Österreichisches Förderungsprogramm für Sicherheitsforschung
Gefördert durch das Bundesministerium für Verkehr, Innovation und Technologie

Kooperatives FuE-Projekt EVE
Effiziente Bevorrangung von Einsatzfahrzeugen im automatisierten Straßenverkehr

D5.3

Generalized Protection Profile for a Roadside ITS Station Gateway, Version 1.0

based on BSI-CC-PP-0106

Dokumentinformation	
Titel	Generalized Protection Profile for a Roadside ITS Station Gateway based on BSI-CC-PP-0106
Version	1.0
Autoren	Stefan Ruehrup, Stefan.Ruehrup@asfinag.at Arndt Bonitz, Arndt.Bonitz@ait.ac.at Christoph Schmittner, Christoph.Schmittner@ait.ac.at
Beschreibung	Das vorliegende Dokument enthält Vorschläge für ein generalisiertes Schutzprofil für C-ITS-Straßeneinheiten (Roadside ITS Stations). Es basiert auf einem zertifizierten Schutzprofil für ein Gateway auf Baustellen-Warnanhängern, das unter der Zertifizierungsnummer „BSI-CC-PP-0106“ veröffentlicht wurde: https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0106.html Die vorgeschlagenen Änderungen bzgl. BSI-CC-PP-0106 stammen nicht von den ursprünglichen Autoren von BSI-CC-PP-0106. Die Änderungen wurden nicht zertifiziert. Das vorliegende Dokument dient nur zur Information. Es ist kein zertifiziertes Schutzprofil. Es erhebt keinen Anspruch auf Korrektheit oder Vollständigkeit.
Klassifizierung	Öffentlich

Document Information	
Titel	Generalized Protection Profile for a Roadside ITS Station Gateway based on BSI-CC-PP-0106
Version	1.0
Authors	Stefan Ruehrup, Stefan.Ruehrup@asfinag.at Arndt Bonitz, Arndt.Bonitz@ait.ac.at Christoph Schmittner, Christoph.Schmittner@ait.ac.at
Beschreibung	The present document contains proposals for a generalised protection profile for Roadside ITS Stations. It is based on a certified protection profile for a road works warning gateway that has been published unter certification ID „BSI-CC-PP-0106“: https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0106.html The proposed changes to BSI-CC-PP-0106 have not been made by the original authors of BSI-CC-PP-0106. The changes have not been certifed. The present document is for information purposes only. It is not a certified protectioni profile. There is no guarantee of correctness or completeness.
Classification	Public

1 INTRODUCTION

The security of C-ITS stations is an important aspect for a system that is used for applications related to road safety and traffic efficiency. C-ITS is an overall system that is characterised by decentral components. Consequently, there need to be common requirements for the security of its components, especially the roadside C-ITS stations (aka. roadside units) and vehicle C-ITS stations (aka. on-board units) which implement the air interface for direct communication between road infrastructure and vehicles as well as among vehicles. The EU C-ITS Security Policy refers to an assessment and certification according to Common Criteria (CC), an international standard for security evaluation (ISO/IEC 15408). Common Criteria define a generic framework to specify security requirements for information technology systems. The domain specific requirements can be described by a Protection Profile (PP), which is an implementation-independent specification that describes threats, security objectives, and security functional requirements for a class of systems, such as C-ITS stations. C-ITS stations have many commonalities when it comes to interfaces and message exchange, however, the implementation environment for roadside C-ITS stations and vehicle C-ITS stations differ. Thus, two different paths were taken to define separate protection profiles for C-ITS stations in vehicles and roadside infrastructure. At the time of writing this deliverable, there is only one certified protection profile available for roadside C-ITS stations, and this profile is tailored to the environment of a roadworks warning trailer. Thus, this valuable existing work was taken within the project EVE to derive a generalised protection profile that is suitable for general roadside C-ITS stations in that can be operated on motorway gantries, on signalled intersections, and not only on road works warning trailers.

The present document contains proposals for such a generalised protection profile, and presented as a “delta” to the existing protection profile for a road works warning gateway that has been published unter certification ID „BSI-CC-PP-0106“.

GUIDANCE TO THE READER

Changes are introduced by stating the line numbers given in BSI-CC-PP-0106 Version 1.1. The original text is stated in black color, the changed or newly introduced text in blue color. Deletions are omitted for better readability, and sometimes indicated by “_”.

Comments on the editing are given inline in italics, e.g. *[item deleted]*. Comments on the PP, which are not directly part of the proposed changes are placed in boxes:

COMMENT: …

2 PROPOSED CHANGES

LINE 113-114 (1.1 INTRODUCTION)

The Roadside ITS Station (R-ITS-S) is an electronic device and part of an Intelligent Transport System (ITS). It exhanges ITS messages with other ITS Stations in the context of Infrastructure to Vehicle (I2V) and Vehicle to Infrastructure (V2I) communication. The data exchange includes events, warnings, regulation and informations related to road traffic. Communication from the Roadside ITS Station to vehicle ITS Stations can be regarded as a digital equivalent to physical road signs and physical light signals.

LINE 117 (TABLE 1: SPECIFIC TERMS)

Original Term	New Term	Description
CAM	(no change)	(no change)
-	CRL	Certificate Revocation List
-	CTL	Certificate Trust List
DENM	(no change)	(no change)
GNSS	(no change)	(no change)
ICS	C-ITS-S	Central ITS Station

Original Term	New Term	Description
		Fixed control station with network connection to R-ITS-S, potentially connecting to further (backend) systems.
IRO	RO	Roadside ITS Station Operator Administrator of R-ITS-S.
IRS	RSU	Roadside Unit ITS computing platform, including communication and processing capacity, linked to road infrastructure.
ITS	(no change)	(no change)
-	IVIM	In Vehicle Information Message
IVS	V-ITS-S	Vehicle ITS Station Mobile platform transmitting CAMs and DENMs in ITS scenarios (e.g. vehicles)
PKI	(no change)	(no change)
RWWG	RGW	Roadside ITS Station Gateway
RWWU	(replaced)	(replaced by R-ITS-S)
-	RTC	Real Time Clock
-	TCC	Traffic Control Centre
-	TLS	Transport Layer Security

Table 1: Specific terms

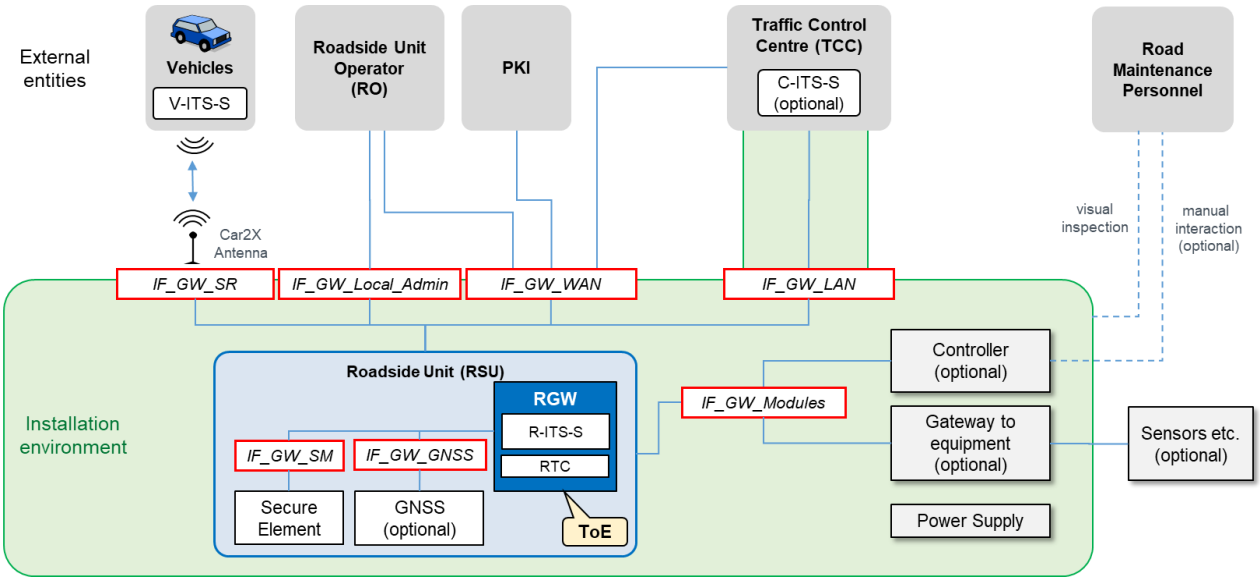
LINE 122-128

The Target of Evaluation (TOE) described in this Protection Profile is a Roadside ITS Station Gateway (RGW) as a part of the corresponding Roaside ITS Station (R-ITS-S), which is an electronic device, mounted, e.g., at light signals, overhead gantries, or on trailers that warn approaching traffic that road works is carried out.

LINE 129-134

The TOE itself is the electronic module, which is able to transmit ITS messages and also to collect ITS messages sent by bypassing vehicles.

LINE 141 (FIGURE 1: TOE AND ITS ENVIRONMENT)



COMMENT: The target of evaluation (ToE) is the Roadside ITS Station gateway. It contains the necessary parts of the protocol stack of a Roadside ITS Station (R-ITS-S) for communication with other ITS stations, therefore it is termed “gateway”. A gateway does not need to contain application logic. The term “Roadside Unit” describes the physical entity that hosts also the secure element and the (optional) GNSS receiver, which are not part of the PP.

LINE 144-147

The TOE is an electronic device that is able to receive ITS messages sent by other ITS stations (e.g. vehicles passing by) using wireless access in vehicular environments (IEEE 802.11p). It is also able to send ITS messages (e.g. road works warning, in-vehicle-information, signal phase and timing etc.) to other ITS stations.

LINE 155-164

1.4.4.1 Local Traffic Information

C-ITS Infrastructure-to-Vehicle services are 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. This information needs to be on time. To realize this objective, the R-ITS-S broadcasts appropriate information towards the vehicles approaching the R-ITS-S location, using ITS messages such as Decentralised Environmental Notification Messages ([DENM]), IVIM, SPATEM, MAPEM, SSEM etc.

When the R-ITS-S is used in combination with a road works trailer, variable message signs or traffic lights, the services of the RGW will be a service on top of the basic functionality of the physical infrastructure. This means that even in the case when the RGW is shortly not functioning due to breakdown or maintenance, the physical infrastructure element (trailer, VMS, traffic light) must remain available.

LINE 165-170

1.4.3.2 Local Traffic Surveillance and other V2I services

This service receives ITS messages being broadcasted by the vehicles (e.g. DENM and CAM _ [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.

LINE 179-186 (TOE PHYSICAL SCOPE)

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

- Communication segment(s), at least one mandatory:
  - Network interface (e.g. Ethernet)
  - Mobile cellular communication (e.g. GSM, UMTS, LTE)
- Car-2-X communication, mandatory
  - IEEE 802.11p
- Positioning technology, optional
  - _GNSS receiver

Note 1: Please note that the Secure Element is physically integrated into the RSU even though it is not part of the TOE.

LINE 203

- Ensure authenticity of information content received from or send to involved TOE Security Functions Interfaces (TSFIs).

LINE 211

- TLS communication to RSU or TCC after receiving decrypted session key from Secure Element

LINE 218 (TABLE 2: MANDATORY TOE EXTERNAL INTERFACES)

Interface Name	Description
IF_GW_WAN	Via this interface, the RGW has to establish all wide area communication connections, e.g. for interaction with a remote RO with the PKI respectively or for transmitting or receiving data from/to the TCC.
IF_GW_SR	This interface is responsible for every short range communication from gateway to other ITS stations, usually in vehicles. This includes the reception of ITS messages such as DENMs or CAMs from the V-ITS-S, the potential warning of all V-ITS-S in the direct surrounding if necessary, or a locally connected RO.
IF_GW_Local_Admin	This interface is used for local _ROs 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 RGW position.
IF_GW_SM	The interface connects the TOE with the Secure Element.
IF_GW_Modules	Via this interface, further functional modules in the installation environment of the RSU are connected. Such modules could be a traffic light controller, or a roadworks trailer controller, or a gateway that serves the connection to external equipment (analog-to-digital conversion of sensor inputs, etc.)

LINE 221

The RSU contains a Secure Element, […]

LINE 223-226

The Secure Element is a different sub-module of the RSU, for which a separate PP exists (e.g. [CSP-PP] or comparable; it is therefore not part of the TOE as described in this PP. Nevertheless, it is physically embedded into the RSU and protected by the same level of physical protection.

LINE 252

- Storage of (cryptographic) keys,

LINE 260-236

The main application of the RGW 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 V-ITS-Ss arrive at the RGW, 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 any private key.

LINE 237-250

1.6 Life cycle

The Life Cycle of the TOE_ consist of the following consecutive phases_:

1. **Design/Development**
   The development of the TOE itself.
2. **Manufacturing/Assembly**
   The production itself like hardware assembly, or software installation. This includes the initial ITS-S configuration during manufacture.
3. **Enrolment**

Enrolment of the ITS-S at a PKI.

4. **Initial Authorization**
   Initial transfer of certificates from the PKI to the TOE.
5. **Normal Operation and Maintenance**
   Operational phase of the TOE. All security functions shall be working as specified.
6. **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 and certificate material that is contained in the TOE is destroyed in a secure manner as described in the guidance documentation of the mandatory Secure Element.

–

The lifecycle is usually a sequential process, however, a re-enrolment at a different PKI is possible. In this case, normal operation ends and can only be resumed only start after successful enrolment and authorization.

An overview of the ITS-S security lifecycle is included in ETSI TS 102 941.

Application Note:	It is recommended to embed the use of the TOE in an Information Security Management System (ISMS) according to ISO 270001
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.

LINE 267

[…] the work of the developer of the RGW refers to the integration of those components

LINE 272

- the **external entities** that are envisoned to interact with the TOE,

LINE 280 (TABLE 3: EXTERNAL ENTITIES)

Role	Description
Roadside Unit Operator (RO)	The roadside unit operator is responsible for initial setup of the RGW, installing key and certificate material, firmware updates, and for the continued operation including the potential data connection to the TCC.
Traffic Control Center (TCC)	The traffic control center sends and receives traffic data to/from the RGW, directly or via C-ITS-S.
Vehicles (V-ITS-S)	Vehicles are sending and receiving traffic/road works data to/from the RGW.
–	–
Road Maintenance Personnel	The Road Maintenance Personnel are maintaining the road infrastructure and are responsible for visual inspection of road infrastructure elements. Such personnel are not maintaining the RGW and therefore not accessing maintenance interfaces of the TOE.
PKI	The public key infrastructure issuing certificates to the RGW required for signing and verifying ITS messages exchanged between the RGW and V-ITS-S.

LINE 285 (TABLE 4: ASSETS)

Primary Assets	In(coming)/	Source/	Protection	Comment

	Out(going)	Destination	Requirements	
Input from local controller	In	Local controller		Optional, only for TOE with connected local controller, such as a trailer controller that offers manual switching of the trailer sign board. Correctness of data has to be assumed.
Status information from external equipment (e.g. external sensors or status of a variable message sign)	In & Out	Various external equipment	-	Optional, only if gateway to equipment is used. Correctness of incoming data has to be assumed. Outgoing status information is out of evaluation scope
~~CAM~~	–	–	–	–
~~DENM~~	–	–	–	–
ITS message reception	In	Other ITS-S to TOE	Integrity, Authenticity	TOE verifies signature.
ITS message transmission	Out	TOE to other ITS-S	Integrity, Authenticity	TOE creates and signs ITS message. In case of message forwarding, the verified message is re-transmitted without creating a new signature.
Payload of ITS message	Out	TOE to TCC	Integrity, Authenticity	This applies if the TOE forwards parts of an ITS message to TCC without the original signature. The signature of the ITS message has been verified by the TOE upon reception. Payload does not need to be signed, if TOE communicates to TCC via a trusted channel.
Information from TCC	In	TCC to TOE	Integrity, Authenticity	Correctness of incoming data has to be assumed. Out of evaluation scope
RO data	In & Out	RO	Integrity, Authenticity,	Incoming: TOE verifies integrity

			Authentication	and authenticity; Outgoing: Admin data for RO, e.g. acknowledgements, logs, etc.
Firmware Update	In	RO	Integrity, Authenticity, Authentication	TOE verifies integrity and authenticity
Certificate Update	In & Out	TOE requests, PKI responds	Integrity, Authenticity	TOE requests a certificate from the PKI
Update of Trust Lists, Revocation Lists	In & Out, Out	TOE requests from PKI, TOE broadcasts to other ITS-S	Integrity, Authenticity	The TOE requests an update of the CTL and CRL from the PKI
Secondary Assets	**Description**		**Protection Requirements**	**Comment**
Cryptographic keys	[…]		[…]	[…]

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

[…]

COMMENTS: Regarding Payload of ITS messages: In order to fulfil Authenticity for outgoing information, the TOE does not need to trust the TCC, but the TCC needs to trust the TOE.

Regarding the Update of Trust Lists: Revocation Lists: Secure CTL and CRL updates are defined in ETSI TS 102 941.

LINE 288 (TABLE 5: ASSUMPTIONS)

Assumption	Description
A.SecureSetup	It is assumed that appropriate security measures are taken during the assembly/setup of the RGW to guarantee for the confidentiality, authenticity and integrity of the initial cryptographic data.
A.TrustedAdministrator	It is assumed that the _ RO is trustworthy, non-hostile and well-trained.
A.PhysicalProtection	It is assumed that the RGW is physically protected, or at least that manipulations can be identified within a manageable timespan. Option 1: The RSU is firmly mounted and not easily accessible. Option 2: The RSU is mounted on a movable platform (e.g. road works trailer). It 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 either on-site or by remote monitoring in the TCC. In addition, it is assumed that a visual examination_ 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 RGW is able to determine its correct location within a defined error bound. Option 1: The position can be determined externally with a suitable GNSS equipment and configured in the TOE via the maintenance interface. This applies only to fixed installation locations. Option 2: The position is determined by a GNSS receiver. This applies to fixed and mobile installations.
A.Information	It is assumed that the information that the TOE receives from other devices and sensors (via IF_GW_Modules) are correct and protected against manipulation.

LINE 292-316 (3.4.1 THREAT AGENTS (ATTACKERS))

Threat agents can be classified according to various characteristics.

Attack paths can be:

- 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.
- The TOE may be accessed remotely via one of its network interfaces (mobile cellular networks and other wireless networks).

A threat agent can be classified after the **target**_. An attack can be targeted at 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:

- _individuals or organizations _outside of the listed external entities (3.1). They may perform attacks via the Internet, mobile networks, or ITS G5 network,
- an authorized user of listed external entities,
- an employee of listed external entities.

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. _
- Another motivation is vandalism.
- Also there could be financial reasons. An attacker could manipulate the functionality for ransom. _
- Industrial espionage could be another motivation.

[*moved from Line 309*:] In the motivation of the attacker lays the main limitation for the attack potential that is considered in this Protection Profile. As outlined in section 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.

LINE 317 (TABLE 6: THREATS)

Threat	Description
T.Extraction	An attacker tries to extract key material from the TOE. […] […] As an example, the attack could aim at impersonating the TOE and to send false traffic status data to the TCC or false road works warnings to V-ITS-S afterwards.
T.LocalMalfunction	An attacker tries to induce faulty behaviour of the RGW by applying environmental or physical stress, by injecting malformed messages to local interfaces or by manipulating internal connections of the RGW.

Threat	Description
T.LocalDataManipulation	An attacker tries to inject false traffic_ or status data of his own choice by accessing local interfaces. The injected data would then be processed by the TOE.
T.SoftwareManipulation	[…]
T.RemoteDataManipulation	An attacker injects false traffic data by impersonating a TCC or a V-ITS-S. (This includes replayed out-dated messages.) Data could also be injected after accessing the remote maintenance interface.
T.RemoteMalfunction	An attacker tries to induce faulty behaviour of the RGW by sending malformed messages to the TOE.
T.Interception	An attacker tries to intercept traffic data (incl. content of ITS messages) or status data sent between the RGW and the TCC/RO.

LINE 329

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

LINE 330 (TABLE 8: SECURITY OBJECTIVES FOR THE TOE)

Objective	Description
O.Crypt	The TOE shall provide cryptographic functionality as follows: • authentication, integrity protection and encryption of the communication and data to the PKI and external entities using IF_GW_WAN or IF_GW_LocalAdmin, • replay detection for all communications with external entities.
O.ReceiveAuthenticatedData	The RGW shall only accept and process traffic data by the V-ITS-Ss, RO 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, RO or the V-ITS-Ss if the corresponding messages comply with the defined message formats and if it is authenticated.
O.SecureChannel	For communication with the TCC and RO the TOE shall establish a mutually authenticated and confidential channel.
O.Protect	[…]
O.Authentication	The RGW shall provide authentication mechanisms for all roles, which are defined in Table 3.
O.Access	[…]
O.SecureFirmwareUpdate	[…]
O.Management	The TOE shall provide the following management functionality to authorized administrators only: • Start firmware update • Configuration change • Certificate management • Obtain write permissions to system log files

COMMENT: Regarding O.ReceiveAuthenticatedData, it could be argued that also non-authenticated data (without signature) could be processed, e.g. for statistical reasons, as long as such messages are not re-broadcasted and forwarded without a clear indication that they were not authenticated.
Regarding O.Authentication and the requirement to provide authentication for all roles in Table 3: Road Maintenance Personnel has no access to IT interfaces, since it performs visual inspections and operational tasks.

LINE 332/330 (TABLE 9: SECURITY OBJECTIVES FOR THE ENVIRONMENT)

In Table 9, "RWWG" *is replaced by* "RWG"

LINE 336

In Table 10 "Rationale for Security Objectives", two new entries are inserted for the column O.Mananagement in the rows T.RemoteDataManipulation and T.RemoteMalfunction:

Security Problem Definition / Security Objective	O.Manana gement
T.Extraction	
T.LocalMalfunction	**X**
T.LocalDataManipulation	**X**
T.SoftwareManipulation	
T.RemoteDataManipulation	**X**
T.RemoteMalfunction	**X**
T.Interception	
OSP.SM	

LINE 367-374 (4.3.2.3 T.LOCALMALFUNCTION)

The induction of faulty behavior of the RGW by injecting malformed messages […]
O.Management is hereby also necessary to restrict firmware updates or examine log entries to administrators only.

LINE 387 (4.3.2.4 T.LOCALDATAMANIPULATION)

O.Management also supports the countermeasures against this threat by restricting firmware updates or examine log entries to administrators only.

LINE 367-374 (4.3.2.6 T.REMOTEDATAMANIPULATION)

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

[…] only verified messages are accepted at the RGW. **O.Management** also supports the countermeasures against this threat by restricting firmware updates or examine log entries to administrators only.

LINES 406-412 (4.3.2.7 T.REMOTEMALFUNCTION)

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

[…] only verified messages are accepted at the RGW. **O.Management** also supports the countermeasures against this threat by restricting firmware updates or examine log entries to administrators only.

LINE 415 (T.INTERCEPTION)

In line 416, "RWWG" *is replaced by* "RWG"

LINE 490

In the application note under line 490, "IVS" *is replaced by* "V-ITS-S"

LINE 498 (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 no other than the _cipher suites as recommended by [TR-02102-2] for TLS 1.2 with Perfect Forward Secrecy and for TLS 1.3.

_ [*list of cipher suites deleted*]

Further, the following requirements shall be followed by the TOE: […]

COMMENT: The list of cipher suites from an older version of TR-02012-2 is deleted and replaced by the updated reference to TR-02102-2, since the list misses some CBC-MAC versions of cyphers for TLS 1.2 and the cipher suites for TLS 1.3

LINES 480-582

- RO authentication is required to upload the firmware update data (acc. FIA_UAU.2 and FIA_UID.2),
- Automatic firmware update is not allowed, if the previous points cannot be guaranteed.

COMMENT: Automatic firmware is made conditional. Automation may be needed for a large number of devices. Secure firmware update can be ensured if an authorised user of the RO initiates the automated firmware update and the ToE checks authenticity and integrity of the received firmware.

LINES 531, 532

In lines 531 (FDP_ACC.1.1) and 532 (FDP_ACF.1.1), "RWWG" *is replaced by* "RWG"

LINE 533, FDP_ACF.1.2

[…] [

- *an authorized RO 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 RO is allowed to start the firmware update process.*
- *an authorized TCC is only allowed to interact with the TOE via a WAN interface (IF_GW_WAN) or via a LAN interface (IF_GW_LAN)*].

LINE 535, FDP_IFC.2.1

The TSF shall enforce the [*RGW IFP*] on [

- *Subjects: TOE, TCC, V-ITS-S, PKI, Gateway to equipment, Controller [assignment: other or none]*

[…]

COMMENT: Regarding the TCC as a subject: The interface to the TCC, the Gateway, or the Controller might be optional and described by an assignment.

LINE 536, FDP_IFF.1.1

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

- *Subjects: TOE, TCC, V-ITS-S, RO, PKI, Gateway to equipment, Controller, [assignment: other or none]*
- *Information: messages and their signature*
- *Attributes: source_interface (TOE), destination_interface (TCC, PKI, Gateway to equipment, Controller, or RO), destination_authenticated*
- *Attributes: destination_interface (TOE), source_interface (TCC, V-ITS-S, PKI, Gateway to equipment, Controller, or RO), source_authenticated*

].

COMMENT: Vehicles are reached on a broadcast channel. On a broadcast channel the destination cannot be authenticated, and it does not need to be authenticated. Therefore, the attributes are split.

LINE 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 = RO or source_interface=TCC) and destination_interface = V-ITS-S*
  - *Source_interface = V-ITS-S and (destination_interface= RO or destination_interface=TCC)*
  - *Source_interface = RO and destination_interface=TCC*
  - *Source_interface= TCC and destination_interface=RO*
  - *Source_interface= PKI and destination_interface=TOE*
  - *_ [connection between TOE and modules deleted]*
- *All messages sent to TCC, all RO 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=V-ITS-S, or source_interface=RO, or source_interface=Gateway to equipment or source=Controller 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 = V-ITS-S that do not fulfill the standard of [assignment: standards or list of standards, based on the implemented set of ITS messages] shall be dropped*].

COMMENT 1: The connection between TOE and modules cannot be denied, since the TOE could poll the controller state or the gateway to equipment.
COMMENT 2: Regarding “The signature of every message […] must be verified”: Messages could reach the TOE via a secure connection (TLS), in this case individual message signing does not apply.

LINE 543, FIA_UAU.5.2

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

- *_ROs shall be authenticated via TLS-certificates at IF_GW_WAN or IF_GW_Local_Admin only*
- *TCCs shall be authenticated via TLS-certificates at IF_GW_WAN interface only*
- *V-ITS-S shall be authenticated via certificates at IG_GW_V-ITS-S only*

[assignment: rules describing how the multiple authentication mechanisms provide authentication]].

LINE 547, FMT_MSA.1.1

The TSF shall enforce the [*RGW access policy*] to restrict […]

LINE 549, FMT_SMF.1.1

The TSF shall maintain the roles [

- *RO,*
- *TCC,*
- *V-ITS-S, and*

[assignment: additional roles or none]].

COMMENT: The TCC role might be described conditionally: [assignment: TCC, if a connection to the TCC is intended]

Line 552, Application Note under FPT_STM.1.1

Therefore the local clock shall be able to measure time in a granularity that is required for TLS connections.
[reference to RFC5246 deleted, since there is no requirement on local clocks]

Line 556, FTP_ITC.1.1 (b)

b) Authenticated communication channel using TLS as defined in [RFC5246] or newer for server authentication.

COMMENT: RFC5246 is TLS Version 1.2 and superseded by RFC 8446 https://tools.ietf.org/html/rfc8446

Lines 684-687

- **FCS_COP.1/TLS** defines the requirements around the encryption and decryption capabilities of the RGW for communications with external parties in the WAN_.
- **FCS_COP.1/SIGVER** defines the requirements around the verification of signatures.

Line 658 (6.1 Glossary)

[…]

TLS	Transport Layer Security protocol according to RFC5246 or newer.

[…]

Line 660 (6.2 References)

[Missing references:]

[CSP-PP]	Cryptographic Service Provider, Version 0.9.8, BSI-CC-PP-0104-2019 https://www.commoncriteriaportal.org/files/ppfiles/pp0104b_pdf.pdf
[FIPS 180-4]	NIST FIPS 180-4, Secure Hash Standard (SHS), August 2015
[FIPS 186-4]	NIST FIPS 186-4, Digital Signature Standard (DSS), July 2013

[Changed references:]

[DENM]	ETSI EN 302 637-3 *[version number deleted]*: 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 *[version number deleted]*: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service
[TR-02102-1]	Technische Richtlinie TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2020-01
[TR-02102-2]	Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2020-01

[Deleted references:]

~~[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~~