Allianz

Guidelines

AZT Automotive GmbH * Allianz Center for Technology

Requirements for “virtual vehicle keys”

Technical guidelines for implementing networked and security-critical functions from the insurance company’s perspective

Version dated March 18

TABLE OF CONTENTS

1. Introduction

Theft is a dominant theme in motor insurance and is characterized by high average damages. This leads to significantly increased claims costs for a large number of vehicle models. Theft includes not only total theft, which is significantly related to the vehicle type, but also partial theft and theft from the vehicle, which is accompanied by high consequential damages.

Nowadays, the development and integration of electronic components in the automotive industry is taking on a new dimension, in that an increasing number of innovative, networked convenience and customer functions are being put on the market. Among other things, OEMs also offer their customers a virtual key as an application on a mobile end device, in addition to the conventional physical vehicle keys, and other digital after-sales services which are based on global networked systems. Current and future developments in the consumer and automotive industries result in new attack vectors on interfaces between the entities of these networked systems.

In this document, the Allianz Zentrum für Technik [Allianz Center for Technology] presents the requirements for the ”virtual vehicle keys” from the insurance company’s perspective, which are intended in particular to make the access and driving authorizations secure. Automakers can meet these requirements when designing the system and protecting it against misuse. At the same time, they take requirements regarding underwriting and forensics in the case of a claim into account.

The following requirements are the result of a generic risk analysis and therefore leave room for implementing digital business processes, technologies such as cloud computing or the use of mobile devices. The risk analysis was carried out by the Fraunhofer Institut für Sichere Informationstechnologie [Fraunhofer Institute for Secure Information Technology] SIT on behalf of the AZT and in principle can be applied to any networked system where the vehicle itself is to be considered a self-contained participant and can be replaced or enhanced by a mobility concept.

The requirements defined in this document are based on the technical guidelines of the Bundesamt für Sicherheit in der Informationstechnik [German Federal Office for Information Security] BSI, which specify the IT baseline security[1] in Germany through necessary IT measures and methods. The specifications of the BSI are regarded as minimum requirements and should be taken into consideration and implemented in the development process to ensure system reliability. As a counterpart to the BSI, the National Institute of Standards and Technology (NIST) in the USA, for example, is responsible for standardization processes in IT security.

In the following, a relevant reference architecture with the entities involved will firstly be described. This results in the requirements for the “virtual vehicle keys” as a system networked via multiple entities. Lastly, the requirements for the forensic process will be set out.

2. Reference architecture and process sequence

In Figure 1, a possible reference architecture for the “virtual vehicle keys” (VVK) ecosystem and the entities involved in the context of virtual vehicle keys are shown.

The ecosystem essentially consists of three entities:

1. a vehicle
2. a backend
3. a user with their mobile end device (MED).

To maintain the clarity of the figure and the subsequent descriptions, the vehicle and the user are each considered to be a single entity, however, the architecture shown here also remains valid when scalable to multiple vehicles and users with corresponding mobile end devices (e.g. including combinations of smartphones and smartwatches). From this architecture, car-sharing concepts can be derived, such as the multi-user case, in which multiple users are given access to one vehicle or, as in the multi-key case; it is possible to access multiple vehicles by means of a mobile end device.

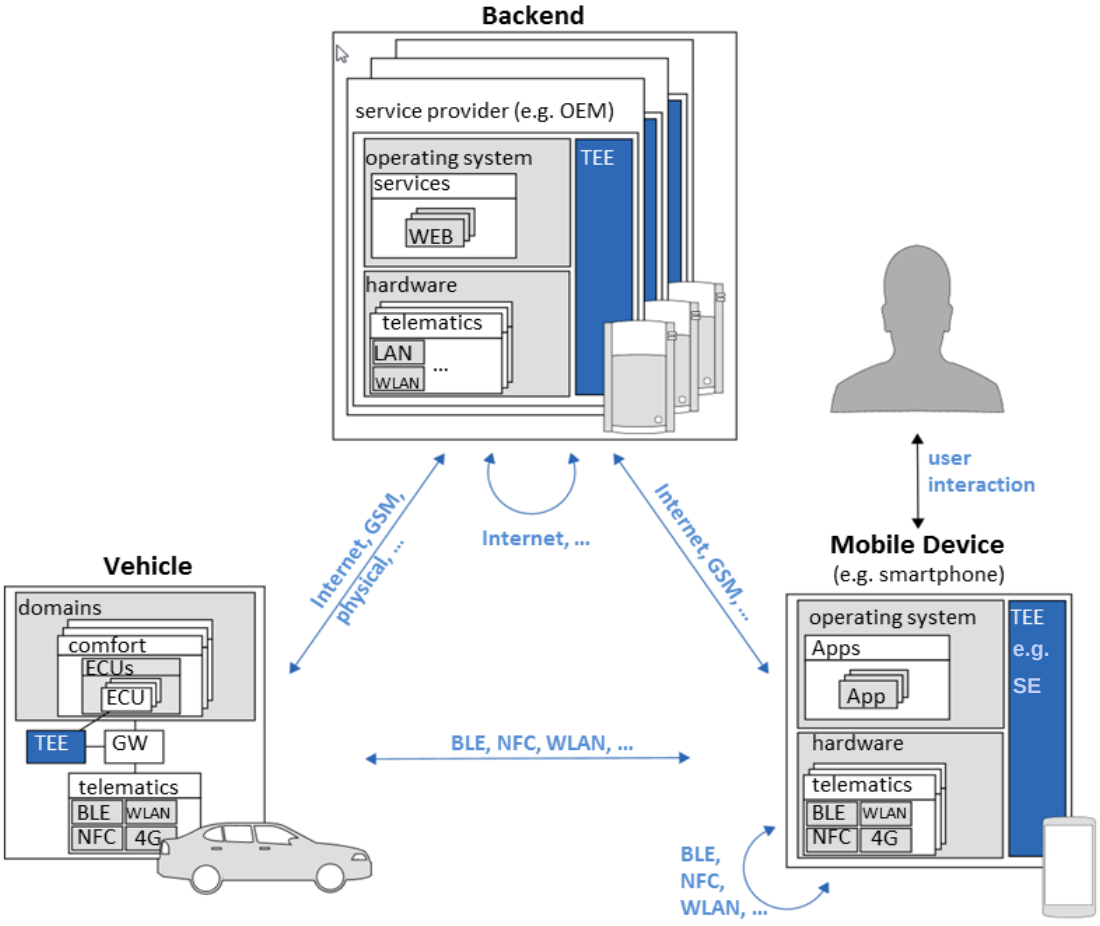

Figure 1: Ecosystem and entities involved

The reference architecture is intentionally kept simple so as not to restrict the functional design and to make it possible to include new technologies whose development cannot be foreseen at the present time.

The backend can be operated by various parties' service providers (SP) (e.g. original equipment manufacturers (OEMs), mobile network operators (MNOs), distributors, car-sharing providers). Furthermore, the mobile end device includes for example smartphones, smartwatches and tablets, that is to say all the devices which are carried around by the user as an ever-present companion.

As can be seen in Figure 1, the individual entities communicate with one another via various interfaces and communication connections. The communication between the vehicle and the backend, and between the mobile end device and the backend can take place for example via an internet connection or a Global System for Mobile communications (GSM) connection. This communication should take place exclusively via mutually authenticated channels to ensure the clear authentication of the communication participants. This measure protects against threats from (entity) spoofing or against the authorized sending of unencrypted messages on the bus system in the vehicle.

For communication between the vehicle and the mobile end device, short-range wireless technologies such as Bluetooth Low Energy (BLE), Near Field Communication (NFC) or Wireless Local Area Network (WLAN) can be used in ad-hoc mode, which allows a direct connection between the two entities without interposing infrastructure. In order to avoid replay and MitM attacks which are already known, only the short-range wireless technologies should be used, which can be found in the recommendations by the BSI. An indirect connection from the mobile end device to the vehicle via the backend is also possible. Various service providers in the backend can communicate with one another for example via internet connections.

The general process sequence essentially consists of four steps which are fundamentally necessary for authentication between the user and the vehicle:

1. system initialization
2. user registration
3. virtual vehicle key download
4. authentication to the vehicle.

During the system initialization, each vehicle will be paired with its backend. The backend should be provided with individual certificates so as to be able to carry out mutually authenticated and encrypted communication. Since protecting the cryptographic key material is of particular importance, these keys should be stored in a secure storage and execution environment such as a trusted execution environment (TEEs) in all the entities involved. In particular in the vehicle and also later in the mobile end device in which the virtual vehicle key is executed, only TEEs with high protection, e.g. hardware-based TEEs or TEEs with appropriate certifications, should be used.

After the "virtual vehicle keys" system is initialized, the user can be registered to download a virtual vehicle key and later authenticate themselves to the relevant vehicle. During the

registration, the unique identity of the driver or user must be recorded so that the authorization can be checked during later authentications.

Whereas entities such as the vehicle and the backend verify their credentials, which are considered to be security-critical data, in the form of key-dependent cryptographic hash functions or digital signatures, the user can authenticate themselves to the ecosystem with various authentication techniques such as knowledge (e.g. of a password, a personal identification number (PIN), code tables, but also of cryptographic keys), possession (e.g. of a token such as a smartcard) or biometric identifiers (e.g. fingerprints or facial recognition). If two authentication techniques are combined (e.g. multi-factor authentication) in this context, the BSI refers to strong authentication[2]. In its Technical Guidelines[3], the BSI provides an assessment and long-term guidance for current cryptographic methods, protocols to be used and key lengths as well as the respective scopes in which these are presumed to be secure and can be used.

In order to limit damages in the event of vehicle theft, revocation mechanisms must be implemented in the system that make it possible to revoke issued usage authorizations. In this case, a distinction is made between active and passive measures. Active measures include revocation lists, which are stored and updated directly on the vehicle. Passive measures can be implemented through a time restriction in the issued keys. In order to also cover the offline case, in which it is not possible to establish a connection to the vehicle to update revocation lists, the active revocation mechanism should be combined with the passive to enforce regular communication with the backend for the purpose of issuing keys so that additional key issuing can be prevented.

If certification should become necessary, it must be acquired in accordance with the internationally accepted standard Common Criteria for Information Technology Security Evaluation (CC), as well as in the USA by the Federal Information Processing Standard (FIPS).

3. Requirements for designing the overall function of virtual vehicle key

The following requirements should be implemented fundamentally when designing the overall system.

1. A virtual vehicle key must be configured in accordance with the current IT Baseline Protection of the BSI[1]:

   1.1. All the interfaces between the entities involved and along the initialization and registration process chain must be configured and checked in accordance with the BSI in order to ward off unauthorized access to the system and to issue locking and/or driving authorizations only to authorized users.

   1.2. During implementation, only standardized cryptographic methods[1] may be used to ensure system security within the service life of a vehicle and to retroactively adapt it in accordance with new findings in the field of IT security.

   1.3. For authentication between the entities involved, only strong authentication methods may be used (e.g. 2/multi-factor authentication), and these must also be able to be adapted during the vehicle life cycle so as to stay up to date.

2. It must not be possible to copy a virtual vehicle key, i.e. similarly to a physical vehicle key, it must not be possible to make a 1:1 copy of the key or a duplicate.

3. An individual virtual vehicle key must be implemented for each vehicle.
   Background: what is known as a “general key” must not exist; in order to eliminate threats that affect the whole series of vehicles, each vehicle, each vehicle immobilizer (VI) and each user must have individual cryptographic keys which meet the BSI requirements for strong cryptography.

4. The role and privilege management[6] should be configured in such a way that unauthorized users or malware cannot gain access to security-critical data, such as credentials, and processes, such as algorithms, within the system.

5. A secure timestamp for the overall function must be implemented across all entities.

6. For communication between the vehicle and the mobile end device, standardized protocols and a timestamp should be used to prevent known attacks such as replay, MitM and DoS attacks.

7. The virtual vehicle key is not allowed to be stored in plain text or unencrypted in any control unit.

8. All the communication channels in a vehicle, such as BLE, NFC, internet, GSM, etc., as well as physical channels such as the OBD interface, must be protected against known replay, MitM or similar interception threats.

9. The unauthorized sending of messages to the internal vehicle on-board network for access and driving authorization must be prevented.

10. A vehicle immobilizer must be activated immediately when:

    10.1. The mobile end device is no longer registered inside the vehicle interior.

    10.2. The driver's seat is no longer occupied.

    10.3. The virtual vehicle key is entered in the revocation list.

11. Access authorization, i.e. opening and closing doors and/or the trunk compartment, must be implemented separately from driving authorization, i.e. deactivating the vehicle immobilizer and allowing the engine to be started:

    11.1. Enabling the driving authorization must be done separately and only after enabling the access authorization.

    11.2. Driving authorization may not be enabled after only enabling the trunk compartment to be opened (e.g. to protect the package delivery services).

    11.3. The vehicle immobilizer may be deactivated only after driving authorization has been granted.

    11.4. The access authorization and the deactivation of the vehicle immobilizer must be implemented by separate authentication processes.

12. Revocation lists and policies must be filed in accordance with BSI approved tamper-proof methods and standards.

4. Requirements for the virtual vehicle key on a mobile end device

The following requirements should be implemented when configuring the usage concept on a mobile end device:

1. A virtual vehicle key on a mobile end device must not be able to be manipulated by the user or third parties at any time.
2. Security-critical functions (e.g. enabling driving authorization or creating signatures) must be executed in the mobile end device in a secure storage and execution environment (e.g.: TEE, secure element, etc.).
3. Security-critical data, such as credentials, must be stored in a secure storage and execution environment.
4. Access to the virtual vehicle key should additionally be protected by a password, fingerprint, etc.
5. Separation must be ensured between the regular execution environment of the mobile end device (e.g. the operating system) and the secure storage and execution environment (e.g.: TEE, Secure Element, etc.) in order to prevent attacks on security-critical data. No undefined access to the memory content of the trusted execution environment may take place.
6. Authentication of messages between the virtual vehicle key on a mobile end device and the vehicle is absolutely necessary to prevent replay attacks.
7. The user and their mobile end device must authenticate themselves to the system using authentication processes according to the BSI.

5. Requirements for the backend

The backend in the “virtual vehicle keys” ecosystem is considered to be particularly critical, since an attacker can not only gain possession of security-critical data, such as credentials of all the users registered on the system, but by means of the internet access, can also carry out any attacks on the backend, such as altering or deleting log files, from a safe distance.

The BSI, in its own study on safeguarding the backend, provides a series of basic measures for safeguarding generic servers against various attacks[5]. These measures are to be implemented as minimum requirements.

The following requirements should be implemented when integrating a backend into the overall system:

1. Only protocols which are standardized and recommended by BSI may be used for data transmission to prevent known attacks such as DoS, MitM, etc.
2. Cryptographic material for authentication and for encrypting communication channels must be protected against unauthorized access or manipulation.
3. All security-critical data and processes must be stored on the secure storage and execution environment of the backend so as to be protected against manipulation or reading.
4. The role and privilege management[6] is to be configured so that the number of persons authorized to manage security-critical data is kept to a minimum and the risk of attacks through social engineering is thus minimized.
5. The logfiles for usage authorization and virtual vehicle key administration must be protected against manipulation and attacks of any type.
6. Identified attack attempts on these logfiles should be documented transparently.
7. In order to detect attempts to attack the backend and reduce damage over time, a monitoring process according to BSI[11] must be established, so that no new unauthorized virtual vehicle keys shall be created and affected keys are revoked as quickly as technically possible.

6. Plausibility of data and forensics

It must be possible for insurance companies to check the plausibility of total theft. In this case, the manufacturer and the service providers are required to provide support, for example by providing and analyzing data. This applies even more in the case of virtual keys than in the case of physical keys.

Particularly in the case of subsequent legal disputes, this data must be stored for forensic use for a period of time longer than 200 working days. These considerations result in particular requirements for logging, which – as in the case of conventional investigations as well – relate to data-protection aspects. Whereas the policy holder's statement of agreement has been sufficient up to now, in the case of virtual keys, other users' rights could also be affected. The OEMs and service providers have an obligation to take into consideration and avoid such conflicts and to design their systems accordingly.

The following requirements are imposed on the *forensic* process:

1. In the event of theft, in order to be able to provide information about the valid virtual vehicle keys, a corresponding logfile must be stored on the backend, which logs the issuing of keys.
2. The logfiles must be stored in immutable form in order to prevent subsequent manipulation by third parties.
3. The logfiles must transparently and clearly reproduce a forensic record to protect the customer from false suspicion.
4. To avoid fraudulent or improper use of the usage authorization, it must be possible to deactivate a virtual vehicle key (or all registered virtual vehicle keys) and to offer the following options:

   4.1. Deactivation by the customer by means of their customer account.

   4.2. Deactivation by the OEM or the service provider on behalf of the customer.
5. In the event of a reported theft, an immediate deactivation of all the virtual vehicle keys must be possible.
6. Deactivation of the virtual vehicle key must trigger an immediate synchronization of all the entities.
7. In the case where one of the entities cannot be reached in offline mode, it must be ensured that

   7.1. the revocation of the virtual vehicle key is documented transparently,

   7.2. authentications of all the entities including pending authentications are documented transparently.

8. From the point of view of forensics, a reporting process analogue to the US-CERT process [12] must be established in order to ensure the transparency of attack attempts and the IT security of connected and security-critical functions.

9. The forensic data set plays a decisive role in the plausibility check and resolution of a total theft and should contain the following information:

    9.1 The timestamp of all user registrations

    9.2 The timestamp of all virtual vehicle keys downloads

    9.3 The timestamp of all authentications to the vehicle

    9.4 The number of all active virtual vehicle keys including multi-keys, card keys and temporary virtual vehicle keys

    9.5 The timestamp of a virtual vehicle key deletion, i.e. a complete list of all revoked virtual vehicle keys

    9.6 The timestamp and the geographic coordinates of the most recent virtual vehicle key use.

7. References

1 *BSI. IT-Grundschutz-Kataloge. 2017. URL:* https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

2 Bundesamt für Sicherheit in der Informationstechnik. M 4.133 Geeignete Auswahl von Authentikationsmechanismen. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04133.html

3 Bundesamt für Sicherheit in der Informationstechnik (BSI). *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. 2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile%5C&v=2

4 BSI. M 4.456 Authentisierung bei Web Services. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04456.html.

5 BSI. *Absicherung eines Servers (ISi-Server) – BSI-Studie zur Internet-Sicherheit (ISiS)*. Sep. 2013. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi-server_pdf.pdf?__blob=publicationFile

6 BSI. G 2.191 Unzureichendes Rollen- und Berechtigungskonzept. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g02/g02191.html

7 ISO. *ISO/IEC 154082:2008*. 2014. URL: https://www.iso.org/standard/46414.html

8 Bundesamt für Sicherheit in der Informationstechnik. *Zertifizierung von Produkten*. 2016. URL: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/Produktzertifizierung_node.html

9 The Common Criteria. *Members of the CCRA*. 2016. URL: http://www.commoncriteriaportal.org/ccra/members/#DE

10 National Institute of Standards und Technology. *FIPS Publications*. 2015. URL: http://csrc.nist.gov/publications/PubsFIPS.html.

11 BSI. Leitfaden zum Informationssicherheitsmanagementsystems (ISMS). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3

12 US-SERT Gouvernement.URL: https://www.us-cert.gov/

8. Abbreviations

Table 1: List of abbreviations

Abbreviation	Complete explanation of term
Authenticator	An authenticator is used as the input for authentication methods
BLE	Bluetooth Low Energy
BSI	Bundesamt für Sicherheit in der Informationstechnik [German Federal Office for Information Security]
Entity	Entity (also referred to as an information object) is used in data modeling to refer to an object which is to be clearly defined and which is to be used to store or process information. The object can be tangible or non-tangible, concrete or abstract. Exempels: a vehicle, a person
CC	Common Criteria (for Information Technology Security Evaluation)
Credentials	Credentials are an instrument for authenticating to a system the identity of another system or of a user
SP	Service Provider
ECU	Electronic Control Unit
FIPS	Federal Information Processing Standards
GW	Gateway
MED	Mobile End Device
MitM	Man in the Middle
MNO	Mobile Network Operator
NFC	Near Field Communication
OBC	Out of Band Channel
OEM	Original Equipment Manufacturer
PIN	Personal Identification Number
TEE	Trusted Execution Environment.
Timestamp	Day and time of the event
TPM	Trusted Platform Module
VVK	Virtual Vehicle Key
WLAN	Wireless Local Area Network
VI	Vehicle Immobilizer
Vehicle lifecycle	Period between SOP and substantial update of function VFS or EOP plus two years