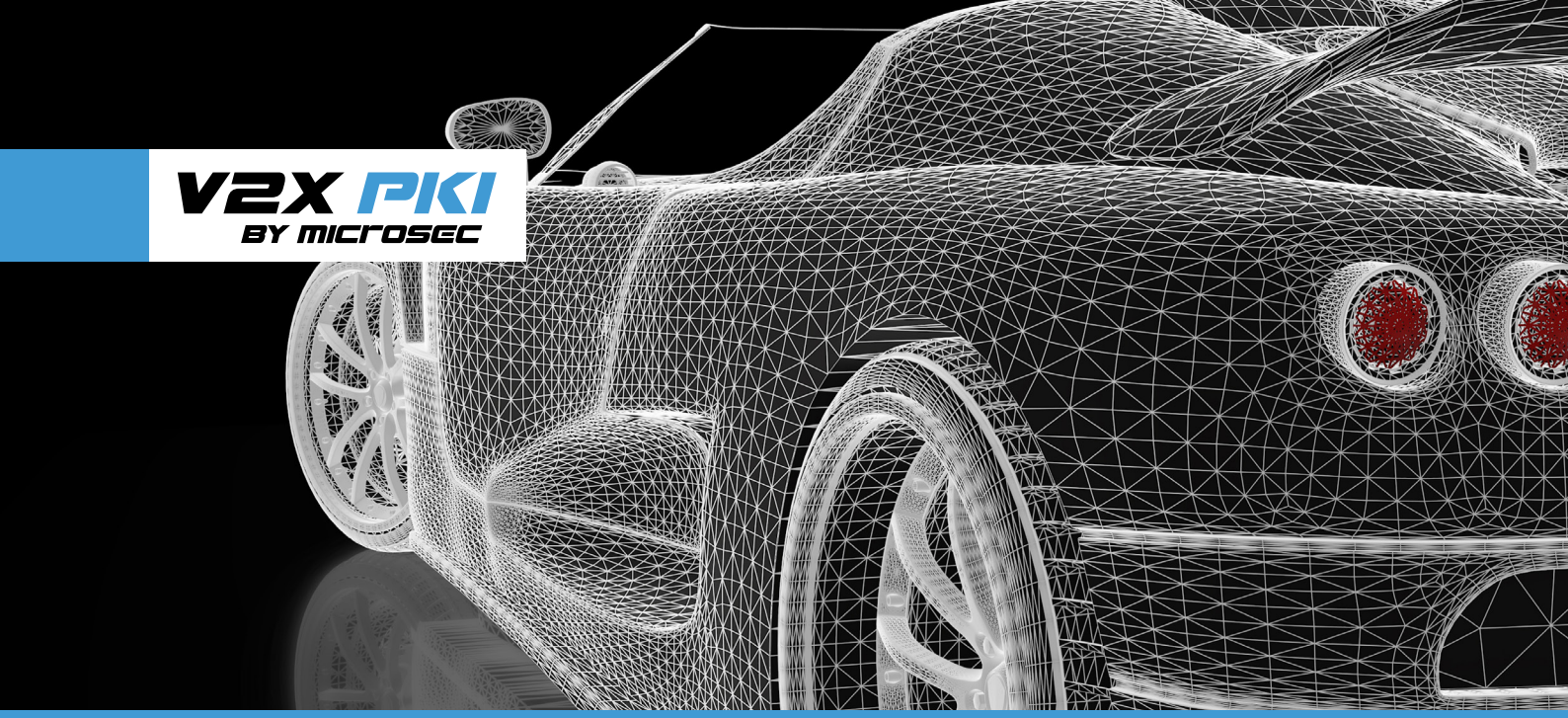

Introducing the Microsec V2X PKI security solution

About V2X public key infrastructures

If one works in IT security or a related field, they can hear the acronym “PKI” a lot. Some may know it stands for public key infrastructures, and even a couple of terms related to trust relationships and trust services, like certificate authorities (CA), website certificates and such. What most people do not know is the countless application fields for PKI; the usual association with it is digital signatures or timestamping, but among others, it can even be applied to connected vehicle communication.

Microsec V2X PKI is a security framework for providing the safety of vehicle-to-everything communication. In such environments, public key infrastructures are used to secure the environment by verifying the participants’ permissions with the usage of certificates. V2X PKI does this so with the most up-to-date cryptographic solutions, including Elliptic Curve Cryptography (ECC) which is a more secure encryption method than the widely used RSA algorithm.

Certificates are used in order to prevent unauthorized parties to interfere with the exchange of data and in order to pseudonymize the communication in a secure way. The hierarchy and mechanism of V2X PKI in a few words is the following: on top, there is a RootCA, that will issue certificates for two other authorities, the Enrolment Authority (EA) and the Authorization Authority (AA). The Enrolment Authority’s main task is to authenticate the car’s On-Board Unit canonical ID or certificate. If everything is in order, it issues a so-called Enrolment Credential (EC). The ECs are required by the AAs to issue Authorization Tickets which guarantee the pseudonymity of certificates as described in the standards.

Standard compliance and testing

The **Microsec V2X PKI solution** has been developed based on (thus compliant with) various standards and specifications; these, for example include the Institute of Electrical and Electronics Engineering (IEEE)'s WAVE and the European Telecommunications Standards Institute (ETSI)'s ITS standards, such as:

- IEEE Std 1609.2 (IEEE Standard for Wireless Access in Vehicular Environments);
- ETSI TS 102 940 (ITS-S security (PKI) architecture and application groups);
- ETSI TS 102 941 (Trust and Privacy Management);
- ETSI TS 103 097 (Certificate and message structure definitions for C2CPKI).

Microsec also pays attention to standardization processes and drafts, so when a new standard comes out, it is ready to be implemented.

Microsec V2X PKI has been tested on a number of occasions, in ETSI events even including ETSI's first C-V2X (Cellular Vehicle-to-Everything) Plugtests™, where, through test scenarios based on the above mentioned standards and specifications, Microsec's V2X team tested the interoperability of the V2X implementations created by the vendors present; these tests included road hazard signaling, road works warning, longitudinal collision risk warning and intersection collision risk warning. The tests were successful, as indicated in the event's overall 95% success rate.

The Microsec V2X PKI solution is ready to be used, offering public key infrastructure background that provides the framework through V2X certificates with full professional support for connected car test areas, car manufacturers, vendors, roadside and onboard unit developers, transportation and smart city infrastructure operators.

Microsec V2X PKI inter alia includes certificates for On-Board Units (OBU) and Road Side Units (RSU), also test track and pilot project certificates. There is even the possibility to require a unique PKI hierarchy or other solutions or consultation for security implementations.

A quick guide to get Microsec V2X PKI certificates

STEP 1 Please visit our registration site at **https://v2x-pki.com/** and fill in your details including certificates of interest. You will then be contacted by our Microsec V2X PKI administrators to clarify your exact requirements.

STEP 2 Based on the requirements, the administrators will make a recommendation whether the best solution is an offline certificate bundle or registration to the certificate authority. If the latter is the more suitable option, one can request certificates anytime based on authorization. The types of credentials Microsec needs for the infrastructure to work is based on this classification as well.

STEP 3 If it is more practical that the Microsec V2X PKI team generates the certificates, then the Public Key, Key Type (e.g. NistP256), the requested PSID and SSP pairs (if there is any specific except 36-01FFFC, 37-01FFFFFF and 141) and optionally Geographic regions (other than 250 and 380) are needed. If the requester is to be registered to the CA, the same details need to be given, supplemented by a Canonical Id.

STEP 4 Once these are provided and set up, the infrastructure is ready to go, and the requester is ready to test and use the certificates.

Please contact us and request the certificates at https://v2x-pki.com/

ABOUT MICROSEC

Microsec Ltd. is a mid-sized qualified trust service provider (QTSP) and a PKI technology expert independent software vendor (ISV), located in Budapest, Hungary. Regarding only V2X-related associations, the company is a member of the European Telecommunications Standards Institute (ETSI), the CAR 2 CAR Communication Consortium (C2C-CC) and the 5G Automotive Association (5GAA), also actively participating in the work of these organizations. The firm has partnerships with notable V2X-related manufacturers and test sites as well.