Allianz

Guidelines

AZT Automotive GmbH | Allianz Zentrum für Technik

Updated requirements for the electronic immobilizer

Technical guidelines for implementing anti-theft protection from the insurer's perspective

04/04/2023

INDEX

1. DEFINITIONS

Term	Complete definition of term
Authentication	Authentication verifies who the user is (identity)
Authorization	Authorization determines what resources a user can access (privileges)
BLE	Bluetooth Low Energy
eIM	Electronic immobilizer
Manufacturer	The vehicle OEM or distributor
Life cycle of the vehicle model	Time period between SOP and EOP plus two years
NFC	Near Field Communication
OEM	Original Equipment Manufacturer
PIN	Personal Identification Number
System-Operator	A third party authorized by the vehicle OEM to take over legal obligations and system responsibilities, e.g. backend, instead of the OEM
UWB	Ultra Wide Band
VIN	Vehicle Identification Number
VVK	Virtual Vehicle Key

2. Introduction

Theft is a major theme in motor insurance and is characterized by high average damages. For particularly affected models, the percentage of claims costs can exceed 50% of the total costs in the comprehensive insurance and have a significant impact on the type class.

The most effective anti-theft measure is a tamper-proof electronic immobilizer (eIM), which prevents unauthorized engine start and reuse of a stolen vehicle. Therefore, a qualified immobilizer is a requirement of the entire insurance industry.

The eIM requirements presuppose the fulfillment of legal regulations and guidelines (such as UN Regulation No.116, GRSG-106-38) and technical standards (such as ECE, DIN, ISO). The requirements are formulated generically so that they can be applied to different technologies. This should enable the manufacturer to implement them individually, but at the same time the manufacturer is obliged to apply the state of the art as best as possible in the interest of his own customers.

The requirements for the electronic immobilizer as a system are formulated first. Then the requirements for the key set and the forensics are described. The special requirements for Virtual Vehicle Keys (VVK[1]) as a part of the complete key set was published as RCAR Standard[2].

[1] Smartphone or equivalent personal device as key

[2] https://rcar.org/working-groups/cyber-security

3. Electronic immobilizer requirements

From the insurers' point of view, the following requirements should be implemented generally:

1. An eIM must ensure the level of theft protection achieved at initial classification for the entire life cycle of the vehicle model.
2. An eIM must be updatable over the life cycle of the vehicle model in order to be able to fix reported security vulnerabilities.
3. Deactivating (disarming) the eIM must fulfill the following requirements:

   3.1. The access authorization and the driving authorization must be implemented using separate processes.

   3.2. The eIM must be deactivated only after a successful verification of valid access permission and valid driving permission.

   3.3. Driving authorization may not be given when only permitted to open the trunk (e.g. delivery service).

4. Activating (arming) the eIM must fulfill the following requirements:

   4.1. As soon as[3] the driver leaves the vehicle cabin[4], the engine/motor must be switched off and the driving mode must be terminated.

   4.2. As soon as the authorized key leaves the vehicle cabin[5], the engine/motor must be switched off and the driving mode must be terminated. If the driver remains inside the vehicle and no key is detected, the driver should be informed about the upcoming loss of driving authorization.

   4.3. The eIM must be activated immediately as soon as the (electric) motor is switched off and no driving mode is active.

5. Unauthorized deactivation or disabling of the eIM must not be possible.
6. Unauthorized access, e.g. by manipulating the on-board network from outside, must not be possible.

[3] Regarding to UN Regulation No.116

[4] Example: Combination "Seat occupation detection = not occupied" and "Driver's door = open".

[5] Combination "Key = not detected" and "Driver's door = open".

7. Unauthorized replacement of control units - such as the eIM control unit or other control units involved in the functionality of the eIM - and subsequent recovery of the eIM function must not be possible without documented authorization by the manufacturer[6].

8. Cryptographic material for checking and releasing the driving authorization:

   8.1. must be stored in control units in a tamper-proof way

   8.2. must be vehicle-specific and non-transferable

   8.3. must not be stored in plain text or in unencrypted data formats.

9. The functionality of the eIM must be designed to be robust and secure against man-in-the-middle attacks and tested in compliance with ISO 21434. All implemented transmission technologies must be considered, such as RFID, NFC, BLE, UWB.

[6] (Vehicle) manufacturer or system operator: The vehicle OEM or a third party authorized by the vehicle OEM to assume legal obligations and system responsibilities in place of the OEM.

4. Physical key requirements

Although virtual vehicle keys are becoming more widespread, physical keys still retain their classic function and will continue to be used by insurance participants in everyday life. In the case of a total theft, physical keys are included in the damage analysis in order to verify the reported theft and exclude fraud.

The following requirements are specified for the physical keys:

1. Secure copy protection for the complete key set, i.e. especially electronic key components, must be provided.
2. Manual input of a PIN or a passcode to deactivate the immobilizer is not permitted.
3. Programming of additional keys may only take place whilst the vehicle is online and only via a secure data channel to the manufacturer backend.
4. Any programming of new or additional keys must be documented transparently by immediately logging the changes in the key set on the manufacturer backend.
5. Any key programming, overwriting or extension of the original key set without an existing verified online data connection to the manufacturer backend must not be possible worldwide.
6. Neither a PIN nor a passcode may be handed over in plain text to the vehicle owner or a workshop for the assignment procedure of new keys.

5. Forensics and data plausibility

Total theft must be possible to be verified by the insurers. Event- and vehicle-related data from the manufacturer's backend is required for plausibility checks. Particularly in the case of police investigations or legal disputes, last-use data must be stored in a forensically usable form over a longer period of time. It must be assured that any automated deletion routines are not applied in these cases.

The declaration of consent from the policyholder[7] within the scope of their duty of cooperation to clarify the facts entitles the insurer to request necessary information from the manufacturer and to use it for the clarification of the total theft. Taking into account the circumstances of the individual case it must be ensured, in particular in the interest of the policyholder, that the latter is able to fulfill their contractual obligations to cooperate.

The following information regarding physical and virtual vehicle keys is required for claims handling and forensic plausibility checks of a total theft:

1. Affiliation of the presented keys to the stolen vehicle - Do the mechanical locking key code, the electronic encoding and the VIN match each other?

2. Completeness of the presented key set - Is it the original set of keys incl. VVK that was delivered with the stolen vehicle complete?

3. Validity of the presented set of keys - According to the manufacturer's database, how many keys were in working order for the vehicle at the time of theft?

4. Subsequent deliveries of spare parts and keys - If and when were additional keys and/or locks delivered for the vehicle that was stolen?

5. Modifications of the complete original key set – If, at what time and by which company did an authentication query or online reprogramming take place?

6. Anomalies in the presented key set - Are there any indications of mechanical manipulations or anomalies in the database or in the vehicle history?

7. Usage data, e.g. mileage, date or operating data of the last use in the context of the theft.

[7] According to the insurance policy law in Germany

8. Information regarding protective measures against total theft, which is helpful for the evaluation of the claims-related data. For example, what technologies, if any, have been implemented to protect against the known theft scenario of relay station attack? For example, has a locking system with passive keys in combination with motion sensors and/or with UWB technology been installed?

9. Specific information on Virtual Vehicle Keys - If the policyholder uses a VVK, they will be confronted with particular difficulties in their obligation to cooperate in the verification of details of the theft. Forensics must therefore be supported by the system operator with the following information in accordance with the international RCAR Standard:

   - User registrations
   - Issuance of VVK, including key type (e.g. multi-key, card key, temporary), along with current total number of valid keys
   - Most recent authorization to perform access functions, with location data
   - Most recent authorization to perform driving functions, with location data
   - Revocation of VVK, along with current total number of valid keys
   - Revocation notice sent to each system entity
   - Revocation acknowledgement received from each system entity