Protection Profile for a Road Works Warning Gateway

RWWG-PP

Version 1.1

Certification-ID: BSI-CC-PP-0106

Bundesministerium für Verkehr und Digitale Infrastruktur
Referat StB 12
TRDir Konstantin Sauer
Robert-Schuman-Pl. 1
53175 Bonn
Internet: http://www.bmvi.de

Table of content

List of Tables

List of Figures

1 PP introduction

1.1 Introduction

This Protection Profile defines the Security Functional Requirements and the Security Assurance Requirements for a Road Works Warning Unit.

The Road Works Warning Unit is an electronic device that warns approaching traffic about road works. It is the electronic pendant of a physical sign that would warn the drivers against approaching traffic.

1.2 PP Reference

Title:	Protection Profile for a Road Works Warning Gateway
Version:	1.1
Authors:	Dr. Brian Niehöfer (TÜViT), b.niehoefer@tuvit.demailto: Markus Wagner(TÜViT), m.wagner@tuvit.de Sandro Berndt (BASt), berndt@bast.de
Certification-ID:	BSI-CC-PP-0106
Evaluation Assurance Level:	EAL 3
CC-Version:	3.1 Revision 5
Keywords:	Road Works Warning Unit

1.3 Specific terms

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

Term	Description
CAM	Cooperative Awareness Message Status information periodically exchanged between vehicles by means of car-to-car communication (C2C) or road side units (RSU) by means of car-to-infrastructure communication (C2I), potentially including other road users (e.g. pedestrians, cyclists) and communication partners (C2X, car-to-everything). (Standardized in [ETSI EN 302 637-2]).
DENM	Decentralized Environmental Notification Message Event-based notifications exchanged between vehicles by means of car-to-car communication (C2C) or road side units (RSU) by means of car-to-infrastructure communication (C2I), potentially including other road users (e.g. pedestrians, cyclists) and communication partners (C2X, car-to-everything). DENM is also used to indicate road hazards, e.g. road works warning (RWW). (Standardized in [ETSI EN 302 637-3])
GNSS	Global Navigation Satellite System The system can be used for providing position, navigation or for tracking the position of something fitted with a receiver
ICS	ITS Central Station Fixed control station with broadband connection to IRS, potentially connecting

Term	Description
	various (backend) systems.
IRO	IRS Operator Administrator of IRS.
IRS	ITS Roadside Station ITS computing platform, including communication and processing capacity, linked to road infrastructure.
ITS	Intelligent Transport Systems Advanced application which, without embodying intelligence as such, aims to provide innovative services relating to different modes of transport and traffic management and enable users to be better informed and make safer, more coordinated, and 'smarter' use of transport networks.
IVS	ITS Vehicle Station Mobile platform transmitting CAMs and DENMs in ITS scenarios (e.g. vehicles)
PKI	Public Key Infrastructure A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption.
RWWG	Road Works Warning Gateway
RWWU	Road Works Warning Unit

Table 1: Specific terms

1.4 TOE Overview

1.4.1 Introduction

The TOE described in this Protection Profile is a Road Works Warning Gateway (RWWG) as a part of the corresponding Road Works Warning Unit (RWWU), which is an electronic device, mostly mounted on trailers that warn approaching traffic that road works is carried out. Seen from the road works trailer point of view, the services of the RWWG will be a service on top of the basic functionality of the road works trailer, i.e. barrier with physical warning sign. This means that even in the case when the RWWG is shortly not functioning due to breakdown or maintenance, the trailer must be available all times and the signboard must remain functional.

The TOE itself is the electronically driven module, which is able to collect data sent by bypassing vehicles near temporary road works using them for different features, like traffic surveillance or warnings. In Germany, the Road Works Warning service will be implemented for temporary road works only (typically one-day construction sites). The local traffic surveillance service will cover the vicinity of the road works site, with the objective to derive local traffic flow data and to provide input data to other cooperative services.

1.4.2 TOE type

The TOE is an embedded device within the Road Works Warning Unit, controlling the basic functionalities and communication aspects as well as the data aggregation.

1.4.3 System Overview

The following figure provides an overview over the TOE, its separation from the RWWU and RWWG respectively and its immediate environment.

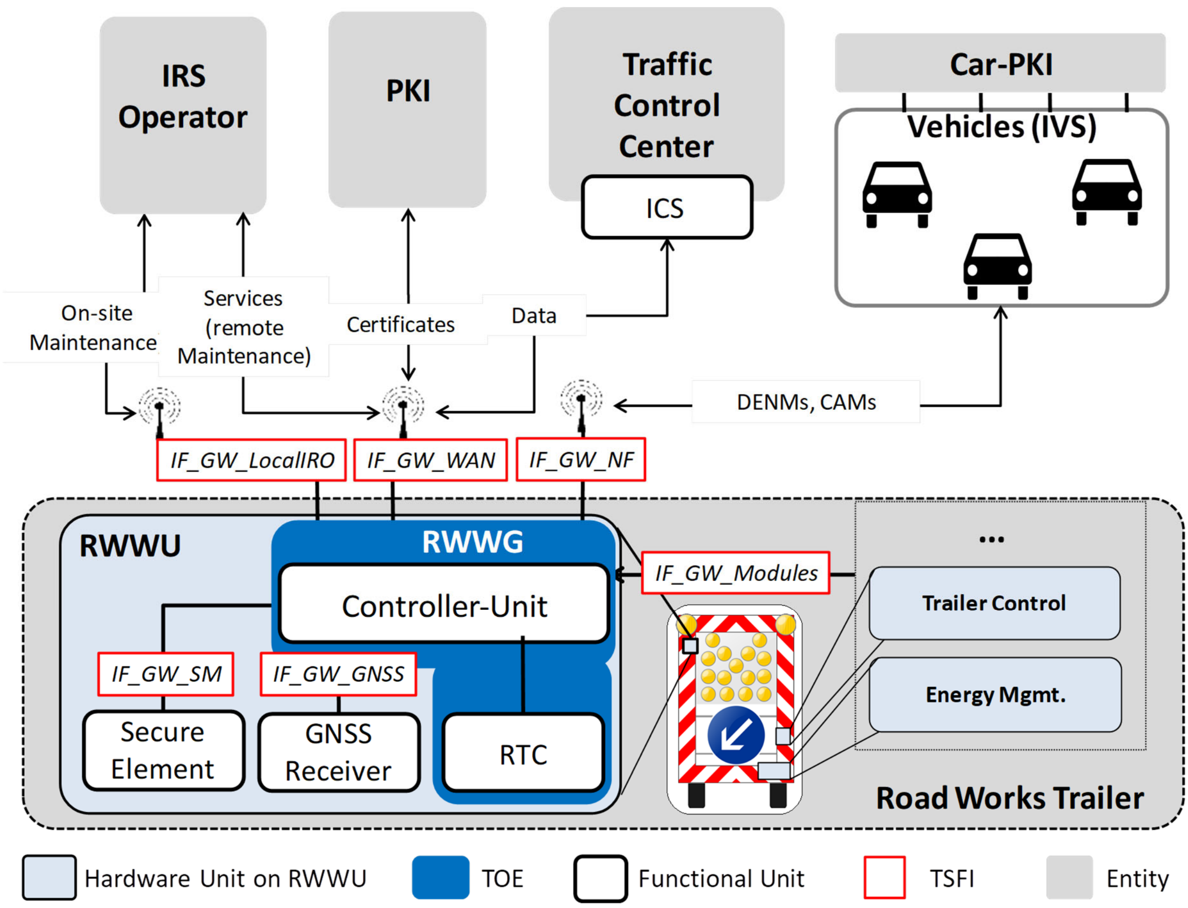

Figure 1: TOE and its environment

The TOE is an electronic device that is able to collect data sent by bypassing vehicles near temporary road works using wireless access in vehicular environments (IEEE 802.11p). It is the electronic part of a sign that would be able, among others, to trigger a warning to drivers of approaching traffic, which additionally supports further services like local traffic surveillance.

The Gateway utilises the services of a Secure Element (e.g. a smart card) as a cryptographic service provider and as a secure storage for confidential assets.

1.4.4 **Services of the TOE**

The following paragraphs introduce the functionality of the TOE in a more detailed manner and contribute to the logical boundary of the TOE. The purpose of the services enabled by the TOE is to improve road traffic in various ways, e.g. in terms of increased traffic safety as well as improved traffic flow and efficiency.

1.4.4.1 Road Works Warning

The Road Works Warning service is used to inform road users within the communication range of the TOE about the actual situation on the road, i.e. vehicles in the vicinity of the TOE when approaching an ongoing temporary road works. This information needs to be on time. To realize this objective, the road works trailer broadcasts appropriate information towards the vehicles approaching the road works, using Decentralised Environmental Notification Messages ([DENM]).

As mentioned above, the services of the RWWG will be a service on top of the basic functionality of the road works trailer, i.e. barrier with physical warning sign. This means that even in the case when the RWWG is shortly not functioning due to breakdown or maintenance, the trailer must be available all times and the signboard must remain functional.

1.4.4.2 Local Traffic Surveillance

This service receives information being broadcasted by the vehicles using DENM and CAM (Cooperative Awareness Messages) ([CAM]), potentially aggregates the received data and makes the information available for improved traffic management services. This kind of potential aggregation may be done partly or completely in the TCC and/or may also be used by other services of the road operators and may be re-used by other service providers.

1.4.5 **TOE physical scope**

The TOE described in this Protection Profile aims on the provision of at least all mentioned functionalities (cmp. Section 1.4.4). 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 section1.4.6.

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

- Mobile communication segments (at least one mandatory)
  - GSM,
  - UMTS,
  - LTE.
- Car-2-X communication (mandatory)
  - IEEE 802.11p
- Positioning technology (recommended)

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

- GPS / Galileo / GNSS receiver

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.

1.4.6 TOE logical scope

The TOE realizes the functional blocks primary belong to the group “message generation, processing and handling:

- Detection, definition, generation and storage of security-relevant events for logging and their mapping to corresponding entities.
- Information flow policies and rules.
- 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 (incl. initial values)
- Secure Firmware Update
- Provide self-test possibilities
- Replay detection
- Secure data deletion
- Reliable time-stamp generation
- Trusted communication establishment
- TLS communication to IRS or ICS after receiving decrypted session key from Secure Element

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.

1.4.7 The logical interfaces of the TOE

The TOE offers its functionality as outlined before via a set of external interfaces. Figure 1 also indicates the cardinality of the interfaces. The following table provides an overview of the mandatory external interfaces of the TOE and provides additional information:

Interface Name	Description
IF_GW_WAN	Via this interface, the RWWU has to establish all wide area communication connections, e.g. for interaction with a remote IRS Operator with the PKI respectively or for transmitting or receiving data from/to the TCC.
IF_GW_IVS	This interface is responsible for every near-field communication. This includes the reception of DENMs or CAMs from the IVS, the potential Warning of al IVS in the direct surrounding if necessary or a locally connected IRO.
IF_GW_LocalIRO	This interface is used for local IROs only, aiming on allowed administration tasks.
IF_GW_GNSS	This interface is used for the connection to optional GNSS receiver, and the provision/estimation of the RWWG position.
IF_GW_SM	The interface connects the TOE with the Secure Element.
IF_GW_Modules	Via this interface, further functional modules on the road works trailer are

Interface Name	Description
	connected to the RWWG.

Table 2: Mandatory TOE external interfaces

Application Note: Within this PP, it is assumed that IF_GW_Modules is wired. Should any ST author prefers wireless connections, this shall be modeled accordingly to ensure received the integrity of the received data, e.g. by a corresponding encryption.

1.5 Secure Element (not part of the TOE)

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

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

In practice the Secure Element can be realised by a smart card for example. The main application of the RWWG should be capable of verifying the authenticity of the Secure Element on startup.

Application Note: Since it is expected that on some occasions a large number of messages from IVSs arrive at RWWG, it may be necessary that the verification of the corresponding digital signatures (and certificates) is done outside the Secure Element. This operation is less critical as it does not need access to the private key.

1.6 Life cycle

The Life Cycle of the TOE just consist of four consecutive phases without declines:

1. **Design/Development**
   The development of The TOE itself.
2. **Manufacturing/Assembly**
   The production itself like hardware assembly, or software installation.
3. **Normal Operation**
   Operational phase of the TOE. All security functions shall be working as specified.
4. **End of Life**
   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.

All steps (including those, which are not parts of this Protection Profile) are further explained in [SiKo_RWWG].

Application Note: If the return of a TOE to the certified state at the process level should be possible (e.g. repair processes), the ST author shall also model this by means of appropriate specifications.

251

2 Conformance Claims

2.1 Conformance statement

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

2.2 CC Conformance Claims

This 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 claim rationale

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

2.5 Package Claim

This PP is conforming claims assurance package EAL3 as defined in [CC] Part 3.

Hint:	This PP acknowledges that the various components of the TOE may be developed by different companies and that a large amount of the work of the developer of the RWWG refers to the integration of those components. However, as the Evaluation Assurance Level in this Protection Profile has been chosen to be EAL 3, this should not introduce intractable problems during the evaluation process.

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 organisation in charge of the overall system including the TOE.

3.1 External entities

The following external entities are allowed to interact with the TOE.

Role	Description
IRS Operator (IRO)	The IRS operator is responsible for initial setup of the RWWG, installing key and certificate material, firmware updates, and/or for the potential provision of the collected data to the TCC.
Traffic Control Center (TCC)	The traffic control center sending and receiving traffic data to/from the RWWG, typically via ICS.
Vehicles (IVS)	Vehicles are sending and receiving traffic/road works data to/from the RWWG.
Maintenance Authority	The motorway maintenance authority/road works staff is setting up the trailer at the road works site. This entity does not operate the RWWG directly however.
Maintenance Personnel	The Maintenance personnel are responsible for periodic local maintenance and repairs.
PKI	The public key infrastructure issuing certificates to the RWWG and traffic control center (TCC) required for establishing a secure connection between the RWWG and TCC.

Table 3: External Entities

3.2 Assets

The following table lists the assets that will need to be protected by the TOE.

Primary Assets	**In(coming)/ Out(going)**	**Source/ Destination**	**Protection Requirements**	**Comment**
Status of Signboard	In	Sign-board	-	Status of the signboard on the trailer, where the TOE is mounted (e.g. on tour or placed). Correctness of data has to be assumed
Status of illuminated arrow sign	In	Sign-board	-	Status of the illuminated arrow sign on the trailer, where the TOE is mounted (e.g. arrow down-left). Correctness of incoming data has to be assumed.
Status information (e.g. battery status, status of the board)	In & Out	Various sensor devices	-	Correctness of incoming data has to be assumed. Outgoing status information is out of evaluation scope
CAM	In & Out	IVS, TCC	Integrity, Authenticity	Incoming: TOE verifies signature; Outgoing: TOE forwards parts of CAM to TCC.
DENM	In & Out	IVS	Integrity, Authenticity	Incoming: TOE verifies signature; Outgoing: TOE forwards DENMs with original signature from IVS to IVS; TOE creates and signs DENM.
Payload of DENM	Out	TCC	Integrity, Authenticity	TOE forwards parts of DENM to TCC
Information from TCC	In	TCC	Integrity, Authenticity	Correctness of incoming data has to be assumed. Out of evaluation scope

IRO data	In & Out	IRO	Integrity, Authenticity	Incoming: TOE verifies integrity and authenticity; Outgoing: Admin data for IRO, e.g. acknowledgements, logs, etc.
Firmware Update	In	IRO	Integrity, Authenticity	TOE verifies integrity and authenticity
Secondary Assets	**Description**		**Protection Requirements**	**Comment**
Cryptographic keys	Ephemeral or long-term cryptographic material used by the TOE for cryptographic operations.		Integrity and Authenticity (for all keys), Confidentiality (at least for all private keys)	At least the private keys have to be stored in the Secure Element.

286 **Table 4: Assets**

Application Note: The integrity of the CAMs and DENMs received via IF_GW_IVS is given by the defined ETSI standards ([CAM] and [DENM]), the required PKI and additionally protected in case of forwarding to the ICS by the TLS channel, which is also mandatory.

If a data aggregation of the defined assets CAMs and DENMs are provided by the implementation-specific TOE, the ST shall include the aggregated data as additional asset and protect it accordingly against further manipulation (see T.LocalDataManipulation and T.RemoteDataManipulation) within the TOE using the following SFRs or appropriate:

- FDP_SDI.2 - Stored data integrity monitoring and action
  (to protect the stored aggregated and raw data from manipulation)
- FCO_NRO.2 - Enforced proof of origin
  (to prevent data injection from unauthorized entities and enable the evidence of origin of information for further entities)

287 3.3 Assumptions

288 In the following assumptions about the intended operational environment of the RWWG are stated.

Assumption	Description
A.SecureSetup	It is assumed that appropriate security measures are taken during the assembly/setup of the RWWG to guarantee for the confidentiality, authenticity and integrity of the initial cryptographic data.
A.TrustedAdministrator	It is assumed that the administrator of the RWWG (IRS operator) is trustworthy, non-hostile and well-trained.
A.PhysicalProtection	It is assumed that the RWWG is firmly mounted to the trailer, which is used in the context of road works, e.g. lane marking, construction or other lane-blocking events. Therefore, the TOE may also be left unobserved for a certain time (e.g. overnight during long-time road works) and hence the environment of the TOE cannot be assumed to

	provide a continuous and comprehensive level of physical protection. During the non-monitored phases, unauthorized physical access to the TOE cannot be completely avoided. Nevertheless, it is assumed that a theft of the TOE or an intervention that directly influences its telemetry is recognizable due to the existing communication link to the TCC. In addition, it is assumed that a visual examination at the beginning of the daily work by authorized personnel, which have to be included in the corresponding procedures, can securely ensure an identification of manipulations within a manageable timespan.
A.CorrectLocation	It is assumed that the RWWG is able to determine its correct location within a defined error bound.
A.Information	It is assumed that the information that the TOE receives from other devices and sensors on the trailer are correct and cannot be manipulated.

Table 5: Assumptions

3.4 Threats

3.4.1 Threat agents (attackers)

Compared to other embedded devices, the TOE has a very specific attack scenario that it is exposed to. Attackers can be classified after various characteristics. Basically, one can distinguish based on the **attack path**. On the one hand, the TOE is exposed to local attacks. Local attacks are directly driven against the device of the TOE, i.e. they assume physical access to the TOE. On the other hand, the TOE may be access remotely via one of its network interfaces (WLAN, GSM, WCDMA, and LTE).

Further, the attacker can be classified after the **target** that they follow. An attack can be targeted locally at the device of the TOE (i.e. it can be the target to read out confidential information) or the TOE can be misused in order to attack one of the parties that the TOE is communicating with (specifically the TCC may be of interest for an attacker).

Attackers can be:

- external individuals or organizations located outside the community of the Cooperative ITS Corridor. They may perform attacks via the Internet, mobile networks, or ITS G5 network.
- an authorized user of the Cooperative ITS Corridor.
- an employee of any actor within the Cooperative ITS Corridor.

Attackers can also be characterized by their **motivation**. One possible motivation to perform attacks can be to gain reputation. By publishing the performed attacks the person is respected as an expert e.g. for security within the ITS context. This respect could for example be used to be employed or to strengthen a position (within a company, a consortium, ...). In the motivation of the attacker lays the main limitation for the attack potential that is considered in this Protection Profile. As outlined in chapter 5.10.11.1 the analysis of all assets that are handled by the TOE showed that the value of those assets is limited. Based on the consideration of the limited value of the assets, the motivation of an attacker to attack such assets is limited. Concretely, it can be assumed that an attacker only possesses a basic attack potential.

Another motivation is vandalism. Also there could be financial reasons. A company could successfully perform attacks violating one actor in such a way that this actor will be replaced by the attacker (e.g. a vendor of RWWG). Industrial spying could be another motivation.

3.4.2 Threats

Threat	Description
T.Extraction	An attacker tries to extract secret key data from the TOE. The attack can either be performed by directly accessing interfaces of the Secure Element (IF_GW_SM) or by the use of the external

Threat	Description
	interfaces of the TOE (i.e. by observing the data that the TOE send/receives). As a specific aspect, the attacker may observe and analyse side-channel information that is leaked by the TOE. Classical examples for such side channel information include but are not limited to power consumption and light. It can be the attacker's motivation to impersonate the TOE and to send false traffic, road works or status data to the TCC or IVS afterwards.
T.LocalMalfunction	An attacker tries to induce faulty behaviour of the RWWG by applying environmental or physical stress, by injecting malformed messages to local interfaces or by manipulating internal connections of the RWWG.
T.LocalDataManipulation	An attacker tries to inject false traffic, road works or status data of his own choosing by accessing local interfaces. The injected data would then be processed by the TOE.
T.SoftwareManipulation	An attacker tries to install hostile software or firmware updates on the TOE. The attacker can try to achieve this either by directly accessing local interfaces of the TOE or by accessing remote interfaces.
T.RemoteDataManipulation	An attacker injects false traffic data by impersonating a TCC or an IVS. (This includes replayed out-dated messages.)
T.RemoteMalfunction	An attacker tries to induce faulty behaviour of the RWWG by sending malformed messages to the TOE.
T.Interception	An attacker tries to intercept traffic, road works or status data sent between the RWWG and the TCC/IRO.

Table 6: Threats

3.5 Organizational Security Policies (OSPs)

Organizations security policies (OSPs) are means to require functionality from a system that is considered in this Protection Profile even though such functionality is not directly needed to mitigate an attack against the system.

The following OSPs shall be implemented by the devices in this system.

OSP	Description
OSP.SM	The TOE shall use 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 to Protection Profiles like [CSP-PP] or comparable and shall be used only in accordance with its corresponding guidance documentation and certification report.

Table 7: Organizational security policies

Application Note: 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].

Application Note: The ST author shall consider, that the evaluation body have to examine guidance and certification report of the used secure element for an appropriate application to the TOE (e.g. in terms of used data formats, implemented interactions as well as storage and destruction of the Secure Element).

326

4 Security Objectives

4.1 Security Objectives for the TOE

In this section the security objectives for the RWWG and its environment are described.

Objective	Description
O.Crypt	The TOE shall provide cryptographic functionality as follows: • authentication, integrity protection and encryption of the communication and data to external entities using IF_GW_WAN or IF_GW_LocalIRO, • replay detection for all communications with external entities.
O.ReceiveAuthenticatedData	The RWWG shall only accept and process traffic data by the IVSs, IRO and the TCC if the corresponding messages comply to the defined message formats and if its authenticity and integrity can be verified.
O.SendAuthenticatedData	The TOE shall only send traffic, road works or status data to the TCC, IRO or the IVSs if the corresponding messages comply with the defined message formats and if it is authenticated.
O.SecureChannel	For communication with the TCC and IRO the TOE shall establish a mutually authenticated and confidential channel.
O.Protect	The TOE shall implement functionality to protect its security functions against malfunctions and tampering. Specifically, the TOE shall • overwrite relevant information that is no longer needed to ensure that it is no longer available • 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 Maintenance Personnel • ensure that the TOE fails into a secure state in case of a security relevant malfunction • write a log of security relevant events
O.Authentication	The RWWG shall provide authentication mechanisms for all roles, which are defined in Table 3.
O.Access	The TOE shall provide access control mechanisms for its functions and stored data.
O.SecureFirmwareUpdate	The TOE shall implement functionality for a secure firmware update. The TOE shall accept firmware updates only if their authenticity and integrity can be verified.
O.Management	The TOE shall provide the following management functionality to authorized administrators only:

Objective	Description
	• Start firmware update

331 **Table 8: Security Objectives for the TOE**

Application Note: Concerning O.Authentication and O.Access, the ST author shall only provide authentication and access mechanisms for those roles, which need to have access to TOE configuration items. For all other users and entities, the ST author shall prevent any kind of access.

332 4.2 Security objectives for the operational environment

Objective for environment	Description
OE.SM	The environment shall provide the services of a certified Secure Elementfor: • 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 [CSP-PP] or comparable and shall be used in accordance with its relevant guidance documentation.
OE.SecureSetup	It shall be ensured that appropriate security measures are taken during the assembly/setup of the RWWG to guarantee for the confidentiality, authenticity and integrity of the initial cryptographic data.
OE.TrustedAdministrator	It shall be ensured that the administrator of the RWWG is trustworthy, non-hostile and well-trained.
OE.PhysicalProtection	It is shall be ensured that the RWWG is firmly mounted to the trailer, which is used in the context of road works, e.g. lane marking, construction or other lane-blocking events. The TOE may also be left unobserved for a certain time (e.g. overnight during long-time road works) and hence the environment of the TOE cannot ensure to provide a continuous and comprehensive level of physical protection. During the non-monitored phases, unauthorized physical access to the TOE cannot be completely avoided. Nevertheless, it is shall be ensured that a theft of the TOE or an intervention that directly influences its telemetry is recognizable due to the existing communication link to the TCC. In addition, it shall be ensured that a visual examination at the beginning of the daily work by authorized personnel, which have to be included in the corresponding procedures, can securely ensure an identification of manipulations within a manageable timespan.
OE.CorrectLocation	It shall be ensured that the RWWG is able to determine its correct location within a defined error bound.
OE.Information	It shall be ensured that the information that the TOE receives from other devices and sensors on the trailer are correct and cannot be manipulated.

333 **Table 9: Security Objectives for the Environment**

334

4.3 Security Objectives rationale

4.3.1 Overview

Security Problem Definition \ Security Objective	Security Objectives for														
	the TOE									the Operational Environment					
	O.Crypt	O.ReceiveAuthenticatedData	O.SendAuthenticatedData	O.SecureChannel	O.Protect	O.Authentication	O.Access	O.SecureFirmwareUpdate	O.Manangement	OE.SM	OE.SecureSetup	OE.TrustedAdinistrator	OE.PhysicalProtection	OE.CorrectLocation	OE.Information
T.Extraction	X			X	X	X	X								
T.LocalMalfunction					X				X						
T.LocalDataManipulation	X	X	X		X	X	X		X						
T.SoftwareManipulation	X				X		X	X							
T.RemoteDataManipulation	X	X	X		X	X	X								
T.RemoteMalfunction	X	X	X		X	X									
T.Interception	X			X	X	X	X								
OSP.SM	X				X					X					
A.SecureSetup											X				
A.TrustedAdministrator												X			
A.PhysicalProtection													X		
A.CorrectLocation														X	
A.Information															X

Table 10: Rationale for Security Objectives

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 General objectives

The security objectives **O.Protect** counter each threat using self-tests on a regular basis, physical protection against tampering etc., whereby **O.Management** is needed as it defines the requirements around the management of the Security Functions and to document whether the TOE works as specified using adequate logging information. Additionally, **O.Authentication** on the other hand to verify the corresponding administrators. **O.SecureChannel** secures the usage of appropriate communication channels, secured by the corresponding crypto-algorithms based on **O.Crypt** (cryptographic operations). **O.ReceiveAuthenticatedData** and **O.SendAuthenticatedData** allow import and export of required data, while its integrity and authenticity is ensured by digital signatures. **O.Access** ensures that only authorized roles are able to access the TOE parts.

Those general objectives that have been argued in the previous paragraphs will not be addressed in detail in the following paragraphs.

4.3.2.2 T.Extraction

The extraction of secret data is covered by the security objectives **O.Crypt, O.SecureChannel, O.Protect, O.Authentication** and **O.Access**.

Hereby, **O.SecureChannel** secures the usage of appropriate communication channels and **O.Crypt** enforces the usage of reliable signature generation, TLS-ensured communication channels and side-channel resistant cryptographic algorithms. **O.Protect** protect the TOE's security functions against malfunctions and tampering, and **O.Authentication** and **O.Access** undertake the authentication and access procedures in a way that only the appropriate personnel may access the TOE itself and the user-corresponding functionalities.

4.3.2.3 T.LocalMalfunction

The induction of faulty behavior of the RWWG by injecting malformed messages or manipulations is covered by **O.Protect** and **O.Management**.

Hereby**, O.Protect** explicit implements the necessary functions against malfunctions and tampering by overwriting redundant data, provide self-test functionalities and prevent emitting any information that may be used to obtain secret data. Additionally, **O.Protect** ensures a corresponding log to track security relevant information. **O.Management** is hereby also necessary to start firmware updates or examine log entries for administrators only.

4.3.2.4 T.LocalDataManipulation

The injection of false traffic or network/traffic information is countered by **O.Crypt, O.Protect, O.Authentication, O.Access,** and **O.Management**.

O.Crypt generates the necessary key data and signature , which will be stored in the mandatory Secure Element. **O.Protect** implements the necessary functions against malfunctions and tampering by overwriting redundant data, providing self-test functionalities and prevention against emitting any information that may be used to obtain secret data. Additionally, **O.Protect** further ensures a corresponding log to track security relevant information. **O.ReceiveAuthenticatedData** and **O.SendAuthenticatedData** allow import and export of required data, while its integrity and authenticity is ensured by digital signatures. **O.Access** enables the necessary access control, which provides the rights to the corresponding user whereby **O.Authentication** provide authentication mechanisms. **O.Management** also supports the countermeasures against this threat by adding the functionalities to start firmware updates or examine log entries for administrators only.

4.3.2.5 T.SoftwareManipulation

The installation of hostile SW or FW updates on the TOE using (in-)direct access is countered by **O.Crypt, O.Protect, O.Access** and **O.SecureFirmwareUpdate**.

This threat is also countered by **O.Crypt, O.Protect and O.Access,** based on the same explanations like in chapter 4.3.2.4. Additionally **O.SecureFirmwareUpdate** only allows verified updates to be installed.

4.3.2.6 T.RemoteDataManipulation

The injection of false traffic data by impersonating a TCC or an IVS is countered by **O.Crypt, O.SendAuthenticatedData, O.ReceiveAuthenticatedData, O.Protect, O.Authentication** and **O.Access**.

This threat is countered by nearly the same objectives like in 4.3.2.5 (**O.Crypt, O.Protect and O.Access**) based on the same reasons and application. Additionally, **O.SendAuthenticatedData** and **O.ReceiveAuthenticatedData** ensure, in combination with **O.Authentication** that only verified messages are accepted at the RWWG.

4.3.2.7 T.RemoteMalfunction

The induction of faulty behaviour of the RWWG by sending malformed messages to the TOE is countered by **O.Crypt, O.SendAuthenticatedData, O.ReceiveAuthenticatedData and O.Protect**.

O.Protect is used to counter this threat concerning to the explanations in 4.3.2.3. Additionally, **O.Crypt** enforces the usage of reliable signature generation, TLS-ensured communication channels and side-channel resistant cryptographic algorithms. **O.SendAuthenticatedData** and **O.ReceiveAuthenticatedData** ensure, in combination with **O.Authentication** that only verified messages are accepted at the RWWG.

4.3.2.8 T.Interception

The interception of traffic, road works or status data sent between the RWWG and the TCC is countered by **O.Crypt, O.SecureChannel, O.Protect, O.Authentication** and **O.Access**.

O.Crypt enforces the usage of reliable signature generation, TLS-ensured communication channels and side-channel resistant cryptographic algorithms. In combination with **O.SecureChannel** the TOE can establish a mutually authenticated and confidential channel, whereby **O.Authentication** provides authentication mechanisms. **O.Protect** implements the necessary functions against malfunctions and tampering by overwriting redundant data, providing self-test functionalities and prevention against emitting any information that may be used to obtain secret data. Additionally, **O.Protect** further ensures a corresponding log to track security relevant information. **O.Access** enables the necessary access control which provides the rights to the corresponding users.

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.SM

The Organizational Security Policy **OSP.SM** that mandates that the TOE utilises the services of a certified Secure Element is directly addressed by the security objectives **OE.SM** and **O.Crypt**. The objective **OE.SM** addresses the functions that the Secure Element shall be utilised for as defined in **OSP.SM** and also requires a certified Secure Element according to the specified requirements in **OE.SM**. **O.Crypt** 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.

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.SecureSetup

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

4.3.4.2 A.TrustedAdministrator

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

4.3.4.3 A.PhysicalProtection

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

4.3.4.4 A.CorrectLocation

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

4.3.4.5 A.Information

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

5 Security Requirements

5.1 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 3 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 assign 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. FMT_MOF.1/Mode).

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_GEN.1	Audit data generation
FAU_GEN.2	User identity association
Class FCS: Cryptographic Operation	
FCS_COP.1/SIGVER	Cryptographic operation for signature verification
FCS_COP.1/Hash	Cryptographic operation for hash value generation
FCS_COP.1/TLS	Cryptographic operation (TLS encryption/decryption)
FCS_CKM.1/TLS	Cryptographic key generation for TLS
FCS_CKM.2/TLS	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
Class FDP: User Data Protection	
FDP_ACC.1	Subset 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.1	Subset residual information protection
Class FIA: Identification and Authentication	

FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.2	User identification before any action
Class FMT: Security Management	
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_MSA.1	Management of security attributes
Class FPT: Protection of the TSF	
FPT_FLS.1	Failure with preservation of secure
FPT_STM.1	Reliable time stamps
FPT_PHP.1	Passive detection of physical attack
FPT_TST.1	TSF testing
Class FTP: Trusted path/channels	
FTP_ITC.1:	Inter-TSF trusted channel

Table 11: List of Security Functional Requirements

486 5.2 Class FAU: Security audit

487 5.2.1 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 non-privacy relevant auditable events***].

FAU_GEN.1.2 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* ***or none***].

488 5.2.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

489 5.3 Class FCS: Cryptographic Support

490 5.3.1 FCS_COP.1/SIGVER Cryptographic operation for signature verification

FCS_COP.1.1/SIGVER The TSF shall perform [*signature verification*] in accordance with a specified cryptographic algorithm [*ECDSA NIST P256 and [assignment: cryptographic algorithm* ***or none****]*] and cryptographic key sizes [*256 bit and [assignment: cryptographic key sizes* ***or none****]*] that meet the following: [*ETSI TS 103 097*] or [assignment: *list of standards* ***or none***].

Application Note: The signature generation will always be performed by the built in Secure Element while signature verification of received IVS transmissions may also be performed by a software implementation.

491 5.3.2 FCS_COP.1/Hash Cryptographic operation for hash value generation

FCS_COP.1.1/HASH The TSF shall perform [*cryptographic hashing*] in accordance with a specified cryptographic algorithm [*SHA-256, SHA-384, SHA-512*] and cryptographic key sizes [*256-bit, 384-bit, 512-bit*] that meet the following: [*ETSI TS 103 097 and FIPS Pub 180-4*].

492 5.3.3 FCS_COP.1/TLS Cryptographic operation (TLS encryption/decryption)

FCS_COP.1.1/TLS The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*cryptographic algorithms as identified in chapter 5.3.7*] and cryptographic key sizes [*key sizes as identified in chapter 5.3.7*] that meet the following: [*standards as listed in chapter 5.3.7*].

493 5.3.4 FCS_CKM.1/TLS Cryptographic key generation for TLS

FCS_CKM.1.1/TLS The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*algorithms for key generation as listed in chapter 5.3.7*] and specified cryptographic key sizes [*key sizes as listed in chapter 5.3.7*] that meet the following: [*standards as listed in chapter 5.3.7*].

Application Note: The Secure Element is used for parts of the TLS key negotiation.

5.3.5 FCS_CKM.2/TLS Cryptographic key distribution for TLS

FCS_CKM.2.1/TLS The TSF shall distribute cryptographic key in accordance with a specified cryptographic key distribution method [*see Table 12*] that meets the following: [*see Table 12*].

Operation/Purpose	Algorithms / Cipher Suite	Standard
Key Agreement	Ephemeral elliptic curve DH key exchange supports the P-256 and the P-384 curves	FIPS186-4

Table 12: Cryptographic Key Exchange

5.3.6 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*].

Application Note: Please note that as against the requirement FDP_RIP.1 the mechanisms implementing the requirement from FCS_CKM.4 shall be suitable to avoid attackers with physical access to the TOE from accessing the keys after they are no longer used.

5.3.7 TLS – cryptographic requirements at a glance

The TOE implements a TLS channel that is modelled in a variety of SFRs. In this context the TOE shall implement the following cipher suites as recommended by [TR2102-2]:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA384
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Further, the following requirements shall be followed by the TOE:

- The TLS connection as required by FTP_ITC.1 shall be based on TLS v1.2 [RFC5246] or newer.
- The TOE shall be technically prevented from establishing a TLS connection with another external entity using TLS v1.0 [RFC2246], TLS v1.1 [RFC4346] or SSL.
- Session renegotiation shall only take place on the basis of [RFC5746].

5.3.8 Firmware update at a glance

The TOE performs a secure firmware update, which requires the TOE to implement the following:

- Verify firmware update signature to ensure authenticity and integrity prior to installation (acc. FCS_COP.1/SIGVER),
- IRO authentication is required to upload the firmware update data (acc. FIA_UAU.2 and FIA_UID.2),
- Automatic firmware update is not allowed.

The term firmware update applies to any security relevant software update in the TOE.

531 5.4 Class FDP: User data protection

532 5.4.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [*RWWG access policy*] on [

- *Subjects: external entities using any TSFI*
- *Objects: any information that is sent to, from or via the TOE and any information that is stored in the TOE]*
- *Operations: all operations among subjects and objects covered by the SFP*

].

533 5.4.2 FDP_ACF.1 Security attribute based access control

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

subjects: external entities using any TSFI

objects: any information or data that is sent to, from or via the TOE

attributes: destination interface and [assignment: further SFP-relevant security attributes ***or none****]*].

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

- *an authorized IRO is allowed to have access via wide-area communication or local interfaces, but is not allowed to read, modify or write stored and/or processed assets within the TOE, except status, logging and update information*
- *only an authorized IRO is allowed to start the firmware update process.*
- *an authorized TCC is only allowed to interact with the TOE via a WAN interface*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes that explicitly authorise access of subjects to objects*].

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

- *private cryptographic keys must never be readable,*
- *TCC is not allowed to read logging information,*
- *[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]*].

Application Note: Please note, that the PP is based on the assumption, that only static attributes will be defined in FDP_ACF.1. If an ST author include any dynamic ones, the author also shall model corresponding management functionalities and rules within FMT_MSA.3 and adapt the SFR dependencies table (Table 15).

534

535 5.4.3 **FDP_IFC.2 Complete information flow control**

FDP_IFC.2.1 The TSF shall enforce the [*RWWG IFP*] on [

- *Subjects: TOE, TCC, IVS, PKI, Modules on road works trailor [assignment: other or none]*
- *Information: messages*
- *Operation: send, receive*

] 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.

536 5.4.4 **FDP_IFF.1 Simple security attributes**

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

- *Subjects: TOE, TCC, IVS, IRO, PKI, Modules on road works trailer [assignment: other or none]*
- *Information: messages and their signature*
- *Attributes: destination_interface (TOE, TCC, IVS, PKI, Modules of the road works trailer or IRO), source_interface (TOE, TCC, IVS, PKI, Modules of the road works trailer or IRO), 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: [

- *an information flow shall only be possible if allowed by a corresponding communication profile within the TOE*].

537

FDP_IFF.1.3 The TSF shall enforce the [*following rules:*

- *Connection establishment is only allowed between the introduced destination_interfaces and source_interfaces.*
- *Connection establishment is especially denied in the following cases:*
  - *(Source_interface = IRO or source_interface=TCC) and destination_interface = IVS*
  - *Source_interface = IVS and (destination_interface= IRO or destination_interface=TCC)*
  - *Source_interface = IRO and destination_interface=TCC*
  - *Source_interface= TCC and destination_interface=IRO*
  - *Source_interface= PKI and destination_interface=TOE*
  - *Source_interface=TOE and destination_interface=Modules of the road works trailer*
- *All messages sent to TCC, all IRO roles and the PKI must only be sent via an encrypted TLS channel and must be signed prior to sending*
- *The signature of every message received by source_interface = TCC, or source_interface=IVS, or source_interface=IRO and source_interface=Modules of the road works trailer must be verified*
  - *If the signature is found to be invalid, the message must be dropped*
  - *Only messages with a valid signature may be processed*
- *Received messages from source_interface = IVS that do not fulfill the standard of CAM or DENM [assignment: other standards or none] shall be dropped*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

Application Note: Please note, that the PP is based on the assumption, that only static firewall rules will be defined in FDP_IFF.1. If an ST author include any dynamic ones, the author also shall model corresponding management functionalities and rules within FMT_MSA.3 and adapt the SFR dependencies table (Table 15).

538 ### 5.4.5 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [*cryptographic keys (and session keys), all received messages, all sent messages, aggregated information, [assignment: other objects or none]*].

539 ## 5.5 Class FIA: Identification and authentication

540 ### 5.5.1 FIA_ATD.1 User attribute definition

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

- *User identity*

- *Connecting network*
- *Role membership*
- *[assignment: list of security attributes]*].

541

542 5.5.2 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.

543 5.5.3 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [

- *TLS-authentication via certificates at the WAN interface to IROs and TCCs*
- *[assignment: list of multiple authentication mechanisms]*

] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [

- *IROs shall be authenticated via TLS-certificates at IF_GW_WAN or IF_GW_LocalIRO only*
- *TCCs shall be authenticated via TLS-certificates at IF_GW_WAN interface only*
- *IVS shall be authenticated via certificates at IG_GW_IVS only*
- *[assignment: rules describing how the multiple authentication mechanisms provide authentication]*].

Application Note: The ST author is reminded that the assignment in FIA_UAU.5 shall cover the authentication mechanisms for the TLS connection as well as the authentication mechanisms for local maintenance.

544

545 5.5.4 FIA_UID.2 User identification before any action

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

546 5.6 Class FMT: Security Management

547 5.6.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*RWWG access policy*] to restrict the ability to [modify, delete, [assignment: *other operations*]] the security attributes [*all relevant security attributes*] to [*authorised identified roles*].

548 5.6.2 **FMT_SMF.1 Specification of Management Functions**

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- *Firmware Update*
- *[assignment: list of additional management functions to be provided by the TSF or none]*].

549 5.6.3 **FMT_SMR.1 Security roles**

FMT_SMR.1.1 The TSF shall maintain the roles [

- *IRO,*
- *TCC,*
- *IVS, and*
- *[assignment: additional roles or none]*].

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

550 5.7 Class FPT: Protection of the TSF

551 5.7.1 **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: [

- *the deviation between local system time of the TOE and the reliable external time source is too large,*
- *[assignment: other of types of failures in the TSF]*].

552 5.7.2 **FPT_STM.1 Reliable time stamps**

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

Application Note: The time stamps as defined by FPT_STM.1 shall be of sufficient exactness.

Therefore, the local system time of the TOE is synchronised regularly with a reliable external time source. However, the local clock also needs a sufficient exactness as the synchronisation will fail if the deviation is too large (the TOE will preserve a secure state according to FPT_FLS.1).

Therefore the local clock shall be as exact as required by [RFC5246].

553 5.7.3 **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 or TSF's elements has occurred.

554 5.7.4 **FPT_TST.1 TSF testing**

FPT_TST.1.1 The TSF shall run a suite of self tests [during initial start-up, periodically during normal operation, at the request of the authorised user] to demonstrate the correct operation of [the TSF].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [TSF data].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [TSF].

555 5.8 Class FTP: Trusted path/channels

556 5.8.1 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 **using the following mechanisms**:

- **a) Cryptographically-protected communication channel between the TOE and all IRO and TCC partners 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/Hash**

  as defined in [RFS5246].
- **b) Authenticated communication channel using TLS as defined in [RFC5246] for server authentication.**
- **c) Authenticated communication channel using a password authentication scheme as defined in FIA_UAU.2.**

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*all security functions specified in the ST that interact with remote trusted IT systems and no other conditions or functions*].

557 5.9 Security Assurance Requirements for the TOE

558 The minimum Evaluation Assurance Level for this Protection Profile is **EAL 3.**

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

560

Assurance Class	Assurance Component
Development	ADV_ARC.1
	ADV_FSP.3
	ADV_TDS.2
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.3
	ALC_CMS.3

Assurance Class	Assurance Component
	ALC_DEL.1
	ALC_DVS.1
	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.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	AVA_VAN.2

Table 13: Assurance Requirements

5.10 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.Crypt	**O.ReceiveAuthentificatedData**	**O.SendAuthenticatedData**	**O.SecureChannel**	**O.Protect**	**O.Authentication**	**O.Access**	**O.SecureFirmwareUpdate**	**O.Management**
FAU_GEN.1					X				
FAU_GEN.2					X				
FCS_COP.1/SIGVER	X	X			X			X	

	O.Crypt	O.ReceiveAuthentificatedData	O.SendAuthenticatedData	O.SecureChannel	O.Protect	O.Authentication	O.Access	O.SecureFirmwareUpdate	O.Management
FCS_COP.1/HASH	X					X			
FCS_COP.1/TLS	X			X					
FCS_CKM.1/TLS	X			X					
FCS_CKM.2/TLS	X			X					
FCS_CKM.4	X								
FDP_ACC.1							X		
FDP_ACF.1							X		
FDP_IFC.2		X	X	X					
FDP_IFF.1		X	X						
FDP_RIP.1					X				
FIA_ATD.1						X	X		X
FIA_UAU.2						X			X
FIA_UAU.5						X			X
FIA_UID.2						X	X		X
FMT_SMF.1									X
FMT_SMR.1									X
FMT_MSA.1									X
FPT_FLS.1					X				
FPT_STM.1					X				

	O.Crypt	O.ReceiveAuthentificatedData	O.SendAuthenticatedData	O.SecureChannel	O.Protect	O.Authentication	O.Access	O.SecureFirmwareUpdate	O.Management
FPT_PHP.1					X				
FPT_TST.1					X				
FTP_ITC.1				X					

Table 14: Security Requiremtens Rationale

The following paragraphs contain more details on this mapping.

5.10.1 O.ReceiveAuthenticatedData

O.ReceiveAuthenticatedData is met by the following SFR:

- **FDP_IFC.2** which defines the complete information flow control
- **FDP_IFF.1** defines the corresponding security attributes
- **FCS_COP.1/SIGVER** verifies incoming data

5.10.2 O.SendAuthenticatedData

O.SendAuthenticatedData is met by the following SFR:

- **FDP_IFC.2** which defines the complete information flow control.
- **FDP_IFF.1** defines the corresponding security attributes.

5.10.3 O.SecureChannel

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

- **FCS_COP.1/TLS** defines the cryptographic operations for the TLS channel.
- **FCS_CKM.1/TLS** defines the cryptographic key generation for the TLS connection.
- **FCS_ITC.1** defines the inter-TSF trusted channel itself.
- **FDP_IFC.2** defines the information flow control within the given architecture.

5.10.4 O.Authentication

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

- **FIA_ATD.1** defines the security attributes for all users.
- **FIA_UAU.2** defines requirements around the authentication of users.
- **FIA_UID.2** defines requirements around the identification of users.

5.10.5 O.Access

O.Access is met by a combination of:

- **FDP_ACC.2** and **FDP_ACF.1**, which define the required access control policy.
- **FIA_ATD.1** defines the security attributes for all users.

5.10.6 O.SecureFirmwareUpdate

- O.SecureFirmwareUpdate is met by a combination of the following SFRs: **FCS_COP.1/SIGVER** verifies the firmware update signature to ensure authenticity and integrity prior to installation.
- **FIA_UAU.2** and **FIA_UAU.5** addresses to valid authentication of a responsible administrator

5.10.7 O.Protect

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

- **FDP_RIP.1** defines that the TOE shall make information unavailable as soon as it is no longer needed.
- **FPT_FLS.1** ensures that the TOE fails into a secure state in case of a security relevant malfunction
- **FPT_TST.1** defines the self testing functionality.
- **FPT_PHP.1** defines the requirements around the physical protection that the TOE has to provide.
- **FAU_GEN.1** defines the necessary audit data generation
- **FAU_GEN.2** defines the corresponding user identity association

5.10.8 O.Management

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

- **FIA_ATD.1** defines how authorised administrator might be able to define additional security attributes for users.
- **FIA_UAU.2** defines requirements around the authentication of users.
- **FIA_UID.2** defines requirements around the identification of users.
- **FMT_MSA.1** defines the management of the security attributes.
- **FMT_SMF.1** defines the management functionalities that the TOE must offer.
- **FMT_SMR.1** defines the role concept for the TOE.

5.10.9 O.Crypt

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

- **FCS_CKM.4** defines the requirements around the secure deletion of ephemeral cryptographic keys.
- **FCS_CKM.1/TLS** defines the requirements on key negotiation for the TLS protocol.
- **FCS_COP.1/TLS** defines the requirements around the encryption and decryption capabilities of the Gateway for communications with external parties in the WAN and (if not implemented in one physical device) to Meters.
- **FCS_COP.1/SIGVER** defines the requirements around the encryption and decryption of signatures.

- **FCS_CKM.2/TLS** defines the allowed key distribution mechanisms.
- **FCS_COP.1/HASH** defines the requirements for the hash operations.

5.10.10 **Fulfilment of the dependencies**

The following table summarises all TOE functional requirements dependencies of this PP and demonstrates that they are fulfilled.

SFR	Dependencies	Fulfilled by
FAU_GEN.1	FPT_STM.1 Reliable Time Stamps	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FAU_GEN.1 FIA_UID.2
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/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	1st dependency need to be fulfilled within the production or installation phase of the TOE, during the implementation of the corresponding key value. FCS_CKM.4
FCS_COP.1/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	1st dependency need to be fulfilled within the production or installation phase of the TOE, during the implementation of the corresponding key value. FCS_CKM.4

SFR	Dependencies	Fulfilled by
FCS_CKM.1/TLS	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.2/TLS FCS_CKM.4
FCS_CKM.2/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_CKM.4	[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/TLS Cryptographic key generation]	FCS_CKM.1/TLS
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3 does not have to be fulfilled here because all the defined in ACF attributes are static and unchangeable. If an ST author include any dynamic attributes, the author also has to model FMT_MSA.3 (see application note in FDP_ACF.1)
FDP_IFC.2	FDP_IFF.1 Simple security attributes	FDP_IFF.1

SFR	Dependencies	Fulfilled by
FDP_IFF.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.2 FMT_MSA.3 does not have to be fulfilled here, because all in IFF defined attributes are static and unchangeable. If an ST author include any dynamic rules, the author also has to model FMT_MSA.3 (see application note in FDP_IFF.1)
FDP_RIP.1	-	
FIA_ATD.1	-	
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2 User identification before any action
FIA_UAU.5	-	
FIA_UID.2	-	
FMT_SMF.1	-	
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
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.1 FMT_SMR.1 FMT_SMF.1
FPT_FLS.1	-	
FPT_STM.1	-	
FPT_PHP.1	-	
FPT_TST.1	-	
FTP_ITC.1	-	

642 **Table 15: SFR dependencies**

643

5.10.11 **Security Assurance Requirements rationale**

5.10.11.1 Justification for selection of assurance level

The main decision about the assurance level has been taken based on the assumed attackers that exist against the TOE. Many discussions and a structured threat model have shown that one can act on the assumption that the potential of the assumed attackers is only of basic potential. This lead to the selection of the component AVA_VAN.2 for vulnerability assessment. This component is contained in two evaluation assurance levels, namely EAL 2 and EAL 3.

As the discussions around the threat model further lead to the fact that the security of the development environment and of the development processes is an important aspect for the security of the TOE, it has been decided to use EAL 3 as the assurance level in this Protection Profile.

5.10.11.2 Dependencies of assurance components

The dependencies of the assurance requirements taken from EAL 3 are fulfilled automatically.

6 Appendix

6.1 Glossary

CA	Certificate Authority or Certification Authority, an entity that issues digital certificates.
EAL	Evaluation Assurance Level
LAN	Local Area Network
Personally Identifiable Information (PII)	Personally Identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
TSF	Transport Layer Security protocol according to RFC5246
TOE	Target of Evaluation - set of software, firmware and/or hardware possibly accompanied by guidance
WAN	Wide Area Network

6.2 References

[AIS20] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 2013-05-15, Herausgeber: Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas, Bundesamt für Sicherheit in der Informationstechnik.

[AIS31] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik.

[CC] Common Criteria for Information Technology Security Evaluation –

- Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5
- Part 2: Security functional requirements, dated April 2017, version 3.1, Revision 5
- Part 3: Security assurance requirements, dated April 2017, version 3.1, Revision 5

[DENM] ETSI EN 302 637-3 V1.2.2 (2013-08): Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service

[CAM] ETSI EN 302 637-2 V1.3.2 (2013-08): Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service

[TR2102-1] Technische Richtlinie TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2018-012 29. Mai 2018

[TR2102-2] Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), (Version 2019-01)

[TR3111] Technical Guideline TR-03111, Elliptic Curve Cryptography, Version 2.10, 01.06.2018

[SiKo_RWWG] Informationssicherheitskonzept C-ITS Corridor, Version 1.2, March 2018

[ETSI TS 103 097] Security Header & Certificates ETSI TS 103 097, Version 1.3.1, October 2017

[RFC5246] RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2, August 2008

[RFC2246] RFC 2246, The TLS Protocol, January 1999

[ETSI TS 102 941] Intelligent Transport Systems (ITS); Security; Trust and Privacy Management, version 1.2.1, May 2018

[C-ITS-Policy] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transportation Systems (C-ITS), release 1.1, June 2018

661