Protection Profile for a Roadside ITS Station Gateway

Roadside ITS Station Gateway PP

Version 1.0

Certification-ID: BSI-CC-PP-0122

Co-financed by the Connecting Europe Facility of the European Union

Table of content

116

List of Tables

131

List of Figures

133

1 PP Introduction

1.1 Introduction

This Protection Profile defines the Security Functional Requirements (SFRs) and the Security Assurance Requirements (SARs) for a Roadside ITS Station Gateway.

The Roadside ITS Station (R-ITS-S) is an electronic device and part of an Intelligent Transport System (ITS). It exchanges ITS/C-ITS messages with other ITS/C-ITS stations in the context of Infrastructure to Vehicle (I2V) and Vehicle to Infrastructure (V2I) communication.

The data exchange includes events, warnings and information related to road traffic. Communication from the Roadside ITS Station to Vehicle ITS Stations can be seen as a digital complement to physical road signs and physical light signals.

Hint

C-ITS stands for Cooperative ITS, which is a subset of ITS. “C-ITS messages” are also referred to as “ITS messages” in the respective standards. Since this Protection Profile has been developed in the context of [SP] and [CP], where the term “C-ITS message” is used, the term “C-ITS message(s)” is used throughout the document.

1.2 PP Reference

Title:	Protection Profile for a Roadside ITS Station Gateway		
Version:	1.0		
Date	23.01.2024		
Authors:	Markus Wagner,	(TÜVIT),	m.wagner@tuvit.de
	Maximilian Wahner,	(TÜVIT),	m.wahner@tuvit.de
	Sandro Berndt-Tolzmann,	(BASt),	berndt@bast.de
Certification-ID:	BSI-CC-PP-0122		
Evaluation Assurance Level:	EAL3		
CC-Version:	CC:2022 Revision 1		

1.3 TOE Overview

1.3.1 Introduction

The Target of Evaluation (TOE) described in this Protection Profile is a Roadside ITS Station Gateway (RGW) as a part of the corresponding Roadside ITS Station (R-ITS-S), in line with the respective requirements of [SP]. The R-ITS-S 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.

The TOE itself is the part of the R-ITS-S, which is able to transmit C-ITS messages based on input coming from sensors connected to the R-ITS-S or from the Traffic Control Center (TCC) and also to collect C-ITS messages sent by bypassing vehicles.

It should be noted that this Protection Profile does not aim to imply any concrete system architecture or product design as long as the security requirements from this Protection Profile are fulfilled. Only in cases where the implementation of the Security Functional Requirements will definitely require a certain architecture, this architecture is described in this Protection Profile in a mandatory way.

1.3.2 TOE Type

The TOE is part of the R-ITS-S, controlling the basic functionalities and communication aspects as well as the data aggregation.

This Protection Profile is a generalisation of the Road Works Warning Gateway Protection Profile under Certification-ID BSI-CC-PP-0106.

1.3.3 System Overview

The following figure provides an overview of the TOE with its logical interfaces, its relation to the R-ITS-S and its immediate environment.

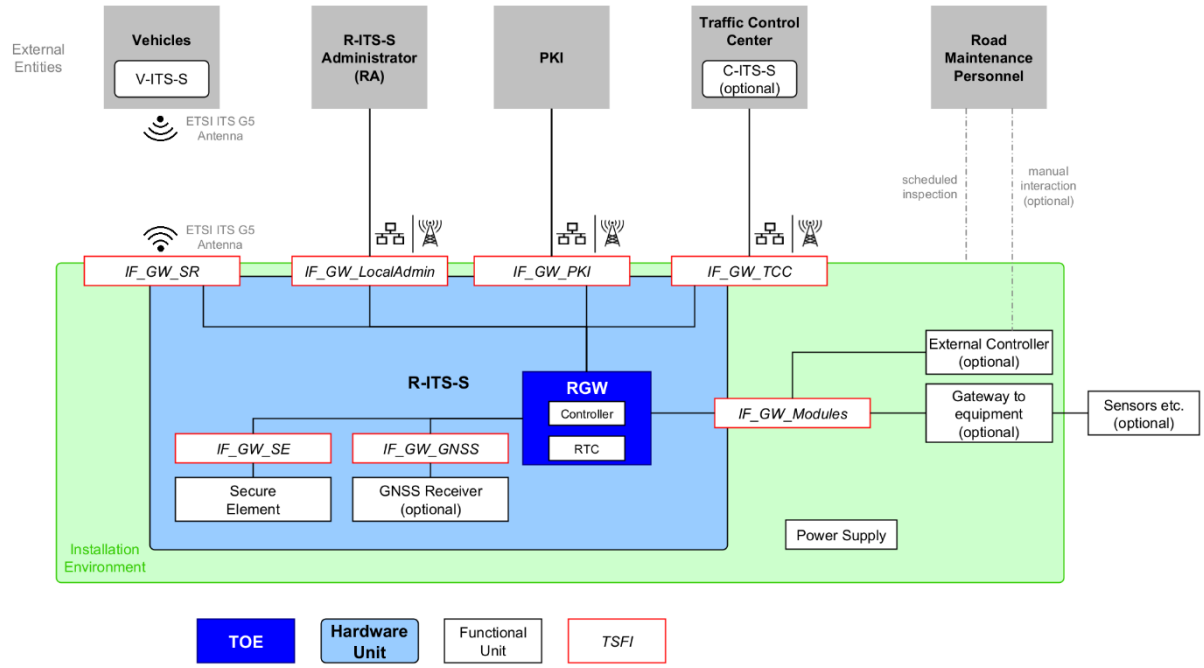

Figure 1: TOE and its environment

The R-ITS-S provides the physical enclosure, in other words the R-ITS-S is the technical system in which the TOE is integrated, as well as the Secure Element and an optional GNSS receiver.

The TOE is able to send and receive C-ITS messages to/from other C-ITS stations using ITS-G5. It may receive C-ITS messages and/or content from a TCC in order to send C-ITS messages to other C-ITS stations via ITS-G5.

The gateway utilises the services of a Secure Element as a cryptographic service provider and as a secure storage for confidential assets.

1.3.4 Services of the Roadside-ITS-Station

The following paragraphs introduce the overall functionality of the TOE in a more detailed manner but are not representing the covered logical scope of the TOE. The purpose of ITS systems in general is to improve road traffic in various ways, e.g. in terms of increased traffic safety as well as improved traffic flow and efficiency with the following services.

1.3.4.1 Local Traffic Information

C-ITS Infrastructure-to-Vehicle services are used to inform road users within the communication range of the TOE in a timely manner about the situation on the road, i.e. vehicles in the vicinity of the TOE. These services can be triggered by the TCC/C-ITS-S or by the R-ITS-S. The required information is time sensitive. To realise this objective, the R-ITS-S broadcasts appropriate information towards the vehicles approaching the R-ITS-S location, using C-ITS messages like DENM, IVIM, SPATEM, MAPEM, SSEM.

193 **Hint**

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

199 #### 1.3.4.2 Local Traffic Surveillance and Other V2I Services

200 This service receives C-ITS messages being broadcasted by vehicles (e.g. DENM and CAM), potentially
201 aggregates the received data and makes the information available for improved traffic management
202 services. In addition to the potential aggregation on the R-ITS-S, additional processing may be done
203 partly or completely in the TCC and/or may also be used by other services of the road operators and
204 may be re-used by other service providers.

205 ### 1.3.5 TOE Physical Scope

206 The TOE comprises the hardware and software that is relevant for the security functionality of the R-
207 ITS-S as defined in this PP. The Secure Element that is utilised by the TOE is considered being not part
208 of the TOE[1].

209 As mentioned in Section 1.3.1, this PP does not want to imply any concrete physical architecture for the
210 components that make up the R-ITS-S. Specifically, the TOE described in this PP only includes an
211 independent computing system (labelled as “controller” in Figure 1) and a real-time clock, along with
212 the corresponding software parts for monitoring and controlling the functionalities described in Section
213 1.3.4.

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

215 - (LAN/WAN) Communication segment(s), at least one mandatory:
216 - Network interface (e.g. Ethernet)
217 - Mobile cellular communication (e.g. GSM, UMTS, LTE, 5G)
218 - (Short-range) Communication segment, mandatory
219 - ETSI ITS-G5 short-range communication based on [ETSI EN 302 663]
220 - Positioning technology, optional
221 - GNSS receiver

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

227 **Hint**

228 The actual antennas for the communication segments listed above are not part of the TOE.

229

230 **Hint**

231 In the product evaluation process, also the guidance parts belong to the physical scope of the TOE.

232

[1] Please note that the Secure Element is physically integrated into the R-ITS-S, even though it is not part of the TOE.

1.3.6 TOE Logical Scope

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

- Sufficiently encrypted communication to the RA, the TCC and the PKI.
- Trusted communication establishment with the PKI (according to [CP]), the R-ITS-S Administrator (RA), the TCC.
- Replay detection of messages sent from the TCC and/or the RA.
- 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.
- Assurance of authenticity of information content received from or send to mandatory TOE Security Functional Interfaces (TSFIs).
- Assurance of secure state in case of error events (incl. initial values).
- Secure firmware update.
- Self-test possibilities including verifying the authenticity of the Secure Element on start-up.
- Secure data deletion.
- Reliable time-stamp generation.

The services of the Secure Element are not part of this Protection Profile. The necessary service will be outlined in Section 1.4 in more detail.

Application Note 1

The ST author shall define the protocol to be used for the connections to the RA and the TCC (i.e. TLS [RFC8446], IPsec [RFC4301] or SSH [RFC4254]) and specify it in SFR FTP_PRO.1/Backend (including all dependencies).

The protocol chosen by the ST author should have a comparable level of security as the protocols mentioned in the example above.

Should different protocols be used for the connection to the TCC and the connection to the RA, it is recommended to iterate the SFR FTP_PRO.1 (including all dependencies) to model the additional protocol.

The ST author shall also consider Application Note 27 and OSP.StrongCrypto (see Table 6).

Application Note 2

When requesting new certificates required for the C-ITS communication of the TOE, the message exchange (Authorisation Request/Response and Enrolment Request/Response) with the PKI (Authorisation Authority (AA) and Enrolment Authority (EA)) shall be protected by the cryptographic algorithms AES-CCM and ECIES as described in [ETSI TS 102 941].

1.3.7 The Logical Interfaces of the TOE

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

Interface Name	Description
IF_GW_PKI	This interface is used for the connection to the PKI for certificate-related operations.

Interface Name	Description
IF_GW_TCC	This interface is used for the connection to the TCC to receive or transmit data to it.
IF_GW_SR	This interface is responsible for every short-range communication from and to other ITS stations, usually in vehicles. This includes the reception of C-ITS messages such as DENMs or CAMs from the V-ITS-S, and the potential warning of all V-ITS-S in the direct surrounding if necessary.
IF_GW_ Admin	This interface is used for R-ITS-S Administrators only, aiming on allowed administration tasks. This can be realized as a local and/or remote interface.
IF_GW_GNSS (optional)	This interface is used for the connection to optional GNSS receivers, and the provision/estimation of the current position.
IF_GW_SE	This interface connects the TOE with the Secure Element.
IF_GW_Modules (optional)	This interface is used to communicate with other optional local functional modules linked to the RGW/R-ITS-S. 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.)

Table 1: TOE external interfaces

Application Note 3
Within this PP, it is assumed that IF_GW_Modules is wired. Should any Security Target (ST) author prefer wireless connections, this shall be modelled accordingly to ensure the integrity of the received data, e.g. by a corresponding authenticated encryption scheme.

Application Note 4
Table 1 lists mandatory and optional interfaces. Additional interfaces to the TOE are possible and can be defined and modelled by the ST author. For each additional interface, an adequate security level shall be ensured, e.g. by fulfilling FTP_ITC.1 or FTP_PRO.1.

1.4 Secure Element (not Part of the TOE)

The RGW is linked to a Secure Element that acts as a provider of the required cryptographic operations used in the aforementioned functions. It provides strong cryptographic functionality such as random number generation and secure storage of secrets, and supports the authentication of external entities. The Secure Element is a different sub-module of the R-ITS-S for which separate PP exist (e.g. [SE-PP], [CSP-PP] or comparable); it is therefore not part of the TOE as described in this PP. Nevertheless, it is physically embedded into the R-ITS-S and protected by the same level of physical protection.

Following from the SFRs and the defined application scenario the Secure Element shall be used for

- generation of random numbers,
- management of relevant (cryptographic) keys according to [CP]:
  - storage of private keys,
  - generation of ECC asymmetric key pairs for ECDSA,
  - generation of ephemeral ECC asymmetric key pairs for ECIES encryption, and
  - secure deletion of keys,
- digital signature generation (ECDSA) for data and entity authentication, and
- ECIES encryption of secret data encryption keys.

Application Note 5

In the context of C-ITS messages, a SE needs to be present according to [CP]. If required in the context of backend communication with RA and the TCC, e.g. for TLS, it is allowed to include one or more of the functionalities defined above within the TSF. If done so, the Security Target (ST) author is advised to also model the corresponding SFRs within his/her ST to implement a secure realisation of these functionalities.

Application Note 6

The Secure Element shall be protected against unauthorised removal, replacement, and modification.

Hint

Since it is expected that on some occasions a large number of messages from V-ITS-S 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.

1.5 Life Cycle

The life cycle of the TOE consists of the following consecutive phases:

1. **Design/Development**
   The development of the TOE.
2. **Manufacturing/Assembly**
   The production like hardware assembly or software installation. This comprises the initial ITS-S configuration during manufacturing, including the installation of the initial Trust List Manager (TLM) certificate.
3. **Registration**
   Registration of the R-ITS-S at a PKI.
4. **Enrolment**
   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, defective state or shall be taken out of order for other reasons, it shall be ensured that the key and certificate material that is contained within the TOE is destroyed in a secure manner. This also includes potentially necessary actions to / with the Secure Element as described in the corresponding guidance documentation (e.g. kill command).

The life cycle 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 after successful enrolment and authorisation.

Application Note 7

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.

Hint

344 It is recommended to embed the use of the TOE in an Information Security Management System (ISMS)
345 according to [ISO27001] or similar.

2 Conformance Claims

2.1 CC Conformance Claims

This Protection Profile has been developed using Common Criteria version CC:2022 Revision 1 [CC], and is

- Common Criteria [CC] Part 2 conformant, and
- Common Criteria [CC] Part 3 conformant.

2.2 PP Conformance Claim

This PP does not claim conformance to any other PP.

2.3 Conformance Claim Rationale

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

2.4 Package Conformance Claim

This PP is conforming claims assurance package EAL3 as defined in [CC] Part 5.

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 RGW refers to the integration of those components. However, as the Evaluation Assurance Level (EAL) in this PP has been chosen to be EAL3, this should not introduce intractable problems during the evaluation process.

2.5 Conformance Statement

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

3 Security Problem Definition

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

- the **external entities** that are envisioned 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, and
- **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
R-ITS-S Administrator (RA)	The R-ITS-S Administrator is responsible for initial setup of the R-ITS-S including 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, typically via C-ITS-S. In addition, the TCC is also able to configure non security-related settings via functional parametrisation.
Vehicles (V-ITS-S)	Vehicles sends and receives traffic related data to / from the RGW.
Road Maintenance Personnel	The Road Maintenance Personnel maintains the road infrastructure and is responsible for visual inspection of road infrastructure elements including R-ITS-S. Such personnel is not responsible for maintaining the R-ITS-S and therefore not accessing maintenance interfaces of the RGW.
PKI	The Public Key Infrastructure (PKI) comprises different services, including issuing certificates, CTLs and CRLs to the RGW as a prerequisite for a trusted exchange of C-ITS messages between the RGW and V-ITS-S. EA and AA are part of the PKI.

Table 2: External entities

Hint

In terms of [CP] and [SP], the RA can be seen as an instantiation of an "operator" and/or "manufacturer", depending on the actual organisational and contractual setup. Similar considerations apply to the TCC, which might or might not be identical to the "operator" in [CP] and [SP].

3.2 Assets

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

Assets	Description		Protection Requirements	Comment
	In(coming)/ Out(going)	Source/ Destination		
Input from external controller	In	External Controller	-	Optional, only for TOE with a locally connected external controller, such as a traffic light controller or 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.
C-ITS message reception	In	Other ITS-S to TOE	Integrity, Authenticity	TOE verifies signature.
C-ITS message transmission	Out	TOE to other ITS-S	Integrity, Authenticity	TOE creates C-ITS messages and utilises SE to sign them. In case of message forwarding, the verified message is re-transmitted without creating a new signature.
Payload of C-ITS message	Out	TOE to TCC	Integrity, Authenticity	This applies if the TOE forwards parts of a C-ITS message to TCC without the original signature. The signature of the C-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	In	TCC to TOE	Integrity,	Correctness of incoming data has to be

Assets	Description		Protection Requirements	Comment
	In(coming)/ Out(going)	Source/ Destination		
TCC			Authenticity	assumed. Out of evaluation scope.
Log data	Out	TOE to RA	Integrity	TOE generates security relevant entries for log data.
RA data	In & Out	RA to TOE, TOE to RA	Integrity, Authenticity	Incoming: admin data for RA, e.g. configuration. Outgoing: admin data for RA, e.g. acknowledgements, configuration, etc.
Firmware update	In	RA to TOE	Integrity, Authenticity	TOE verifies integrity and authenticity.
Request of certificates	In & Out	TOE requests, PKI responds	Integrity, Authenticity, and Confidentiality.	TOE requests a new certificate from the AA, which is required to sign C-ITS messages. TOE requests a new certificate from the EA, which is required to stay enrolled in the PKI.
Update of Trust Elements	In	PKI provides information	Integrity, Authenticity	TOE receives updates of the CTLs and CRLs provided by the PKI. TOE receives updates of certificates provided by the PKI (i.e. certificates of TLM, Root CA, EA and AA).
Private cryptographic keys	Ephemeral or long-term cryptographic material used by the TOE for cryptographic operations.		Integrity, Authenticity, and Confidentiality.	According to the [CP], all private keys used for the communication in the C-ITS context (i.e. for signing of C-ITS messages) have to be stored in the Secure Element. Private keys used for communication with backend systems (i.e. RA or TCC) must be adequately secured.
Public cryptographic keys	Ephemeral or long-term cryptographic material used by the TOE for cryptographic		Integrity, Authenticity	All public keys have to be adequately secured.

Assets	Description		Protection Requirements	Comment
	In(coming)/ Out(going)	Source/ Destination		
	operations.			

Table 3: Assets

Hint

The integrity and authenticity of the C-ITS messages received via IF_GW_SR is ensured as described in the respective message standards, relying on a PKI and the use of certificates according to [ETSI TS 103 097]. Additionally, every communication to the TCC or RAs has to be protected by an encrypted and authenticated communication channel, even if information is just forwarded by the TOE.

Application Note 8

If data aggregation of the defined asset ”Payload of C-ITS messages” is provided by the TOE, the ST author shall include the aggregated data as an 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 unauthorised entities and enable the evidence of origin of information for further entities)

3.3 Assumptions

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

Assumption	Description
A.SecureSetup	It is assumed that appropriate security measures are taken during the setup of the TOE to guarantee for the confidentiality, authenticity, and integrity of the initial cryptographic data.
A.TrustedAdministrator	It is assumed that the administrator of the TOE (R-ITS-S Administrator) is trustworthy, non-hostile and well-trained.
A.PhysicalProtection	It is assumed that the TOE is physically protected, or at least that manipulations can be identified within a manageable timespan. During the non-monitored phases, unauthorised 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 recognisable either on-site or by remote monitoring. In addition, it is assumed that a visual examination by authorised 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 TOE 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 (via IF_GW_Modules) are correct and protected against manipulation.

Table 4: Assumptions

Application Note 9

There are various options for mounting the R-ITS-S (including the TOE), e.g.:

- Option 1: The R-ITS-S is firmly mounted and not easily accessible.
- Option 2: The R-ITS-S 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.

The guidance documentation shall consider how the R-ITS-S (including the TOE) is mounted.

Regardless of how the R-ITS-S (including the TOE) is mounted, the assumption A.PhysicalProtection applies.

Application Note 10

There are various options for the determination of the correct location for the TOE, e.g.:

- 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.

The guidance documentation shall consider the option for the determination of the correct location.

Regardless of the method for determination of the location, the assumption A.CorrectLocation applies.

3.4 Threats

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, i.e.:

- Individuals or organisations outside of the listed external entities (see Section 3.1). They may perform attacks via the Internet, mobile networks, or ITS-G5 network.

Attackers can also be characterised by their **motivation**:

- Gaining reputation. By publishing the performed attacks, the person is respected as an expert, e.g. for security within the ITS/C-ITS context.
- Gaining traffic priority.
- Financial reasons. An attacker could manipulate the functionality for ransom.
- Vandalism.
- Industrial espionage.
- Cyber terrorism and cyber warfare.

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 6.10.12.1 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.

3.4.2 Threats

Threat	Description
T.Extraction	An attacker tries to extract private key material from the TOE. The attack might be performed by the use of the external interfaces of the TOE (i.e. by observing the data that the TOE sends/receives). 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 TOE by applying environmental or physical stress, by injecting malformed messages to local interfaces or by manipulating internal connections of the TOE.
T.LocalDataManipulation	An attacker tries to modify the configuration of the TOE or 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	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 tries to modify the configuration of the TOE or inject false traffic data by impersonating a V-ITS-S, a TCC, the RA or the PKI. (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 TOE by sending malformed messages to the TOE.
T.Interception	An attacker tries to intercept traffic data (incl. content of C-ITS messages), road works data, status data or configuration data sent between the TOE and the TCC/RA/PKI.

Table 5: Threats

Hint

Faulty behaviour as stated in T.LocalMalfunction and T.RemoteMalfunction comprises various types, e.g. misinterpretation of certificate lists, start-up errors, connection problems etc. As a consequence, these threats can be directed against different assets.

3.5 Organisational Security Policies (OSPs)

Organisational 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.SE	The TOE shall use the services of a certified Secure Element for[2]:
	• generation of random numbers,
	• management of relevant (cryptographic) keys according to [CP]:
	  o storage of private keys,
	  o generation of ECC asymmetric key pairs for ECDSA,
	  o generation of ephemeral ECC asymmetric key pairs for ECIES encryption, and
	  o secure deletion of keys;
	• digital signature generation (ECDSA) for data and entity authentication, and
	• ECIES encryption of secret data encryption keys.
	The Secure Element shall be certified according to Protection Profiles such as [SE-PP] or comparable and shall be used only in accordance with its corresponding guidance documentation and certification report.

OSP.StrongCrypto	All cryptographic algorithms used by the security functionality of the TOE shall provide a cryptographic strength of at least 120 bit.[3]
OSP.Log	The TOE shall maintain a log of relevant events in order to allow an authorised RA to analyse the status of the TOE. The TOE may overwrite the oldest log events in case that the audit trail gets full.

459 **Table 6: Organisational security policies**

460 **Application Note 11**
461 If a Random Number Generation (RNG) functionality is provided by the TOE itself, the ST author shall
462 model it appropriately using the SFR FCS_RNG.1 or FCS_RBG.1.

463

464 **Application Note 12**
465 The ST author shall consider that the evaluation body has to examine the certification report of the used
466 Secure Element for an appropriate application to the TOE (e.g. in terms of used data formats,
467 implemented interactions as well as storage and disposal of the Secure Element).

[2] The defined security functionalities may be included within the TOE and thereby excluded from the Secure Element within the specific TOE. If so, corresponding SFRs have to be modeled by the ST author. Hence, the PP author highly recommend to realise the mentioned services within a Secure Element.

[3] During certification of a specific R-ITS-S, the certification body in charge may impose additional requirements concerning the choice and minimum strength of cryptographic functions.

468 4 Security Objectives

469 In this chapter, the security objectives for the RGW and its environment are described.

470 4.1 Security Objectives for the TOE

Objective	Description
O.Crypt	The TOE shall provide cryptographic functionality as follows: • authentication, integrity and confidentiality protection of the communication and data to external entities using IF_GW_Admin, IF_GW_PKI, or IF_GW_TCC, • replay detection for communications with the external entities TCC and RA, and • authentication and integrity protection by signature verification of messages sent from V-ITS-S using IF_GW_SR.
O.ReceiveAuthenticatedData	The TOE shall only accept and further process data received from V-ITS-S, RA, TCC, and PKI 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 data to V-ITS-S, RA, TCC and PKI if the corresponding messages comply with the defined message formats and if authenticity and integrity are ensured.
O.SecureChannel	For communication with the TCC and the RA, the TOE shall establish a mutually authenticated and confidential channel. For communication with the PKI, the TOE shall establish an authenticated message exchange (Authorisation Request/Response and Enrolment Request/Response) according to [ETSI TS 102 941].
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, • make any physical manipulation within the scope of the intended environment detectable for Road Maintenance Personnel, • ensure that the TOE falls into a secure state in case of a security-relevant malfunction.
O.Authentication	The TOE shall provide authentication mechanisms for the roles RA, TCC, V-ITS-S, and PKI which are defined in Table 2.
O.Access	The TOE shall provide access control mechanisms for its functionalities 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 of the security functionality to authorised RA only:

Objective	Description
	• start firmware update, and • configuration change.
O.Log	The TOE shall maintain a log of relevant security events in order to allow an authorised RA to analyse the status of the TOE. The TOE may overwrite the oldest log events in case that the audit trail gets full.

471 **Table 7: Security objectives for the TOE**

472 **Application Note 13**

473 Concerning O.Access, the ST author shall only provide access mechanisms for those roles which need
474 to have access to TOE configuration items, i.e. the RA. For all other users and entities, the ST author
475 shall prevent any kind of access.

476 ## 4.2 Security Objectives for the Operational Environment

Objective for environment	Description

OE.SE	The operational environment shall provide the services of a certified Secure Element for[2]:
	• generation of random numbers,
	• management of relevant (cryptographic) keys according to [CP]:
	  o storage of private keys,
	  o generation of ECC asymmetric key pairs for ECDSA,
	  o generation of ephemeral ECC asymmetric key pairs for ECIES encryption, and
	  o secure deletion of keys,
	• digital signature generation (ECDSA) for data and entity authentication, and
	• ECIES encryption of secret data encryption keys.
	The Secure Element shall be certified according to Protection Profiles like [SE-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 setup of the TOE to guarantee for the confidentiality, authenticity, and integrity of the initial cryptographic data.
OE.TrustedAdministrator	It shall be ensured that the administrator of the TOE is trustworthy, non-hostile and well-trained.
OE.PhysicalProtection	It shall be ensured that the TOE is physically protected, or at least that manipulations can be identified within a manageable timespan. During the non-monitored phases, unauthorised physical access to the TOE cannot be completely avoided. Nevertheless, it shall be ensured that a theft of the TOE or an intervention that directly influences its telemetry is recognisable either on-site or by remote monitoring. In addition, it shall be ensured that a visual examination by authorised 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 TOE 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 (via IF_GW_Modules) are correct and protected against manipulation.

477 **Table 8: Security objectives for the operational environment**

478

4.3 Security Objectives Rationale

4.3.1 Overview

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

Table 9: 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.Access** ensures that only authorised roles are able to access the TOE parts and also **OE.TrustedAdministrator** contributes to this aspect as it provides the requirements on the availability of a trustworthy administrator. **O.Authentication** is needed to ensure authentication for the different roles.

O.SecureChannel secures the usage of appropriate communication channels, secured by the corresponding cryptographic algorithms based on **O.Crypt** (cryptographic operations). **O.ReceiveAuthenticatedData** and **O.SendAuthenticatedData** allow import and export of required data, while its integrity and authenticity are ensured by digital signatures.

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, cryptographic secured communication channels and side-channel resistant cryptographic algorithms. **O.Protect** protects 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 behaviour of the TOE by injecting malformed messages or manipulations is covered by **O.Protect** and **O.Management**.

Hereby**, O.Protect** explicitly 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. **O.Management** is hereby also necessary to restrict firmware updates and configuration changes.

In addition, the **OE.PhysicalProtection** contributes to counter this threat by ensuring that manipulations can be identified within a manageable timespan.

4.3.2.4 T.LocalDataManipulation

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

O.Crypt enforces the usage of reliable signature verification, cryptographic secured communication channels and side-channel resistant cryptographic algorithms. **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. **O.ReceiveAuthenticatedData** and **O.SendAuthenticatedData** allow import and export of required data, while its integrity and authenticity are ensured by digital signatures. **O.Access** enables the necessary access control, which provides the rights to the corresponding user whereby **O.Authentication** provides authentication mechanisms. **O.Management** also supports the countermeasures against this threat by restricting firmware updates and configuration changes.

In addition, the **OE.PhysicalProtection** contributes to counter this threat by ensuring that manipulations can be identified within a manageable timespan.

4.3.2.5 T.SoftwareManipulation

The installation of hostile software or firmware 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 Section 4.3.2.4. Additionally **O.SecureFirmwareUpdate** only allows verified updates to be installed.

In addition, the **OE.PhysicalProtection** contributes to counter this threat by ensuring that manipulations can be identified within a manageable timespan.

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**.

This threat is countered by nearly the same objectives like in Section 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 TOE. **O.Management** also supports the countermeasures against this threat by restricting firmware updates and configuration changes.

4.3.2.7 T.RemoteMalfunction

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

O.Protect is used to counter this threat concerning to the explanations in Section 4.3.2.3. Additionally, **O.Crypt** enforces the usage of reliable signature verification, cryptographic secured 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 TOE. **O.Management** also supports the countermeasures against this threat by restricting firmware updates and configuration changes.

4.3.2.8 T.Interception

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

O.Crypt enforces the usage of reliable signature verification, cryptographic secured 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. **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 operational environment and the TOE cover the organisational security policies.

4.3.3.1 OSP.SE

The organisational security policy **OSP.SE** that mandates that the TOE utilises the services of a certified Secure Element is directly addressed by the security objectives **OE.SE** and **O.Crypt**. The objective **OE.SE** addresses the functions that the Secure Element shall be utilised for as defined in **OSP.SE** and

also requires a certified Secure Element according to the specified requirements in **OE.SE**. **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.

4.3.3.2 OSP.StrongCrypto

The organisational security policy **OSP.StrongCrypto** mandates that all cryptographic functions of the TOE shall have a security level of at least 120 bit. **O.Crypt** ensures that the respective security level is applied by the security functionalities.

4.3.3.3 OSP.Log

The organisational security policy **OSP.Log** that mandates that the TOE maintains an audit log is directly addressed by the security objective for the TOE **O.Log**.

O.Log ensures security relevant information is tracked and can be examined by an authorised RA.

O.Access contributes to the implementation of the OSP as it defines that authorised RAs are not allowed to modify the log data. This is of specific importance to ensure the integrity of the log data as required by the **OSP.Log**.

4.3.4 Coverage of Assumptions

The following sections provide more detailed information about how the security objectives for the operational 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 operational 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 operational 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 operational 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 operational 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 operational environment are drafted in a way that the correspondence is obvious.

5 Extended Component Definition

This Protection Profile uses no components which are not defined in [CC] Part 2.

6 Security Requirements

6.1 Overview

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE. Those requirements comprise functional components from part 2 of [CC] and the assurance components as defined for the Evaluation Assurance Level 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
FAU_SAR.1	Audit review
FAU_STG.2	Protected audit data storage
FAU_STG.5	Prevention of audit data loss
Class FCS: Cryptographic Operation	
FCS_COP.1/AES	Cryptographic operation of AES-CCM
FCS_COP.1/Backend	Cryptographic operation for backend communication
FCS_COP.1/Hash	Cryptographic operation for hash value generation
FCS_COP.1/SigVer	Cryptographic operation for signature verification
FCS_COP.1/SigVerFW	Cryptographic operation for signature verification of firmware updates
FCS_CKM.1/AES	Cryptographic key generation of AES keys and nonces
FCS_CKM.1/Backend	Cryptographic key generation for backend communication
FCS_CKM.5/Backend	Cryptographic key derivation for backend communication
FCS_CKM.6	Timing and event of 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_MSA.1	Management of security attributes
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
Class FPT: Protection of the TSF	
FPT_FLS.1	Fail secure
FPT_PHP.1	Passive detection of physical attack
FPT_RPL.1	Replay detection
FPT_STM.1	Reliable time stamps
FPT_TDC.1	Inter-TSF basic TSF data consistency
FPT_TST.1	TSF self-testing
Class FTP: Trusted path/channels	
FTP_PRO.1/Backend	Trusted channel protocol for the backend communication
FTP_PRO.1/PKI	Trusted channel protocol for the communication with the PKI
FTP_PRO.2/Backend	Trusted channel establishment for the backend communication
FTP_PRO.3/Backend	Trusted channel data protection for the backend communication
FTP_PRO.3/PKI	Trusted channel data protection for the communication with the PKI

Table 10: List of Security Functional Requirements (SFRs)

6.2 Class FAU: Security Audit

6.2.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1

The TSF shall be able to generate audit data of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [basic] level of audit;

c) [assignment: **other non-privacy relevant auditable events**].

FAU_GEN.1.2

The TSF shall record within the audit data at least the following information:

a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;

b) For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [assignment: *other audit relevant information* ***or none***].

6.2.2 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.

6.2.3 FAU_SAR.1 Audit review

FAU_SAR.1.1

The TSF shall provide [*the RA, [assignment: other authorized users]*] with the capability to read [assignment: *list of audit information*] from the audit data.

FAU_SAR.1.2

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

6.2.4 FAU_STG.2 Protected audit data storage

FAU_STG.2.1

The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG.2.2

The TSF shall be able to [prevent] unauthorized modifications to the stored audit data in the audit trail.

6.2.5 FAU_STG.5 Prevention of audit data loss

FAU_STG.5.1

The TSF shall [overwrite the oldest stored audit records], [assignment: *other actions to be taken in case of audit storage failure and conditions for the actions*] if the audit data storage is full.

Hint

The size of the audit trail that is available before the oldest event is overwritten can either be a static value or dynamically configurable by the RA.

6.3 Class FCS: Cryptographic Support

6.3.1 FCS_COP.1/AES Cryptographic operation of AES-CCM

FCS_COP.1.1/AES

The TSF shall perform [*authenticated encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES-CCM*] and cryptographic key sizes [*128-bit*] that meet the following: [

AES	*[FIPS 197],*
AES-CCM	*[NIST SP 800-38C]*

691].

692 **Application Note 14**

693 Please note that [NIST SP 800-38C] requires that the nonce shall be unique for each encrypted message
694 protected by the same key.

695 The PP requires that, in addition to the uniqueness of the nonce, it should also be freshly generated at
696 random. Please refer to FCS_CKM.1/AES and Application Note 17.

697

698 **Hint**

699 AES-CCM is used to encrypt the Authorisation/Enrolment-Request and to decrypt the
700 Authorisation/Enrolment-Response exchanged between the TOE and the PKI (see [ETSI TS 102 941]).
701 Via FCS_CKM.1/AES, the respective AES key and the nonce are generated.

702 6.3.2 FCS_COP.1/Backend Cryptographic operation for backend communication

703 **FCS_COP.1.1/Backend**

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

707 **Application Note 15**

708 Please note that the PP is based on the assumption that all cryptographic keys required for the backend
709 connection are stored inside the TOE. If an ST author include cryptographic key that are stored outside
710 of the TOE, the author also shall model the corresponding cryptographic key access using FCS_CKM.3
711 and adjust the table of SFR dependencies (Table 13).

712 6.3.3 FCS_COP.1/Hash Cryptographic operation for hash value generation

713 **FCS_COP.1.1/Hash**

714 The TSF shall perform [*cryptographic hashing*] in accordance with a specified cryptographic algorithm
715 [*SHA-256, SHA-384, [assignment: other hash algorithms or none]*] and cryptographic key sizes [*none*]
716 that meet the following: [

SHA-256, *SHA-384*	*[FIPS 180-4],*
[assignment: other standards or none]	

717].

718 6.3.4 FCS_COP.1/SigVer Cryptographic operation for signature verification

719 **FCS_COP.1.1/SigVer**

720 The TSF shall perform [*signature verification*] in accordance with a specified cryptographic algorithm
721 [*ECDSA with SHA-256 and ECDSA with SHA-384*] and cryptographic key sizes [*NIST P-256,*
722 *brainpool256r1, brainpool384r1 and [assignment: curve or none]*] that meet the following: [

ECDSA	*[FIPS 186-4],*
NIST P-256	*[FIPS 186-4],*
brainpoolP256r1, *brainpoolP384r1*	*[RFC5639],*
SHA-256, *SHA-384*	*[FIPS 180-4],*
[assignment: other standards or none]	

723].

Hint

The signature generation will always be performed by the built in Secure Element while signature verification of received V-ITS-S transmissions may also be performed in the TOE.

6.3.5 FCS_COP.1/SigVerFW Cryptographic operation for signature verification of firmware updates

FCS_COP.1.1/SigVerFW

The TSF shall perform [*signature verification for firmware updates*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 16

The ST author is reminded that the PP author assumes a simple update process, in which a secure implementation is carried out without any security-relevant pre-processing of the update data. If pre-processing of the update data is performed, applicable processing rules should be modelled using FDP_ITC.1 or FDP_ITC.2.

6.3.6 FCS_CKM.1/AES Cryptographic key generation of AES keys and nonces

FCS_CKM.1.1/AES

The TSF shall generate cryptographic **AES** keys **and nonces** in accordance with a specified cryptographic key generation algorithm [*[selection: utilizing random source of the SE, utilizing random source as specified in FCS_RNG.1, utilizing random source as specified in FCS_RBG.1, [assignment: other source]*] and specified cryptographic key sizes [*128-bit for AES keys, 96-bit for nonces*] that meet the following: [

IEEE Std 1609.2 [IEEE 1609.2],

[assignment: other standards or none]

].

Application Note 17

Please note that [IEEE 1609.2] requires that the nonces shall be freshly generated at random for each invocation of AES-CCM.

Application Note 18

If a random source other than the SE is used for key generation, this must be modelled accordingly by the ST author, including adding new SFRs such as FCS_RNG.1 or FCS_RBG.1 (see Application Note 11) and resolving the dependencies of FCS_CKM.1/AES and all new introduced SFRs.

6.3.7 FCS_CKM.1/Backend Cryptographic key generation for backend communication

FCS_CKM.1.1/Backend

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

6.3.8 FCS_CKM.5/Backend Cryptographic key derivation for backend communication

FCS_CKM.5.1/Backend

The TSF shall derive cryptographic keys [assignment: *key type*] from [assignment: *input parameters*] in accordance with a specified key derivation algorithm [assignment: *key derivation algorithm*] and specified cryptographic key sizes [assignment: *list of key sizes*] that meet the following: [assignment: *list of standards*].

6.3.9 FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.6.1

The TSF shall destroy [assignment: list of cryptographic keys (including keying material)] when [no longer needed, *[assignment: other circumstances for key or keying material destruction **or none**]*].

FCS_CKM.6.2

The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Application Note 19

Please note that as against the requirement FDP_RIP.1 the mechanisms implementing the requirement from FCS_CKM.6 shall be suitable to avoid attackers with physical access to the TOE from accessing the keys after they are no longer used.

6.4 Class FDP: User Data Protection

6.4.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1

The TSF shall enforce the [*RGW access SFP*] 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 RGW access SFP.*

].

6.4.2 FDP_ACF.1 Security attribute-based access control

FDP_ACF.1.1

The TSF shall enforce the [*RGW access SFP*] 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 authorised RA is allowed to have access via IF_GW_Admin but is not allowed to read, modify or write stored and/or processed assets within the TOE, except reading status, logging, update information and configuration data,*
- *only an authorised RA is allowed to start the firmware update process and change configuration data,*
- *an authorised TCC is only allowed to interact with the TOE via IF_GW_TCC, and*
- *[assignment: rules, based on security attributes, that allow operations among controlled subjects and controlled objects]*.

].

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize 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 20

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 adjust the SFR dependencies table (Table 13).

6.4.3 FDP_IFC.2 Complete information flow control

FDP_IFC.2.1

The TSF shall enforce the [*RGW information flow control SFP*] on [

- *Subjects: TOE, RA, TCC, V-ITS-S, PKI, and [selection: Gateway to equipment, External Controller, [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.

6.4.4 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1

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

- *Subjects: TOE, RA, TCC, V-ITS-S, PKI, [selection: Gateway to equipment, External Controller, [assignment: other or none]];*
- *Information: messages;*
- *Attributes:*
  - *source_interface (TOE, RA, TCC, V-ITS-S, PKI, or [selection: Gateway to equipment, External Controller, none]),*
  - *destination_interface (TOE, RA, TCC, V-ITS-S, PKI, or [selection: Gateway to equipment, External Controller, none]),*
  - *signatures for ITS-M.*

].

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: [

- *Connection establishment is only allowed between the introduced destination_interfaces and source_interfaces.*
- *All messages sent to the roles TCC, RA and PKI must only be sent via a cryptographic secured communication channel.*
- *All ITS-M must be signed prior to sending utilising the SE.*
- *The signature of every ITS-M received by*
  - *source_interface = TCC*
  - *source_interface = V-ITS-S*

  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.*

].

FDP_IFF.1.3

The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4

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

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [

- *Connection establishment is especially denied in the following cases:*
  - *(Source_interface = RA or source_interface = TCC) and destination_interface = V-ITS-S*
  - *Source_interface = V-ITS-S and (destination_interface = RA or destination_interface = TCC)*
  - *Source_interface = RA and destination_interface = TCC*
  - *Source_interface = TCC and destination_interface = RA*
  - *Source_interface = PKI and destination_interface = TOE*
- *Received messages from source_interface = V-ITS-S that do not comply to a standard of [assignment: standards or list of standards, based on the implemented set of C-ITS messages] shall be dropped.*
- *[assignment*: *other rules, based on security attributes, that explicitly deny information flows]*

].

Application Note 21

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 13).

6.4.5 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]*].

6.5 Class FIA: Identification and Authentication

6.5.1 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, and*
- *[assignment: list of security attributes]*.

].

6.5.2 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

6.5.3 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1

The TSF shall provide [

- *authentication via validation of the authentication tag of AES-CCM at the IF_GW_PKI interface,*
- *[assignment: appropriate authentication mechanism] at the IF_GW_Admin interface,*
- *[assignment: appropriate authentication mechanism] at the IF_GW_TCC interface,*
- *authentication via certificates at IF_GW_SR, and*
- *[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 [

- *RAs shall be authenticated via [assignment: appropriate authentication mechanism] at IF_GW_Admin only,*
- *TCCs shall be authenticated via [assignment: appropriate authentication mechanism] at IF_GW_TCC interface only,*
- *PKIs shall be authenticated via validation of the authentication tag of AES-CCM at IF_GW_PKI only,*
- *V-ITS-S shall be authenticated via certificates at IF_GW_SR only,*
- *[assignment: rules describing how the multiple authentication mechanisms provide authentication]*.

].

Application Note 22

The ST author is reminded that the assignments in FIA_UAU.5 shall cover the authentication mechanisms for the protected communication channels (FTP_PRO.1/Backend, FTP_PRO.1/PKI, etc) as well as the authentication mechanisms for local maintenance by the RA.

6.5.4 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 TSF-mediated actions on behalf of that user.

6.6 Class FMT: Security Management

6.6.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1

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

6.6.2 FMT_SMF.1 Specification of management functions

FMT_SMF.1.1

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

- *firmware update,*
- *configuration change, and*
- *[assignment: list of additional management functions to be provided by the TSF or none].*

].

Application Note 23

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/SigVerFW), and
- RA authentication is required to upload the firmware update data (acc. FIA_UAU.2 and FIA_UID.2).

An automatic firmware update is not allowed if the previous points cannot be guaranteed.

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

6.6.3 FMT_SMR.1 Security roles

FMT_SMR.1.1

The TSF shall maintain the roles [

- *PKI,*
- *RA,*
- *TCC,*
- *V-ITS-S, and*
- *[assignment: additional roles or none].*

].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Application Note 24

The ST Author can add the additional role SOC for a Security Operations Center (SOC) and model it accordingly in the SFRs (i.e FMT_SMR.1, FDP_IFF.1, FDP_ACF.1, FIA_UAU.5). This additionally specified role is only allowed to have read access to the security-relevant log. All other security requirements regarding connections between the SOC and the TOE shall be the same as those between the RA and the TOE.

6.7 Class FPT: Protection of the TSF

6.7.1 FPT_FLS.1 Fail secure

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].*

].

6.7.2 FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1

The TSF shall provide unambiguous detection of physical tampering that can 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.

6.7.3 FPT_RPL.1 Replay detection

FPT_RPL.1.1

The TSF shall detect replay for the following entities: [*TCC, RA*].

FPT_RPL.1.2

The TSF shall perform [*ignore replayed data*] when replay is detected.

Hint

Replay detection for communication with V-ITS-S and PKI is not in the scope of this PP. For the communication to these external entities, the replay detection is not covered by individual SFRs but it is part of the functional specification and the respective communication standards.

6.7.4 FPT_STM.1 Reliable time stamps

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

Application Note 25

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 able to measure time in a granularity that is appropriate for the required TSF.

6.7.5 FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1

The TSF shall provide the capability to consistently interpret [*information about the validity of certificates and certificate lists (CTLs, CRLs)*] when shared between the TSF and ~~an~~other trusted IT product**s (V-ITS-S and servers that provide the certificates and/or certificate lists (CTLs, CRLs))**.

FPT_TDC.1.2

The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

Application Note 26

The ST author shall refine the interpretation rules in FPT_TDC.1.2 appropriately, based on the current version of [SecReq]. These interpretation rules must include verification of the signature of the certificates and certificate lists (CTLs, CRLs).

6.7.6 FPT_TST.1 TSF self-testing

FPT_TST.1.1

The TSF shall run a suite of the following self-tests [during initial start-up, periodically during normal operation, at the request of the authorized user, [selection: *at the conditions [assignment: conditions under which self-test should occur]*, ***none***]] to demonstrate the correct operation of [the TSF]: [assignment: *list of self-tests run by the TSF*].

FPT_TST.1.2

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

FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of [TSF].

6.8 Class FTP: Trusted Path/Channels

6.8.1 FTP_PRO.1/Backend Trusted channel protocol for the backend communication

FTP_PRO.1.1/Backend

The TSF shall implement [assignment: *trusted channel protocol*] acting as [assignment: *defined protocol role(s)*] in accordance with: [assignment: *list of standards*].

FTP_PRO.1.2/Backend

The TSF shall enforce usage of the trusted channel for [*[selection: communication with the TCC, communication with the RA, [assignment: additional purpose(s) of the trusted channel]]*] in accordance with: [assignment: *list of standards*].

FTP_PRO.1.3/Backend

The TSF shall permit [selection: *itself, its peer*] to initiate communication via the trusted channel.

FTP_PRO.1.4/Backend

The TSF shall enforce the following rules for the trusted channel: [assignment: *rules governing operation and use of the trusted channel and/or its protocol]*.

FTP_PRO.1.5/Backend

The TSF shall enforce the following static protocol options: [assignment: *list of options and references to standards in which each is defined*].

FTP_PRO.1.6/Backend

The TSF shall negotiate one of the following protocol configurations with its peer: [assignment: *list of configurations and reference to standards in which each is defined*].

Application Note 27

The TOE shall implement a trusted and protected communication channel to the RA and the TCC that shall be modelled in a variety of SFRs by the ST author. This channel shall be protected by adequate and state of the art security and cryptographic mechanisms. Suitable communication protocols are e.g. TLS [RFC8446], IPsec [RFC4301] or SSH [RFC4254]. Should one of these or another protocol be used, appropriate recommendations for cryptographic mechanisms from e.g. SOGIS or a certification authority shall be complied with.

For the protocols mentioned as an example, the following recommendations for cryptographic mechanisms of the BSI can be considered: [TR-02102-1] (general recommendations), [TR-02102-2] (TLS), [TR-02102-3] (IPsec), and [TR-02102-4] (SSH).

6.8.2 FTP_PRO.1/PKI Trusted channel protocol for the communication with the PKI

FTP_PRO.1.1/PKI

The TSF shall implement [*Authorization Requests/Responses and Enrolment Requests/Responses*] acting as [*requester*] in accordance with: [

ETSI TS 102 941 [ETSI TS 102 941],

[assignment: other standards or none]

].

FTP_PRO.1.2/PKI

The TSF shall enforce usage of the trusted channel for [*message exchanges (Authorization Requests/Responses and Enrolment Requests/Responses) with the PKI (Authorization Authority and Enrolment Authority)*] in accordance with: [

ETSI TS 102 941 [ETSI TS 102 941],

[assignment: other standards or none]

].

FTP_PRO.1.3/PKI

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

FTP_PRO.1.4/PKI

The TSF shall enforce the following rules for the trusted channel: [

- *Generation of random AES key and random nonce (using FCS_CKM.1/AES).*
- *Encryption/Decryption of request/response with AES-CCM (using FCS_COP.1/AES).*
- *The AES key is encrypted with ECIES utilizing the cryptographic functionality of the SE (by transferring the AES key and public key of the recipient to the SE).*
- *Transmission of the encrypted AES key, the authentication tag, the nonce, the encrypted request, and the ephemeral public key to the recipient.*
- *Reception of the encrypted response and authentication tag from the recipient.*
- *Validation of authentication by checking the authentication tag (AES-CCM) of the received respond (using FCS_COP.1/AES).*
- *[assignment: rules governing operation and use of the trusted channel and/or its protocol]*.

].

FTP_PRO.1.5/PKI

The TSF shall enforce the following static protocol options: [*None specified*].

FTP_PRO.1.6/PKI

The TSF shall negotiate one of the following protocol configurations with its peer: [*None specified*].

Hint

FTP_PRO.2 is not iterated for the PKI connection since the establishment of the AES key is based on ECIES and the calculation of ECIES is performed by the SE (and not by the TOE itself) (cf. FTP_PRO.2.1 as defined in [CC] Part 2). Furthermore, no cryptographic keys are derived from a shared secret (cf. FTP_PRO.2.3 as defined in [CC] Part 2). The primary data encryption key (AES) is encrypted with ECIES (by the SE) and then transmitted to the PKI as stated in [IEEE 1609.2]. The authentication is performed on both sides by validating the authentication tag of AES-CCM (cf. FTP_PRO2.2 as defined in [CC] Part 2).

6.8.3 FTP_PRO.2/Backend Trusted channel establishment for the backend communication

FTP_PRO.2.1/Backend

The TSF shall establish a shared secret with its peer using one of the following mechanisms: [assignment: *list of key establishment mechanisms*].

FTP_PRO.2.2/Backend

The TSF shall authenticate [its peer, itself to its peer] using one of the following mechanisms: [assignment: *list of authentication mechanisms*] and according to the following rules: [assignment: *list of rules for carrying out the authentication*].

FTP_PRO.2.3/Backend

The TSF shall use [assignment: *key derivation function*] to derive the following cryptographic keys from a shared secret: [assignment: *list of cryptographic keys*].

6.8.4 FTP_PRO.3/Backend Trusted channel data protection for the backend communication

FTP_PRO.3.1/Backend

The TSF shall protect data in transit from unauthorised disclosure using one of the following mechanisms: [assignment: *list of encryption mechanisms*].

FTP_PRO.3.2/Backend

The TSF shall protect data in transit from [modification, deletion, insertion, replay, [selection: *[assignment: other],* ***none***]] using one of the following mechanisms: [assignment: *list of integrity protection mechanisms*].

6.8.5 FTP_PRO.3/PKI Trusted channel data protection for the communication with the PKI

FTP_PRO.3.1/PKI

The TSF shall protect data in transit from unauthorised disclosure using one of the following mechanisms: [*AES-CCM*].

FTP_PRO.3.2/PKI

The TSF shall protect data in transit from [modification, deletion, insertion, replay] using one of the following mechanisms: [*AES-CCM*].

6.9 Security Assurance Requirements for the TOE

The minimum Evaluation Assurance Level for this Protection Profile is **EAL3.**

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

Assurance Class	Assurance Component
Development	ADV_ARC.1
	ADV_FSP.3
	ADV_TDS.2
Guidance Documents	AGD_OPE.1
	AGD_PRE.1
Life-Cycle Support	ALC_CMC.3
	ALC_CMS.3
	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 11: Assurance requirements

6.10 Security Requirements Rationale

This section 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	O.Log
FAU_GEN.1										X
FAU_GEN.2										X
FAU_SAR.1										X
FAU_STG.2										X
FAU_STG.5										X
FCS_COP.1/AES	X	X	X	X		X				
FCS_COP.1/Backend	X	X	X	X		X				
FCS_COP.1/Hash	X									
FCS_COP.1/SigVer	X	X				X				
FCS_COP.1/SigVerFW	X							X		
FCS_CKM.1/AES	X			X						
FCS_CKM.1/Backend	X			X						
FCS_CKM.5/Backend	X			X						
FCS_CKM.6	X									
FDP_ACC.1							X			
FDP_ACF.1							X			
FDP_IFC.2		X	X	X						

	O.Crypt	O.ReceiveAuthentificatedData	O.SendAuthenticatedData	O.SecureChannel	O.Protect	O.Authentication	O.Access	O.SecureFirmwareUpdate	O.Management	O.Log
FDP_IFF.1		X	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_MSA.1									X	
FMT_SMF.1									X	
FMT_SMR.1									X	
FPT_FLS.1					X					
FPT_PHP.1					X					
FPT_RPL.1				X						
FPT_STM.1										X
FPT_TDC.1					X	X				
FPT_TST.1					X					
FTP_PRO.1/Backend				X						
FTP_PRO.1/PKI				X						
FTP_PRO.2/Backend				X						
FTP_PRO.3/Backend				X						

	O.Crypt	O.ReceiveAuthentificatedData	O.SendAuthenticatedData	O.SecureChannel	O.Protect	O.Authentication	O.Access	O.SecureFirmwareUpdate	O.Management	O.Log
FTP_PRO.3/PKI				X						

Table 12: Security requirements rationale

The following paragraphs contain more details on this mapping.

6.10.1 O.Crypt

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

- **FCS_COP.1/AES** defines the requirements for the cryptographic algorithm AES-CCM used for the communication with the PKI.
- **FCS_COP.1/Backend** defines the requirements for the protection of the communication with the RA and the TCC.
- **FCS_COP.1/Hash** defines the requirements for the hash operations.
- **FCS_COP.1/SigVer** defines the requirements around the verification of signatures in C-ITS context.
- **FCS_COP.1/SigVerFW** defines the requirements on verification of the firmware update signature to ensure authenticity and integrity prior to installation.
- **FCS_CKM.1/AES** defines the requirements for the generation of the keys and the nonces used in the cryptographic algorithm AES-CCM.
- **FCS_CKM.1/Backend** defines the requirements on key generation for the communication with the RA and the TCC.
- **FCS_CKM.5/Backend** defines the requirements on key derivation for the communication with the RA and the TCC.
- **FCS_CKM.6** defines the requirements around the secure deletion of ephemeral cryptographic keys.

6.10.2 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 from V-ITS-S.
- **FCS_COP.1/AES** verifies incoming data from PKI (with AES-CCM).
- **FCS_COP.1/Backend** verifies incoming data from RA and TCC.

6.10.3 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.
- **FCS_COP.1/AES** defines a method for providing authentication assurance (AES-CCM).
- **FCS_COP.1/Backend** defines a method for providing authentication assurance.

6.10.4 O.SecureChannel

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

- **FCS_COP.1/AES** defines the cryptographic operations for the authenticated encryption and decryption for the communication with the PKI.
- **FCS_COP.1/Backend** defines the cryptographic operations for the secured backend channel.
- **FCS_CKM.1/AES** defines the cryptographic key generation for the secure channel with the PKI.
- **FCS_CKM.1/Backend** defines the cryptographic key generation for the secured backend channel.
- **FCS_CKM.5/Backend** defines the cryptographic key derivation for the secured backend channel.
- **FTP_PRO.1/Backend** defines the protocol for the trusted channel to the RA and TCC.
- **FTP_PRO.1/PKI** defines the protocol for the trusted channel to the PKI.
- **FTP_PRO.2/Backend** defines the establishment of the trusted channel to the RA and TCC.
- **FTP_PRO.3/Backend** defines the data protection mechanisms of the trusted channel to the RA and TCC.
- **FTP_PRO.3/PKI** defines the data protection mechanisms of the trusted channel to PKI.
- **FDP_IFC.2** defines the information flow control within the given architecture.
- **FDP_IFF.1** defines the corresponding security attributes.
- **FPT_RPL.1** defines the mechanism for a detected replay.

6.10.5 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** and **FIA_UAU.5** define the requirements around the authentication of users.
- **FIA_UID.2** defines requirements around the identification of users.
- **FCS_COP.1/SigVer** ensures authentication of data from V-ITS-S.
- **FCS_COP.1/Backend** ensures authentication of data from RA or TCC.
- **FCS_COP.1/AES** ensures authentication of data from PKI.
- **FPT_TDC.1** ensures authentication by validation of certificates of V-ITS-S.

6.10.6 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.

- **FIA_UID.2** defines requirements around the identification of users.

6.10.7 O.SecureFirmwareUpdate

O.SecureFirmwareUpdate is met by the following SFR:

- **FCS_COP.1/SigVerFW** verifies the firmware update signature to ensure authenticity and integrity prior to installation.

6.10.8 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_PHP.1** defines the requirements around the physical protection that the TOE has to provide.
- **FPT_TST.1** defines the self-testing functionality.
- **FPT_TDC.1** defines the requirements that the TOE correctly interprets information about the validity of certificates and certificate lists (CTLs, CRLs).

6.10.9 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** and **FIA_UAU.5** define the 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.

6.10.10 O.Log

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

- **FAU_GEN.1** defines the necessary audit data generation.
- **FAU_GEN.2** defines the corresponding user identity association.
- **FAU_SAR.1** defines the requirements around the audit review functions for the log and that access to them shall be limited to RAs via IF_GW_Admin only.
- **FAU_STG.2** defines the protection of the audit data.
- **FAU_STG.5** defines the requirements on what should happen if the audit log is full.
- **FPT_STM.1** defines the requirement on reliable time stamps.

6.10.11 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

SFR	Dependencies	Fulfilled by
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.2	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.5	FAU_STG.2 Protected audit data storage	FAU_STG.2
FCS_COP.1/AES	[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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	FCS_CKM.1/AES 2nd dependency is not relevant since the used cryptographic keys are not stored outside of the TOE.
FCS_COP.1/Backend	[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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	FCS_CKM.1/Backend 2nd dependency is not relevant since it is assumed that keys are not stored outside the TOE. Should cryptographic keys be stored outside the TOE, it has to be modelled by the ST author (see Application Note 15).
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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	The hash algorithm does not need any key material. Therefore, for this SFR, there is no dependency on an import or generation of key material and a key access.
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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	1st dependency does not need to be fulfilled, as there is no direct import, generation, or derivation of the public key of the sender's certificate for the verification of the corresponding messages. The interpretation of the

SFR	Dependencies	Fulfilled by
		certificates is performed by FPT_TDC.1. 2nd dependency is not relevant since the used cryptographic keys are not stored outside of the TOE.
FCS_COP.1/SigVerFW	[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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	1st dependency needs to be fulfilled within the production phase of the TOE, during the implementation of the corresponding key value. 2nd dependency is not relevant since the used cryptographic keys are not stored outside of the TOE.
FCS_CKM.1/AES	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction	FCS_COP.1/AES 2nd dependency is not relevant since the used cryptographic keys are not stored outside of the TOE. 3rd dependency is not relevant since it is assumed that the keys are generated utilizing random source of the SE. Should another random source be used, it has to be modelled by the ST author (see Application Note 18). FCS_CKM.6
FCS_CKM.1/Backend	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction	FCS_CKM.5/Backend FCS_COP.1/Backend 2nd dependency is not relevant since it is assumed that keys are not stored outside the TOE. Should cryptographic keys be stored outside the TOE, it has to be modelled by

SFR	Dependencies	Fulfilled by
		the ST author (see Application Note 15). 3rd dependency is not relevant since it is assumed that the keys are generated utilizing random source of the SE. Should another random source be used, it has to be modelled by the ST author (see Application Note 18). FCS_CKM.6
FCS_CKM.5/Backend	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.6 Timing and event of cryptographic key destruction	FCS_COP.1/Backend FCS_CKM.6
FCS_CKM.6	[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.1/AES FCS_CKM.1/Backend
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 20).
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 21).
FDP_RIP.1	-	-
FIA_ATD.1	-	-
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UAU.5	-	-
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
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FPT_FLS.1	-	-
FPT_PHP.1	-	-
FPT_RPL.1	-	-
FPT_STM.1	-	-
FPT_TDC.1	-	-
FPT_TST.1	-	-
FTP_PRO.1/Backend	FTP_PRO.2 Trusted channel establishment FTP_PRO.3 Trusted channel data protection.	FTP_PRO.2/Backend FTP_PRO.3/Backend
FTP_PRO.1/PKI	FTP_PRO.2 Trusted channel establishment FTP_PRO.3 Trusted channel data protection.	In the defined protocol, no shared secret is generated for

SFR	Dependencies	Fulfilled by
		encryption using a key derivation function. Therefore, FTP_PRO.2 is not used. For more information refer to the Hint at FTP_PRO.1/ PKI. FTP_PRO.3/PKI
FTP_PRO.2/Backend	FTP_PRO.1 Trusted channel protocol [FCS_CKM.1 Cryptographic key generation, or FCS_CKM.2 Cryptographic key distribution] FCS_CKM.5 Cryptographic key derivation FCS_COP.1 Cryptographic operation	FTP_PRO.1/Backend FCS_CKM.1/Backend FCS_CKM.5/Backend FCS_COP.1/Backend
FTP_PRO.3/Backend	FTP_PRO.1 Trusted channel protocol FTP_PRO.2 Trusted channel establishment FCS_COP.1 Cryptographic operation.	FTP_PRO.1/Backend FTP_PRO.2/Backend FCS_COP.1/Backend
FTP_PRO.3/PKI	FTP_PRO.1 Trusted channel protocol FTP_PRO.2 Trusted channel establishment FCS_COP.1 Cryptographic operation.	FTP_PRO.1/PKI In the defined protocol, no shared secret is generated for encryption using a key derivation function. Therefore, FTP_PRO.2 is not used. For more information refer to the Hint at FTP_PRO.1/ PKI. FCS_COP.1/AES

Table 13: SFR dependencies

6.10.12 Security Assurance Requirements Rationale

6.10.12.1 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 EAL2 and EAL3.

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 EAL3 as the assurance level in this Protection Profile.

6.10.12.2 Dependencies of Assurance Components

The dependencies of the assurance requirements taken from EAL3 are fulfilled automatically.

7 Appendix

7.1 Glossary & Specific Terms

Term	Description
AA	Authorisation Authority A CA that provides a C-ITS station with authoritative proof that it may use specific ITS services (according to [CP]).
AES	Advanced Encryption Standard
Application Note	Application Note An application note defines the restrictions and requirements that shall be performed by the ST author.
CA	Certificate Authority or Certification Authority An entity that issues digital certificates.
CAM	Cooperative Awareness Messages
CCM	Counter with Cipher Block Chaining-Message Authentication Code
C-ITS	Cooperative ITS
C-ITS Station	C-ITS Station A set of hardware and software components required to collect, store, process, receive and transmit secured and trusted messages in order to enable the provision of a C-ITS service. This includes personal, central, vehicle and roadside ITS stations as defined in [ETSI EN 302 665].
C-ITS-S	Central ITS Station Fixed control station with network connection to R-ITS-S, potentially connecting to further (backend) systems.
CP	Certificate Policy, also see [CP]
CRL	Certificate Revocation List
CTL	Certificate Trust List
DENM	Decentralised Environmental Notification Message
EA	Enrolment Authority A CA that authenticates a C-ITS station and grants it access to ITS communications (according to [CP]).
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm

Term	Description
ECIES	Elliptic Curve Integrated Encryption Scheme
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.
GSM	Global System for Mobile Communications
Hint	Hint Hints are intended to help the reader of the PP to gain a further understanding. In addition, they contain rationales of the PP author.
IEEE	Institute of Electrical and Electronics Engineers
IPsec	Internet Protocol Security IPsec extends the Internet Protocol (IP) with encryption and authentication mechanisms. It is specified in [RFC4301], among others.
ISMS	Information Security Management System
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.
ITS-G5	ITS-G5 Intelligent Transport Systems operating in the 5 GHz frequency band.
ITS-M	ITS-Messages Collective term for all messages and message formats used in the C-ITS context.
ITS-S	Intelligent Transportation Systems – Station Station within the C-ITS context. Covering the following station types: • C-ITS-S (Central ITS Station), • P-ITS-S (Personal ITS Station), • R-ITS-S (Roadside ITS Station), and • V-ITS-S (Vehicle ITS Station).
IVIM	In Vehicle Information Message
LAN	Local Area Network
LTE	Long Term Evolution
MAPEM	MAP Extended Message
NIST	National Institute of Standards and Technology

Term	Description
PII	Personally Identifiable Information PII 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.
PP	Protection Profile
PKI	Public Key Infrastructure A PKI is a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption. In the context of this PP, the term refers to a PKI according to the [CP].
RA	Roadside ITS Station Administrator
RGW	Roadside ITS Station Gateway
R-ITS-S	Roadside ITS Station ITS computing platform, including the TOE (RGW), a communication and processing capacity, linked to road infrastructure.
RNG	Random Number Generation
RTC	Real Time Clock
SE	Secure Element A security device utilised by the gateway for cryptographic operations.
SFP	Security Function Policies
SFR	Security Functional Requirement
SOC	Security Operations Center A SOC has the task of detecting threats at an early stage and reacting to them. This can be set up within the organisation itself or be outsourced.
SP	Security Policy, also see [SP]
SPD	Security Problem Definition
SPATEM	Signal Phase And Timing Extended Message
SSEM	Signal request Status Extended Message
SSH	Secure Shell SSH is a network protocol for secure remote login and other secure network services over an insecure network. This protocol is specified in [RFC4254], among others.
ST	Security Target

Term	Description
TCC	Traffic Control Center
TLM	Trust List Manager Role according to [CP]
TLS	Transport Layer Security TLS is a protocol used to encrypt, verify and authenticate communication in a network. This protocol is specified in [RFC8446].
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UMTS	Universal Mobile Communications System
V-ITS-S	Vehicle ITS Station ITS computing platform, communication, and processing capacity, linked to a vehicle.
WAN	Wide Area Network

1267 **Table 14: Glossary & specific terms**

1268

7.2 References

[CC] Common Criteria for Information Technology Security Evaluation, consisting of:

- Part 1: Introduction and general model, November 2022, Version CC:2022, Revision 1
- Part 2: Security functional requirements, November 2022, Version CC:2022, Revision 1
- Part 3: Security assurance requirements, November 2022, Version CC:2022, Revision 1
- Part 4: Framework for the specification of evaluation methods and activities, November 2022, Version CC:2022, Revision 1
- Part 5: Pre-defined packages of security requirements, November 2022, Version CC:2022, Revision 1

URL: https://www.commoncriteriaportal.org/cc/

[CP] C-ITS Certificate Policy, current version from https://cpoc.jrc.ec.europa.eu/Documentation.html

[CSP-PP] Protection Profile “Cryptographic Service Provider (CSP)”, version 0.9.8, BSI-CC-PP-0104-2020, February 2020

[ETSI EN 302 663] ETSI EN 302 663, Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band, current version

[ETSI EN 302 665] ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture, current version

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

[ETSI TS 103 097] ETSI TS 103 097, Intelligent Transport Systems (ITS); Security; Security header and certificate formats, current version

[FIPS 180-4] FIPS PUB 180-4, Secure Hash Standard (SHS), August 2015

[FIPS 186-4] FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013

[FIPS 197] FIPS 197, Advanced Encryption Standard (AES), November 2001

[IEEE 1609.2] IEEE Std 1609.2™-2022 IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, March 2023

[ISO27001] ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection – Information security management systems – Requirements, edition 3, October 2022

[NIST SP 800-38C] NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, July 2007

[RFC4254] RFC 4254, The Secure Shell (SSH) Connection Protocol, January 2006

[RFC4301] RFC 4301, Security Architecture for the Internet Protocol, December 2005

[RFC5639]	RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010
[RFC8446]	RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3, August 2018
[SE-PP]	Protection Profile “V2X Hardware Security Module by CAR 2 CAR Communication Consortium”, version 1.0.1, BSI-CC-PP-0114-2021, November 2021
[SecReq]	“C-ITS Security Requirements & Specifications” issued by C-Roads, current version, https://www.c-roads.eu
[SP]	C-ITS Security Policy, current version from https://cpoc.jrc.ec.europa.eu/Documentation.html
[TR-02102-1]	Technical Guideline TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths, current version
[TR-02102-2]	Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths, Part 2 – Use of Transport Layer Security (TLS), current version
[TR-02102-3]	Technical Guideline TR-02102-3 Cryptographic Mechanisms: Recommendations and Key Lengths, Part 3 – Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2), current version
[TR-02103-4]	Technical Guideline TR-02102-4 Cryptographic Mechanisms: Recommendations and Key Lengths, Part 4 – Use of Secure Shell (SSH), current version