Microsemi®

Power Matters.™

Introduction to ADAS and Secure Connected Car

WP0199 White Paper

May 2015

Introduction to ADAS and Secure Connected Car

Advanced driver assistance systems (ADAS) enable better situational awareness and control to make driving easier and safer. ADAS technology can be based upon systems local to the car, that is, "vehicle resident systems" like vision/camera systems, sensor technology, or can be based on smart, interconnected networks as in the case of vehicle-to-vehicle (V2V), or vehicle-to-infrastructure (V2I) systems (jointly known as V2X systems).

V2X communications use on-board dedicated short-range radio communication devices to transmit safety related messages about a vehicle's speed, heading, brake status, vehicle size, and so on, to other vehicles and receive the same information about other vehicles from these messages. Using multi-hops to transmit messages through other nodes, the V2X network can communicate over long distances. This longer detection distance and ability to "see" around corners or through other vehicles helps V2X-equipped vehicles perceive some threats sooner than sensors, cameras, or radar can, and warn their drivers accordingly.

In addition to the basic safety message (BSM) developed for safety applications, the network may also be used by other connected vehicle applications such as mobility or weather. Additional messages from vehicles or from the infrastructure may also be developed in the future.

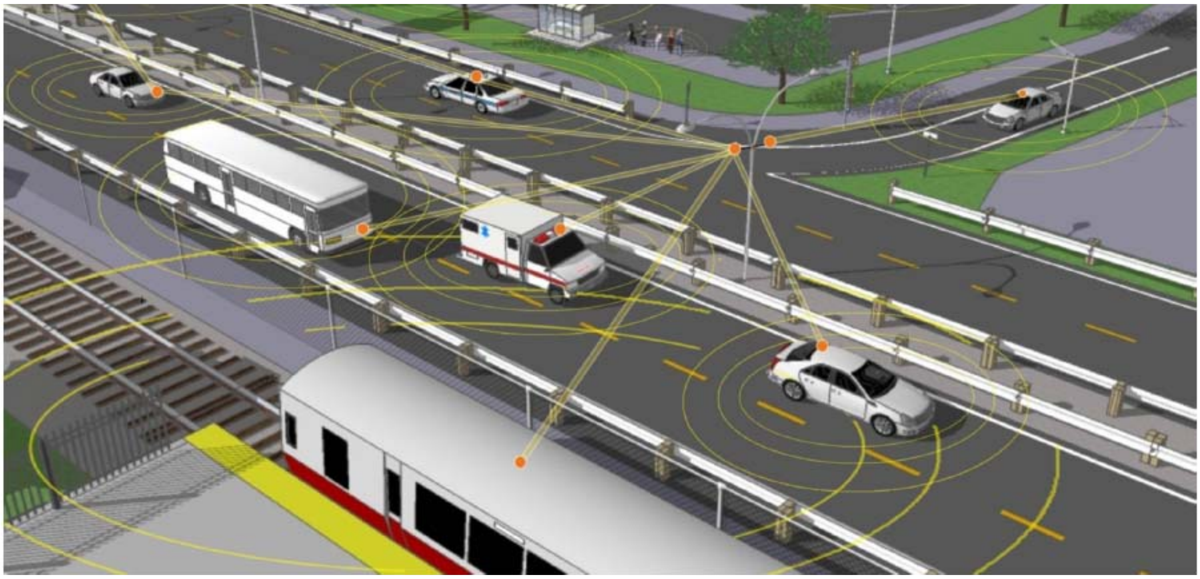


Figure 1: Typical V2X Network Implementation

In terms of safety impacts, based on a study conducted from 2004-2008, the **National Highway Traffic Safety Administration** (NHTSA) estimates that 22 possible different crash scenarios can be prevented by the V2V network. This represents approximately 81% of unimpaired light motor vehicle crashes that can be prevented.

Using 2004-2008 crash data, the approximate average number of fatalities, injuries, and property damage per year caused by these 22 target light-vehicle pre-crash scenarios are 27,000; 1,800,000; and $7,300,000, respectively.

In conjunction with V2I, the potential safety advantages of a wide-scale implementation are enormous. The following is a list of V2I potential safety applications:

- Red Light Violation Warning
- Curve Speed Warning
- Stop Sign Gap Assist
- Reduced Speed Zone Warning
- Spot Weather Information Warning
- Stop Sign Violation Warning
- Railroad Crossing Violation Warning
- Oversize Vehicle Warning

Warning alarms not only inform the vehicle and driver responsible for the safety violation, but through the wireless link they can warn other nearby vehicles, for example, cross-traffic when a red light or stop sign is being run at a blind corner, thus helping to prevent collisions.

Securing the V2X Network

In order for the promise of V2X to be realized, the system must ensure two things:

- Messages originate from a trustworthy source
- Messages are not modified between sender and receiver

The problems originating from a failure of either of the two mentioned scenarios could lead to serious consequences and loss of life.

A bogus message could provide false data about speed and direction of oncoming traffic and lead to accidents, whereas potential data manipulation by miscreants can cause traffic outages and chaos across cities. Imagine a van full of script kiddies traveling down the highway causing chaos, or a drone hovering nearby busy intersections causing misdirection.

In addition to the concerns mentioned above, users are also concerned about privacy and ensuring that messages do not give away the identity and location of the driver, with anonymous vehicular safety information only going to pre-authorized entities such as other vehicles. This is particularly important to ensure wide scale adoption of the V2X system where users must be able to feel confident that the V2X system does not provide access to their personal data.

To prove authenticity, the sender of a message must provide a unique identifier that can be verified at the receiver to confirm that the message comes from a true source.

Typically this is achieved by using either symmetric or asymmetric cryptographic techniques.

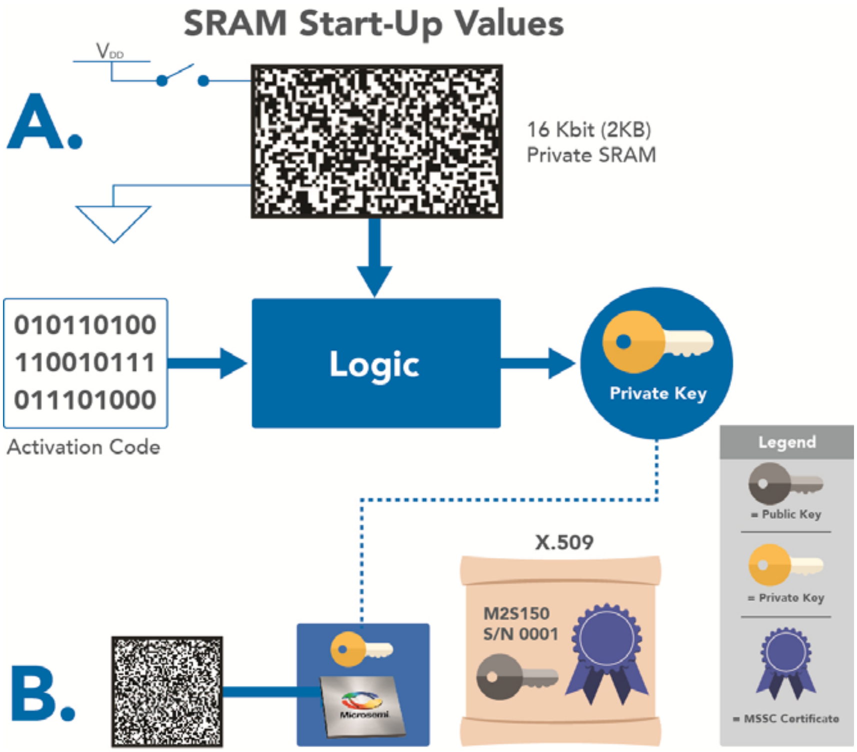
Symmetric cryptography is often suitable for small networks with limited number of nodes, wherein the transmitter and receiver share a common key that is known by both sides before any packet transmission. This key is used to verify the authenticity of the data at the receiver via dynamically generated codes (called message authentication codes – MACs), which are computed based upon the payload and the key to verify packet integrity and source.

This method, although simple, is impossible to use in large networks like large scale V2X networks because either the same key must be used by all nodes, which present an unacceptable security risk, or different keys must be used for each pair of nodes communicating with each other, which is unwieldy.

In asymmetric cryptography the idea is to provide a scalable solution to connect as many nodes as the network may need. To achieve this, each node uses a private key to digitally sign each transmitted message. This digital signature can be verified by the receiver by using an associated public key, which is transmitted to all the receiving nodes. This solution scales better than a symmetric cryptography scheme, and also enables easier replacement of any faulty nodes.

But this poses another question—"How does one ensure that the private and public key used by each node is authentic and not tampered with?"

The best possible solution to the first part of the question is to use "biometric" signatures of silicon ICs based on small physical variations in the manufacturing process of each device. These process variations are never identical and cannot be cloned for any two ICs, and thus provide a unique signature for each. Such signatures are called physically unclonable functions or PUFs. Besides being unclonable, PUF based keys are also very difficult to extract by a hacker because they are typically realized at the atomic level. ICs can base PUFs based on several physical factors like memory elements, logic delays, resistance and so on. SRAM-based ICs, which use the unique and random start-up state of an SRAM cell to generate private keys are further secure because the state of the cell is wiped out at power-off.



Legend

A SRAM start-up values are used to compute a private key made reliable with the aid of an "activation code" saved during the enrollment phase.

B From the private key, a public key is computed and certified by the component manufacturer, giving each component a verifiable globally-unique unclonable identity.

Figure 2: Private and Public Key Computation

The second part of the question can be addressed by a public key infrastructure (PKI). A PKI is a system for the creation, storage, and distribution of digital certificates, which are used to verify whether a particular public key belongs to a certain entity. The PKI creates digital certificates that map public keys to entities, securely stores these certificates in a central repository and revokes them if needed.

In a PKI system, a certificate authority (CA) certifies all nodes by digitally signing their public keys using the CA's own private key. The most common public key certificate format is called X.509. When a device transmits a message digitally signed by its private key this message can be authenticated with the device's public key. The device can also send its X.509 certificate to all nodes receiving its messages so they have its public key. The X.509 certificate including the device's public key can be verified at the receiver using the CA's public key, which is pre-placed in all the nodes and is inherently trusted. Using this scheme a proven, hierarchical, certificate-based chain of trust can be established because the signature applied by the transmitter can be verified by the receiver. This scheme also ensures that imposter machines can be easily detected. Figure 3 shows how a chain of trust is created on the unclonable device identity established by the PUF including the keys certified by the component manufacturer, allowing each system integrator/operator to certify their own independent PKI.

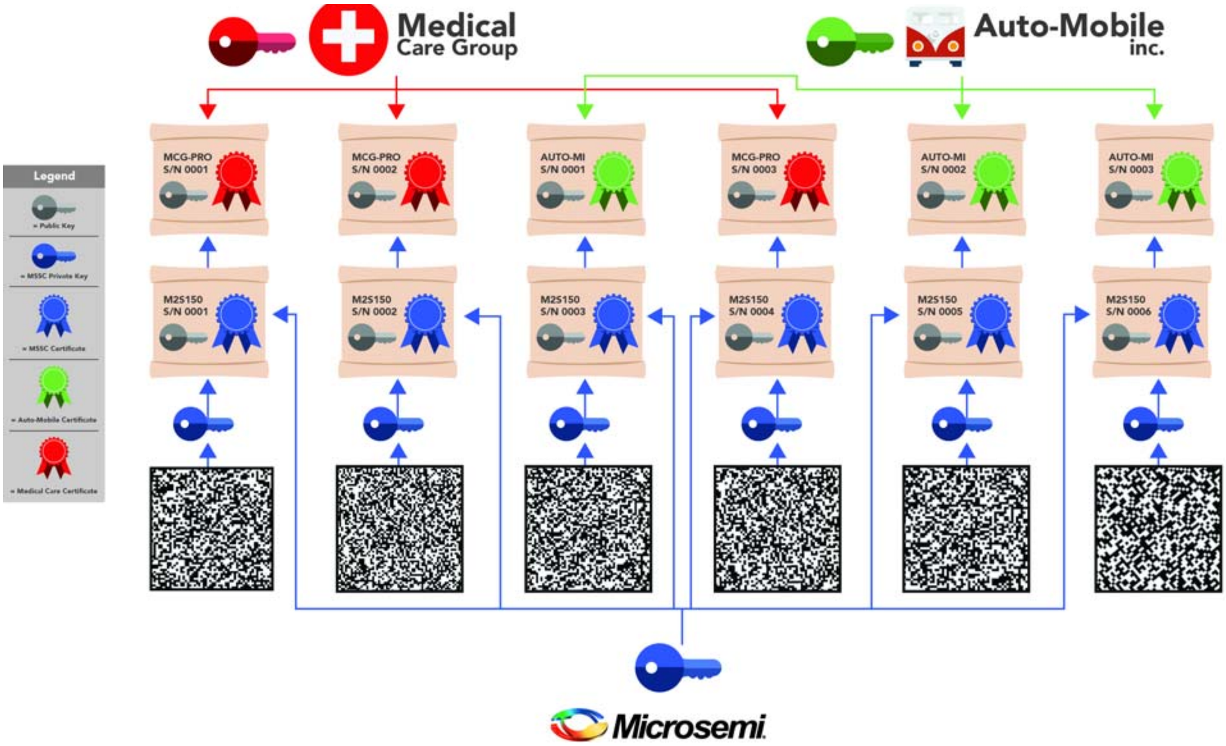


Figure 3: PKI Certification

According to the NHTSA, the PKI option (asymmetric key) using the signature method was deemed to offer the most effective approach to implementing communications security and trusted messaging for a very large set of users. In addition to providing a secure network, a PKI based system also provides an easy to scale infrastructure using a PKI scheme. Importantly, the effectiveness of this approach is highly dependent upon the technical design decisions regarding how to implement this approach in its given environment. The V2X certificate authority issues many anonymous certificates per year for each vehicle, to hinder attempts to track the owner's movements.

Devices such as Microsemi® SmartFusion® 2 System-on-Chip (SoC) and IGLOO® 2 field programmable logic array (FPGA) offer PUF technology to enable a PKI. These device families provide a broad product roadmap with multiple IO and fabric density options to allow users to select a device that fits their requirement. The SRAM PUF in these devices is used to establish a pre-configured certified identity for each node in the network with Microsemi as the certificate authority at the device level. These devices also have built in cryptographic capabilities such as hardware accelerators for AES, SHA, HMAC, and elliptic curve cryptography (ECC), and a cryptographic grade true random number generator. These capabilities can also be used to create a user PKI with the user's own certificate authority or to enroll systems using them in the US or European V2X PKIs.

Because fielded systems like vehicles are accessible by people having malicious intent, it is important for the hardware to be able to protect the secret keys against various physical and side channel attacks, such as differential power analysis (DPA). In addition to the key storage and key generation technologies like PUF's and ECC certain SmartFusion2 and IGLOO2 devices ("S" devices) come with a cryptography research incorporated (CRI) DPA pass through patent license. All SmartFusion2 SoCs and IGLOO2 FPGAs provide secure, remote, DPA resistant update capabilities. The DPA pass through license additionally allows users to harness the massive amount of computational capability in a mainstream FPGA to accelerate PKI transactions in a DPA safe manner using CRI's patented DPA countermeasures. V2X networks thus protected ensures safe and secure communication.

[1] Martin Mason (2007). Know the issues: Applying FPGAs in system-critical automotive electronics.

[2] U.S Department of Transportation, NHTSA (2014). Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application.

[3] Paul Zoratti (2011). Automotive Driver Assistance Systems: Using the processing Power of FPGAs (White Paper).

Microsemi Corporation (MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,600 employees globally. Learn more at **www.microsemi.com**.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA

Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

E-mail: sales.support@microsemi.com

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.