DG JRC – Directorate E – Space, Security and Migration
Cyber and Digital Citizens' Security Unit E3

Common Criteria Protection Profile

Digital Tachograph – External GNSS Facility (EGF PP)

Compliant with Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 (Annex 1C)

Version 1.0, 9 May 2017

Foreword

This Protection Profile (PP) has been developed to outline the IT security requirements as defined in the Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council [5], Annex 1C, using the Common Criteria (CC) language and format (CC version 3.1, Revision 4 ([1], [2], [3])). This is to enable developers of External GNSS Facilities (EGFs) to create their specific Security Target document according to CC, in order for the products to undergo a CC evaluation and certification process. The CC EFG certificate is one pre-requisite to obtain type approval for an External GNSS Facility.

The development of the PP has been sponsored by the Joint Research Centre of the European Commission. The PP has been approved by the governmental IT security certification bodies organised within the Joint Interpretation Working Group (JIWG), which supports the mutual recognition of certificates under the umbrella of the European SOGIS-MRA (Agreement on Mutual Recognition of Information Technology Security Evaluation Certificates.)

The PP supports the intent of the European Commission to ensure a common and comparable level of assurance for the technical components of the Digital Tachograph System in Europe. This PP reflects the security requirements of Annex I C to the Regulation [5]. Detail is added to the security requirements, but in the event of any conflict the wording of the Regulation shall prevail.

Notes and comments to this Protection Profile should be referred to:

European Commission
DG JRC – Directorate E – Space, Security and Migration
Cyber and Digital Citizens' Security Unit E3

PP Context

This section is informative and does not form part of the protection profile requirements.
Reference [5] identifies the need for a family of protection profiles covering the major elements of digital tachograph operation:

- A Protection Profile for vehicle units,
- A Protection Profile for tachograph cards,
- A Protection Profile for motion sensors,
- A Protection Profile for external GNSS facilities (EGF).

This document contains the protection profile for the EGF only. As the EGF is required to interface with the vehicle unit there is a need for alignment of the security functional requirements between them. For this reason the security functional requirements are presented in a modular manner, such that the consistency within the set of documents can be more easily determined.
The following diagram illustrates the operational environment, and the relationship between the protection profiles.

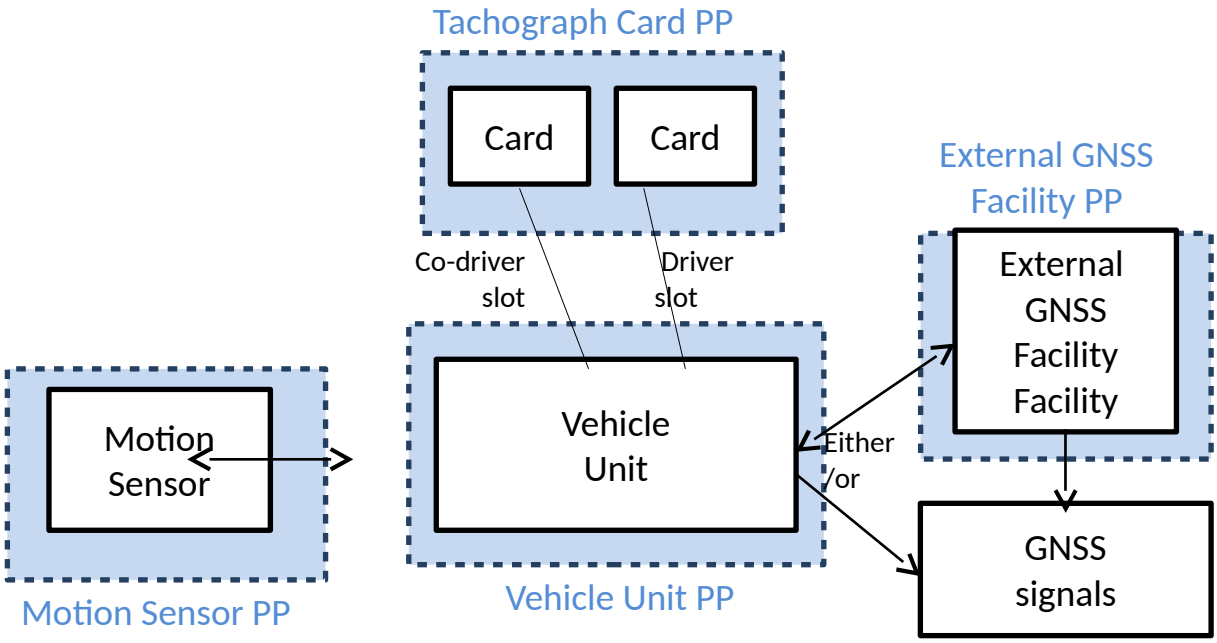

Figure 1: Protection Profile context

The motion sensor monitors the vehicle gearbox and provides signals to the vehicle unit that are representative of vehicle movement and speed. The vehicle unit processes and stores the input data, associates data with human users, and provides external connectivity. Tachograph cards identify and authenticate human users to the vehicle unit, and provide data storage.
A GNSS receiver receives GNSS satellite signals and based on those calculates the vehicle's position and speed, among other quantities. The GNSS receiver can be within the same physical boundary as the vehicle unit. Alternatively, the receiver may have separate physical boundary in the form of an External GNSS Facility (EGF). As mentioned in [5] Annex 1C, the EGF, if present, is considered to be a part of the vehicle unit. When the GNSS receiver is within the same physical boundary as the vehicle unit, its security is addressed by the VU PP [6]. When it has a separate physical boundary its protection is addressed by the current PP.

An External GNSS Facility can only be part of a second-generation digital tachograph system. First-generation vehicle units do not support GNSS-based determination of location and speed and hence cannot be connected to an External GNSS Facility.

Table of Contents

Table of Tables

Table of Figures

Revision history

Version	Date	Changes
1.0	9 May 2017	

1 PP Introduction

1 This section provides document management and overview information being required to register the protection profile and to enable a potential user of the PP to determine whether the PP is of interest.

2 Requirements listed in [5] Annex 1C or its Appendices, but not included in this protection profile, are not the subject of security certification.

3 The EGF general architecture and functions are described in [5] Annex 1C, Appendix 12.

1.1 PP Reference

4

Title:	Common Criteria Protection Profile: Digital Tachograph – External GNSS Facility (EGF PP)
Sponsor:	Joint Research Centre, European Commission
Editors:	Julian Straw, David Bakker, Jacques Kunegel, Luigi Sportiello
CC version:	3.1 (Revision 4)
Assurance level:	EAL4 augmented with ATE_DPT.2 and AVA_VAN.5
Version number:	1.0
Registration:	BSI-CC-PP-0092
Keywords:	Digital Tachograph, External GNSS Facility

1.2 TOE overview

1.2.1 TOE definition and operational usage

5 The Target of Evaluation (TOE) addressed by this protection profile is an External GNSS Facility in the sense of [5] Annex 1C. It is intended to be used[1] within a digital tachograph system. Digital tachograph systems contain vehicle units, motion sensors, tachograph cards, remote communication facilities (if applicable), remote early detection communication readers, etc.

6 If the vehicle unit is used with an external GNSS facility, the external GNSS facility is considered to be a part of the vehicle unit. When the GNSS receiver is within the same physical boundary as the vehicle unit, its security is covered by the Protection Profile for the Vehicle Unit [6]. When it has a separate physical boundary in the form of an EGF, its protection is addressed through the current PP.

7 A External GNSS Facility is a facility which comprises:

a) A GNSS receiver, capable of calculating its geographic location, speed and other quantities based on signals received from satellites forming a Global Navigation Satellite System (GNSS);

1 The use of an External GNSS Facility is optional, the other option being the inclusion of the GNSS receiver into the vehicle unit itself. See [5] Annex 1C, Appendix 12 for more details. It is up to a VU manufacturer to choose one of these options.

b) A GNSS Secure Transceiver, capable of receiving data from the GNSS receiver over an internal interface and storing this data in an ISO 7816-4:2013 compliant file structure;
c) An enclosure system with tamper detection/tamper evidence function, which encapsulates both the GNSS receiver and the GNSS Secure Transceiver;
d) A GNSS antenna either installed on the vehicle and connected to the GNSS receiver or internal to the External GNSS Facility; and
e) The associated guidance documentation.

8 The GNSS Secure Transceiver allows the VU to which it is coupled[2] to read data from its file structure over a physical interface compliant to ISO 7816-12:2005 or to another specification able to support ISO 7816-4:2013. That interface is also compliant to ISO 7816-4:2013 and [5] Annex 1C, Appendix 12, Section 4.2, and to the security mechanisms specified in [5] Annex 1C, Appendix 11, Chapter 11.

9 The basic functions of the External GNSS Facility are to calculate and store the vehicle's location and speed, as well as related quantities such as date and time (so-called RMC data) and receiver status and information on the Global Navigation Satellite System itself (so-called GSA data)[3], and to make this information available to the vehicle unit. The data available to the vehicle unit, through the secure communication specified in [5] Annex 1C, Appendix 12, is not intended to be available to any other entity. However, this does not preclude the provision of other connections that allow access to the received GNSS data. Any such connections must be described in the security target.

10 Concerning write access, during the operational phase of an External GNSS Facility lifecycle (as described in section 1.2.3 of this PP), only data coming from the GNSS receiver internal to the EGF may be written to the EGF's memory.

11 The functional requirements for an External GNSS Facility are specified in [5] Annex 1C, Appendix 12, and the common security mechanisms are specified in [5] Annex 1C, Appendix 11.

1.2.2 TOE major security features for operational use

12 The main security features of the TOE are as follows:

a) The TOE must preserve EGF identification data and security data stored during the manufacturing phase, and identification data of the VU coupled to the EGF stored during the calibration phase;
b) The TOE must preserve RMC sentences and GSA sentences coming from its internal GNSS receiver and stored in the EGF's memory;
c) The TOE must authenticate to the VU to demonstrate that it is an authentic EGF;
d) The TOE must provide a reliable source of authenticated GNSS data to the VU.

13 Specifically the External GNSS Facility aims to:

a) Protect the stored GNSS data against unauthorised access and manipulation;

2 See [5] Annex 1C, Appendix 11 for a description of the coupling mechanism between an EGF and a VU.
3 See [5] Annex 1C, Appendix 12 for a full overview.

b) Detect any such attempts at unauthorized access to and manipulation of GNSS data;
c) Protect the integrity and authenticity of GNSS data exchanged between the vehicle unit and the External GNSS Facility;
d) Protect the authenticity and confidentiality of security data.

14 The main security features stated above are provided by the following major security services:

a) Vehicle unit identification and authentication during the coupling process[4];
b) Access control to functions and stored data;
c) Integrity of stored GNSS data;
d) Reliability of services, including self-testing, physical protection, control of executable code, resource management, and secure handling of events;
e) Data exchange with a coupled Vehicle Unit;
f) Cryptographic support for VU-EGF mutual authentication and secure messaging, including key generation and key agreement, according to [5] Annex 1C, Appendix 11
g) Protection of the authenticity and confidentiality of security data.

15 All cryptographic mechanisms, including algorithms and the length of corresponding keys, have to be implemented exactly as required and defined in [5] Annex 1C, Appendix 11.

Application note 1: Requirement GNS_3 in [5] Annex 1C, Appendix 12 specifies that the GNSS receiver shall have the capability to support authentication on the Open Service of Galileo when such service will be provided by the Galileo system, and supported by GNSS receiver manufacturers. The security mechanisms to support the authentication shall be entirely and autonomously managed by the GNSS receiver enclosed in the External GNSS Facility and are not within the scope of this PP.

1.2.3 TOE type

16 The TOE is an External GNSS Facility, forming part of a Digital Tachograph in the sense of [5] Annex 1C, intended to be used within a digital tachograph system.

17 The TOE is conformant with the following standards:

ISO/IEC 7816 Identification cards – Integrated circuit cards
i) Part 4: Organisation, security and commands for interchange (2013);
ii) Part 8: Commands and mechanisms for security operations.

For the physical layer of the communication with the vehicle unit the TOE supports ISO/IEC 7816-12:2005 or another (identified) standard able to support ISO/IEC 7816-4:2003.

18 The typical TOE lifecycle is depicted in Figure 2.

4 The TOE will verify whether the connected vehicle unit possesses appropriate credentials showing that it belongs to the digital tachograph system.

19 The initialisation step shown in Figure 2 refers to the creation of the file structure defined in [5] Annex 1C, Appendix 12, which may involve the installation of an application or the creation of the MF and the other files. It also includes the assignment of:

a) the extended serial number of the external GNSS facility;
b) the operating system identifier of the GNSS facility;
c) the type approval number of the external GNSS facility;
d) the identifier of the security component of the external GNSS facility.

20 The security data referred to in Figure 2 consists of (see Annex A for definitions of abbreviations used):

a) The EGF_MA key pair and corresponding certificate;
b) The MSCA_VU-EGF certificate containing the MSCA_VU-EGF.PK public key to be used for verification of the EGF_MA certificate;
c) The EUR certificate containing the EUR.PK public key to be used for verification of the MSCA_VU-EGF certificate;
d) The EUR certificate whose validity period directly precedes the validity period of the EUR certificate to be used to verify the MSCA_VU-EGF certificate, if existing;
e) The link certificate linking these two EUR certificates, if existing.

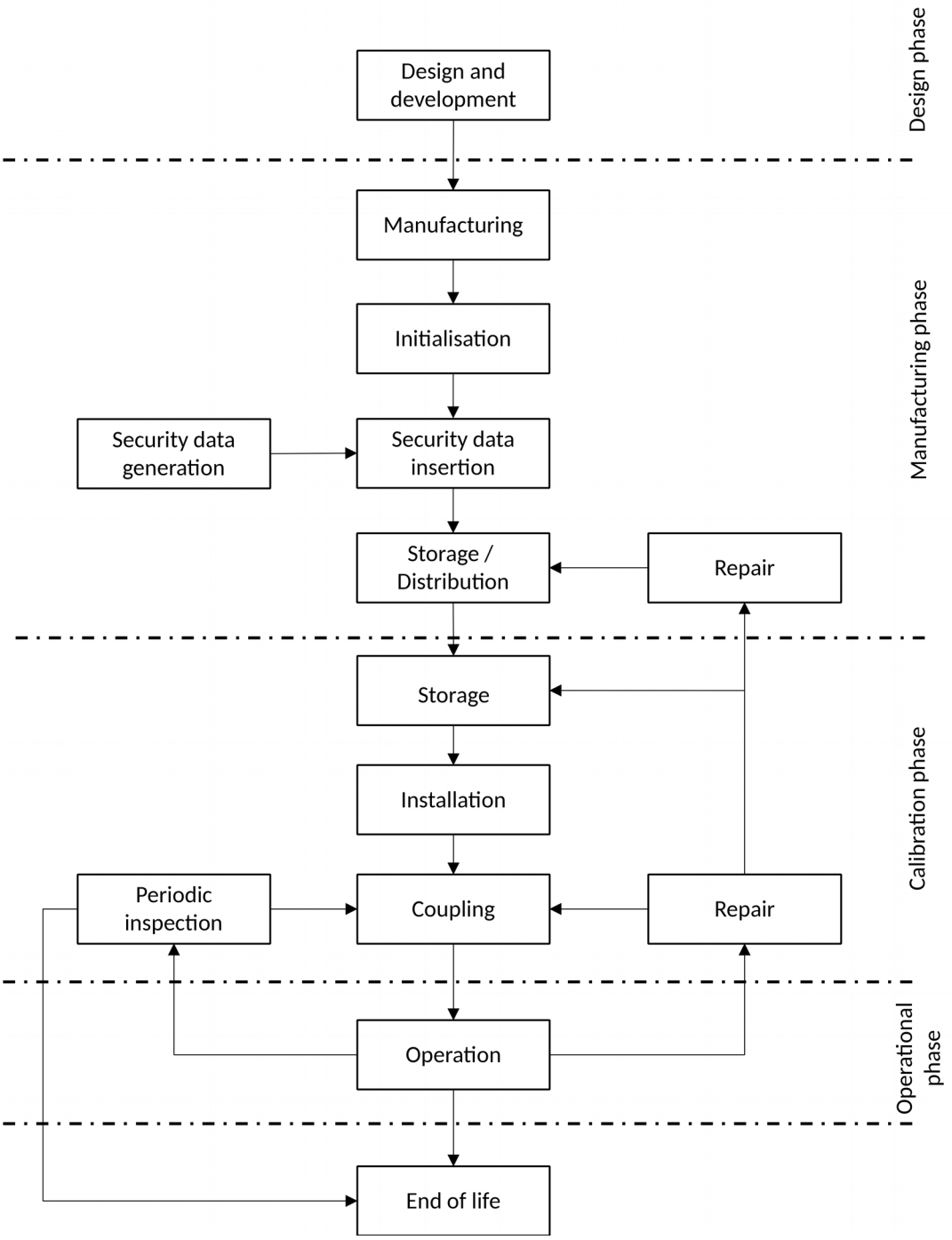

Figure 2 TOE lifecycle

21 The coupling step shown in Figure 2 refers to the coupling process of the TOE to a VU, as described in [5] Annex 1C, Appendix 11.

22 The security policy defined by the current protection profile focuses on the operational phase. However, some properties of the manufacturing and calibration phases, being significant for the security of the TOE in its operational phase, are also considered by the current PP.

23 A security evaluation/certification conformant to this PP will have to consider all life phases to the extent required by the assurance package chosen here for the TOE (see section 6.2 below).

1.2.4 Non-TOE hardware/software/firmware

24 Figure 3 shows the operational environment of the External GNSS Facility. Note that the internal architecture shown for the TOE is not mandatory, and an alternative diagram can be provided in the security target.

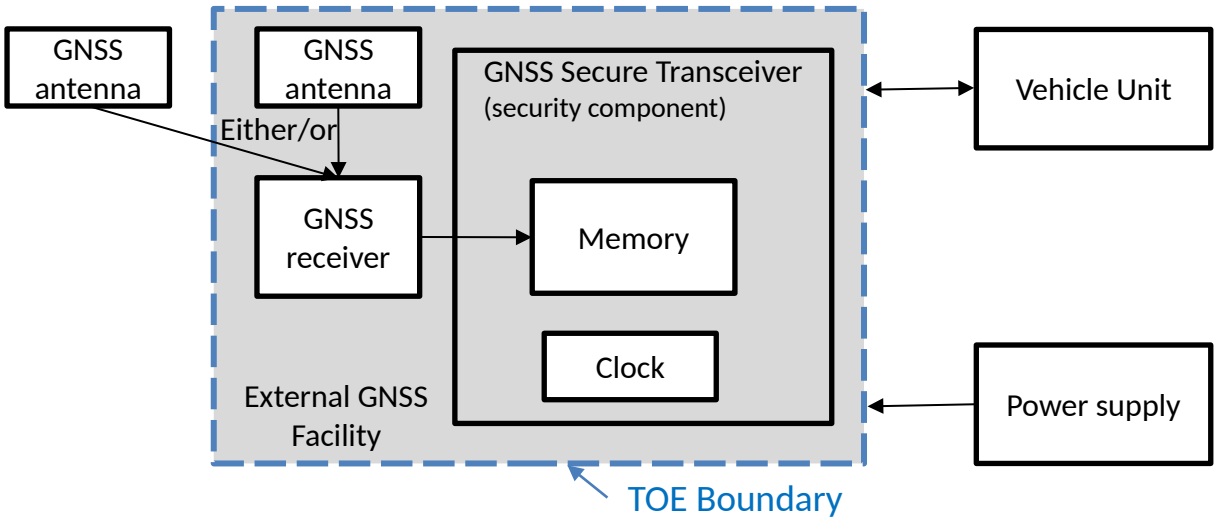

Figure 3 - EGF operational environment

25 The following TOE-external components are mandatory for a proper TOE operation:

a) A power supply;
b) A connection that allows communication with a vehicle unit, complying with [5] Annex 1C, Appendix 12;
c) A connection to an external antenna to receive GNSS signals, if such antenna is not internal to the EGF.

2 Conformance Claims

2.1 CC conformance claim

26 This protection profile claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 4, September 2012 [1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 4, September 2012 [2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 4, September 2012 [3],

as follows:

Part 2 extended,

Part 3 conformant (EAL4 augmented by ATE_DPT.2 and AVA_VAN.5).

2.2 PP claim

27 This protection profile does not claim conformance to any other protection profile.

2.3 Package claim

28 This protection profile claims conformance to the assurance package defined in [5] Annex 1C, Appendix 10, as follows:
“SEC_006 The assurance level for each Protection Profile shall be EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5”.

2.4 Conformance claim rationale

29 This protection profile does not claim any conformance with other protection profiles. Therefore, no conformance claim rationale is provided here.

2.5 Conformance statement

30 This protection profile requires *strict* conformance of any security target or protection profile claiming conformance to this protection profile.

3 Security problem definition

3.1 Introduction

3.1.1 Assets

31 The primary assets to be protected by the TOE and its environment within the operational phase of the TOE's life-cycle are the application data defined in the table below.

No.	Asset	Definition
1	GNSS data	Data received from a GNSS receiver, stored and provided by the TOE to the coupled vehicle unit. The data relates to position (latitude and longitude), time and speed over ground, receiver status and information on the GNSS system itself.

Table 1 - Primary asset

32 The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are:

No.	Asset	Definition
2	TOE stored secret security data	Secret security elements used by the TOE in order to enforce its security functionality. These include private and symmetric keys. (See Annex A)
3	TOE stored non-secret security data	Non-secret security elements used by the TOE in order to enforce its security functionality. These include public keys and certificates. (See Annex A)
4	Identification data	Name of manufacturer, serial number, approval number, operating system identifier.
5	TOE design and software code	Design information and source code (uncompiled or reverse engineered) for the TOE that could facilitate an attack.
6	TOE hardware	Hardware used to implement and support TOE functions.

Table 2 - Secondary assets

3.1.2 Subjects and external entities

33 This Protection Profile considers the following subjects, who can interact with the TOE.

No.	Subject	Definition
1	Vehicle Unit	The Vehicle Unit coupled, or to be coupled, with the TOE.

No.	Subject	Definition
2	GNSS satellites	One or more satellites from which the TOE receives signals.
3	Attacker	Entity (human or non-human) attempting to interfere with the operation of the TOE. The attacker is assumed to possess at most a *high* attack potential.

Table 3 - Subjects and external entities

3.2 Threats

34 This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats arise from the assets protected by the TOE and the method of TOE's use in the operational environment.

35 The threats are defined in the following table.

Label	Threat
T.Environment	**Environmental attacks** – An attacker could compromise the availability, integrity or authenticity of GNSS data through physical attacks on the TOE (thermal, electromagnetic, optical, chemical, mechanical, power supply).
T.Hardware	**Modification of hardware** - An attacker could modify the TOE hardware, and thereby compromise the availability, accuracy or authenticity of GNSS data.
T.GNSS_Data	**Interference with GNSS data** - An attacker could add to, modify or delete the stored GNSS data, and thereby compromise the availability, integrity or authenticity of GNSS data supplied to the VU.
T.Security_Data	**Access to security data** - An attacker could gain illicit knowledge of, or modify secret security data during security data generation or transport or storage in the TOE, thereby allowing a substitute device to be connected, or preventing access to GNSS data by the VU.
T.Software	**Attack on software** - An attacker could modify TOE software code during operation, and thereby compromise the availability, integrity or authenticity of GNSS data.
T.Tests	**Invalid test modes** - The use by an attacker of non-invalidated test modes or of existing back doors could compromise GNSS data.

Table 4 - Threats

3.3 Assumptions

36 This section describes the assumptions that are made about the operational environment in order to be able to provide the security functionality. If the TOE is placed in an

operational environment that does not uphold these assumptions it may be unable to operate in a secure manner.

37 The assumptions are provided in the following table.

Label	Assumption
A.Installation	**Installation Phase Security -** All data structures and security data on the TOE are correct according to [5] Annex 1C, and are handled correctly so as to preserve the integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys for the end-usage (in accordance with the cryptographic algorithms specified for an EGF) and their confidential handling. The manufacturer controls all materials, equipment and information, which is used for initialisation of an authentic EGF, in order to prevent counterfeit of the TOE.
A.Type_Approved	**Type Approved VU** - The EGF will only be operated together with a vehicle unit being type approved according to [5] Annex 1C.[5]

Table 5 - Assumptions

3.4 Organisational security policies

38 This section shows the organisational security policies that are to be enforced by the TOE, its operational environment, or a combination of the two.

39 The organisational security policies are provided in the following table.

Label	Organisational Security Policy
P.Crypto	The cryptographic algorithms and keys described in [5] Annex 1C, Appendix 11 shall be used where data confidentiality, authenticity or integrity need to be protected.

Table 6 - Organisational security policies

5 Type approval requirements include Common Criteria certification against the relevant protection profile.

4 Security Objectives

40 This section identifies the security objectives for the TOE and for its operational environment. The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition. The role of the security objectives is threefold:

- Provide a high-level, natural language solution of the problem;
- Divide this solution into two part-wise solutions, that reflect that different entities each have to address a part of the problem;
- Demonstrate that these part-wise solutions form a complete solution to the problem.

4.1 Security objectives for the TOE

41 The TOE security objectives address the protection to be provided by the TOE, independent of the TOE environment, and are listed in the table below.

Label	Security objectives for the TOE
O.EGF_Main	**Integrity and authenticity of data** - The TOE must ensure the integrity and authenticity of GNSS data made available to the coupled VU, so as to allow this VU to determine fully and accurately the location and movement of the vehicle.
O.Access	**Access to data** - The TOE must control access to GNSS data secret security data, software code and hardware.
O.Audit	**Audit** – The TOE must detect and provide evidence of breaches of its physical security.
O.Authentication	**Authenticated access** – The TOE must authenticate a connected VU before allowing access to data (GNSS data and secret security data) and functions.
O.Reliability	**Reliable service** -The TOE must provide a reliable service.
O.Secure_Communication	**Secure data transfer** - The TOE must secure all data exchanges with the vehicle unit.
O.Physical	**Physical protection** - The TOE must resist attempts to modify the stored or transferred GNSS data through physical attacks on the TOE hardware.
O.Crypto_Implement	**Cryptographic operation** – The cryptographic functions must be implemented within the TOE as required by [5] Annex 1C, Appendix 11.
O.Software_Update	**Software updates** - Where updates to TOE software are possible, the TOE must accept only those that are authorised.[6]

6 Implementation of a software update facility is optional for developers, but, if implemented the requirements of this PP must be met. Where software update is implemented in the TOE the ST author must add iterations of

4.2 Security objectives for the operational environment

42 The security objectives for the operational environment address the protection that must be provided by the TOE environment, independent of the TOE itself, and are listed in the table below.

Specific environment	Label	Security objective for the environment
Design environment	**OE.Development**	**Responsible development** - Developers must ensure that the assignment of responsibilities during TOE development is done in a manner which maintains IT security.
Manufacturing environment	**OE.Manufacturing**	**Protection during manufacture** - Manufacturers must ensure that the assignment of responsibilities during manufacturing of the TOE is done in a manner that maintains IT security, and that during the manufacturing process the TOE is protected from physical attacks that might compromise IT security.
	OE.Data_Generation	**Access to algorithms** - Security data generation algorithms must be accessible to authorised and trusted persons only.
	OE.Data_Transport	**Handling of security data** - Security data must be generated, transported, and inserted into the TOE in such a way as to preserve its appropriate confidentiality and integrity.
	OE.Delivery	**Protection during delivery** – Manufacturers of the TOE, vehicle manufacturers and fitters or workshops must ensure that handling of the TOE is done in a manner that maintains IT security.
	OE.Data_Strong	**Strong cryptography** - Security data inserted into the TOE must be as cryptographically strong as required by [5] Annex 1C, Appendix 11, Part B.
	OE.Test_Points	**Disabled test points** - All commands, actions or test points, specific to the testing needs of the manufacturing phase of the EGF must be disabled or removed before the end of the manufacturing process.

FCS components to describe the approach employed to protect the authenticity and integrity of the update.

Specific environment	Label	Security objective for the environment
Calibration environment	**OE.Approv_Workshops**	**Use of approved workshops** - Installation and repair of the TOE must be carried out by trusted and approved fitters or workshops.
	OE.Faithful_Calibration	**Correct coupling** - Approved fitters and workshops must correctly couple the TOE with a vehicle unit during calibration.
Operational environment	**OE.Regular_inspection**	**Regular inspections** – The TOE must be periodically inspected to detect any interference with its operation.
	OE.Crypto_Admin	**Implementation of cryptography** –All requirements from [5] Annex 1C, Appendix 11 concerning handling and operation of the cryptographic algorithms and keys must be fulfilled.
	OE.Type_Approved_VU	**Type Approved VU** - The vehicle unit connected to the TOE must be type approved according to [5] Annex 1C.
	OE.Antenna_Clear	**GNSS Antenna** – The GNSS antenna must be connected, and sited to allow receipt of GNSS signals.
	OE.EOL	**End of life** – When no longer in service the TOE must be disposed of in a secure manner, which means, as a minimum, that at least the confidentiality of symmetric and private cryptographic keys has to be safeguarded.

5 Extended Components Definition

43 This protection profile uses a component that is defined as an extension to CC Part 2.

44 The extended component is FCS_RNG.1 Random number generation. This component is defined and justified in [8] Section 3. This PP defines a restricted set of ways in which the extended component can be used in a security target. These are set out in Annex B, and further information is provided in [8].

5.1 Rationale for extended component

45 CC Part 2 [2] defines two components FIA_SOS.2 and FCS_CKM.1 that are similar to FCS_RNG.1. However, FCS_RNG.1 allows the specification of requirements for the generation of random numbers in a manner that includes necessary information for intended use, as is required here. These details describe the quality of the generated data that other security services rely upon. Thus by using FCS_RNG a PP or ST author is able to express a coherent set of SFRs that include the generation of random numbers as a security service.

5.2 Extended component definition

46 This section describes the functional requirements for the generation of random numbers, which may be used as secrets for cryptographic purposes or authentication. The IT security functional requirements for a TOE are defined in an additional family (FCS_RNG) of the Class FCS (Cryptographic support).

5.2.1 FCS_RNG Generation of random numbers

Family behaviour

47 This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component levelling

FCS_RNG: Generation of random numbers	1

48 FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

49 There are no management activities foreseen.

Audit: FCS_RNG.1

50 There are no auditable events foreseen

FCS_RNG.1 Generation of random numbers
Hierarchical to: -
Dependencies: -

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

51 FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

6 TOE Security Requirements

52 This section defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements defines the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

53 The CC allows several operations to be performed on security requirements (on the component level); refinement, selection, assignment, and iteration are defined in paragraph 8.1 of Part 1 [1] of the CC. Each of these operations is used in this PP.

54 The refinement operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in bold text and changed words are crossed out.

55 The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP author are denoted by underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are italicised.

56 The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP author are denoted by underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are italicised. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus, this text is underlined and italicised.

57 The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a number and identifier in brackets after the component name, and the iteration number after each element designator.

6.1 Security functional requirements for the TOE

58 This section is subdivided to show security functional requirements that relate to the TOE itself, and those that relate to external communications. This is to facilitate comparison of the communication requirements between this PP and others in the PP family.

6.1.1 Security functional requirements for the EGF

6.1.1.1 Class FAU Audit

6.1.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to: -
Dependencies: FAU_SAA.1 Potential violation analysis
FAU_ARP.1.1 The TSF shall [erase all its memory including cryptographic keys[7], and respond to VU requests with status 6690] upon detection of a potential security violation.

6.1.1.1.2 FAU_SAA.1 Potential violation analysis

Hierarchical to: -

7 Cryptographic keys here means the private asymmetric keys in Table 14 and the symmetric keys in Table 15.

Dependencies: FAU_GEN.1 Audit data generation

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

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

a) Accumulation or combination of [no events] known to indicate a potential security violation;
b) [any breach of physical security shall trigger the actions defined in FAU_ARP.1].

6.1.1.2 Class FDP User data protection

6.1.1.2.1 FDP_ACC.1 Subset access control

Hierarchical to: -

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [access control SFP] on [
Subject: VU
Objects: GNSS data, EGF identification data, Cryptographic keys, TOE software code
Operations: Transfer, Access, Authenticate].

6.1.1.2.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: -

Dependencies: FDP_ACC.1 Subset access control

FDP_ACF.1.1 The TSF shall enforce the [access control SFP] to objects based on the following: [
Subject:
- VU (Attribute: Authenticated)

Objects:
- GNSS data (No attributes)
- Identification data (No attributes)
- Cryptographic keys
- TOE software code].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
Transfer of GNSS data to a VU shall be allowed only under the following conditions

a) The coupling process between the TOE and the VU has been completed as described in [5] Annex 1C, Appendix 11; and
b) The periodic mutual authentication and session key agreement between the VU and the TOE described in [5], Annex 1C, Appendix 11 has been executed with the required frequency].

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

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

a) Identification data shall be written only once (by the manufacturer);
b) TOE software code and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion;
c) All commands, actions, or test points, specific to the testing needs of the manufacturing phase shall be disabled or removed before the end of the manufacturing phase, and it shall not be possible to restore them for later use;
d) TOE software code shall not be accepted from external sources unless successfully authenticated].

6.1.1.2.3 FDP_UIT.1 Data exchange integrity

Hierarchical to: -
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF Trusted channel, or
FTP_TRP.1 Trusted path]
FDP_UIT.1.1 The TSF shall enforce the [access control SFP] to [transmit] user data in a manner protected from [modification and replay] errors.
FDP_UIT.1.2 The TSF shall ~~be able~~ **provide the means** to determine on receipt of user data, whether [modification or replay] has occurred.

6.1.1.3 Class FPT Protection of the TSF

6.1.1.3.1 FPT_PHP.2 Notification of physical attack

Hierarchical to: FPT_PHP.1 Passive detection of physical attack
Dependencies: FMT_MOF.1 Management of security functions behaviour
FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
FPT_PHP.2.3 For [the external GNSS facility casing], the TSF shall monitor the devices and elements and notify [the coupled vehicle unit and/or a human inspector] when physical tampering with the TSF's devices or TSF's elements has occurred.
Application note 2: The TOE shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection by a human inspector, display of status 6690 to the vehicle unit).

6.1.1.3.2 FPT_PHP.3 Resistance to physical attack

Hierarchical to: -
Dependencies: -
FPT_PHP.3.1 The TSF shall resist [physical tampering attacks] to the [TSF software and TSF data] by responding automatically such that the SFRs are always enforced.

6.1.1.3.3 FPT_TST.1 TSF testing

Hierarchical to: -
Dependencies: -

FPR_TST.1.1 The TSF shall run a suite of self tests [during initial start-up and periodically during normal operation] to demonstrate the correct operation of [the TSF].

FPT_TST.1.2 The TSF shall ~~provide authorized users with the capability~~ **run a suite of self tests** to verify the integrity of [TSF data].

FPT_TST.1.3 The TSF shall ~~provide authorized users with the capability~~ **run a suite of self tests** to verify the integrity of [TSF software].

Application note 3: The ST author specifies a strategy for running self-tests in the TOE summary specification, and justifies why this is appropriate. Self-test failures are available to the coupled vehicle unit by means of an error code.

6.1.2 Security functional requirements for external communications

59 The security functional requirements in this section are required to support communications specifically with 2nd generation vehicle units.

6.1.2.1 Class FCS Cryptographic support

6.1.2.1.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: -

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate keys in accordance with a specified key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [key sizes required by [5] Annex 1C, Appendix 11, Part B] that meet the following: [Reference [8] predefined RNG class [selection: PTG.2, PTG.3, DRG.2, DRG.3, DRG.4, NTG.1]].

Application note 4: The ST author selects one of the permitted predefined RNG classes from [8], and completes the operations in FCS_CKM.1 and FCS_RNG.1 as required.

6.1.2.1.2 FCS_CKM.2 Cryptographic key distribution

Hierarchical to: -

Dependencies: [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.2.1 The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [AES session key agreement as specified in [5] Annex 1C, Appendix 11, Part B] that meets the following [[5] Annex 1C, Appendix 11, Part B].

Application note 5: FCS_CKM.1 and FCS_CKM.2 relate to session key agreement with the vehicle unit.

6.1.2.1.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]

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

- Requirements in Table 14 and Table 15;
- Temporary private and secret cryptographic keys shall be destroyed in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means[8];
- [assignment: *list of standards*]].

6.1.2.1.4 FCS_COP.1 Cryptographic operation (1: AES)

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(1:AES)) The TSF shall perform [encryption/decryption to ensure the authenticity and integrity of data exchanged between a vehicle unit and an external GNSS facility] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128, 192, 256 bits] that meet the following: [FIPS PUB 197: Advanced Encryption Standard].

6.1.2.1.5 FCS_COP.1 Cryptographic operation (2: SHA-2)

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(2:SHA-2) The TSF shall perform [cryptographic hashing] in accordance with a specified cryptographic algorithm [SHA-256, SHA-384, SHA-512] and cryptographic key sizes [not applicable] that meet the following: [Federal Information Processing Standards Publication FIPS PUB 180-4: Secure Hash Standard (SHS)].

6.1.2.1.6 FCS_COP.1 Cryptographic operation (3: ECC)

Hierarchical to: -

Dependencies: [FDP_ITC.1 Import of data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(3:ECC) The TSF shall perform [the following cryptographic operations:

a) digital signature generation;
b) digital signature verification;
c) cryptographic session key agreement with a VU;

8 Simple deletion of the keying material might not completely obliterate the information. For example, erasing the information might require overwriting that information multiple times with other non-related information.

d) mutual authentication between a vehicle unit and an external GNSS facility
e) coupling of a vehicle unit and an external GNSS facility]
in accordance with a specified cryptographic algorithm [[5] Annex 1C, Appendix 11, Part B, ECDSA, ECKA-EG] and cryptographic key sizes [in accordance with [5] Annex 1C, Appendix 11, Part B] that meet the following: [[5] Annex 1C, Appendix 11, Part B; FIPS PUB 186-4: Digital Signature Standard; BSI Technical Guideline TR-03111 – Elliptic Curve Cryptography – version 2, and the following standardized domain parameters (see [5] Annex 1C, Appendix 11, Part B)

Name	Size (bits)	Object identifier
NIST P-256	256	secp256r1
BrainpoolP256r1	256	brainpoolP256r1
NIST P-384	384	secp384r1
BrainpoolP384r1	384	brainpoolP384r1
BrainpoolP512r1	512	brainpoolP512r1
NIST P-521	521	secp521r1

Table 7 - Standardised domain parameters

].

Application note 6: Where a symmetric algorithm, an asymmetric algorithm and/or a hashing algorithm are used together to form a security protocol, their respective key lengths and hash sizes shall be of (roughly) equal strength. Table 8Table 8 shows the allowed cipher suites. ECC keys sizes of 512 bits and 521 bits are considered to be equal in strength for all purposes within this PP.

Cipher suite Id	ECC key size (bits)	AES key length (bits)	Hashing algorithm	MAC length (bytes)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Table 8 - Cipher suites

6.1.2.1.7 FCS_RNG.1 Random number generation

Hierarchical to: -
Dependencies: -

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

6.1.2.2 Class FIA Identification and authentication

6.1.2.2.1 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Authentication before any action

Dependencies: FIA_UID.1 Identification before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated **using the method described in [5] Annex 1C, Appendix 11, Chapter 10** before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.2.2 FIA_UAU.6 Re-authenticating

Hierarchical to: -

Dependencies: -

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [

a) at entity connection (coupling);
b) at power supply recovery;
c) periodically].

6.1.2.2.3 FIA_UID.2 User authentication before any action

Hierarchical to: -

Dependencies: -

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

Application note 7: The identification of the vehicle unit is achieved during coupling of the EGF and the vehicle unit.

6.1.2.3 Class FPT Protection of the TSF

6.1.2.3.1 FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: -

Dependencies: -

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [secure messaging attributes as defined by [5] Annex 1C, Appendix 11] when shared between the TSF and ~~another trusted IT product~~ **a vehicle unit**.

FPT_TDC.1.2 The TSF shall use [the interpretation rules (communication protocols) as defined by [5] Annex 1C, Appendix 11] when interpreting the TSF data from ~~another trusted IT product~~ **a vehicle unit**.

6.1.2.4 Class FTP Trusted path/channels

6.1.2.4.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: -

Dependencies:	-
FTP_ITC.1.1	The TSF shall provide a communications channel between itself and ~~another trusted IT product~~ **the vehicle unit** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [another trusted IT product[9]] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [all communications].

6.2 Security assurance requirements for the TOE

60 The assurance level for this protection profile is EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5, as defined in [3].

61 These security assurance requirements are derived from [5] Annex 1C, Appendix 10.

9 The TOE shall establish a secure channel only with a vehicle unit

7 Rationale

7.1 Security objectives rationale

62 The following table provides an overview for security objectives coverage (TOE and its operational environment), also giving an evidence for *sufficiency* and *necessity* of the security objectives defined. It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

	T.Environment	T.Hardware	T.GNSS_Data	T.Security_Data	T.Software	T.Tests	A.Installation	A.Type_Approved	P.Crypto
O.EGF_Main	x	x	x	x	x		x		
O.Access			x	x	x				
O.Audit	x	x							
O.Authentication			x		x				
O.Reliability	x	x		x	x	x	x		
O.Secure_Communication			x	x	x				
O.Physical	x	x			x				
O.Crypto_Implement									x
O.Software_Upgrade					x				
OE.Development		x			x				
OE.Manufacturing		x			x	x	x		
OE.Data_Generation				x			x		
OE.Data_Transport				x			x		
OE.Delivery		x			x		x		
OE.Data_Strong							x		x
OE.Test_Points						x			
OE.Approv_Workshops		x		x	x		x		
OE.Regular_Inspection	x	x			x				
OE.Faithful_Calibration			x				x		
OE.Crypto_Admin							x		x
OE.Type_Approved_VU								x	
OE.Antenna_Clear	x								
OE.EOL				x					

Table 9 - Security objectives rationale

63 A detailed justification required for *suitability* of the security objectives to address the security problem definition is given below.

64 **T.Environment** is addressed by O.EGF_Main, which requires that GNSS data must be available to the VU, and by O.Reliability, which requires a reliable service. O.Physical addresses the need to resist physical attacks, and O.Audit addresses detection and action taken in response to such attacks. OE.Antenna_Clear requires siting of the GNSS antenna to allow receipt of GNSS signals. OE.Regular_Inspection helps to detect signs of interference with TOE hardware.

65 **T.Hardware** is addressed by O.EGF_Main, which requires that GNSS data must be available to the VU, and by O.Reliability, which requires a reliable service. O.Physical addresses the need to resist physical attacks, and O.Audit addresses detection and action taken in response to such attacks. OE.Regular_Inspection helps to detect signs of interference with TOE hardware. Interference with TOE hardware during development, manufacturing, delivery, installation and repair is addressed by OE.Development, OE.Manufacturing, OE.Delivery and OE.Approv_Workshops.

66 **T.GNSS_Data** is addressed by O.EGF_Main, which requires that GNSS data must be available to the VU. O.Access and O.Authentication control the ability to connect to the TOE and to retrieve data, helping to protect against unauthorised access and tampering. O.Secure_Communication addresses security of the data transfer, helping to detect any modification or attempt to replay. OE.Faithful_Calibration requires that workshops couple the TOE with the connected vehicle unit during calibration, so that availability, integrity and authenticity of data supplied to the VU can be protected.

67 **T.Security_Data** is addressed by O.EGF_Main, which requires that GNSS data must be available to the VU, and by O.Reliability, which requires a reliable service. These both rely on maintaining the security data. O.Access and O.Secure_Communication restrict the ability of a connected entity to access this data. OE.Data_Generation, OE.Data_Transport and OE.Approv_Workshops aim to protect the confidentiality and integrity of the security data before the TOE is brought into operational use, or during maintenance. OE.EOL requires that the TOE be disposed of in a secure manner when it is no longer in service.

68 **T.Software** is addressed by O.EGF_Main, which requires that GNSS data must be available to the VU, and by O.Reliability, which requires a reliable service. O.Access, O.Authentication, O.Secure_Communication and O.Software_Upgrade aim to prevent unauthorised connections to the TOE that could attempt to modify software during operation. O. Physical deals with attempts to modify the software by means of a physical attack on the TOE. OE.Development, OE.Manufacturing and OE.Delivery address the prevention of software modification prior to installation. OE.Approv_Workshops helps to detect signs of interference with TOE software during installation and calibration. OE.Regular_Inspection helps to detect signs of interference with TOE software.

69 **T.Tests** is addressed by O.Reliability, OE.Manufacturing and OE.Test_Points. If the TOE provides a reliable service as required by O.Reliability, if its security cannot be compromised during the manufacturing process (OE.Manufacturing) and if all test points are disabled, the TOE can neither enter any non-invalidated test mode nor have any back door. Hence, the related threat will be mitigated.

70 **A.Installation** is supported by OE.Data_Strong, which calls for correct cryptographic material to be loaded into the TOE before operation. OE.Crypto_Admin addresses the handling and operation of cryptographic material to be done in accordance with requirements. OE.Manufacturing, OE.Data_Generation, OE.Data_Transport, OE.Delivery and OE.Approv_Workshops address the prevention of data or data structure modification

prior to installation. OE.Faithful_Callibration helps to ensure that the correct security data is loaded into the TOE before operation. O.EGF_Main requires that GNSS data must be available to the VU, and O.Reliability requires a reliable service.

71 **A.Type_Approved** is supported by OE.Type_Approved_VU, which requires that the vehicle unit that is coupled with the TOE is type approved.

72 **P.Crypto** is supported by O.Crypto_Implement, which calls for the correct cryptographic functions to be implemented in the TOE. OE.Data_Strong calls for correct cryptographic material to be loaded into the TOE before operation, and OE.Crypto_Admin addresses the handling and operation of cryptographic material to be done in accordance with requirements.

7.2 Security requirements rationale

7.2.1 Rationale for SFRs' dependencies

73 The following table shows how the dependencies for each SFR are satisfied.

SFR	Dependencies	Rationale
FAU_ARP.1	FAU_SAA.1	Satisfied by FAU_SAA.1
FAU_SAA.1	FAU_GEN.1	Not satisfied. There is no subset of audits specified to be monitored, only breach of physical security. No audit trail is generated, only an alarm and erasure of memory. The non-satisfaction of the dependency is considered justified.
FDP_ACC.1	FDP_ACF.1	Satisfied by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	Satisfied by FDP_ACC.1
FDP_UIT.1	FDP_ACC.1 or FDP_IFC.1, FTP_ITC.1 or FTP_TRP.1	Satisfied by FDP_ACC.1 and FTP_ITC.1
FPT_PHP.2	FMT_MOF.1	CC Part 2 [2] paragraph 1220 states that the use of FMT_MOF.1 should be considered to specify who can make use of the capability, and how they can make use of the capability. Since the capability is always enabled, use of FMT_MOF.1 is not relevant.
FPT_PHP.3	-	-

SFR	Dependencies	Rationale
FPT_TST.1	-	-
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	Satisfied by FCS_CKM.2, FCS_COP.1 and FCS_CKM.4
FCS_CKM.2	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FCS_CKM.1 and FCS_CKM.4
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FCS_CKM.1
FCS_COP.1(1:AES)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FCS_CKM.1 and FCS_CKM.4
FCS_COP.1(2:SHA-2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Not applicable as no keys are used for SHA-2
FCS_COP.1(3:ECC)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Satisfied by FCS_CKM.1 and FCS_CKM.4
FCS_RNG.1[10]	-	-
FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UAU.6	-	-
FIA_UID.2	-	-
FPT_TDC.1	-	-
FTP_ITC.1	-	-

Table 10 - Dependency rationale

7.2.2 Security functional requirements rationale

74 The following table provides an overview for security functional requirements coverage also giving an evidence for *sufficiency* and *necessity* of the SFRs chosen.

		O.EGF_Main	O.Access	O.Audit	O.Authentication	O.Reliability	O.Secure_Communicat	O.Physical	O.Crypto_Implement	O.Software_Upgrade
FAU_ARP.1	Security alarms	x		x						
FAU_SAA.1	Potential violation analysis	x		x						
FDP_ACC.1	Subset access control		x		x				x	x
FDP_ACF.1	Security attribute based access control		x		x				x	x

10 Extended component

		O.EGF_Main	O.Access	O.Audit	O.Authentication	O.Reliability	O.Secure_Communicat	O.Physical	O.Crypto_Implement	O.Software_Upgrade
FDP_UIT.1	Data exchange integrity	x				x				
FPT_PHP.2	Notification of physical attack	x				x		x		x
FPT_PHP.3	Resistance to physical attack	x				x		x		x
FPT_TST.1	TSF testing	x				x				
FCS_CKM.1	Cryptographic key generation						x		x	
FCS_CKM.2	Cryptographic key distribution						x		x	
FCS_CKM.4	Cryptographic key destruction						x		x	
FCS_COP.1	Cryptographic operation (1:AES)						x		x	
FCS_COP.1	Cryptographic operation (2:SHA-2)						x		x	
FCS_COP.1	Cryptographic operation (3:ECC)						x		x	
FCS_RNG.1	Random number generation						x		x	
FIA_UAU.2	User authentication before any action		x		x					
FIA_UAU.6	Re-authenticating		x		x					
FIA_UID.2	User identification before any action		x		x					
FPT_TDC.1	Inter-TSF basic TSF data consistency					x				
FTP_ITC.1	Inter-TSF trusted channel				x		x			

Table 11 - Coverage of security objectives for the TOE by SFRs

75 A detailed justification required for *suitability* of the security functional requirements to achieve the security objectives is given in the table below.

Security Objective	SFR	Rationale
O.EGF_Main	FAU_ARP.1 FAU_SAA.1	Define the actions to be taken on detection of a breach of the TOE's physical security.
	FDP_UIT.1	Requires a means for the VU to confirm the integrity of the data received from the TOE, and to detect modification and replay.
	FPT_PHP.2 FPT_PHP.3	Requires detection of and resistance to physical attack to help ensure that the integrity of data supplied to the VU is maintained.
	FPT_TST.1	Self-tests help to ensure that the TOE is operating correctly.
O.Access	FDP_ACC.1 FDP_ACF.1	Define the access control policy covering access to user data and security data.
	FIA_UAU.2	Requires that any connected entity be authenticated before any access is granted to the TOE.
	FIA_UAU.6	Requires periodic re-authentication of a connected VU.
	FIA_UID.2	Requires that any connected entity be identified before any access is granted to the TOE.
O.Audit	FAU_ARP.1 FAU_SAA.1	Define the actions to be taken on detection of a breach of the TOE's physical security.
O.Authentication	FDP_ACC.1 FDP_ACF.1	Define the access control policy covering access to user data and security data.
	FIA_UAU.2	Requires that any connected entity be authenticated before any access is granted to the TOE.
	FIA_UAU.6	Requires periodic re-authentication of a connected VU.
	FIA_UID.2	Requires that any connected entity be identified before any access is granted to the TOE.
	FTP_ITC.1	Requires use of a secure channel for communication with the VU that has authenticated end-points.
O.Reliability	FDP_UIT.1	Requires a means for the VU to confirm the integrity of the data received from the TOE, and to detect modification and replay.
	FPT_PHP.2 FPT_PHP.3	Requires detection of and resistance to physical attack to help ensure that the integrity of data supplied to the VU is maintained.
	FPT_TDC.1	Requires a secure protocol such that the attributes of the user data transferred to the VU can be consistently interpreted.
	FPT_TST.1	Self-tests help to ensure that the TOE is operating correctly.
O.Secure_Communication	FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1(1:AES) FCS_COP.1(2:SHA-2) FCS_COP.1(3:ECC	Define the required cryptography to be used by the TOE for authentication and data protection.

Security Objective	SFR	Rationale
	) FCS_RNG.1	
	FTP_ITC.1	Requires use of a secure channel for communication with the VU.
O.Physical	FPT_PHP.2 FPT_PHP.3	Requires detection of and resistance to physical attack to help ensure that the integrity of data supplied to the VU is maintained.
O.Crypto_Implement	FDP_ACC.1 FDP_ACF.1	The defined policy includes a requirement to use only the required cryptographic algorithms.
	FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1(1:AES) FCS_COP.1(2:SHA-2) FCS_COP.1(3:ECC) FCS_RNG.1	Define the required cryptography to be used by the TOE for authentication and data protection.
O.Software_Update	FDP_ACC.1 FDP_ACF.1	Require that unauthenticated software is not accepted.
	FPT_PHP.2 FPT_PHP.3	Requires the TOE to detect and resist physical attacks that may aim to modify application software.

Table 12 – Detailed security objectives rationale

7.2.3 Security assurance requirements rationale

76 The chosen assurance package represents the predefined assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5. This package is mandated by [5] Annex 1C, Appendix 10.

77 This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

78 The selection of the component ATE_DPT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR-enforcing modules

79 The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3: Subjects, entry 'Attacker'). This decision represents a part of the conscious security policy for the recording equipment required by the regulations, and reflected by the current PP.

80 The set of *assurance* requirements being part of EAL4 fulfils all dependencies a priori.

81 The augmentation of EAL4 chosen comprises the following assurance components:

– ATE_DPT.2 and
– AVA_VAN.5.

82 For these additional assurance components, all dependencies are met or exceeded in the EAL4 assurance package.

Component	Dependencies required by CC Part 3	Dependency satisfied by
ATE_DPT.2	ADV_ARC.1	ADV_ARC.1
	ADV_TDS.3	ADV_TDS.3
	ATE_FUN.1	ATE_FUN.1
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.4
	ADV_TDS.3	ADV_TDS.3
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.2

Table 13 - SARs' dependencies (additional to EAL4 only)

7.2.4 Security requirements – internal consistency

83 This part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form an internally consistent whole.

a) SFRs

84 The dependency analysis in section 7.2.1 for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

85 All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these ‘shared’ items. The current PP accurately reflects the requirements of EU Parliament and Council Regulation 165/2014, Annex 1C, which is assumed to be internally consistent.

b) SARs

86 The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 7.2.3 shows that the assurance requirements are internally consistent, because all (additional) dependencies are satisfied and no inconsistency appears.

87 Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met – an opportunity having been shown not

to arise in sections 7.2.1 and 7.2.3. Furthermore, as also discussed in section 7.2.3, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

8 Glossary and Acronyms

8.1 Glossary

Glossary Term	Definition
Application note	Optional informative part of the PP containing sensible supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.
Approved Workshops	Fitters and workshops installing, calibrating and (optionally) repairing EGFs and being under such agreement with an EGF manufacturer.
Authenticity	The property that information is coming from a party whose identity can be verified.
Certification authority	A natural or legal person who certifies the assignment of public keys to the serial number of equipment.
Digital Tachograph	Recording equipment including a vehicle unit and a motion sensor connected to it.
Digital Tachograph System	Equipment, people or organisations, involved in any way with the recording equipment and External GNSS Facilities.
European Root Certification Authority (ERCA)	An organisation being responsible for implementation of the ERCA policy and for the provision of key certification services to the Member States. It is represented by Digital Tachograph Root Certification Authority Traceability and Vulnerability Assessment Unit European Commission Joint Research Centre, Ispra Establishment (TP.360) Via E. Fermi, 2749 21027 Ispra (VA) Italy
External GNSS Facility	A facility which contains the GNSS receiver when the vehicle unit is not a single unit as well as other components needed to protect the communication of GNSS data to the rest of the vehicle unit.
EGF Identification data	Data identifying the EGF: name of manufacturer, serial number, approval number, embedded security component identifier and operating system identifier. EGF identification data are part of user data.
GNSS	Global Navigation Satellite System, a generic term including technologies such as GPS, Galileo and GLONASS
GNSS data	GSA sentences and/or RMC sentences
GSA sentence	GNSS DOP and active satellites sentence, as specified in NMEA 0183 v.4.1 [7]

Glossary Term	Definition
Integrity	The property of accuracy and completeness of information.
Manufacturer	The generic term for a manufacturer producing an EGF as the TOE.
Member State Authority (MSA)	Each Member State of the European Union establishes its own national Member State Authority (MSA), usually represented by a state authority. The national MSA runs some services, among others the Member State Certification Authority (MSCA).
Member State Certification Authority (MSCA)	An organisation established by a Member State Authority, responsible for implementation of the MSA policy and for signing certificates for public keys to be inserted into equipment.
Personalisation	The process by which the equipment-individual data (like identification data and authentication key pairs for VU and EGF or serial numbers and pairing keys for MS) are stored in and unambiguously, inseparably associated with the related equipment.
RMC sentence	Recommended Minimum Specific sentence as specified in NMEA 0183 v.4.1 [7]
Security data	The specific data needed to support security enforcing functions (e.g. cryptographic keys or certificates). Security data are part of sensitive data.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]. In the context of this PP, TSF data are matched by security data.
User	A legitimate user of the TOE, being a coupled vehicle unit.
User data	Any data, other than security data, recorded or stored by the EGF. User data are part of sensitive data. User data include EGF identification data and GNSS data. The CC gives the following generic definitions for user data: • Data created by and for the user that does NOT affect the operation of the TSF (CC part 1 [1]). • Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [2]).
Vehicle Unit	The recording equipment excluding the motion sensor and the cables connecting the motion sensor.

8.2 Acronyms

AES	Advanced Encryption Standard
CA	Certificate Authority

CC	Common Criteria
DOP	Dilution of Precision
EAL	Evaluation Assurance Level (a pre-defined package in CC)
EGF	External GNSS Facility
ERCA	European Root Certification Authority
GNSS	Global Navigation Satellite System
MAC	Message Authentication Code
MS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority
n.a.	Not applicable
OSP	Organisational Security Policy
PKI	Public Key Infrastructure
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
VU	Vehicle Unit

9 Bibliography

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

Digital Tachograph: directives and standards

[5] Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components

Digital Tachograph: Protection Profiles

[6] Common Criteria Protection Profile Digital Tachograph – Vehicle Unit (VU PP)

Other standards

[7] NMEA 0183, Standard for Interfacing Marine Electronics, version 4.10, June 2012

[8] A proposal for: Functionality classes for random number generators, Wolfgang Killmann (T-Systems) and Werner Schindler (BSI), Version 2.0, 18 September 2011

10 Annex A – Key & Certificate Tables

88 This annex provides details of the cryptographic keys and certificates required by an External GNSS Facility during its lifetime, and to support communication with EGFs.

Table 14	– Asymmetric keys generated, used or stored by an EGF
Table 15	- Symmetric keys generated, used or stored by an EGF
Table 16	- Certificates used or stored by an EGF

89 In general, an EGF will not be able to know when it has reached end of life, and thus will not be able to make unavailable its permanently stored keys. Making unavailable the permanently stored keys mentioned in this table, if feasible, is a matter of organisational policy.

Key Symbol	Description	Purpose	Type	Source	Generation method	Destruction method and time	Stored in
EGF_MA.SK	EGF private key for Mutual Authentication	Used by the EGF to perform EGF authentication towards VUs	ECC	Generated by EGF or EGF manufacturer at the end of the manufacturing phase	See section 6.1.2.1.1 if done by EGF. Otherwise, not in scope of this PP.	Made unavailable when the EGF has reached end of life	EGF non-volatile memory
EUR.PK current	The current public key of ERCA (at the time of issuing of EGF)	Used by the EGF for the verification of MSCA certificates issued under the current ERCA root certificate. See also notes for EUR.C (current) contents in Table 16.	ECC	Generated by ERCA; inserted in EGF by manufacturer at the end of the manufacturing phase	Out of scope for this PP	Not applicable	EGF non-volatile memory
EUR.PK previous (conditional; only present if existing at time of EGF issuance)	The previous public key of ERCA (at the time of issuing of EGF)	Used by the EGF to verify MSCA certificates issued under the previous ERCA root certificate. See also notes for EUR.C (previous) contents in Table 16.	ECC	Generated by ERCA; inserted in EGF by manufacturer at the end of the manufacturing phase	Out of scope for this PP	Not applicable	EGF non-volatile memory
EUR.Link.PK (conditional; only if the EGF has successfully authenticated a next-generation VU)	The public key of ERCA following the public key that was current at the time of issuing of the EGF	Used by the EGF to verify MSCA certificates issued under the next ERCA root certificate. Note that EUR.Link.PK is the same as the next EUR.PK. See also Application note 8: and notes for EUR.Link.C contents in Table 16.	ECC	Generated by ERCA; inserted by manufacturer in a VU issued under the next generation of EUR.C as part of the EUR.Link.C; obtained by EGF during mutual authentication towards such a VU	Out of scope for this PP	Not applicable	EGF general non-volatile memory

VU_MA.PK (conditional, maximum one)	VU public key for Mutual Authentication	Used by EGF to perform VU authentication and session key agreement. See also notes for VU_MA.C contents in Table 16.	ECC	Generated by VU manufacturer; obtained by EGF in VU certificate during mutual authentication as part of coupling process.	Out of scope for this PP	Not applicable	EGF non-volatile memory
MSCA_VU-EGF.PK (conditional, possibly multiple)	Public key of MSCA responsible for signing VU and EGF certificates	Used by EGF to verify the certificate of a VU signed by this (foreign) MSCA. See also notes for MSCA_ VU-EGF.C contents in Table 16.	ECC	Generated by MSCA ; obtained by EGF in MSCA_ VU-EGF certificate during mutual authentication	Out of scope for this PP	Not applicable	EGF non-volatile memory

Table 14 – Asymmetric keys generated, used or stored by an EGF

Key Symbol	Description	Purpose	Type	Source	Generation Method	Destruction method and time	Stored in
K_{MAC}	Secure Messaging session key for authenticity	Session key for authenticity between EGF and a VU during a Secure Messaging session	AES	Agreed between EGF and VU during mutual authentication	See section 6.1.2.1.2	Made unavailable when the Secure Messaging session is aborted	Not permanently stored
K_{ENC}	Secure Messaging session key for confidentiality	Session key for confidentiality between EGF and a VU during a Secure Messaging session	AES	Agreed between EGF and VU during mutual authentication	See section 6.1.2.1.2	Made unavailable when the Secure Messaging session is aborted	Not permanently stored

Table 15 - Symmetric keys generated, used or stored by an EGF

Certificate Symbol	Description	Purpose	Source	Stored in	Note
EGF_MA.C	EGF certificate for Mutual Authentication	Used by VU to obtain and verify the EGF_MA.PK they will subsequently use to perform EGF authentication.	Created and signed by MSCA based on EGF manufacturer input; inserted by manufacturer at the end of the manufacturing phase	EGF general non-volatile memory	
MSCA_EGF-VU.C	Certificate of MSCA responsible for signing the EGF_MA and EGF_Sign certificates	Used by a VU to obtain and verify the MSCA_EGF-VU.PK it will subsequently use to verify the EGF_MA or EGF_Sign certificate.	Created and signed by ERCA based on MSCA input; inserted by manufacturer at the end of the manufacturing phase	EGF general non-volatile memory	
EUR.Link.C	Link Certificate signed by previous EUR.SK (see Application note 8:)	Used by a VU issued under the previous ERCA root certificate to obtain and verify the current EUR.PK it will subsequently use to verify the MSCA_EGF-VU certificate.	Created and signed by ERCA; inserted in EGF by manufacturer at the end of the manufacturing phase	EGF general non-volatile memory	Presence in EGF is conditional; only if a previous ERCA root certificate existed at the moment of EGF manufacturing
EUR.C (current) contents	CHR and other contents of current European root certificate	This CHR will be referenced by VUs issued under the current European root public key (see Table 14). The EGF may store the validity period and other certificate data as well.	Generated by ERCA; inserted in EGF by manufacturer at the end of the manufacturing phase	EGF general non-volatile memory	
EUR.C (previous) contents	CHR and other contents of previous European root certificate	This CHR will be referenced by VUs issued under the previous European root public key (see Table 14). The EGF may store the validity period and other certificate data as well.	Generated by ERCA; inserted in EGF by manufacturer at the end of the manufacturing phase	EGF general non-volatile memory	Presence in EGF is conditional; only if a previous ERCA root certificate existed at the moment of EGF manufacturing

EUR.Link.C contents	CHR and other contents of next European root certificate	This CHR will be referenced by VUs issued under the next European root public key (see Table 14). The EGF may store the validity period and other certificate data as well.	Generated by ERCA; inserted by manufacturer in a VU issued under the next generation of EUR.C as part of the EUR.Link.C; obtained and stored by EGF during coupling to such a VU	EGF general non-volatile memory	Presence in EGF is conditional; only if the EGF has been successfully coupled with a next-generation VU
VU_MA.C contents	CHR and other contents of VU certificate for Mutual Authentication	If an EGF has verified a VU_MA certificate before, it shall store the public key (see Table 14), the CHR and possibly the validity period and other data in order to authenticate that VU again in the future.	Created and signed by MSCA_EGF-VU based on VU manufacturer input, inserted in VU by VU manufacturer, obtained and stored by EGF during mutual authentication after successful verification.	EGF general non-volatile memory	Presence in EGF is conditional; only if EGF has been coupled to a VU. The EGF shall store the contents of only one VU_MA.C at any given time.
MSCA_VU-EGF.C contents	CHR and other contents of certificate of MSCA responsible for signing VU certificates	If an EGF has verified a MSCA certificate before, it may store the public key (see Table 14), the CHR and possibly the validity period and other data in order to verify VU certificates based on that MSCA certificate in the future	Created and signed by ERCA based on MSCA input, inserted in VU by VU manufacturer obtained and stored by EGF after successful verification during a previous coupling process with a VU.	EGF general non-volatile memory	Presence in EGF is conditional; only if EGF is designed to store VU certificate contents for future reference and has encountered VUs in the past. The EGF may store the contents of multiple MSCA_VU-EGF.C, e.g. different MSCAs and/or generations.

Table 16 - Certificates used or stored by an EGF

Application note 8: During its lifetime, the EGF can be confronted with two different link certificates:

- If at the time of issuance of the EGF, there are VUs in the field that are issued under a previous EUR.C, then the EGF shall be issued with both the previous EUR.C and an EUR.Link.C signed with the previous EUR.SK. The EGF will need the first one to check the authenticity of an old VU during coupling. The EGF will need the second one to prove its authenticity towards an old VU.

- If, after the issuance of the EGF, a new EUR.C is generated and VUs are issued under this new root certificate, then during coupling such a new VU will present the EGF with an EUR.Link.C signed by the current EUR.SK to prove its authenticity. The EGF can check this certificate with its current EUR.PK. If correct, the EGF shall store the EUR.Link.PK as a new trust point.

11 Annex B – Operations for FCS_RNG.1

90 This annex provides further information on the use of FCS_RNG.1 and FCS_CKM.1 in compliant security targets. The security target author should select one of these classes, as appropriate to the TOE, to complete the selection in FCS_CKM.1, and should complete the operations in FCS_RNG.1 correspondingly. Further information on the application of these classes can be found in [8].

11.1 Class PTG.2

91 Functional security requirements of the class PTG.2 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class PTG.2)

FCS_RNG.1.1 The TSF shall provide a [physical] random number generator that implements:

(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG [*selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy*].

(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.

(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered [*selection: externally, at regular intervals, continuously, applied upon specified internal events*]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

FCS_RNG.1.2 The TSF shall provide [*selection: bits, octets of bits, numbers* [*assignment: format of the numbers*]] that meet:

(PTG.2.6) Test procedure A[11] [*assignment: additional standard test suites*] does not distinguish the internal random numbers from output sequences of an ideal RNG.

(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.

11.2 Class PTG.3

92 Functional security requirements of the class PTG.3 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class PTG.3)

FCS_RNG.1.1 The TSF shall provide a [hybrid physical] random number generator that implements:

(PTG.3.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

(PTG.3.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG [*selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.3 as long as its internal state entropy guarantees the claimed output entropy*].

(PTG.3.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.

(PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

(PTG.3.5) The online test procedure checks the raw random number sequence. It is triggered [*selection: externally, at regular intervals, continuously, upon specified internal events*]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

(PTG.3.6) The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.

11 See [7] Section 2.4.4.

FCS_RNG.1.2 The TSF shall provide [*selection: bits, octets of bits, numbers* [*assignment: format of the numbers*]] that meet:

(PTG.3.7) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A[10] [*assignment: additional test suites*].

(PTG.3.8) The internal random numbers shall [*selection: use PTRNG of class PTG.2 as random source for the post-processing, have [assignment: work factor], require [assignment: guess work*]].

11.3 Class DRG.2

93 Functional security requirements of the class DRG.2 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class DRG.2)

FCS_RNG.1.1 The TSF shall provide a [deterministic] random number generator that implements:

(DRG.2.1) If initialized with a random seed [*selection: using a PTRNG of class PTG.2 as random source, using a PTRNG of class PTG.3 as random source, using an NPTRNG of class NTG.1 [assignment: other requirements for seeding]*], the internal state of the RNG shall [*selection: have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]*].

(DRG.2.2) The RNG provides forward secrecy.

(DRG.2.3) The RNG provides backward secrecy.

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(DRG.2.4) The RNG, initialized with a random seed [*assignment: requirements for seeding*], generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].

(DRG.2.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A[28] [*assignment: additional test suites*].

11.4 Class DRG.3

94 Functional security requirements of the class DRG.3 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class DRG.3)

FCS_RNG.1.1 The TSF shall provide a [deterministic] random number generator that implements:

(DRG.3.1) If initialized with a random seed [*selection: using a PTRNG of class PTG.2 as random source, using a PTRNG*

of class PTG.3 as random source, using an NPTRNG of class NTG.1 [assignment: other requirements for seeding]], the internal state of the RNG shall [*selection: have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]*].

(DRG.3.2) The RNG provides forward secrecy.

(DRG.3.3) The RNG provides backward secrecy even if the current internal state is known.

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(DRG.3.4) The RNG, initialized with a random seed [*assignment: requirements for seeding*], generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].

(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A[10] [*assignment: additional test suites*].

11.5 Class DRG.4

95 Functional security requirements of the class DRG.4 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class DRG.4)

FCS_RNG.1.1 The TSF shall provide a [hybrid deterministic] random number generator that implements:

(DRG.4.1) The internal state of the RNG shall [*selection: use PTRNG of class PTG.2 as random source, have [assignment: work factor], require [assignment: guess work]*].

(DRG.4.2) The RNG provides forward secrecy.

(DRG.4.3) The RNG provides backward secrecy even if the current internal state is known.

(DRG.4.4) The RNG provides enhanced forward secrecy [*selection: on demand, on condition [assignment: condition], after [assignment: time]*].

(DRG.4.5) The internal state of the RNG is seeded by an [*selection: internal entropy source, PTRNG of class PTG.2, PTRNG of class PTG.3, [other selection]*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(DRG.4.6) The RNG generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A[10] [*assignment: additional test suites*].

11.6 Class NTG.1

96 Functional security requirements of the class NTG.1 are defined by component FCS_RNG.1 with specific operations as given below.

FCS_RNG.1 Random number generation (Class NTG.1)

FCS_RNG.1.1 The TSF shall provide a [non-physical true] random number generator that implements:

(NTG.1.1) The RNG shall test the external input data provided by a non-physical entropy source in order to estimate the entropy and to detect non-tolerable statistical defects under the condition [*assignment: requirements for NPTRNG operation*].

(NTG.1.2) The internal state of the RNG shall have at least [*assignment: Min-entropy*]. The RNG shall prevent any output of random numbers until the conditions for seeding are fulfilled.

(NTG.1.3) The RNG provides backward secrecy even if the current internal state and the previously used data for reseeding, resp. for seed-update, are known.

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

NTG.1.4) The RNG generates output for which [*assignment: number of strings*] strings of bit length 128 are mutually different with probability [*assignment: probability*].

(NTG.1.5) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A[10] [*assignment: additional test suites*].

(NTG.1.6) The average Shannon entropy per internal random bit exceeds 0.997.