EasyGo security policy

Annex 1.3 to
Joint Venture Agreement
Toll Service Provider Agreement

Document: 103
Version: 1.0
Date: 28 August 2013

Table of contents

Document Revision History

Version	Date	Author	Main changes
0.1	2013.05.15	ESG	First draft
0.2	2013.05.21	ESG	Review and comments
0.3	2013.08.21	EM	Input from EasyGo management
1.0	2013.08.28	MHA	Approved by steering committee

1 Scope

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 security policy covers aspects of EasyGo only. It covers the common assets and processes of all involved EFC systems at the Toll Chargers (TC) and Toll Service Providers (TSP) and the EasyGo HUB.

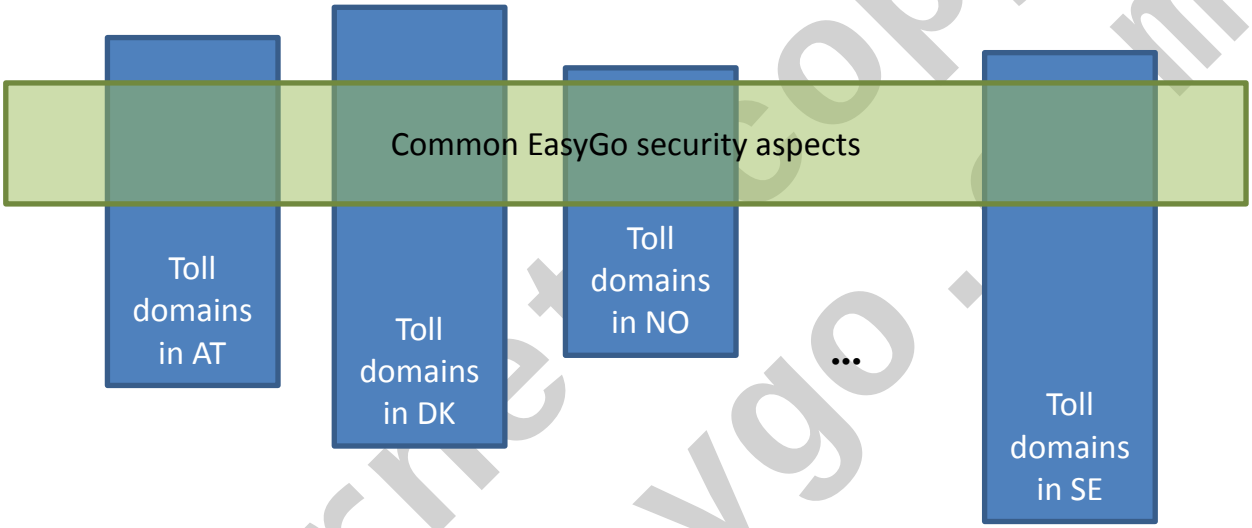

Figure 1 Roles in the toll charging environment

This policy applies to the information and communication infrastructure of EasyGo 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 EasyGo.

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 EasyGo.

While some aspects of security are determined by its governing body and are therefore added to the security policy other aspects will be handled as security requirements or security measures in other documents.

2 Introduction to security

2.1 EasyGo services

The EasyGo services are interoperable electronic fee collection (EFC) services provided by the EasyGo TCs and TSPs.

The EasyGo service covers the following main issues:

- Any Service User using an OBE issued by an EasyGo TSP can use it for toll charging at any TC offering the EasyGo service.
- The service is automatically available to all present and new users (opt-out).

The EasyGo+ service covers the following main issues:

- Any Service User using an OBE issued by an EasyGo+ TSP can use it for toll charging at any TC offering the EasyGo+ service.
- The service has to be specifically requested by the Service User (opt-in).

The development of the EasyGo services has been 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 EasyGo services are based on a fundament of experience from many years of EFC operation as well as results from European EFC projects:

- Agreements and contracts are based on CESARE III principles
- Architecture is based on ISO 17573
- EasyGo is developed without changes to legislation in any of the participating countries
- Different EFC transaction protocols are used, i.e. AutoPASS, PISTA I and EN 15509
- Local transactions are handled within each local toll domain
- The concept allows a dynamic growth across geographical borders and modes of transport (ferry, bridge, motorway …)

The provision and the quality of the EasyGo services as well as the information security is 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 gave a mandate to develop and maintain the information security to the EasyGo Security Group (ESG) which is responsible for developing and maintaining the necessary documents (see chapter 4).

By information security is meant 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.

[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)

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 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 Service Users.

The EasyGo services were 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 EasyGo 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 EasyGo organisation) 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 EasyGo actors, their assets and the data exchange interfaces between them which are subject to the EasyGo information security.

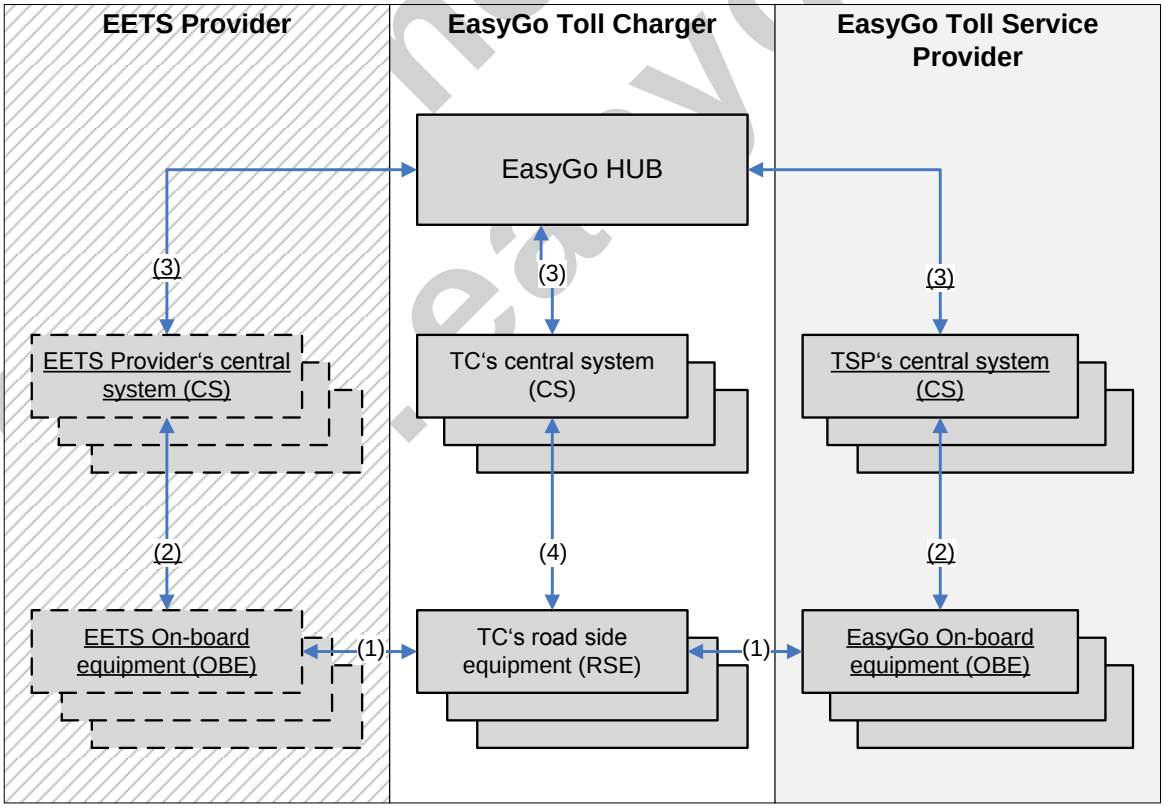

Figure 2 EasyGo actors and data exchange interfaces subject to security

The assets subject to the EasyGo information security are the TSP OBE, the TC RSE and both central systems (CS) of TC and TSP as well as the EasyGo HUB 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 EasyGo HUB, 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).

3 Objectives

The aim of this document is to define an EasyGo security policy which is binding to all actors in EasyGo for all EasyGo information being handled by them.

This document is a living security policy that shall be continuously developed and maintained by the ESG. Each new revision will become binding after the adoption in 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 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 policies will thus facilitate better cooperation between all EasyGo 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 EasyGo organisation's goals and strategies and shall support and protect the organisation's operations, competitiveness, general confidence and reputation.

4 Method of implementing this security policy

The main content of the **EasyGo security policy**, are the security objectives in chapter 5 and the policy statements in chapter 6, expressing the intentions of the EasyGo actors to deal with information security.

Based on this security policy the following documents define the implementation of a common EasyGo information security by analysing security threats, describing concrete security requirements and detailed security measures and device a security test specification on how to test each participating local system against them.

This policy will constitute the baseline from which to develop a second document, the **EasyGo security requirements**. In this document, which shall be based on a risk and

vulnerability evaluation including a simplified risk analysis of the EasyGo information security, requirements are chosen individually from the CEN EFC Security Framework[3].

In a third document, the **EasyGo security specification**, the detailed specification of each of the chosen requirements is described by one or many security measures to be taken for the implementation of a common approach to information security. The details of how to implement these described security measures are determined locally in each toll domain.

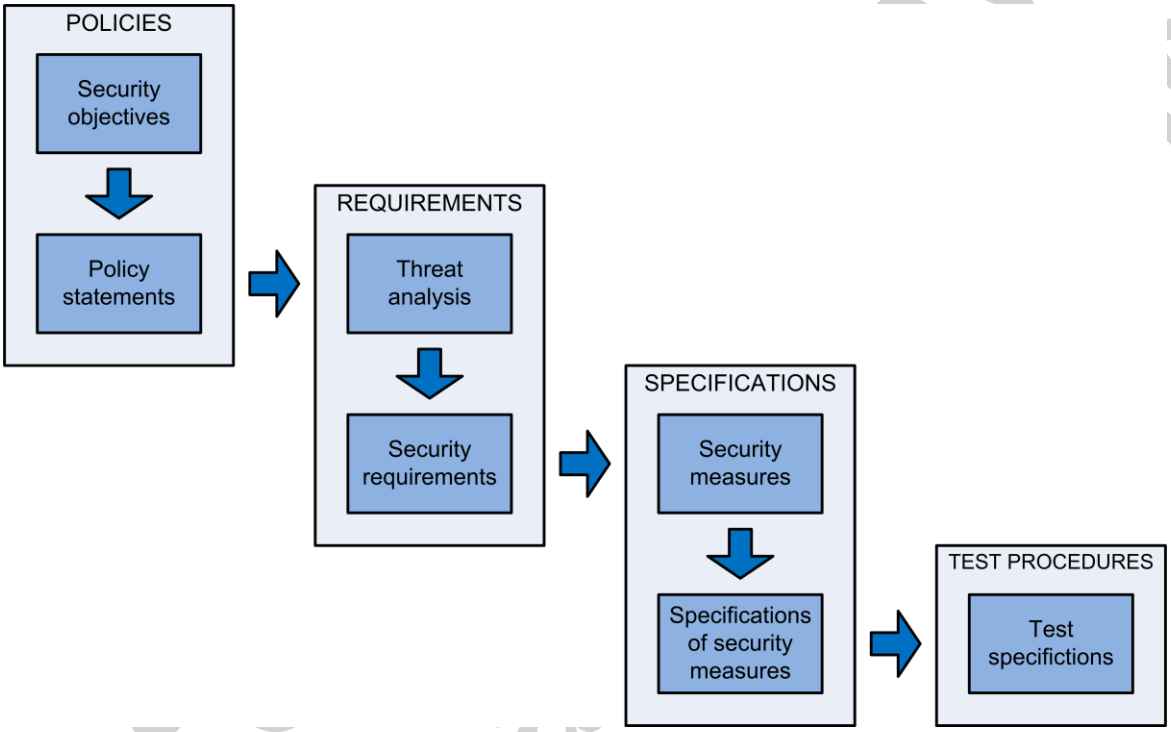

Figure 3 Development path for the security documents

In a fourth document, the **EasyGo security test procedures**, the detailed conformance tests are described to prove that the local implementation of the EasyGo information security covers all defined security requirements, security measures and/or security policies defined. These test procedures shall include an Implementation Conformance Statement (ICS).

5 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 6, have a higher priority. They can also serve as a

[3] CEN TS 16439 - EFC Security Framework

management summary of the approach to security in EasyGo. The security objectives are numbered as SO-n.

[SO-1] Any EasyGo toll data exchanged between a TC and a TSP 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 the EasyGo 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 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.

6 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 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 Service Users and the EasyGo TC and TSP.

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 EasyGo 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] EasyGo will use international and European security standards and European and national legislation for personal integrity.

The standards

- ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements"[4]
- "ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management"[5] and
- EFC Security Framework[6]

shall be adhered to in the EasyGo information security.[7]

[PS-3] 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.

[4] 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.

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

[6] 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.

[7] 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 EasyGo security requirements document and in the EasyGo security specification document respectively.

[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.

6.2 Organisational policy statements

[PS-5] EasyGo information security shall be governed by the ESC, developed and managed by the ESG and reviewed by the EM.

The ESG shall develop, coordinate and maintain and constantly improve the EasyGo information security documents.

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

The ESC shall provide the resources required for these tasks.

[PS-6] The ESG shall develop and maintain the EasyGo security policy (this document)

[PS-7] The ESG shall develop and maintain the EasyGo security requirements. All security requirements shall be chosen based on a risk and vulnerability evaluation including a simplified risk analysis.

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

[PS-8] The ESG shall develop and maintain the EasyGo 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 ESG shall develop and maintain the EasyGo security test procedures to enable the testing of EasyGo actors' assets, interfaces and processes. The EasyGo security test procedures shall be able to prove the compliance to all security measures and security requirements.

[PS-10] The EasyGo 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 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-11] The default solution to establish initial trust between the EETS operators (Toll Chargers and EETS 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 EasyGo 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 EasyGo 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.

6.3 Asset and interface management policy statements

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

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

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

[PS-17] 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 internal guidelines 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-18] Full traceability of processed information shall be guaranteed at all times.

[PS-19] The ESG shall maintain a process for suppliers and TSP to get their components and procedures qualified with regards to the EasyGo security test procedures. The process shall also apply to additions and modifications to the components and procedures.

6.4 Incident management policy statements

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

[PS-21] Any user of EasyGo assets shall report any unwanted information security incident or violation of the EasyGo information security to the EM.

The EM 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.