Aerolink®

SECURITY & PRIVACY FOR CONNECTED CARS

Aerolink is the industry-leading implementation of high speed communications security for connected vehicles based on the IEEE 1609.2 standard. First deployed in 2007, Aerolink has been continually evolving in parallel with the evolving standards, to remain the most up-to-date implementation of message authentication and user privacy for the Connected Vehicle system.

KEY FEATURES

OnBoard Security works within the key sectors of Intelligent Transportation Systems, from standards bodies to chip designers to on board equipment manufacturers, infrastructure providers and vehicle manufacturers. As an active and influential practitioner in this field, and as members of organizations such as **ITS America, OmniAir, Car2Car Communications Consortium** and **ETSI**, we have a deep understanding of the technical specifications and interoperability required to make highly secure platforms for Vehicle-to Vehicle and Vehicle-to-Infrastructure solution providers.

BATTLE TESTED

Aerolink was used in the majority of light vehicles in the Safety Pilot Model Deployment and is securing communications in the 2017 Cadillac CTS, the first production deployment of V2V technology.

HIGH SPEED SECURITY

Aerolink's patent-pending technology provides the optimal mix of security and performance.

PORTABLE & INTEROPERABLE

Aerolink includes support for cryptographic hardware for security and performance, including NXP, Renesas, Autotalks and many other leading semiconductor suppliers.

Unrivaled Expertise

As the editor of the IEEE 1609.2 standard for Connected Vehicle security, OnBoard Security has considerable experience in the development of security standards and is uniquely placed to ensure conformance with this very important specification from day one of the program.

OnBoardSecurity

STANDARDS-BASED

- Supports all Connected Vehicle certificate management protocols in North America and Europe
- Supports European Telecommunications Standards Institute (ETSI) as well as the Car-2-Car Communication Consortium requirements

UNIVERSALLY COMPATIBLE

- Compatible with multiple processors, architectures, operating systems, and hardware accelerators
- Includes a full suite of certificate management protocols and support for hardware acceleration — allowing on board equipment manufacturers to deploy a Connected
- Vehicle security system that is best-of-breed and fully interoperable, with minimum development effort and expense
- Designed to conform with the needs of highly stressed, automotive-grade environments
- Native support for multiple applications with transparent certificate management
- Full logging support for traceability, debugging and field testing
- Thread-safe and robust
- Well documented for easy integration — full SDK including documentation and sample code allows your developers to get working straight out of the box
- Automotive SPICE and MISRA C++ compliance to be completed in 2017

TECHNICAL SPECIFICATIONS

Implementation:

- Supports the secure message formats & processing as defined in IEEE Std 1609.2-2016
- Secure message formats & processing of ETSI TS 103 097
- Extensions to the secure message formats for certificate management, as agreed on by the Vehicle Infrastructure Integration Consortium (VIIC) and CAMP (Collision Avoidance Metrics Partnership)
- Supports US, European and other standards

Deployment:

- A directory structure containing shared libraries, headers, documentation, and demo applications for non-RPM compatible Linux
- A Windows port (library only, no installer)

Operating Systems:

- Linux 2.6.xx
- Windows 32-bit
- QNX version 6.6
- Green Hills Integrity version 11.x
- ThreadX G5.7.5.x

1.978.905.6796 ■ onboardsecurity.com