RCAR

Requirements for Virtual Vehicle Keys

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

Issue 1.0

April 19

EDIT 30 April 2019:

General: file creation

INDEX

1. DEFINITIONS

Term	**Complete definition of term**
Ad-hoc modus	allows one device to communicate with each other directly
Agent	Any user or process that acts upon a system entity
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
ECU	Electronic Control Unit
FIPS	Federal Information Processing Standards
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
SP	Service provider
Verification of identity and access permission	*Authentication* is a first step in testing identity by actively claiming a particular identity and verification of the claimed authentication. *Authorization* is the granting of special rights.
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

2. INTRODUCTION

Theft is a major 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, RCAR presents the requirements for *the Virtual Vehicle Keys* (VVK) from the insurance company’s perspective. The requirements are intended in particular to make the access and driving authorizations secure. By meeting these requirements when designing the system, vehicle manufacturers can protect it against misuse while at the same time taking 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 agnostic to the implementation of digital business processes, technologies such as cloud computing or the use of mobile devices. The risk analysis was carried out by the Fraunhofer Institute for Secure Information Technology (SIT) on behalf of the AZT. In principle, the requirements 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 German Federal Office for Information Security (BSI), which specify standard measures and methods for ensuring baseline IT security in Germany [1]. 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), for example, is responsible for similar IT security process standardization in the USA.

In the following, a relevant reference architecture with the entities involved will first be described. This results in the requirements for the Virtual Vehicle Key as a networked system of multiple entities. Lastly, the requirements for the forensic process will be set out and explained.

3. REFERENCE ARCHITECTURE AND PROCESS SEQUENCE

In Figure 1, a possible reference architecture for the Virtual Vehicle Key (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 different keys on one mobile end device.

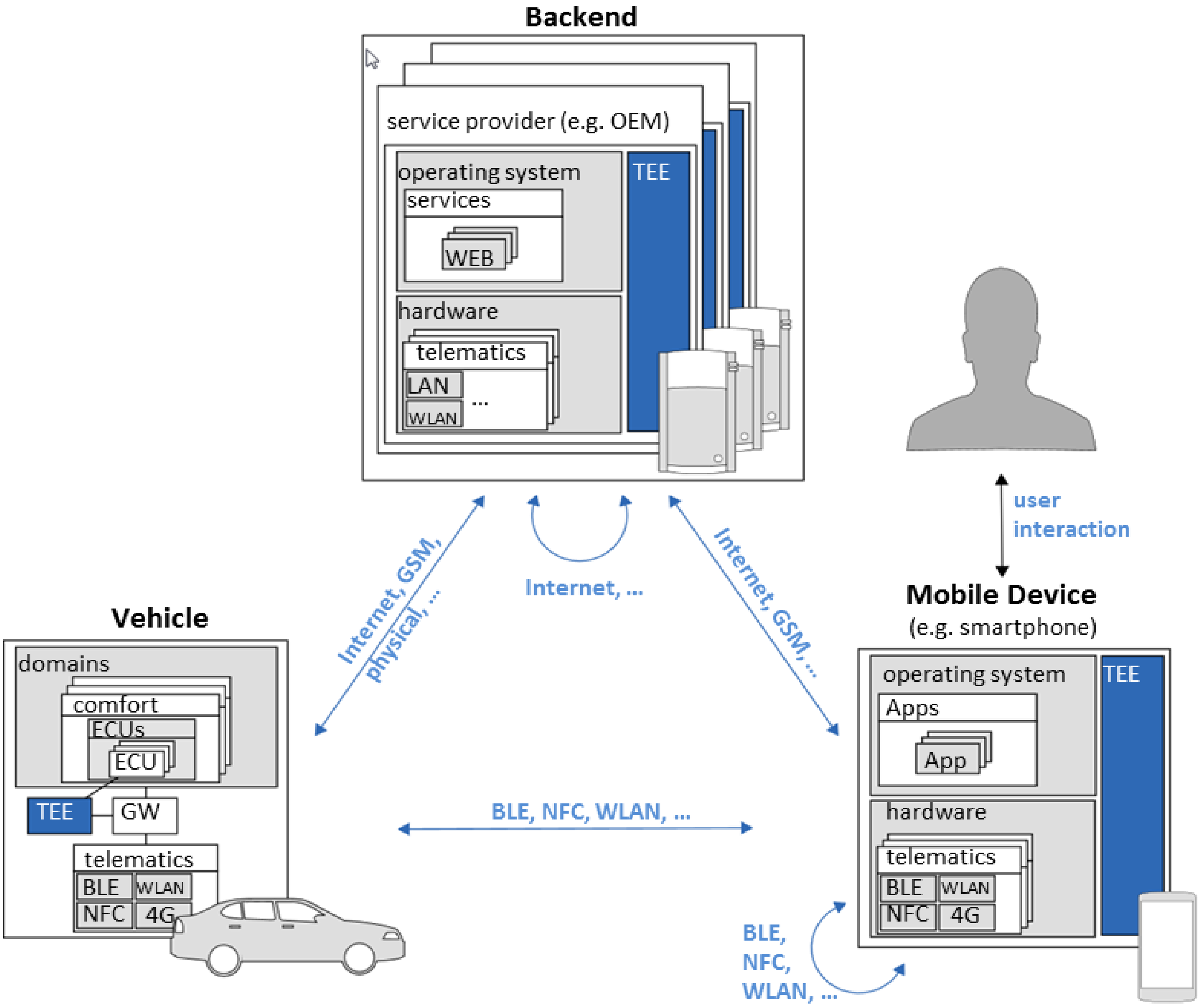

Figure 1: Ecosystem and entities involved

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 or car-sharing providers). Mobile End Devices include smart mobile devices and smart wearables, such as smartphones, smartwatches and tablets.

As can be seen in Figure 1, the individual entities communicate with one another via various interfaces and communications protocols. The communication between the vehicle and the backend and between the mobile end device and the backend typically takes place over a cellular internet connection. This communication should take place exclusively via mutually authenticated channels to ensure the validity of all communication participants. This measure protects against (entity) spoofing threats and unauthorized sending or changing 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 man-in-the-middle (MitM) attacks, only 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. Communication between separate service providers in the backend should be exclusively via mutually authenticated and encrypted channels, typically over standard internet connections.

The general process sequence essentially can consist of four steps necessary for authentication between user and 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 unambiguously 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 (TEE) 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 Key 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. These steps after the initialization are to be performed for each MED or user.

Whereas entities such as the vehicle and the backend typically authenticate using digital certificates, the user can authenticate themselves to the ecosystem with various authentication techniques. These include knowledge of a password or personal identification number (PIN), possession of a smartcard or other physical token or biometric identifiers such as fingerprints or facial features. Combining two or more of these authentication techniques results in a multi-factor authentication system which is described by the BSI as strong authentication [2]. In its Technical Guidelines, 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 authentication factors are presumed to be secure and can be used [3].

In order to limit damages in the event of vehicle theft, mechanisms must be implemented in the system to enable the revocation of previously-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 in the vehicle. Passive measures include enforcement of time-based expiration for issued keys. In order to 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 prohibiting further use of keys. A revocation process must also be implemented on the MED. The actual revocation of the right to use must be documented.

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 by the Federal Information Processing Standard (FIPS) in the USA.

4. OVERALL SYSTEM REQUIREMENTS

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

1. A VVK system must be designed in accordance with current IT Baseline Protection of the BSI [1]:

    1.1. All interfaces between entities involved and along the initialization and registration process chain must be authenticated and encrypted to prevent unauthorized access to the system and to ensure that locking and driving functions are initiated only by authorized users.

    1.2. Cryptographic algorithms and key lengths must be at least as strong as baseline recommendations from the BSI [1] or other appropriate standard-making body.

    1.3. Authentication between a VVK user and one of the system entities must be ensured with at least two factors.

    1.4. Authentication methods and cryptographic mechanisms must be updatable during the vehicle life cycle.

2. The system must be designed to ensure that duplicating a VVK is not feasible.

3. A unique VVK must be generated for each combination of vehicle and mobile device. It must not be feasible to assign an individual key to more than one vehicle.

4. Role-based access control [6] should be used to ensure that unauthorized users or agents cannot gain access to security-critical data within the system.

5. A secure time reference for the overall system must be maintained.

6. Cryptographic keys may not be stored unencrypted by any system entity.

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

8. All the communication channels implemented for the VVK ecosystem, such as BLE, NFC, internet, GSM, etc., as well as physical channels such as the OBD interface, must be effectively 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 not be deactivated if the MED is not present within the vehicle interior (analogously to current conventional key systems).

11. Authorization of physical access functions (opening and closing passenger and cargo area doors) must be implemented separately from authorization of driving functions (deactivating the vehicle immobilizer and allowing the engine to be started):

11.1. The access authorization and the deactivation of the vehicle immobilizer must be implemented separately.

11.2. Driving authorization must be granted only after successful access authorization.

11.3. Driving authorization must be granted only after authorization to open a passenger door, not a cargo area door (e.g. to protect the package delivery services).

12. Revocation lists and policies stored in the vehicle must be cryptographically signed in accordance with recommendations by the BSI or other appropriate standard-making body in order to prevent unauthorized changes.

5. MOBILE END DEVICE REQUIREMENTS

The following design requirements apply to the mobile end device and the installed application that comprise the virtual vehicle key:

1. A VVK 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 like granting driving authorization or creating digital signatures must be executed in a secure storage and execution environment on the mobile end device.
3. Security-critical data like credentials, tokens and cryptographic keys must be stored in a secure storage and execution environment on the MED.
4. Access to the VVK application should be protected by a password, PIN or biometric authentication.
5. Authentication of messages between the VVK on a MED and the vehicle is absolutely necessary to prevent replay attacks.
6. The user and their MED must authenticate themselves to the system using authentication processes according to the BSI.

6. BACKEND REQUIREMENTS

Because of the volume and sensitivity of vehicle and user data stored, the security of backend entities is of particular importance. In addition, the need for backend entities to be exposed to the internet for communication with vehicles and MEDs results in an attack surface that may be exploited remotely by malicious actors.

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 rights 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.

7. FORENSIC REQUIREMENTS

Vehicle thefts represent a significant source of auto insurance claims, and the ability to investigate theft cases is of primary importance to insurers. Vehicle manufacturers also have a vested interest in maintaining the ability to conduct thorough theft investigations for diagnostic purposes and for product liability defense. Thus the vehicle manufacturer and any service providers contributing to the VVK system should make every effort to collect appropriate log messages and system state information and retain it for a reasonable period.

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

1. Logs and system state data which clearly record the issuance and revocation of VVK should be stored on a backend entity.
2. Particularly in the case of legal disputes, logs and system state data should be retained for a period of at least 200 working days.
3. To avoid fraudulent or improper use of the usage authorization, it must be possible to deactivate a VVK (or all registered VVK) and to offer the following options:
   - 3.1. Deactivation by the customer by means of their customer account.
   - 3.2. Deactivation by the vehicle manufacturer or a service provider on behalf of the customer.
4. In the event of a reported theft, an immediate revocation of all issued VVK must be possible.
5. Revocation of any VVK must be immediately communicated to all appropriate entities.
6. The system should receive and log an acknowledgement of the status of the revocation from each other entity in the system. In cases where one or more entities is offline or otherwise unable to perform the revocation, a *pending* or *failed* status must be recorded transparently, in a non-proprietary format.
7. Logs and system state data must be stored in immutable form to prevent subsequent manipulation by third parties.
8. OEM reports must transparently and clearly reproduce a forensic record to protect the customer from false suspicion.
9. From the point of view of forensics, a reporting process similar to the US-CERT process [12] is to be established in order to ensure the transparency of attack attempts and the IT security of connected and security-critical functions.
10. The forensic data set plays a decisive role in the plausibility check and resolution of a total theft and should contain the following information, with associated accurate timestamps:
    - 10.1. User registrations
    - 10.2. Issuance of VVK, including key type (e.g. multi-key, card key, temporary), along with current total number of valid keys
    - 10.3. Most recent authorization to perform access functions, with location data

10.4. Most recent authorization to perform driving functions, with location data

10.5. Revocation of VVK, along with current total number of valid keys

10.6. Revocation notice sent to each system entity

10.7. Revocation acknowledgement received from each system entity

8. REFERENCES

1 BSI. Technical Guidelines. URL: https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_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-CERT. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf