infineon

Security Partner

Partner Use Case

Securing connected vehicle technology for Florida drivers

OnBoardSecurity
STAY AHEAD OF THE CURVE

Implementing one of the most important safety improvements since the invention of the seatbelt

Products

SLI 97

OnBoardSecurity
STAY AHEAD OF THE CURVE

Use case

Application context and security requirement

Traffic accidents have been steadily increasing over the past few years, with over 40,000 United States (US) road fatalities in 2016 and the leading cause of death in young adults. The cost is estimated at over $300 Billion a year, with an additional $230 Billion due to avoidable road congestion. Vehicle to Vehicle (V2V) communication is a new capability that can prevent up to 80% of accidents while increasing the efficiency of the transportation system. In support of this technology, the US government is funding three connected vehicle pilot (CVP) sites to evaluate the system; one of which is in Tampa, Florida. The Tampa Connected Vehicle Pilot uses V2V to transform the experience of drivers, pedestrians and transit riders in the downtown area by preventing crashes, enhancing traffic flow and shortening transit trip times while reducing the emission of greenhouse gases.

Challenge

V2V-equipped vehicles carry short range, high speed radios to allow them to transmit 10 messages a second regarding their speed, direction of travel and many other factors to other road users within a radius of at least 300 meters, thereby giving the receiving vehicles sufficient time to avoid potentially dangerous situations. In order to encourage adoption and ensure public trust in the capability, personal privacy and vehicle security are key requirements of the system. To be effective, drivers need to know that the system is both safe and secured.

Implementation

This is where OnBoard Security and Infineon come in. Since the message security protocol is a public standard, Savari, a major supplier of in-vehicle and roadside units, was faced with a choice of engineering its own solution or searching for a suitable commercially available product. After a careful review, Savari selected OnBoard Security and Infineon as solution partners for this application. All messages sent between vehicles or to infrastructure devices such as traffic lights must be authenticated as trustworthy while protecting anonymity. This is achieved through a specially developed Private Key Infrastructure called the Security Credential Management System (SCMS). The equipment supplied by Savari relies on Infineon and OnBoard Security for all the necessary aspects of message security and privacy. OnBoard Security's Aerolink® software manages the signing and verification of all V2V messages before giving the safety and other application programs access to the transmitted data. Because the V2V system uses a public/private key security system, it is essential that the private keys are stored and managed within a highly secured environment, known as a Hardware Security Module (HSM). The HSM in this case is the Infineon SLI 97, an automotive-grade semiconductor device that has already been implemented for eCall applications in tens of millions of vehicles. The SLI 97 has been reprogrammed and optimized to support the mission-critical performance requirements of V2V and the Tampa Connected Vehicle Pilot represents Infineon's first live implementation of the technology.

Benefits for the user:

- Wrong way entry warning for reversible express lanes
- Reduced streetcar conflicts
- Warning of sudden braking beyond line-of-sight
- Forward collision alerts
- Intersection movement and red light running warning
- Intelligent traffic light and traffic flow optimization
- Pedestrian collision warning
- Do Not Pass and Lane Change warnings
- Transit and emergency vehicle priority

Solution

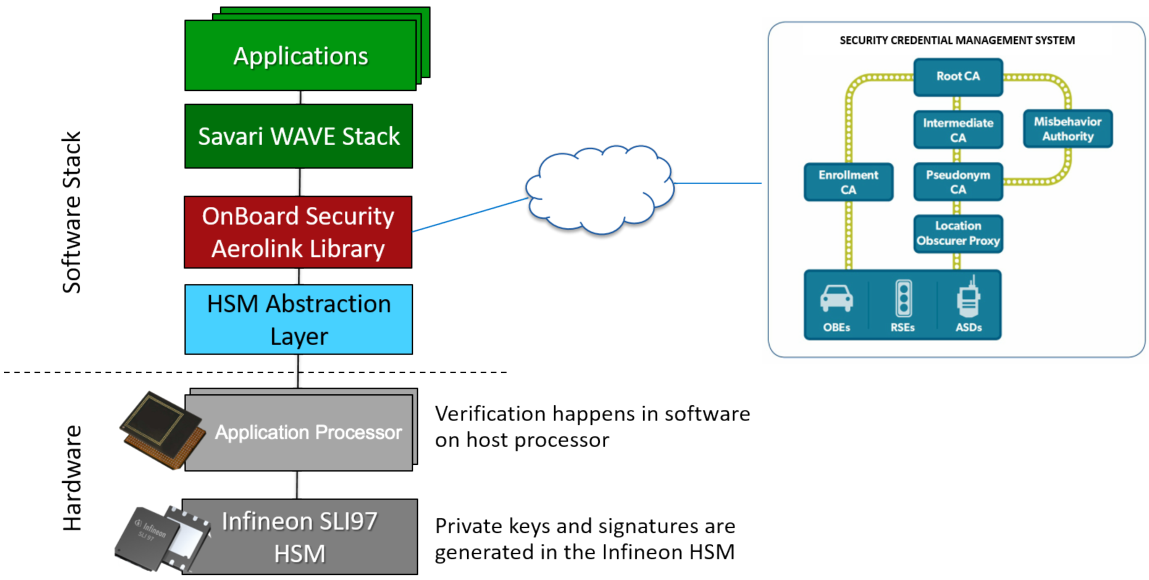
Essential for any in-vehicle hardware is automotive certification, and the SLI 97 Solid Flash device has already achieved the necessary endurance requirements. In addition, the physical and logical requirements to prevent tampering and other interference in V2X devices have also been implemented for the pilot implementation.

The security and privacy requirements have been standardized within IEEE 1609.2 and all the Tampa vehicles will use the latest version of this standard.

Aerolink provides standard interfaces to applications that run in the vehicle so they can sign, verify and secure messages. And when applications need to transmit sensitive information, such as credit card details or travel history, Aerolink manages the encryption and decryption of this sensitive data. Aerolink also performs relevance checks on incoming messages, such as whether they were signed too long ago, or by a vehicle too far away to be of interest. Aerolink also performs consistency checks to check the authenticity of not only the signer’s certificate, but every certificate in the chain of trust, all the way up to the root certificate server.

Aerolink is a leader in securing Vehicle to Vehicle and Vehicle to Infrastructure (V2I) communications. Whether running in software or deeply integrated with cryptographic acceleration hardware, Aerolink provides the optimal mix of automotive security and performance. Aerolink has been selected to provide security and privacy for the 2017 Cadillac CTS, the first commercially available vehicle with V2V capabilities. It has also been successfully implemented in the majority of Ann Arbor Safety Pilot vehicles through a program sponsored by the University of Michigan Transportation Research Institute (UMTRI).

The Infineon SLI 97 chip has proven to be an excellent choice. Not only does it enjoy a large and loyal automotive user base, it has proven to be flexible enough to be repurposed quickly and easily as an HSM in time for the Tampa implementation and is demonstrating excellent performance in a very demanding environment.



Verification happens in software on host processor

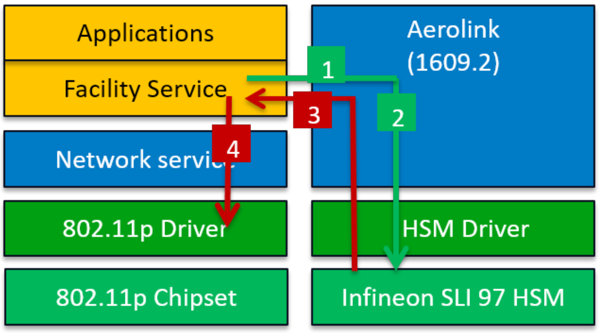
Private keys and signatures are generated in the Infineon HSM

Infineon Security Partner

OnBoardSecurity STAY AHEAD OF THE CURVE

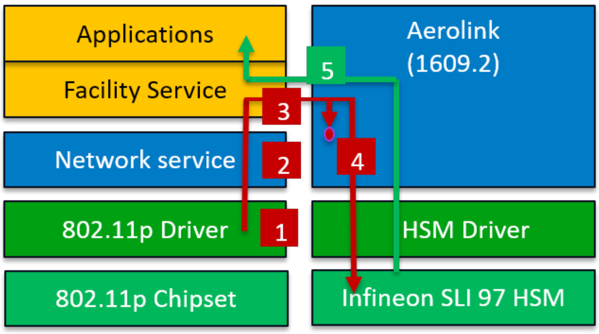
Solution

Signing



1. BSM message generated by facility service. Facility service sends it to Aerolink for signing the message
2. Aerolink requests HSM to sign the message
3. On success, Aerolink sends signed message to facility services
4. Facility service request network service to transmit the message

Verification



1. V2X message received from 802.11p by network service
2. Sent to facility service module
3. Facility service sends it to Aerolink for signature verification
4. Aerolink does relevance check and requests ECDSA HW for signature verification.
5. After successful verification, message decoded, processed and is sent to application

Partner Use Case

Partner

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.

OnBoard Security

OnBoard Security was created to help automotive and IoT organizations stay ahead of the curve through superior cybersecurity.

For over 10 years, the world-renowned experts at OnBoard Security have been pioneering technologies that protect the Internet of Things, now and for the future. We address three significant challenges, ensuring the security and privacy of connected vehicles, making hardware roots of trust easy to use, and avoiding the existential threat from quantum computers to the integrity of the internet.

We are best known for the award-winning Aerolink® V2X libraries that are the de facto standard for connected vehicle security and privacy; our NTRU algorithm which is the most tested and trusted quantum-resistant cryptosystem; and our TrustSentinel TSS 2.0 middleware that simplifies implementation of Trusted Platform Modules. Headquartered in Wilmington, MA, OnBoard Security is a subsidiary of Security Innovation, with 25 employees.

OnBoard Security's contribution to the Infineon Security Partner Network

OnBoard Security is committed to partnerships which help solidify our leadership in automotive security solutions. We work with the world's largest providers for connected vehicle hardware and software to provide an integrated, resilient and highly secured operating platform for the safety and convenience applications of the future.

Infineon is a worldwide leader in automotive semiconductors, and it is our privilege to help expand their reach to include support of the rapidly growing vehicle to Vehicle to Vehicle and Vehicle to Infrastructure requirements.

As the most respected name in the field and as an ISPN partner, OnBoard Security is in the unique position to accelerate Infineon's growth in automotive safety applications and the future deployment of trusted computing and post quantum cybersecurity technology within the next generation of vehicles.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 10 / 2017

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.