Introduction to ADAS and the Secure Connected Car

By
Prem Arora, Director of Marketing, Microsemi (www.microsemi.com)

The Advanced Driver Assistance System (ADAS) simplifies driving while making it safer by improving situational awareness and control. The technology can be based upon systems that are local to the car, such as vision/camera and other "vehicle resident" systems. Alternatively, ADAS technology can be based on intelligent, interconnected networks. This is the case with Vehicle-to-Vehicle (V2V), or Vehicle-to-Infrastructure (V2I), systems, which together are known as V2X systems.

Security is imperative. In order for the promise of V2X to be realized, the system must ensure two things. First, it is critical that all V2X messages originate from a trustworthy source. Second, there must be safeguards to ensure that no message is modified between sender and receiver.

How V2X Communications Works

Using on-board dedicated short-range radio communication devices, a V2X communications system transmits safety-related messages to other vehicles. These messages include information about the vehicle's speed, heading, brake status, size, among other data. The systems also receive the same information about other vehicles. The V2X network can communicate over long distances by using multi-hops to transmit messages through other nodes. V2X-equipped vehicles are "aware" of, and can alert drivers to, some threats much more quickly than sensors, cameras or radar because of their longer detection distance and ability to "see" around corners or through other vehicles.

In addition to the Basic Safety Message (BSM), the network can communicate messages associated with other connected vehicle applications such as mobility or weather. Applications for delivering additional messages – either from vehicles or from the infrastructure -- may also be developed in the future.

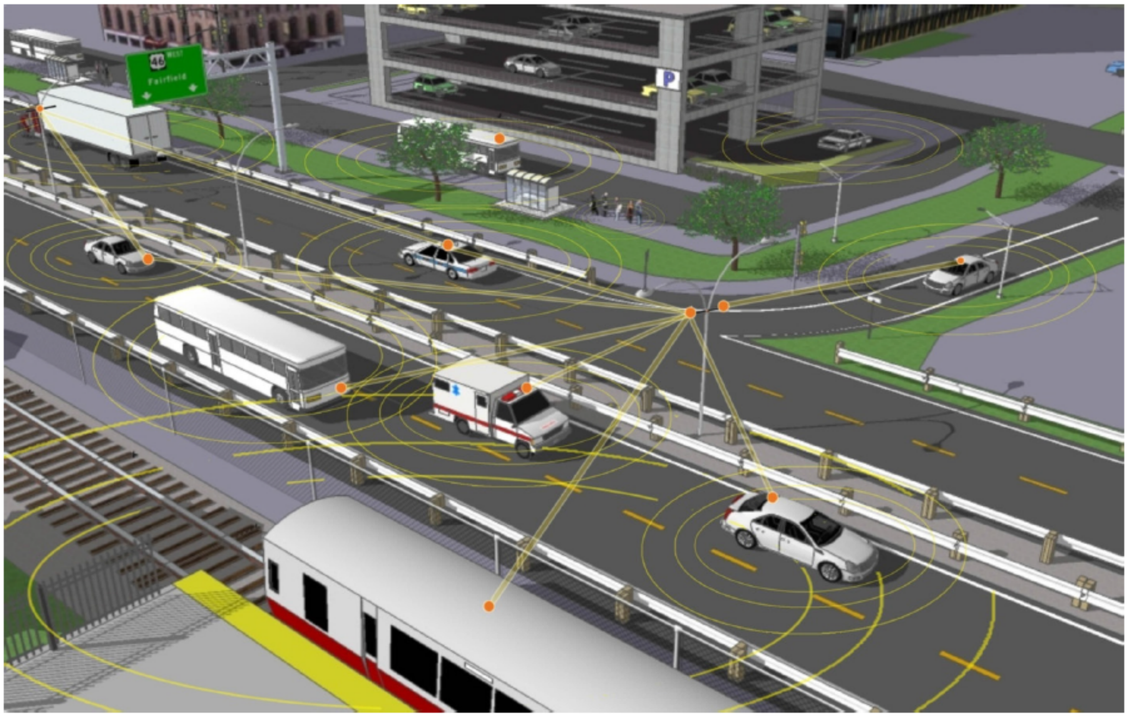

Figure 1: A typical V2X network implementation

V2V networks are expected to significantly improve safety. According to a study conducted from 2004-2008 by the National Highway Traffic Safety Administration (NHTSA), 22 possible crash scenarios can be prevented by the V2V network, or approximately 81 percent of unimpaired light motor vehicle crashes. By preventing these crashes, the study estimates that an average of 27,000 fatalities, 1.8 million injuries, and $7.3 million in property damage could be avoided each year.

In conjunction with V2I, the potential safety advantages of a wide-scale implementation are sizable. 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, and
- Oversize Vehicle Warning.

Warning alarms offer two benefits. First, they inform the vehicle and driver responsible for the safety violation. Additionally, their availability through the wireless link means nearby vehicles can also be used to warn other nearby vehicles; for example, those in cross-traffic that are at risk if a vehicle runs a red light or stop sign at a blind corner, thus helping to prevent collisions.

Importance of Security

There can be serious consequences, up to and including loss of life, if the V2X system cannot ensure messages originate from a trustworthy source and are not modified between sender and receiver.

A fake message could cause accidents by providing false data about the speed and direction of oncoming traffic. Or, malicious data manipulation might cause traffic outages and associated chaos throughout the city.

In addition to the aforementioned threats, users are also concerned about privacy and ensuring that messages do not divulge driver identity or location information. Anonymous vehicular safety information should only go to pre-authorized vehicles and other entities. Users must feel confident that V2X systems will not threaten personal data privacy.

Best Practices for
Securing the V2X Network

In order to prove authenticity, the sender of a V2X message must provide a unique identifier that can be verified at the receiver to confirm that the message originated 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 a limited number of nodes. The transmitter and receiver share a common key which is known by both sides in advance of any packet transmission. This key is used to verify the authenticity of the data at the receiver through dynamically generated codes (called Message Authentication Codes, or MACs) which are computed based upon the payload and the key and are used to verify packet integrity and source.

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

Asymmetric cryptography works better in the V2X environment. The idea is to provide a scalable solution so that as many nodes as are needed can be connected to to the network. Each node uses a private key to give each transmitted message a digital signature that can be verified by the receiver using an associated public key which is transmitted to all the receiving nodes. This solution not only scales better than a symmetric cryptography scheme but also simplifies replacement of any faulty nodes.

Another important requirement is ensuring that the private and public key used by each node is authentic and has not tampered with. The best solution to the first element of this requirement is to use “biometric” signatures of silicon ICs called Physically Unclonable Functions (PUFs) that are based on small physical variations in the manufacturing process of each device. These process variations are never identical and PUF-based keys are not only unclonable, but also very difficult to extract by a hacker because they are typically realized at the atomic level. PUFs can be based on several physical factors like memory elements, logic delays, resistance etc. SRAM-based ICs (which use the unique and random start-up state of an SRAM cell to generate private keys) are particularly secure because the state of the cell is wiped out at power off.

The second element for ensuring keys are authentic and haven't been tampered with can be addressed by a Public Key Infrastructure (PKI). A PKI is a system for creating, storing and distributing digital certificates used to verify that a public key actually belongs to an entity. The PKI creates digital certificates that are used to map public keys to entities. The PKI also securely stores 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 Certificate Authority's (CA's) own private key. X.509 is the most common Public Key certificate format. When a device transmits a message that has been digitally signed by its private key that 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. Because the signature applied by the transmitted can be verified by the receiver, a proven, hierarchical, certificate-based chain of trust can be established, imposter machines can be easily detected.

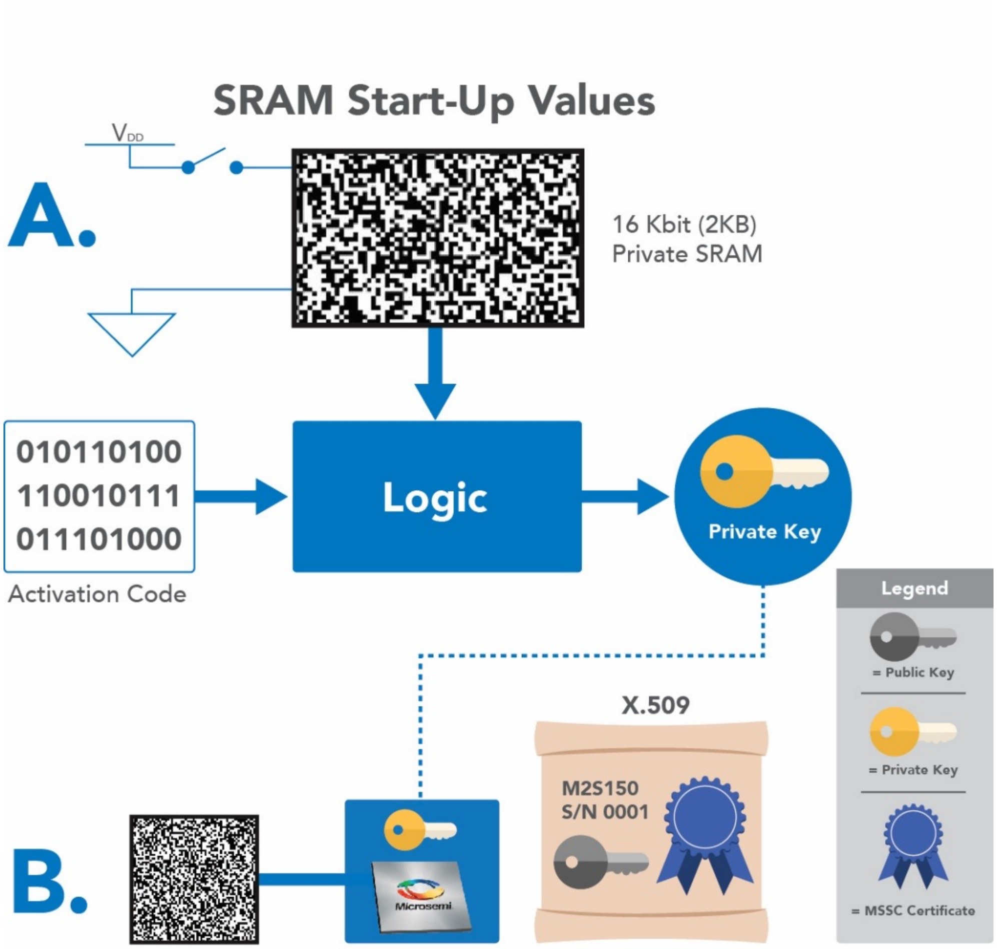

Figure 2: (A.) SRAM start-up values are used to compute a private key that has been made reliable with the aid of an "activation code" saved during the enrollment phase. (B.) From the private key, a public key is computed and certified by the component manufacturer, giving each component a verifiable and globally-unique un-clonable identity.

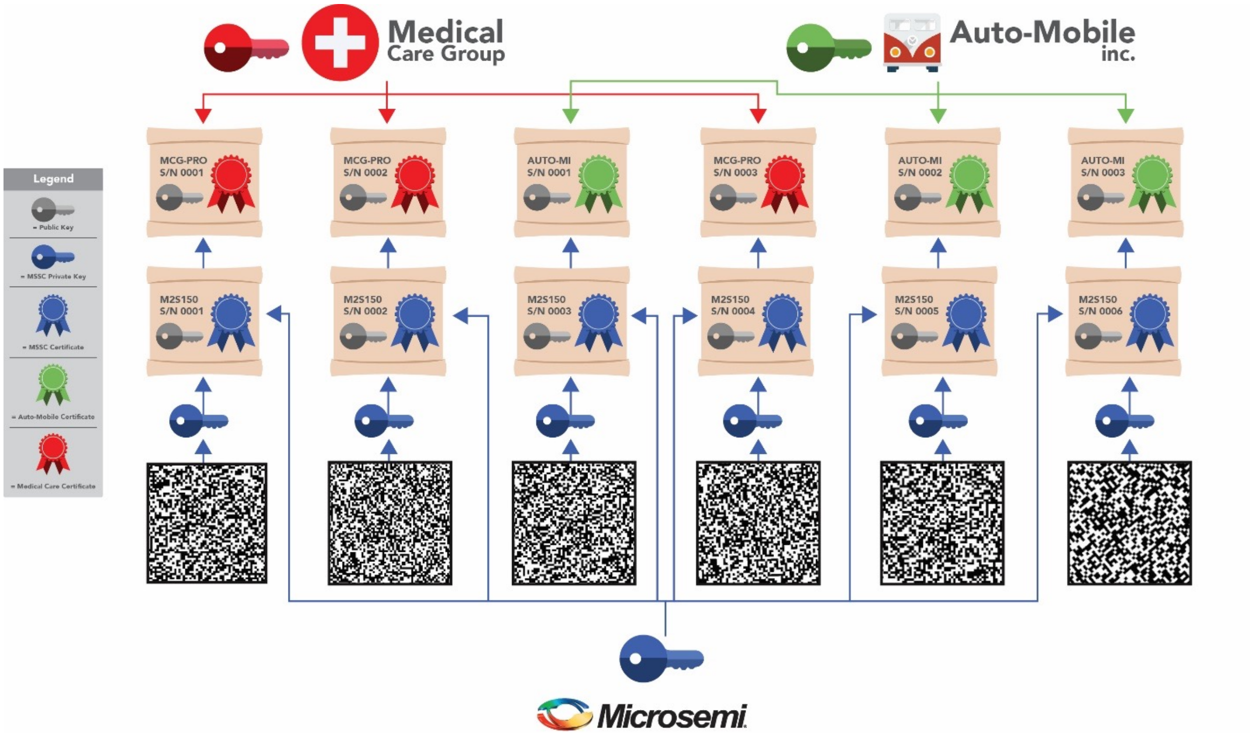

Figure 3: A chain-of-trust is created founded on the unclonable device identity established by the PUF including keys certified by the component manufacturer, allowing each system integrator/operator to certify their own independent PKI.

According to the NHTSA, the PKI option with its asymmetric key and the signature method is the most effective way to implement communications security and trusted messaging across a very large set of users. In addition to securing the network, a PKI-based system also provides an easy-to-scale infrastructure. The effectiveness of this approach is highly dependent upon how the approach is implemented in a given environment. Each year, the V2X CA issues many anonymous certificates for each vehicle. This is done to hinder any attempts to track a vehicle owner's movements.

Devices such as Microsemi's SmartFusion®2 SoCs and IGLOO®2 FPGAs offer the necessary PUF technology to enable a PKI, along with multiple I/O and fabric density options to meet diverse system requirements. The SRAM PUF in these devices is used to establish a pre-configured certified identity for each node in the network. Microsemi serves as the CA at the device level. For optimal effectiveness, devices used in a V2X system should also have built-in cryptographic capabilities such as hardware accelerators for AES, SHA, HMAC, and elliptic curve cryptography (ECC), plus 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 U.S. or European V2X PKIs.

There are other important features to consider. Vehicles are fielded systems that are accessible by people with malicious intentions, so it is important that hardware be capable of protecting secret keys against various types of physical and side channel attacks, such as differential power analysis

(DPA). For this reason, in addition to advanced key storage and key generation technologies like PUFs and ECC, hardware devices should feature a pass-through patent license to DPA countermeasure capabilities such as those from Cryptography Research Incorporated (CRI). They should also provide for secure, remote, DPA-resistant update capabilities. The DPA pass-through license additionally allows users to harness the massive amount of computational capability in today's mainstream FPGAs to accelerate PKI transactions in a DPA-safe manner using DPA countermeasures. V2X networks that are protected in this manner will ensure safe and secure communication.