The CarPKI prototype

*The **CarPKI** prototype is the outcome of a cooperation industrial project being co-funded by the Federal Ministry of Economics and Energy within the Zentrales Innovationsprogramm Mittelstand: The aim of the "Universal and adaptable security solution for Car2x communication: Gateway, client-server security software and scalable PKI (**CarPKI**) project was to prototype a harmonized Public Key Infrastructure (PKI) for Car-to-Car and in-Car communication scenarios and to conceptualize a security blueprint for many other distributed, low cost, reliable embedded applications, be it in automotive, industrial, or home automation.*

Nowadays, security becomes a buzzword helping market divisions to increase company revenue, but growing global connectivity of devices turns security feature into a requirement. The latter applies to many fast-growing IT areas, such as: automotive, industrial automation, or cyber physical systems. Where security framework possesses a list of required components, such as: state-of the art cryptographic protocols, open and clear system design (Kerckhoffs' principle), process definitions and last but not least embedded systems support.

At the Institute of reliable Embedded Systems and Communication Electronics (ivESK) at Offenburg University of Applied Sciences we address all of the mentioned issues with one generic approach. From our perspective, the secure communication system of deeply embedded devices shall rely on a well-known, flexible and powerful protocol based on open standards, such as Transport Layer Security Protocol (TLS, and his derivative DTLS), commonly used in junction with HTTPS. Due to its flexibility, we believe it is a suitable solution not only for Ethernet and TCP/IP systems, but also for small, constrained control devices. Therefore, the ***CarPKI*** prototype aims to demonstrate a possibility to have strong security protocol based on PKI. Our framework was specifically designed, but not limited to in-Car communication system based on *CANbus*.

At the time of our research, there were no centralized effort to standardize security for in-car communication system, although standards for Car-to-Car communication exist. Therefore, our solution was derived from a PKI based on the European Telecommunications Standards (ETSI) Institute Intelligent Transport System (ITS) specifications. More precisely, we used *ETSI ITS* certificate structure, which in contrast to traditional X509 certificates requires significantly less data space (i.e. less than 200 bytes, against more than 400 bytes). Moreover we have implemented TLS protocol (an in-house software developed and continuously maintained for more than 12 years) with *ETSI ITS* certificates handler on top of a traditional CAN-bus widely used in automotive and automation domains. As embedded system carrier we used ARM Cortex M4 based and A9 based boards.

A corresponding standardization within the CAN in Automation e.V. (CiA) is ongoing.