EasyGo Security Policy

Annex 1.3 to
Joint Venture Agreement
Toll Service Provider Agreement

Document:	103
Version:	3.0
Date:	9 October 2019

Table of contents

Document Revision History

Version	Date	Author	Main changes
1.0	2013.08.28	MHA	Approved by steering committee
2.0	2018.05.28	HHA	Commented and approved by ESC
2.1	2018.12.05	SR	Procedure chapter 6
2.2	2018.12.28	MHS	Split of document into this public EasyGo security policy and the confidential EasyGo security framework
2.3	2019.02.15	ESG	Small update in chapter 2
2.4	2019.05.16	ESG	Small corrections
2.5	2019.08.27	ESG	Update of references in chapter 4 Update of chapter 2.3.2
2.6	2019.09.12	MHS	Update of chapter 1
2.7	2019.09.16	ESG	Small update in chapter 1
3.0	2019.10.08	ESG	Approved with comments by ESC on 24/9

1 Scope

1.1 General

The information security is not covered by the Joint Venture Agreement and the Toll Service Provider Agreement. Hence, this document is also a supplement to these two basic agreements in the EasyGo contractual framework.

This public EasyGo security policy covers the management aspects of security in EasyGo. It contains the security objectives and policies for all common assets and processes of all involved EFC systems at the Toll Chargers (TC) and Toll Service Providers (TSP) connected to the EasyGo Hub (EGH) and the EasyGo Hub itself.

The confidential EasyGo security framework (see document 103-A) covers the technical aspects of security in EasyGo. This document is only available to the EasyGo actors.

Both documents are valid for the EasyGo Hub and all EasyGo actors, being TCs and TSPs as well as external toll service providers and toll chargers (these external TCs and TSPs are also referred to as service recipients) who send or receive transactions via the EasyGo Hub.

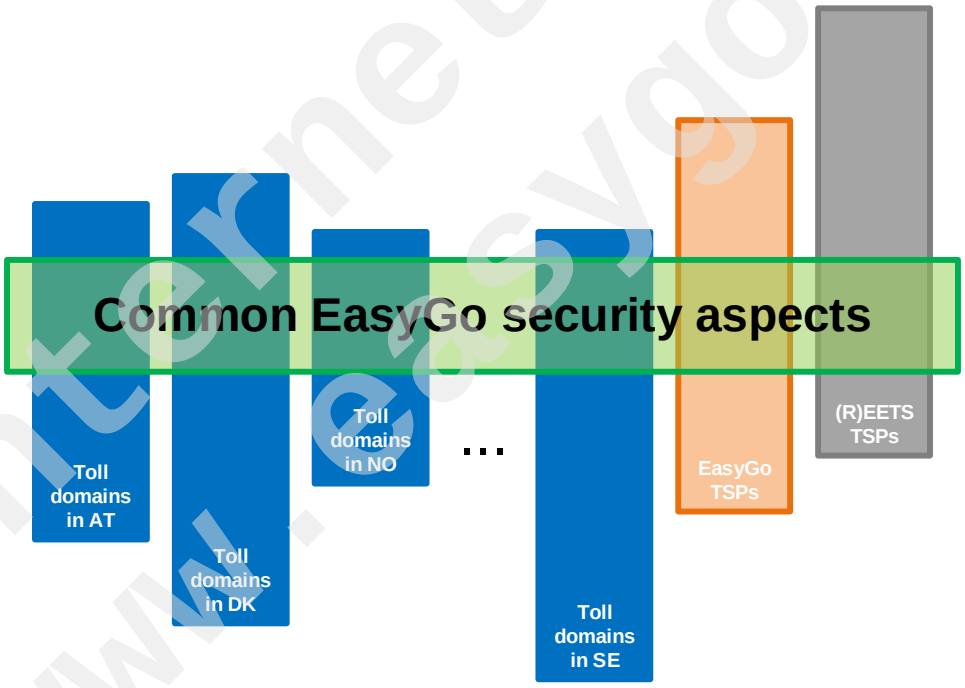

Figure 1 Scope of the EasyGo security policy

The baseline of the EasyGo security policy are the security objectives in chapter 3.1of this document. Based on the security objectives the policy statements in chapter 3.2 are developed according to the procedure shown in **Figure 2**.

The relevant security requirements and security measures are contained in the confidential document 103-A, which is available to EasyGo actors only. They were selected according to the procedure shown in **Figure 2**

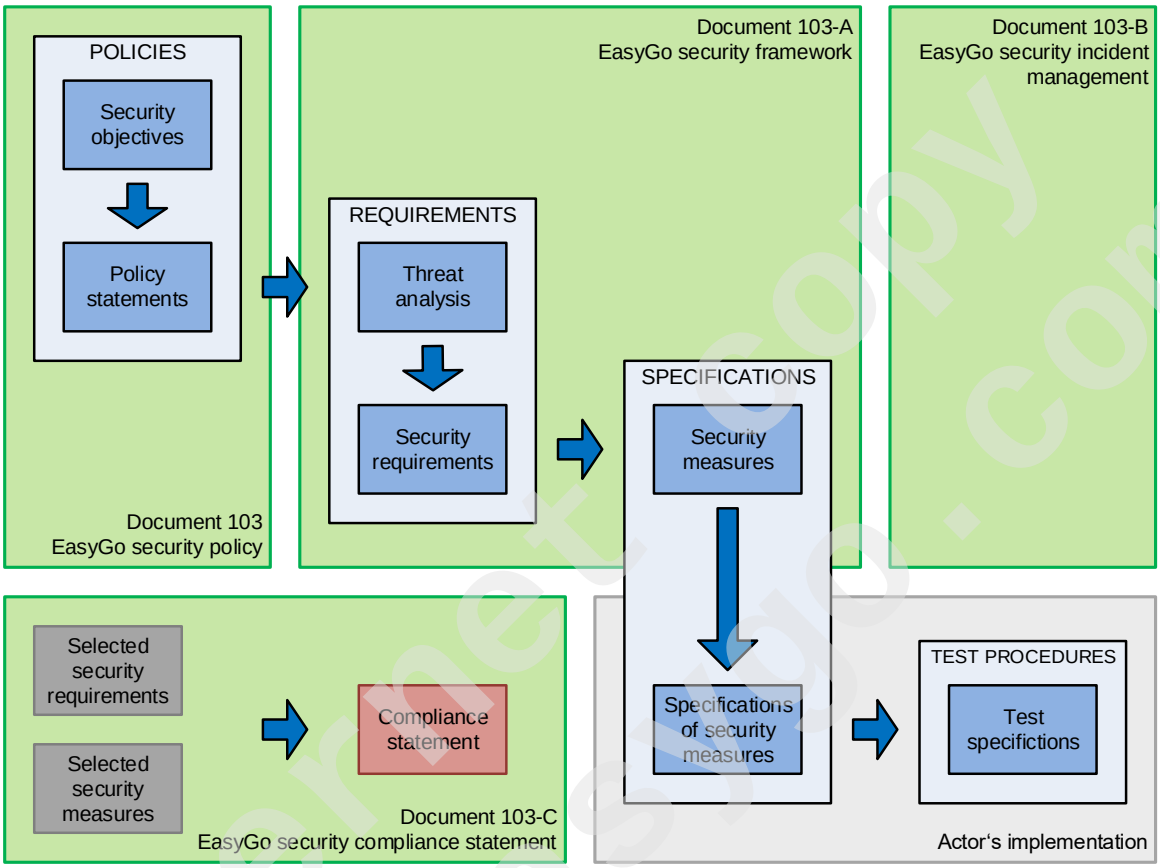

Figure 2. Development path for the security elements

Specifications of security measures and **Security test procedures** are out of scope of this document, because such procedures must be tailored for a specific system/subsystem by the responsible actor (TCs, TSPs, EGH).

The adherence to the EasyGo security policy and the EasyGo security framework is evaluated by each actor individually in a self-assessment procedure (see document 103-C).

1.2 Document contents

The public EasyGo security policy covers the aspects of information security in the EasyGo environment of all involved central Electronic Fee Collection (EFC) systems (EGH), TCs and TSPs. This policy applies to the information and communication assets of the EasyGo parties and service recipients and to organizations and their sub-contractors that are part of EasyGo.

This security policy applies to:

- Information and communication infrastructure of EasyGo including:
  - Physical assets such as the EGH, On Board Equipment (OBE), Road Side Equipment (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
- Organisations and their sub-contractors that send or receive transactions via the EGH and also organisations delivering services for the EasyGo infrastructure.
  - EasyGo TCs and TSPs
  - Entities delivering services to the EasyGo infrastructure
  - External TCs and TSPs (service recipients) sending/receiving data via the EGH
  - Subcontractors of any of the above
- All employees including permanent and temporary staff and any other persons who require access to information and/or manage information as part of any of the organisations listed above.

The confidential EasyGo security framework covers the selection of security requirements and security measures based on the guiding principles of the security policy and a threat analysis to identify the security requirements relevant for the EasyGo security implementation.

A given security requirement may not apply in all environments. Therefore EasyGo security requirements make a distinction on the type of the affected actor and the specific interface(s).

1.3 Objectives

The aim of this document is to define the EasyGo security policy, which sets the governing objectives and policies that are binding for all actors in EasyGo, organisations exchanging data via the EGH and other organisations using or supporting the EasyGo infrastructure, for all EasyGo related information being handled by them.

The provision and the quality of the EasyGo services as well as the information security is within the responsibility of the EasyGo Steering Committee (ESC). This EasyGo security policy expresses the ESC's commitment to the implementation, maintenance, and improvement of its information security management system.

The ESC has given a mandate to develop and maintain the information security to the EasyGo Security Group (ESG) which is responsible for developing and maintaining the necessary security documents.

The security documents shall be continuously developed and maintained by the ESG. Each new revision will become binding after the adoption by the ESC.

The objective of this document is to provide support for information security in accordance with business requirements and relevant laws and regulations.

It defines the security objectives and security policies to govern the implementation of information security within EasyGo both during their creation, but also as they evolve during their life cycle.

The security policy shall also contribute to the EasyGo organisation's goals and strategies and shall support and protect the organisation's operations, competitiveness, general confidence and reputation.

2 Introduction to security

2.1 Background

Information security is based on the ISO "Information Security Management System" family of standards (ISO 27001 to 27007) and EFC specific standards ISO 17573 and ISO/TS 19299. The interrelations between these standards are shown in **Figure 3.**

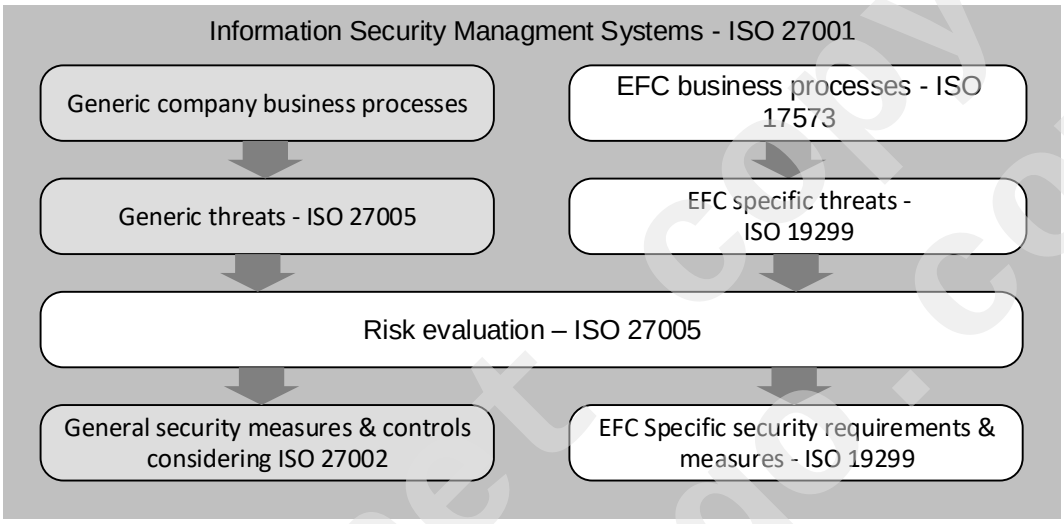

Figure 3. Information Security related standards and their relations

These standards deal with all relevant aspects of information security for a tolling environment.

Information security is the protection of information (with focus on electronic data) stored and/or handled by the personnel and assets involved in the provision of the EasyGo services and the service recipients.

Information and the supporting processes, systems and networks are very important business assets in EFC systems. The whole business model is based on collecting information, handling it and then collecting the payment from Service Users (SU) based on the collected toll data. Information security is essential for the accuracy, trustworthiness, reliability and availability of the EFC system as well as for the privacy of the SUs.

The EasyGo services provide a common interface for TSPs to several toll domains with formerly separate interfaces, thus enabling a standardized data exchange. It is evident that the security threats, vulnerabilities and consequences of any breaches of security are much greater in the whole integrated EasyGo area than they are in each separate system of independent TCs. The threats can both be internal (inside each local organisation or inside the EasyGo organisation) and external.

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

Figure 4 shows in principle the EasyGo actors, their assets and the data exchange interfaces between them which are subject to the EasyGo information security. The figure also shows that external organisations can connect to EasyGo TCs and TSPs via the EGH without being an EasyGo TSP or TC, but through bilateral agreements with one or more EasyGo TC or TSP. Such external organisations are equally bound by the EasyGo security principles if they are connected to the EGH.

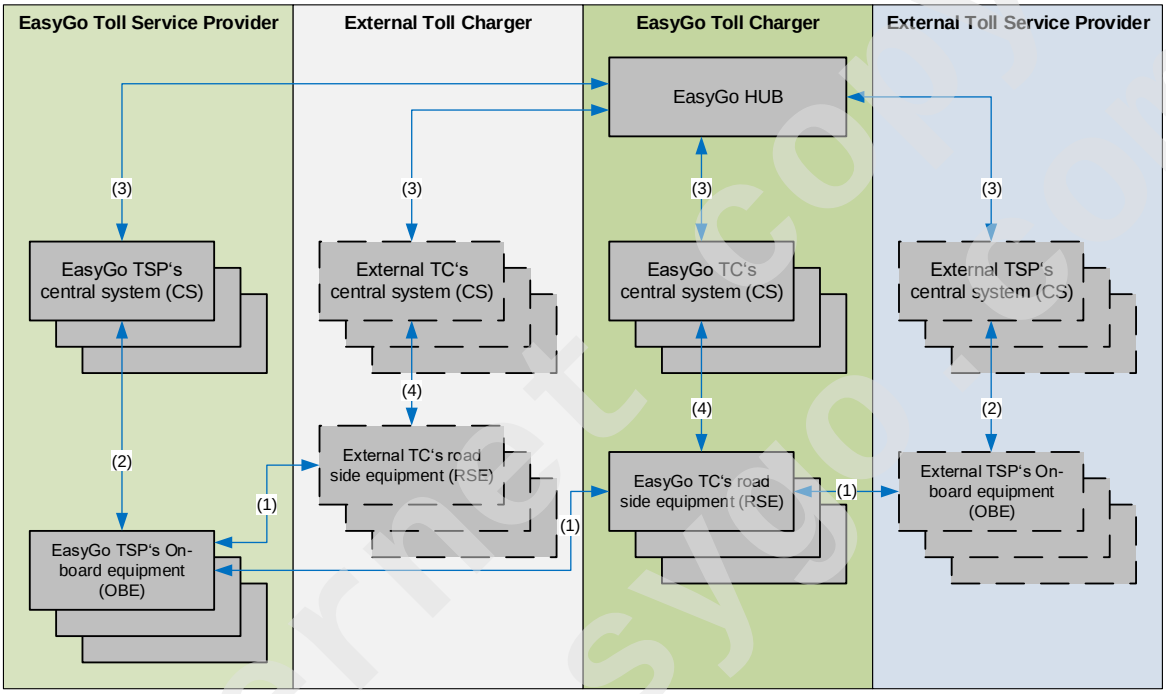

Figure 4 Actors and data exchange interfaces subject to security

The assets subject to the EasyGo information security are the TSP OBE, the TC RSE and the central systems (CS) of EasyGo TCs, external TCs, EasyGo TSP and external TSPs as well as the EGH connecting the different actors.

The interfaces subject to the EasyGo information security are between TSP OBE and TC RSE (1), between TSP OBE and TSP CS (2), between TSP CS and TC CS via the EGH, marked (3) in the above figure, and between TC RSE and TC CS (4).

Although only the interfaces (1) and (3) are interoperable interfaces in EasyGo, security threats may also exist for the TSP internal interface (2) and the TC internal interface (4).

2.2 Security environment

The diagram in **Figure 5** is based on a diagram from ISO/TS 19299 and shows the overall security environment of tolling systems. The diagram is enhanced by the inclusion of the EGH and extends the interoperability interfaces shown in Figure 2 with additional TSP and TC internal and external interfaces. The connections with the Interoperability Management are not shown (see chapter 2.3).

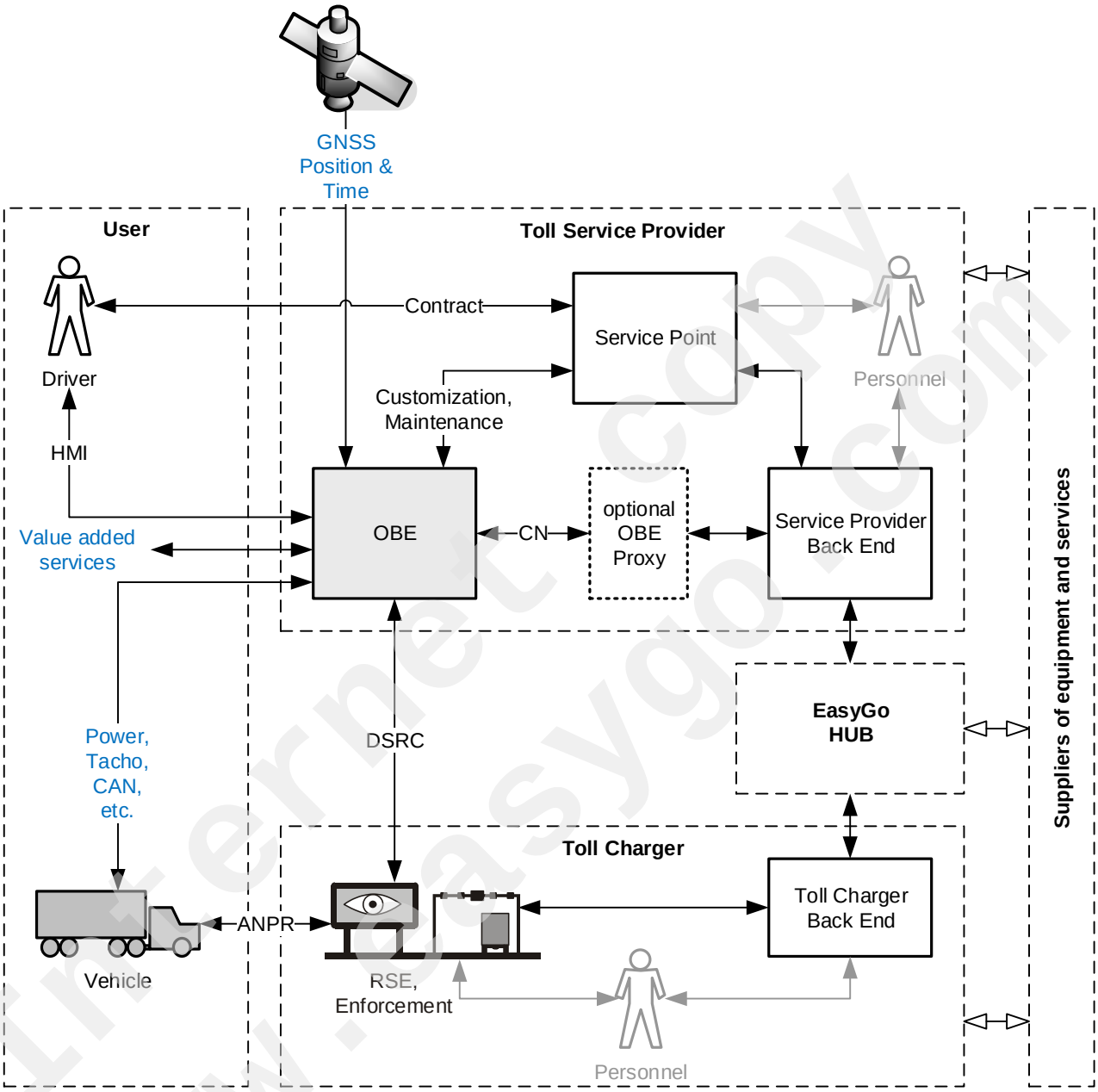

Figure 5. Security environment of tolling systems

Figure 5 outlines major areas of responsibility. Most of them correspond to the general roles defined in the EFC system architecture (ISO 17573):

1. EasyGo TC or external TC
2. EasyGo TSP or external TSP
3. Service user (User in ISO 17573)
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, additional roles have to be mentioned:

5. The EGH as data exchange platform between TSP and TC
6. The Interoperability Management (which has no technical communication interface to other roles in the daily operation)
7. Communication interfaces used by EETS providers like Global Navigation Satellite System (GNSS) functionalities for other toll domains (Shown in blue in Figure 5) currently without any direct relevance to EasyGo.

The data exchange across interfaces is shown in **Figure 5** as arrows. Some of these interfaces are covered by international 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 an EasyGo security implementation basically on securing interfaces among participating actors taking on a specific EFC role.

2.3 Trust model

2.3.1 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:

- TCs and TSPs
- TSPs and Interoperability Management
- TCs and EGH

The definition of a trust model implies a choice between:

- Hierarchical approach
- peer-to-peer approach
- or a combination of both

The default solution for the EasyGo parties shall be a peer-to-peer trust model, but a mixed model also allowing for hierarchical trust models and for service recipients (external TCs and TSPs) shall be supported as well.

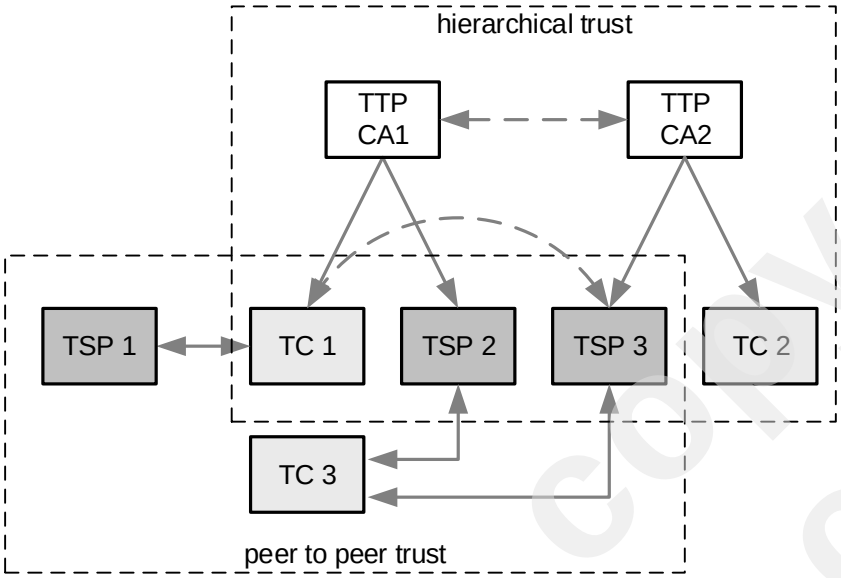

Figure 6 Trust model in EasyGo

2.3.2 Trust model implementation

The choice of all implementation details for the trust model is beyond the scope of the present document and will be handled in EasyGo documents 201 and 203 where the actual implementation of the trust model in EasyGo is described.

3 Security Policy

3.1 Security objectives

The EasyGo 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 3.2 have a higher priority. They can also serve as a management summary of the approach to security in EasyGo. The security objectives are numbered as SO-n.

[SO-1] Any data exchanged via the EGH shall fall under the EasyGo security rules

[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.

  This statement also covers the transmission of data between actors through the EGH 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 proven 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 requirement for confidentiality, integrity, authenticity, and non-repudiation.

[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 SU 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 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 SU to be compliant with the system.

[SO-4] The EasyGo security requirements shall cover any risks specific to the interoperability between the EasyGo actors as well as between EasyGo and external TCs and TSPs including subcontractors and entities supporting the EasyGo infrastructure and operation.

EasyGo is a compound of many separate toll domains that differ in many ways. The different charging technologies shall be respected, possibly leading to specific security requirements for the different types of toll domains in addition to the common EasyGo security requirements. The common EasyGo security requirements resulting from this policy shall therefore be limited to the common aspects of EasyGo but allow the co-existence of additional local security requirements for local systems.

Examples:

- technical solutions: barriers vs. free-flow
- legal requirements: fee vs. tax
- operational procedures: mandatory vs. non-mandatory OBE
- 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 and with external TCs and TSPs.

3.2 Policy statements

The EasyGo security policy contains policy statements on how the ESC intends to protect information in EasyGo. Each statement requires more detailed procedures and practices in the form of security measures 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 EasyGo organisation and its information and communication architecture and infrastructure for the benefit of the SUs, the EasyGo TCs and TSPs as well as service recipients.

3.2.1 General policy statements

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

- ensure confidentiality, integrity, authenticity, non-repudiation and availability of all information in the EasyGo EFC service operation and management – and for service recipients and their sub-contractors connected to the EGH
- prevent and limit the consequences of unwanted or unexpected information security events
- build the required trust and confidence between the involved actors.

EasyGo will use international and European security standards and European and national legislation for data protection (For a list of security related standards see chapter 0)
The standards

- ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems – Requirements

  covering all types of organisations (e.g. commercial enterprises, government agencies, non-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;

- "ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management",

  establishing guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation;

- ISO/TS 19299 EFC Security Framework,

  describing 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;

- General Data Protection Regulation 2016/679

  defining the general European requirements on personal data protection

- EasyGo documents “004 Personal Data Processing Terms - Toll Charger” and “005 Personal Data Processing Terms - Toll Service Provider”

  defining the Personal Data Processing Terms for TCs and TSPs

shall be adhered to in the EasyGo information security.

[PS-2] The EasyGo 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-3] 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 2016/79/EC on data protection shall be observed.

3.2.2 Organisational policy statements

[PS-4] EasyGo information security shall be governed by the ESC, developed and managed by the ESG and reviewed by the EasyGo Management (EM).

The ESG shall develop, coordinate and constantly improve the EasyGo information security procedures and make sure that they comply with all relevant standards and European legislation.

The ESG shall review the progress of implementing the EasyGo information security and ensure the continued compliance by the EasyGo actors and the service recipients and report any deviations to the EM.

The EM shall review all actions taken by the ESG.

The ESC shall mandate the implementation of the EasyGo information security and provide the required resources.

[PS-5] The ESG shall develop and maintain the EasyGo security policy (this document), the EasyGo security framework (document 103-A) and the EasyGo security compliance statement (document 103-C)

The ESG shall develop and maintain the EasyGo security policy statements.

The ESG shall choose security requirements and security measures relevant for EasyGo (see document 103-A). All security requirements and security measures shall be chosen based on a risk and vulnerability evaluation including a simplified threat analysis from ISO 19299.

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

The ESG shall develop and maintain a compliance statement form (see document 103-C) based on the chosen security requirements and measures to be used by the EasyGo actors and the service recipients in their reports.

[PS-6] The EasyGo actors and the service recipients shall provide a completed compliance statement (see document 103-C) on the EasyGo security framework to the ESG every two years pointing out any deviations. A measure shall be defined for each deviation.

The ESG shall keep a register of all defined measures and regularly check the status of their implementation.

Each EasyGo actor or service recipient shall implement a defined measure within 6 months or provide an indication and a reason for a longer implementation period, if needed. In such a case each EasyGo actor or service recipient shall provide an update on the status of implementation for each defined measure every 6 months.

The ESG shall verify the implementation of each measure and the provision of status reports of each measure.

The ESG will propose an action to the ESC if an EasyGo actor or service recipient does not implement a measure on time or does not provide a status report on an implementation of a measure. This action could be either a prolongation of the implementation deadline or a (temporary) disconnection of the EasyGo actor or service recipient if it poses a threat to the overall security in EasyGo.

[PS-7] Each EasyGo actor or service recipient shall develop and maintain security test procedures for a specific system/subsystem. The security test procedures shall be able to prove the compliance to all security measures and security requirements.

The ESG shall provide feedback on security test procedures to the EasyGo actors and service recipients if requested by an actor.

[PS-8] The EasyGo information security shall be subject to regular reviews every two years or when significant changes related to information security occur.

Regular risk evaluations shall be carried out as a revision of EasyGo's 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-9] The default solution to establish initial trust between TCs and TSPs shall be a peer-to-peer trust model.

3.2.3 Asset and interface management policy statements

[PS-10] There shall be compliance checks for all new assets, interfaces and processes introduced by existing or new EasyGo actors and service recipients based on the security test procedures.

[PS-11] The level of EasyGo information security shall not be reduced by the introduction of new EasyGo actors, services, products or service recipients.

[PS-12] All assets required for the operation of EasyGo shall be accounted for and have a nominated owner.

[PS-13] Any users of EasyGo 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 EasyGo assets shall follow the rules and requirements described within this document for secure use. These internal guidelines for secure use will be included as set of measurements in the EasyGo security specification and shall be adopted by each EasyGo actor.

[PS-14] Full traceability of processed information shall be guaranteed at all times.

3.2.4 Incident management policy statements

[PS-15] The EasyGo information security shall limit the consequences of security incidents.

[PS-16] Each EasyGo actor and service recipient shall actively limit the consequences of any security incident or violation of the EasyGo information security.

[PS-17] Each EasyGo actor and service recipient shall report any security incident or violation of the EasyGo information security to the EM and ESG without delay.

The EasyGo actor or service recipient shall initiate immediately all necessary inspections of his systems and countermeasures to accommodate a systematic improvement and learning process to minimise the risk of similar events and non-conformances.

The ESG shall initiate a review of the EasyGo security framework to accommodate a systematic improvement and learning process to minimise the risk of similar events and non-conformances.

4 References

For dated references, subsequent amendments to or revisions of any of these publications apply only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

4.1 Standards and external documents

Reference	Document Ref	Document title
	ISO 17573-1	Electronic fee collection — Systems architecture for vehicle-related tolling — Part 1: Reference model
	ISO 19299	Electronic fee collection — Security Framework
	ISO/TS 17574	Electronic fee collection — Guidelines for security protection profiles
	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
	ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls
	ISO/IEC 15408-1	Information technology — Security techniques — Evaluation criteria for IT security —Part 1: Introduction and general model
	ISO/IEC 15408-2	Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements
	CEN/TR 16968	Electronic Fee Collection — Assessment of security measures for applications using Dedicated Short Range Communication

4.2 European directives, decisions and regulations (legislative acts)

Reference	Document Ref	Document title
	(EU) 2016/679	General Data Protection Regulation
	2009/750/EC	European Commission Decision on the definition of the European Electronic Toll Service and its technical elements
	2004/52/EC	Directive on the interoperability of electronic road toll systems in the Community
	(EU) 2019/520	Directive on the interoperability of electronic road toll systems and facilitating cross-border exchange of information on the failure to pay road fees in the Union

4.3 EasyGo documents

Reference	Document Ref	Date / Version	Document title
[EasyGo-103-A]	103-A		EasyGo security framework (confidential)
[EasyGo-103-B]	103-B		EasyGo information security incident management (strictly confidential)
[EasyGo-103-C]	103-C		EasyGo security compliance statement (strictly confidential)
[EasyGo-004]	004		Personal Data Processing Terms – TC
EasyGo-005]	005		Personal Data Processing Terms - TSP
[EasyGo-205	205		DSRC Key Management