EETS Security Policy
**Terms and abbreviations**

<table>
<thead>
<tr>
<th>Term/Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>EETS</td>
<td>European Electronic Toll Service</td>
</tr>
<tr>
<td>EETS Information Security</td>
<td>The protection of information stored, exchanged and handled by the personnel and assets specifically involved in the provision of the EETS.</td>
</tr>
<tr>
<td>EETS operators</td>
<td>EETS Providers and Toll Chargers of toll domains under the scope of the European Directive 2004/52/EC</td>
</tr>
<tr>
<td>EETS parties</td>
<td>EETS Providers and Toll Chargers of toll domains under the scope of the European Directive 2004/52/EC as well as member states of the European Union and organisations performing the EETS Interoperability role</td>
</tr>
<tr>
<td>EFC</td>
<td>Electronic Fee Collection</td>
</tr>
<tr>
<td>ESG</td>
<td>EETS Security Group</td>
</tr>
<tr>
<td>TC</td>
<td>Toll Charger</td>
</tr>
<tr>
<td>Toll Data</td>
<td>Toll Declarations and Toll Domain Statements according to the definitions in CEN ISO 12855 and the European Commission Decision 2009/750</td>
</tr>
<tr>
<td>TTP</td>
<td>Trusted Third Party</td>
</tr>
</tbody>
</table>
# Table of contents

1 Introduction ..................................................................................................................5
   1.1 EETS Background ................................................................................................. 5
   1.2 EETS Security Background .................................................................................... 5
   1.3 Objectives ............................................................................................................... 6
   1.4 Scope of this security policy .................................................................................... 6
   1.5 Method of implementing this policy ........................................................................ 7

2 High level policy statements .........................................................................................9

3 Detailed policy statements ..........................................................................................11
   3.1 Overall security objectives ...................................................................................... 11
   3.2 Governance and management ................................................................................ 11
   3.3 Trust model ........................................................................................................... 12
   3.4 Compliance checking .............................................................................................. 12
   3.5 Compliance with standards .................................................................................... 12

Annex A Interoperability Management regarding EETS security ...................................14

Annex B Establishing the EETS Security Group ..............................................................15
1 Introduction

1.1 EETS Background

The Commission decision on the definition of the European Electronic Toll Service (EETS) and its technical elements adopted on 6th October 2009 lays down that EETS will be available within three years for all road vehicles above 3.5 tonnes or which are allowed to carry more than nine passengers (including the driver), and within five years for all other vehicles respectively.

Time is short and there is high pressure on all actors involved. Many stakeholders feel uneasy because of a lack of certain definitions, especially organisational matters and in terms of specifications. The Directive 2004/52/EC, Decision 2009/750 and a significant number of technical standards are in place. An Application Guide for further explanation on how to use and implement the EETS has been created by the EU Commission. However, it is still unclear how everything is connected and what is missing in particular. Certain definitions need to be more precise and mandatory to allow a smooth implementation of EETS by all stakeholders.

The discomfort among stakeholders increased as the Toll Chargers published the EETS Domain Statements. They turned out to be quite different in scope and depth, which is why, in summary, it can be stated that uncertainty prevails on what the parties of the EETS can rely on.

In the effect of this resonance the Stockholm Group has decided to launch four work packages consisting of several work items on missing specifications, which were identified in an assessment done by Rapp Trans on behalf of ITS Sweden.

Each item emphasises relevant details that need to be harmonised or even made binding to enable the interoperability scheme to work and to support an efficient implementation by the EETS stakeholders.

In a follow up Stockholm Group workshop, attended by the European Commission, the Security work item was emphasised as especially critical.

1.2 EETS Security 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 accumulating information, handling it and then collecting the corresponding payment from service users. Information security is essential for the accuracy, trustworthiness, reliability and availability of the EFC system as well as for the privacy of the users.

The EETS system is intended to combine several currently independent EFC systems into a network covering the whole of 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 EETS system than they are in a system of independent EFC operators. The threats can both be internal (inside each local organisation or inside the EETS 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.

1.3 Objectives

This document is a proposal from the Stockholm Group (with the support of the Swedish road user charging research and development project ARENA). The aim of the proposal is to reduce uncertainties on security policy issues by giving a clearly formulated position of the members of Stockholm Group. The group is convinced that a more harmonized view on security issues is needed to speed up the process of EETS implementation. Stockholm Group believes that EETS will have to evolve even after October 2012, which is when the EETS comes into effect according to Decision 2009/750. The objective of the EETS Security Policy is to guide all EETS parties on security issues in this continuous process.

This document should be seen as a proposal for a security policy that could be adopted and maintained by an Interoperability Management entity (e.g. represented by an organisation or an association of stakeholders, see Annex B for a discussion on its implementation).

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 thus facilitates better cooperation.

This security policy underpins and motivates the requirements and the technical security and test specifications (see section 1.5) both during their creation, but also as they evolve during their life cycle.

1.4 Scope of this security policy

This security policy covers aspects of the EETS only. It covers the interoperability constituents as defined in the Decision 2009/750, i.e. common assets and processes of all EFC systems involved.

![Figure 1 Security policy scope](image.png)
This policy applies to the information and communication infrastructure of the EETS system 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 the EETS.

Some aspects of the policy are expected to be determined by its governing body (see Annex B for a discussion on its implementation) and should be added to the policy, the requirements or the specifications documents later. Some aspects that need to be defined for the security policy are

- frequency of policy reviews,
- frequency and criteria for which aspects should be considered as common assets and processes of all EFC systems involved and thus fall into the scope of the policy.

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 the EETS.

1.5 Method of implementing this policy

The main content of this report, the EETS Security Policy, are the policy statements in Chapter 2 and 3, expressing the intentions of the EETS stakeholders to deal with EETS Information Security.

Based on this policy further documents will need to be worked out which define the implementation of a common EETS Information Security by describing concrete requirements and detailed measures and how to test each participating local system against them.

This policy will constitute the baseline from which to develop a second document, the EETS Security Requirements. In this document, which shall be based on a risk and vulnerability evaluation including a simplified risk analysis of the EETS information security, requirements are chosen individually from the CEN EFC Security Framework\(^5\).

In a third document, the EETS 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.

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

\(^5\) prCEN TS 16439 - EFC Security Framework
Figure 2 Division of content between the documents; EETS Security Policy, EETS Security Requirements, EETS Security Specification and EETS Security Test Procedures
2 High level policy statements

The EETS Security Policy shall be guided by the high level policy statements listed below. They express broad objectives and shall, in the case of a conflict with any of the detailed policy statements in chapter 3, have a higher priority. They can also serve as a management summary of this whole document. All policy statements, both high-level and detailed, are numbered as PS-1, PS-2 etcetera.

| PS-1: TOLL DATA SHALL BE CORRECT, COMPLETE, TRACEABLE AND PROTECTED |
| NOTE: this statement covers the Confidentiality-Integrity-Availability (CIA) triad, see below. |
| Correct Toll data fully and accurately records all required road usage parameters according to the rules of the toll scheme in question. |
| This statement also covers the transmission of data between actors and thereby requires data integrity in communication. |
| Complete Toll data means that no toll data is lost, deliberately or otherwise according to the rules of the toll scheme in question. |
| 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 emphasises the need to secure not only correct recording, but also correct reporting and thereby requires data availability. |
| Traceable Toll data can be traced back to its originator/owner in a manner such 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 stakeholder to another, the responsibility and ownership of data must be clear at each step. In particular, if errors or falsifications are added in one in 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 Toll data can only be accessed by authorised parties. |
| The EETS system shall for all parts of the Toll data clearly define which actors under which conditions can access it. The upholding of these definitions shall be supported by cryptographic, administrative and other procedures. This statement requires data confidentiality. |

For example, if in one toll scheme road usage shall be reported as visited locations with a sample interval of two seconds and maximum error of twenty meters, then each reported position in the Toll Declaration shall fulfil this requirement. In another toll scheme, road usage shall be reported as the number of kilometres driven per month and tariff zone. While the second example requires considerably less reporting detail, the correctness statement applies equally. The statement can also be enforced with equal severity in both schemes.

| PS-2: EETS INFORMATION SECURITY SHALL TREAT EETS USERS WITH THE SAME CHARACTERISTICS EQUALLY |
| Differing treatment based on known and relevant individual characteristics, such as vehicle type or known history of user behaviour may be employed in the EETS. In contrast, discrimination, for example special procedures for users from a specific country, shall not be allowed. |
**PS-3: Efficiency should be considered when implementing EETS Information Security**

As the EETS will transfer large funds between stakeholders of the system 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 entity which used this infrastructure.

But it will never be possible to achieve perfect security and reliability in an operational system. Rather, the question is how reliable and secure a system has to be to fulfil its needs for the involved stakeholders. 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 efficiency statement calls for this evaluation to be made when developing requirements and security measures.

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

---

**PS-4: EETS Information Security requirements shall be limited to supporting interoperability between toll domains**

EETS is a compound of many separate toll domains that differ in many ways, for example in technical solutions, legal requirements and operational procedures. The toll domains can broadly be categorised into two interoperable types of Toll Contexts; autonomous and DSRC-based.

The different charging technologies of EETS (GNSS, GSM, DSRC as listed in Directive 2004/52/EC) shall be respected, possibly leading to specific security requirements for the two types of toll domains. The common security requirements resulting from this policy shall therefore be limited to 1) the common aspects of the whole of EETS and either 2) of DSRC-systems or of 3) autonomous-based systems.

This limitation in scope represents a pragmatic recognition of the history of the different toll domains and the difficulty of fitting them into a common interoperable framework.

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 member states.

The implementation of a compliance checking solution will have specific requirements on information security which have to be dealt with on an individual basis but with a resulting common interface with its specified procedures on the exchange of compliance checking data. It is up to the specific toll domain to decide on the details of its compliance checking system (e.g. frequency of compliance checks) as long as it utilises the common interface with its specified procedures.

Many of the EETS Information Security aspects that can be said to be truly common to all toll domains are related to the EETS Providers. It is nonetheless important to recognise that there are common security aspects that have a direct impact on the Toll Charger as well. An important example is the protection of keys in DSRC-portals. If a key is compromised due to poor inadequate security in one Toll Chargers system, it directly affects all the other Toll Chargers and at least one Toll Service Provider as well.
3 Detailed policy statements

The detailed policy statements elaborated and expand on the overall security principles to be followed by the organisations of the EETS system. Together with the policy statements of the previous chapter they also form the motivation for the security requirements.

3.1 Overall security objectives

Apart from the high level policy statements, there are also overall security objectives to be taken into account to implement and operate a secure system.

PS-5: EETS Information Security shall limit the consequences of unwanted information security incidents

PS-6: EETS 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-7: Sensitive personal data shall be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data (where following applicable rules and regulations, for example Directive 2006/24/EC, is a minimum).

3.2 Governance and management

For the governance and management of EETS Information Security an organisation or association of stakeholders needs to be established (see Annex B for a discussion on its implementation). This entity shall create and, through needed updates, maintain the EETS Information Security by the means of the 4 documents described in section 1.5. It shall also define the process through which the information security solutions of Toll Chargers and EETS Providers are accepted and the implementation conformance statement to be used by that process.

PS-8: EETS Information Security shall be governed and managed by an EETS Security Group (ESG). ESG will coordinate and support the implementation, maintenance and improvement of all information security management systems specifically covering the EETS and provide the resources required for this commitment.

PS-9: ESG shall maintain the EETS Security Policy (this document)

PS-10: ESG shall maintain the definition of security measures fulfilling the requirements of the EETS Security Policy in an EETS Security Specification. Security Requirements shall be chosen based on a risk and vulnerability evaluation including a simplified risk analysis.

PS-11: ESG shall maintain EETS Security test procedures to enable testing of EETS components and procedures ensuring that they are compliant with the EETS Security Specification. ⁶

PS-12: ESG shall maintain a process for suppliers and EETS Providers specifying how they can get their components and procedures qualified with regards to the EETS Security test procedures. The process shall also apply to additions and modifications to the components and procedures. ⁷

---

⁶ It is not necessary that the ESG develops the specification of security measures. This could be a task for standardisation organisations, Notified Bodies or other certification organisations. The ESG will support such activities.

⁷ It is not necessary that the ESG develops the specification of security measures. This could be a task for standardisation organisations, Notified Bodies or other certification organisations. The ESG will support such activities.
3.3 Trust model

A trust model describes how to establish trusted digital communication between the EETS operators. The prCEN/TS 16439 “Electronic Fee Collection - Security Framework” standard describes a suitable framework for a trust model of an EFC system with the options of establishing initial trust either through peer-to-peer procedures, using a hierarchical solution with a so-called trusted third party or a mix of the two.

A hierarchical solution is commonly used for example in personal computing. Some stakeholders consider the potential financial liabilities in case of a security breach to be much higher in the case of EETS and therefore favour a peer-to-peer solution. Other stakeholders instead emphasise a greater efficiency in data exchange and financial settlements in a multi-party environment.

Nevertheless, peer-to-peer communications to establish initial trust is well suited to be the default solution for EETS as the number of actors involved is relatively limited and most of the parties have long standing business relations (e.g. those between Toll Charger and a Payment Service Provider considering taking on the new role of EETS Provider) or are organized in some way (e.g. ASECAP).

Avoiding the need for establishing a trusted third party also makes the peer-to-peer model organisationally simpler. Under such an arrangement establishment of initial trust is seen to be a step in the process of negotiating contracts between the EETS operators. This analysis is supported by Recommendation 21 of the European Commission’s Toll Committee’s Expert Group 12 and is in line with the chosen solution for the Scandinavian/Austrian interoperability cooperation EasyGo+.

As good arguments for both solutions exist a mixed model should be used for the EETS system, where both approaches are covered.

PS-13: The security measures shall be implemented through a common trust model according to chapter 5 of prCEN/TS 16439 Electronic Fee Collection - Security Framework.

PS-14: 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.

In addition the implementation of the trust model can be harmonised by EETS operators agreeing and conforming to common security requirements, potentially audited by external entities.

3.4 Compliance checking

PS-15: EETS Providers shall provide common compliance checking interfaces and procedures where the correctness and completeness of any specific set of Toll data can be verified (see PS-1: ).

PS-16: EETS Providers shall ensure that data supporting the compliance checking procedures of the Toll Chargers are traceable (see PS-1: ).

3.5 Compliance with standards

PS-17: EETS Information Security shall be based on international and European security standards.

---


9 EasyGo+ is the name of the EasyGo DSRC tolling interoperability partnership (http://easygo.com/en) including Austria.

\(^{10}\) Covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations) and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization’s overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

\(^{11}\) Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.

\(^{12}\) 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.

\(^{13}\) 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 EETS Security Requirements document and in the EETS Security Specification document respectively
Annex A  Interoperability Management regarding EETS security

The original concept of EETS called for a role called the Interoperability Management to provide governance and overarching functionalities that were seen to be common. The emphasis on this role has since been minimised, largely due to the difficulty in creating such an organisation.

However, it is clear that EETS needs coordination and ownership in order to be created and to in order to operate. At least two organisations are foreseen to be needed for EETS Information Security Interoperability Management, the EETS Security Group and the Coordination Group of Notified Bodies.

Figure 3 Foreseen organisation of the EETS Information Security Interoperability Management

EETS Security Group (ESG)

ESG will coordinate and support the implementation, maintenance and improvement of all information security management systems specifically covering the EETS. It will maintain the EETS Security Policy, Requirements, Specification and Test procedures required for the implementation of EETS Information Security in a local toll domain. Annex B presents a discussion on suitable organisation candidates for this role and proposes an association of Toll Chargers advised by EU member states and EETS Providers.

Coordination Group of Notified Bodies

EETS Notified Bodies are one possible way to ensure the conformity to specifications of the interoperability constituents of an EETS Provider (an EETS Provider can then carry on to the stage of suitability for use tests with individual Toll Charger organisations). The need for an organisation that ensures that the same conformity criteria and procedures are used is obvious. This group is currently forming as mandated by article 18 of the EETS decision 2009/750.
Annex B  Establishing the EETS Security Group

The ESG has a central role for the security of the EETS system. It is the owner of the security policy, requirements, specifications and the test procedures. Thereby it defines the demands on the concerned stakeholders and their equipment, interfaces and processes. The question remains how this ESG is organised, i.e. who establishes, operates and controls the ESG and by which legal power does it act.

The following stakeholders have been identified as main candidates for establishing the ESG, by themselves or in combinations:

1. The European Commission
2. Member states of the EU
3. The Toll Chargers in scope of the EETS directive
4. The EETS Providers

Review of alternatives

If the European Commission were to establish the ESG it would benefit from the fact that it has the power to put European wide legislation in place in the form of directives and decisions. As the responsibility to establish EETS has not explicitly been passed to any other organisation the European Commission could also be seen as the one still “owning” the problem. However, the process risks being slow both in a first implementation and in later revisions.

To let ESG be established by the member states of the European Union might represent a pragmatic solution to introduce a governing function with legal powers. But it would require that the European Commission explicitly delegated this responsibility to the members states (which is currently not the case), for example incorporated into the existing remit of the Coordination Group of Notified Bodies.

If the ESG was composed of an association of Toll Chargers it would mean that the negotiations to find a common view on needed requirements and security measures would be carried out directly with the largest stakeholders with direct operational experience. This could potentially be a faster process than if it was carried out in the European Commission. The Toll Chargers also wield the power of implementing their requirements and prescribed security measures through the EETS Domain Statements. The possible motivation for Toll Chargers to want to take on such a role would be two-fold. Firstly, the possibility of creating cost efficient tolling systems of higher quality through harmonisation of requirements. Secondly, it could be seen as a proactive approach to reduce the uncertainty and risk that will continue to exist in a situation with unclear requirements. The quite large number of EETS Domains (approximately 150 today based on the reporting of the member states also including Norway) is a complicating factor as it risks producing a deadlock when trying to reach multi-lateral agreements. This risk could be mitigated by instead involving already existing national or multi-national Toll Charger associations representing the views of its members.

Another possibility is that the ESG consists of an association of EETS Providers. Such an association would wield less power than the other alternatives. It could be made binding under private law but in contracts that themselves would have to be voluntary. The association would consist of a comparably small number of organisations (the EETS providers association AETIS had eight founding members), which are direct competitors on the market that may make negotiations complicated with a risk for deadlocks.
If a Provider loses certification it would then no longer be part of the common security system and would need to negotiate new security measures with the individual Toll Chargers before being able to communicate with them.

The quality label would simplify the establishment of EETS contracts with the Toll Chargers. Toll Chargers might even make possession of the ESG label a condition (but for non-discrimination reasons would also need to accept proof of security compliance by other means - compare to "quality management according to ISO 9000 or equivalent" often required in public call for tenders).

**Proposal – a working group lead by Toll Chargers**

The above exploration of alternatives points to a working group under lead of Toll Chargers but in strong cooperation with all other EETS stakeholders as the most attractive alternative to establish ESG. However, an institution with legally binding powers to prescribe a security with associated requirements and security measures is not foreseen in the EETS legislation. In general it has proven very difficult to establish any function in the EETS Management role, at least those far in excess of jurisdiction of Member States or European Commission.

Instead this annex proposes that the ESG is established as a working group consisting of representatives of Toll Chargers, Member States and EETS Providers (either with each Toll Charger as a full member or with some represented by already existing national or multi-national Toll Charger associations). Participation in this working group would be voluntary but would come with the advantages of greater harmonisation as well as a reduction of uncertainty and risk. The Stockholm Group could take the lead in organising this working group.

This working group would develop and maintain the security policy, organise the dissemination of the results and advocate for the adoption of the results by the Toll Chargers in their EETS domain statements and/or for the adoption of the results by the Member States in local law. Toll Chargers not adopting the proposed EETS Information Security would potentially have a greater freedom in defining their own security framework. However this would be at the cost of the benefits of harmonisation. They would also run the risk of standing isolated from its peers were the European framework to change.

As a working group the ESG cannot enforce the use of its specifications nor impose sanctions on any organisation in case of breaches. The ESG could discuss and evaluate options for promoting the adoption of the EETS Information Security, e.g. by organising the issuing of a quality label, say "ESG approved security". Toll Chargers adhering to the EETS Information Security may ask for this from any EETS Provider in their EETS Domain Statement giving these requirements a considerable weight. In addition a Member State may also adopt the adherence to the EETS Information Security in local law, giving it even a higher weight.

In summary this Annex sketches a possible way how the ESG might be set up by existing stakeholders of the EETS without requiring new legislation.

**Open Issue – allocation of operational duties**

An issue that should benefit from further discussion is the allocation of the operational duties of (certifications and audits associated to the labelling). The ESG could not assume this role directly. Alternatives should be investigated, such as the Coordination Group of Notified Bodies.
**ARENA reports** (available for download at arena-ruc.se)

<table>
<thead>
<tr>
<th>Year</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012:01</td>
<td>EETS Security Policy</td>
</tr>
<tr>
<td>2011:07</td>
<td>Möjlig forskning kring införandeprocesser för ITS</td>
</tr>
<tr>
<td>2011:06</td>
<td>A practical approach to road user charging (summary report)</td>
</tr>
<tr>
<td>2011:05</td>
<td>Vägavgifter i praktiken (sammanfattande slutrapport)</td>
</tr>
<tr>
<td>2011:04</td>
<td>Sammanfattning av pågående forskning inom ARENA</td>
</tr>
<tr>
<td>2011:03</td>
<td>Test Site NetPort – ett försöksområde inom ITS</td>
</tr>
<tr>
<td>2011:02</td>
<td>ARENA 2 Concept</td>
</tr>
<tr>
<td>2011:01</td>
<td>Distansbaserade vägavgifter</td>
</tr>
<tr>
<td>2010:03</td>
<td>ARENA Field Trials – Final report</td>
</tr>
<tr>
<td>2010:02</td>
<td>Hantering av utländska fordon i svenska vägavgiftssystem</td>
</tr>
<tr>
<td>2010:01</td>
<td>Transport policy vs. distance-based road user charging tariff scheme design</td>
</tr>
<tr>
<td>2008:14</td>
<td>Summary of ARENA RUC Seminar 3 – a market-based approach</td>
</tr>
<tr>
<td>2008:13</td>
<td>Published papers within ARENA</td>
</tr>
<tr>
<td>2008:12</td>
<td>ARENA RUC Seminar 1 &amp; 2 – a summary</td>
</tr>
<tr>
<td>2008:11</td>
<td>Kilometerskatt för tunga lastfordon i Sverige – Kostnadsbedömning</td>
</tr>
<tr>
<td>2008:10</td>
<td>ARENA Demo</td>
</tr>
<tr>
<td>2008:09</td>
<td>Kilometerskatt för tunga lastfordon – Legala förutsättningar</td>
</tr>
<tr>
<td>2008:08</td>
<td>A Criteria-Based Approach to Evaluating Road User Charging Systems</td>
</tr>
<tr>
<td>2008:07</td>
<td>Hotanalys för positionsangivelsekedjan</td>
</tr>
<tr>
<td>2008:06</td>
<td>Dimensioning study for Road User Charching</td>
</tr>
<tr>
<td>2008:05</td>
<td>A market based approach to achieve EFC interoperability in Europe</td>
</tr>
<tr>
<td>2008:04</td>
<td>A New Approach to Control in the ARENA concept för HGV kilometre tax in Sweden</td>
</tr>
<tr>
<td>2008:03</td>
<td>A kilometre tax for heavy goods vehicles in Sweden – A conceptual system design. Part 2 Proposal for system design</td>
</tr>
<tr>
<td>2008:02</td>
<td>A kilometre tax for heavy goods vehicles in Sweden – A conceptual system design. Part 1 Requirements and preconditions</td>
</tr>
<tr>
<td>2008:01</td>
<td>Kilometre tax for Heavy Goods Vehicles in Sweden (summary report)</td>
</tr>
<tr>
<td>2008:01</td>
<td>Kilometerskatt för lastbilar – ett konceptförslag (sammanfattande slutrapport)</td>
</tr>
</tbody>
</table>