Security Partner
Preferred

Partner Use Case

Securing V2X communications with Infineon HSM

Savari and Infineon – The Sign of Trust for V2X

Products

SLI 97

Use case

Application context and security requirements

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, collectively referred as vehicle-to-everything (V2X), is a wireless technology aimed at enabling data exchanges between a vehicle and its surroundings. In V2X environment, vehicles, roadside equipment, and mobile devices cooperatively exchange messages and generate data that allows them to inform users about driving, mobility, and environment conditions around them. The technology is expected to greatly transform the experience of drivers, pedestrians and transit riders by preventing crashes, enhancing traffic flow and shortening transit trip times while reducing the emission of greenhouse gases.

A V2X system is thus built on cooperative exchange of data. A cooperative system can only work when devices are able to trust the messages from other connected devices. To establish trust and preserve the privacy of participates, the V2X security infrastructure must perform following operations:

- Authenticate the sender to check that the message originated from a trustworthy source
- Check message integrity to test that the contents of the message were not altered
- Protect the privacy of participants by making sure that no personal or equipment-identifying information that can be used to monitor or track the users is transmitted

The V2X systems essentially use a sophisticated Public Key Infrastructure (PKI)-based approach to facilitate trusted communication. Authorized participants use digital signatures and digital certificates issued by the Security Credentials Management System (SCMS) to authenticate others and validate V2X messages. Figure 1.0 shows how the essential steps of the scheme works*.

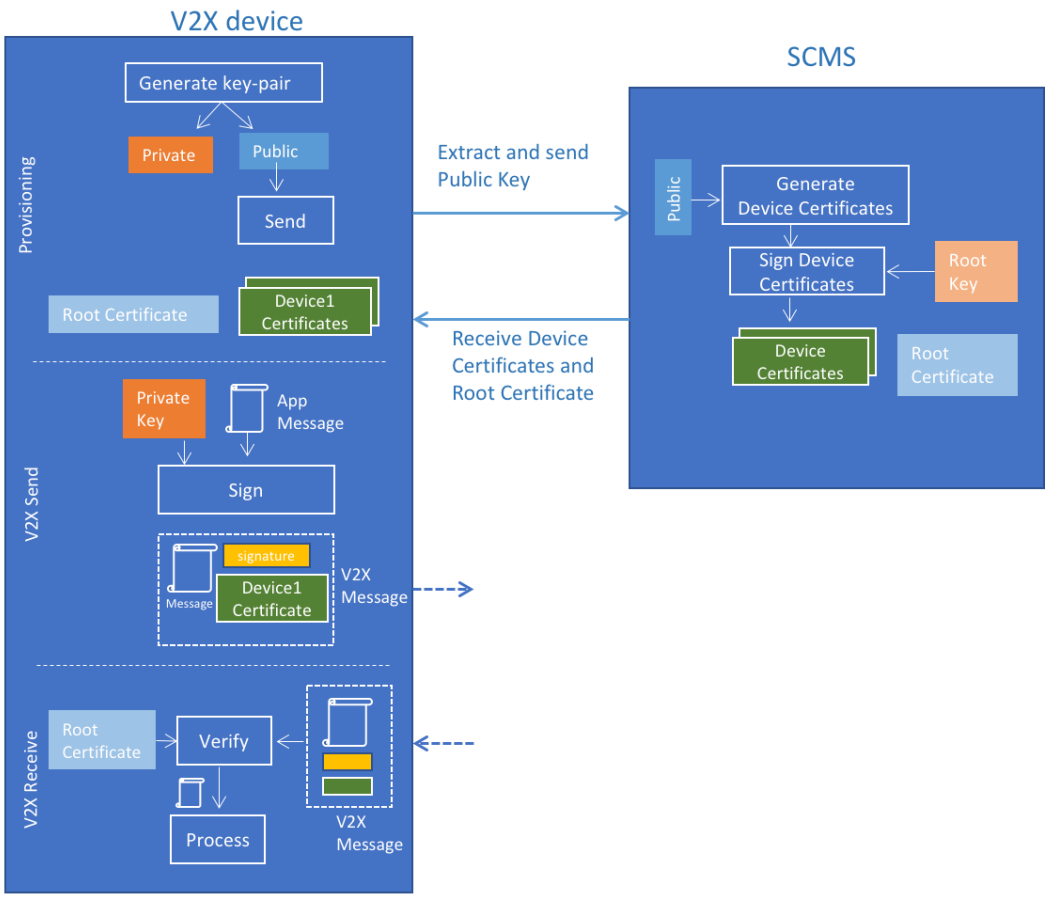

Figure 1.0: V2X Device Interactions

Use case

Application context and security requirements

- Device generates asymmetric key-pair. The public key is extracted and sent to the SCMS, while the private key is securely stored on the device.
- SCMS uses device's public key and generates device specific certificates and signs the certificate using the root key. The device certificates and the root certificates are then sent back to the device.
- To send a message, device signs the message using the private key. Signature calculation involves computing the hash of the message and encrypting the hash with the private key. The device then bundles message, signature, and one of device certificates and transmits the bundle as a V2X message.
- When the device receives a message, it authenticates the sender by verifying the root signature on sender's certificate. It then verifies the signature on the message to check the integrity of the message. This involves decrypting the sender's signature with sender's public key in the certificate and comparing that value with the hash of the message. By comparing the values, the system can check that the message has not been altered.

* Notes:

- Device enrollment and root hierarchy details have been omitted for simplicity
- Commercial V2X systems use innovative ways to reduce the size of certificates and optimize these

Challenge

In order for the trust framework to work securely and effectively, following main challenges must be addressed:

- V2X systems use Elliptical Curve Cryptography (ECC). Device must be able to securely and efficiently generate ECC keys
- The random numbers generator must have high entropy
- Root-certificates must be protected by usage of secured storage
- Device must have tamper resistance, including physical attacks
- Private keys must have protection against side channel attacks
- Private keys must to be protected and used securely
- V2X device are required to generate up to 40 messages per second. The signing latency must be low to support this frequency

Above challenges necessitate the use of dedicated hardware. Savari stack/devices use Infineon's embedded Secure Element (eSE) – also called Hardware Security Module (HSM) - for this purpose.

Use case

Implementation

Savari has integrated Infineon's eSE in their aftermarket On Board Equipment (OBE) and Road Side Equipment (RSE) devices as shown by figure 2.0.

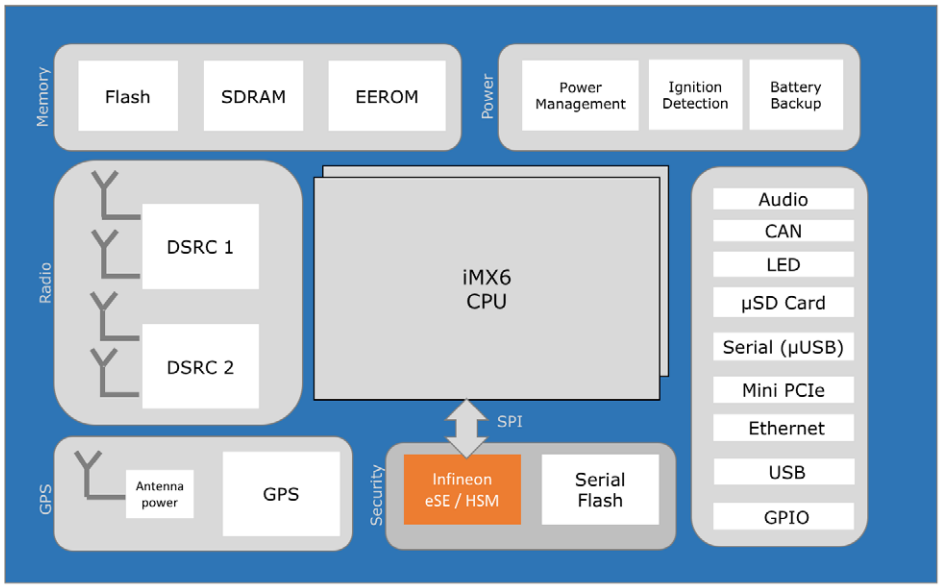

Figure 2.0: Block diagram Road Side Equipment (RSE) devices

Benefits for the user

Savari is a supplier (more than 80% of the On Board Units) to the United States Department of Transportations (US-DOT) Connected Vehicle Pilot at Tampa, Florida. Using Infineon Hard- and Software, Savari is able to supply a complete solution to V2X Connected Vehicle Pilots sponsored by US-DOT. Through this integration and work, Savari has also developed tools and practices which be utilized for bootstrapping and provisioning keying material and certificates on OBEs in high volumes.

Solution

Figure 3.0 shows the software architecture of Savari Infineon solution.

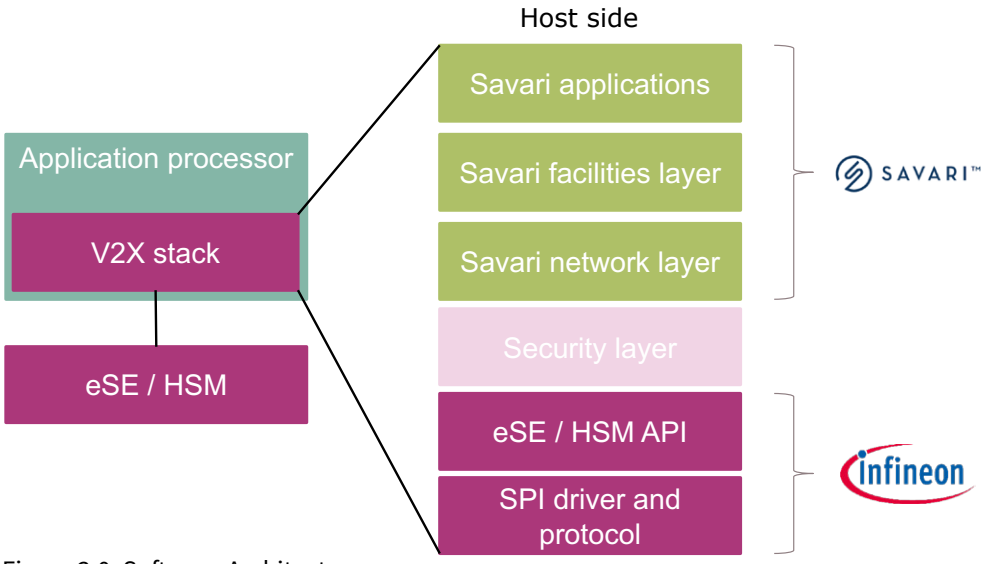

Figure 3.0: Software Architecture

The Savari stack uses a third-party security module that implements the relevant V2X Security protocols per standards (e.g. IEEE 1609.2). Savari and Infineon worked together to create an Application Programming Interface (API) to the security module and other components in Savari stack. Using this API, the V2X stack can securely communicate with the HSM and use its services to carry out necessary operations.

Savari also developed tools and practices to fully integrate the eSE / HSM into device bootstrapping and security credential provisioning workflows to achieve end-to-end compliance with US-DOT / SCMS / CAMP (Crash Avoidance Metrics Partners) standards. Figure 4.0 shows the workflow.

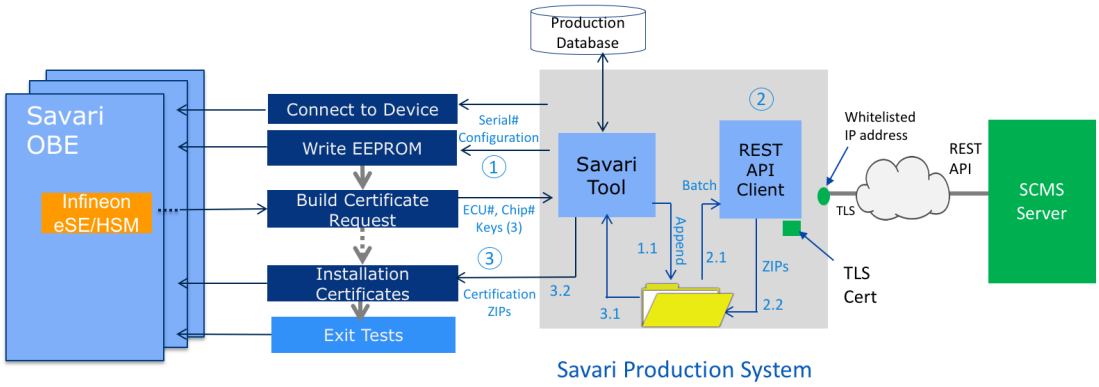

Figure 4.0: Security Credential Provisioning

Solution

Main benefits of the Infineon product

Infineon's eSE / HSM provides a fully functional, highly flexible HSM that can be integrated with any V2X radio.
The Savari-Infineon solution is field proven, interoperable, US-DOT OmniAir-CoC certified and deployed in several field trials. In addition, all of the Prototype Software, APIs and documentation required for quick integration and test of software to manufacture test of hardware are available.

Infineon Security Partner Preferred

Partner

SAVARI®

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf; while for others, offers are custom-built.

About Savari

Savari seeks to make the world's roadways and vehicles automated and safer by deploying advanced wireless sensor technologies and software. Savari builds software and hardware sensor solutions for automotive car manufacturers, the automotive aftermarket and smart cities. The company pioneered V2X radio technology, which is crucial for vehicles to achieve Level 4 and Level 5 of automation. The technology allows vehicles to share data with other vehicles, traffic lights and smartphones. With more than 150 man-years of V2X learning and development and 15 million-plus miles per year of public testing, Savari is a leader in V2X technology. Savari is headquartered in Santa Clara, California and has offices in Detroit, Mich., Munich, Germany, Seoul, Korea, Bengaluru, India, Shanghai, China. For more information, visit savari.net.

Savari contribution to the Infineon Security Partner Network

Savari has been working on V2X since its inception in 2009 and is a proven leader in the industry. We work with the world's largest providers for connected vehicle hardware and software to provide an integrated, full functionality and highly secured V2X platform for the safety and mobility applications of the future.

Infineon is a worldwide leader in automotive semiconductors, and it has been our pleasure to partner with them to help expand their reach to include support of the rapidly growing V2X market.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 02 / 2019

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Please note!
THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.