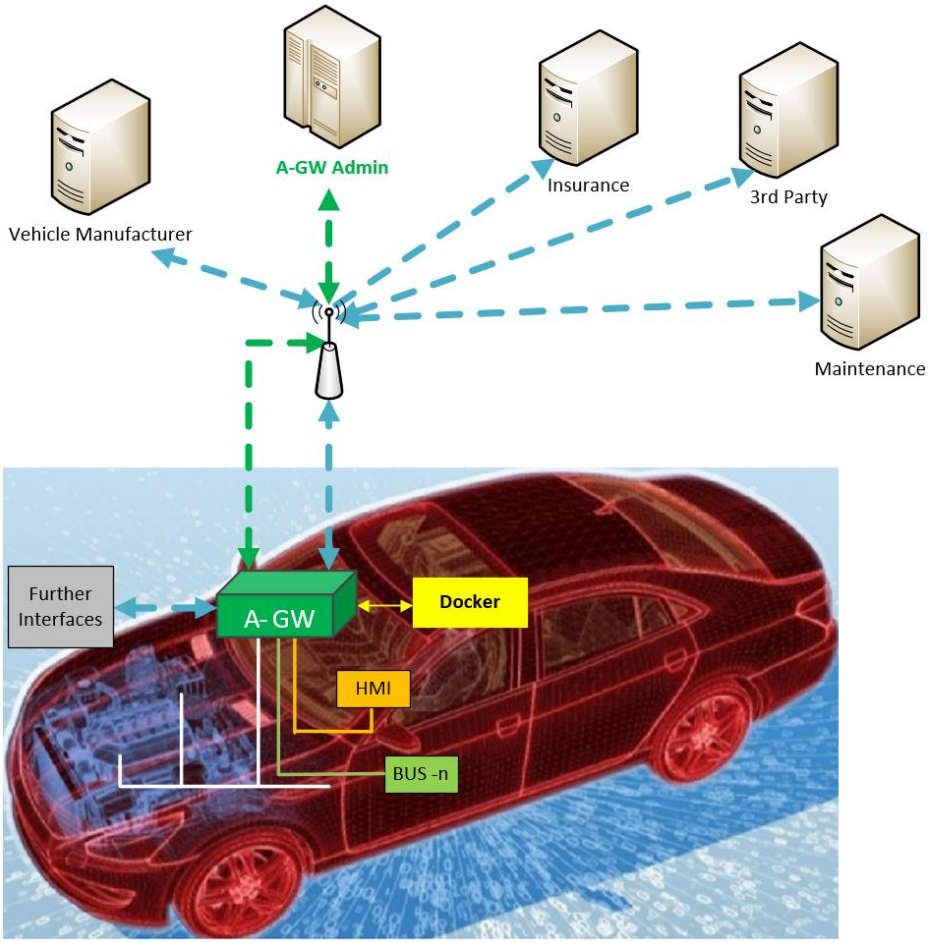
FEDERATION INTERNATIONALE DE L'AUTOMOBILE
REGION I - EUROPE, THE MIDDLE EAST AND AFRICA

OTP Protection profile

of an

Automotive Gateway



Version:	**1.02**
Date:	**2020-06-02**
Author(s):	**Markus Bartsch** **Alexander Bobel** **Dr. Brian Niehöfer** **Markus Wagner** **Maximilian Wahner**

Table of Contents

1 PP introduction 4
1.1 Introduction 4
1.2 PP Reference 4
1.3 Specific Terms 4
1.4 TOE Overview 5
1.4.1 Introduction 5
1.4.2 TOE Type 5
1.4.3 TOE physical Scope 6
1.4.4 TOE logical Scope 6
1.4.5 The logical Interfaces of the TOE 7
1.4.6 Hardware, Firmware, and Software Supplied by the IT Environment 7
1.5 Secure Element (not part of the TOE) 7
1.6 Lifetime 8
1.6.1 Development 8
1.6.2 Production 8
1.6.1 Personalization 8
1.6.2 Operation 9
1.6.2.1 OEM Support 9
1.6.2.2 Service Stations 9
1.6.2.3 Updates 9
1.6.2.4 Incidents 9
2 Conformance Claims 10
2.1 Conformance Statement 10
2.2 CC Conformance Claim 10
2.3 PP Claim 10
2.4 Conformance Rationale 10
2.5 Package Claim 10
3 Security Problem Definition 11
3.1 External entities 11
3.2 Assets 13
3.3 Assumptions 13
3.4 Threats 14
3.5 Organisational Security Policies 15
4 Security Objectives 16
4.1 Security Objectives for the TOE 16
4.2 Environment 17
4.3 Security Objectives Rationale 18
4.3.1 Overview 18
4.3.2 Countering the Threats 19
4.3.2.1 T.LocalDataModify 19
4.3.2.2 T.RemoteDataModify 19
4.3.2.3 T.LocalDisclosure 19
4.3.2.4 T.LocalPhysical 19
4.3.3 Coverage of Organisational Security Policies 20
4.3.3.1 OSP.SE 20
4.3.3.2 OSP.Pairing 20
4.3.4 Coverage of Assumptions 20
4.3.4.1 A.Update 20
4.3.4.2 A.AutomotiveGatewayAdministrator 20
4.3.4.3 A.AdministrativeGroup 20
4.3.4.4 A.AuditSpecialEvents 20
4.3.4.5 A.PKI 20
4.3.4.6 A.CommunicationBypass 21
5 Extended Components Definition 22
6 Security Requirements 23
6.1 Overview 23
6.2 Security Functional Requirements 24
6.2.1 Class FAU: Security Audit 24
6.2.1.1 FAU_ARP.1 Security audit automatic response 24
6.2.1.2 FAU_GEN.1 Audit Data Generation 24

6.2.1.3 FAU_SAA.1 Security audit analysis 24
6.2.1.4 FAU_SAR.1 Security Audit Review 24
6.2.1.5 FAU_STG.2 Guarantees of Audit Data Availability 24
6.2.1.6 FAU_STG.4 Prevention of Audit Data Loss 25
6.2.2 Class FCS: Cryptographic Support 25
6.2.2.1 FCS_CKM.1/SigVer Cryptographic Key Generation for Signature Verification 25
6.2.2.2 FCS_CKM.1/TLS Cryptographic Key Generation for TLS 25
6.2.2.3 FCS_CKM.4 Cryptographic Key Destruction 25
6.2.2.4 FCS_COP.1/SigVer Cryptographic Operation for Signature Verification 25
6.2.2.5 FCS_COP.1/TLS Cryptographic Operation for TLS 25
6.2.2.6 FCS_COP.1/TLS.HASH Cryptographic Operation for Hashing 25
6.2.2.7 FCS_COP.1/MEM Cryptographic Operation, encryption of TSF and user data 25
6.2.3 FDP: User Data Protection 26
6.2.3.1 Introduction to the Security Functional Policy 26
6.2.3.2 FDP_ACC.2 Complete Access Control 26
6.2.3.3 FDP_ACF.1 Security Attribute based Access Control 26
6.2.3.4 FDP_IFC.2 Complete Information Flow Control 27
6.2.3.5 FDP_IFF.1 Simple Security Attributes 27
6.2.3.6 FDP_RIP.2 Full Residual Information Protection 27
6.2.3.7 FDP_SDI.2 Stored Data Integrity Monitoring and Action 27
6.2.4 Class FIA: Identification and Authentication 28
6.2.4.1 FIA_ATD.1 User attribute definition 28
6.2.4.2 FIA_UAU.2 User Authentication before any Action 28
6.2.4.3 FIA_UID.1 Timing of Identification 28
6.2.4.4 FIA_USB.1 User-subject Binding 28
6.2.5 Class FMT: Security Management 28
6.2.5.1 FMT_MOF.1: Management of security functions behaviour. 28
6.2.5.2 FMT_SMF.1 Specification of Management Functions 29
6.2.5.3 FMT_SMR.1 Security Roles 29
6.2.5.4 FMT_MSA.1 Management of Security Attributes 29
6.2.5.5 FMT_MSA.3 Static Attribute Initialisation 29
6.2.6 Class FPT: Protection of the TSF 29
6.2.6.1 FPT_FLS.1 Failure with preservation of secure state 29
6.2.6.2 FPT_RPL.1 Replay Detection 29
6.2.6.3 FPT_STM.1 Reliable Time Stamps 29
6.2.6.4 FPT_TST.1 TST Testing 29
6.2.6.5 FPT_PHP.1 Passive detection of physical attack 29
6.2.7 Class FTP: Trusted path/channels 30
6.2.7.1 FTP_ITC.1 Inter-TSF Trusted Channel 30
6.3 Security Assurance Requirements 30
6.3.1 Fulfilment of the Dependencies 31
6.4 Security Requirements Rationale 31
6.4.1 O.Authentication 32
6.4.2 O.Crypto 32
6.4.3 O.Management 32
6.4.4 O.SecureFirmwareUpdate 32
6.4.5 O.Protect 33
6.4.6 O.Firewall 33
6.4.7 O.Log 33
6.4.8 O.Time 33
6.4.9 Fulfilment of the Dependencies 33
6.4.10 Justification for missing dependencies 35
7 References 36

1 PP introduction

1.1 Introduction

For years, road safety and environmental protection have been drivers for more innovation, investment, growth and jobs in car manufacturing. Today, information technology is the key innovation driver of connected vehicles. This development of technology can significant contribute to safety, mobility, environment protection and comfort.

But IT-induced change entails new challenges for the IT security against hacker attacks as well as for data protection based on the fact that all data generated by vehicles are personal data once being connected to the vehicle identification number (VIN) of the license plate. The top priority of a modern data policy must remain the protection of the fundamental right to privacy, of the right to the consumer empowerment and his freedom of choice. For this reason, a smarter communication and authorization concept shall be implemented.

This Protection Profile identifies the threats, organizational security policies and assumptions that are relevant for securing vehicular communication in an Intelligent Transport System (ITS, see [C-ITS-Korridor]) by using an OTP as described in [OTP]. Based on that, it defines the security objectives, the Security Functional Requirements and the Security Assurance Requirements that need to be fulfilled by the Automotive Gateway responsible for securing the V2X communication.

The security functionality of the TOE comprises

- Protection of confidentiality, authenticity, integrity of data and
- Information flow control

mainly to protect the privacy of consumers and to ensure a secure way of smart communication in interconnected road traffic.

This Protection Profile is intended to serve as an example on how an OTP security architecture [OTP] could be built and acts as a recommendation.

1.2 PP Reference

Title:	OTP Protection Profile of an Automotive Gateway
Version:	1.02
Evaluation Assurance Level:	EAL2 augmented with ALC_FLR.2 and ALC_LCD.1
CC-Version:	3.1 Revision 5

1.3 Specific Terms

The following specific terms are used in the context of this document

Term	Description
AA	Authorization Authority
A-GW	Automotive Gateway
A-GWA / A-GW Admin	Automotive Gateway Administrator
AT	Authorization Ticket
BSI	Federal Office for Information Security
CA	Certificate Authority
Car2X (C2X, V2X)	Car-to-Everything
Car2I (C2I, V2I)	Car-to-Infrastructure
C2C (V2V)	Car-to-Car
CC	Common Criteria for Information Technology Security Evaluation
C-ITS	Cooperative Intelligent Transport Systems
EA	Enrolment Authority
EAL	Evaluation Assurance Level
ECU	Electronic Control Unit

GDPR	General Data Protection Regulation
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
IT	Information Technology
ITS	Intelligent Transport System
ITS-S	Intelligent Transport System Station
KBA	German Federal Motor Transport Authority
OBAP	On-Board Application Platform
OBD	On-Board Diagnostics
OBM	On-Board Monitoring
OEM	Original Equipment Manufacturer
OTP	Open Telematics Platform
PKI	Public Key
PP	Protection Profile
RNG	Random Number Generator
R&M	Repair & Maintenance
SE	Secure Element
TOE	Target of Evaluation
TSF	TOE Security Functionalities
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VCS	Vehicle C-ITS Station
VIN	Vehicle Identification Number
WAN	Wide Area Network (of ITS)

1.4 TOE Overview

1.4.1 Introduction

The TOE described in this Protection Profile is an **Automotive Gateway** (A-GW) of an OTP that is designed to be placed inside a vehicle that is part of an Intelligent Transport System (ITS). The Automotive Gateway serves as the communication component inside the vehicle in order to secure and manage the communication and information flow between the vehicle, OEM and all other parties of an ITS. The gateway uses cryptographic credentials of a Hardware Security Module (HSM or SE) as part of the Automotive Gateway controller, but not part of the TOE.

The TOE relies on trusted Public Key Infrastructures (PKI) to perform its operation. All cryptographic credentials inside the SE of the infrastructural components and cars are managed by PKI's of the different communication service providers. Aside from that, the TOE does not need any additional hardware, software or firmware to perform its security functions.

1.4.2 TOE Type

The TOE is a communication gateway of an OTP (Automotive Gateway: A-GW) based on [OTP]. It is placed within a vehicle intended to secure and manage the communication. It consists of a message generation, procession, and management logic, a tamper-resistant security module and additional guidance documentation for the integration of the TOE into a vehicle and for the operation of the TOE. The purpose of the services enabled by the TOE is to secure and manage data and information flow in communication.

The Automotive Gateway serves as a communication interface in a vehicle. All communication from outside (for example, over the WAN or via an external interface) is managed centrally using this gateway.

1.4.3 TOE physical Scope

The TOE described in this Protection Profile aims on the provision of at least all mentioned functionalities. Hence, only those components are integrated in the physical boundaries, which are mandatory. Therefore, the TOE comprises the hardware and firmware that is relevant for the security functionality of the Gateway as defined in this PP. The Secure Element that is utilised by the TOE is considered being not part of the TOE[1]. Specifically, the TOE described in this PP only includes, next to a real-time clock, an independent computing system, and the corresponding software parts to control and steer the mentioned functionalities described in chapter 6.

Furthermore, additional modules only support the TOE without being part of it:

- Mobile communication segments,
- Car-2-X communication,
- Positioning technology.

It should be noted that this overview of possible physical implementations does not claim being a complete overview of all possibilities. The Common Criteria allow to combine multiple TOE into one device and have the flexibility to identify functionality that is not relevant for the security functionality of the TOE or the environment. However, when focussing on a system of multiple TOEs, it is not possible to move security features from the scope of one TOE to another.

1.4.4 TOE logical Scope

The logical boundary of the TOE can be defined by its security features:

- Detection, definition, generation and storage of security-relevant events for logging and their mapping to corresponding entities.
- Authorisation concept with flow policies and rules and an authentication and identification mechanism including the implementation of access rules and policies.
- Information flow policies and rules (Authorisation Concept).
- Authentication and identification mechanisms including the implementation of access rules and policies.
- Management functionalities including the management of security attributes for the different entities.
- Ensure authenticity of information content received from or send to involved TSFIs.
- Guarantee secure state in case of error events.
- Secure Firmware Update
- Provide self-test possibilities.
- Replay detection
- Secure data deletion
- Reliable time-stamp generation
- Trusted communication establishment via TLS

The services of the Secure Element are not part of this protection profile. The necessary service will be outlined in chapter 1.5 in more detail.

[1] Please note that the Secure Element is physically integrated into the Automotive Gateway even though it is not part of the TOE.

1.4.5 The logical Interfaces of the TOE

The TOE offers its functionality as outlined before via a set of external interfaces. The following table provides an overview of the mandatory external interfaces of the TOE and provides additional information:

Interface Name	Description
IF_GW_AGWA	This interface enables the neutral Automotive Gateway Administrator to set and manage the rights of the individual groups.
IF_GW_Administrative	This interface gives members of the Administrative Group read and write access to messages sent into or out of the vehicle.
IF_GW_Audit	This interface gives members of the Audit Group read access to messages sent into or out of the vehicle.
IF_GW_Docker	This interface gives members of the Docker Group read/write access to messages sent into or out of the vehicle.
IF_GW_Driver	This interface gives members of the Driver Group read access to messages sent into or out of the vehicle.
IF_GW_Information	This interface gives members of the Information Collection Group read access to messages sent in to or out the vehicle.

Table 1: Logical Interfaces Overview

A more detailed description of the different groups is provided in Chapter 3.1.

Application Note 1: This Set of interfaces is an example set in dependency to which user groups the A-GWA has configured. There can be additional interfaces that shall be added by the writer of the ST.

1.4.6 Hardware, Firmware, and Software Supplied by the IT Environment

The following hardware, firmware or software, which are supplied by the IT environment, are excluded from the TOE boundary but needed for operation.

- Secure Element
- Vehicle
- Intelligent Transport System (ITS)

1.5 Secure Element (not part of the TOE)

The Automotive Gateway contains a Secure Element (SE), which acts as a provider for the required cryptographic operations, as a secure key storage and for other needed cryptographic functionality used in the functions mentioned above. The SE provides strong cryptographic functionality, random number generation, secure storage of secrets and supports the authentication of external entities. It is a different IT product and thus not part of the TOE as described in this PP, but it is embedded into the Automotive Gateway and protected by the same level physical protection.

The SE shall be used for:

- Decryption of session key,
- Generating and using of random numbers and digital signatures,
- Secure deletion of private keys, and
- Storage of keys.

The SE shall be protected against unauthorized removal, replacement and modification. The ST author shall define mechanisms to protect the link between the SE and the TOE.

In practice the SE can be realised by a smart card for example. The main application of the Automotive Gateway should be capable of verifying the authenticity of the SE on start up.

1.6 Lifetime

The Lifecycle of the TOE just consists of five consecutive phases without declines (see [OTP]):

1. **Development**

   The software development process of the Automotive Gateway.

2. **Production**

   The production itself like hardware assembly or software installation.

3. **Personalization**

   When changing the ownership of the vehicle an initial configuration has to be done in order to personalize all security functions for the normal operation to the new owner.

4. **Operation**

   Operational phase of the TOE. All security functions shall be working as specified. Here Maintenance and Repair activities can happen. The operation of a car could be modelled as any operation cycle, as during the lifetime different ownerships of the vehicle occur, user and usage policies as well as spare part and their digital mappings are exchanged.

5. **Scrapping**

   In case the TOE comes to an irreparable, defect state or shall be taken out of order for other reason, it is ensured that the key material that is contained in the TOE is destroyed in a secure manner as described in the guidance documentation of the mandatory Secure Element.

In order to stay flexible in the regulation and to give every participant in the lifetime process of the Automotive Gateway the opportunity to individually incorporate and implement a secure lifetime, a generic general set of rules is built to be followed. Every participant in the lifetime should therefore obliged to integrate the following rules that apply to them into their processes.

1.6.1 Development

1. The A-GW shall be developed in a secure development environment.
2. A secure management system (Software, Configuration and Update) shall be implemented (preferable acc. to. [ISO21434]).

1.6.2 Production

1. The A-GW shall be manufactured in a secure production environment.
2. A cybersecurity engineering process shall be implemented by the production area acc. to [ISO21434].
3. Before integration into the vehicle, the shipment of the A-GW between different manufacturing facilities shall be in a secure supply-chain acc. to [TISAX].
4. The A-GW be shall installed in the vehicle in a secure way.
5. The A-GW shall be paired with the vehicle via the Vehicle Identification Number (VIN).

1.6.1 Personalization

1. By changing the ownership (selling or reselling) all ownership relevant usage profiles of the A-GW shall be first reset to an initial and neutral configuration. Any links to the data of the last owner shall be deleted.
2. The A-GW is personalized to the new owner by updates of the A-GWA of the new initial usage profiles to the A-GW.
3. Based on the owner usage profiles additional driver usage profiles could be installed. This depends on the detailed role of the owner and differs if the owner is a private person or for instance a rental company.

1.6.2 Operation

1.6.2.1 OEM Support

1. The OEM shall be obliged to provide support and updates for the A-GW throughout the entire lifetime of the vehicle (until scrappage).

1.6.2.2 Service Stations

2. A service station is registered officially for maintenance and repair work by the owner or driver.
3. Service stations have to use licensed diagnostic tool. Any connectivity approaches by non-licensed tools are neglected by the A-GW.
4. Service station employees shall be trained in the work with licensed diagnostic tools.

1.6.2.3 Updates

1. An update of the Automotive Gateway shall be possible in terms of software. If security exploits require (parts of) the hardware to be upgraded the vehicle manufacturer shall ensure that these high security relevant components can be exchanged/replaced. In the event of a complete hardware exchange of the A-GW the VIN must be paired with the new A-GW and a new initial configuration and personalization (see above) must be carried out.
2. A check of the actuality of the security software shall be checked at least at each maintenance in pre-defined periods. Highly secured remote monitoring by using the A-GW shall be preferred instead of periodical checks.
3. The updates shall be made available by the OEM by using the A-GWA.
4. Regular checks of the A-GW shall be done at least in pre-defined periods by neutral test facilities. Highly secured remote monitoring by using the A-GW shall be preferred instead of periodical checks by using self-test functionalities.

1.6.2.4 Incidents

1. There shall be an audible signal or tell-tale illuminated on the instrument cluster that indicates security incidents or misbehaviour of the A-GW or of other high-security relevant components. In this case and depending on the incident it shall be mandatory to visit a service station as soon as possible, connectivity may be disrupted and automated driving support may be disabled.
2. Any security incident has to be sent to the **A-GWA**.

2 Conformance Claims

2.1 Conformance Statement

This PP requires strict conformance of any PP/ST to this PP.

2.2 CC Conformance Claim

The PP has been developed using Version 3.1 Revision 5 of Common Criteria [CC].

- Conformance of this PP with respect to [CC] Part 2 (security functional components) is CC Part 2 conformant.
- Conformance of this PP with respect to [CC] Part 3 (security assurance components) is CC Part 3 conformant.

2.3 PP Claim

This PP does not claim conformance to any other PP.

2.4 Conformance Rationale

Since this PP does not claim conformance to any Protection Profile, this section is not applicable.

2.5 Package Claim

This PP conforms to assurance package **EAL2 augmented with ALC_FLR.2 and ALC_LCD.1** as defined in [CC] part 3 for product certification.

Application Note 2:	This PP only addresses the conceptual points published in the corresponding report [OTP], and hence, cannot be regarded as comprehensive. Therefore, the ST author is requested to add further implementation-specific functionalities or assurance components to ensure an IT security consideration of the complete specifically given IT system.

3 Security Problem Definition

The Security Problem Definition (SPD) is the part of a PP, which describes

- the external entities that are foreseen to interact with the TOE.
- the assets which the TOE shall protect.
- the assumptions on security relevant properties and behavior of the TOE's environment.
- threats against the assets, which shall be averted by the TOE together with its environment.
- operational security policies, which describe overall security requirements defined by the organization in charge of the overall system including the TOE.

3.1 External entities

The following external entities interact with the Automotive Gateway. Those groups have been defined for the use in this Protection Profile.

Group 0: **Automotive Gateway Administrator**	The Automotive Gateway Administrator (A-GWA) is an entity that manages the following groups, the data usage model and the underlying security mechanisms for the Automotive Gateway. All roles listed below and their user/usage policies are flexibly managed by the A-GWA based on signed messages sent from the relevant roles. Since the A-GWA is a neutral entity, the A-GWA itself has no access rights to content related data and information and cannot change user and usage profiles on his own in full compliance with the 'separation of duties' principle.
Group 1: **Administrative**	Group 1 is intended for "Administrative" entities of the vehicle and grants, therefore, privileged reading and writing access to the vehicles data. However, privileged access does not mean full access. Personal data of the driver (among others private data and all data leaving the vehicle without specific consent), for example, should not be accessible for this administrative group per default. It is of paramount importance that the driver/owner/vehicle occupants have the possibility to withdraw consent and can opt-in, opt-out to the services provided by this group. The OEM belongs to the group as the vehicle is developed, manufactured and also supported by him. As the OEM grants technical services and customer supports, he needs to have privileged reading and writing access for those data and functions that allow compliance with the approval requirements in terms of safety, security (providing security updates over the vehicle's lifetime) and environmental protection. Because of that some OEM related usage profiles (*master usage profile*) could not be changed by profiles of the groups like the user profiles of driver/owner (opt-in, opt-out). Data can also be analysed and evaluated by the OEM in order to further develop their own vehicles and improve the existing systems. For data and functions on which the manufacturer competes with ISPs once the vehicle is registered, the rights to access data and functions shall be equal to those par-ties that are competing. Also the OEM's services shall be accepted/declined by the driver/owner by opting-in/out. This conclusion also applies to the Tier 1 automotive supplier. Such a supplier also needs some vehicle data in order to analyse and evaluate it to improve their parts of the car. In order to offer active and fast support of their parts of the vehicle, a supplier could also have write access in order to fix problems as fast as possible. Here, it should be decided on a case-by-case basis which administrative write and read rights are given. This should depend on the built-in parts of the supplier and be tailored to the needs that arise in the context of these components. It shall be ensured that the independent after-market parts suppliers can

also get the necessary data to develop their products so that the systems and parts market remains competitive with pressure on the prices and offering best value for money to the consumer.

Maintenance is a regular service that is required for a vehicle in order to prolong the life and functionality. In order to diagnose and reset faults, read out in-vehicle data, conduct actuator testing, communicate with the driver and vehicle occupants in a safe and secure manner, determine and solve problems inside a vehicle competently and efficiently, service stations need privileged read and write access to the vehicles data, functions and resources. As part of the maintenance also lifetime aspects, such as regular updates and integrity checks, are carried out by service stations.

Group 2:

Audit

Group 2 is intended for "Auditable" users of the vehicle, therefore, privileged read access. However, this access should not exist permanently, but on an ad-hoc basis and should only contain information that is strictly required for the purpose of the role. Here, the police should be able to access location data in order to identify stolen or damaged cars in order to find and reach them faster, if mandated by a court. The emergency services need information about the status of one or more vehicles and location data in order to get more details about accidents to be able to prepare and conduct their rescue mission more efficiently. Also during a technical inspection, the inspector needs access to certain vehicle data during the inspection. If, during such inspections, also the integrity and actuality of the OTP'S Automotive Gateway and the other high-security relevant components will be checked, additional information packages will be required in order to carry out those checks. Similar applies to the role of the enforcement authorities that test production conformity, roadworthiness and carry out market surveillance tests, for which temporarily information is needed.

The focus in this group should be set on the ad-hoc basis. All roles mentioned here require access for their purposes only temporarily and only in special situations such as a car accident or a technical inspection. Permanent access should definitely not be permitted here. In certain cases, like e.g. remote OBM it must be ensured that data is anonymised and cannot be used to track down the individual vehicle, driver, owner or occupants. Here, an exception of this statement and with that a permanent monitoring of individual vehicles is recommended, that can be done by the government and in particular by the police based on a special request and empowerment concept that needs to be defined.

Group 3:

Docker

Group 3 is intended for 3rd-party developers who implement applications and products for the infotainment system of the vehicle or that place their own diagnostic software on-board of the vehicle that can be used by ISPs to perform remote diagnostic support or prognostics.

In order to do this, such developers should get reading and writing access in a compartment separated from the rest of the vehicle (docker), but with direct access to some in-vehicle data, its functions and resources as well as to the vehicle occupants via the in-vehicle's HMI (e.g. instrument cluster, infotainment display etc). Application (Apps) can be run on-board of the vehicle, using minimum processing and storage capabilities required by legislation, related to support the driver (navigation systems, telecommunication apps, messengers, etc.) developed by OEMs, Suppliers or ISPs running e.g. a prognostic / diagnostic app.

With this access regulation, it is possible for the developer to develop adequately and efficiently ISP applications and accessories without accessing information that is not required or not permitted or gaining further access to the vehicle outside the own area. This also pre-vents

	unauthorised access by applications to other important functions of the vehicle.
Group 4: **User**	Group 4 is intended for the “Direct Use”. This access includes every access of drivers, vehicle occupants and the owner to their own car. Here, an unprivileged “low-level” reading and writing access to the usage data of the vehicle is introduced. Thus, the user has all access to the functions he needs and should have for driving and using his vehicle. Furthermore the owner/driver has the right to control the behaviour of all groups 1-3: He shall be provided with opt-in, opt-out features to decline services if not any longer given consent. An exception of opt-out are mandatory remote services that must be used by the vehicle due to legislation like e.g. eCall.
Group 5: **Public**	Group 5 is aimed at everyone who needs to “collect information” from other traffic participants in order to maintain his service. These are above all road users and road infrastructure which, send and receive information packets to other road users in order to enable more advanced, safe and partly autonomous driving. Here, especially location and driving behaviour data is required and collected. The overall condition is that the data request shall be laid down in legislation (e.g. C-ITS V2V, V2I communication). Any commercial, public request to access to in-vehicle data shall per definition be subject to explicit consent. The possibility shall be provided by vehicle design for the driver / occupants to (partly) opt-in and out and stop the data stream to and from the external party if consent is withdrawn.

3.2 Assets

Authorisation Rules	Files that contain access characteristics in order to configure the read and write access of the external groups. It is also possible to change the individual groups and their members in these files.
Application Notes 3:	The A-GWA can change the access characteristics for the different external entities. The set of access characteristics presented in this PP (see chapter 3.1) is only an example set.
Configuration Data:	Files that contain information used for the configuration of the transmission/reception characteristics, Medium Access Control parameterization, network configuration and supported facilities, and types of messages.
Firmware:	Encoded instructions that regulate the behaviour of the TOE.
Firmware Update:	A new firmware version to replace the old one
HSM2Gateway Data:	Any user data exchanged between the Gateway and the HSM.
ITS Message:	Any standard compliant message sent or received over the Intelligent Transport System (ITS) interface by the TOE from/to other TOEs or ITS-Stations. Message is rated as personal data.
IVN Message:	Any message sent or received over the In Vehicle Network (IVN) interface by the TOE. IVN include the LIN, FlexRay, CAN, and RF communication protocols.

3.3 Assumptions

A.Update	It is assumed that firmware updates for the A-GW that can be provided by an authorised external entity (Group 0 or Group 1) have undergone a certification process according to this Protection Profile before they are issued and can therefore be assumed to be correctly implemented. It is further assumed that the external entity (Group 0 or Group 1) that is authorised to provide the

	update is trustworthy and will not introduce any malware into a firmware update.
A.AutomotiveGatewayAdministrator	It is assumed that the A-GWA (Group 0) is trustworthy and well-trained.
A.AdministrativeGroup	It is assumed that members of the Administrative group (Group 1) are trustworthy and well-trained.
A.AuditSpecialEvents	It is assumed that in cases of a special event, selected members of the Audit group (Group 2) get reading access to data in the vehicle. These members are in such situations trustworthy.
Application Note 4:	The special events have to be defined by the ST writer.
A.PKI	It is assumed that the TOE operational environment provides a Public Key Infrastructure (PKI).
A.CommunicationBypass	It is assumed that the A-GW serves as the central communication for V2X (Vehicle to Vehicle, Vehicle to Infrastructure and Vehicle to any smart automotive service) and therefore will not be bypassed by any other component of the car (e.g. HMI, Docker, ECU).

3.4 Threats

The A-GW can be attacked either by local attacks, by nearfield attacks or by remote attacks:

- **Local attack**: Local Attackers having physical access to the A-GW, the direct environment (vehicle), or a connection between these components, trying to disclose or alter assets while stored in A-GW or transmitted between A-GW and vehicle components.
- **Nearfield attack**: Nearfield Attackers trying to compromise the confidentiality and/or integrity and/or authenticity of assets transmitted via nearfield communication modules and services.
- **Remote attack**: Remote Attackers trying to compromise the confidentiality and/or integrity and/or authenticity of assets transmitted via the ITS (WAN modules and services).

The following threats against the TOE are identified:

T.LocalDataModify	A local attacker may try to modify (i.e. alter, delete, insert, replay or redirect) IVN Messages when transmitted between Gateway and vehicle components or Gateway and external entities. In order to achieve the modification, the attacker may try to modify also assets like the Authorisation Rules, Firmware, Firmware Update or the Configuration Data of the Gateway.
T.RemoteDataModify	An attacker in the nearfield may try to modify (i.e. alter, delete, insert, replay or redirect) ITS Messages when transmitted between the Gateway and an external entity in the nearfield or in the WAN. In order to achieve the modification, the attacker may try to modify also assets like the Authorisation Rules, Firmware, Firmware Update or the Configuration Data of the Gateway.
T.LocalDisclosure	A local attacker may try to violate the privacy of external entities by disclosing transmitted IVN Messages or the HSM2Gateway Data between the TOE and vehicle components, or the TOE and external entities in the nearfield or in the WAN. In order to achieve the modification, the attacker may try to disclose also assets like the Authorisation Rules, Firmware, Firmware Update or the Configuration Data of the Gateway.

T.LocalPhysical	A local attacker may try to modify or get access to IVN Messages, the Firmware or HSM2 Data by physical attack, e.g. an attack implemented with the destroying of an asset or a resource, connecting unknown equipment to the TOE or manipulate hardware to mispresent activities or data.

3.5 Organisational Security Policies

This chapter lists the organizational security policies (OSP) that the gateway shall comply with:

OSP.SE:	The TOE shall use the services of a certified Secure Element for • Decryption of session key, • Generating and using of random numbers and digital signatures, • Secure deletion of private keys, • Storage of keys The Secure Element shall be certified according to [PP-C2C-HSM] and shall be used in accordance with its relevant guidance document.
Application Note 5:	When the RNG functionality is provided by the TOE itself, it has to be appropriately modelled by the ST author using SFR FCS_RNG according to [AIS20] or [AIS31]. Using this SFR, the ST author should consider all necessary modifications concerning an extended SFR component.
Application Note 6:	Since it is expected that on some occasions a large number of messages from other ITS' arrive at the Automotive Gateway, it may be necessary that the verification of the corresponding digital signatures (and certificates) is done outside of the Secure Element. This operation is less critical as it does not need access to the private key.
OSP.Pairing:	During production, the TOE shall be paired with the ITS via the Vehicle Identification Number (VIN) in a secure production environment.

4 Security Objectives

In this chapter the security objectives for the Automotive Gateway and its environment are described.

4.1 Security Objectives for the TOE

O.Authentication

The TOE shall control the access of external entities in WAN or the local network to any information that is sent to, from or via the TOE via its external interfaces. Access control shall depend on the destination interface that is used to send that information.

O.Crypto

The TOE shall provide cryptographic functionality as follows:

- Authentication, integrity protection and encryption of the communication and data to the AGW-A using IF_GW_AGWA.
- Authentication, integrity protection of the communication and data to members of the Audit and Information Collection groups using IF_GW_Audit and IF_GW_Information.
- Replay detection for all communications with external entities.
- encryption of the persistently stored TSF and user data of the TOE.

The cryptographic algorithms performed in the Secure Element of the Automotive Gateway shall be implemented in such a way that they resist known side-channel attacks.

O.Firewall

The TOE shall serve as the connection point for the connected ECUs within the IVN to external entities within the WAN and the V2X environment and shall provide firewall functionality in order to protect the ECUs in the IVN and itself against threats from the WAN side or threats in the V2X environment.

The firewall shall only allow connections from the logical interfaces as defined in chapter 3.1.

O.Management

The TOE shall only provide authorised AGW-A with function for the management of the security features and the read and write permissions of the different groups.

The TOE shall ensure that any change in the behaviour of the security functions can only be achieved from the IF_GW_AGWA interface (WAN). Any management activity from another interface may not be allowed.

O.Log

The TOE shall maintain a set of log files as follows:

1. A system log of relevant events in order to allow an authorised AGW-A or an authorised member of the Administrative group to analyse the status of the TOE. The TOE shall analyse the system log automatically for a cumulation of security relevant events.

The TOE shall further limit access to the information in the different log files as follows:

Access to the information in the system log shall only be allowed for an authorised AGW-A via IF_GW_AGWA or for members of the Administrative group via IF_GW_Admin. In case of a special situation, selected authorised members of the audit group are also allowed access to the system log.

Application Note 7:	The ST author is allowed to define additional sets of logfiles and associated access rules in the Security Objective **O.Log**. Thereby, the ST author has to consider the underlying Authorisation Concept and shall not define any rules that violate the definition of the access rights of the individual groups.
O.Protect	The TOE shall implement functionality to protect its security functions against malfunctions and tampering. Specifically, the TOE shall • encrypt its TSF and user data as long as it is not in use. • overwrite relevant information that is no longer needed to ensure that it is no longer available. • monitor user data and the TOE firmware for integrity errors. • implement and conduct a self-test on a regular basis. • physically protect the secret key material within the Secure Element against tampering. • ensure that the TOE does not emit any information that can be used to obtain information about the secret key material within the Secure Element. • make any physical manipulation within the scope of the intended environment detectable for members of the Administrative Group. • ensure that the TOE fails into a secure state in case of a security relevant malfunction.
O.Time	The TOE shall provide reliable time stamps and update its internal clock in regular intervals by retrieving reliable time information from a dedicated reliable source in the WAN.
O.SecureFirmwareUpdate	The TOE shall implement a secure mechanism to update the firmware of the TOE that ensures that only authorised entities are able to provide updates for the TOE and only authentic and integrity protected updates are applied.

4.2 Environment

OE.SecureSetup	It shall be ensured that appropriate security measures are taken during the assembly/setup of the Automotive Gateway to guarantee for the confidentiality, authenticity and integrity of initial cryptographic data.
OE.SecureElement	The environment shall provide the services of a certified Secure Element for • Storage of Keys, • Generating and using of random numbers and digital signatures, • Secure deletion of private keys, and • Decryption of session key (for TLS connection with the TCC). The Secure Element shall be certified according Protection Profiles like [PP-C2C-HSM] or comparable and shall be used in accordance with its relevant guidance documentation.
OE.Pairing	It shall be ensured that the Automotive Gateway is paired with the Vehicle Identification Number (VIN) during the production.
OE.UpdateSource	The firmware updates for the Automotive Gateway that can be provided by an authorised external entity shall undergo a

	certification process according to this Protection Profile before they are issued to show that the update is implemented correctly. The external entity that is authorised to provide the update shall be trustworthy and ensure that no malware is introduced via a firmware update.
OE.TrustedAutomotiveGateway Administrator	It shall be ensured that the Automotive Gateway Administrator is trustworthy, non-hostile and well-trained.
OE.TrustedAdministrativeGroup	It shall be ensured that members of the Administrative group are trustworthy, non-hostile and well-trained.
OE.TrustedAuditSpecialEvents	It shall be ensured that the members of the audit group are trustworthy, non-hostile and well trained when they are granted reading access to the ITS in the situations of a specific event.
OE.PKI	The environment shall provide a PKI.
OE.CommunicationBypass	It shall be ensured that the A-GW serves as the central communication for V2X (Vehicle to Vehicle, Vehicle to Infrastructure and Vehicle to any smart automotive service) and therefore will not be bypassed by any other component of the car (e.g. HMI, Docker, ECU).

4.3 Security Objectives Rationale

4.3.1 Overview

	O.Authentication	O.Crypto	O.Firewall	O.Management	O.Log	O.Protect	O.Time	O.SecureFIrmewareUpdate	OE.SecureSetup	OE.SecureElement	OE.Pairing	OE.UpdateSource	OE.TrustedAutomotiveGateway Administrator	OE.TrustedAdministrativeGrou	OE.TrustedAuditSpecialEvents	OE.PKI	OE.CommunicationBypass
T.LocalDataModify	X	X	X	X	X	X	X	X									
T.RemoteDataModify	X	X	X	X	X	X	X	X									
T.LocalDisclosure	X	X	X	X	X	X											
T.LocalPhysical						X											
OSP.SE				X		X			X	X							
OSP.Pairing					X						X						
A.Update												X					
A.AutomotiveGateway Administrator													X				
A.Administrative-Group														X			
A.AuditSpecialEvents															X		
A.PKI																X	
A.Communication-Bypass																	X

4.3.2 Countering the Threats

The following sections provide more detailed information on how the threats are countered by the security objectives for the TOE and its operational environment.

4.3.2.1 T.LocalDataModify

The threat **T.LocalDataModify** is countered by a combination of the security objectives **O.Authentication, O.Crypto, O.Management, O.SecureFirmwareUpdate, O.Protect, O.Firewall, O.Log** and **O.Time**.

O.Authentication defines policies and access regulations that the TOE will enforce via the TSF to regulate access to the internal data via the different interfaces for each group. **O.Crpyto** defines the required cryptographic functionality. **O.Management** defines that the access rights to the internal data can only be set by the AGW-A. **O.SecureFirmwareUpdate** defines that the TOE provides a secure mechanism ensuring that only authorised entities are allowed to install updates. **O.Protect** is present to ensure that all security functions are working as specified. **O.Firewall** defines the connections for the devices within the IVN to external entities within the WAN or the V2X environment and shall provide firewall functionality in order to protect the ECUs in the IVN and itself from threats from the WAN side or in the V2X environment. **O.Log** defines that all relevant events within the IVN are recorded. **O.Time** defines that the TOE needs a reliable time stamp mechanism that is also updated from reliable sources regularly in the WAN.

4.3.2.2 T.RemoteDataModify

The threat **T.LocalDataModify** is countered by a combination of the security objectives **O.Authentication, O.Crypto, O.Management, O.SecureFirmwareUpdate, O.Firewall, O.Log** and **O.Time**.

O.Authentication defines policies and access regulations that the TOE will enforce via the TSF to regulate access to the internal data via the different interfaces for each group. **O.Crpyto** defines the required cryptographic functionality. **O.Management** defines that the access rights to the internal data can only be set by the AGW-A. **O.SecureFirmwareUpdate** defines that the TOE provides a secure mechanism ensuring that only authorised entities are allowed to install updates. **O.Protect** is present to ensure that all security functions are working as specified. **O.Firewall** defines the connections for the devices within the IVN to external entities within the WAN or the V2X environment and shall provide firewall functionality in order to protect the ECUs in the IVN and itself from threats from the WAN side or in the V2X environment. **O.Log** defines that all relevant events regarding remote communication are recorded. **O.Time** defines that the TOE needs a reliable time stamp mechanism that is also updated from reliable sources regularly in the WAN.

4.3.2.3 T.LocalDisclosure

The threat **T.LocalDataModify** is countered by a combination of the security objectives **O.Authentication, O.Crypto, O.Management, O.Protect, O.Firewall** and **O.Log**.

O.Authentication defines policies and access regulations that the TOE will enforce via the TSF to regulate access to the internal data via the different interfaces for each group. **O.Crpyto** defines the required cryptographic functionality. **O.Management** defines that the access rights to the internal data can only be set by the AGW-A. **O.Protect** is present to ensure that all security functions are working as specified. **O.Firewall** defines the connections for the devices within the IVN to external entities within the WAN or the V2X environment and shall provide firewall functionality in order to protect the ECUs in the IVN and itself from threats from the WAN side or in the V2X environment. **O.Log** defines that all relevant events regarding within the IVN are recorded.

4.3.2.4 T.LocalPhysical

The threat **T.LocalDataModify** is countered the security objective **O.Protect**.

O.Protect is present to ensure that all security functions are working as specified. In particular, this ensures that a physical attack is detected and appropriate countermeasures such as a fallback to the secure state are taken.

4.3.3 Coverage of Organisational Security Policies

The following sections provide more detailed information about how the security objectives for the environment and the TOE cover the organizational security policies.

4.3.3.1 OSP.SE

The Organisational Security Policy **OSP.SE** that mandates that the TOE utilises the services of a certified Secure Element is directly addressed by the security objectives **OE.SecureElement**, **O.Crypto, O.Management and O.Protect.** The objective **OE.SecureElement** addresses the functions that the Secure Element shall be utilised for as defined in **OSP.SE** and also requires a certified Secure Element according to the specified requirements in **OE.SecureElement**. **O.Crypto** defines the cryptographic functionalities for the TOE itself. In this context it has to be ensured that the Secure Element is operated in accordance with its guidance documentation. **O.Management** is indispensable as it defines the requirements around the management of the Security Functions. **O.Protect** is present to ensure that all security functions are working as specified.

4.3.3.2 OSP.Pairing

The Organisational Security Policy **OSP.Pairing** that mandates that the TOE is paired with the VIN during the production is directly addressed by the security objective **OE.Pairing**. The security objective **O.Log** addresses that the TOE records whether the pairing with the VIN was successful or has failed.

4.3.4 Coverage of Assumptions

The following sections provide more detailed information about how the security objectives for the environment cover the assumptions.

4.3.4.1 A.Update

The assumption **A.Update** is directly and completely covered by the security objective **OE.UpdateSource.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

4.3.4.2 A.AutomotiveGatewayAdministrator

The assumption **A.AutomotiveGatewayAdministrator** is directly and completely covered by the security objective **OE.TrustedAutomotiveGatewayAdministrator.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

4.3.4.3 A.AdministrativeGroup

The assumption **A.AdministrativeGroup** is directly and completely covered by the security objective **OE.TrustedAdministrativeGroup.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

4.3.4.4 A.AuditSpecialEvents

The assumption **A.AuditSpecialEvents** is directly and completely covered by the security objective **OE.TrustedAuditSpecialEvents.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious

4.3.4.5 A.PKI

The assumption **A.PKI** is directly and completely covered by the security objective **OE.PKI.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious

4.3.4.6 A.CommunicationBypass

The assumption A.CommunicationBypass is directly and completely covered by the security objective OE.CommunicationBypass. The assumption and the objective for the environment are drafted in a way that the correspondence is obvious

5 Extended Components Definition

This protection profile does not define any extended components.

6 Security Requirements

6.1 Overview

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE. Those requirements comprise functional components from part 2 of [CC] and the assurance components as defined for the Evaluation Assurance Level 2 augmented with ALC_FLR.2 and ALC_LCD.1 from part 3 of [CC].

The following notations are used:

- **Refinement** operation (denoted by **bold text**) is used to add details to a requirement, and thus further restricts a requirement. In case that a word has been deleted from the original text this refinement is indicated by ~~**crossed out bold text**~~.
- **Selection** operation (denoted by underlined text) is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicised text*) is used to assig a specific value to an unspecified parameter, such as the length of a password.
- **Iteration** operation are identified with a suffix in the name of the SFR (e.g. FDP_IFC.2/FW).

It should be noted that the requirements in the following chapters are not necessarily be ordered alphabetically. Where useful the requirements have been grouped.

The following table summarises all TOE security functional requirements of this PP:

Class FAU: Security Audit	
FAU_ARP.1	Security audit automatic response
FAU_GEN.1	Audit Data Generation
FAU_SAA.1	Security audit analysis
FAU_SAR.1	Security Audit Review
FAU_STG.2	Guarantees of Audit Data Availability
FAU_STG.4	Prevention of Audit Data Loss
Class FCS: Cryptographic Support	
FCS_CKM.1/SigVer	Cryptographic Key Generation for Signature Verification
FCS_CKM.1/TLS	Cryptographic Key Generation for TLS
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/SigVer	Cryptographic Operation for Signature Verification
FCS_COP.1/TLS	Cryptographic Operation for TSL
FCS_COP.1/TLS.HASH	Cryptographic Operation for Hashing
FCS_COP.1/MEM	Cryptographic Operation for TSF and User Data Encryption
Class FDP: User Data Protection	
FDP_ACC.2	Complete Access Control
FDP_ACF.1	Security Attribute based Access Control
FDP_IFC.2	Complete Information Flow Control
FDP_IFF.1	Simple Security Attributes
FDP_RIP.2	Full Residual Information Protection
FDP_SDI.2	Stored Data Integrity Monitoring and Action
Class FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_UAU.2	User Authentication before any Action
FIA_UID.1	Timing of Identification
FIA_USB.1	User-subject Binding
Class FMT: Security Management	
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
Class FPT: Protection of the TSF	
FPT_FLS.1	Failure with preservation of secure state

FPT_RPL.1	Replay Detection
FPT_STM.1	Reliable Time Stamps
FPT_TST.1	TST Testing
FPT_PHP.1	Passive detection of physical attack
Class FTP: Trusted path/channels	
FTP_ITC.1	Inter-TSF Trusted Channel

Table 2: List of Security Functional Requirements

6.2 Security Functional Requirements

6.2.1 Class FAU: Security Audit

6.2.1.1 FAU_ARP.1 Security audit automatic response

FAU_ARP.1.1 The TSF shall ~~take~~ [*inform the A-GWA and [*assignment: *list of actions]*] upon detection of a potential security violation.

6.2.1.2 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [basic] level of audit; and
c) [assignment: *other specifically defined auditable events*].

FAU_GEN1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

6.2.1.3 FAU_SAA.1 Security audit analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;
b) [assignment: *any other rules*].

6.2.1.4 FAU_SAR.1 Security Audit Review

FAU_SAR.1.1 The TSF shall provide [*only user of the group "Administrative" and "Direct Use"*] with the capability to read [assignment: *list of audit information*] from the audit records.

FAU_SAR.1.1 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.5 FAU_STG.2 Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail form unauthorised deletion

FAU_STG.2.2 The TSF shall be able to [detect] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [assignment: *metric for saving audit records*] stored audit records will be maintained when the following conditions occur: [selection, *audit storage exhaustion, failure, attack*]

6.2.1.6 FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and [*inform the belonging user of the group "Administrative"*] if the audit trail is full.

6.2.2 Class FCS: Cryptographic Support

6.2.2.1 FCS_CKM.1/SigVer Cryptographic Key Generation for Signature Verification

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following [assignment: *list of standards*].

6.2.2.2 FCS_CKM.1/TLS Cryptographic Key Generation for TLS

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following [assignment: *list of standards*].

6.2.2.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

6.2.2.4 FCS_COP.1/SigVer Cryptographic Operation for Signature Verification

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

6.2.2.5 FCS_COP.1/TLS Cryptographic Operation for TLS

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

6.2.2.6 FCS_COP.1/TLS.HASH Cryptographic Operation for Hashing

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

6.2.2.7 FCS_COP.1/MEM Cryptographic Operation, encryption of TSF and user data

Class FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryp-*

tographic algorithm] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 8:	Please note that for the key generation process an external security module 1680is used during TOE production.

6.2.3 FDP: User Data Protection

6.2.3.1 Introduction to the Security Functional Policy

The security functional requirements that are used in the following sections implicitly define a Security Functional Policy (SFP). This policy is introduced in the following paragraphs in more detail to facilitate the understanding of the SFRs:

- The access control SFP is a policy to control the access to objects under the control of the TOE. It also implements an information flow policy to fulfil the objective O.Firewall. All requirements around the communication control that the TOE poses on communications between the different networks are defined in this policy. The details of this access control policy highly depend on the concrete application of the TOE.

6.2.3.2 FDP_ACC.2 Complete Access Control

FDP_ACC.2.1 The TSF shall enforce the [*access control SFP*] on [

Subjects: all external entities

Objects: any information that is sent to, from or via the TOE and any information that is stored in the TOE] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.2.3.3 FDP_ACF.1 Security Attribute based Access Control

FDP_ACF.1.1 The TSF shall enforce the [*access control SFP*] to objects based on the following: [

Subjects: all external entities

Objects: any information that is sent to, form or via the TOE

Attributes: destination interface].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- *A user of the group "Automotive Gateway Administrator is only allowed to have read and write access to Authorisation Rules via the interface IF_GW_AGWA.*
- *A user of the group "Administrative" is allowed to have read and write access to Configuration Data, Firmware Update, logs and IVN message via the interface IF_GW_Administrative.*
- *A user of the group "Audit" is allowed to heave temporarily read access to Configuration Data, ITS Message and IVN Message via the interface IF_GW_Audit.*
- *A user of the group "Docker" is allowed to have limited read and write access to in vehicle data limited and defined by users of the group "Administrative" via the interface IF_GW_Docker.*
- *A user of the group "Direct User" is allowed to have read and write access to usage data of the vehicle and all functions he*

need and should have for driving and using his vehicle. In addition a user of this group has read access to logs. All access is done via the interface IF_GW_Driver.

- *A user of the group "Information Collection" is only allowed to have read access to ITS messages that is send over the interface IF_GW_Information.*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

- *The A-GWA is not allowed to have access to any data except the Authorisation Rules.*
- *No other Group except the A-GWA is allowed to have access to the Authorisation Rules.*
- *Nobody must be allowed to read the symmetric keys used for encryption*].

6.2.3.4 FDP_IFC.2 Complete Information Flow Control

FDP_IFC.2.1 The TSF shall enforce the [*access control SFP*] on [*the TOE, external entities and all information flowing between them*] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.2.3.5 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [access *control SFP*] based on the following types of subject and information security attributes: [

Subjects: The TOE and all external entities

Information: Any information that is sent to, from or via the TOE

Attributes: destination interface, source interface, destination authenticated].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].

FDP_IFF.1.3 The TSF shall enforce [*none*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*none*].

6.2.3.6 FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] all objects.

6.2.3.7 FDP_SDI.2 Stored Data Integrity Monitoring and Action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all objects, based on the following attributes: [*hash value and valid signature, if expected*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*inform the user of the group "Administrative"*].

6.2.4 Class FIA: Identification and Authentication

6.2.4.1 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*Authorisation Rules*].

6.2.4.2 FIA_UAU.2 User Authentication before any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.3 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note 9: The identification is done automatically via Certificates.

6.2.4.4 FIA_USB.1 User-subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*attributes as defined in FIA_ATD.1*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

6.2.5 Class FMT: Security Management

6.2.5.1 FMT_MOF.1: Management of security functions behaviour.

FMT_MOF.1.1 The TSF shall restrict the ability to [modify the behaviour of] the functions [*for management as defined in FMT_SMF.1*] to [*roles and criteria as defined in Table 3*].

Function	Limitation
Firmware Update	The firmware update must only be possible after the authenticity of the firmware update has been verified (using the Services of the SE) and if the version number of the new firmware is higher to the version of the installed firmware.
Authorisation Rules	The management functions for the Authorisation Rules must only be accessible for the A-GWA and only via the interface IF_GW_AGWA
All other management functions as defined in FMT_SMF.1	The management functions must only be accessible for users of the group "Administrative" and only via the interface IF_GW_Administrative.

Table 3: Restrictions on Management Functions

6.2.5.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

6.2.5.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [*all groups that are defined as external entity*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.5.4 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [*access control SFP*] to restrict the ability to [query, modify, delete, [*none*]] the security attributes [*all relevant security attributes*] to [*user of the groups "A-GWA" and "Administrative"*].

6.2.5.5 FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the [*access control SPF*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*user of the group "A-GWA"*] to specify alternative initial values to override the default values when an object or information is created.

6.2.6 Class FPT: Protection of the TSF

6.2.6.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [

- *[assignment: other of types of failures in the TSF]*].

6.2.6.2 FPT_RPL.1 Replay Detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [*all*].

FPT_RPL.1.2 The TSF shall perform [assignment: *list of specific actions*] when replay is detected.

6.2.6.3 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note 10: The local system time of the TOE is synchronised regularly with a reliable external time source provided by a user of the group "Administrative". Radio controlled clocks are not used. A maximum deviation of 3% of the measuring period is allowed to be in conformance with this PP.

6.2.6.4 FPT_TST.1 TST Testing

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]*] to demonstrate the correct operation of [selection: *[assignment: parts of TSFI], the TSF*].

6.2.6.5 FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices of TSF's elements has occurred.

6.2.7 Class FTP: Trusted path/channels

6.2.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure**:**

a) Cryptographically-protected communication channel using the external interface to external entities with a combination of the following cipher suites defined there:
1. Symmetric cipher defined in FCS_COP.1/TLS
2. Keyed hash algorithms defined in FCS_COP.1/TLS.HASH as defined in [RFC5246].

b) Authenticated communication channel using TLS as defined in [FRC5246] for server authentication.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

6.3 Security Assurance Requirements

The minimum Evaluation Assurance Level for this Protection Profile is **EAL2 augmented with ALC_FLR.2 and ALC_LCD.1.**

According to [CC, Part 3, §§99f]:

EAL2 requires the co-operation of the developer in terms of delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time. EAL2 is therefore applicable in those circumstances where developers or users require a low moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

The augmentation with ALC_FLR.2 has been chosen to include also the aspect on how security flaws are discovered, tracked and correct by the developer. This provides assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE.

The augmentation with ALC_LCD.1 has been chosen to include also the aspect of a controlled development and maintenance of the TOE. This provides assurance that the TOE meets all of its SFRs.

The following table lists the assurance components which are therefore applicable to this PP:

Assurance Class	Assurance Component
Development	ADV_ARC.1
	ADV_FSP.3
	ADV_TDS.1
Guidance Documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle Support	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
	ALC_FLR.2
	ALC_LCD.1
Security Target Evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1

	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	AVA_VAN.2

Table 4: Assurance Requirements

6.3.1 Fulfilment of the Dependencies

The dependencies of the assurance requirements taken from EAL 2 augmented by ALC_FLR.2 and ALC_LCD.1 are fulfilled automatically.

6.4 Security Requirements Rationale

This chapter proves that the set of security requirements (TOE) is suited to fulfil the security objectives described in chapter 4 and that each SFR can be traced back to the security objectives. At least one security objective exists for each security requirement.

	O.Authentication	O.Crypto	O.Management	O.SecureFirmwareUpdate	O.Potect	O.Firewall	O.Log	O.Time
FAU_ARP.1							X	
FAU_GEN.1							X	
FAU_SAA.1							X	
FAU_SAR.1							X	
FAU_STG.2							X	
FAU_STG.4							X	
FCS_CKM.1/SigVer		X						
FCS_CKM.1/TLS		X						
FCS_CKM.4		X						
FCS_COP.1/SigVer		X						
FCS_COP.1/TLS		X						
FCS_COP.1/TLS.HASH		X						
FCS_COP.1/MEM		X			X			
FDP_ACC.2	X							
FDP_ACF.1	X							
FDP_IFC.2						X		
FDP_IFF.1						X		
FDP_RIP.2					X			
FDP_SDI.2					X			
FIA_ATD.1			X					
FIA_UAU.2			X					
FIA_UID.1			X					
FIA_USB.1			X					
FMT_MOF.1			X	X				
FMT_SMF.1			X					
FMT_SMR.1			X					
FMT_MSA.1			X					
FMT_MSA.3			X					
FPT_FLS.1					X			
FPT_RPL.1		X						

FPT_STM.1							X	X
FPT_TST.1		X	X		X	X	X	X
FPT_PHP.1					X			
FTP_ITC.1						X		

Table 5: Fulfilment of Security Objectives

The following paragraphs contain more details on this mapping.

6.4.1 O.Authentication

O.Authentication is met by a combination of the following SFRs:

FDP_ACC.2 and **FDP_ACF.1** define the access control policy as required to address O.Access.

6.4.2 O.Crypto

O.Crypto is met by a combination of the following SFRs:

- **FCS_CKM.1/SigVer** defines the requirements on key negotiation for the Signature Verification
- **FCS_CKM.1/TLS** defines the requirements on key negotiation for the TLS protocol
- **FCS_CKM.4** defines the requirements around the secure deletion of the cryptographic keys.
- **FCS_COP.1/SigVer** defines the requirements for the Signature Verification.
- **FCS_COP.1/TLS** defines the requirements around the encryption and decryption capabilities of the Gateway for communications with external parties.
- **FCS_COP.1/TLS.HASH** defines the requirements on hashing that are needed in the context of digital signatures (which are created and verified by the security module).
- **FCS_COP.1/MEM** defines the requirement around the encryption of TSF data.
- **FPT_RPL.1** ensures that a replay attack for communications with external entities is detected.
- **FPT_TST.1** defines the requirement in order to run self-tests for all security functionalities.

6.4.3 O.Management

O.Management is met by a combination of the following SFRs:

- **FIA_ATD.1** defines the attributes for users.
- **FIA_UAU.2** defines the requirements around the authentication of users.
- **FIA_UID.1** defines requirements around the identification of users.
- **FIA_USB.1** defines that the TOE must be able to associate users with subjects acting on behalf of them.
- **FMT_MOF.1** defines requirements around the limitations for management of security functions.
- **FMT_SMF.1** defines the management functionalities that the TOE must offer.
- **FMT_SMR.1** defines the role concept for the TOE.
- **FMT_MSA.1** defines requirements around the limitations for management of attributes.
- **FMT_MSA.3** defines the default values for the access control SFP.
- **FPT_TST.1** defines the requirement in order to run self-tests for all security functionalities.

6.4.4 O.SecureFirmwareUpdate

O.SecureFirmwareUpdate is met by a combination of the following SFRs:

- **FMT_MOF.1** defines requirements around a secure firmware update.

6.4.5 O.Protect

O.Protect is met by a combination of the following SFRs:

- **FCS_COP.1/MEM** defines that the TOE shall encrypt its TSF and user data as long as it is not in use.
- **FDP_RIP.2** defines that the TOE shall make information unavailable as soon as it is no longer needed.
- **FDP_SDI.2** defines requirements around the integrity protection for stored data.
- **FPT_FLS.1** defines requirements that the TOE falls back to a safe state for specific error cases.
- **FPT_PHP.1** defines the exact requirements around the physical protection that the TOE has to provide.
- **FPT_TST.1** defines the requirement in order to run self-tests for all security functionalities.

6.4.6 O.Firewall

O.Firewall is met by a combination of the following SFRs:

- **FDP_IFC.2** defines that the TOE shall implement an information flow policy for its firewall functionality.
- **FDP_IFF.1** defines the concrete rules for the firewall information flow policy.
- **FTP_ITC.1** defines the policy around the trusted channel to the A-GWA.

6.4.7 O.Log

O.Log is met by a combination of the following SFRs:

- **FAU_GEN.1**, **FAU_ARP.1** and **FAU_SAA.1** define the implementation of a log.
- **FAU_SAR.1** defines the requirements around the audit review functions and that access to them shall be limited to authorised A-GWA via the IF_GW_AGWA interface.
- **FAU_STG.2** guarantees that the audit data is always available and cannot be deleted or modificated.
- **FAU_STG.4** defines the requirements on what would happen if the audit log is full.
- **FPT_STM.1** defines that the TOE shall be able to provide reliable time stamps for the logs.
- **FPT_TST.1** defines the requirement in order to run self-tests for all security functionalities.

6.4.8 O.Time

O.Time is met by a combination of the following SFRs:

- **FPT_STM.1** defines that the TOE shall be able to provide reliable time stamps.
- **FPT_TST.1** defines the requirement in order to run self-tests for all security functionalities.

6.4.9 Fulfilment of the Dependencies

The following table shows how each dependency of the security function requirement is fulfilled:

Security Functional Requirement	Dependency according to [CC2]	Dependency fulfilled
FAU_ARP.1	FAU_SAA.1 Potential violation analysis	FAU_SAA.1
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAA.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_SAR.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.2	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.4	FAU_STG.1 Protected audit trail storage	FAU_STG.2

FCS_CKM.1/SigVer	[FCS_CKM.2 Cryptographic key distribution, or CS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/SigVer FCS_CKM.4
FCS_CKM.1/TLS	[FCS_CKM.2 Cryptographic key distribution, or CS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/TLS FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1/SigVer FCS_CKM.1/TLS FCS_CKM.1/MEM
FCS_COP.1/SigVer	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/SigVer FCS_CKM.4
FCS_COP.1/TLS	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/TLS FCS_CKM.4
FCS_COP.1/TLS.HASH	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 Please refer to chapter 6.4.10 for missing dependency.
FCS_COP.1/MEM	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 Please refer to chapter 6.4.2 for missing dependency.
FDP_ACC.2	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset control FMT_MSA.3 Static attribute initialisation	FDP_ACC.2 FMT_MSA.3

FDP_IFC.2	FDP_IFF.1 Simple security attributes	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.2 FMT_MSA.3
FDP_RIP.2	-	-
FDP_SDI.2	-	-
FIA_ATD.1	-	-
FIA_UAU.2	FIA_UID.1 Timing of Identification	FIA_UID.1
FIA_UID.1	-	-
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.2 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FPT_FLS.1	-	-
FPT_RPL.1	-	-
FPT_STM.1	-	-
FPT_TST.1	-	-
FPT_PHP.1	-	-
FTP_ITC.1	-	-

Table 6: Fulfilment of Security Objectives

6.4.10 Justification for missing dependencies

The hash algorithm as defined in **FCS_COP.1/TLS.HASH** does not need any key material. As such dependency to an import or generation of key material is omitted for this SFR.

The key material as defined in **FCS_COP.1/MEM** will be generated and stored into the security module while the integration phase of production of the TOE.

7 References

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Common Criteria Management Board, Version 3.1, Revision 5, April 2017

[CC2] *Common Criteria for Information Technology Security Evaluation, Part 2: Functional security components*
Version 3.1, Revision 5, April 2017

[CC3] *Common Criteria for Information Technology Security Evaluation, Part 3: Assurance security components*
Version 3.1, Revision 5, April 2017

[CEM] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*
Version 3.1, Revision 5, April 2017

[CSA] *Cybersecurity Act*
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
http://data.europa.eu/eli/reg/2019/881/oj

[C-ITS-Korridor] *Cooperative ITS Corridor*
Joint deployment of Ministry of Infrastructure and the Environment of the Netherlands, Federal Ministry of Transport and Digital Infrastructure, and Austrian Ministry for Transport, Innovation and Technology
https://c-its-korridor.de

[ENISA1] *Cyber Security and Resilience of smart cars – Good practices and recommendations*
ENISA, December 2016, ISBN 978-92-9204-184-7

[ENISA2] *ENISA good practices for Security of Smart Cars*
ENISA, November 2019, ISBN 978-92-9204-317-9

[ISO21434] *ISO/SAE DIS 21434 – Road vehicles – Cybersecurity engineering*
International Standardisation Organisation, Committee Draft

[JRC] *Access to digital car data and competition in aftersales services*
B. Martens, F. Müller-Lang
European Commission, DG JRC, September 2018
https://ec.europa.eu/jrc/sites/jrcsh/files/jrc112634.pdf

[OTP] *Report: On-Board Telematics Platform Security*
Bartsch, Bobel, Niehöfer, Wagner, Wahner
FIA, May 2020

[PP-C2C-HSM] *Protection Profile V2X Hardware Security Module*
Car2Car Communication Consortium, April 2020

[PP-C2C-TX] *Protection Profile V2X Gateway - Draft*
Car2Car Communication Consortium (in specification)

[PP-CSP] *Common Criteria PP, Cryptographic Service Provider*
BSI, BSI-CC-PP-0104, V.9.8, February 2019
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0104.html

[PP-DT-EGF] *Common Criteria PP, Digital Tachograph – External GNSS Facility (EGF PP)*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0092b_pdf.pdf

[PP-DT-MS] *Common Criteria PP, Digital Tachograph – Motion Sensor (MS PP)*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0093b_pdf.pdf

[PP-DT-TC1] *Common Criteria PP, Digital Tachograph – Smart Card (Tachograph Card)*
BSI, BSI-CC-PP-0070, V1.02, November 2011
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0070.html

[PP-DT-TC2] *Common Criteria PP*, *Digital Tachograph – Tachograph Card*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0091b_pdf.pdf

[PP-DT-VU1] *Common Criteria PP*, *Digital Tachograph – Vehicle Unit*
BSI, BSI-CC-PP-0057, V1.0, July 2010
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0057.html

[PP-DT-VU2] *Common Criteria PP*, *Digital Tachograph – Vehicle Unit (VU PP)*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0094b_pdf.pdf

[PP-RWU] *Protection Profile for a Road Warning Unit*
BASt, BSI-CC-PP-0104, V1.1, July 2019
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0106.html

[PP-Safertec1] *The Protocol Control / Communication Unit Protection Profile Module*
K. Maliatsos, Safertec, April 2019

[PP-Safertec2] *Sensor Monitor Protection Profile Module*
K. Maliatsos, Safertec, April 2019

[PP-Safertec3] *The V-ITS-S Base Protection Profile*
K. Maliatsos, Safertec, July 2019

[PP-SMGW] *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*
BSI, BSI-CC-PP-0073, V1.3, March 2014
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0073.html

[PP-SMGW-SE] *Protection Profile for a Security Module for Smart Metering Systems (Security Module PP)*
BSI, BSI-CC-PP-0077-V2, V1.03, December 2014
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0077+V2.html

[PP-Taxi] *Beveiligingsprofiel Boordcomputer Taxi (PP-BCT)*
Ministerie van Infrastructuur en Milieu – Netherlands
V1.8, February 2015
https://www.commoncriteriaportal.org/files/ppfiles/[BCT%20PP]%20BeveiligingsprofielBCTV1.8.pdf

[SOG-IS] *Senior Officials Group Information Systems Security*
Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, V 3.0, January 2010
https://www.sogis.eu/

[TISAX] *TISAX (Trusted Information Security Assessment Exchange): Questionnaire for checking Information Security Assessment and Information Security Management*
VDA, Vers. 4.1.1
https://www.vda.de/en/services/Publications/information-security-assessment.html

[TRL] *TRL: Access to In-vehicle Data and Resources, Final report*
M. McCarthy, M. Seidl, S. Mohan, J. Hopkin, A. Stevens, F. Ognissanto
European Commission, DG MOVE, 18.05.2017