sim^{TD} Security Architecture:

Deployment of a Security and Privacy Architecture in Field Operational Tests

Norbert Bißmeyer, Hagen Stübing†, Manuel Mattheß*, Jan Peter Stotz*, Julian Schütte*, Matthias Gerlach‡, Florian Friederici‡*

**Fraunhofer SIT, Germany, Secure Mobile Systems*
Email: {norbert.bissmeyer | manuel.matthess | jan-peter.stotz | julian.schuette}@sit.fraunhofer.de

†Adam Opel GmbH, Germany GME GTE E&E Advanced Engineering
Email: hagen.stuebing@de.opel.com

‡Fraunhofer FOKUS, Germany, Automotive Services and Communication Technologies
*Email: {matthias.*gerlach *| florian.*friederici*}@fokus.fraunhofer.de*

***Abstract*— sim^{TD} [1] is the worldwide first field operational trial for car-to-x (C2X) technology that applies several hundred vehicles and roadside stations in a real-life environment in order to evaluate the entire spectrum of applications with regard to effects on traffic safety and traffic efficiency.**

For a comprehensive integration of security into the sim^{TD} architecture several challenges have to be met. It has to be examined which security standards can be deployed with the given architecture. Adaptations and further extensions of common standards are necessary in order to fit the security and privacy mechanisms into the entire C2X architecture. Furthermore the security mechanisms have to deal with hardware restrictions due to the high availability requirements and the restrictions in terms of costs and resources that are typical for automotive environments. Finally novel concepts have to be developed with regard to the scale factor of the large fleet consisting of vehicles and infrastructure.

In this work we give a first glance on a near-series security architecture for C2X communications. We present the different concepts, protocols and cryptographic procedures used in sim^{TD}. Furthermore strategies to protect the driver´s privacy based on pseudonyms are proposed.

1. Introduction

Intelligent Transportation Systems (ITS) based on car-to-x technology are considered to be one of the most promising attempts towards the improvement of active vehicle safety and traffic efficiency in the near future. The term car-to-x (C2X) thereby refers to both, the information interchange between cars themselves as well as between cars and the infrastructure. That way oncoming and subsequent traffic is informed about potential danger so that the driver may react in time.

In sim^{TD} partners from the automotive domain, the telecommunication domain, the federal state government, several universities and research institutes have been gathered to validate technologies and applications for C2X communications in a setup that is representative for a realistic deployment scenario. For that purpose about 100 controlled vehicles with hired drivers are responsible for creating certain traffic situations where applications may be tested and validated. Additional 300 vehicles provide a permanent base load to the C2X network which makes the field trial comparable to the later deployment scenario. This so called “free flow fleet” ensures a sufficient covering of the test area, needed for a comprehensive forwarding of C2X messages inside the entire sim^{TD} network.

About 100 road side stations and two central traffic center are deployed in sim^{TD} to forward messages between the different ITS domains. The traffic centers are mainly responsible for smooth traffic flow and reduce traffic congestion as much as possible.

With such an infrastructure sim^{TD} is the worldwide first field operational test, large enough to examine the entire spectrum of C2X applications with regard to traffic safety and traffic efficiency.

[1] This work was funded within the project sim^{TD} by the German Federal Ministries of Economics and Technology as well as Education and Research, and supported by the German Federal Ministry of Transport, Building, and Urban Affairs. We are grateful to our colleagues at Audi AG, HTW (Hochschule für Technik und Wirtschaft des Saarlandes), Robert Bosch GmbH, Uni Erlangen, T-Systems, Volkswagen AG for their support, collaboration and valuable feedback.

Despite all benefits that the car-to-x technology contributes to traffic safety and traffic efficiency, such systems are highly vulnerable towards attacks against security and privacy. The challenges the sim^{TD} security architecture has to meet are manifold:

On the one hand, the sim^{TD} field trial itself has to be secured. Meaning, measurements taken during the field trial have to be reliable. A comprehensible and meaningful test evaluation is only possible, if all data flowing through the sim^{TD} network is properly secured (e.g., ensuring message authenticity). Already the possibility to inject false messages challenges the entire test results and thus has to be prevented by all means.

On the other hand the security architecture, just as the overall sim^{TD} architecture, is considered as a first prototype for a later roll-out of the C2X technology. Consequently, the sim^{TD} security architecture has to make use of existing standards and suggests new standards for later approval.

The security architecture has to meet requirements concerning authenticity, integrity and privacy of exchanged message as already elaborated in the IEEE 1609.2 standard [1]and various C2X projects such as Sevecom, NoW and Pre-Drive C2X[2]. Compared to these projects the sim^{TD} security architecture considers a heterogeneous communication network. Depending on its geographic validity, a message may be routed via several ITS stations using different communication protocols. This requires a seamless security protection of all protocols deployed in sim^{TD}.

Furthermore, the security architecture has to deal with limited resources. A Public Key Infrastructure (PKI) and all related activities impose additional workload onto all ITS stations as well as the wireless channel and have to be kept to a minimum.

This paper is organized as follows: In section 2 we give an overview over the sim^{TD} system architecture. Basic components and available communication channels are presented. Section 3.1 describes how existing security standards like IEEE 1609.2 [1] are applied in sim^{TD}. Security techniques based on cryptography and plausibility checks are presented in section 3.2. Furthermore their deployment on the different protocols in sim^{TD} is explained. The approaches for securing the different communication channels are presented in section 3.4. Section 4 focuses on privacy protection in sim^{TD}. Finally we conclude this paper in section 5 and give an outlook to the future work for the sim^{TD} security architecture.

2. System architecture of sim^{TD}

The sim^{TD} architecture aims at a comprehensive and seamless networking of vehicles and infrastructure. This goal is an ambitious challenge because many different protocols and data formats are required, and many stakeholders are involved. The multitude of sim^{TD} actors includes vehicles, roadside stations as well as infrastructural facilities for traffic and test management. Additionally, several third parties are involved to provide access to additional ITS services and support systems.

The main communication partners are furthermore distributed over a wide area including highway, suburban and urban scenarios. As a result, such a system requires a commonly accepted architecture and a seamless communication network for reliable and efficient information interchange.

Figure 1 shows the system architecture from the viewpoint of its individual components and their interactions. In general the sim^{TD} architecture involves three communication parties which are named accordingly to the ETSI terminology [2] as: ITS Vehicle Station (IVS), ITS Roadside Station (IRS) and ITS Central Station (ICS).

The ITS Vehicle Station is comprised of the Communication & Control Unit (CCU) and the Application Unit (AU). The components implemented on the CCU handle all communication from the physical up to the network layer. This includes the implementation of respective sender/receiver modules for each communication channel, as well as techniques for channel access and congestion control on top of it. Applications that require low latency are also running on the CCU. Beside the data derived from external communication, the CCU also

[2] See respective project web sites: http://www.sevecom.org, www.network-on-wheels.de, www.pre-drive-c2x.eu

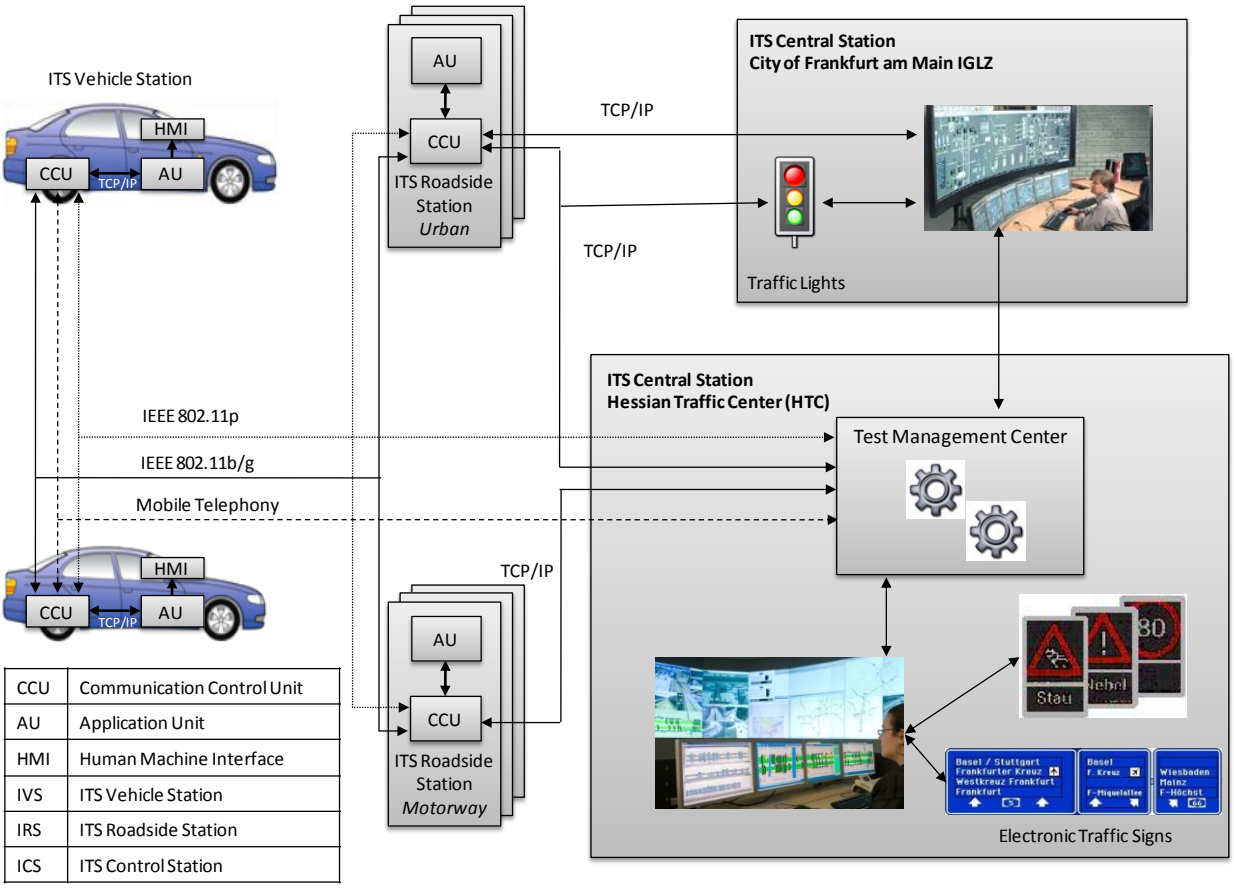
provides the AU with internal vehicle data observed via the CAN bus. Furthermore security components responsible for performing all cryptographic operations are located on the CCU. A detailed description of the entire security architecture is given in subsequent sections.

The Vehicle AU hosts the sim^{TD} applications. Connected to the CCU via Ethernet it receives the pre-processed messages and delivers them to the applications for further processing. All system components and applications are realized as Java/OSGi[3] Bundles. That way integration and remote management during the field trial may be realized in a comfortable and easy way.

As a direct interface between the ITS Vehicle Stations and the infrastructure the ITS Roadside Station is responsible for aggregating and forwarding the data between the different domains. Except for additional wired interfaces the ITS Roadside Station is composed of the same CCU than the ITS Vehicle Station. The AU is slightly different for both stations. A description of the IRS can be found in [3].

As mentioned before, the sim^{TD} test field consists of different types of road networks which are covered by two ITS Central stations. These are the Hessian Traffic Center (HTC)[4] which covers motorways, trunk roads and rural roads, and the IGLZ[5], which covers the urban road network.

As the central control instance the Test Management Center constantly monitors the communication flow inside the sim^{TD} network. Depending on the test scenario the Test Management Center is capable of directly influencing the test procedure.



CCU	Communication Control Unit
AU	Application Unit
HMI	Human Machine Interface
IVS	ITS Vehicle Station
IRS	ITS Roadside Station
ICS	ITS Control Station

Figure 1: sim^{TD} System Architecture

[3] See respective OSGI alliance website: www.osgi.org
[4] Hessian Traffic Center (HTC) stands for Verkehrszentrale Hessen (VZH) and is the ITS Central Station of the Hessian State Office for Road and Traffic Affairs
[5] IGLZ (Integrierte Gesamtverkehrs-Leitzentrale) is the ITS Central Station of the City of Frankfurt am Main

The sim^{TD} architecture basically integrates three communication channels which differ in technology and functionality:
The main communication flow will be processed among IVSs and respectively between IVSs and IRSs. For single-hop communication those stations use the 802.11p standard. Most safety and traffic efficiency related messages require low latency and are therefore exchanged via this communication link. These so called *C2X Messages* are further divided into subtypes where CAMs (Cooperative Awareness Message) and DENMs (Decentralized Environment Notification Message) are two examples. CAMs are considered as regular beacons that are broadcasted with maximal 2 Hz in the direct neighborhood, used as basis information by nearly every application. Additionally the mobility information from these messages is used on the network layer in order to implement message dissemination per geo-routing and store-and-forward [4] mechanisms. Compared to CAMs the DENMs are always related to local events and used by applications to distribute safety related warning messages. IP-based communication is possible on the entire sim^{TD} test area using GPRS, EDGE or HSDPA. It is used as a store-and-forward infrastructure for distributing certain safety and traffic efficiency related messages between remote areas which cannot be connected by the single-hop 802.11p communication due to its limited reception range. Furthermore ITS Vehicle Stations use these access links to establish IP-based communication via Internet with the Test Management Center or other backend services. The 802.11b/g communication link is dedicated for IP based connections. In a test phase this communication standard is also used for safety and traffic efficiency related message exchange.

3. Data security in sim^{TD}

The sim^{TD} security concept is based on asymmetric cryptographic which includes mechanisms to ensure authenticity, data integrity and confidentiality. In simTD, in-car security is considered out-of-scope, i.e. the hardware and software platform as well as the cryptographic key material inside the IVS are assumed to be authentic. Every participant in the ITS is equipped with a key pair consisting of a private key and a public key including the corresponding certificate that is signed by a Certification Authority (CA) placed inside the Test Management Center. Certificates used for signing C2X messages are called pseudonyms.

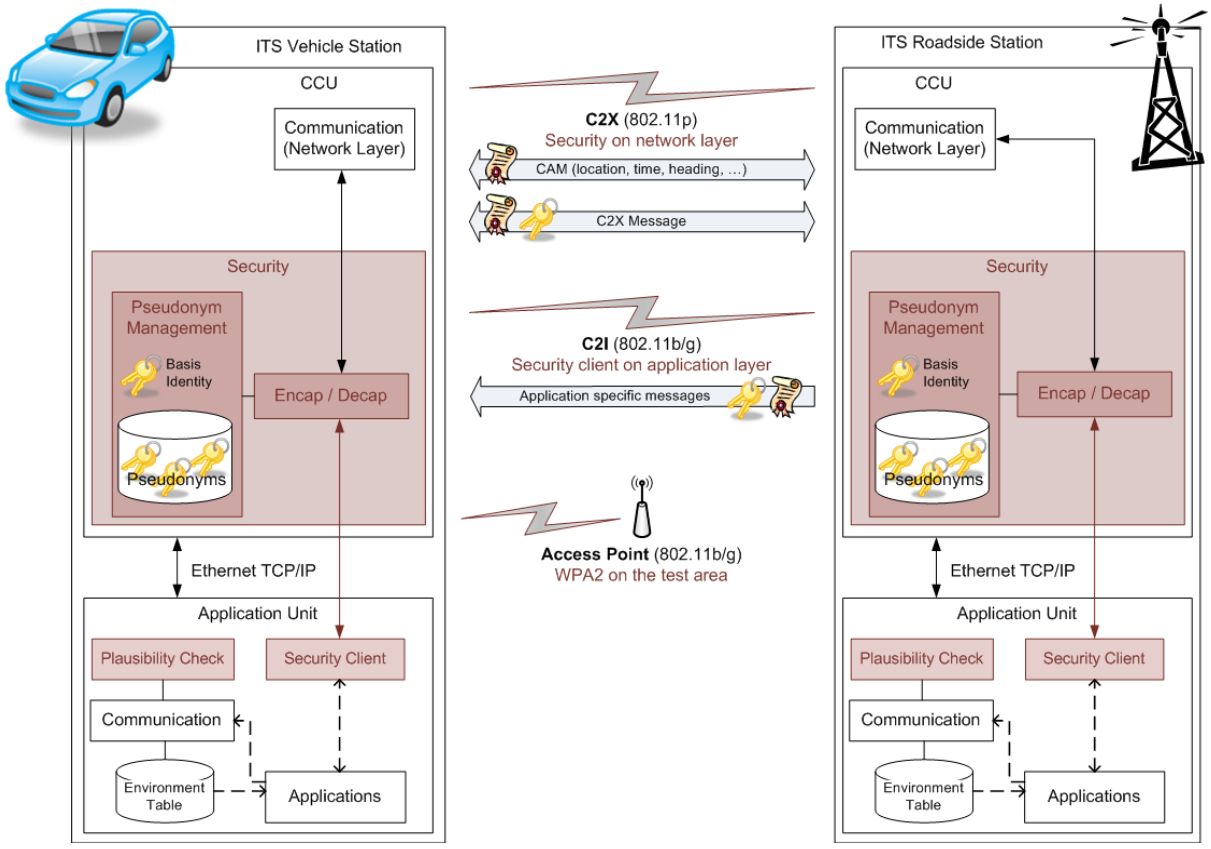


Figure 2: Security in C2X Communication

The following section presents the applied security standards as well as their embedment into the system architecture. Subsequently details are presented for integrity and confidentiality checks of incoming messages and their content. Finally the security concepts for the different communication channels are discussed. Figure 2 provides an overview of the security components used in vehicles and roadside station.

3.1. Deployment of IEEE 1609.2 in sim^{TD}

sim^{TD} is expected to provide valuable information to common security standards such as IEEE 1609.2 – WAVE (Wireless Access in Vehicular Environments) [1]. IEEE 1609.2 is especially developed with respect to communications in wireless vehicular networks and therefore taken as a reference for the sim^{TD} security concept. Due to special requirements regarding the overall sim^{TD} system architecture parts of the specifications had to be adapted and extended.

The exchange of mobility information such as position, speed, heading and corresponding timestamp, is performed in sim^{TD} on the network layer of the OSI Reference Model. In order to apply multi hop communication or store-and-forward mechanisms a dedicated network layer protocol for C2X Communications has been created [5]. To guarantee the integrity of all data outgoing network messages have to be signed. Compared to IEEE 1609.2, where the signing of messages is supposed to be done on the application layer, in sim^{TD} the sign and verify process is shifted down to the network layer. The message formats, as defined in IEEE 1609.2 had to be extended accordingly to enhance this decision. A more detailed description of the sim^{TD} secure message format is given in section3.2.

Due to hardware restrictions in sim^{TD} all crypto operations have to be executed on general purpose hardware. Using Elliptic Curve Digital Signature Algorithm (ECDSA) as proposed by IEEE 1609.2 would result into an inacceptable computation delay. In contrary, the usage of RSA algorithms provides faster verification times than ECDSA as shown in Table 1. The larger security overhead of approximately 25% with RSA compared to ECDSA is outweighed by approximately 28 times faster verification and approximately 5 times faster signature processing. The application of symmetric keys in sim^{TD} is not acceptable because basic functionality cannot be applied.

Criterion	ECDSA 256	RSA 512 / 1024	Symmetric Keys
PKI necessary	Yes	Yes	No
Key distribution	Yes	Yes	Yes
Revocation possible	Yes	Yes	No
Additional HW	Yes (Crypto HW , PKI)	Yes (PKI)	No
Verification time	> 54 ms	~ 1.9 ms	< 1 ms
Security overhead per message	~ 200 Byte	~ 250 Byte	~ 60 Byte
Authentication	Yes	Yes	No
Auditabilty	Yes	Yes	No
Risk (Security)	Low	Low - Medium	Medium - High
Privacy	Yes	Yes	No
Experience for Future ITS	Yes	Yes	No
Standards	IEEE 1609.2	Adapted IEEE 1609.2	No C2X

Table 1: Comparison of Cryptographic Algorithms

For the sim^{TD} security architecture a compromise had to be found to match requirements regarding small key size and fast verification time. In order to solve this conflict a RSA solution based on different key sizes and regular updated certificates is proposed. For the signing of C2X messages, certificates with 512 Bit key size are issued while 1024 Bit keys are used by vehicles, roadside stations and the Certificate Authority (CA) in the request process of new pseudonyms. As a consequence of the shorter key sizes the validity period of

certificates has to be reduced. This further requires a frequently change of pseudonyms as detailed in section 4.2.

3.2. Security based on Cryptography

All cryptographic operations in sim[TD] are running on the CCU and are performed by a component called *Security Daemon* [6] which is available as open source software[6]. The Security Daemon is responsible for guaranteeing message authenticity, integrity and confidentiality by means of cryptographic primitives.

The CCU itself is equipped with a 400 MHz processor based on PowerPC architecture[7] which is already heavily occupied by several network applications. The possibility to unload the main processor by shifting cryptographic calculations to an attached DSP Co-Processor is currently under evaluation in sim[TD]. In general the limited hardware resources available on the CCU represent a main challenge for the security in sim[TD]. In situations with high vehicle density such as crossroads or traffic jams the amount of messages to be verified may increase so that a cryptographic verification of all messages becomes hardly realizable. For that purpose a fall-back strategy is applied. In order to complete the security architecture light-weighted plausibility checks are performed on higher layers as it will be discussed in section 3.3.

Every outgoing C2X message is signed per default by the Security Daemon. If requested by one of the applications, the message is also encrypted. For signing or encrypting a message the network layer component hands over the complete network packet to the Security Daemon including transport header and payload. The Security Daemon signs or encrypts the packet and returns a security header without integrated payload. In case of encryption the encrypted payload is additionally returned and substitutes the unencrypted application payload in the C2X message as displayed in Figure 3. Subsequently the secured network packet is forwarded to the message queue for transmission.

The procedures for signing and encryption are following the IEEE 1609.2 standard and the certificates used in sim[TD] are conform to this standard. The final message composition is illustrated in Figure 3. Contrary to IEEE 1609.2 the newly developed security header formats do not contain the payload. In case of signing only the signature of the payload is stored in the security header as well as further security information defined by IEEE 1609.2.

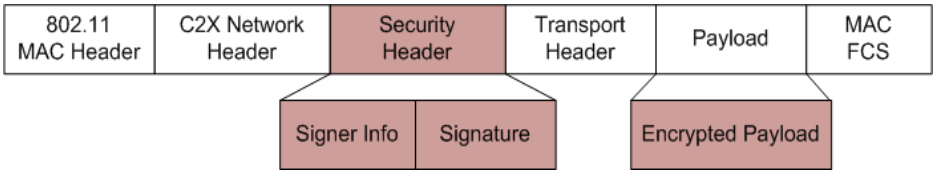


Figure 3: Sim[TD] C2X Message Format

3.3. Security based on Plausibility Checks

The plausibility checks are integrated into the communication stack and responsible for the detection of faulty information in C2X messages. Especially the plausibility check of message content is important in sim[TD] because faulty vehicles and roadside stations have to be detected. Faulty nodes can be manually deactivated or excluded from the C2X communication afterwards. All messages are stored in an environment table after the cryptographically security checks and the plausibility checks are done. Subsequently, the applications are able to access the messages including the results of the security and plausibility checks.

The plausibility component is placed on the AU in order to access additional information such as observed data from the CAN bus. The plausibility checker pursues different strategies to detect messages with faulty content:

At first the messages are checked regarding the contained mobility information. This includes checks on the geographical position, speed, heading, acceleration and accuracy of the mobility data. Furthermore, the plausibility component checks the sending frequency of incoming messages from adjacent nodes in order to

[6] See respective web site: http://certifiedc2x.berlios.de/
[7] See respective web site: http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=MPC5121e

avoid Denial of Service (DoS) attacks. Finally, the movement plausibility of all adjacent nodes is evaluated constantly.

3.4. Security concepts for the different communication channels

IEEE 802.11p
All messages transmitted via IEEE 802.11p are handled by the Security Daemon on the network layer. The messages are signed by default as described in section 3.2. Unicast messages that contain confidential information are additionally encrypted.

IEEE 802.11b/g
The communication via commercial WiFi (IEEE 802.11b/g) is used in sim^{TD} for different purposes. On the one hand, existing security concepts of sim^{TD} can be used but on the other hand standards have to be adapted to functional requirements.

At first, the commercial WiFi will be used as an extension to IEEE 802.11p in order to exchange C2X messages. In this case the same security mechanisms are applied in the same way as proposed in section 3.2.

In the second case, WiFi Access Points owned by sim^{TD} are provided that can be used for direct IP communication between vehicles and the Test Management Center. These Access Points are dedicated for transmitting log files for test evaluations and are therefore only available on car-parks and the test area of sim^{TD}. In order to secure the communication, encryption via IEEE 802.11i in personal mode (WPA2) is proposed. All Access Points and vehicles are equipped with a common secret that is used as symmetric key. In the case of a compromise of symmetric key all Access Points and vehicles have to be updated with a new key. The access to the Test Management Center is secured by firewalls.

The third purpose of IEEE 802.11b/g concerns the distribution of application specific messages from roadside stations to vehicles via broadcast. UDP/IP is defined as transport protocol with previously defined port numbers for the applications. Due to the fact that the data transmission via Internet Protocol (IP) is transparent for the CCU communication stack, security mechanisms such as signing or encryption have to be applied on application layer. Contrary to the security mechanisms implemented for the communication via IEEE 802.11p the standard mechanisms of IEEE 1609.2 are used for securing the UDP/IP communication via IEEE 802.11b/g. All outgoing messages have to be encapsulated by a security stub of the Security Daemon on the AU by adding the application payload to a secure message according to the WAVE standard. The application on the receiving vehicle has to listen on the predefined UDP port. Every incoming message has to be decapsulated by the security stub of the Security Daemon on the AU in order to get the payload from the secure message.

Cellular Communication
The data transmission via cellular networks can be divided into two different types:

In the first case application specific TCP/IP data is transmitted over the cellular network between mobile participants such as vehicles or special roadside stations and the Test Management Center. In sim^{TD} all mobile nodes are equipped with a special SIM card from the mobile network provider. The special equipment enables the nodes to use a Virtual Private Network (VPN) between the gateways of the mobile network and the Test Management Center network. As result the security components of sim^{TD} are not responsible for implementing secure end-to-end tunnels between mobile participants and the Test Management Center. This solution is used in sim^{TD} in order to save valuable resources on the vehicle and roadside systems.

In the second case C2X messages are transmitted via cellular communication between vehicles and a routing system of the Test Management Center. For securing this communication no additional concepts have to be implemented. The transmission of all information over the mobile network is encrypted as described above and integrity of C2X messages is guaranteed by means of signatures that are applied by the Security Daemon.

4. Privacy protection in sim^{TD}

In order to protect the driver's privacy, the vehicle should not be traceable over a long time by internal or external systems. Nevertheless, an overview of the exact location of all vehicles is provided in sim^{TD} for the trial control and its evaluation. Digital certificates build the basis of the sim^{TD} security architecture that are changed frequently as discussed in section 4.2. They are used for realizing authentication, message integrity, confidentiality and privacy of exchanged C2X messages. In order to achieve these security goals different certificate types are used.

At first, every system in sim^{TD} that is involved in the C2X communication is equipped with a basic identity. This identity is requested by the vehicle or roadside station from a central Public Key Infrastructure (PKI). The response contains a 1024 Bit RSA key signed by the CA. The basic identity is only used for requesting further pseudonyms.

The pseudonyms applied in sim^{TD} consist of certificates with 512 Bit RSA key pairs that are used for signing and encrypting C2X messages. The validity time of these pseudonyms is restricted to 24 hours due to the short key length. Vehicles in sim^{TD} are equipped in the deployment phase with enough pseudonyms for the whole test phase in order to cover outages. The driver's privacy is protected by additional pseudonyms that are requested by every vehicle on top of the basic pseudonym pool. The pseudonyms requested in this process are valid for short future time slot. If the vehicle has enough pseudonyms, then a regular pseudonym change is processed. Otherwise the pseudonym is only changed as soon as the validity is expired. The roadside stations do not have to consider privacy issues. But following the communication security concept, it is reasonable to use for all messages the same pseudonym certificate type. Due to the key lengths of 512 Bit RSA keys the roadside stations have to change their pseudonym regularly as well.

All basic identities and pseudonyms are signed in sim^{TD} by the CA (Certification Authority) of the PKI. The self-signed certificate of the CA must be valid for the complete test phase of sim^{TD} and therefore a long RSA key pair is used. The CA certificate is distributed at the deployment phase of sim^{TD} systems.

4.1. Distribution of pseudonyms

The automated distribution service in sim^{TD} provides digital certificates such as the basic identities in the deployment phase and pseudonyms in the subsequent test phase. It is designed to transmit public keys from the requester to the PKI and responses signed certificates. Figure 4 provides an overview of the involved parties.

In the deployment phase of sim^{TD} the basic identity can only be requested if the system is equipped with a digital token. This token and the CA certificate are stored manually on the vehicle or roadside station and can be used subsequently as trust anchor for the request of the basic identity. As soon as the signed certificate of the basic identity is responded, pseudonyms can be requested. The cellular network communication is used by the distribution service, because it guarantees a confidential transmission and it is widely available in the field operational test area of sim^{TD}.

Before the pseudonym pool is empty the security system generates several new pseudonym key pairs and stores the private keys in the local database. The public keys are signed by the basic identity and subsequently transmitted to the PKI. This request is appended with a snapshot of the software configuration in order to check the validity of the vehicle or roadside station software components. Both, pseudonyms and software configuration are signed and transmitted subsequently to the Test Management Center. Finally the PKI creates the pseudonym certificates, sends them back to the requester and creates a link between the basic identity and the issues pseudonym in the PKI database.

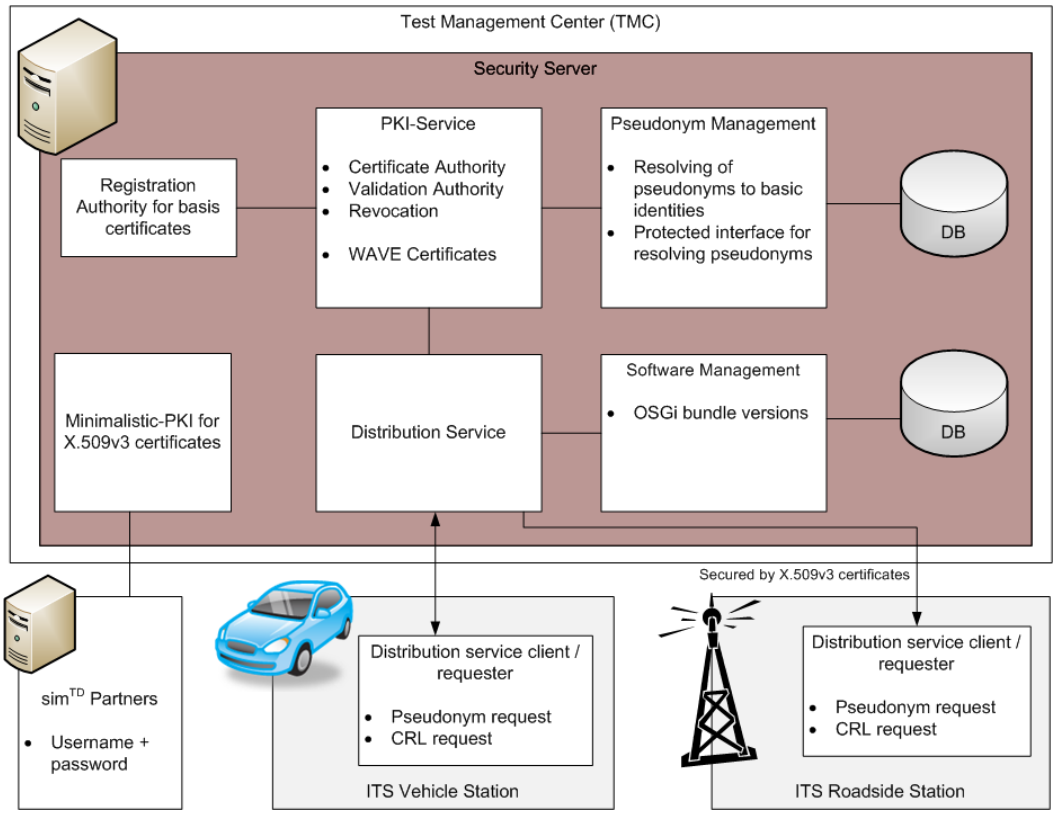


Figure 4: Security Systems in the Test Management Center

In the sim[TD] security concept a Certificate Revocation List (CRL) is necessary because a basic set of pseudonyms are distributed for the complete test phase. In case of a compromise all valid pseudonyms of the affected system have to be revoked. The CRL is requested regularly with the distribution service. The Security Daemon ensures during every message verification process that the pseudonyms are valid and have not been revoked.

4.2. Pseudonym Change

A concept of changing pseudonyms is implemented in sim[TD] in order to protect the driver's privacy needs. Furthermore, the main intention is the evaluation of privacy mechanisms in the context of the overall system architecture, because it has been shown that a security architecture for a series production is only accepted if privacy aspects are considered.

With a irregular pseudonym change approximately every 30 minutes the vehicle obfuscates its mobility track because all identifiers of the vehicle are changed without external notification. For some sim[TD] applications it is important that the pseudonym change is not performed in critical traffic situations. Therefore, the security system provides an interface to the applications that can be used to block pseudonym changes. If a lock is active then an upcoming pseudonym change is delayed until the situation is uncritical from the point of view of all active applications.

4.3. Pseudonym management on the vehicle and roadside station

As previously mentioned the ITS Stations have to manage different types of digital certificates. At first the vehicle or roadside station stores the CA certificate and the basic identity. In the deployment phase all systems that are involved in the C2X communication have to request a basic set of pseudonyms that cover the sim[TD] field operational test runtime. This basic set of pseudonyms is used at systems that do not need to consider privacy protection such as roadside stations. Vehicles are requesting additional pseudonyms that can be changed regularly in order to consider the privacy protection. Due to the fact that WAVE certificates are applied in sim[TD] that are much smaller – approximately 200 Bytes – the restricted disc space on the CCU is not a major problem.

Furthermore the public key and a fingerprint of all pseudonyms of adjacent ITS Stations are stored with a link to their current MAC address in the database of the vehicle or roadside station pseudonym management. If a message should be encrypted and transmitted per unicast this link is important. Additionally, the fingerprint of the pseudonym is used for an optimization strategy in the verification process.

4.4. Central pseudonym management

Figure 4 provides an overview of the applied security components in the infrastructure. The security server inside the Test Management Center is running a PKI that is responsible for the management of WAVE certificates. It is also providing a minimalistic PKI that manages self-signed X.509v3 certificates for securing the access of sim^{TD} partners to all sim^{TD} systems including the Test Management Center. The central component of the distribution service is connected to the PKI for creating and signing the requested basic identities and pseudonyms. Furthermore the distribution service checks the software components of the requester with the central software management. In order to provide the resolvability of pseudonyms for later field trial evaluation a database is maintained that links the basic identity to issued pseudonyms.
The revocation is applied in sim^{TD} in two ways. At first the basic identity is internally revoked in the PKI as soon as a node is compromised. Every pseudonym request of this node is subsequently revoked by the PKI. Secondly, pseudonyms have to be revoked that are issued for a future time interval as described in section 4.3. As described in section 4.1 the vehicles and roadside stations are requesting the CRL regularly from the central distribution service.

5. Conclusion and Outlook

The presented security architecture considers data integrity, authenticity, confidentiality and privacy individually for the communication channels used in sim^{TD}. In order to support current standardization efforts this security architecture applies the standard IEEE 1609.2. Due to functional requirements and restriction in sim^{TD} the standard has to be adapted. Developed systems such as distribution services and the PKI have to be enhanced for a future deployment. The security and privacy protection mechanisms discussed are deeply integrated into the system architecture. Therefore, the results of the field operation test can provide valuable information for subsequent implementations of a secure ITS.

For future implementation, the protection of in-vehicle systems should be considered by using special hardware. For the application of ECDSA cryptographic algorithms further hardware is necessary that is not available in sim^{TD}. Finally, the experience from the field operation test can be used in order to enhance privacy protection mechanisms.

References

[1] I. T. S. Committee, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," IEEE Vehicular Technology Society Standard 1609.2™-2006, 2006.

[2] ETSI, "Intelligent Transport Systems (ITS); Communications; Architecture," ETSI Draft TS 102 665, 2009.

[3] H. Wieker, et al., "Management of Roadside Units for the SIM-TD field test (Germany)," in *16th World Congress and Exhibition on Intelligent Transport Systems and Services*, Stockholm, 2009.

[4] Car-to-Car Communication Consortium. [Online]. www.car-to-car.org

[5] A. Festag, et al., "CAR-2-X Communication SDK - A Software Toolkit for Rapid Application Development and Experimentations," in *Workshop on IEEE Vehicular Networking and Applications Workshop - Future Wireless Technologies for Vehicle Infrastructure Integration (VII) Applications (VehiMobil 2009)*, Dresden, 2009.

[6] Gerlach, M. & Friederici, F., "Implementing Trusted Vehicular Communications," in *VTC2009-Spring*, Barcelona, 2009.

[7] SIM-TD. [Online]. http://www.simTD.de