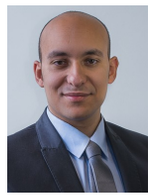


About the project

The **CarPKI** prototype is the outcome of a co-operation 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.

Authors:
M. Eng. Artem Yushev
Dipl.-Phys. Andreas Walz
Prof. Dr.-Ing. Axel Sikora
M. Sc. Mohammed Barghash

ivesk.hs-offenburg.de

Institute of Reliable Embedded Systems and Communication Electronics (ivESK)
Offenburg University of Applied Sciences
Badstraße 24, 77652 Offenburg

Prof. Dr.-Ing. Axel Sikora
Scientific Director
axel.sikora@hs-offenburg.de
Tel: +49 (0) 781 / 205 416

Project Webpage

Hochschule Offenburg
offenburg.university

ivESK Institut für verlässliche Embedded Systems und Kommunikationselektronik

ivesk.hs-offenburg.de

Secure End-to-End Connectivity over Field Busses

CarPKI

Institute of Reliable Embedded Systems and Communication Electronics (*ivESK*)

ivesk.hs-offenburg.de

Concept Goals

Make use of the European Telecommunications Standards Institute (ETSI) Intelligent Transport Systems (ITS) proposals and standards

Harmonize ETSI ITS Public Key Infrastructure (PKI) Car2X domain with the proposed in-Car PKI:

- Root Certificate Authority (RCA), Long-Term Certificates (LTC), Pseudonym Certificates (PC) from core ETSI ITS security architecture
- Electronic Control Unit Quality Seal (ECU QS or EQS) for permanent identity and In-Vehicle Certificates (IVC) for temporal identity

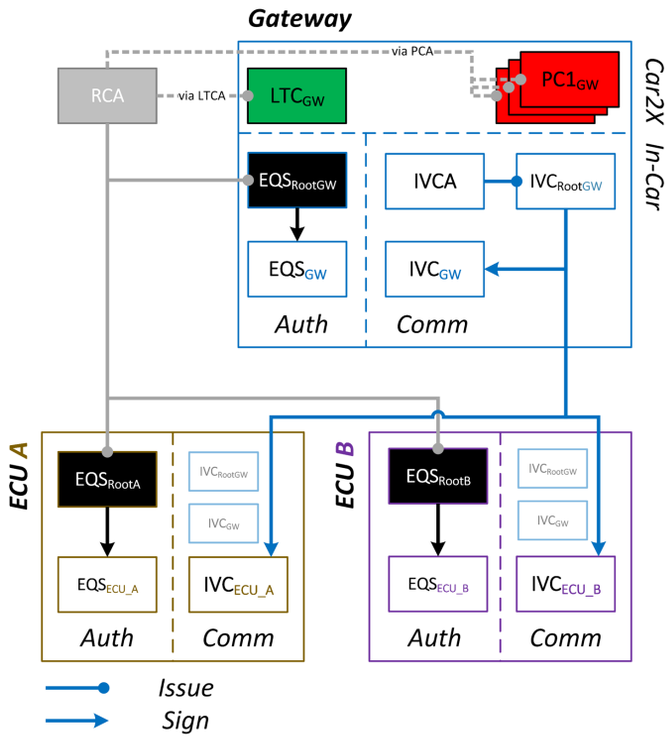
Use state-of-the art transport level security protocol TLS over a communication interface to protect sensitive data

Make security solution suitable for various field busses; e.g. CANbus

Use Elliptic Curves Cryptography; e.g. ECDHE and ECDSA

Use Symmetric Authenticated Encryption; e.g. AES128 in CCM mode

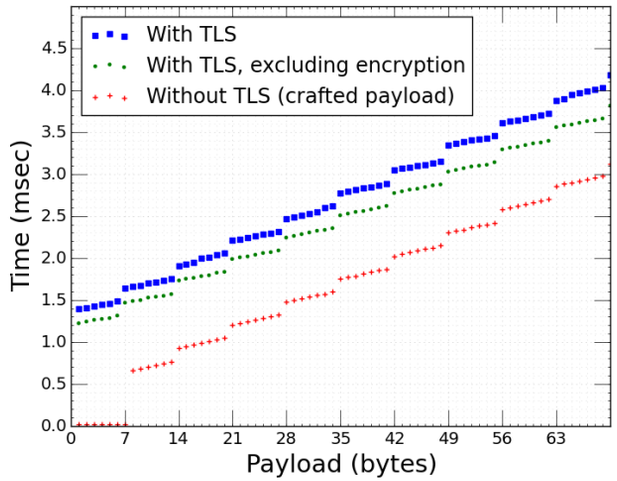
Architecture



Features

- 1 ms processing time per transaction for TLS with encryption (ARM Cortex™-M4)
- Static 21 bytes payload overhead due to encryption/ authentication
- More than 2 times smaller certificate size comparing to X509, 160 bytes per certificate

Security With Small Overhead



Because of extra 21 bytes overhead due to the security payload, the data-rate is lower comparing to non -secure transmission, although respective values for non-secure and secure cases; e.g. 70 bytes for the first and 49 bytes for the second (plus 21 bytes overhead) are of the same order.

Secure Handshake

- Full TLS 1.2 Handshake with Mutual Authentication using proposed certificates takes in average 0.5 s for Cortex-A9 and 5 s for Cortex-M4
- Secure TLS 1.2 session resumption takes less than 0.2 s.
- For the Handshake ECDHE_ECDSA based cipher suite

ivesk.hs-offenburg.de
ivesk.hs-offenburg.de