Secure Integration of a C2X Public Key Infrastructure
- Integration Support -

1 Motivation

The Public Key Infrastructure (PKI) is a key element of the security and privacy concept of C2X communications. All stations (i.e., vehicles and roadside units) that are equipped with a C2X communication unit have to be registered with the PKI and certificates have to be stored in the security subsystem of an On-Board Unit (OBU), as exemplarily depicted in Figure 1.

For this purpose, companies involved in the equipment of OBUs have to operate their own C2X PKI or have to use the service of an external Enrolment Authority (EA) and Authorization Authority (AA). In both cases, new enrolment processes are necessary that may affect existing production and distribution processes of vehicles and roadside units and require additional quality management tests.

There are at least two processes that have to be done before an OBU can be actively used for C2X communication:
Secure Integration of a C2X Public Key Infrastructure

2013-11-28 Secure Integration of a C2X Public Key Infrastructure

2 Offer of Fraunhofer SIT

Fraunhofer SIT offers support in the C2X pre-operation phase in order to prepare for a productive PKI. A fully functional test PKI can be used for internal and external integration tests and the evaluation of required processes. Furthermore, Fraunhofer SIT offers to support the PKI integration phase by elaborating concepts and developing solutions for a secure and privacy friendly integration of the C2X PKI into the production and maintenance environment of interested companies.

A generic basis C2X PKI developed by Fraunhofer SIT can be easily enhanced and adapted according to the customer’s specific requirements. Besides the integration tests, a test C2X PKI could be used for quality management tests during production, independent from final C2X certificates that are used after distribution.

Finally, Fraunhofer SIT offers to perform validation and penetration tests in order to ensure that the security and privacy protection demands are fulfilled.

The basis C2X PKI of Fraunhofer SIT provides the following key elements and functions:

- Pre-productive C2X PKI solution with Root CA (RCA), Enrolment Authority (EA), and Authorization Authority (AA) according to the PKI design of the Car-to-Car-Communication Consortium (C2C-CC)¹, ETSI TS 102 940 v1.1.1, and ETSI TS 102 941 v1.1.1.
- Security header and certificate formats according to:

¹ C2C-CC PKI Memo
Secure Integration of a C2X Public Key Infrastructure

- IEEE Std 1609.2-2013 or
- ETSI TS 103 097 v1.1.1

- Different interfaces for packet-based (i.e. UDP-IP) or session-based (i.e. SOAP web service using HTTPS) data transmission.
- A graphical user interface to easily operate and maintain the C2X PKI.

In summary, Fraunhofer SIT offers to provide a C2X PKI solution:

1. to support the PKI integration into the customer company’s infrastructure in the pre-production phase and
2. to allow C2X communication tests for quality management purposes.

3 Related activities of Fraunhofer SIT

Fraunhofer SIT is deeply involved in the European C2X security and privacy activities since 2008. In 2009 a first specialized C2X PKI was designed and subsequently implemented and operated within the German project simTD2. From 2011 on, Fraunhofer SIT developed and currently operates partly the C2X PKI of the European project PRESERVE3. Since 2013 the Pilot PKI of the C2C-CC4 is also partly operated by Fraunhofer SIT. Moreover, Fraunhofer SIT is deeply involved in the Task Force PKI of the working group Security of the C2C-CC and active as an expert in the security working group and its task forces of the European Telecommunications Standards Institute (ETSI) since 2010.

In order to identify possible future security and privacy issues Fraunhofer SIT is active in the scientific research for C2X PKI operation. Several publications were published and presented on international conferences regarding misbehavior detection in C2X communications and the related revocation of attackers.

---

2 http://www.simtd.de/index.dhtml/95c1d880c54c5c5ba95f/object.media/enEN/6468/CS/-/Backup_publications/Projektergebnisse/simTD-Deliverable-D215_Spezifikation_der_IT_Sicherheitslosung.pdf
3 http://www.preserve-project.eu/
4 http://www.car-to-car.org/
4 Contact at Fraunhofer SIT

Norbert Bissmeyer  
Fraunhofer Institute for Secure Information Technology (SIT)  
Mobile Networks  
Rheinstrasse 75, 64295 Darmstadt, Germany  
Phone + 49 6151 869-324 | Fax - 224  
norbert.bissmeyer@sit.fraunhofer.de

Dr. Kpatcha Bayarou  
Fraunhofer Institute for Secure Information Technology (SIT)  
Department Head of Mobile Networks  
Rheinstrasse 75, 64295 Darmstadt, Germany  
Phone + 49 6151 869-274 | Fax - 224  
kpatica.bayarou@sit.fraunhofer.de