REETS

REETS-TEN

Activity 4:
Back Office Interfaces

D 4.3 Report on security requirements in different toll domains and proposal for a security profile

21.07.2014

V 2.0

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

Document revision history:

Date	Version	Description	Document Status	Responsible
16-04-2014	1.0	First complete draft for commenting	Draft	Lecit Consulting
12-05-2014	1.1	REETS security policy added	Draft	ASFINAG
14-05-2014	1.2	New introduction and changes according WP4 meeting of May 9th in Vienna	Draft	EZV / Rapp Trans
25.05.2014	1.3	Comments after GTM concall and after 1.3 made by MH	Draft	Aiscat Servizi
26.05.2014	1.4	Editorial revision and inclusion of ASFA comments	Draft	Aiscat Servizi
30.05.2014	1.5	Further comments received by A, CH and PL	Draft	Aiscat Servizi
03.06.2014	1.6	Comments received by BMVI and approval after meeting in Vienna of June 3rd	Final Draft	Aiscat Servizi
12.06.2014	2.0Final	Insertion of final comments by participants	Final	Aiscat Servizi
01.07.2014	2.0Closed	Insertion of glossary and front page	Final	Aiscat Servizi
21.07.2014	2.0Closed-SC ok	Final consideration after the 16.07.14 Steering Committee	Final	Paolo Giorgi

Contents

Index of tables

Index of figures

1 Executive summary

This document D4.3 from work package 4 of the REETS (Regional European Electronic Toll Service) project defines some suitable and shared security policy elements and gives an interpretation for a choice of a security policy. Being no absolute definition what a security policy is, the project has taken as a guideline the definition of security policy content provided in clause 5.1 of ISO/IEC 27002 to develop some main policy elements.

A first element is the "high level" part of a security policy covering the so-called security objectives (SO) and detailed policy statements (PS). The security policy provided in the current document was adopted form a policy which was originally developed in the Stockholm group and then further elaborated for the EasyGo service.

The security policy in Chapter 3 covers the aspects of information security in the REETS environment. It covers the common assets and processes of all involved EFC systems at the toll chargers and toll service providers. In this context, the word „assets“ refers to interoperability constituents and to any hardware and software component that may have an impact on information security. The security policy is strongly recommended to all actors in REETS or at least form a common understanding of the guiding principles to be used during the implementation of REETS for all information being handled by the actors in regard to REETS.

The overall target of the security policy is summarized by the four security objectives listed below:

[SO-1] Any REETS toll data exchanged between a TC and a SP shall fall under the REETS security rules

[SO-2] REETS toll data shall be correct, complete, traceable and protected

[SO-3] Risk and efficiency should be considered when implementing security in REETS

[SO-4] The REETS security requirements shall be limited to supporting interoperability between the involved actors

The derived 21 policy statements define in more detail how it is intended to protect information in REETS. The policy statements cover general aspects, organisational issues, asset and interface management as well as incident management. The intention of the set of defined policy statements is to ensure the confidentiality, integrity and availability of assets in the REETS and its information and communication architecture and infrastructure, for the benefit of the service users and the TCs and SPs participating in REETS.

This security policy shall support the REETS project among others especially:

- When explaining and discussing security issues with management or with less security technical oriented project members;
- In order to achieve consensus and/or when security decisions in the REETS environment are required.

An important security policy element is the so-called "common set of REETS security requirements" provided in chapter 5, agreed among REETS participants. This set of requirements has been selected from those provided in the standard CEN TS 16439 - EFC security framework. The resulting set of requirements in the current document should be used as guidance during the REETS implementation phase, by both the TCs and SPs.

Based on these assumptions, an analysis of the security implementation issues for the REETS environment has been provided. The recommendations derived are to be considered generally valid and they might be taken into consideration for future EETS implementation.

Recommendations for further work and the EFC Security Framework:

1. Most of the relevant standards, especially the EFC Security Framework have been in revision process during the writing of the current document. It is therefore recommended to review the results in the current document that are based on the EFC Security Framework after the new version of it, i.e. CEN ISO TS 19299, has been adopted.
2. A REETS ICS (Implementation Conformance Statement) pro-forma statement based on ICS of CEN ISO TS 19299 applied to the REETS common set of requirements including the applicable

security measures should be developed. This REETS ICS shall be used to check the security implementation according to the security conformance test process for SPs provided in the REETS deliverable D2.3 "Technical accreditation of EETS Providers in a toll domain". This REETS security ICS should also be a checklist used by TCs.

3. CEN ISO TS 19299 should provide guidance how and on what basic guidelines an EFC security policy for an EFC system or an EFC cluster shall be defined. The EFC Security Framework should also describe what parts of such security policy can be developed with support from the framework.
4. We suggest that the common set of REETS requirements provided in Chapter 5 of this document is to be included in CEN ISO 19299 in an informative annex as the “REETS requirements profile”.
5. In particular, the group stresses the fact that the choice of not imposing RQ.DS.01 (*Access to stored data shall only be granted after authorization*) mandatory for the OBE, is due to considerations related to the difficulties arising in implementing the measure in short time for all the toll domains comprised in the REETS scenario. However, to achieve a high level of data security and privacy in the European context, the group highly recommends to reconsider this choice in a subsequent phase.
6. We suggest that the REETS WP5 takes over the results of the work done by WP4 in order to define the rules to be followed by the Interoperability Management with regards to the development and maintenance work in the Security Policy framework.

2 Scope and methodology of the work

2.1 Scope

The main objective of the sub activity 4.2 and its deliverable D4.3 was to define suitable and shared security policy elements for the specific EETS environment. Therefore, the first issue to be addressed has been to find an agreed definition about what a security policy is and which elements it shall contain. The present document may be considered as a reference in order to provide a common understanding of what a REETS or EETS security policy could contain.

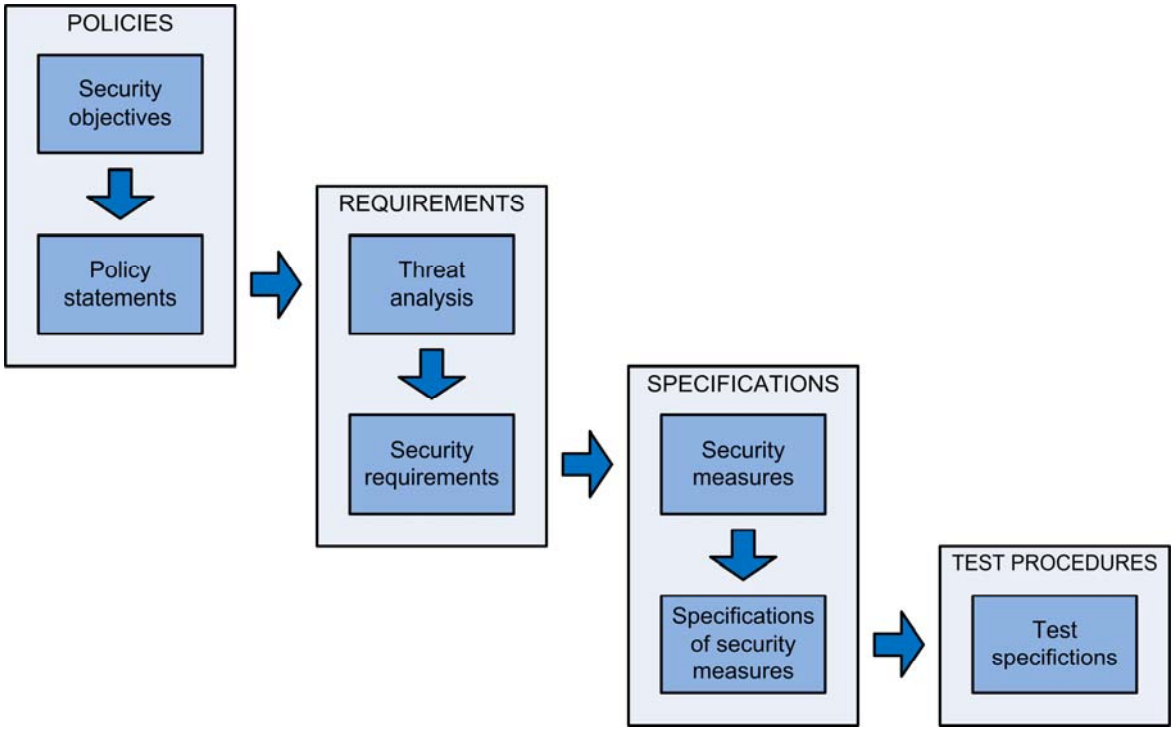

Figure 1: Development path for the security documents

There is not a one only definition of Security Policy and many examples are easy to find even in reliable websites on the Internet. Moreover, several EU Directives related to data privacy have to e considered when defining a REETS Security Policy (in Annex B a non-exhaustive list of Directives is described). A security policy, in fact, aims at providing management directions and support for information security in accordance to business requirements and relevant laws and regulations at EU and national level.

An example of the possible contents for a (information) security policy is provided below, taken from clause 5.1 of ISO/IEC 27002:

"The information policy document should state management commitment and set out the organisation's approach to managing information security. The policy document should contain statements concerning:

- *a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;*
- *b) a statement of management intent, supporting the goals and principle of information security in-line with the business strategy and objectives;*
- *c) a framework of setting control objectives and controls**,** including the structure of risk analysis and risk management;*
- *d) a brief explanation of the security policies principles and objectives, standards and compliance requirements of particular importance to the organisation, including:*
  - *1) compliance with legislative, regulatory and contractual requirements;*
  - *2) security education, training and awareness requirements;*
  - *3) business continuity requirements;*
  - *4) consequences of information security policy violations;*
- *e) a definition of general and specific responsibilities for information security management, including reporting information on security incidents ;*
- *f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.*

The information security policy should be communicated throughout the organisation to users in a form that is relevant, accessible and understandable to the intended reader."

Although the sub activity 4.2 of Activity 4 is called Security Policy, from the content point of view a definition of a binding security policy (as outlined in clause 5 of ISO/IEC 27002) is out of the scope of this deliverable and beyond the possibilities of the current project. In regard to security policy in the frame of REETS, the main objective of the sub activity was to deliver **security policy elements**, required to fulfill such a guideline. The outcome of the current document covers more or less point a) and parts of point b), d) and e) – the security policy in chapter 3 – and the first part of point c) – the security requirements in chapter 5 – from the list above.
One of the main objectives (and one of the outcome mentioned before) of this sub activity was also to look at the individual security requirements of toll domains by analyzing inputs from EETS domain statements and in particular from project members. The result shall be a recommendation about the potential for harmonization of security requirements with the possible inclusion of the definition of a common set of security elements that shall be used to improve trust between all REETS stakeholders and to simplify technical implementations and testing.

2.2 Terms and definitions

In the frame of the REETS project and in particular in this document, the acronym used to indicate the provider of electronic toll collection service is SP (unless otherwise specified or derived from another document taken as a reference). EETSP (or EP) is used, when referred explicitly to a SP registered at European level in its country. As an additional explanation, the following are possible stages for a SP before becoming a EETSP:

i. Service Provider (SP) is an entity providing a general Service to its customers (including any kind of toll collection service);

ii. Toll Service Provider (TSP) is a an entity providing any kind of Toll Service to its customers, on one or more toll domains for one or more classes of vehicles;

iii. Electronic Toll Service Provider (ETSP) is an entity providing Electronic Toll Service (by means of an OBU) to its customers, on one or more toll domains for one or more classes of vehicles. The term is dealing with services offered in a limited area of operation (e.g. national, cross border,…) or in Toll Domains of several countries in Europe (for instance TIS-PL, Ecotaxe, Via-T, Via Verde, Telepass and Liefkenshook) .

iv. European Electronic Toll Service Provider (EETSP or also EP for brevity) is a legal entity registered in the country where it is established, and recognized at European level providing the EETS (European Electronic Toll Service) to its customers, as stated in the acts defined by the Directive 2004/52/EC, Decision 2009/750/EC and Application Guide published in 2011.

2.3 Methodology

The group decided to follow two complementary approaches to develop some of the elements of a security policy (as indicated in ISO/IEC 27002). They are basically derived in the top-down and bottom-up approaches. The both of them have been applied to develop one of the two main outputs of this deliverable:

a) The top-down approach was applied to derive the security policy;

b) The bottom-up approach was applied to derive a common set of security requirements.

In addition, one more step has been followed:

c) an analysis of the security implementation issues containing a description of further recommended steps to be taken into consideration in relationship with the agreed concept of security policy.

However, it is to be underlined that recommendations made within the REETS environment are to be considered generally valid and they might be taken into consideration for future EETS implementation.

a) Top-down approach:

A first approach is the top-down method, starting with the over all security objectives and then detailing these objectives into security policy statements. These policy statements will then be the guideline together with a risk analysis to select the required security requirements and measures, for example form a requirements and measures catalogue as provided by the EFC Security Framework in CEN TS 16439.

Chapter 3 of the current document contains this approach with a security policy adopted form a policy which was originally developed in the Stockholm group (Report EETS SECURITY POLICY, V1.2, 07 September 2012) and then further elaborated for the EasyGo project (EasyGo security policy, V1.0, 28 August 2013). It shows the outcome of the first two steps without selecting requirements and measures.

The choice to use the EasyGo security policy as a starting point was made because it has been considered a solid base and some Toll Chargers in the EU are already working with it. In addition some of the REETS project members have been involved in drafting the Stockholm Group EETS security policy which was the starting point for the EasyGo policy. In addition, another benefit was given by the "high level security objectives" listed in Annex A.2.1, already fulfilled completely for the TC in Austria/Denmark and Switzerland and mostly in Germany, following the original wording of the EasyGo security policy objectives and statements. Some other contexts (like TIS-PL, VIA-T, Autostrade per l'Italia) have been analysed as well, taking into account their existing security policy in place for some ten-to-fifteen years, due to the operational experience regarding security and considering the amount collected per year.

Such a top-down approach is more appropriate when explaining and discussing security issues with management or in general with less technical oriented project members in order to achieve consensus or when security decisions are required.

b) Bottom-up approach:

The more or less bottom-up approach has been used to analyse the individual security requirements using two questionnaires sent out to the REETS project toll domains. The first questionnaire was about the applicable security requirements and the second one about the security measures that are implemented (or planned to be implemented) for the EETS (not all project members have already a complete EETS system and interface implementation). Both questionnaires have been based on the requirements and measures provided by CEN TS 16439 with the request to include additional, system specific requirements or measures.

The synthesis of the answers from the project members is provided in Annex A. The extract from that synthesis is the lists of security requirements that can be considered commonly agreed among REETS participants. This so called "common set of REETS security requirements" is provided in chapter 5.

This bottom-up approach is especially then useful when analysing the security of existing implementations or only parts of it, which is the case in the REETS project.

Chapter 4 of the current document describes the context and environment for a toll system as an introduction and explaining the grouping or classes of selected security requirements.

c) Security implementation issues:

A collection of security implementation issues to be decided for the REETS implementation phase is provided in chapter 7 to 9. Chapter 7 is pointing out that a technical trust model has to be selected and details the open implementation issues. For the security measures to be implemented it was assumed that they will be selected based on the recommendations from CEN TS 16439 (see chapter 6). But there was no deep investigation on the details of how the security measures should be implemented technically. The detailed solution was taken whenever possible form CEN TS 16439. In case the EFC Security Framework provides several options for the implementation, the open issues and decisions have been pointed out in these chapters.

i. Further recommended steps:

The selection process of the security requirements needs to be agreed by all REETS stakeholders based upon the commonly agreed security policy. The choice of security requirements as well as the associated measures selected from the European standards should be enhanced by a risk analysis of the REETS system during the implementation phase in order to protect those data processes not already covered by the standard resulting in being threatened in the relationships between TC and SP.

2.4 Revision of referenced standards

CEN TS 16439 is currently under revision and will be issued in the next version as CEN ISO TS 19299. In addition also EN ISO 12855, EN ISO 12813, EN ISO 13141 and CEN ISO TS 17575 part 1 to 4 are under revision. Some of the security related definitions defined in the EFC security framework CEN TS 16439 have been defined there to fill gaps in the other mentioned standards. During the revision of all these standards the security definitions will be moved whenever possible to the standard where they belong to.

It is therefore recommended to revisit the current document after the revision of these standards in order to align the references to standards but also in particular to include changes in the lists of security requirements and measures in CEN ISO TS 19299. Also the open security implementation issues should be revisited taking into account possible new definitions in the standards.

3 Security Policy

3.1 Scope of a security policy

This security policy covers the aspects of information security in the REETS environment. It covers the common assets and processes of all involved EFC systems at the toll chargers (TC) and toll service providers (SP).

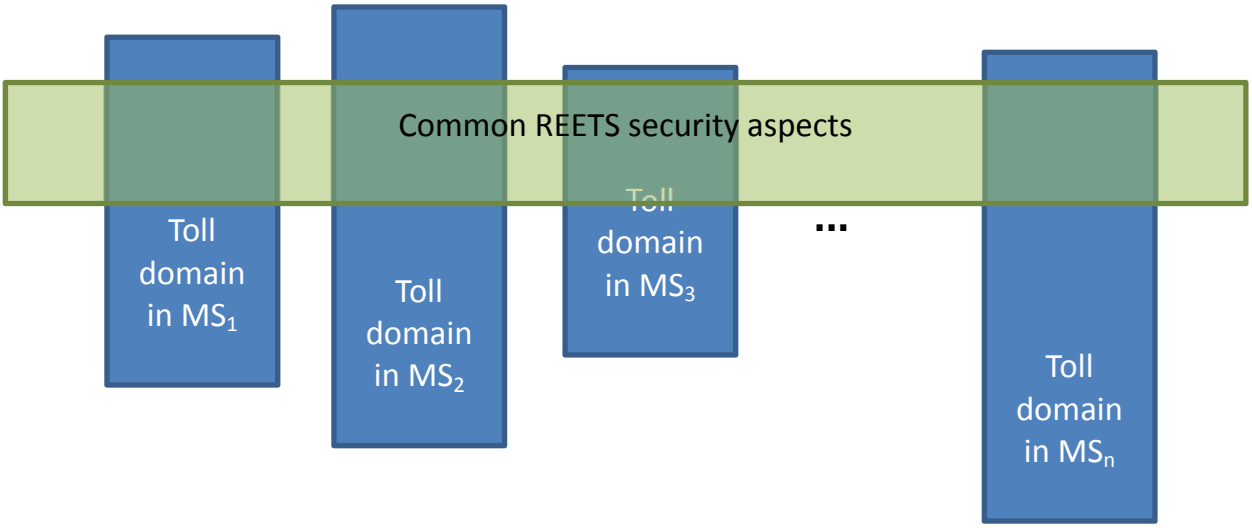

Figure 2: Roles in the toll charging in the REETS service environment

This policy applies to the information and communication infrastructure of the REETS parties including:

- Physical assets such as OBE, RSE, computer equipment etc.
- Software assets stored and used by the physical assets
- Information assets such as information stored in databases, information exchanged on interfaces between the physical assets, user manuals, procedures etc.
- Interfaces between the physical assets

This policy applies to organisations and their sub-contractors that are part of REETS.

This policy also applies to all employees including permanent and temporary staff and any other persons who require access to information and/or manage information as part of REETS.

While some aspects of security are determined as overall governing high level objectives and are therefore stated in this chapter other aspects are more detailed and will be handled as security requirements or security measures in later chapters.

3.2 Introduction to security

3.2.1 REETS service

The REETS service is an interoperable electronic fee collection (EFC) service provided by the participating TCs and SPs.

The REETS service shall cover the following main issues:

- Any service user using an OBE issued by a REETS SP can use it for toll charging at any TC offering the REETS service.

- The service has to be specifically requested by the service user (opt-in).

The development of the REETS service shall be done in accordance with the EU Directive 2004/52/EC[1], Decision 2009/750[2] and coordinated with on-going European research & development and standardisation work.

The REETS service is based on a foundation of experience from many years of EFC operation by the participating TC's and SP's as well as results from European EFC projects:

- Agreements and contracts are based on CESARE III and CESARE IV principles
- Architecture of the service is based on ISO 17573
- Different EFC transaction protocols are used, i.e. DSRC according to EN 15509 or ETSI ES 200674-1 or GNSS/CN
- The concept allows a dynamic growth across geographical borders and modes of transport (ferry, bridge, motorway …) to finally reach an EETS service

The provision and the quality of the REETS service as well as the information security is the responsibility of a governing body to be developed by WP5 Interoperability Management. This REETS security policy expresses the TC's and SP's commitment to the implementation, maintenance, and improvement of its information security management system. The REETS project mandated the WP4 to develop an initial information security and its necessary elements (see chapter 3.4). The further maintenance of the information security needs to be organized then in the governing body to be developed by WP5.

By information security is meant the protection of information (with focus on electronic data) stored and/or handled by the personnel, transferred over various interfaces and the assets involved in the provision of the REETS service.

3.2.2 Background

Information and the supporting processes, systems and networks are very important business assets in electronic fee collection systems. The whole business model is based on collecting information, handling it and then collecting the payment from service users based on the collected data. Information security is essential for the accuracy, trustworthiness, reliability and availability of the involved EFC systems as well as for the privacy of the service users.

The REETS service is intended to combine several formerly independent toll domains into a network covering a broad area in Europe. It is evident that the security threats, vulnerabilities and consequences of any breaches of security are much greater in the whole integrated and interoperable REETS area than they are in each separate system of an independent TC. The threats can both be internal (inside each local organisation or inside the REETS organisation to be developed by WP5) and external.

Examples of such threats are computer-assisted fraud, sabotage, vandalism and service denial (e.g. 'I was not there') enabled by unauthorised access, computer hacking and malicious code.

Figure 2 shows in principle the REETS actors, their assets and the data exchange interfaces between them that are subject to the REETS information security. A more detailed description of the assets is given in Figure 5 in chapter 4.1.

[1] Directive 2004/52/EC of the European Parliament and of the Council
[2] Commission Decision of 6 October 2009 on the definition of the European Electronic Toll Service and its technical elements (2009/750/EC)

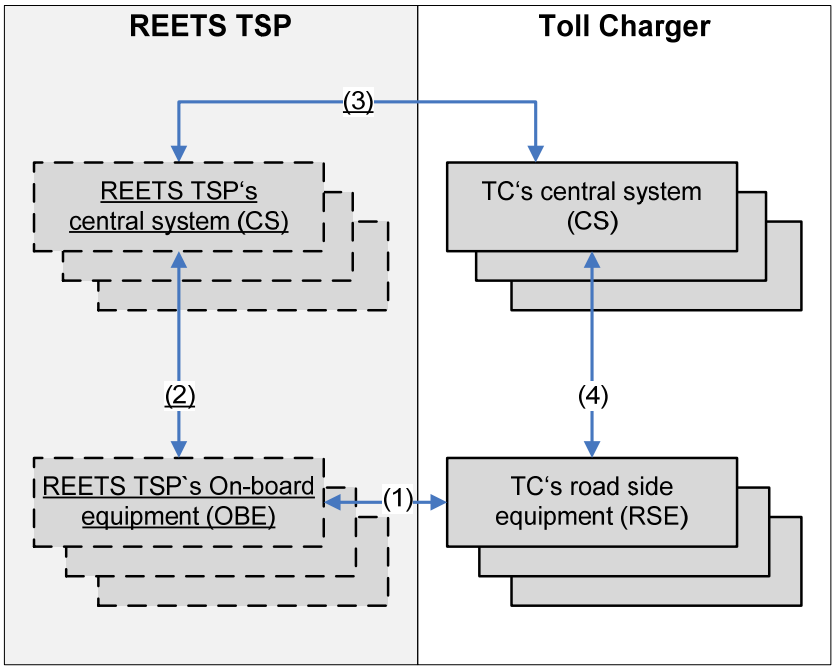

Figure 3 actors and data exchange interfaces subject to security in REETS

The interoperability constituents subject to the REETS information security are the REETS SP`s OBE, the TC's RSE and both central systems (CS) of TC and SP.

The interfaces subject to the REETS information security are between REETS SP`s OBE and TC`s RSE (1), between REETS SP`s OBE and REETS SP`s CS (2), between REETS SP`s CS and TC`s CS (3), and between TC`s RSE and TC`s CS (4).

The interface (1) is an interoperable interface in REETS: security threats may also exist for the interface (1) and (3).,The SP internal interface (2) and the TC internal interface (4) also need to be covered.

3.3 Objectives

The aim of this chapter is to define a REETS security policy which is strongly recommended to all actors in REETS or at least form a common understanding of the guiding principles to be used during the implementation of REETS for all information being handled by the actors in regard to REETS.

The security policy is composed by a set of rules and procedures that shall be continuously developed and maintained by the governing body entitled within the REETS WP5. Each new revision will become in force as a recommendation and substitutes the previous one.

The objective of it is to provide support for information security in accordance with business requirements and relevant laws and regulations. It sets a clear framework and demonstrates support for, and commitment to, information security through its initial issuing and continuous maintenance. A common set of security elements will thus facilitate better cooperation between all REETS actors while mitigating the common security threats.

This security policy underpins and motivates the requirements and the technical security specifications both during their creation, but also as they evolve during their life cycle.

The security policy shall also contribute to the REETS goals and strategies and shall support and protect the operation, competitiveness, general confidence and reputation of REETS.

3.4 Implementation method

The main content of the **REETS security policy** are the security objectives in chapter 3.5 and the policy statements in chapter 3.6, expressing the intentions of the REETS actors to commonly deal with information security.

Based on this security policy the following part of chapter 3 aims at defining the implementation of a common REETS information security by applying the security threat analysis taken from the EFC security

framework CEN TS 16439 and the input given by the project participants in Annex A, describing concrete security requirements and detailed security measures and develop a security test specification on how to test each participating system. This last step may only be developed after the implementation of REETS becomes clearer and is thus not yet covered by this deliverable.

This policy will constitute the baseline from which to develop the **REETS security requirements**. It should be based on a REETS risk and vulnerability evaluation[3]. During this, the requirements should be chosen individually from the CEN EFC Security Framework[4].

The **REETS security specification** contains the detailed specification of each of the chosen requirements that is described by one or many security measures to be taken for the implementation of a common approach to information security. These are also derived from the CEN EFC Security Framework. The details of how to implement these described security measures are determined locally in each toll domain.

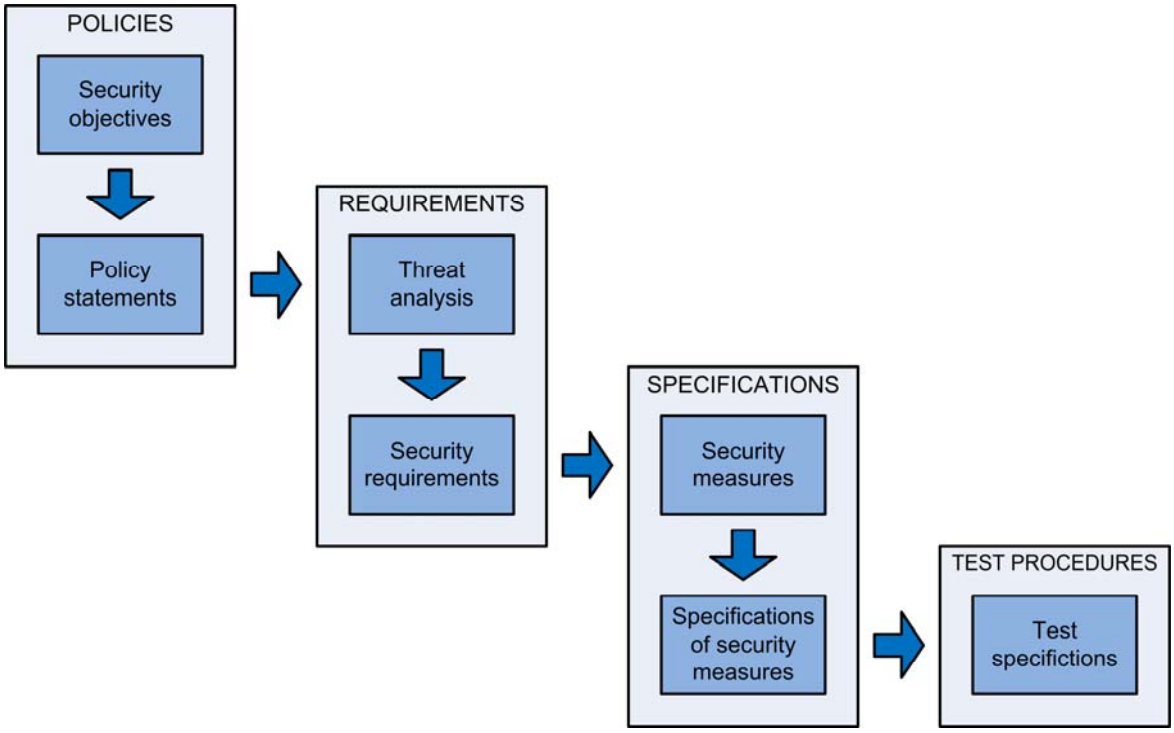

Figure 4 Development path for the security documents

The **REETS security test procedures** will describe the detailed conformance tests to prove that the local implementation of the REETS information security covers all defined security requirements, security measures and/or security policies. These test procedures shall include an Implementation Conformance Statement (ICS) to be provided by each REETS actor.

3.5 Security objectives

The REETS security policy shall be guided by the security objectives listed below. They express a general guideline and shall, in the case of a conflict with any of the detailed policy statements in chapter 3.6, have a higher priority. They can also serve as a management summary of the approach to security in REETS. The security objectives are numbered as SO-n.

[SO-1] Any REETS toll data exchanged between a TC and a TSP shall fall under the REETS security rules

The REETS security rules apply only to the toll data relevant for the REETS services.

[3] The security requirements in chapter 5 in this document have been collected by a questionnaire and are not driven by a risk analysis. The synthesis from the answers of the involved Toll Domains is provided in Annex A.
[4] CEN TS 16439 - EFC Security Framework

[SO-2] REETS toll data shall be correct, complete, traceable and protected

- Correct REETS toll data fully and accurately records all required road usage parameters according to the rules of the REETS toll scheme.

  This statement also covers the transmission of data between actors and thereby delivers data integrity in communication.

- Complete REETS toll data means that no toll data is deliberately or otherwise lost according to the rules of the REETS toll scheme.

  As a complement to the correctness requirement, toll data must also be complete. That means that no data that shall be reported can be suppressed. This statement emphasizes the need to secure not only correct recording, but also correct reporting and thereby ensures data availability.

- Traceable REETS toll data can be traced back to its originator/owner in a manner that its veracity can be contested and proved with enough confidence to be able to stand as evidence in a dispute.

  As data is refined through its process chain, passing from one actor to another, the responsibility and ownership of data must be clear at each step. In particular, if errors or falsifications are added in one part of the chain, while the other parts are correct and in compliance with system requirements, it shall still be clear which actor is accountable.

- Protected REETS toll data can only be accessed by authorised parties.

  The various REETS systems shall for all parts of the REETS toll data clearly define which actors under which conditions can access it. The upholding of these definitions shall be supported by cryptographic, administrative and/or other procedures. This statement delivers data confidentiality.

NOTE: SO-2 thus covers the Confidentiality-Integrity-Availability (CIA) triad

[SO-3] Risk and efficiency should be considered when implementing security in REETS

As large funds will be transferred between the individual actors in the REETS toll scheme it is a top priority that it delivers a high level of security and reliability. It is very important that the toll due for the usage of an infrastructure can be imposed to the correct service user which used this infrastructure.

It will never be possible to achieve perfect security and reliability in any operational system. Rather, the question is how reliable and secure a system has to be to fulfil its needs for the involved actors. At a certain point, the marginal costs that must be incurred in order to increase security and reliability one more step will represent a disproportionate effort, the costs will exceed the additional benefits.

The evaluation of risk and efficiency shall be made when implementing the requirements and security measures based upon the threat analysis from the EFC security framework CEN TS 16439.

Costs and benefits shall in this context refer to both the economic resources of all actors and to the time and effort needed from the service user to be compliant with the system.

[SO-4] The REETS security requirements shall be limited to supporting interoperability between the involved actors

REETS is a compound of many separate toll domains that differ in many ways, for example in technical solutions, legal requirements and operational procedures.

The different charging scenarios shall be respected, possibly leading to specific security requirements for the different types of toll domains. The common security requirements resulting from this policy shall therefore be limited to the common aspects of the whole of REETS.

- Security requirements shall be applicable to different charging scenarios: barriers vs. free-flow
- different technical solutions:, DSRC vs. autonomous systems
- different legal requirements: fee vs. tax
- different operational procedures: mandatory vs. non-mandatory OBU

This limitation in scope represents a pragmatic recognition of the history of the currently participating toll domains and the difficulty of fitting them into a common interoperable framework as well as to expand the REETS service to new toll domains to form the EETS service.

3.6 Policy statements

The security policy contains policy statements on how it is intended to protect information in REETS. Each statement requires more detailed procedures and practices to be implemented which in turn will contribute to the overall reduction in risk as a whole. The security policy is a way of assuring the confidentiality, integrity and availability of assets in the REETS and its information and communication architecture and infrastructure for the benefit of the service users and the TC`s and SP`s participating in REETS.

3.6.1 General policy statements

[PS-1] The objective of the information security is to:

- ensure confidentiality, integrity and availability of all information in the EFC service operation and management;
- prevent and limit the consequences of unwanted or unexpected information security events;
- build the required trust and confidence between the involved actors.

[PS-2] REETS will use international and European security standards and European and national legislation for personal data integrity.

The standards

- ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements"[5]
- "ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management"[6] and
- EFC Security Framework[7]

shall adhere to in the REETS information security or equivalent standards, guidelines or specifications, like the "IT-Grundschutz Catalogues" of the German Federal Office for Information Security.[8]

[PS-3] The REETS information security shall provide the involved parties with the means (specifications, procedures etc.) to fulfil legal, regulatory and contractual requirements regarding information security, data protection and privacy.

[PS-4] Sensitive personal data shall be protected by reasonable security safeguards against the risks of loss or unauthorized access, destruction, use, modification or disclosure of data.

The rules of the EU Directive 2006/24/EC on data protection shall be observed.

3.6.2 Organisational policy statements

[PS-5] REETS information security shall be governed, developed and managed by the interoperability management to be established by WP5 and reviewed by the actors in REETS.

[5] Covers all types of organisations (e.g. commercial enterprises, government agencies, not-for profit organisations) and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organisation's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of individual organisations or parts thereof.

[6] Establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation.

[7] Describes a set of requirements and security measures for stakeholders to implement and operate their part of an EFC system as required for a trustworthy environment according to its basic information security policy. In general the overall scope is an information security framework for all organisational and technical entities and in detail for the interfaces between them.

[8] Since a majority of the requirements and security measures in the draft EFC Security Framework are optional, adhering to the standard still requires selecting the appropriate ones. This should be done in the REETS security requirements document and in the REETS security specification respectively.

The interoperability management shall develop, coordinate and maintain and constantly improve the REETS information security.

The actors in REETS shall support the implementation of the REETS information security and review all actions taken by the REETS actors.

The actors in REETS shall provide the resources required for these tasks.

[PS-6] The REETS Interoperability Management shall develop and maintain the Security Policy.

WP5 will define the rules for the work of the Interoperability Management.

[PS-7] The interoperability management shall develop and maintain the selected REETS security requirements. All security requirements shall be chosen from the EFC security framework based on the return on experience of the REETS partners in Annex A and a continued risk and vulnerability evaluation including a simplified risk analysis.

The REETS information, assets, interfaces and processes shall be assessed and grouped to indicate the need, priorities and expected degree of protection.

[PS-8] The interoperability management shall develop and maintain the REETS security specification. All security measures shall be derived from the identified security requirements. The choice of security measures shall be based on the required level of protection.

The chosen security measures shall be capable to prevent, detect, track and handle unwanted information security incidents.

[PS-9] The interoperability management shall develop and maintain the REETS security test procedures to enable the testing of REETS actors' assets, interfaces and processes. The REETS security test procedures shall be able to prove the compliance to all security measures and security requirements.

[PS-10] The REETS information security shall be subject to regular reviews with planned intervals or when significant changes related to information security occurs.

Regular risk evaluations shall be carried out as a revision of the REETS security measures and operative practice. In addition, risk evaluations shall be carried out when there are significant changes to the threat situation or vulnerabilities have been detected.

[PS-11] The default solution to establish initial trust between the REETS operators (Toll Chargers and REETS Providers) shall be a peer-to-peer trust model but a mixed model also allowing for hierarchical trust models shall be supported as well.

[PS-12] Technical audits will be undertaken, as determined by the REETS interoperability management. Any technical audit work must be carried out under the supervision of technically competent and authorised personnel.

Any auditing of operational systems shall be carefully planned to minimise disruption to the continuous operation of the system. All auditing work requires an approval from the management of involved system(s) before it starts.

Such audits may include penetration testing after the targeted REETS actor or asset has been informed.

[PS-13] The auditing of live data shall be limited to read only checks. Any type of audit requiring a change of data shall be carried out on copies of the data, which shall be destroyed after it is no longer required.

3.6.3 Asset and interface management policy statements

[PS-14] There shall be a compliance check for all new assets, interfaces and processes introduced by existing or new REETS actors based on the REETS security test procedures.

[PS-15] The level of REETS information security shall not be reduced by the introduction of new REETS actors, services or products.

[PS-16] All REETS assets shall be accounted for and have a nominated owner.

[PS-17] Any users of REETS assets shall be granted access to the appropriate systems, their resources and their information only after this access was authorised by the owner of the asset.

Anyone granted access to REETS assets shall follow the internal guidelines for secure use. These internal guidelines for secure use will be included as set of measures in the REETS security specification and shall be adopted by each REETS actor.

[PS-18] Full traceability of processed information shall be guaranteed at all times.

[PS-19] The interoperability management shall maintain a process for suppliers and TSP to get their components and procedures qualified with regards to the REETS security test procedures specified by WP2. The process shall also apply to additions and modifications to the components and procedures.

3.6.4 Incident management policy statements

[PS-20] The REETS information security shall limit the consequences of unwanted information security incidents.

[PS-21] Anyone using the REETS assets shall report any unwanted information security incident or violation of the REETS information security to the interoperability management.

The interoperability management shall initiate a security revision and/or other necessary internal inspections to accommodate a systematic improvement and learning process to minimise the risk of similar events and non-conformances.

4 Security environment and requirement classes

4.1 Security environment

The diagram in the following Figure 5, taken from CEN TS 16439, shows the overall security environment of tolling systems. The diagram enhances the interoperability interfaces shown in Figure 2 with additional SP and TC internal and external interfaces. The connections with the Interoperability Management are not shown.

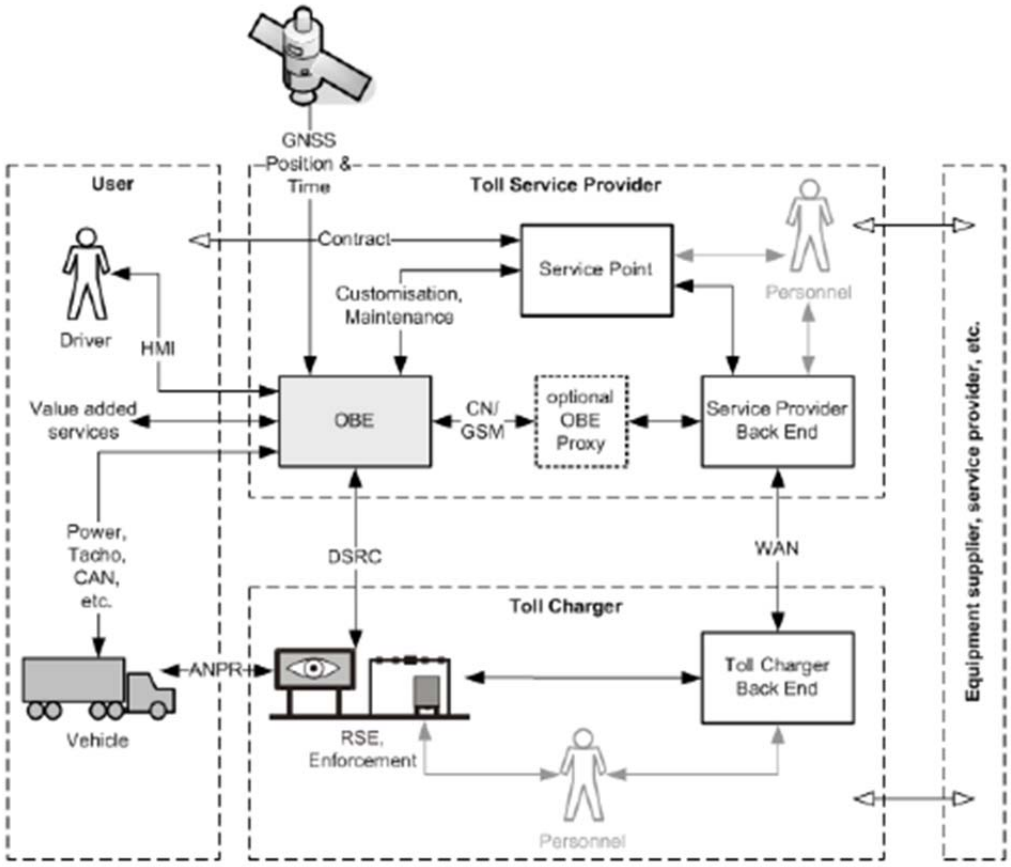

Figure 5. Security environment of tolling systems

The diagram outlines four major areas of responsibility. Three of them correspond to the general roles defined in the EFC system architecture (ISO 17573):

1. The Toll Charger
2. The Toll Service Provider
3. The User
4. Other external entities (manufacturers, communication service provider, etc.). This is not covered by the EFC architecture standard but is needed to cover the security related interfaces.

In addition to cover the issues in an interoperable tolling environment, a not shown role has to be mentioned:

5. The Interoperability Management (which has no communication interface to other roles in the daily operation)

The data exchange across interfaces is shown in the diagram as arrows.. Some of these interfaces are covered by standards. Securing these interfaces is a pre-requisite to ensure security in the whole system.

The present selection of security requirements and measures defines the foundations for a REETS security implementation basically on securing interfaces among participating actors incarnating a specific EFC role. However, some requirements and measures to ensure end-to-end security in some cases have been identified.

4.2 Security requirement classes

4.2.1 Introduction

The organisation of the REETS security requirement selection in the following chapters and Annex A is based on the grouping of security requirements according to CEN TS 16439. The security requirement groups or classes are briefly described in the sub-sections that follow.

4.2.2 Information Security Management System

The ISO "Information Security Management System" family of standards (ISO 27001 to 27007) is covering in theory all the well known and common aspects of information technology systems. Some parts of an EFC system are from the IT perspective not different from any other IT system. Therefore this requirement class covers all well known and common security requirements for the general IT system parts of an EFC system (e.g. data centre access, password rules …).

4.2.3 Communication interfaces

The requirements contained in this class refer to the data exchange communication system as a whole and, consequently, include the requirements for the DSRC charging transactions, the compliance check (ISO TS12813 Compliance Check Communication for Autonomous Systems - CCC), the localization transaction (ISO TS 13141 Localisation augmentation communication for autonomous systems - LAC), in autonomous systems the OBE to Proxy/SP communication (e.g. according to CEN/ISO TS 17575) as well as the communication between TC and SP according to EN ISO 12855. Moreover, these requirements are also related to internal interfaces using communication services of a third party. This includes but is not limited to the use of a telecommunication provider for:

- TC to RSE communication;
- SP to OBE communication;
- Internal Back End WAN communication.

4.2.4 Data storage

Data storage requirements are intended to be independent of the data processing. This class of requirements considers an OBE in the User environment, (e.g. a personalized OBE mounted into a vehicle) and the RSE at a public location without any additional external protection measure. The sections related to Back End data storage are covered by the ISMS requirements.

4.2.5 Toll Charger

The Toll Chargers' requirements defined in the EFC Security Framework have several different purposes, among which:

- Protection of Toll Charger's assets
- Assurance and protection of correct income to the Toll Charger
- Protecting the User and SP from overcharging
- Protecting the User from being wrongly enforced

This implies, for some of them, the involvement and support of the Toll Service Provider.

4.2.6 Toll Service Provider

Toll Service Provider requirements are mainly referred to the protection of the Toll Service Provider's assets and income, and this may imply in some cases the involvement of the Toll Charger.

4.2.7 User

User requirements for security (mainly privacy and user data protection) lead to requirements for the SP and TC.

4.2.8 Interoperability Management

The main security requirement for an Interoperability Management is to ensure the trust of all stakeholders in the interoperability scheme.

5 Security requirements

5.1 Generalities

This chapter lists the security requirements that can be considered as commonly agreed among REETS participants. The requirement list is derived by inputs by the REETS participants, therefore it is to be considered as a REETS proposal, independently on the standards referred to. No additional mandatory option has been forced where no explicit reference was made by every participant. A given requirement may not apply in all environments (example: specific requirements for autonomous-based tolling systems do not apply for DSRC related systems, and vice versa). Requirements are, however, listed here as REETS requirements, with no distinction on the type of tolling system, rather, on specific interface(s). Requirement identifiers are taken from CEN TS 16439.

For each class of requirements, a table has been produced, where for each requirement the REETS selection is expressed in terms of either **M** (Mandatory) or **R** (Recommended).

5.2 Information Security Management System

The requirements as in Table 1 have been identified as of interest in the REETS project.

No	Requirement	REETS selection
RQ.ISMS.1	Establish, implement, operate, monitor, review, maintain and improve an Information Security Management System (ISMS) according to ISO/IEC 27001	**R**

Table 1. ISMS requirements

5.3 Communication interfaces

Requirements for the communication interfaces may apply for three classes of interfaces, namely:

1. The DSRC interface, which, in turn, can relate to
    a. a tolling transaction for DSRC based tolling systems
    b. an enforcement transaction (CCC) for autonomous based tolling system
    c. a location augmentation transaction (LAC) for autonomous based tolling systems.
2. The interface between the Toll Charger and the Service Provider
3. The interface with the Communication Provider, that is the interface between Road Side Equipment and Toll Charger and the interface between the front end/OBE and the SP.

The following Table 2 shows the requirements related to the above interfaces.

No	Requirement	DSRC	TC/TSP Interface	Comm. Provider
RQ.IF.02	Data exchange shall be done using transmission channels with reliable availability.	**M**	**M**	**M**
RQ.IF.10	Data exchange shall guarantee data confidentiality.	**R**	**M**	**M**
RQ.IF.11	Data exchange shall guarantee data integrity.	**M**	**M**	
RQ.IF.12	Data exchange shall guarantee the authenticity of the data originator.	**M**	**M**	**R**
RQ.IF.13	Data exchange shall guarantee non-repudiation with proof of origin.	**M**	**M**	**R**
RQ.IF.14	Data exchange shall guarantee non-repudiation with proof of delivery.		**M**	**R**
RQ.IF.30	Data exchange shall allow the detection of resent messages (protection against replay attacks).	**M**	**M**	

Table 2 Interface requirements

NOTE: The current analysis does not cover the GNSS satellite interface because to add any security requirement or measure to the specification and implementation of this interface is out of the scope of the REETS project.

5.4 Data storage

The following Table 3 shows the requirements related to data storage.

No	Requirement	OBE	RSE
RQ.DS.01	Access to stored data shall only be granted after authorisation.	**R**	**M**
RQ.DS.02	Access to store data shall only be granted via defined interfaces and defined procedures.	**M**	**M**
RQ.DS.03	Stored data shall have an independent backup storage.		
RQ.DS.05	Data storage shall guarantee data integrity.	**M**	**M**

Table 3 Data storage requirements

NOTE:

1. RQ.DS.01 for OBEs is only possible for the DSRC interface introducing security level 1.
2. The back office interfaces are dealt with in the ISMS requirements section.

5.5 Toll Charger

The following Table 4 lists the requirements that are specific to Toll Chargers

No	Requirement	REETS selection
RQ.TC.01	The Toll Charger shall determine if factual road usage is represented by a corresponding set of toll declarations (enabled by RQ.TSP.51).	**M**

No	Requirement	REETS selection
RQ.TC.02	The Toll Charger shall be able to determine if a toll declaration is based on correct and complete road usage data (enabled by RQ.TSP.52).	M
RQ.TC.03	The TC shall determine, in a spot check, if an OBE is in an OK operational state.	M
RQ.TC.04	The TC shall check the integrity and authenticity of the received data as compared to the data sent from the Front End.	R
RQ.TC.05	The TC shall determine if toll declarations are based on data originating from a legitimate Front End and/or TSP back office (enabled by RQ.TSP.55).	M
RQ.TC.20	The TC shall detect RSE damaging and recover the RSE functionality.	M
RQ.TC.21	The TC shall detect theft of RSE parts and recover the RSE functionality by a replacement of the stolen part.	M
RQ.TC.22	The TC shall implement RSE authentication measures for DSRC communication.	M
RQ.TC.23	The TC shall detect RSE malfunction and correct the malfunctioning RSE functionality.	M
RQ.TC.91	Distributed EFC context data shall feature non-repudiation with proof of origin and delivery.	M
RQ.TC.92	The TC shall only accept an OBE after detecting if an OBE belongs to a trusted Service Provider and if the Service Provider guarantees payment for that specific OBE (enabled by RQ.TSP.62).	M
RQ.TC.93	The TSP shall protect the TC against repudiation by users of invoices and CCC events.	M
RQ.TC.94	Received Exception Lists shall feature non-repudiation with proof of origin.	M
RQ.TC.95	The TC shall be responsible for the availability of his interfaces according to agreed service levels.	M

Table 4. Toll Charger requirements

5.6 Toll Service Provider

The following Table 5 shows the Service Provider specific requirements

No	Requirement	REETS selection
RQ.TSP.07	An OBE shall not allow the User to modify fixed vehicle parameters.	M
RQ.TSP.09	The TSP shall notify the driver if the OBE is not working correctly.	M
RQ.TSP.13	The TC shall guarantee that distributed EFC context data features non-repudiation with proof of origin.	M
RQ.TSP.14	The TC shall guarantee that distribution of exception lists features non-repudiation with proof of delivery.	M
RQ.TSP.19	The TSP shall provide the TC with the means to identify the stolen OBEs.	R
RQ.TSP.20	The TSP shall manage stolen OBEs.	R
RQ.TSP.21	The TSP shall detect cloned OBEs and black list the detected OBEs.	R
RQ.TSP.40	The OBE shall not allow change of internal data via the user interface, except the data allowed to be changed.	M
RQ.TSP.41	The OBE shall only present intended data by the User interface.	R
RQ.TSP.42	The toll Service Providers implementation of the Front End and gathering and processing of data should be in compliance with the privacy requirements.	M

No	Requirement	REETS selection
RQ.TSP.51	The TSP shall enable the TC to determine if factual road usage is represented by a corresponding set of Toll Declarations (required to enable RQ.TC.01).	**M**
RQ.TSP.52	The TSP shall enable the TC to determine if a toll declaration is based on correct and complete road usage data (required to enable RQ.TC.02).	**M**
RQ.TSP.62	The TSP shall enable the TC to detect if an OBE belongs to the TSP (required to enable RQ.TC.92).	**M**
RQ.TSP.90	The Toll Service Providers systems should be designed in a way that access to stored or processed data is only possible within the legal context of the respective country (lawful interception).	**R**
RQ.TSP.91	The data communication between Front End (OBE) and Back End (TSP) back office shall be protected against interception in a way that access to stored or processed data is only possible within the legal context of the respective country (lawful interception).	**R**
RQ.TSP.92	Customisation of OBE shall be done in a secure way.	**R**
RQ.TSP.95	The TSP shall guarantee the availability of its interfaces according to agreed service levels.	**M**

Table 5. Toll Service Provider requirements

5.7 User

The analysis in Annex A has shown that no specific User security requirements have been identified. While this does not mean that security is not applied for user interactions, yet it does show that users security can and will be dealt with individually in liaison with the European Decision(s) on privacy.

5.8 Interoperability Management

The following Table 6 shows the security requirements for Interoperability Management. Although no input has been received and documented in Annex A, yet is has been deemed that these requirements are relevant for the implementation phase.

No	Requirement	REETS selection
RQ.IM.01	The Interoperability Management shall issue an EFC scheme security policy in collaboration with the involved stakeholders.	**R**
RQ.IM.02	The Interoperability Management shall have or define one or more auditing bodies supervising the security implementation of the TSP and TC involved in the interoperable EFC scheme.	**R**

Table 6. Interoperability management requirements

6 Security measures

Chapter 7 of the Security Framework standard, CEN TS 16439 lists the security measures satisfying a stated requirement. The selected requirements in the previous chapter will therefore define the common set of security measure(s) to implement for the REETS project. If the requirement covering an interoperable interface (e.g. the DSRC interface) is stated to be mandatory in chapter 5 the associated security measure defined in the EFC security framework CEN TS 16439 will be mandatory to implement for the REETS project.

Annex A provides the tables with the security requirements and the reference number of related security measures from the EFC security framework that Toll Chargers have already implemented in existing systems or they intend to implement in systems under development or improvement within the specified toll domain(s).

7 Trust model

7.1 Technical trust model: introduction

A technical trust model allows the identification of the entities involved in a common security framework as well as for the identification of the trust (expressed by security certificates) those entities can claim. Trust has to be established between:

1. Toll Chargers and Service Providers
2. Service Providers and Interoperability Management
3. Toll Chargers and Interoperability Management

The definition of a trust model implies a choice between:

1. *Hierarchical approach*
2. *peer-to-peer approach*

   or a combination of both

The default solution for the REETS members shall be a peer-to-peer trust model, but a mixed model also allowing for hierarchical trust models shall be supported as well (see [PS-11]).

7.2 Trust model implementation issues

The choice of all implementation details for the trust model is beyond the scope of the present document. The list of open decisions below is mentioned here as a prerequisite for the actual project implementation phase:

- ROOT- and self-signed certificate (i.e. trust relation) expiry times: How long shall be the validity of a root certificate?
- Certificate revocation procedures for every type of certificates: Is a certificate revocation list (CRL) used and what are the distribution mechanisms for the possibly several CRLs?
- Allowed certificate extensions: Which critical certificate extensions are required and supported? Are non-critical certificate extensions allowed?
- Issuing procedures for sub CA and entity certificates
- Certificate Revocation List profile and format

8 Security specifications for interoperable interface implementation

8.1 General

This section specifies the security mechanisms that have to be put in operation during the implementation phase according to the selected security measures. It includes the signature and hash algorithms to be used, as well as the detailed security specifications for interoperability constituents.

8.2 Signature implementation issues

8.2.1 Signature algorithm

CEN TS 16439 defines in clause 8.1.2 two different signature algorithms[9].

1. RSA according to ISO/IEC 14888-2:2008 clause 6

[9] During the current revision of CEN TS 16439, the specification oft the signature algorithm may be moved into the new versions of the interface standards, i.e. ISO 12855 and ISO 17575-1.

2. EC-DSA according to ISO/IEC 14888-3:2006 clause 6.4

The algorithm 1 is mandatory for back office interfaces. The decision for one of the two options for the algorithm used by the front end for the charge report signature has been left open.

The EC-DSA version has basically been introduced to support asymmetric signatures over the DSRC interface for the "compliance checking - secure monitoring" concept. Because there is no such implementation in the REETS project, the EC-DSA option for charge report signatures shall be prohibited to simplify implementations.

8.2.2 Signature length

During the implementation phase the required RSA length for CA and entity certificates signatures as well as the length of data signatures must be specified.

8.3 Definition of security algorithms

The following references to clauses of CEN TS 16439[10] specifying the security algorithms for the REETS implementation phase:

- The MAC algorithm whit its underlying block cipher as defined in clause 8.1.3
- The MAC key derivation algorithm as defined in clause 8.1.4.
- The key encryption algorithm as defined in clause 8.1.5
- The padding algorithm as defined in clause 8.1.6

8.4 DSRC security specifications

The following references to clauses of CEN TS 16439[11] specifying the DSRC security mechanisms for the REETS implementation phase:

DSRC-EFC:

- The OBE shall comply with clause 8.2.2 (NOTE: This requirement allows only the use of OBEs that support security level 1 of EN 15509)
- The RSE shall comply with clause 8.2.3

Clarification: each SP delivers OBUs with a specific security level selected in the profiles specified in EN 15509. Consequently, the RSEs shall have to be able to manage all the security levels specified in EN 15509. The implementation in RSEs is of responsibility of TCs.

DSRC-CCC:

- The OBE shall comply with clause 8.3.2
- The RSE shall comply with clause 8.3.3

DSRC-LAC:

- The OBE shall comply with clause 8.4.2
- The RSE shall comply with clause 8.4.3

[10] As a result oft the current revision of CEN TS 16439, the definitions may be moved to the interface standards.
[11] As a result oft the current revision of CEN TS 16439, the definitions may be moved to the interface standards ISO 12813 and ISO 13141.

8.5 Security specifications for Front End to SP interface

8.5.1 Front End to SP transport protocol security

No requirements to have a common set of security specifications of the transport protocol for the Front End to SP interface have been raised for REETS. Security for the transport protocol at this interface has to be thus implemented according to each entity's own security policy.

8.5.2 Charge Report authentication

In case the Charge Report has to be authenticated by the Front End and forwarded by the SP unchanged to the TC, the security solution according to CEN TS 16439 clause 8.6.5 shall be used.

8.6 Security specifications for TC to SP interface

8.6.1 Secure communication channel

The communication channel between TC and SP should be realised by using a VPN connection in order to satisfy the choice of requirements RQ.IF.21 and RQ.IF.30, and the consequently selected security measures SM241 and SM250,. How the term VPN connection should be interpreted is open, e.g. if it is a permanent or a session orientated connection. Nonetheless CEN TS 16439 recommends in clause 8.6.2 three different solutions for the implementation of this secure communication channel.

The analysis in WP4.1 has shown that the usage of web service communication and data exchange using File-transfer-Protocol are the transport protocols used the most by the participating partners.

Depending on that insight, the REETS project should decide for the implementation phase if a single security protocol from the choice of the recommendations of CEN TS 16439 is applicable and sufficient for the different implemented transport protocols or if individual security solutions are more appropriate.

8.6.2 Message authentication

The security implementation shall be according to CEN TS 16439 clause 8.6.3 to satisfy the requirements RQ.IF.12 and RQ.IF.13, and the related measures SM255, SM256, SM253 and SM254 that have been selected in REETS.

8.6.3 Proof of message delivery

The security implementation shall be according to CEN TS 16439 clause 8.6.4 to satisfy the requirements RQ.IF.1 and the related measures SM253 and SM254 that have been selected in REETS.

9 Key management

The key management procedures for REETS implementation phase shall be according to the specifications given in the EFC security framework CEN TS 16439 clause 9.

During the implementation phase, the set of allowed standards and protection profiles in CEN TS 16439 for the certification of cryptographic modules should be reviewed.

10 Final considerations

The security policy described in Chapter 3 of this document covers the aspects of information security in the REETS environment of all involved EFC systems, TCs and SPs. This policy applies to the information and communication assets of the REETS parties. This policy applies to organizations and their subcontractors that are part of REETS.

The security environment described in Chapter 4 of this document outlines five areas of responsibility:

i. The Toll Charger

ii. The Toll Service Provider

iii. The User

iv. Other external entities (manufacturers, communication service provider, etc.).

v. The Interoperability Management

The selection of security requirements and measures based on the guiding principles of the security policy and a risk analysis can be considered as basis for a REETS security implementation.

The requirements provided in Chapter 5 of this document are to be considered a guide to EETS Providers and Toll Chargers during the implementation phase of the system.
As stated, the security requirement list has been derived by the inputs given by the REETS participants since the beginning of the analysis. Any final adoption in terms of Recommended (R) or Mandatory (M) measure is fruit of the cross check among the inputs. A given requirement may not apply in all environments, but REETS requirements make no distinction neither on the type of tolling system nor on specific interface(s). For each class of requirements, we recommend the TCs and SPs to follow what are the indications produced in the related environment tables (ISMS, Communication Interfaces, Data Storage, TCs, SPs), where for each requirement the REETS selection is expressed in terms of either **M** (Mandatory) or **R** (Recommended).

In particular, the group stresses the fact that the choice of not imposing RQ.DS.01 (Access to stored data shall only be granted after authorization) mandatory for the OBE, is due to considerations related to the difficulties arising in implementing the measure in short time for all the toll domains comprised in the REETS scenario. However, to achieve a high level of data security and privacy in the European context, the group highly recommends to reconsider this choice in a subsequent phase.

Chapter 7, 8 and 9 are then to be considered a guideline for the application of the security policy in terms of model identification, interface implementation and check for the compliance.

Annex A : Inputs from REETS Participants

A.1 Introduction

The present Annex contains the synthesis of inputs received by the REETS Project participants about the security requirements and related security measures they have implemented or intend to implement within the specified Toll Domain(s), to then identify commonalities in requirements and in adopted measures.

The organisation of the present document is based on the classes of security requirements defined in ISO EN 16439. For each security requirements class, tables are provided that identify:

1. The requirements identified and described in the standard (taking into consideration possible evolutions)
2. Possible additional requirements identified in the REETS project
3. The security measures that the standard **prescribes** when a specific requirement is selected.
4. The security measures **adopted** by the participants to the REETS project.

The following criteria had been used in order to keep the tables' sizes to an acceptable minimum:

1. All requirements that are not requested by REETS participants have been removed from the tables.
2. Some requirements, as defined in the standard, have no corresponding security measures. Unless REETS participants have signalled specific measures for those requirements, the requirements have been removed from the tables, even though they had been marked as requested by some or all REETS participants.

A.2 Toll Chargers in the REETS project

The following table specifies for each Member State involved in the REETS project the Toll Charger(s) and the offered EETS services.

MS	Network and Toll Chargers	Description of Service offered in the network
CH	Federal Customs Administration (FCA) for the mileage-related heavy vehicle charge (LSVA)	• LSVA specific OBE • At present time no EETS service offered.
DE	Federal Office for Goods Transport	German Truck Toll system" / "LKW-Maut Deutschland

MS	Network and Toll Chargers	Description of Service offered in the network
F	1. ASFA Road Network - 18 Toll Domains (some are interconnected), with common technical and operational ETC procedures coordinated by the "Commission de Télépéage" led by ASFA 2. MEDDE – Ministry of Ecology, Sustainable Development and Energy	1. TIS PL for HGV- 5 qualified ETS Providers (Axxès, DKV; Eurotoll, Telepass, Total / AS24); these ETS P are also qualified for other Toll do-mains in Europe. • ASFA is insuring a single contact point in order to open and ease the whole accreditation procedure and facilitate the bilateral relationship to obtain accreditation. • Each Toll Charger,for its network (Roads, bridges, tunnels) signs a contract with each ETS Provider and only when all bilateral contracts are signed, the ETS Provider may start the operation. • Each Toll Charger has its own communication channel with each ETS Provider (for operational and monetary procedures) and is responsible/prime actor for any transaction payment occurred in its payment stations (for both inter-connected and non-interconnected transits). • The Toll Chargers are transmitting to ETS Providers all information regarding charging data and amount due; With this information, ETS Providers are issu-ing invoices to their customers on behalf of the Toll Chargers; • the payment by ETS Providers to Toll chargers is guaranteed; • the payment of the invoices by their customers to the ETS Providers is fully managed by the ETS P. Bilateral data exchanges between ETS Providers and Toll Chargers are based on Files exchanges and fully secured (see details hereafter in this document) The organization of the ASFA Road Network, with the qualified ETS P, is fully compliant to the ETS European scheme as defined by the Directive and the Decision. 2. ECOTAXE - To be completed
I	Italian interconnected network: set of 23 interconnected Toll Domains, in which common technical standards and operational procedures are shared among Toll Chargers.	SIT-MP (Italian Interoperable ETC Service for HGV): • A single contact point for SIT-MP Providers has been created (Aiscat Servizi) in order to open and ease the whole accreditation procedure and prevent a 1 to N starting relationship to obtain accreditation.. • Each Toll Charger within the interconnected network signs a contract with the SIT-MP Provider and only when the list of signatures is complete the SP may start the operation. • Each Toll Charger has its own communication channel with the SP (for operational and monetary procedures) and is responsible/prime actor for any transaction payment occurred in its exit stations (for both interconnected and non-interconnected transits). • After receiving the payment from SP, subsequent procedures (internal to the set of interconnected TCs) will provide the balance among TC.
PL	GDDKiA – General Directorate for National Roads and Motorways	viaTOLL Mandatory freeflow ETC system applying to all vehicles above 3.5 Tonnes maximum permissible gross vehicle train weight on specified roads (and ETC at plazas with barriers on state operated motorways).
E	Spanish toll network: 34 concessionaires with common technical and operational ETC procedures coordinated by the ETC Monitoring Committee led by ASETA	Via-T ETC system for light and heavy vehicles. Around 60 financial Service Providers and 7 non financial Service providers

MS	Network and Toll Chargers	Description of Service offered in the network
A/DK	Asfinag+Sund & Baelt (plus Sweden and Norway)	Toll Service Provider (SP): BroBizz A/S (Denmark) and ASFINAG ETS (Austria) EasyGo The EasyGo HUB acts as an interconnecting collection and forwarding system between the connected TCs and SPs. All data files that are to be exchanged between the central systems of the connected TCs and SPs will be routed through the EasyGo HUB. In addition to being an intermediary between the central systems of the connected TCs and SPs, the EasyGo HUB generates the following types of data available for TC and SP system supervisors: • Alarms • Warnings and other messages to supervisor(s) of data exchange operation • Statistics and reports of data exchange operations and general data traffic Data exchange between the EasyGo HUB, TCs and SPs is based on an FTP transfer through an encrypted VPN tunnel. The public internet is used as the underlying communication media. The EasyGo HUB and the central systems of the connected TCs and SPs shall be connected to the internet with the capacity and security architecture that is required to perform a smooth and secure operation of EasyGo.

Table 7: Toll Chargers involved in the REETS project

A.2.1 High level security objectives

The Table 8 that follows lists high level security objectives that some Member States have expressed. Detailed security requirements are derived from these high level objectives.

MB	High level security objectives
CH	Although there exists currently no CH EETS security policy, we have formulated some high level objectives: End-To-End Security Toll declarations data shall be undeniable assigned to its originating Front-End (authenticity): It shall be possible for the FCA to trace back toll declaration data to its originating Front-End in a manner that its veracity can be contested and proved with enough confidence to be able to stand as evidence in a dispute. Any alteration of Front-End generated toll declaration data shall be detectable by the EETS Provider and the FCA (integrity): • Front-End toll declaration data received by the EETS Provider or the FCA shall be complete (no data lost or suppressed) and correct (no data changed). The EETS Provider and the FCA shall be able to detect that there is missing or changed data B**ack-Office Interface Security** The back office interface between FCA and EETS provider shall guarantee confidentiality, integrity, availability and non-repudiation for all data transactions: • Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. • Integrity means that data cannot be modified in an unauthorized or undetected manner. • Availability of the interface shall be according to agreed service levels. The EETS provider shall deliver the required data during the defined timeframes. Loss of data caused by interface unavailability or malfunction shall not be possible. • Non-repudiation guarantees that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. **Privacy requirements regarding "data record of the assessment decision"** (from LSVA EETS Domain Statement, clause 3.4) The EETS Provider undertakes to disclose the assessment date to the EETS User in full and without alteration. The EETS Provider also undertakes to make further use of the data and/or to disclose the data to third parties only with the consent of the EETS User. As a result from this statement, the EETS Provider is obliged to protect the EETS User data from disclosing

MB	High level security objectives
	to third parties without the consent of the EETS User.
D	**Requirements on IT security are formulated in the EETS domain statement:** The technical system of the EETS Provider shall implement security measures to protect stored and processed data in the EETS context. The EETS Provider shall implement a comprehensive IT security concept. This concept shall be orientated on applicable security requirements of ISO 27001 and the recommendations of the German Federal Office for Information Security (BSI) in the baseline protection standards and catalogues. This security concept shall protect EETS stakeholders from damages from lack of availability, confidentiality, integrity, authentication, non-repudiation and access control of sensitive personal data in a European context with many users. Effective data security and access procedures shall be used. Procedures to ensure integrity of data shall be implemented by technical and organisational means. Operational procedures of EETS Providers shall prohibit unauthorized data access within the EETS Providers system. Responsibilities and permissions of all stakeholders shall be defined in an unambiguous way. Security measures shall be adapted to reflect the technologies state of the art. EETS Providers shall implement measures to detect fraud and unauthorized access to the system and avoid negative impact on the toll charging process. These measures shall also allow the Toll Charger to detect such incidents.
F	
I	
PL	
E	
A/DK	[SO-1] Any EasyGo toll data exchanged between a TC and a SP shall fall under the EasyGo security rules. The EasyGo security rules apply only to the toll data relevant for the EasyGo services. Any other toll data associated to local contracts is in the sole responsibility of the TC. [SO-2] EasyGo toll data shall be correct, complete, traceable and protected. Correct EasyGo toll data fully and accurately records all required road usage parameters according to the rules of the EasyGo toll scheme. This statement also covers the transmission of data between actors through theEasyGo HUB and thereby delivers data integrity in communication. Complete EasyGo toll data means that no toll data is lost, deliberately or otherwise according to the rules of the EasyGo toll scheme. As a complement to the correctness requirement, toll data must also be complete. That is, no data that shall be reported can be suppressed. This statement emphasizes the need to secure not only correct recording, but also correct reporting and thereby ensures data availability. Traceable EasyGo toll data can be traced back to its originator/owner in a manner that its veracity can be contested and proved with enough confidence to be able to stand as evidence in a dispute. As data is refined through its process chain, passing from one actor to another, the responsibility and ownership of data must be clear at each step. In particular, if errors or falsifications are added in one part of the chain, while the other parts are correct and in compliance with system requirements, it shall still be clear which actor is accountable. Protected EasyGo toll data can only be accessed by authorised parties. The EasyGo system shall for all parts of the EasyGo toll data clearly define which actors under which conditions can access it. The upholding of these definitions shall be supported by cryptographic, administrative and/or other procedures. This statement delivers data confidentiality. NOTE: SO-2 thus covers the Confidentiality-Integrity-Availability (CIA) triad [SO-3] Risk and efficiency should be considered when implementing security in EasyGo. As EasyGo will transfer large funds between the individual actors the toll scheme it is a top priority that it delivers a high level of security and reliability. It is very important that the toll due for the usage of an infrastructure can be imposed to the correct Service User which used this infrastructure. It will never be possible to achieve perfect security and reliability in any operational system. Rather, the question is how reliable and secure a system has to be to fulfil its needs for the involved actors. At a certain point, the marginal costs that must be incurred in order to increase security and reliability one more

MB	High level security objectives
	step will represent a disproportionate effort, the costs will exceed the additional benefits. The evaluation of risk and efficiency shall be made when developing requirements and security measures based upon the threat analysis. Costs and benefits shall in this context refer to both the economic resources of all actors and to the time and effort needed from the Service User to be compliant with the system. [SO-4] The EasyGo security requirements shall be limited to supporting interoperability between the EasyGo actors. EasyGo is a compound of many separate toll domains that differ in many ways, for example in technical solutions, legal requirements and operational procedures. The different charging technologies shall be respected, possibly leading to specific security requirements for the different types of toll domains. The common security requirements resulting from this policy shall therefore be limited to the common aspects of the whole of EasyGo. Examples: technical solutions: barriers vs. free-flow legal requirements: fee vs. tax operational procedures: mandatory vs. non-mandatory OBU For example, while a good protection for the privacy of the individual is desirable, it does not directly affect interoperability. Therefore, this policy shall limit itself to supporting the implementation of existing common rules and regulation on privacy and refrain from creating requirements that cater to the needs of specific EasyGo actors. This limitation in scope represents a pragmatic recognition of the history of the currently participating toll domains and the difficulty of fitting them into a common interoperable framework as well as to expand the EasyGo services to new toll domains.

Table 8. High level security objectives

A.3 ISMS Requirements and measures

A.3.1 ISMS requirements

The following Table 9 lists the Information Security Management System (ISMS from now on) **standard** security requirements.

No	Requirement
RQ.ISMS.1	Establish, implement, operate, monitor, review, maintain and improve an Information Security Management System (ISMS) according to ISO/IEC 27001
RQ.ISMS.2	Threat requires a security measure or security control defined by the ISO/IEC 27002 standard.

Table 9: Standard ISMS security requirements

Remarks:

1) RQ.ISMS.1 is a rather generic requirement, not bound to any specific security measure.
2) RQ.ISMS.2 makes no sense. It was introduced in the security framework for completeness in the threat analysis only.

The following Table 10 shows the ISMS requirements in the different REETS environments. No specific REETS requirements than those defined in the standard were presented.

	CH	DE	F1	F2	I	PL	E	A/DK
RQ.ISMS.1	YES Each BO of a TC and TSP shall fulfil this requirement.	YES	NO	No input	YES	YES	NO	YES

	CH	DE	F1	F2	I	PL	E	A/DK
RQ.ISMS.2		YES	NO	No input	YES	YES	NO	YES

Table 10: REETS ISMS security requirements

Remarks:

1) CH:
   a) Yes (14) = Only applicable for the TC, because the SP is obliged to forward the TC (Swiss FCA) created invoice details unchanged to the user.
   b) n. a. (15) = Currently no such obligation exists in Switzerland.
2) IT: Adoption of a general IT process organisation for back-office interfaces based upon ITIL and COBIT best practices, being at the basis of the ISO 27001; the full ISO 27001 certification is not required
3) DE: The EETS Provider shall operate an ISMS according to ISO 27001 or equivalent. The security measures can be derived from ISO 27002 but this is not an obligation.

A.3.2 ISMS related security measures

There are no explicit security measures associated with requirement ISMS.1, rather than being compliant to ISO 27001.

A.4 Generic Interface requirements and measures

A.4.1 Generic interface requirements

The following Table 11 lists the generic interface **standard** security requirements.

No	Requirement
RQ.IF.01	Data exchange shall be done using an authenticated channel that shall guarantee data integrity, confidentiality and non-repudiation (proof of origin and delivery). **This requirement will be removed in the new version of the EN 16439 standard.**
RQ.IF.02	Data exchange shall be done using transmission channels with reliable availability.
RQ.IF.10	Data exchange shall guarantee data confidentiality.
RQ.IF.11	Data exchange shall guarantee data integrity.
RQ.IF.12	Data exchange shall guarantee the authenticity of the data originator.
RQ.IF.13	Data exchange shall guarantee non-repudiation with proof of origin.
RQ.IF.14	Data exchange shall guarantee non-repudiation with proof of delivery.
RQ.IF.20	Data exchange shall only be done between authenticated entities for the respective data exchange.
RQ.IF.30	Data exchange shall allow the detection of resent messages (protection against reply attacks).

Table 11: Standard Generic interface security requirements

The following Table 12 shows the generic interface requirements in the different REETS environments. No other requirements than those defined in the standard were presented.

	CH	DE	F1	F2	I	PL	E	A/DK
RQ.IF.02	YES	YES	YES	No input	YES	YES (1)	YES	YES
RQ.IF.10	YES	YES	YES	No input	YES	YES	YES	YES
RQ.IF.11	YES	YES	YES	No input	YES	YES	YES	YES
RQ.IF.12	YES	YES	YES	No input	YES	YES (2)	YES	YES
RQ.IF.13	YES	YES	YES	No input	YES	YES (3)	NO	NO
RQ.IF.14	YES (1)	YES	YES	No input	YES	YES (4)	NO	NO
RQ.IF.20	YES (1)	YES	YES	No input	YES	YES	NO	YES
RQ.IF.21	NO	YES	YES	No input	NO	YES (5)	NO	YES
RQ.IF.30	YES	YES	YES	No input	YES	YES (6)	NO	YES

Table 12: REETS Generic Interface security requirements

Remarks:

1) CH:
   a) RQ.IF.01 contains RQ.IF.10 to RQ.IF.14.
   b) The list of detailed requirements in the EFC Security Framework was introduced to show that not all different EFC interface requires the same level of protection.
   c) (1) Only Back Office interface, no End-To-End requirement.
2) PL:
   a) (1) High availability of communication channel including service levels and monitoring procedures
   b) (2) Communication channel encryption and ADU message authentication
   c) (3) ADU message authentication
   d) (4) Proof of message delivery
   e) (5) Communication channel encryption and Secure handover of DSRC keys
   f) (6) Communication channel encryption
3) DE:
   a) RQ.IF.02 – VPN connection
   b) RQ.IF.10 – VPN connection with encryption
   c) RQ.IF.11 – VPN connection and web service signature
   d) RQ.IF.12 – VPN connection and web service signature
   e) RQ.IF.13 – web service signature
   f) RQ.IF.14 – web service signature and signed response
   g) RQ.IF.20 – VPN connection
   h) RQ.IF.21 – VPN connection
   i) RQ.IF.30 – web services and unique message identifier in ISO 12855 compatible messages

A.4.2 Generic Interface related security measures

The following Table 13 shows the **standard** security measures that must be implemented when an interface requirement is selected.

Requirement	Measure code(s)	Measure(s)
RQ.IF.02	SM.200	The contracting parties of communication providers shall have proper service levels agreed and monitoring procedures in place that are able to detect any non-compliant behaviour of the communication provider.

Requirement	Measure code(s)	Measure(s)
RQ.IF.10	SM.241	The bidirectional Front End to TSP Back End communication shall be implemented using a secure connection.
	SM.250	The bidirectional TC to TSP communication shall be implemented using a secure connection with authentication.
	SM.415	The communication between OBE and proxy shall guarantee confidentiality, integrity and authenticity.
RQ.IF.11	SM.210	The RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for Toll Charger (MAC_TC) over at least the EN ISO 14906 attributes PaymentMeans, using a key known only to the Toll Charger and the Toll Service Provider during an EFC transaction. The OBE shall respond accordingly.
	SM.220	The RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for Toll Charger (MAC_TC) over at least the EN ISO 14906 attributes PaymentMeans, using a key known only to the Toll Charger and the Toll Service Provider during a CCC transaction. The OBE shall respond accordingly.
	SM.230	The RSE shall provide a MAC_TC over the LAC data sent to the OBE calculated with a key known only to the Toll Charger and the lACtime.
	SM.241	The bidirectional Front End to TSP Back End communication shall be implemented using a secure connection.
	SM.250	The bidirectional TC to TSP communication shall be implemented using a secure connection with authentication.
	SM.415	The communication between OBE and proxy shall guarantee confidentiality, integrity and authenticity.
RQ.IF.12	SM.220	The RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for Toll Charger (MAC_TC) over at least the EN ISO 14906 attributes PaymentMeans, using a key known only to the Toll Charger and the Toll Service Provider during a CCC transaction. The OBE shall respond accordingly.
	SM.230	The RSE shall provide a MAC_TC over the LAC data sent to the OBE calculated with a key known only to the Toll Charger and the lACtime.
	SM.256	The originator of a Trust Object shall undeniably sign it.
RQ.IF.13	SM.253	Distribution of EFC context data shall be undeniably signed by the Toll Charger, and confirmed by the Toll Service Provider in an agreed time frame with an authenticated response.
	SM.254	Distribution of the exception list shall be undeniably signed by the Toll Service Provider, and confirmed by the Toll Charger in an agreed time frame with an authenticated response.
	SM.256	The originator of a Trust Object shall undeniably sign it.
RQ.IF.14	SM.253	Distribution of EFC context data shall be undeniably signed by the Toll Charger, and confirmed by the Toll Service Provider in an agreed time frame with an authenticated response.
	SM.254	Distribution of the exception list shall be undeniably signed by the Toll Service Provider, and confirmed by the Toll Charger in an agreed time frame with an authenticated response.
RQ.IF.20	SM.202	The Toll Charger and the Toll Service Provider shall only allow access to stored data for an authorised and authenticated entity.

Table 13. Standard Interface related security measures

The following Table 14 shows the security measures for interfaces in the different environments. Grey shaded cells indicate that the requirement does not apply in the related environment. The standard security measure(s) are outlined in **bold**. Possible additional measures are outlined in **red**.

	CH	DE	F1	I	PL	E	A/DK
RQ.IF.02	•**SM.200**	•**SM.200**	•**SM.200**	•**SM.200**	•**SM.200**	•**SM.200**	•**SM.200**
RQ.IF.10	•**SM.241** •**SM.250** •**SM.415**	•**SM.250** •	•**SM.250**	•**SM.250**	•**SM.250**	•**SM.250**	•**SM.250**
RQ.IF.11	•**SM.210** •**SM.220** •**SM.230** •**SM.241** •**SM.250** •**SM.415**	•**SM.220** •**SM.230** •**SM.250** •	•**SM.210** •**SM.250**	•**SM.210** •**SM.230** •**SM.250**	•**SM.210** •**SM.220** •**SM.230** •**SM.250**	•**SM.210** •**SM.220** •**SM.230** •**SM.250**	•**SM.210** •**SM.250**
RQ.IF.12	•**SM.220** •**SM.230** •**SM.256**	•**SM.220** •**SM.230** •**SM.256**	•**SM.256**	•**SM.230** •**SM.256**	•**SM.220** •**SM.230** •**SM.256**	•**SM.220** •**SM.230** •**SM.256**	•**SM.256**
RQ.IF.13	•**SM.253** •**SM.254** •**SM.256**	•**SM.253** •**SM.254** •**SM.256**	•**SM.253** •**SM.254** •**SM.256**	•**SM.253** •**SM.254** •**SM.256**	•**SM.253** •**SM.254** •**SM.256**		
RQ.IF.14	•**SM.253** •**SM.254**	•**SM.253** •**SM.254**	•**SM.253** •**SM.254**	•**SM.253** •**SM.254**	•**SM.253** •**SM.254**		
RQ.IF.20	•**SM.202**	•**SM.202**	•**SM.202**	•**SM.202**	•**SM.202**		•**SM.202**

Table 14: REETS General Interface related security measures

A.5 Data storage requirements and measures

A.5.1 Data Storage requirements

The following Table 15 lists the data storage **standard** security requirements.

No	Requirement
RQ.DS.01	Access to stored data shall only be granted after authorisation.
RQ.DS.02	Access to stored data shall only be granted via defined interfaces and defined procedures.
RQ.DS.03	Stored data shall have an independent backup storage.

No	Requirement
RQ.DS.05	Data storage shall guarantee data integrity.

Table 15: Standard Data Storage security requirements

The following Table 16 shows the data storage requirements in the different REETS environments. No other requirements than those defined in the standard were presented.

	CH	DE	F1	F2	I	PL	E	A/DK
RQ.DS.01	YES	YES	YES	No input	YES	YES	YES	YES
RQ.DS.02	YES	YES	YES	No input	YES	YES	YES	YES
RQ.DS.03	YES	YES	YES	No input	YES	YES	YES	YES
RQ.DS.05	YES	YES	YES	No input	YES	YES	YES	YES

Table 16: REETS Data Storage security requirements

Remarks:

1) DE:
   a) The requirements are assessed from the perspective of the Toll Chargers EETS system and its access to data. Specific provisions for the EETS Providers system are not given. General requirements are the implementation of a ISO 27001 compatible security management system and the implementation of corresponding measures.

A.5.2 Data Storage security measures

The following Table 17 shows the **standard** security measures that must be implemented when a data storage requirement is selected.

Requirement	Measure code(s)	Measure(s)
RQ.DS.01	SM.202	The Toll Charger and the Toll Service Provider shall only allow access to stored data for an authorised and authenticated entity.
RQ.DS.02	SM.201	The Toll Charger and the Toll Service Provider shall agree on defined interfaces and procedures for the access to stored
RQ.DS.03	SM.203	A security measure (security control) is defined by the ISO/IEC 27002 standard and is thus outside the scope of the standard.
RQ.DS.05	SM.203	A security measure (security control) is defined by the ISO/IEC 27002 standard and is thus outside the scope of the standard.

Table 17. Standard Data Storage related security measures

The following Table 18 shows the security measures for data storage in the different REETS environments. Grey shaded cells indicate that the requirement does not apply in the related environment. The standard security measure(s) are outlined in **bold**. Possible additional measures are outlined in **red**.

	CH	DE	F1	I	PL	E	A/DK
RQ.DS.01	SM.202	SM.203	SM.202	SM.202	SM.202	SM.202	SM.202
RQ.DS.02	SM.201	SM.203	SM.201	SM.201	SM.201	SM.201	SM.201

	CH	DE	F1	I	PL	E	A/DK
RQ.DS.03	SM.203	SM.203	SM.203	SM.203	SM.203	SM.203	SM.203
RQ.DS.05	SM.203	SM.203	SM.203	SM.203	SM.203	SM.203	SM.203

Table 18: REETS Data Storage related security measures

A.6 Toll Chargers requirements and measures

A.6.1 Toll charger requirements

The following Table 19 lists the Toll Charger **standard** security requirements.

No	Requirement
RQ.TC.01	The Toll Charger shall determine if factual road usage is represented by a corresponding set of toll declarations (enabled by RQ.TSP.51).
RQ.TC.02	The Toll Charger shall be able to determine if a toll declaration is based on correct and complete road usage data (enabled by RQ.TSP.52).
RQ.TC.03	The TC shall determine, in a spot check, if an OBE is in an OK operational state.
RQ.TC.04	The TC shall check the integrity and authenticity of the received data as compared to the data sent from the Front End.
RQ.TC.05	The TC shall determine if toll declarations are based on data originating from a legitimate Front End and/or TSP Back End (enabled by RQ.TSP.55).
RQ.TC.11	The TC shall detect faked or cloned OBEs (for DSRC systems) and inform the TSP to black list the detected OBEs (enabled by RQ.TSP.61).
RQ.TC.20	The TC shall detect RSE damaging and recover the RSE functionality.
RQ.TC.21	The TC shall detect theft of RSE parts and recover the RSE functionality by a replacement of the stolen part.
RQ.TC.22	The TC shall implement RSE authentication measures for DSRC communication.
RQ.TC.23	The TC shall detect RSE malfunction and correct the malfunctioning RSE functionality.
RQ.TC.91	The TC shall provide non-repudiation with proof of origin for distributed EFC context data and shall oblige TSPs receiving this EFC context data to provide non-repudiation with proof of delivery.
RQ.TC.92	The TC shall only accept an OBE after detecting if an OBE belongs to a trusted Service Provider and if the Service provider guarantees payment for that specific OBE (enabled by RQ.TSP.62).
RQ.TC.93	The TC shall oblige the TSP to deliver protection against repudiation by users of invoices and CCC events.
RQ.TC.94	Received Exception List shall only be accepted after verification of non-repudiation with proof of origin. The TC shall also provide for the exception list non-repudiation with proof of delivery to the TSP.
RQ.TC.95	The TC shall be responsible for the availability of his interfaces according to agreed service levels.

Table 19: Standard Toll Charger security requirements

The following Table 20 shows the Toll Charger security requirements in the different REETS environments. No other requirements than those defined in the standard were presented.

	CH	DE	F1	F2	I	PL	E	A/DK
RQ.TC.01	NO	YES	YES	No input	NO	YES	NO	YES
RQ.TC.02	YES	YES	YES	No input	NO	YES	NO	YES
RQ.TC.03	YES	YES	YES	No input	NO	YES	NO	YES
RQ.TC.04	YES	NO	n.a.	No input	NO	YES	NO	YES
RQ.TC.05	YES	YES	n.a.	No input	NO	YES	NO	YES
RQ.TC.11	NO	NO	YES	No input	YES	YES	YES	YES
RQ.TC.20	YES (1)	YES	YES	No input	YES	YES	YES	YES
RQ.TC.21	YES (1)	YES	YES	No input	YES	YES	YES	YES
RQ.TC.22	YES	YES	YES	No input	NO	YES	NO	YES
RQ.TC.23	YES (1)	YES	YES	No input	YES	YES	YES	YES
RQ.TC.91	YES	YES	YES	No input	YES	YES	NO	NO
RQ.TC.92	YES	YES	YES	No input	YES	YES	YES	YES
RQ.TC.93	NO (2)	YES	n.a.	No input	NO	YES	NO	YES
RQ.TC.94	YES	YES	YES	No input	YES	YES	NO	NO
RQ.TC.95	YES	YES	YES	No input	YES	YES	YES	YES

Table 20: REETS Toll Charger security requirements

Remarks:

1) CH:
   a) There are several sources for the TC requirements:
      i) The TC itself to protect its assets and income
      ii) The User to be not wrongly enforced or overcharged
      iii) The SP to be able to provide the required service

      It has to be discussed which of the requirements (because of the source and intention) are relevant for the EETS/REETS interoperable environment. The intention of some of the requirements above is, outside of the whole context and explanations of the EFC Security Framework, not self explaining
   b) (1) = Enforcement and CH border RSE only. No charging RSE.
   c) (2) = SP payment guarantee = not applicable

2) PL:
   a) RQ.TC.90 needs to clarify country for which the jurisdiction is assumed to apply – i.e. is it that of TC, SP or User ?

A.6.2 Toll Charger security measures

The following Table 21 shows the **standard** security measures that must be implemented when a Toll Charger requirement is selected.

Requirement	Measure code(s)	Measure(s)
RQ.TC.01	SM.210	The RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for Toll Charger (MAC_TC) over at least the EN ISO 14906 attributes PaymentMeans, using a key known only to the Toll Charger and the Toll Service Provider during an EFC transaction. The OBE shall respond accordingly.
	SM.223	The OBE shall provide an undeniable proof of correct registration of usage data for the given location and moment in time of the CCC transaction..
	SM.310	The Front End shall be designed as a clearly distinguished entity with a defined interface to the TC RSE. The Front End's functionality shall be tested to guarantee its functionality and it shall be auditable according to a suitability for use procedure
	SM.313	The Toll Charger shall compare the toll declarations acquired by the Toll Service Provider with his own observations, in accordance with privacy regulations.
	SM.316	The Toll Charger shall determine if the toll declaration has been produced by a trusted Front End by a message authentication code (MAC_TC) or signature
	SM.317	The Toll Charger shall verify the integrity of the ChargeReport based on the Front End MAC_TSP or signature.
	SM.318	The registration of usage data by the Toll Service Provider shall be based on a minimum set of functions in the Front End trusted by both the Toll Service Provider and the Toll Charger. These functions shall directly or indirectly ensure the integrity of the toll declarations including non-repudiation with proof of origin.
	SM.320	The Toll Charger shall compare the proof of correct registration of usage data with his own observations, in accordance with privacy regulations.
	SM.410	The OBE shall support a Compliance Checking Communication transaction over an interface with security as defined in chapter 8.3 in a GNSS environment
	SM.513	In case of toll declarations provided by the Toll Service Provider, the dedicated compliance checking RSE of the TC shall perform a Compliance Checking Communication transaction over an interface with security as defined in chapter 8.3 when the OBE passes it.
	SM.514	In case of compliance checking via DSRC, the Toll Charger shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.
	SM.530	The Toll Charger shall compare the toll declarations that he himself has acquired with his own observations, in accordance with privacy regulations.

Requirement	Measure code(s)	Measure(s)
RQ.TC.02	SM.230	The RSE shall provide a MAC_TC over the LAC data sent to the OBE calculated with a key known only to the Toll Charger and the lACtime.
	SM.310	The Front End shall be designed as a clearly distinguished entity with a defined interface to the TC RSE. The Front End's functionality shall be tested to guarantee its functionality and it shall be auditable according to a suitability for use procedure.
	SM.311	"The correct and trustworthy Front End functionality shall be periodically audited by the Toll Service Provider and optionally by the Toll Charger or an independent entity on his behalf. NOTE An audit process can compare charge data of sample vehicles equipped with the OBE with known independent trip data."
	SM.312	The Toll Charger shall perform plausibility and completeness checks on toll declarations acquired by the Toll Service Provider in a GNSS environment.
	SM.314	The Toll Charger shall verify if toll declaration(s) acquired by the Toll Service Provider correctly correspond(s) to ChargeReport(s) and/or usage data.
	SM.316	The Toll Charger shall determine if the toll declaration has been produced by a trusted Front End by a message authentication code (MAC_TC) or signature.
	SM.317	The Toll Charger shall verify the integrity of the ChargeReport based on the Front End MAC_TSP or signature.
	SM.318	The registration of usage data by the Toll Service Provider shall be based on a minimum set of functions in the Front End trusted by both the Toll Service Provider and the Toll Charger. These functions shall directly or indirectly ensure the integrity of the toll declarations including non-repudiation with proof of origin.
	SM.510	In case of toll declarations acquired via the DSRC interface, the Toll Charger shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.
	SM.520	The Toll Charger shall perform plausibility and completeness checks on toll declarations that he himself has acquired.
RQ.TC.03	SM.410	The OBE shall support a Compliance Checking Communication transaction over an interface with security as defined in chapter 8.3 in a GNSS environment.
	SM.513	In case of toll declarations provided by the Toll Service Provider, the dedicated compliance checking RSE of the TC shall perform a Compliance Checking Communication transaction over an interface with security as defined in chapter 8.3 when the OBE passes it.
RQ.TC.04	SM.240	The TSP shall implement a MAC_TSP authenticator in the OBE to proof its authenticity and integrity.
	SM.316	The Toll Charger shall determine if the toll declaration has been produced by a trusted Front End by a message authentication code (MAC_TC) or signature.
	SM.317	The Toll Charger shall verify the integrity of the ChargeReport based on the Front End MAC_TSP or signature.
	SM.521	The Toll Charger shall verify the MAC_TC if the toll declarations provided by the TSP are based on LAC data.

Requirement	Measure code(s)	Measure(s)
RQ.TC.05	SM.316	The Toll Charger shall determine if the toll declaration has been produced by a trusted Front End by a message authentication code (MAC_TC) or signature.
	SM.317	The Toll Charger shall verify the integrity of the ChargeReport based on the Front End MAC_TSP or signature.
	SM.521	The Toll Charger shall verify the MAC_TC if the toll declarations provided by the TSP are based on LAC data.
RQ.TC.11	SM.511	In case of toll declarations acquired via the DSRC interface, the Toll Charger shall store the value of the Transaction Counter read-out of the OBE as part of the Billing Details.
	SM.513	In case of toll declarations provided by the Toll Service Provider, the dedicated compliance checking RSE of the TC shall perform a Compliance Checking Communication transaction over an interface with security as defined in chapter 8.3 when the OBE passes it.
	SM.514	In case of compliance checking via DSRC, the Toll Charger shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.
RQ.TC.20	SM.204	The Toll Charger and Toll Service Provider shall agree on a service level agreement defining quality goals and response times.
RQ.TC.21	SM.204	The Toll Charger and Toll Service Provider shall agree on a service level agreement defining quality goals and response times.
RQ.TC.22	SM.222	The OBE shall implement an access control mechanism for EFC commands addressing its CCC data attributes. The RSE shall implement the calculation of the corresponding access codes.
	SM.231	The OBE shall implement an access control mechanism for EFC commands addressing the LAC data attributes. The RSE shall implement the calculation of the corresponding access codes.
RQ.TC.23	SM.204	The Toll Charger and Toll Service Provider shall agree on a service level agreement defining quality goals and response times.
RQ.TC.91	SM.253	Distribution of EFC context data shall be undeniably signed by the Toll Charger, and confirmed by the Toll Service Provider in an agreed time frame with an authenticated response.
RQ.TC.92	SM.201	The Toll Charger and the Toll Service Provider shall agree on defined interfaces and procedures for the access to stored data.
	SM.214	In case of compliance checking via DSRC, the Toll Charger shall check the value of the MAC_TC using the key addressed by KeyRef and the RndRSE.
RQ.TC.93	SM.221	The RSE shall request the OBE to calculate and provide a DSRC Message Authentication guaranteeing Non-Repudiation to the Toll Charger (MAC_NR) over at least the PaymentMeans attribute, using a key known only to the Toll Service Provider during a CCC transaction. The OBE shall respond accordingly.
	SM.231	The Toll Charger shall forward a complete compliance check record to the Toll Service Provider if he collects an amount due for this CCC event. This excludes the transfer of pictures but includes any information that can be gained from looking at a picture (e.g. license plate information). The Toll Charger shall not forward a complete compliance check record to the Toll Service Provider if he just supports the TC by delivering the SU address data."
	SM.515	In case of compliance checking via DSRC, the Toll Charger shall store the value of the authenticated AttributeList, MAC_TC, MAC_NR, KeyRef and RndRSE as part of the compliance check record.

Requirement	Measure code(s)	Measure(s)
RQ.TC.94	SM.254	Distribution of the exception list shall be undeniably signed by the Toll Service Provider, and confirmed by the Toll Charger in an agreed time frame with an authenticated response.
RQ.TC.95	SM.204	The Toll Charger and Toll Service Provider shall agree on a service level agreement defining quality goals and response times.

Table 21. Standard Toll charger related security measures

The following Table 22 shows the security measures for toll chargers in the different REETS environments. Grey shaded cells indicate that the requirement does not apply in the related environment. The standard security measure(s) are outlined in **bold**. Possible additional measures are outlined in **red**.

	CH	DE	F1	I	PL	E	A/DK
RQ.TC.01		**•SM.223** **•SM.310** **•SM.313** **•SM.320** **•SM.410** **•SM.513** **•SM.514** **•SM.530**	**•SM.210** **•SM.530**		**•SM.210** **•SM.530**		**•SM.210** **•SM.316** **•SM.530**
RQ.TC.02	**•SM.230** **•SM.310** **•SM.311** **•SM.312** **•SM.314** **•SM.316** **•SM.317** **•SM.318** **•SM.510** **•SM.520**	**•SM.230** **•SM.310** **•SM.311** **•SM.312** **•SM.314** **•SM.510** **•SM.520**	**•SM.314** **•SM.510** •		**•SM.230** **•SM.314** **•SM.510** **•SM.520**		**•SM.310** **•SM.311** **•SM.316** **•SM.510** **•SM.520**
RQ.TC.03	**•SM.410** **•SM.513**	**•SM.410** **•SM.513**					
RQ.TC.04	**•SM.240** **•SM.316** **•SM.317** **•SM.521**	•			**•SM.240**		**•SM.240** **•SM.316**
RQ.TC.05	**•SM.316** **•SM.317** **•SM.521**	**•SM.521**					**•SM.316**

	CH	DE	F1	I	PL	E	A/DK
RQ.TC.11		•SM.511 •SM.513 •SM.514	•SM.511	•SM.511	•SM.511	•SM.511	•SM.511
RQ.TC.20	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204
RQ.TC.21	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204
RQ.TC.22	•SM.222 •SM.231	•SM.222 •SM.231	•	•SM.222	•SM.222		
RQ.TC.23	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204
RQ.TC.91	•SM.253	•SM.253	•SM.253	•SM.253	•SM.253		
RQ.TC.92	•SM.201 •SM.220 •SM.514	•SM.201 •SM.214	•SM.201 •	•SM.201 •SM.220 •SM.514	•SM.201 •SM.220 •SM.514	•SM.201 •SM.220 •SM.514	•SM.201 •SM.220 •SM.514
RQ.TC.93		•SM.221 •SM.231 •SM.515			•SM.221		
RQ.TC.94	•SM.254	•SM.254	•SM.254	•SM.254	•SM.254		
RQ.TC.95	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204	•SM.204

Table 22: REETS Toll Charger related security measures

A.7 Toll Service Providers requirements and measures

A.7.1 Toll Service Provider requirements

The following Table 23 lists the Toll Service Provider **standard** security requirements.

No	Requirement
RQ.TSP.01	The Toll Service Provider shall determine if factual road usage is represented by a corresponding set of toll declarations. NOTE This means that toll declarations are not altered and completely transmitted.
RQ.TSP.02	The Toll Service Provider shall determine if a toll declaration is based on correct and complete road usage data. NOTE This means that tolling related events are correctly collected.
RQ.TSP.04	The TSP shall check the integrity and authenticity of the received data as compared to the data sent from the Front End.
RQ.TSP.05	The TSP shall determine if toll declarations are based on data originating from a legitimate Front End.

No	Requirement
RQ.TSP.06	An OBE shall prevent or at least detect illegal modification of parameters through its external interfaces. Illegal modification shall result in "NOT OK" OBE state.
RQ.TSP.07	An OBE shall not allow the User to modify fixed vehicle parameters.
RQ.TSP.08	TSP shall detect duplicate (also false) OBE identities and black list such duplicated OBE identities.
RQ.TSP.09	The TSP shall notify the driver if the OBE is not working correctly.
RQ.TSP.10	The TSP shall determine if billing details are based on correct and complete road usage data.
RQ.TSP.11	The TSP shall determine if factual road usage is represented by a corresponding set of billing details.
RQ.TSP.12	The TSP shall verify the calculation of amounts in the billing details.
RQ.TSP.13	The TSP shall accept only distributed EFC context data having non-repudiation with proof of origin.
RQ.TSP.14	The TSP shall oblige the TC to guarantee that distribution of exception lists features non-repudiation with proof of delivery.
RQ.TSP.15	The TSP shall oblige the TC to enable the TSP to determine the correctness and relevance of a CCC event via the corresponding record.
RQ.TSP.16	The OBE shall detect signal input inconsistencies and in such case signal not OK to the User and send an indication to TSP.
RQ.TSP.19	The TSP shall provide the TC with the means to identify the stolen OBEs.
RQ.TSP.20	The TSP shall manage stolen OBEs.
RQ.TSP.21	The TSP shall detect cloned OBEs and black list the detected OBEs.
RQ.TSP.22	TSP shall avoid exaggerate loss of OBE caused by Users.
RQ.TSP.23	The TSP shall validate the User contract information.
RQ.TSP.30	The TSP shall validate payment means of a User.
RQ.TSP.31	The TSP shall monitor the validity of payment means.
RQ.TSP.40	The OBE shall not allow change of internal data via the user interface, except the data allowed to be changed.
RQ.TSP.41	The OBE shall only present intended data by the User interface.
RQ.TSP.42	The Toll Service Providers implementation of the Front End and gathering and processing of data should be in compliance with the privacy requirements.
RQ.TSP.50	The TSP shall assure that only authenticated Users have access to systems that manage their personal data.
RQ.TSP.51	The TSP shall enable the TC to determine if factual road usage is represented by a corresponding set of Toll Declarations (required to enable RQ.TC.01).

No	Requirement
RQ.TSP.52	The TSP shall enable the TC to determine if a toll declaration is based on correct and complete road usage data (required to enable RQ.TC.02).
RQ.TSP.55	The TSP shall enable the TC to determine if toll declarations are based on data originating from a legitimate Front End (required to enable RQ.TC.05).
RQ.TSP.56	The TSP shall enable the TC to audit invoices to customers for tolls of his toll domain (required to enable RQ.TC.06).
RQ.TSP.58	The TSP shall enable the TC to check the model and make of OBE during a vehicle check (required to enable RQ.TC.08). NOTE: These fields are set by the manufacturer during production. The responsibility of the TSP is to provide the TC with the different possible values for these fields to distinguish between the different OBU models and makes."
RQ.TSP.61	The TSP shall provide measures to the TC to detect faked or cloned OBEs (required to enable RQ.TC.11).
RQ.TSP.62	The TSP shall enable the TC to detect if an OBE belongs to the TSP (required to enable RQ.TC.92).
RQ.TSP.90	The Toll Service Providers systems should be designed in a way that access to stored or processed data is only possible within the legal context of the respective countries (lawful interception).
RQ.TSP.91	The data communication between Front End (OBE) and Back End (TSP) Back End shall be protected against interception in a way that access to stored or processed data is only possible within the legal context of the respective country (lawful interception).
RQ.TSP.92	Customisation of OBE shall be done in a secure way.
RQ.TSP.93	The Toll Service Provider shall implement monitoring procedures to detect any non-compliant behaviour.
RQ.TSP.94	The TSP shall implement technical and organisational measures to prevent that billing details are revealed to unauthorised parties.
RQ.TSP.95	The TSP shall guarantee the availability of its interfaces according to agreed service levels.

Table 23: Standard Toll Service Providers security requirements

The following Table 24 lists two additional requirements that come from the REETS project participants.

OTHER REQUIREMENTS	
RQ.TSP.R1	TSP shall provide and implement measures in order to identify fraudulent or abusive operation in its subsystem and in order to prevent negative side effects on toll collection. The documentation of these measures shall enable the Toll Charger to identify such operations
RQ.TSP.R2	TSP has to consider relevant security requirements of ISO 27001 and relevant recommendations provided in by national legal documents and TC's documents with respect to IT baseline protection standards.

Table 24. REETS Toll Service Provider additional security requirements

The following Table 25 shows the Toll Service Provider security requirements in the REETS different environments. These include the standard requirements and the additional REETS requirements.

	CH	DE	F1	F2	I	PL	E	A/DK
RQ.TSP.01	NO (2)	YES	YES	No input	NO	NO	NO	NO
RQ.TSP.02	YES	YES	YES	No input	NO	NO	NO	NO
RQ.TSP.04	YES	NO	YES	No input	NO	YES	NO	NO
RQ.TSP.05	YES	NO	YES	No input	NO	YES	NO	YES
RQ.TSP.06	YES	YES	YES	No input	NO	YES	NO	YES
RQ.TSP.07	YES	YES	YES	No input	NO	YES	YES	YES
RQ.TSP.09	YES	YES	YES	No input	NO	YES	NO	YES
RQ.TSP.10	NO (3)	YES	YES	No input	NO	YES	YES	NO
RQ.TSP.12	NO (3)	YES	n.a.	No input	NO	NO	YES	YES
RQ.TSP.13	YES	YES	YES	No input	YES	YES	NO	NO
RQ.TSP.14	YES (4)	YES	YES	No input	YES	NO	NO	NO
RQ.TSP.15	NO (5)	YES	n.a.	No input	NO	NO	NO	NO
RQ.TSP.16	YES	YES	NO	No input	NO	YES	NO	NO
RQ.TSP.19	YES (6)	YES	YES	No input	YES	YES	NO	YES
RQ.TSP.20	YES (6)	YES	YES	No input	NO	YES	YES	YES
RQ.TSP.21	YES (6)	YES	YES	No input	NO	YES	YES	YES
RQ.TSP.40	YES	YES	YES	No input	NO	YES	YES	YES
RQ.TSP.41	YES	YES	YES	No input	NO	YES	n.a.	YES
RQ.TSP.42	YES (9)	YES	YES	No input	NO	YES	YES	NO
RQ.TSP.51	YES (10)	YES	YES	No input	NO	YES	NO	NO
RQ.TSP.52	YES (10)	YES	YES	No input	NO	YES	NO	NO
RQ.TSP.62	n. a. (12)	YES	YES	No input	YES	YES	YES	YES
RQ.TSP.90	YES (13)	NO	YES	No input	NO	YES	YES	YES
RQ.TSP.91	YES (13)	NO	YES	No input	NO	YES	YES	NO
RQ.TSP.92	n. a. (7)	NO	YES	No input	NO	YES	YES	YES
RQ.TSP.95	YES	YES	YES	No input	NO	YES	YES	YES
RQ.TSP.R1		YES		No input	YES	YES		
RQ.TSP.R2		YES		No input	YES	YES		

Table 25: REETS Toll Service Provider requirements

Remarks:

1) CH:
   a) (2) = The requirement is included in RQ.TSP.02
   b) (3) = The TSP is not forced to do that in the LSVA scheme and also in some cases not able to calculate the correct billing details.
   c) (4) = AckADU sent by TC.
   d) (5) = Not foreseen in CH because CCC events for EETS journeys cannot happen. Every check is done at CH entry and if not a valid and correct EETS contract exists manual fall back solution will be used.
   e) (6) = This requirement will be fulfilled using a TSP OBE black list.
   f) (7) = Not applicable from TC perspective. It is in the TSP's own interest
   g) (8) = TSP payment guarantee = not applicable from TC perspective. It is in the TSP's own interest.
   h) (9) = Which is the relevant privacy legislation? It is assumed that this requirement has to fulfil the TSP and User countries privacy requirements.
   i) (10) = TSP has to send the EETS journey position data n request of the TC.
   j) (11) = Not applicable because the TSP is obliged to forward the TC (Swiss FCA) created invoice details unchanged to the user.
   k) (12) = During the CCC communication at CH entrance, every of theses details will be checked. Therefore the requirements are covered but have not to be fulfilled explicitly in another manner.
   l) (13) = Which is the relevant legislation? It is assumed that this requirement has to fulfil the TSP and User countries and/or CH legislation requirements.
2) PL:
   a) RQ.TSP.15 this isn't required but should not be excluded.
3) DE:
   a) RQ.TSP.01: Requirement in the EETS domain statement and checked during technical accreditation
   b) RQ.TSP.02: Requirement in the EETS domain statement and checked during technical accreditation
   c) RQ.TSP.04: No explicit requirement, only in the context of general quality assurance
   d) RQ.TSP.05: No explicit requirement, only in the context of general quality assurance
   e) RQ.TSP.06: Requirement in the EETS domain statement
   f) RQ.TSP.07: Responsibility of the EETS Provider for correctness of these parameters
   g) RQ.TSP.08: General requirement for EETS Providers to implement measures to detect fraud
   h) RQ.TSP.09: Requirement in the EETS domain statement
   i) RQ.TSP.10: Requirement in the EETS domain statement and checked during technical accreditation
   j) RQ.TSP.11 Requirement in the EETS domain statement and checked during technical accreditation
   k) RQ.TSP.12: Requirement in the EETS domain statement
   l) RQ.TSP.13: Contractual requirement and regulated by interface specification 003 for EFC context data
   m) RQ.TSP.14: Contractual requirement and regulated by interface specification 001 for exception lists
   n) RQ.TSP.15: Contractual regulation that TC supports TSP in clearing of transactions
   o) RQ.TSP.16: Requirement in the EETS domain statement
   p) RQ.TSP.19: Support for black lists
   q) RQ.TSP.20: General requirement for EETS Providers to implement measures to detect fraud
   r) RQ.TSP.21: General requirement for EETS Providers to implement measures to detect fraud
   s) RQ.TSP.22: No explicit requirement, realm of TSP
   t) RQ.TSP.23: No explicit requirement, realm of TSP
   u) RQ.TSP.30: No explicit requirement, realm of TSP
   v) RQ.TSP.31: No explicit requirement, realm of TSP
   w) RQ.TSP.40: Responsibility of the EETS Provider for correctness of these parameters
   x) RQ.TSP.41: Requirement in the EETS domain statement
   y) RQ.TSP.42: Requirement in the EETS domain statement
   z) RQ.TSP.50: No explicit requirement, realm of TSP
   aa) RQ.TSP.51: Requirement in the EETS domain statement and checked during technical accreditation

bb) RQ.TSP.52: Requirement in the EETS domain statement and checked during technical accreditation
cc) RQ.TSP.55: Requirement in the EETS domain statement and checked during technical accreditation
dd) RQ.TSP.56: No explicit requirement
ee) RQ.TSP.58: Requirement in the EETS domain statement to support enforcement activities of TC
ff) RQ.TSP.61: Requirement in the EETS domain statement
gg) RQ.TSP.62: Requirement in the EETS domain statement
hh) RQ.TSP.90: No explicit requirement
ii) RQ.TSP.91: No explicit requirement
jj) RQ.TSP.92: No explicit requirement
kk) RQ.TSP.93: General requirement for EETS Providers to implement measures to detect fraud
ll) RQ.TSP.94: General security requirements in the EETS domain statement
mm) RQ.TSP.95: Contractual agreement and technical provisions in the interface specifications
nn) RQ.TSP.R1: Requirement in the EETS domain statement
oo) RQ.TSP.R2: Requirement in the EETS domain statement
pp) General remark: For many of the requirements which have been assessed with a NO and where no explicit requirement is foreseen in the German EETS context, general requirements on security or fraud detection would apply. However, to be specific and enable reasonable evaluation, these requirements were evaluated accordingly.

A.7.2 Toll Service Provider security measures

The following Table 26 shows the **standard** security measures that must be implemented when a Toll Service Provider requirement is selected.

Requirement	Measure code(s)	Measure
RQ.TSP.01	SM.421	The Toll Service Provider shall determine if the ChargeReport has been produced by a trusted Front End.
	SM.422	The Toll Service Provider shall verify the integrity of the ChargeReport.
RQ.TSP.02	SM.211	The RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for Toll Service Provider (MAC_TSP) over at least the EN ISO 14906 attributes PaymentMeans, using a key known only to the Toll Service Provider during an EFC transaction. The OBE shall respond accordingly.
	SM.213	The RSE shall read, increment and write a transaction counter to the OBE. The OBE shall support this.
	SM.230	The RSE shall provide a MAC_TC over the LAC data sent to the OBE calculated with a key known only to the Toll Charger and the lACtime.
	SM.312	The Toll Charger shall perform plausibility and completeness checks on toll declarations acquired by the Toll Service Provider in a GNSS environment.
	SM.420	The Toll Service Provider shall verify if toll declaration(s) correctly correspond(s) to ChargeReport(s) and/or usage data.
	SM.421	The Toll Service Provider shall determine if the ChargeReport has been produced by a trusted Front End.
	SM.512	In case of toll declarations acquired via the DSRC interface, the Toll Charger shall store the value of the authenticated AttributeList, MAC_TSP, KeyRef and RndRSE as part of the billing Details.
	SM.520	The Toll Charger shall perform plausibility and completeness checks on toll declarations that he himself has acquired.

Requirement	Measure code(s)	Measure
RQ.TSP.04	SM.240	The TSP shall implement a MAC_TSP authenticator in the OBE to proof its authenticity and integrity.
RQ.TSP.05	SM.421	The Toll Service Provider shall determine if the ChargeReport has been produced by a trusted Front End.
RQ.TSP.06	SM.212	The OBE shall implement an access control mechanism for EFC commands addressing its data attributes. The RSE shall implement the calculation of the corresponding access codes.
	SM.222	The OBE shall implement an access control mechanism for EFC commands addressing its CCC data attributes. The RSE shall implement the calculation of the corresponding access codes.
	SM.231	The OBE shall implement an access control mechanism for EFC commands addressing the LAC data attributes. The RSE shall implement the calculation of the corresponding access codes.
	SM.413	The OBE shall implement a role based access control mechanism for its DRSC interface: any commands reserved to the Toll Service Provider (i.e. other than those for DSRC-EFC, CCC and LAC) shall be usable only by the Toll Service Provider.
	SM.414	The Service User shall be notified about the OBE working status.
	SM.416	The OBE shall prohibit any illegal modification or switch to a "NOT OK" state if it detects an illegal modification of parameters through it's external interfaces.
RQ.TSP.07	SM.205	The OBE shall not allow the Service User to modify any data in the OBE, except the data allowed to be changed via the user interface.
RQ.TSP.09	SM.414	The Service User shall be notified about the OBE working status.
RQ.TSP.10	SM.251	The Toll Charger shall link the billing details to a set of toll declarations provided by the Toll Service Provider or include the associated event data for those toll declarations which have been acquired by himself.
RQ.TSP.12	SM.252	The TSP shall compare the received billing details against the sent toll declarations to detect modifications and/or missing or additional toll declarations not sent to the TC in a GNSS environment.
	SM.258	"The Toll Charger shall provide the tariff table and all the relevant EFC Context data to the Toll Service Provider to allow him to calculate the amount given in the Billing Details. NOTE: Other means than ISO TS 17575-3 could be used, e.g. publication on a web site."
	SM.259	The Toll Service Provider shall be able to perform plausibility and completeness checks on received billing details. Those checks comprise the verification of the physical feasibility of trips on the Toll Domain compared with the received EFC Context data.
RQ.TSP.13	SM.253	Distribution of EFC context data shall be undeniably signed by the Toll Charger, and confirmed by the Toll Service Provider in an agreed time frame with an authenticated response.
RQ.TSP.14	SM.254	Distribution of the exception list shall be undeniably signed by the Toll Service Provider, and confirmed by the Toll Charger in an agreed time frame with an authenticated response.

Requirement	Measure code(s)	Measure
RQ.TSP.15	SM.321	"The Toll Charger shall forward a complete compliance check record to the Toll Service Provider if he collects an amount due for this CCC event. This excludes the transfer of pictures but includes any information that can be gained from looking at a picture (e.g. license plate information). The Toll Charger shall not forward a complete compliance check record to the Toll Service Provider if he just supports the TC by delivering the SU address data."
	SM.515	In case of compliance checking via DSRC, the Toll Charger shall store the value of the authenticated AttributeList, MAC_TC, MAC_NR, KeyRef and RndRSE as part of the compliance check record.
RQ.TSP.16	SM.417	The OBE shall switch to a "NOT OK" state if it detects signal input inconsistencies and the TSP shall be informed by the GNSS OBE.
RQ.TSP.19	SM.220	The RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for Toll Charger (MAC_TC) over at least the EN ISO 14906 attributes PaymentMeans, using a key known only to the Toll Charger and the Toll Service Provider during a CCC transaction. The OBE shall respond accordingly.
	SM.423	The TSP shall include stolen or cloned OBEs in the exception list.
RQ.TSP.20	SM.420	The TSP shall include stolen or cloned OBEs in the exception list.
RQ.TSP.21	SM.424	The TSP shall detect a cloned OBE by using the transaction counter or by detecting multiple locations for the same OBE at the same time.
	SM.511	In case of toll declarations acquired via the DSRC interface, the Toll Charger shall store the value of the Transaction Counter read-out of the OBE as part of the Billing Details.
	SM.512	In case of toll declarations acquired via the DSRC interface, the Toll Charger shall store the value of the authenticated AttributeList, MAC_TSP, KeyRef and RndRSE as part of the billing Details.
RQ.TSP.40	SM.212	The OBE shall implement an access control mechanism for EFC commands addressing its data attributes. The RSE shall implement the calculation of the corresponding access codes.
	SM.222	The OBE shall implement an access control mechanism for EFC commands addressing its CCC data attributes. The RSE shall implement the calculation of the corresponding access codes.
	SM.231	The OBE shall implement an access control mechanism for EFC commands addressing the LAC data attributes. The RSE shall implement the calculation of the corresponding access codes.
	SM.413	The OBE shall implement a role based access control mechanism for its DRSC interface: any commands reserved to the Toll Service Provider (i.e. other than those for DSRC-EFC, CCC and LAC) shall be usable only by the Toll Service Provider.
RQ.TSP.41	SM.212	The OBE shall implement an access control mechanism for EFC commands addressing its data attributes. The RSE shall implement the calculation of the corresponding access codes.
	SM.222	The OBE shall implement an access control mechanism for EFC commands addressing its CCC data attributes. The RSE shall implement the calculation of the corresponding access codes.

Requirement	Measure code(s)	Measure
	SM.231	The OBE shall implement an access control mechanism for EFC commands addressing the LAC data attributes. The RSE shall implement the calculation of the corresponding access codes.
	SM.413	The OBE shall implement a role based access control mechanism for its DRSC interface: any commands reserved to the Toll Service Provider (i.e. other than those for DSRC-EFC, CCC and LAC) shall be usable only by the Toll Service Provider.
RQ.TSP.42	SM.102	The TC and the TSP shall sign a Personal Data Assistant Agreement to be compliant to the national data protection regulations of the TC. In this agreement the duties and rights of the TSP are stated in regard to the data processing.
	SM.103	The contracting parties of communication providers shall sign a Personal Data Assistant Agreement to be compliant to the national data protection regulations of the TC. In this agreement the duties and rights of the communication provider are stated in regard to the data processing.
	SM.104	The TC shall perform audit(s) of the TSP systems and procedures to proof the adherence to the registered data processing application and the Personal Data Assistant Agreement.
	SM.105	The contracting parties of communication providers shall perform audit(s) of the communication providers systems and procedures to proof the adherence to the registered data processing application and the Personal Data Assistant Agreement.
RQ.TSP.51	SM.223	The OBE shall provide an undeniable proof of correct registration of usage data for the given location and moment in time of the CCC transaction.
	SM.257	The Toll Service Provider shall provide data underlying a specific toll declaration acquired through his system, on demand of the Toll Charger (ChargeReport and/or more detailed road usage data).
	SM.310	The Front End shall be designed as a clearly distinguished entity with a defined interface to the TC RSE. The Front End's functionality shall be tested to guarantee its functionality and it shall be auditable according to a suitability for use procedure.
	SM.311	"The correct and trustworthy Front End functionality shall be periodically audited by the Toll Service Provider and optionally by the Toll Charger or an independent entity on his behalf. NOTE An audit process can compare charge data of sample vehicles equipped with the OBE with known independent trip data."
	SM.318	The registration of usage data by the Toll Service Provider shall be based on a minimum set of functions in the Front End trusted by both the Toll Service Provider and the Toll Charger. These functions shall directly or indirectly ensure the integrity of the toll declarations including non-repudiation with proof of origin.
	SM.319	The Toll Service Provider shall provide an undeniable proof of correct registration of usage data for a defined location and moment in time, or for a defined range of time and for a specified set of OBU(s) on demand to the Toll Charger.
	SM.410	The OBE shall support a Compliance Checking Communication transaction over an interface with security as defined in chapter 8.3 in a GNSS environment.

Requirement	Measure code(s)	Measure
	SM.412	In case of Localisation Augmentation received via DSRC, the Toll Service Provider shall store the value of the MAC_TC, KeyRef and lACtime as part of the charge data and provide them as part of the ChargeReport.
RQ.TSP.52	SM.257	The Toll Service Provider shall provide data underlying a specific toll declaration acquired through his system, on demand of the Toll Charger (ChargeReport and/or more detailed road usage data).
	SM.310	The Front End shall be designed as a clearly distinguished entity with a defined interface to the TC RSE. The Front End's functionality shall be tested to guarantee its functionality and it shall be auditable according to a suitability for use procedure.
	SM.311	"The correct and trustworthy Front End functionality shall be periodically audited by the Toll Service Provider and optionally by the Toll Charger or an independent entity on his behalf. NOTE An audit process can compare charge data of sample vehicles equipped with the OBE with known independent trip data."
	SM.312	The Toll Charger shall perform plausibility and completeness checks on toll declarations acquired by the Toll Service Provider in a GNSS environment.
	SM.314	The Toll Charger shall verify if toll declaration(s) acquired by the Toll Service Provider correctly correspond(s) to ChargeReport(s) and/or usage data.
	SM.318	The registration of usage data by the Toll Service Provider shall be based on a minimum set of functions in the Front End trusted by both the Toll Service Provider and the Toll Charger. These functions shall directly or indirectly ensure the integrity of the toll declarations including non-repudiation with proof of origin.
	SM.412	In case of Localisation Augmentation received via DSRC, the Toll Service Provider shall store the value of the MAC_TC, KeyRef and lACtime as part of the charge data and provide them as part of the ChargeReport.
RQ.TSP.55	SM.255	The Front End and/or the TSP Back End shall undeniably sign charge reports and/or toll declarations.
RQ.TSP.61	SM.410	The OBE shall support a Compliance Checking Communication transaction over an interface with security as defined in chapter 8.3 in a GNSS environment.
RQ.TSP.62	SM.220	The RSE shall request the OBE to calculate and provide a DSRC Message Authentication Code for Toll Charger (MAC_TC) over at least the EN ISO 14906 attributes PaymentMeans, using a key known only to the Toll Charger and the Toll Service Provider during a CCC transaction. The OBE shall respond accordingly.
RQ.TSP.90	SM.101	The TC shall register the data processing application of the EFC system with the national data protection commissioner or authority for compliance with national data protection regulations.
	SM.102	The TC and the TSP shall sign a Personal Data Assistant Agreement to be compliant to the national data protection regulations of the TC. In this agreement the duties and rights of the TSP are stated in regard to the data processing.

Requirement	Measure code(s)	Measure
	SM.103	The contracting parties of communication providers shall sign a Personal Data Assistant Agreement to be compliant to the national data protection regulations of the TC. In this agreement the duties and rights of the communication provider are stated in regard to the data processing.
	SM.104	The TC shall perform audit(s) of the TSP systems and procedures to proof the adherence to the registered data processing application and the Personal Data Assistant Agreement.
	SM.105	The contracting parties of communication providers shall perform audit(s) of the communication providers systems and procedures to proof the adherence to the registered data processing application and the Personal Data Assistant Agreement.
RQ.TSP.91	SM.101	The TC shall register the data processing application of the EFC system with the national data protection commissioner or authority for compliance with national data protection regulations.
	SM.102	The TC and the TSP shall sign a Personal Data Assistant Agreement to be compliant to the national data protection regulations of the TC. In this agreement the duties and rights of the TSP are stated in regard to the data processing.
	SM.103	The contracting parties of communication providers shall sign a Personal Data Assistant Agreement to be compliant to the national data protection regulations of the TC. In this agreement the duties and rights of the communication provider are stated in regard to the data processing.
	SM.104	The TC shall perform audit(s) of the TSP systems and procedures to proof the adherence to the registered data processing application and the Personal Data Assistant Agreement.
	SM.105	The contracting parties of communication providers shall perform audit(s) of the communication providers systems and procedures to proof the adherence to the registered data processing application and the Personal Data Assistant Agreement.
RQ.TSP.92	SM.322	The Front End shall be designed as a clearly distinguished entity with a defined interface to the proxy or TSPs Back End. The Front End's functionality shall be tested to guarantee ist functionality and it shall be auditable according to a defined procedure.
RQ.TSP.95	SM.204	The Toll Charger and Toll Service Provider shall agree on a service level agreement defining quality goals and response times.

Table 26. Standard Toll Service Provider related security measures

The following Table 27 shows the security measures for toll service providers in the different REETS environments. Grey shaded cells indicate that the requirement does not apply in the related environment. The standard security measure(s) are outlined in **bold**. Possible additional measures are outlined in **red**.

	CH	DE	F1	I	PL	E	A/DK
RQ.TSP.01		• **SM.421** • **SM.422**	•		• **SM.421** • **SM.422**		•
RQ.TSP.02	• **SM.211** • **SM.213** • **SM.230** • **SM.312**	• **SM.213** • **SM.230** • **SM.312** • **SM.420**	•		• **SM.211** • **SM.213** • **SM.230** • **SM.420**		• **SM.211** • **SM.213** • **SM.512** • **SM.520**

	CH	DE	F1	I	PL	E	A/DK
	• SM.420 • SM.421 • SM.512 • SM.520	• SM.421 • SM.512 • SM.520			• SM.421 • SM.512 • SM.520		
RQ.TSP.04	• SM.240	•	•		• SM.240		• SM.240
RQ.TSP.05	• SM.421	•			• SM.421		•
RQ.TSP.06	• SM.212 • SM.222 • SM.231 • SM.413 • SM.414 • SM.416	• SM.222 • SM.231 • SM.413 • SM.414 • SM.416			• SM.212 • SM.222 • SM.413 • SM.414 • SM.416		• SM.212 • SM.413 • SM.414 • SM.416
RQ.TSP.07	SM.205	SM.205			SM.205	SM.205	SM.205
RQ.TSP.09	SM.414	SM.414			SM.414		SM.414
RQ.TSP.10					SM.251	SM.251	SM.251
RQ.TSP.12	•	• SM.252 • SM.258 • SM.259	•	•	• SM.252 • SM.258 • SM.259	• SM.252 • SM.258 • SM.259	• SM.258 • SM.259
RQ.TSP.13	• SM.253	• SM.253	•	• SM.253	• SM.253	•	•
RQ.TSP.14	• SM.254	• SM.254	•	• SM.254	• SM.254		•
RQ.TSP.15	•	• SM.321 • SM.515	•		• SM.321	•	•
RQ.TSP.16	SM.417	SM.417			SM.417		
RQ.TSP.19	• SM.220 SM.423	• SM.220 SM.423		• SM.423	• SM.220 SM.423		SM.423
RQ.TSP.20	• SM.420	• SM.420	•		• SM.420	SM.420	
RQ.TSP.21	• SM.424 • SM.511 • SM.512	• SM.424	•		• SM.424 • SM.511 • SM.512	• SM.424 • SM.511 • SM.512	• SM.424 • SM.511 • SM.512
RQ.TSP.40	• SM.212 • SM.222 • SM.231 • SM.413	• SM.222 • SM.231 • SM.413	•	•	• SM.212 • SM.222 • SM.413	• SM.212 • SM.222 • SM.413	• SM.212 • SM.222 • SM.413
RQ.TSP.41	• SM.212 • SM.222	• SM.222 • SM.231	•	•	• SM.212 • SM.222	•	• SM.212 • SM.413

	CH	DE	F1	I	PL	E	A/DK
	• SM.231 • SM.413	• SM.413			• SM.413		
RQ.TSP.42	• SM.102 • SM.103 • SM.104 • SM.105	• SM.102 • SM.103 • SM.104 • SM.105	•	•	• SM.102 • SM.103 • SM.104 • SM.105	• SM.102 • SM.103 • SM.104 • SM.105	• SM.102 • SM.103 • SM.104 • SM.105
RQ.TSP.51	• SM.223 • SM.257 • SM.310 • SM.311 • SM.318 • SM.319 • SM.410 • SM.412	• SM.223 • SM.257 • SM.310 • SM.311 • SM.318 • SM.319 • SM.410 • SM.412					
RQ.TSP.52	• SM.257 • SM.310 • SM.311 • SM.312 • SM.314 • SM.318 • SM.412	• SM.257 • SM.310 • SM.311 • SM.312 • SM.314 • SM.318 • SM.412	•	•	• SM.314	•	
RQ.TSP.55	• SM.255	•			• SM.255		
RQ.TSP.61	•	• SM.410					
RQ.TSP.62	•	• SM.220	•		• SM.220	• SM.220	
RQ.TSP.90	• SM.220 • SM.102 • SM.103 • SM.104 • SM.105	•	•	•	• SM.220 • SM.102 • SM.103 • SM.104 • SM.105	• SM.220 • SM.102 • SM.103 • SM.104 • SM.105	• SM.102 • SM.103 • SM.104 • SM.105
RQ.TSP.91	• SM.220 • SM.102 • SM.103 • SM.104 • SM.105	•	•	•	• SM.220 • SM.102 • SM.103 • SM.104 • SM.105	• SM.220 • SM.102 • SM.103 • SM.104 • SM.105	• SM.102 • SM.103 • SM.104 • SM.105
RQ.TSP.92	•	•	•	•	• SM.322 •	• SM.322 •	•
RQ.TSP.95	• SM.204	• SM.204	•	•	• SM.204	• SM.204	• SM.204
RQ.TSP.R1	• No REETS security measures specified						

	CH	DE	F1	I	PL	E	A/DK
RQ.TSP.R2	• No REETS security measures specified						

Table 27: REETS Toll Service Provider related security measures

Remarks:

1) DE
   a) RQ.TSP.10: In the German EETS context, the TSP is linking billing details to toll declarations

A.8 User related requirements and measures

A.8.1 User related security measures

No standard security measures are defined for the User related requirements. In addition, no explicit security measures have been identified for the REETS environment.

Annex B : list of Directives related to data privacy

PRIVATE DATA PROTECTION
DATA RETENTION DIRECTIVE 2006/24/EC:
“Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58 EC”
(15 March 2006)

PRIVACY AND ELECTRONIC COMMUNICATIONS DIRECTIVE 2002/58/EC:
“Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector”
(12 July 2002)

CORRIGENDUM: DIRECTIVE 2009/136/EC:
“Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws”
(25 November 2009)

CORRIGENDUM: DIRECTIVE 2009/140/EC:
“Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services”
(25 November 2009)

DATA PROTECTION DIRECTIVE 95/46/EC:
“Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”
(24 October 1995)

REGULATION (EC) NO 45/2001:
“Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data”
(18 December 2000)

DECISION 2008/597/EC:
“Commission Decision of 3 June 2008 adopting implementing rules concerning the Data Protection Officer pursuant to Article 24(8) of Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data”
(3 June 2008)

Annex C Glossary

No.	Terminus	Abbrev.	(short) description
1	Service Provider	SP	Company / Entity offering the services of an EETS-Provider but not necessarily formally registered as an EETS-Provider. Since the REETS Project shall facilitate the transition to EETS, it is recommended, to generally use "Service Provider (SP)", except if "EETS-Provider shall be explicitly addressed (e.g. in the context of registration).
2	EETS-Provider	EP	A legal entity fulfilling the requirements of Art 3 and registered in a Member State where it is established, which grants access to EETS to an EETS user (see Art 2 b) Decision 2009/750/EC).
3	Member State	MS	EU Member State
4	European Electronic Toll Service	EETS	The abbreviation EETS stands for European Electronic Toll Service. It is a service that enables the payment of tolls with a single contract at a single EETS provider and just one on-board unit throughout the European Union.
5	Regional European Electronic Toll Service	REETS	The REETS-TEN project aims at deploying EETS compliant services in a cross-border regional project. The Project shall cover the electronically toll network of 7 Member States (Austria, Denmark, France, Germany, Italy, Poland and Spain) and Switzerland.
6	Toll Charger	TC	Public or private organisation which levies tolls for the circulation of vehicles in a toll domain (see Art 2 k) Decision 2009/750/EC)
7	User		Physical or legal person who subscribes a contract with a Service Provider in order to have access to EETS compliant services (see Art 2 c) Decision 2009/750/EC).
8	On Board Equipment	OBE	The complete set of hardware and software components required for providing EETS compliant services which is installed in a vehicle in order to collect, store, process and remotely receive/transmit data (see Art 2 e) Decision 2009/750/EC)
9	Interoperability constituents		Any elementary component, group of components, subassembly or complete assembly of equipment incorporated or intended to be incorporated into EETS upon which the interoperability of the service depends directly or indirectly, including both tangible objects and intangible objects such as software, see Article 2 of the EETS Decision. Examples of interoperability constituents are on-board equipment (including connected back office systems), roadside equipment (including charging beacons, localization augmentation beacons and enforcement devices), EETS Providers' and Toll Chargers' back-office data exchange systems.
10	Toll		A charge, tax or duty levied in relation with circulating a vehicle in a toll domain (see Art 2 j) Decision 2009/750/EC)
11	Toll domain		An area of EU territory, a part of the European road network or a structure (such as a tunnel, a bridge, a ferry,..) where toll is collected (see Art 2 n) Decision 2009/750/EC).

No.	Terminus	Abbrev.	(short) description
12	Tariff class		The set of vehicles treated similarly by a Toll Charger (see Art 2 g) Decision 2009/750/EC).
13	Vehicle classification parameters		The vehicle related information according to which tolls are calculated based on the Toll Context Data (see Art 2 q) Decision 2009/750/EC).
14	Certification		Certification is defined as an EETS Provider's or its representative's official written statement that its interoperability constituents comply with the associated specified (technical) requirements.
15	Technical accreditation		Technical accreditation covers the technical aspects of the accreditation of an already registered EETS Provider in individual toll domains under responsibility of a Toll Charger (or a cluster of Toll Chargers).
16	Technical requirements for registration		Requirements defined by the Member State responsible for the registration to check against Article 3b of the EETS decision
17	Toll domain independent specifications		Technical specifications for interoperability constituents that are defined by technical standards or other regulations or specifications independently from individual toll domain requirements
18	Toll domain specific specifications		Technical specifications for interoperability constituents that comprise requirements that are specific to the needs of a toll domain
19	Security Policy		A Security Policy is a set of requirements and applicable counter measures specified by the party responsible for the security in a system exposed to threats. These counter measures are based upon a risk analysis of the system in order to protect those data exposed to threats in the relationships between TC and SP.
20	Cluster		A cluster of ETC Toll Domains is a set of Toll Domains, interconnected or not, which feature the same or very similar ETC toll collection context(s) in a contractual framework like Memorandum Of Understanding or any other agreement between the Toll Domain representatives, *i.e.* the Toll Chargers. This agreement specifies the rules regarding interoperability and its management within that cluster of ETS Toll Domains; it includes references to mutually agreed and shared detailed contractual, procedural and operational documentation as well functional and technical specifications (particularly, interfaces for OBU // RSE and for Toll Charger // Service Provider central systems). A cluster of Toll Domains may have a unique representative for some common subjects. Relationship between Toll Domains and Service Providers are fixed by bilateral contracts. Common validity periods of bilateral contracts with a given ETC Provider allow the interoperability for the global cluster.

No.	Terminus	Abbrev.	(short) description
21	Accreditation		The Accreditation covers the whole procedure (contractual and technical) to be successfully fulfilled by a Service Provider in order that its technical system could be accepted on a Toll Domain and that the TC entrusts the SP with the toll collection and the invoicing process to the SU. When the Accreditation is successfully completed, the Service Provider is “accredited” in the relevant Toll Domain.