

Press release

ESCRYPT GmbH

Am Hain 5,
44789 Bochum, Germany
Phone: +49 234 43870-200

Press and Public Relations:
Martin Delle

martin.delle@escrypt.com
www.escrypt.com

High-performance IT security solutions protect V2X communication against cyberattacks

Connected driving is the future. However, data exchange between vehicles and roadside equipment will only become genuinely beneficial when it is securely protected against unauthorized access. Cybersecurity specialist ESCRYPT is unveiling its secure V2X communication solution at CES 2018 in Las Vegas.

The future benefits of V2X communication such as increased driving and traffic safety and intelligent traffic management are undeniable. It will help avoid accidents, shorten journey times, and make finding parking spaces a breeze. There is, however, an absolutely vital precondition: real-time communication from vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) must be reliably safeguarded from misuse, manipulation, and data spying. Even the thought that hackers could attack infrastructure and traffic management systems, create movement profiles, or access the onboard network communications of individual vehicles via V2X would deal a fatal blow to connected mobility.

Security credentials management: the security infrastructure behind V2X

V2X requires its own supporting security infrastructure which guarantees effective safeguarding of the mutual exchange of authenticated messages. ESCRYPT has developed software toolkits and security infrastructure products to help implement the Security Credentials Management System (SCMS) used to secure V2X communications. The system secures the communication of vehicles with each other and with roadside

equipment in two ways: by means of digital signatures, which protect messages against manipulation and unauthorized access; and by means of certificates, which identify the respective sender as trustworthy.

Overall, the V2X data exchange has to be secured on two levels: first of all, in the embedded systems themselves, in the vehicle ECUs, and in the roadside equipment's electronic controllers; and secondly, through a backend that effectively and securely manages the huge number of certificates required for secure V2X communication.

Complementary end-to-end solution:

Smart certificate management ensures authentication and anonymity

As a leading expert for automotive and IoT security, ESCRYPT provides complementary solutions that cover both these levels. The CycurV2X software development kit makes it possible for carmakers, tier-1 suppliers, and manufacturers of roadside equipment to implement V2X security protocols in their automotive embedded systems. To this end, CycurV2X supplies a robust V2X security solution that isolates the security infrastructure interfaces via a simple API. The special advantage of this system is that V2X security can be expanded seamlessly at any time – from cautious introductions through to real-time operation with fully comprehensive IT security functions.

In this complete solution, data security and data protection go hand in hand. The V2X messages are reliably authenticated at all times to ensure that only authorized vehicles and roadside equipment are communicating. In addition, the privacy of vehicle users is protected: the movements of road users cannot be tracked, as CycurV2X always holds a batch of concurrently valid certificates and replaces the active certificate with a new one on a rolling basis during the journey, at intervals of every few minutes.

With CycurV2X-SCMS, ESCRYPT also supplies the requisite backend security infrastructure components for the public key infrastructure. CycurV2X-SCMS offers here a

comprehensive, standards-compliant platform for the supply and blocking of certificates for vehicles and roadside equipment. Both solutions are compliant with North American and European standards. Moreover, in their performance capability and scalability, they are already designed to manage the permanent exchange of authenticated messages between millions upon millions of vehicles and roadside equipment.

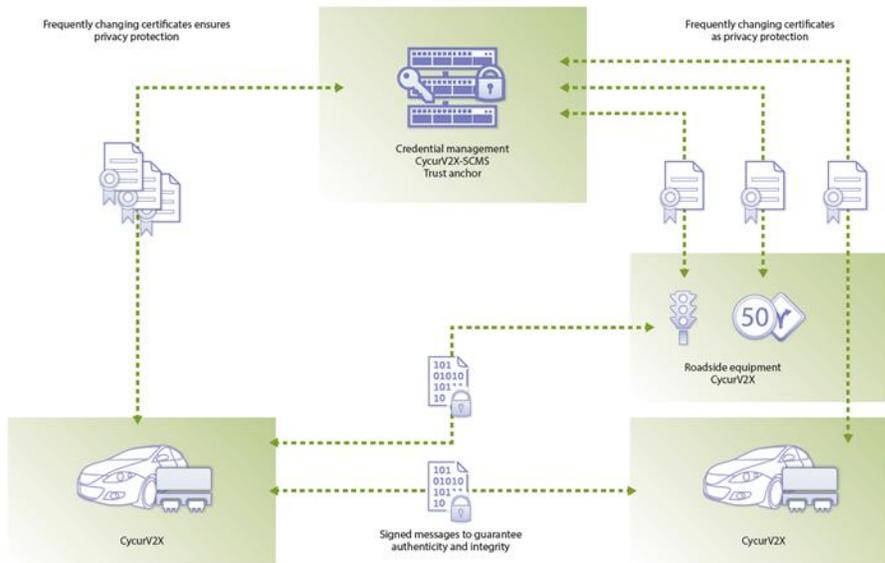
When completed, the V2X security system will be by far the largest public key infrastructure in the world. At the same time, it will have to provide space to various different players. Accordingly, the security design of the ESCRYPT solutions is based on a distributed architecture with a separation of roles. This allows auto manufacturers and the managers of intelligent transport systems (ITS) to work independently of each other in one system based on a single trust anchor. Vehicles and roadside equipment can securely exchange authenticated messages even if they are managed by different organizations between which there is no official connection. Equally, data protection and the anonymity of road users is guaranteed at all times.

Proven in ITS pilot projects

The CysurV2X solutions are demonstrating their practicality for providing a functioning V2X security infrastructure in several ITS pilot projects. In North America, for example, ESCRYPT has been working with the U.S. Department of Transportation and the Crash Avoidance Metrics Partnership (CAMP) initiative to support various reference projects for vehicle connectivity. In Europe, the German Federal Office for Information Security (BSI) entrusted ESCRYPT with providing the requisite public key infrastructure for secure V2X communication for the Cooperative ITS Corridor project.

Connected driving has moved way beyond just a model for the future. Thanks to intelligently linked IT security solutions, it is well on the path to becoming everyday reality.

Secure V2X communication at a glance



ESCRYPT GmbH - Embedded Security

Martin Delle

+49 234 43870-290

martin.delle@escrypt.com

ESCRYPT GmbH – Embedded Security

ESCRYPT - Embedded Security is the leading system provider for embedded security world-wide. With locations in Germany, UK, Sweden, USA, Canada, India, China, Korea, and Japan we have security specialists available to help with current security topics such as secure M2M-communication, IT-security in the Internet of Things, protection of e-business models and automotive security and they develop highly secure, worldwide valued products and solutions which are tailored to the specific requirements of embedded systems and the relevant IT-infrastructure and are tested and proven a million times in automotive series production.

For further information: www.escrypt.com