2) in its Trust List Manager:

L0 – Just a simple CA certificate is required, with no protection mandated

L1 – The CA and generated certificates need to be audit ready

L2 – The CA is audited based on EU C-ITS certificate policy

Once Cooperative Intelligent Transport Systems are rolled out at scale, the number of digital certificates that will need to be generated for just a single region will be exponentially higher than all those used for today's websites. As such, those looking to meet the stringent L2 in the ECTL Trust List Manager will need to deploy the infrastructure required to facilitate this. This is especially true for those departments and organizations managing the certificates associated with emergency and other priority vehicles, which will be uniquely identifiable and require enhanced security due to their privileged traffic status.

Microsec has focused its efforts on developing the certificate authority software that would incorporate the necessary new attributes into the digital certificates required for V2X communications. Microsec is able to meet the stringent ECTL audit requirements with the help of Entrust nShield HSMs to create and protect the private keys used to issue the digital certificates.

"While the C-ITS ecosystem consists of several different players (e.g., vehicle manufacturers, road operators), they do not have the same technical capacity, performance and privacy requirements to send and receive C-ITS communication messages. Some of them require their V2X PKI instances, and other players need to rely on SaaS implementations to ensure message security. Backed by Entrust hardware security modules, Microsec provides as-a-service and on-premises solutions to equip the market with V2X message signing certificates." said Roland Kraudy, PKI expert at Microsec.

"Microsec is creating a trusted and established certificate and key management platform for V2X communication based on Entrust nShield HSMs. Developing, deploying, and managing this type of platform is where Microsec can help."

« Microsec is creating a trusted and established certificate and key management platform for V2X communication based on Entrust nShield HSMs. Developing, deploying, and managing this type of platform is where Microsec can help. »

Roland Kraudy, PKI expert at Microsec

Microsec V2X Case Study

CUSTOMER PROFILE

Business need

- Deploy the Cooperative Intelligent Transport Systems (C-ITS)
- Implement and offer secure, standardized solution for vehicle-to-everything (V2X) communication

Technology need

- Secure creation and management of millions of digital certificates and keys

Solution

- Developing and offering the certificate authority solutions that would incorporate the necessary new attributes into the digital certificates required for V2X communications
- Entrust nShield HSMs to securely generate and store cryptographic keys, and supports a formerly unprecedently high volume of cryptographic operations

Result

- Result 1: ECTL Level 0+ registered SaaS solution, supported by Entrust HSMs
- Result 2: License, hardware and know-how for on-premises implementations

Result

Microsec's V2X PKI security framework can deliver:

- Trust
- Access
- Privacy

For more information visit: Microsec V2X PKI

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223