Security aspects of the EETS

Prepared by

Expert Group 12

Working to support the European Commission
on the work on Directive 2004/52/EC

File name:	EG 12 Final Report v1.0 5apr07.doc
Status:	Final (submitted to DG TREN)
Document nature:	Draft report endorsed by DG TREN
Dissemination level:	EFC Expert Group
Date of issue:	5 April 2007

Contact persons:

Stefan Eisses
Rapp Trans NL, Amsterdam, the Netherlands
Tel: +31 645 69 68 64
Email: stefan.eisses@rapptrans.nl

Philippe Hamet
DG TREN
Tel : +32.2.295.18.61
Fax : +32.2.296.53.72
Email: philippe.hamet@cec.eu.int

CONTENTS

1 OBJECTIVES AND SCOPE

1.1 MOTIVATION AND BACKGROUND

This is the final report of expert group number 12 (EG12) on security aspects of the EETS. At the moment EG12 started its work most of the other expert groups already delivered their final report. As security has a relation with other aspects of the EETS, several other expert groups (notably EG9, EG10 and EG11) as well as CESARE-III already addressed specific security issues[1]. DG TREN felt that this did not guarantee that all security issues important for the EETS were dealt with in a balanced and consistent way.

EG12 was installed to have security as primary focus.

1.2 SCOPE OF WORK

Expert Group 12 received the following scope description from the Commission:

1. make a risk analysis for the EETS on a system level: identify and classify threats and indicate which risks should be dealt with on a European level and which can be left to individual EETS entities or bilateral arrangements
2. define a system-wide security concept including responsibilities of actors, security monitoring concept, system security management, protection level of interfaces
3. propose individual countermeasures/requirements for the most relevant risks that should be dealt with on a European level
4. take into account experience from other sectors, e.g. public transport fare collection.

The Commission further recommended not to focus on (technical) details but on the overall strategic security issues.

1.3 RELATION TO OTHER WORK

Extensive work has been done already that concerns or relates to security for EFC in an interoperable context and the EETS in particular. EG12 tried to build on this work as far as possible. It is noted that while some of the inputs are accepted CEN/ISO standards, many of the relevant documents do not always provide a stable basis as they represent work in progress, did not pass the acceptance/voting process yet, or are not intended for decision making. EG12 has taken a pragmatic approach: use approaches from other material where deemed convenient while indicating that other options exist.

Most important inputs to the work of EG12 are:

- CESARE III, concerning EETS roles, responsibilities and contractual issues, see [CESARE-III].
- A set of standards dealing with security in EFC, in particular: TS 17574, EN 14906, EN 15509.
- [EG 9 Report], concerning architectures for GNSS/CN

[1] See [EG9 Report], [EG10 Report], [EG11 Report] and [CESARE-III].

- [EG 11 Report], concerning the transaction for DSRC-only systems (incl. results from the CARDME and PISTA projects, see [CARDME] and [PISTA]).

A comprehensive list of relevant inputs can be found in ANNEX A.

The outcome of EG12 is intended as input for EC decision making and further elaboration by CEN and ISO workgroups.

1.4 DOCUMENT STRUCTURE

Section 1, this Section, contains objectives, scope and structure of this document.

Section 2, Security Principles and Approach, lists a set of starting points for the EETS security concept as identified by the expert group.

Section 3, Reference Model and Trust Relations, describes the role model and the trust relations that can be derived from it.

Section 4, Observations from other Application Areas, deals with issues from public transport fare collection and credit card payments, which have some characteristics in common with the EETS.

Section 5, High Level Threat Analysis, contains a high level threat analysis for the EETS.

Section 6, Security concept for DSRC-based systems, addresses security services, risks and security implementation issues for DSRC-based systems.

Section 7, Security concept for GNSS/CN based systems, addresses cryptographic concepts and specific security issues for autonomous OBE systems.

Section 8, Specific security issues, addresses remaining issues that are common to DSRC- and GNSS/CN-based systems.

Section 9, Overview of recommendations, provides an overview of all recommendations of the other sections.

The following annexes are attached to this report:

ANNEX A Relevant inputs, contains an overview and short content description of input documents.

ANNEX B References.

ANNEX C Abbreviations.

ANNEX D Expert Group Members, contains the names of all members of the expert group and other contributors.

ANNEX E Entities and Trust Relations in the Cesare III Model contains a detailed trust analysis based on CESARE III.

ANNEX F EMV contains a description of the security concept of EMV (new standard for credit and debit transactions).

ANNEX G High-level risk analysis.

ANNEX H Evaluation CARDMe transaction by Brightsight, contains the results of an independent security review on EG11/CARDMe by Brighsight b.v.

2 SECURITY PRINCIPLES AND APPROACH

2.1 SECURITY PRINCIPLES

In order to arrive at a number of recommendations for the security concept of EETS, EG12 formulated a number of security principles that should drive such

recommendations. They are regarded of vital importance for the political, organisational and financial feasibility of the EETS.

1. The EETS security concept shall adhere to the objectives of the Directive [IO Directive]. In particular, the concept should allow for European interoperability.
2. EETS-entities shall be provided with means to protect their interests against fraud/abuse by other EETS-entities, including the Service User. Trust between EETS-entities is not assumed to exist by itself, but only as a consequence of technical or procedural measures.
3. Fraud or breach of security in the domain of one EETS-entity should have minimum impact on the business of other EETS-entities.
4. EETS-entities are responsible for risk management within their own domain and entitled to make individual choices on security/enforcement measures within the constraints of Principles 1 and 3.
5. Security requirements imposed by EETS on the operations of individual EETS-entities shall be minimal.
6. Requirements for central co-ordination and supervision of EETS security should be minimal.
7. EETS shall be organised in such a way that responsible EETS-entities can protect the privacy of the Service User, i.e. process personal data in accordance with (national legislation based on) Directive 95/46/EC [IO Directive].

It is deemed a legal and political reality that Toll Chargers will remain in control of their business (reflected by Principles 2 and 4). This implies however that Toll Chargers and EETS Providers shall not take any measures that may impose a threat for the business of another entity (Principle 3). In an ideal case the 'technical security concept' enforces this by itself. In practice it is unavoidable that entities also adhere to certain EETS-imposed security requirements on their operations. The security concept shall have the property that such requirements are minimal (Principle 5). This will strengthen trust in the overall security and help acceptance by the stakeholders.

Some form of central management to manage and monitor EETS-security will always be required. The responsibilities and operational size of central security should however be minimal to avoid overhead costs and complex implementation issues (Principle 6).

2.2 GENERIC APPROACH TO SECURITY

EETS security concerns the protection of data stored, handled and transferred between actors and/or entities in EETS environment. The main objective of data protection in the EETS environment is to protect the interests of those relying on the EETS from any harm or damage caused by lack of availability, confidentiality, integrity, non-repudiation and privacy of personal data.

This subsection describes a formal, comprehensive and co-ordinated approach that is recommended for further elaboration of EETS security after basic decisions on the legal and organisational constellation of EETS have been made by the EC. The approach covers the full life cycle of EETS and its components. It goes far beyond the scope of work and resources available for EG 12.

2.2.1 Security in EETS

The model shown in Figure 1 provides a general framework for the planning, design and operation of data protection schemes:

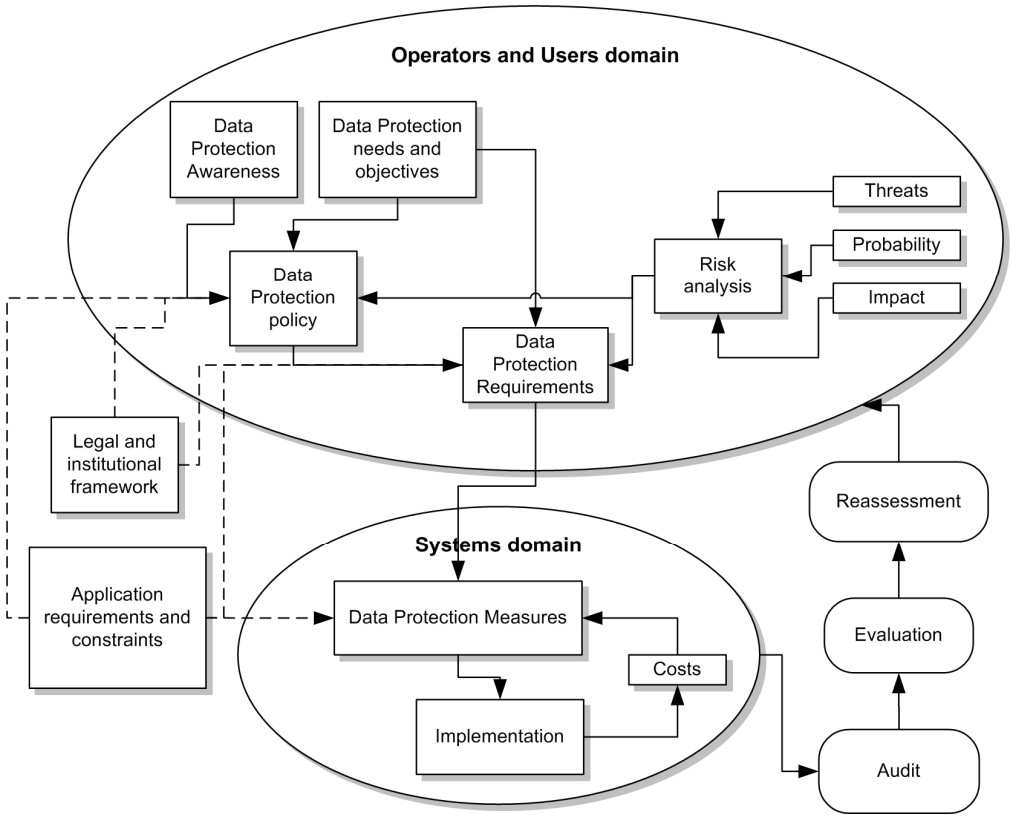

Figure 1: Data Protection Framework (from CEN ISO/TS 17474)

In the Operator and Users domain, a data protection policy is to be defined, based on the overall needs and objectives of the operators and users of the EETS, the results of the risk analysis, and the awareness of the general issues involved in data protection (i.e. data protection principles).

The results of the risk analysis — which consists mainly in an evaluation of the possible threats to the EETS, their probability of occurrence and the possible impact — as well as the data protection policy and the overall needs and objectives, are used to define detailed and precise Data Protection Requirements.

These requirements are in turn used as the basis for the definition of the measures to be applied in the EETS environment to counter the threats or minimise their effect. In the associated process the constraints and additional requirements of the application domain, as well as the costs associated with the measures and their implementation — in accordance with the proportionality principle — are also taken into account when defining the countermeasures.

In addition, the legal and institutional framework, as well as the constraints and other requirements of the application domain need to be considered when establishing the data protection policy and data protection requirements for the system(s).

Finally, in accordance with the reassessment principle, the system in operation is subjected to auditing procedures, resulting in an evaluation and a reassessment of the threats, their probability and their impact.

2.2.2 EETS Security strategy

Figure 2 shows the proposed strategy for the planning, design and operation of a data protection scheme for EETS.

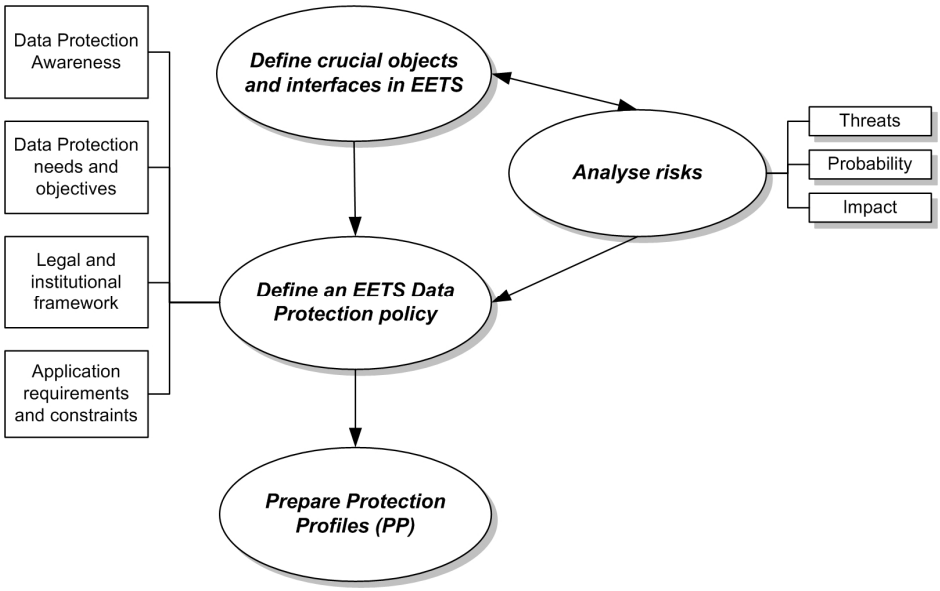

Figure 2: Security strategy (from CEN ISO/TS 17474)

Define crucial objects and interfaces

The EETS system involves several types of operators, EFC equipment, interfaces and users. There are also differences concerning vulnerability which means that there will be different levels and sets of threats, security requirements and security measures. Hence, an important task to start with will be to describe all objects and interfaces in the EETS system in order to point out the most crucial objects and interfaces. This will probably require a high level of risk analyses which is shown as a two-way arrow between the two first tasks in the Figure.

Analyze risks

The next task will be to carry out the risk analysis for the crucial objects and interfaces defined in the previous task. The risk analyses are based on the possible threats to the objects and interfaces, their probability of occurrence and their possible impacts.

An important issue concerning the risk analyses will be the overall operational requirement on a stepwise implementation of the security measures meeting the security objectives. The measures should be defined in a way that enables a rather low level of security from the very start of the system increasing to higher levels as the number of EFC systems is increased and the use of the EETS becomes widespread all over the European countries.

Define an EETS Data Protection Policy

The EETS Data Protection Policy should cover the whole EETS system. However, one possibility is to limit the policy to the crucial objects and interfaces. In any case the Data Protection Policy should take into account:

- Data Protection Awareness amongst users and operators
- Data Protection needs and objectives as defined by the users and operators
- Legal and institutional framework. A major challenge here will be the differences between the European countries.
- EFC application requirements and constraints
- Risk analysis

Define Protection profiles (for crucial objects and interfaces)

By a Protection Profile (PP) is meant a set of security requirements for a category of products or systems which meet specific needs. A typical example would be a PP for the OBEs to be used in EETS and in this case the PP would be an implementation-independent set of security requirements for the OBEs meeting the operators and users needs for security. Protection Profiles (PP) are further defined in ISO/IEC 15408 Evaluation criteria for IT security and ISO/IEC PDTR 15446 Guide for the production of protection profiles and security target.

The main purpose of a PP is to analyse the security environment of a subject and then to specify the requirements meeting the threats being the output of the security environment analysis. The subject studied is called the Target of Evaluation (TOE).

A Protection Profile includes the following elements: Introduction, Target of Evaluation (TOE) Models, Security Environments, Security Objectives, Security Requirements and Rationale. CEN ISO/TS 17474 describes how a protection profile can be worked out using an OBE as an example.

[R 1] An EETS Data Protection Policy should be developed as an anchor for the further elaboration of EETS security.

- The EETS Data Protection Policy shall have its main focus on the On-Board Equipment (OBE) and the interfaces between the OBE and the equipment operated by the Toll Chargers and the EETS Providers.
- The EETS Data Protection Policy shall enable a flexible, multi-level and stepwise implementation of the data protection policy.
- The EETS Data Protection Policy shall lead to EETS Protection Profiles for the OBE and the interfaces between the OBE and the equipment operated by the Toll Chargers and the EETS Providers following the guidelines given in CEN ISO/TS 17474 RTTT – EFC – Guidelines for EFC security protection profiles.

3 REFERENCE MODEL AND TRUST RELATIONS

3.1 REFERENCE MODEL

This Section describes the EETS reference role model used by EG12. As indicated in Figure 3 the model uses four classes of roles. In practice, one organisation may have two or more roles from one or more classes of roles. For instance, very often the same organisation, e.g. a toll collection company, may cover all the different roles in the Provision of the EETS as well as the Charging of the Toll. The EETS reference model is based mainly on the work done by CESARE III with some amendments and additions based on the work done by CEN TC 278 WG 1 EFC SG1 System Architecture and Security.

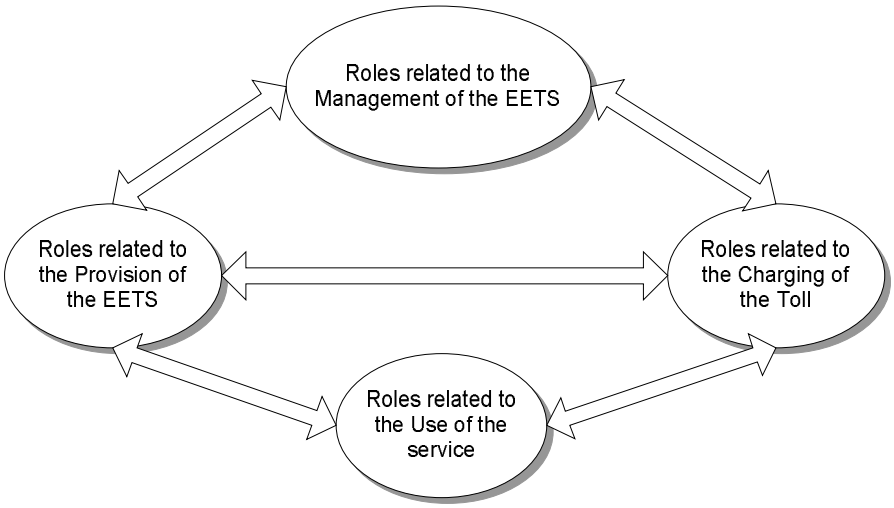

Figure 3: EETS reference model

EETS provisioning

The two main activities of the EETS provisioning cover provision of the OBE and provision of the EETS contract. Of specific interest from a security viewpoint are the following responsibilities:

- Initialising the OBE in a secure way
- Maintaining the functionality of the OBE
- Implementing and adhering to the security and privacy policies for EETS.

Toll Charging

The three main activities of the Toll Charging cover providing the transport service, defining the charging principles, e.g. tariffs, and operating the charging point or area. Of specific interest from a security viewpoint are the following responsibilities:

- Collecting the attributes related to the toll calculation, e.g. characteristics of a vehicle and distance travelled
- Communicating in a secure way with the OBE exchanging information needed for the fee charging
- Communicating in a secure way with actors having roles related to the issuing of the EETS contract, payment means and OBE
- Implementing and adhering to the security and privacy policies for the EETS system.

Use of the service

The main activities of the EETS usage cover driving the vehicle, signing the EETS contract, acquiring and installing the OBE and paying for the use of the service. Of specific interest from a security viewpoint is the responsibility related to the installation of the OBE in those cases where the OBE is connected to other vehicles sensors and/or data stores. Another crucial issue is the storing and protecting of the contractual data and eventually the payment means needed for the fee charging and communicating the data to other actors having roles related to issuing or fee charging.

Management of the EETS

There is also a need for an overall management of the EETS system defining and organising the policy that enables the daily operation of the EETS system involving several different actors. A specific class of roles is identified to manage the EETS system. i.e., defining and maintaining a Set of Rules that, taken together, defines the policy of the EETS system.

The Set of Rules will as a minimum define the following responsibilities related to security:

- Defining the security and privacy policies for the EETS system
- Defining the certification requirements for actors involved and equipment used in the EETS system
- Define and maintain ID-schemes and, if necessary, support the issuing of IDs ensuring unique registration codes for organisations and components as well as unique identifiers or rules for generating unique identifiers for the EETS applications and messages
- Managing disputes.

3.2 TRUST MODEL

The reference model based on CESARE-III is a rather high-level and abstract presentation of the involved entities and arrangements in a conceivable implementation of the EETS. For simplicity and clarity it is preferred that the roles and responsibilities defined by the reference model form the basis of the trust framework for the EETS. This approach assumes there is always an entity that has all EETS Provider (EP) responsibilities for a certain EETS Service User, and that there is always an entity having all responsibilities of the Toll Charger (TC) class of roles for a certain toll domain. EPs and TCs may still outsource various tasks to subcontractors. This will lead to security requirements on subcontractors and the exchanges between them, but this could be regarded as an 'internal affair' under the responsibility of the principal (respective EP or TC).

It is noted that the approach has its risks. Security decisions based on abstract models without sufficient consideration of real-life complexity have repeatedly resulted in weak security or unnecessarily costly security designs. Of course there is no experience with the operations of EETS to learn from. As a second best, current non-EETS compliant toll operations and the detailed (implicit) tasks and responsibilities identified by CESARE III can be used to analyze trust relations. This should lead to an assessment whether the high-level split of responsibilities allows an effective realization of security. A first step has been taken by EG12. The results are to be found in ANNEX E.

The analysis in ANNEX E concludes that in an interoperable EFC system according to CESARE III, there are two distinct trust relation types or trust layers. The organizational trust layer covers the trust relations between legal entities, i.e. natural persons and corporate or public bodies. The second layer involves technical entities, basically OBE, RSE and central systems. The two layers can be separated with interfaces at the operational sub-entities of the major roles.

The layers are complementary and should be analysed in conjunction. To secure the trust relations in the two trust layers, different approaches should be taken. The organizational trust layer will involve legal measures such as placing of contracts and service level agreements. The technical trust layer must use technical means to protect trust relations such as security protocols using cryptography as well as clearly defined interfaces with logging and monitoring. Both should be audited on a regular basis, preferably achieving or confirming certifications.

The analysis suggests that CESARE III does not go into sufficient detail of its entities and their relations from a security perspective. Therefore, additional research by a future EETS Management Board into this area is highly recommended.

[R 2] A future EETS Management Board shall initiate additional research into an adequate trust model for the EETS.

3.3 TRUST RELATIONS

Based on the trust model analysis and the role interaction specified by CESARE[2], it becomes obvious that any protection of trust relationships between entities, technical or organizational, must scale with the number of expected participants. The following key points regarding the scale of the resulting system must be considered:

- CESARE III requires any-to-any relationships between any EETS Provider and any Toll Charger in the participating countries.
- The resulting number of direct links is large and grows over time.
- It should be noted that the developed trust relation diagrams in ANNEX E include only one EETS Provider and one Toll Charger, but already lead to a large number of trust links.

Not every EETS Provider will trust every Toll Charger at the same level. In fact, the different actors and business model combinations suggested by CESARE III clearly indicate a network of non-trusted partners. Participants will initially not trust any other participant; they have to establish trust on a basis of organisational and technical measures to a level that is sufficient for both.

The above facts lead to the following requirements for the model:

- A set of strong standard measures per relation is needed.
- The standard measures must be applicable to individual trust relations.
- A peer-to-peer model is required to prevent extensive organizational overhead.

As to the third point: central or hierarchical models do not allow for such flexibility. They also require that every potential trust relation is known beforehand and catered to, which appears not achievable given the expected complexity of the system. In a peer to peer model however, two participants are able to set up a trust relation independent from the entire remaining system. This approach also allows to chain existing security domains, without redefining trust relations and measures within these domains. This concept is further elaborated in CEN/ISO 20828.

[R 3] The actors in the Cesare III Model should be treated as non-trusted partners with a variety of trust relations that should be secured. The complexity of the relations implies that standard measures should be developed for protecting them. The protection should be based on a peer to peer trust model, so that trust can be established between two actors without requiring a third party.

[2] See CESARE III, D1.1, Page 27, Figure 2

4 OBSERVATIONS FROM OTHER APPLICATION AREAS

4.1 PUBLIC TRANSPORT FARE COLLECTION

The EETS has several similarities with Public Transport Fare Collection (often referred to as Electronic Ticketing or Interoperable Fare Management, 'IFM'). ENV ISO 24014 Public Transport – Interoperable fare management system -- Part 1: Architecture is the result of standardisation work in this area. It has a strong relation with security.

The standard provides a high level risk analysis framework. It defines:

- Types of threat agents types (people or organisations who may initiate an attack on the system)
- Threat targets (system assets that are the subject of an attack)
- The various aspects of public interest that have to be protected, e.g. quality of service, fairness of payment and privacy.

The similarities between EETS and Interoperable Fare Management (IFM) systems include:

- The components held by the user (EETS) and the Customer which will be the OBE for EETS users and Customer Media (CM) for PT customers. They are both in the control of the user/customer and probably the most vulnerable asset in the system.
- The components that communicate with the OBE or CM: RSE (Toll Charger) and initialisation equipment (EETS Provider) for EETS versus MAD (Media Accepting Devices at application retailers, product retailers and PT service providers) in the context of IFM.
- The nature of messages generated and sent in EETS or IFM systems.
- The type of information to be protected (its relation to payment as well as its privacy-sensitive nature).

The security policy of an IFM system should as a minimum reflect the protection of the interests of the public as well as the detection and prevention of loss for the operators. This leads to a set of required properties/tasks contained in the security policy:

- Provide the confidence that information is not made available or disclosed to unauthorised individuals, entities or processes (confidentiality)
- Provide the confidence that information has not been altered or destroyed in an unauthorised manner (information integrity)
- Provide the confidence that ensures that the identity of a subject or resource is the one claimed (Authenticity).
- Provide the confidence of protection against an entity's false denial of having created the content of a message (non-repudiation of creation), e.g. a customer claiming that he has not benefited from a transport service at a specific location and time.
- Provide the confidence of protection against a recipient's false denial of having received the message and recognised the content of the message (non-repudiation of delivery).
- Provide the confidence that each message is unique, e.g. a transaction describing the use of a Product.
- Manage security keys including the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation

and destruction of public or secret keying material in accordance with the Security Policy, at the general security level.

The IFM system architecture defines two important sub-roles being part of the role describing the management of IFM systems: the security manager and the registrar.

Security Manager

The Security Manager is responsible for establishing and the coordination of the Security Policy and:

- certification of Organisations, Application Templates, Components and Product Templates
- auditing of Organisations, Application Templates/Applications, Components and Product Templates/Products
- monitoring the system operation of the security of the IFMS, e.g. key management.

Registrar

The Registrar issues unique registration codes for Organisations, Components, Application Template, Product Templates. The Registrar function also issues unique identifiers or rules for generating unique identifiers for the Applications, Products and messages.

4.2 CREDIT CARD TRANSACTIONS (EMV)

EMV is a relatively new standard – work on EMV started in the mid nineties – defining the use of chip technology for payment cards: debit, credit and cash withdrawal. EMV is named after the initiating organisations Europay, Mastercard and VISA. EMV comprises a gradual global migration from an extensive magnetic-stripe card based infrastructure of millions of payment terminals and several hundreds of millions of payment cards. The rationale for this costly and complex operation is security: steadily increasing losses from card fraud required a higher security level. With chip technology and the cryptographic measures enabled by it, payment cards will become less susceptible to fraud by skimming (copying credit card information). EMV should also lead to more open payment infrastructures.

It is of vital importance that EMV-entities have certainty on the identity of other parties and on the integrity, confidentiality, origin and receipt of a message. This is reflected in the security architecture of which the backbone is a Public Key Infrastructure (PKI). In a PKI asymmetric cryptography is used: the key for encryption is different from the key for decryption. One of the keys, the public key, can be distributed to any party while the other one, the private key, needs to be kept secret by its owner. The receiver of the public key must have certainty that this key indeed belongs to whom it claims to belong to. This problem is usually solved by using certificates. A certificate consists of a public key and related data (including an identifier of the party and a validity period) with a digital signature attached. This digital signature is generated by a trusted third party, the Certification Authority (CA). Any party having a copy of the CA public key can verify all certificates generated by that CA. The important advantages of asymmetric keys in EMV are the following:

- Public keys are easy to distribute as they do not have to be kept secret.
- Entities and terminal equipment do not need to comply to high security standards for storing public keys (as their confidentiality is not important). Consequently asymmetric keys are cost-effective for offline transactions, i.e. without online connection to the issuer.

- Messages signed with private keys can be assigned the property of non-repudiation (origin can't deny that the message was sent), which is by its nature not feasible with symmetric solutions.

Within the EMV scheme, the scheme provider (e.g. VISA) will act as the CA. It creates certificates for each issuer by signing the issuer public keys with the CA public key. The CA public keys are distributed to the payment terminals through the various acquiring banks. If an EMV-card is equipped with asymmetric capabilities, it may contain a card public key certificate (and the corresponding key pair), signed by the issuer using its issuer private key. The terminal may first verify the issuer public key certificate using the CA public key, then the card public key certificate using the issuer public key and finally use the card public key to validate the card's signature over essential data elements presented in the transaction. Symmetric encryption is only used for signing and encrypting data exchanged between the card and the issuer.

The EMV security architecture does not require the card issuer (who is in the end liable if the merchant and acquirer act in compliance with the scheme rules) to share any secrets with other entities. It allows the issuer to remain in full control of his business, while providing the required guarantee of payment to all accepting parties.

Although the scope and scale of EETS and EMV is quite different, there are some interesting similarities. Similarities between EETS and EMV are the large number of largely independent entities between which interactions are possible. A Toll Charger may have to interact with service users having a contract and equipment from some remote EETS Provider, and trust that he will receive payment – just as a merchant and his acquiring bank have to accept payments with a card from an unknown issuer claiming to be member of the same scheme. In both cases there is no a priori trust existing between any set of actors. Trust is based on the guarantees and liabilities defined by the scheme, and the set of technical and operational measures supporting it.

Without neglecting the differences in scope and context, EMV may be a source of inspiration for EETS in the following respects:

- Issuers remain in control of their security and do have to not share secret keys with any other party. This provides the flexibility needed in a global context with a large number of entities.
- The scheme owner plays an important role as CA, for the definition of standards, arbitration, accreditation of certification bodies and admission and dismissal of new members. It does not control the operational security of payment transactions.
- Although the operational rules vary between EMV schemes, differ between issuers and even depend on payment environment, merchants/acquirers always have a guarantee of payment if they follow the applicable rules.

5 HIGH LEVEL THREAT ANALYSIS FOR EETS

5.1 INTRODUCTION

This threat analysis is based on the CESARE III based reference model as described in 3.1.

The threat analysis is performed at a high level of abstraction, to keep away from implementation aspects that are yet unknown and that will strongly influence the way in which certain attacks can be realised, their likelihood, resulting possible damage and possible countermeasures. Threats are described in a way that they are largely independent of a specific system concept.

Some threats do not need to be catered for on an EETS level, but can be left to the responsibility of individual actors (EPs or TCs).

In this section the most important results are presented. The complete analysis is included as ANNEX G.

5.2 RISKS IN THE EP AND SU DOMAIN

Nr	Description of damage	Possible attacks causing the damage (not exhaustive)	To be addressed in EETS definition ?	Possible measures (not exhaustive)	Comments
EP3	Wrong vehicle characteristics declared (characteristics in OBE do not match vehicle in which it is used) – loss of income or enforcement	• EP Personnel enters erroneous data in personalisation process. • OBE used in wrong vehicle. • OBE memory altered without authorisation	Yes	To be implemented by EP • Entry of vehicle characteristics in OBE only by authorised personnel. • Entry and modification of OBE data only possible with authorised equipment. • EP data entry process subject to certification and audit.	One Liable for Toll will always remain end responsible to declare the right vehicle characteristics. The EP is however responsible for entry of vehicle characteristics and their integrity.
EP5	Unauthorised disclosure or use of customer/travel-related data – privacy infringement	Interception of declaration data from OBE or stored data at EP premises.	No	• Encryption of personal data exchanged over open networks. • Separation of processing domains. • No more data kept than necessary for the purpose – and no longer than necessary. • Access to personal data only by authorised personnel on need-to-know basis. • Access to personal data subject to audit trail.	The proper handling of personal data is the responsibility of the entity who is to be seen as the 'controller' of these data, as defined in 95/46/EC. Each controller will have to comply with applicable national legislation on processing of personal data. EP's will obviously qualify as controllers of personal data.
EP6	Non-available or incorrect raw data from OBE sensors – loss of income to TC.	E.g. GPS shielding or spoofing. Sabotage of sensors or modification of data from sensors.	Partly	• EETS OBE requirements should include detective measures against manipulation of sensors. • Enforcement / spot check policy is responsibility of TC – but the mechanisms are to be facilitated by EP / OBE.	This applies to autonomous OBE concepts (GNSS/CN) only.
EP7	Declaration of incorrect data by the OBE – loss of income, complaints from SU or TCs	Modification of software or stored data in OBE, modification of OBE declaration data or toll context data	Partly	• EETS OBE requirements shall include measures to maintain integrity and authenticity of all data and software.	
EP8	OBE malfunction because toll context	Communication of toll context data is	No / Partly	• Basically this is a matter between EP and his	In the end, the one liable for toll is

	data not available or incorrect – loss of income or enforcement of 'honest user'	obstructed, modified or made unavailable		Contract Holder, yet: • Minimum service levels should be part of EETS requirements on EPs	responsible for an accurate declaration / functioning equipment.
EP9A	False OBE – unjustified charges to existing SU or loss of income	OBE/SAM cloned, or fake OBE used	Yes	• EETS OBE requirements shall include measures to maintain integrity, confidentiality and authenticity of data and software. • Blacklisting.	
EP9B	Use of stolen OBE – unjustified charges to EETS contract holder.	OBE/SAM stolen and used by other person.	Partly	• Blacklisting. • A periodic on-line reactivation mechanism can be used to make an OBE dysfunctional within a certain time after reported loss.	Procedures to report OBE loss to EP can be left to individual EPs. A global rule on dealing with blacklists by EPs/TCs is important.
EP12	Secret keys compromised – may lead to loss of income to Toll Chargers and or EPs	Several types of attack on devices storing keys, encrypted text exchanged and in generation process.	Partly	• Crypto-concept should require no or minimum central co-ordination. • Avoid sharing of secret keys between parties. • Storage of secret/private keys only in protected environment. • Asymmetric crypto where possible. • Measures to limit damage and recover after compromise of keys.	

5.3 RISKS IN THE TC DOMAIN

Nr	Description of threat and damage	Possible causes (not exhaustive)	To be addressed in EETS definition ?	Possible measures (not exhaustive)	Comments
TC1	Fees cannot be collected from EP – loss of income	EP bankrupt	Yes	• Certification requirements on EPs should include financial stability.	This issue is not related to security, but has to be addressed.
TC2	No toll declarations received from OBE or EP – loss of income	Sabotage of communication, OBE or RSE	Partly	• EP Backoffice charging process subject to certification and audit. • EETS OBE requirements should include measures to maintain integrity of data and software. Data may be delayed but not lost before arriving correctly in backoffice.	TC enforcement should cater for the situation that a correctly operating OBE may not send an OBE declaration at a later time.
TC3	No/wrong recording of movement data – loss	Local GNSS jamming or	Partly	• EETS OBE requirements should include detective	This applies to GNSS/CN tolling.

	of income and/or enforcement of honest users	spoofing.		measures against manipulation of sensors or anomalous sensor input. • EETS OBE requirements may include additional sensors for dead-reckoning / detecting erroneous GNSS input.	

5.4 RISKS IN THE IM DOMAIN

Nr	Description of threat and damage	Possible causes (not exhaustive)	To be addressed in EETS definition ?	Possible measures (not exhaustive)	Comments
IM1	Loss of income for Toll Chargers – EETS Provider bankrupt	• Insufficient requirements on EETS Providers.	Yes	• Adequate certification and financial auditing of EPs.	
IM3	Erroneous OBE declarations – loss of income for TCs, complaints from SUs, or enforcement of honest users	EETS certified OBE incapable of fulfilling TC requirements (insufficient accuracy or functionality) as a result of insufficient or erroneous certification.	Yes	• EETS OBE requirements shall include accuracy/performance aspects to assert that required accuracy for a variety of toll environments is sufficient.	This is primarily an issue for the respective EP but listed here as it is caused by deficiencies of the EETS certification.

5.5 CONCLUSIONS

The threat analysis leads to the following recommendations:

[R 4] The EETS OBE shall be subject to type approval procedures, comprising security features as well as accuracy and availability.

[R 5] In GNSS/CN based systems, the correctness of toll declarations depends on the complete data processing by the EETS provider. Therefore, the related operations of the EETS Provider shall be subject to certification and audit procedures.

[R 6] The EETS will involve handling of data that are to be regarded as personal data by the definition of 95/46/EC. The individual entity controlling such data will have to comply with national privacy legislation derived from 95/46/EC. A central coordination on EETS/EMB level is not required.

6 SECURITY CONCEPT FOR DSRC-BASED SYSTEMS

6.1 INTRODUCTION

European standardisation and harmonisation of DSRC-based EFC has been a difficult and lengthy process but has resulted in mostly similar technology across Europe and has made interoperability a feasible step.

It is therefore logical and straightforward to build the EETS for DSRC-systems as much as possible on existing application standards, on which products and operational systems are based. Major changes could easily lead to significant development costs for the industry, costs of upgrading RSE for existing Toll Chargers and new efforts for standardisation.

Expert Group 11 (EG11) has defined the EETS transaction for charging systems based on DSRC technology. Based on the background presented above, EG11 has followed a route close to existing implementations and standards for the EETS.

It should be noted that the EETS creates a new dimension in DSRC-based tolling. Solutions that perfectly fit a local situation or interoperability with a few neighbouring operators, are not by definition suitable for the EETS. A new environment requires a new assessment.

EG12 tried to evaluate EG11 recommendations from a security perspective. Within EG11 a number of measures are described or implied, but without defining an overarching security concept and management. It was therefore deemed necessary to suggest how these measures should be implemented, depending on characteristics of a local toll system. Attention is also paid to a sensible staged introduction of the measures.

It is impossible to say whether the security measures implied by EG11 are sufficient or not as this depends on the risks entities are willing to take, the subjective assessment of the magnitude of a risk versus the cost of mitigating the risk effectively. The self-assigned task of EG12 is to pin-point the residual risks, clearly indicate which party would be responsible, provide a view on a balanced set of measures and indicate possible alternatives.

An aspect to consider is the evolution of technology. Starting from the optimistic assumption that the EETS will be formalised by the end of 2007, it will start to become effective by the end of 2010 for freight and only by the end of 2012 for passenger cars. The basic OBE security concept will by then be 15 years old. In general, the strength of IT-security erodes over time due to the increase of processing power, lower hardware costs, and the development and spread of know-how. 15 years is a long period in IT-development. Assuming that the concept currently on the table would suffice for the first 5 years, it would make sense to develop a strategy for the second generation and implied migration issues.

Subsection 6.2 describes the current situation of DSRC EFC. The next subsections describe the security services offered by EG11 (6.3) and recommendations how these services should be implemented (6.4). Some attention is paid to the issue of access credentials in 6.5. Subsection 0 lists the so-called ‘residual risks’ of the suggested concept and 6.7 presents some thoughts on a future successor of the current DSRC transaction.

6.2 CURRENT SITUATION

DSRC technology has widely been introduced in national charging systems in order to offer users a convenient electronic service as an alternative to manual payment. Due to the initially strictly local context of these systems, security measures usually have been of a non-cryptographic nature.

Most European DSRC systems currently in operation do not rely on cryptographic security measures to protect against fraud. Nevertheless fraud by manipulation of DSRC equipment or of DSRC transactions is practically unknown. In current charging systems loss of revenue rather stems from user debts that cannot be collected, from fraudulent credits cards (in manual lanes), und users declaring the wrong vehicle class (free flow systems).

Today, system security of DSRC systems mostly rests on non-cryptographic measures, namely:

- transactions are central account or token-based, hence a break of security only leads to free rides but not to fraudsters being able to directly generate income
- users are mostly local and 'known' to the operators
- DSRC technology used was partly proprietary and for users not available on the open market
- the scale of systems is comparatively small, not making a business case for organised fraud

It is now generally accepted that with the advent of the EETS, system security has to be substantially increased. Reasons are that

- the market for fraud has increased since by breaking one type of OBE the whole of Europe can be attacked
- DSRC technology and DSRC transactions are fully standardised. Equipment is becoming available from many sources
- in the EETS roles are split between different entities. Responsibility, liability and traceability cannot be handled without strong system wide security mechanisms

Discussions around the introduction of the EETS have shown that there is no agreed view among EETS participants on the risks and on level of security required. Toll Chargers are reluctant to invest in costly security measures when the threat is unclear.

In order to operate DSRC systems in a cost effective way, an adaptive approach to security is required. An overly secure system is not cost effective, as is a too insecure system where too much revenue is lost due to fraud. In practice, the level of fraud that a Toll Charger can accept is rather low, since trust of the users in the security of the system is of high importance for successful operations and is not risked light-heartedly.

Ideally, system security would continuously be adapted to the threat, always being sufficiently ahead of the threats such that the risk of sudden breaks of system security are minimised. The following proposes an adaptive approach to security based on the tools available in DSRC charging standards today (i.e. the recommendations of EG11 and their formalisation in the standard EN 15509 on an "Interoperability Application Profile for DSRC").

6.3 SECURITY SERVICES FORESEEN BY EG11

The DSRC transaction defined by EG 11 foresees a number of security services but does not go into great detail as how to make use of them. This chapter provides for an overview of the security services foreseen by EG11, while the next chapter proposes a cost effective way of how to operate these services in the EETS.

Payment Authentication to the EETS Provider

EETS Providers need a proof of passage for OBE they have issued. As soon as a proof of passage is given by the Toll Charger, the EETS Provider has the obligation to pay.

For this proof the specification of EG11 foresees a dynamic Authenticator that is calculated by the OBE using a challenge-response mechanism and diversified keys. The Dynamic Authenticator is transferred in a GET_STAMPED command (as defined in the basic EFC application standard EN 14906). This mechanism is used in many European EFC transactions. The EETS Provider calculates the individual key for each OBE (to be precise: for each PAN) from a set of master keys. The individual keys are entered into the OBE by the EETS Provider upon personalisation and shall not be known by any other party. The EETS Provider is the only party in possession of the Master Keys.

When an OBE passes under a gantry, the Toll Charger sends a GET_STAMPED command for the attribute PaymentMeans, and he will receive the attribute together with the Authenticator. There is no need for the RSE of the Toll Charger to conduct any cryptographic calculation since the Authenticator is produced by the OBE. The Toll Charger sends the Authenticator as part of his claim to the EETS Provider. The EETS Provider validates the Authenticator. A valid Authenticator proves that an OBE of the EETS Provider has indeed passed a gantry of the Toll Charger and hence the EETS Provider has the obligation to reimburse the claim of the Toll Charger. The Payment Authenticator is essential for the operation of the CESARE model.

OBE Authentication to the RSE

The Toll Charger is not in possession of the keys of the EETS Provider. Hence, he is not able to check the validity of the transaction before asking the EETS Provider for authentication. For the Toll Charger to gain confidence in the transaction, he may optionally conduct a second GET_STAMPED, using a different key identifier, in order to obtain an Authenticator that he can check either at transaction time in the beacon or later in the back office. The Authenticator is calculated from keys common to all Toll Chargers using this mechanism (for a given EETS Provider).

It has to be noted that this security feature is proposed to be an optional element of the EETS and is left to the discretion of the Toll Charger. The Toll Charger can decide on the level of confidence he wants to achieve. In addition not all Toll Chargers are currently able to perform cryptographic operations on the road-side and only a small number of road-side installations can store the required Master Keys safely.

Transaction Counter

The Transaction Counter is a value stored in the OBE and incremented by the RSE in each charging transaction. The EETS Provider will be able to assemble the data related to a sequence of transactions for any OBE and check that the Transaction Counter is correctly incremented. Numbers out of order indicate potential security breaches that might need to be investigated.

EG 11 recommends to use the Transaction Counter as it is a very simple and easy to implement mechanism that offers an excellent quality check of the EETS since lost or double transactions can be identified. In addition it is very useful to identify a massive breach of system security, namely the appearance of cloned OBE.

Receipt Authenticator

Toll Chargers in closed tolling systems use the receipts written into the OBE on entry as an entry ticket which is read out on exit of the motorway. If users are able to forge or change entry tickets they can fraud the system.

The Receipt Authenticator is calculated by one beacon, written into the OBE, then carried by the OBE to the next beacon, read out again and checked. Toll Chargers are free whether or not to use this mechanism, and which algorithms to apply for its calculation.

With this security service Toll Chargers can both protect receipts from being manipulated and make sure that an OBE does not change identity between beacons (which might happen with completely falsified OBE that this way disables the blacklisting mechanism).

6.4 IMPLEMENTATION OF EG11

6.4.1 Cost-effective security management

Expert Group 11 has identified a number of security threats and has proposed a list of countermeasures. Clearly the highest risks for Toll Chargers not receiving payment or for EETS Providers not being able to charge the users is from users attacking the OBE, i.e. either manipulating OBE data or cloning OBE.

In the EETS, responsibility for the OBE rests with the EETS Provider. The EETS Provider specifies and orders OBE, personalises the units with user, vehicle and account data and then issues them to the Service Users. The EETS Provider is also responsible to store the required security keys in the OBE and to distribute them to the Toll Chargers.

Each OBE carries two sets of diversified keys:

- Four diversified Payment Authentication keys. At transaction time the road side sends a (pseudo-)random challenge which the OBE uses together with the PAN to create an authenticator and send it to the road side. The master keys are not distributed and, hence, the authenticator can only be checked by the EETS Provider issuing the PAN.
- Four diversified OBE Authentication keys. The master keys are distributed to all Toll Chargers which enables them to check whether passing OBE is genuine.

There are four keys each in a set in order to allow EETS Providers to migrate to the next key generation when the first generation has been in use for some time and the risk has increased that the key is broken.

6.4.2 Security Management by the EETS Provider

The following outlines an approach how EETS Providers might manage their security.

OBE procurement

The EETS Provider is responsible for the OBE. When OBE issued by an EETS Provider proves to be vulnerable in operation, the EETS Provider risks to have to pay Toll Chargers for transactions that have been performed with cloned or manipulated OBE that carry a false PAN (a PAN that has not been issued) or the copied PAN of a real user. In both cases the EETS Provider will not be able to obtain the fee from a user. Note that according to the basic rules of the EETS, EETS Providers unconditionally have to pay Toll Chargers for transactions that have valid authenticators.

Hence, upon procurement EETS Providers have to make sure that the OBE has a high level of protection. In particular:

- OBE should be tested that under all circumstances data that are defined as read-only on the DSRC cannot be changed by the user (especially fixed classification data and the PAN).
- The OBE personalisation interface must be highly protected. Note that neither the DSRC standards nor specifications of the EETS make prescriptions regarding the personalisation interface. The EETS Provider has the sole responsibility to define the protection level of this interface. There is also a conflict of interests as on the one hand the interface needs to be highly protected and on the other hand there needs to be easy access in order to enable flexible distribution and simple initialisation by retailing outlets acting on behalf of the EETS Provider.
- The keys should be safely stored in the OBE, ideally in a secure application module, or equivalent (some microprocessors have for that purpose a reserved memory area with special access conditions realised in hardware). It has to be noted that DSRC security for performance reasons (high speed requirement, power limitation due to battery) uses the DES algorithm which is no longer accepted as safe against attack given reasonable time and processing power. Nevertheless attacks on the link itself are not very likely since the Authenticators exchanged are truncated from an eight byte DES result to a four byte Authenticator, making a backwards calculation difficult. More likely are attacks on the OBE to obtain the keys. Hence, safe storage of the keys is of utmost importance. (Note that the keys in the OBE are diversified using the PAN. If an OBE key is hacked, only this OBE can be cloned, which will in short time be blacklisted. There is only a very small risk that the Master Keys can be derived from the triple-DES diversified keys).
- Ideally the OBE should have “fast response”, i.e. it should be able to answer a request by the road side in the private uplink window allocated with the request. This gives the OBE about 400 microseconds to calculate the response, including the DES security calculations. This is only possible with dedicated hardware where the DES hardware is on the same chip as the general DSRC protocol processing. Calculation of DES in software leads to a slow response, and also calculation in a dedicated security chip costs too much time due to the communication time required between the chips. Accepting only “fast response” makes sure that OBE are not easily cloned in software or in ready-made hardware. Only mainstream DSRC manufactures have the chipsets that are able to produce a “fast response”. Industry sells only to known parties and only in large quantities, making it very difficult for fraudsters to obtain suitable equipment in an economic way. Every EETS Provider should contractually make sure that over time Toll Chargers do not accept “slow response” OBE for his contracts.
  Requiring “fast response” is not an ultimate security measure since technology will in some time outpace such hard-ware related mechanisms. But for the time being, the mechanism is a cost effective and simple way to make cloning OBE much harder and costly.

[R 7]	The EETS Provider is responsible for protection of the personalisation interface. Certification of OBE for the EETS shall include requirements and tests regarding this protection.
[R 8]	Certification of OBE shall require and test for safe storage of keys.

Check on incoming transactions

EETS Providers have to check incoming transactions for consistency and breaches of security. As a minimum EETS Providers should as quickly as possible check for every transaction:

- Existence of the PAN. A PAN that has not been issued is a reason for alarm meaning that either OBE data have been manipulated or false OBE is in circulation.
- Correctness of the Payment Authenticator. A correct PAN with correct corresponding Payment Authenticator triggers the payment obligation of the EETS Provider. Hence, the Payment Authenticator can be considered as the core security element for the EETS Provider. Its calculation does not require the distribution of Master Keys. It is virtually impossible to obtain the Master Keys from the individual keys stored in OBE. The level of security provided is quite strong and under full control of the EETS Provider.
- Check transaction counter for correct increment over time. If a transaction at a later time and date has a lower counter value than a previous transaction, the EETS Provider should investigate possible causes. Inconsistent counter values are an indication that OBE has been cloned. Ultimately, the transaction counter is the only means to find out whether cloning has occurred. Missing counter values are not alarming and only mean that transactions are missing and will most likely be received later. Counter values out of order, however, are alarming since cloning is the most likely reason.
- In order to have a high probability of fraudsters being stopped, these checks should be executed and fraudulent PANs be black-listed as quickly as possible.

[R 9]	EETS Providers shall check PAN, Payment Authenticator and Transaction Counter for every transaction as quickly as possible. Security Processes of the EETS Provider shall be part of the approval process.

Key management

EETS Providers have to make sure that the master keys are safely stored and handled. Master keys must at all times be under total control of the EETS Provider.

- Key diversification and entry into OBE has to occur in a protected environment under control of the EETS Provider. Keys should not be handed to manufacturers for implementation during production, unless when handled in a certified environment.
- Keys for test purposes have to be foreseen (e.g. for certification) and have to be different from operational keys. Those can be made public and are the same for all EETS Providers.
- Keys for OBE Authenticators have to be distributed to all Toll Chargers that want to use them. EETS Providers have to make sure that only Toll Chargers that have a certified safe storage of the OBE Authentication keys at roadside or in the central system will receive the OBE Authentication master keys.
- It is a common misunderstanding that all Toll Chargers share the same OBE Authenticator keys (such that there is only one set of OBE Authentication master keys for the whole EETS system). In fact, there are as many OBE authentication key sets as there are EETS Providers. Every EETS Provider will generate four

Master Keys for OBE Authentication and distribute them (one by one, see below) to all eligible Toll Chargers.

- EETS Providers should actively manage the use of the four OBE Authentication keys and only distribute one key generation at a time. Depending on security strategy the EETS Provider may decide to give different Toll Chargers different master key generations, e.g. according to the security profile of the Toll Charger (say generation 1 to all Toll Chargers, generation 2 only to those with secure storage in the central system and without distribution to the roadside, generation 3 to those with 'safe storage' on the roadside, …)
- The downside of this approach is that it reduces the possibility to go to the next key generation in case one is compromised. It has to be said, though, that as soon as key generations become compromised, moving to the next generation is a very short term solution anyway, since obviously system security as a whole has become weak and fundamentally new security measures have to be foreseen.

[R 10]	For all keys used in the EETS a set of system-wide known test keys shall be foreseen.
[R 11]	EETS Providers should only deliver OBE Authentication Master Keys to Toll Chargers that have a certified secure key storage at the roadside or in the central system.
[R 12]	The Master Keys distributed to Toll Chargers for OBE Authentication on the DSRC link shall be controlled by each EETS Provider and be different from one EETS Provider to the other.
[R 13]	The EETS Provider is responsible for key distribution and for the distribution strategy. No central body is required for key management.

6.4.3 Security Management by the Toll Charger

Toll Chargers enjoy a payment obligation of the EETS Provider if they can produce a valid transaction for a PAN that is not blacklisted. Toll Chargers will normally check several things in a transaction:

- that the PAN and/or OBE is not blacklisted. If the PAN or OBE is blacklisted the Toll Charger will not be reimbursed by the EETS Provider. In this case he has to treat the user as if he were non-equipped and apply the local enforcement procedures.
- that the OBE communicates the right classification information, especially that trailers are declared correctly (only in systems that do not measure class but use declared classification). In case classification information is deemed incorrect, local exception handling processes are triggered.
- in several system it is checked that the OBE is in the right vehicle, i.e. that the declared licence plate and the visible licence plate match.

After these checks the Toll Charger will in an interoperable environment still not be sure whether the EETS Provider will reimburse him since there is no guarantee that the PAN and the associated Payment Authenticator are genuine and correct. For this purpose the DSRC transaction specified by EG11 for the EETS foresees the OBE Authenticator. Every

OBE carries an individual, diversified key (or actually set of four key generations) and calculates with it an OBE Authenticator if requested to do so during the transaction. Every EETS Provider distributes the associated master keys to the Toll Chargers.

Toll Chargers can store the OBE Authentication master keys at roadside and check the authenticity of the transaction at transaction time in order to decide whether enforcement has to be triggered or not. Currently very few roadside equipment is fit to do so. Especially no safe storage for keys is foreseen in most beacons. It has to be noted that potentially hundreds of keys have to be safely stored since there is a least one OBE authentication master key per EETS Provider.

Alternatively OBE Authenticators could be checked by Toll Chargers in the central system, avoiding storage of keys and fast cryptographic calculations at the roadside. OBE with failed authentication are then blacklisted immediately. This is especially a cost effective solution to increase system security from where it now stands without large investments.

It has to be noted that OBE Authentication alone cannot ultimately guarantee that fraudulent devices are always identified. The master keys for OBE Authentication are widely distributed and stored in many roadside systems. Since these are in an uncontrolled environment they cannot be considered safe from attack, even when key storage is reasonably safe (which it rarely is today). Only an adapted use of all security tools provided by the EETS environment can lead to a system that is protected in a cost effective way over several years of operation.

A severe attack on the business of the Toll Charger takes place when OBE appear in his system that produce a structurally valid PAN from a known EETS Provider where the OBE Authentication tests correctly, and hence the transaction looks OK to the Toll Charger, but nevertheless the EETS Provider refuses to pay since either the PAN has not been issued to a user or the Payment Authentication fails. Both facts cannot be known by the Toll Charger beforehand.

The best way to safeguard against this is to obtain on-line authorisation by the EETS Provider. This means that the Toll Charger sends the DSRC transaction to the EETS Provider for processing and asks for an immediate response whether or not the EETS Provider accepts and will reimburse the transaction. Only when the EETS Provider authorises the transaction the Toll Charger accepts the transaction as a valid payment by the user. Otherwise enforcement procedures come into force.

Naturally this approach comes at some cost and is also only possible when there is sufficient time for online authentication with the concerned EETS Provider, e.g. in closed tolling systems between entry and exit, or in systems with barrier as long as the user is stopped by the barrier. At large toll facilities such an approach might quite readily be feasible, but for beacons in remote areas with a low data rate, probably even dial-in connection to the central system, this is out of the question. Also for free-flow systems the typical available transaction time (about 50-100 ms) will not be sufficient for an online authentication.

In these cases, Toll Chargers should ask for authentication as quickly as possible, in order to be able to eventually blacklist the PAN quickly and enforce the OBE at the next possible opportunity. Note that in cleverly designed fraudulent equipment, the OBE will change identity from beacon to beacon. Toll Chargers can to an extent safeguard against this by using the Receipt Authenticator, where information is carried in the receipt stored in the OBE from one beacon to the next.

Ultimately one has to recognise that payment security is under control of the EETS Provider, and hence the EETS Provider is the only entity that can authorise a transaction for payment. Toll Chargers best develop a strategy to come over time as close as possible to an online-authentication.

A phased approach could be followed:

Phase 1:

The Toll Charger is not able to safely store keys at road side nor to request online authorisation.

The Toll Chargers readies and certifies his central system for safe key handling and storage. He is now entitled to receive OBE Authentication keys from the EETS Provider and uses them to check for OBE authenticity offline. Non-authentic OBE is blacklisted.

Phase 2:

As part of the normal system maintenance and renewal road side software is upgraded. The Toll Charger implements into the roadside equipment the ability to accept only OBE with “fast response” for selected EETS Providers, thus safeguarding against OBE software replicas.

The Toll Charger also upgrades roadside software to make use of the Receipt Authenticator mechanism, thus safeguarding against OBE changing identities between beacons and against receipts being manipulated (e.g. manipulated entry tickets in closed systems).

Phase 3:

As beacons have to be exchanged as part of technical lifecycle, the new beacons are able to store hundreds of keys in certified secure modules. At these beacons the Toll Charger begins to online verify the OBE Authenticator.

Phase 4:

The Toll Charger step by step readies the system for on-line authentication with the EETS Provider wherever possible. In a free-flow system, e.g., enforcement pictures might be kept until online verification is available (if allowed by the national legislation). In a classical barrier-controlled closed system, e.g. the Toll Charger starts to authenticate with the EETS Provider first between entry and exit and then during the time the vehicle is stopped at the barrier.

Following this phased approach the ideal situation of online authentication is gradually approached for large parts of the system. For fraudsters there is less and less room, and no financial business case.

With online authentication Toll Chargers will always know when OBE is good for payment and when not. System security is then fully where it should be, namely in the hands of the EETS Provider. The EETS Provider has total control over system security. He will monitor the system for signs of security problems and adapt his strategy accordingly. With every new generation of OBE the EETS Provider can find improved ways to calculate the OBE authenticator. There are no time constraints as long as the OBE can calculate a new authenticator during the passage from one beacon to the next. As long as the authenticator remains 4 bytes long, there is no need to change anything on roadside. Only when this size becomes limiting, as might be the case when using asymmetric cryptography, the currently foreseen security elements in the EETS DSRC transaction are no longer sufficient and a new transaction has to be defined.

[R 14]	Toll Chargers should develop a phased security strategy that allows fast migration to higher protection levels as the need arises.
[R 15]	EETS Providers and Toll Chargers shall cooperatively step-by-step prepare for online authorisation of OBE. As part of the preparation for this, the necessary data exchange protocols and processes need to be defined.

6.5 Access Credentials

Access Credentials are dynamically generated passwords that allow access to OBE data only to parties that have the proper authorisation, i.e. the right keys. Access Credentials are used as a measure against:

- privacy infringements: Only authorised parties can have access to private user data (such as the Payment Means or the receipts that identify the trip made).
- unauthorised use of OBE: When no Access Credentials are required to access OBE data, parties that are not part of the contractual EETS arrangements (other countries or service providers) may make use of the EETS OBE, e.g. for identification purposes.

EG 11 did consider Access Credentials as being important security elements. Unfortunately, RSE that follows the CESARE/PISTA transaction specification have no possibility to handle Access Credentials. This would mean that such equipment would not be able to access OBE data if Access Credentials were required by the EETS.

Hence EG 11 has proposed not to use Access Credentials in the EETS DSRC transaction for the time being, and at the same time encouraged Toll Chargers to develop a migration strategy to enable a later introduction.

Whether or not to use Access Credentials is ultimately a decision of the EETS Provider. EETS Providers carry the risk of unauthorised use and will also have to respond to privacy infringements. As soon as a majority of Toll Chargers can support Access Credentials, EETS Providers should issue OBE that require them.

It should be noted that migration towards Access Credentials can potentially be done in comparatively short time, since it mostly requires software updates to RSE. Safe storage of Access Credentials master keys in the road side equipment is not of primary importance, at least not in the beginning. Access Credentials master keys are not relevant from a security point of view and are not likely targets for attack. Access Credentials mostly serve to make unauthorised access difficult.

[R 16]	It is recommended to move towards the use of Access Credentials as quickly as possible. EETS Providers have to decide when to issue OBE that require Access Credentials.

6.6 Residual Risks of the Concept

The security management concept drafted above is based on the measures offered by current equipment. Some residual risks remain and need to be assessed on a continuous basis. The following items are simple observations that need to be kept in mind.

- It is inherent in the CESARE model that Toll Chargers have no guarantee of payment until authorisation of the payment by the EETS Provider. Over time, online Authorisation needs to be implemented wherever possible, but situations will remain where this is not feasible.

- When keys of an OBE model become compromised it is very difficult to exchange widely distributed equipment in short time. The concept of key generations will not win a lot of time to accomplish this.
- Keys distributed in equipment that is accessible to the public (OBE, but also RSE) cannot be considered safe over longer periods of time.

[R 17] The EETS as a whole, and the DSRC-solution in particular, needs to be continuously monitored for its security status. Risks and security strategy need to be reassessed on a regular basis.

6.7 CONSIDERATIONS FOR A SECOND GENERATION

OBE are out in the field and will eventually be hacked.

The Payment Authenticator is calculated by the OBE, sent to the RSE and passed without change by the Toll Charger to the EETS Provider. Hence the EETS Provider is under total control of the algorithm he uses to calculate the Payment Authenticator.

In the near future OBE use the same DES-based method for both the Payment Authenticator and the OBE Authenticator. Only the OBE Authenticator calculation needs to be standardised and known to all Toll Chargers.

For the Payment Authenticator the EETS Provider is basically free to ask industry to implement different algorithms as long as the length of the resulting authenticator remains the same (4 bytes). The EETS Provider is free to use algorithms that are time intensive to calculate since the authenticator can also be pre-calculated if another nonce value than the one provided by the road side is used.

(Note that the current mechanism used to calculate the Payment Authenticator is standardised in EN 15509. EETS Providers can deviate from this standard without bad consequences as long as they keep the length of the authenticator transmitted on the DSRC interface the same.)

Even with such gradual improvements, system security ultimately rests on the safe storage of a secret in the OBE. As soon as safe storage becomes a problem, new concepts have to be found. This will then almost certainly mean that the 4 byte long authenticator fields foreseen in the current DSRC transaction definition is insufficient to support the new mechanisms required. A new DSRC transaction will then need to be defined.

Whereas the concept discussed so far in this section is in fact tailored to the capabilities of current standard DSRC-tags, a future DSRC EETS transaction can exploit the enhanced (secure) storage, processing and communication capabilities of the EETS OBE. Interesting options to pursue are:

- The ‘always on’ property of an externally powered OBE allows for calculation of asymmetric authenticators, outside the time-critical DSRC window. Asymmetric authenticators can be verified by the RSE without connection to the EP and without storing secret keys.
- The CN communication facility allows for a far more dynamic key management. Keys could be renewed frequently, thus reducing the exposure and possible gain for fraud.

Although the EG11 DSRC transaction may fulfil demands of European interoperability for years to come, its age justifies some thinking about its future.

[R 18] A second generation DSRC-transaction should be further investigated. It should be integrated in the overall crypto-concept for the EETS. The second generation transaction should offer enhanced security, exploiting the capabilities of the EETS OBE.

7 SECURITY CONCEPT FOR GNSS/CN SYSTEMS

7.1 INTRODUCTION

In this section some elements of the recommended security concept for GNSS/CN EETS is described. It should be noted that on all aspects further elaboration is required for the EETS definition. ISO/CEN seems the appropriate forum to take this on, once decisions on the headlines described in this document are taken.

For the discussion in this Section, it is necessary to understand the fundamental difference between DSRC-based and GNSS/CN-based systems:

- GNSS systems and in particular the OBE are autonomous in relation to the roadside. They require no contact to RSE per se.
- GNSS OBE is collecting data from a range of sensors autonomously that is ultimately used to derive the toll due and also to generate court-proof evidence of compliance and non-compliance with the tolling scheme.
- GNSS OBE has a direct communication channel to central EETS Provider systems for updating information on the OBE and possibly[3] for uploading charge data. This channel requires special protection.
- GNSS systems, in particular when implementing a smart client variant, make use of OBE that needs to handle complex tasks. The OBE is more flexible and can be updated with new software, maps and tariffs. This process must be protected.
- In GNSS-systems the OBE "controls" the transaction process, where in DSRC the OBE is "passive" towards the roadside during the transaction.

Additionally, there is a fundamental difference to DSRC when it comes to the communication of the OBE with the main players the Toll Charger and the EETS Provider: Interoperable EFC defines the OBE as property and responsibility of the EETS Provider.

In the DSRC world, the communication however takes place between the OBE and the RSE of the Toll Charger, who in turn verifies the authenticity of the OBE and forwards the tolling event to the respective EETS Provider. The time and location of road usage is directly determined from time and location of the RSE detection.

In a GNSS based system, the OBE autonomously generates and records sensor data to derive time and location of road usage and then communicates directly with the

[3] Alternatively, the OBE may upload charge data to the Toll Charger.

backend systems (of EETS Provider or Toll Charger) via public mobile networks such as GSM. The Toll Charger may use appropriate road side enforcement to detect vehicles using his toll roads and communicate with OBE locally using DSRC.

7.2 ARCHITECTURE ASPECTS

It is important to consider that in case of GNSS/CN based systems, the correct declaration of usage of the service fully relies on the proper functioning of the OBE. The OBE is located in a potentially 'hostile environment': the domain of the Service User who may not be inclined to pay the (full) price for the service. Without any further measures, fraud problems could become unmanageable for both the EETS Provider and the Toll Charger. Two main strategies[4] can be followed to reduce this risk to an acceptable level:

1. Make use of 'tamper-resistant' or 'tamper-evident' OBE
2. Perform spot-checks on the road to verify that OBE is installed, genuine and working properly.

Fully relying on the first strategy will lead to high unit costs of the OBE and will likely be economically infeasible. In addition, even without budget constraints, OBE protection measures are not easily made effective against all attacks, including disconnection from power, jamming/spoofing of GNSS, shielding it from EM radiation or completely removing the unit from the vehicle.

Fully relying on the second strategy also has its issues. Sustaining sufficient enforcement pressure becomes inefficient and costly when the charged network is extensive, e.g. when all roads in a country are being charged. Enforcement on a dense network of minor roads with little traffic cannot be done cost-effectively with the second strategy. In addition, it may be verified that a device is present in the passing vehicle, that the presence of that vehicle at given time/location is not in conflict with the declared usage, and that it is able to produce some data that accurately describe its status (e.g. vehicle characteristics, current position). If there is no trust that the information retrieved is from a 'genuine and authentic OBE', only the information that can be verified against an independent source is of value. A fake device could be constructed that declares usage only as far as needed for consistency with the spot checks encountered. This will leave abundant opportunity for fraud if:

- the density of spot checks is small compared to the number of locations were (incremental) charges are to be declared/registered by the OBE. Distance-based charging on an extended road network can be considered an extreme case.
- the level of detail in the OBE declaration is low[5]. This may be done to protect user privacy.

The recommended approach consists of a mix of the two approaches, combining the advantages of both.

- the OBE as a whole offers a moderate level of security

[4] Analysis / data mining on detailed OBE declaration data can be regarded as a possible additional element of the strategy. It can be effective in case a high level of detail is provided in the OBE declarations. It is left out of the discussion in this section as it can be seen as complementary to the 'main strategies'.

[5] Example: if in case of a flat distance-based charge an OBE declaration would basically consist of a running km-total value, cross-checking with an observed presence of the vehicle at some location and time would be impossible.

- the OBE contains a Trusted Element (TE). Data in the TE have a high level of protection against unauthorised access (read/write/erase). An example of a cost-effective implementation offering a high level of security is a smart card with cryptographic capabilities. The TE is used to store vital fixed data relating to vehicle and contract. It also serves the purpose of a safe relay for usage and status data that are not yet forwarded to the backoffice (TC or EP). The TE contains keys and carries out all cryptographic measures to generate/verify a proof of integrity.

The OBE regularly generates a usage/status update to the TE. Whereas the content of the information may not be correct, once submitted to the TE the data are irrevocable. In a spot-check the TC is able to verify that the retrieved information from the OBE is coming from a genuine, authentic TE and traceable to an EP and account ID. The information retrieved does not only refer to the current OBE status, but also its operation during a definable history. This helps to counter some obvious attacks exploiting the possible low density of spot checks in a GNSS/CN system.

More details concerning spot checking and secure monitoring are provided in 7.4.3.

[R 19] For ensuring an appropriate level of security while keeping OBE cost to a minimum, the EETS OBE shall contain a Trusted Element (TE), e.g. crypto processor smart card or built-in processor with internal security kernel.

7.3 CRYPTO-CONCEPT

The review of applicable models in E.2 shows that the technical protection mechanisms must support different levels of trust relations between the parties. It follows that the means of protection (for example cryptographic key material) must be different for the individual links, since otherwise the different trust levels are not achievable. Traditionally, such scenarios are tackled using a hierarchical key concept with a centrally placed and ultimately trusted key authority.

There are two arguments against such an approach in the interoperable EFC system. For one, it will be politically, legally and commercially difficult to establish such an authority that is trusted by participating nation states as well as corporations acting as EETS Provider or Toll Charger.

If no central authority is installed but a hierarchical key concept is used, the operational risk of a key compromise is huge. By nature, a hierarchical key concept requires that keys higher up in the hierarchy are better protected. Such keys also provide a much more valuable target to fraudsters. Therefore, the protection of important key material will require enormous efforts which may still be insufficient considered the time frame in which the material is used. Additionally, future developments of system attacks must be considered.

To counter these issues, a distributed peering based key model should be used to secure trust relations in the interoperable EFC system. Peering based models allow establishing unidirectional trust relations without the need to have an independent third party and have the significant advantage that the key material of individual links can be changed without affecting any other link. This dramatically reduces the complexity of the task and allows for quicker and more frequent changes. If, for example, the time required to break the cryptographic protection of a link is reduced by future research to a fraction of the currently estimated time, a peer-to-peer model can still survive for a while by changing keys frequently – a hierarchical key model could no longer provide service.

A peer-to-peer model also maps well to the identified requirements of the general security structure of an interoperable EFC system.

7.3.1 Cryptographic Concepts and Standards

An international road tolling system generates a large number of trust relations, both between organizations as between technical entities. Trust relations between technical entities require technological means to secure them. In this area, cryptography plays a major role.

Most of the current national implementations of tolling systems as well as the early standards for international systems such as EN 15509 rely on symmetric cryptography to provide integrity protection and authenticity on their communication channels and trust boundaries. Symmetric algorithms are commonly chosen since they provide better performance and therefore require less computing resources to be applied, which appears to make them better applicable to road vehicle equipment and other embedded devices used in current tolling systems. Since the shared secret (key) is distributed among all participants, it requires a common, very high level of trust between them. It cannot be assumed that all participants of an international and interoperable EFC are willing or allowed to extend the same level of trust to all other international entities. The impact and the likelihood of a compromised secret rises with the number of participating entities. Once the shared secret is compromised, the entire system must agree on a new shared secret while it cannot use the existing channels, which were secured by the former secret and are therefore now open to attacks. Current implementations such as prEN 15509 try to deal with the issue by using derived keys that do not allow the deduction of the master key and include multiple shared secrets to still allow secured communication if a single secret is compromised. However, the full set of primary secrets is still widely distributed. From an operational point of view, such systems require tremendous efforts on the management side. The cost of operation appears to outweigh the effectiveness of the protection mechanism.

Asymmetric cryptographic methods on the other hand allow the use of a personalized key pair for each individual entity in the trust model. Participants can publish the public key part of their key pair while keeping the private key part secret from all other entities. This allows for a trust model of fine granularity, since each link between two entities can be set up and managed individually without requiring the entities to equally trust each other. Additionally, unidirectional trust relations are possible, which cannot be provided by symmetric methods.

All cryptographic entities of the system shall be provided with a well defined time of validity. In case of unusual events, e.g. compromising of a key, any cryptographic entity shall be revocable. The use of individual cryptographic keys for every entity allows the revocation without substantial effect on the overall system. There is no need to distribute new key material throughout the system, only the information about the compromised and replaced key material needs to be published. This is a significantly easier to operate scenario then the replacement of a shared secret.

Asymmetric and symmetric methods can be combined to form so-called hybrid methods. Hereby, larger entities or entity groups use asymmetric methods for their trusted channels while smaller end entities leverage the higher performance of symmetric methods. Additionally, the operation of devices requiring minimum latency can be adjusted to the needs of longer computation by redesigning the protocols and procedures to allow pre-computation of cryptographic values such as digital signatures. Therefore, the performance argument does not prevent the general use of asymmetric methods, symmetric methods can be used in conjunction with them when it is required by operational aspects such as performance and data transfer volume.

ISO 20828 provides a method for securing trust relations between larger entities using asymmetric cryptography. The standard shows that asymmetric cryptography can be used efficiently and without the need for a central trusted authority in the realm of

international tolling systems. It implements a peer to peer trust model, which forms a so-called web of trust. The standard also includes the possibility to specify exactly what trust relation exists between the trusting and the trusted party, further reducing the risk of a participant elevating its privileges above the mutually accepted level. The methods specified in ISO 20828 provide all necessary means to implement dependable asymmetric cryptography in an international EFC system. Due to the complex nature of the potentially evolving structures when implementing the standard on a large scale, a more detailed analysis is recommended.

[R 20] The implementation of a cryptographic concept for GNSS systems should rely on a suitable combination of asymmetric and symmetric algorithms. Every cryptographic entity should be equipped with an individual key or key pair that has a limited validity and can be revoked under well defined circumstances.

[R 21] For establishing trust between multiple entities, a peer to peer trust model should be used, e.g. as described by ISO/CD 20828. While a number of operational aspects of this standards need to be considered more deeply when applied in a large scale scenario, it is recommended that the ISO 20828 standard should be supplemented by a standard profile which describes an implementation in more detail.

7.3.2 Operational Aspects of a Technical Security Concept

When implementing a technical security concept it is of utmost importance to consider various operational aspects. The following (not exhaustive) table provides a number of key aspects. They have to be elaborated in detail in the definition of the technical concept.

[R 22] The EETS technical security concept should cover operational aspects such as flexibility, performance, cost, roll-out and migration, multi-client support, emergency procedures and revocability.

Flexibility	• Security Modules should be initialised with a minimum of data at rollout time. Whenever possible, under consideration of technical and security aspects, other configuration data and cryptographic keys and procedures should be updated in operations phase • The key technical implementation und parameters should be updatable (e.g. cryptographic key length) • Implementation should be based on standards whenever possible
Performance	• Carefully evaluate the characteristics of cryptographic algorithms to be used. Algorithms should be publicly available to make sure that their security can be proven by independent parties. • Consider the specific properties of algorithms such as performance when performing operations (e.g. signature

	creation vs. signature verification time) • Make use of available prognosis of future development of the security applicability of cryptographic algorithms • Analyse Minimal Latency and restricted communication of interfaces to be secured • Make use of pre-calculation of data before initiation of the affected interface
Cost	• Design, Implementation, Rollout and Operation of technical system should be cost-effective • Cost for updating and enhancing the technical system, e.g. co-operating with a new Toll Charger, should be kept at a minimum
Rollout and Migration	• Existing implementations should be migrated under consideration of existing equipment (e.g. RSE) or operated simultaneously • A technical security concept for GNSS systems should support the existing security scheme for DSRC systems. This means that existing cryptographic keys and algorithms should be available for communication in DSRC based systems.
Multi-client support	• Concept must support the implementation of multiple instances of each entity which are strictly separated • All cryptographic components must have a unique identifier which supports dedicated data fields which indicate the instance of the cryptographic system. • Operating of testing environments must be supported which does not affect any productive environments
Emergency Procedures	• Every implementation of cryptographic procedures should carefully evaluate any emergency events. In particular this includes compromising of cryptographic keys. • Emergency procedures should affect the system by the necessary minimum and should not interfere with the rest of the system • The design should provide procedures to detect unusual activity in the system and to report this automatically to appropriate monitoring systems
Revocability	• Every key /TE should be revocable, both actively when a communication happens as well as implicitly if no communication happens by limited validity that can only be extended by communication with key / TE owner

7.4 SPECIFIC PROCESSES FOR GNSS/CN

7.4.1 OBE personalisation and data management

In GNSS EFC systems, protection of the OBE is of outmost importance. In general, there will be the following classes of data requiring protection:

1. The cryptographic key material of the EETS Provider and the Toll Charger
2. The integrity and confidentiality of the personalisation data
3. The integrity of the software operating environment inside the OBE
4. The integrity of the geographic information
5. The integrity of the tariff information

To achieve a dependable protection of all classes listed above, the OBE will implement a trustworthy computing environment with a chain of verification. The trust anchor will be provided by a TE according to 7.2. A starting OBE will use a verified boot loader, who ensures that the main operating software is genuine and not tempered with. The operating software will perform a comparable verification using the TE on all application modules loaded afterwards and also provide verification of any map and tariff data available.

In GNSS, geographic, tariff and other configuration data can and will be received by the OBE via a CN, depending on the implemented model (thin client/smart client). Such transactions will be verified using asymmetric cryptographic methods and based on the trust into the TE.

Correct personalisation is, by the basic rules of EETS, the responsibility of the EETS Provider. It is assumed that an EETS Provider will provide a method for personalisation that can be done by the Service User itself without the need to use a service centre. A suitable method could be the issuing of a personalisation token in form of a smartcard to its users, allowing them to personalise any GNSS OBE by inserting the smartcard. The smartcard will be responsible for signing the transactions performed by the OBE, which allows the EETS Provider and the Toll Charger to verify which Service User is to be billed.

7.4.2 Declaration of usage and variable parameters

OBE declaration

In accordance with the format, contents and protocol defined by the Toll Charger, he will receive declarations of usage of the service, called toll declarations in this document. The toll declaration will contain data from which the usage of the tolled object or network can be derived and vehicle characteristics relevant for the tariff.

Depending on architecture options still open, the Toll Charger may receive such declarations directly from the OBE or through the EETS Provider. Also in the latter case, the OBE declarations provide the basis for the toll declaration to the Toll Charger[6].

It is therefore absolutely vital that the OBE declaration originates from a genuine and correctly operating OBE, that the declaration was not altered after its generation, and that it can be proven that the declaration has actually been sent by a particular OBE.

[R 23]	The declaration of usage from an OBE has to be provided with integrity, authenticity and non-repudiation measures. This security service can be realised with a digital signature.

Variable parameters

The service user may need to declare variable vehicle parameters that are used for fee calculation (e.g. the number of axles or presence of a trailer). The EETS Provider has no means to verify the declared data when it is entered into the OBE.

To counter fraud by intentional or unintentional false declaration, the OBE will either use a secure storage mechanism for logging of any modification of the declaration data by the regular user interface of the OBE. Alternatively or additionally, the OBE will use the CN to send records of modified declaration settings to the EETS Provider, enabling the timely detection of attempted fraud due to frequent re-declaration, for example before a known spot checking point. In any case, the unaltered log data together with respective time stamps will be provided to enforcement entities directly from the OBE.

7.4.3 Secure monitoring & spot checking

As discussed in 7.2, the concept of secure monitoring and spot checking is regarded important for cost-effective protection of GNSS/CN tolling against fraud. The concept is meant to monitor the OBE process of collecting, processing, storing and transmitting data relevant for the calculation of the charge. This subsection provides a more detailed example.

1. The OBE 'continuously' collects position and time data via GNSS. The data may be enhanced by filtering and fusion with data from other sensors. Depending on the basic architecture, data may also be further processed by the OBE into usage or charge data.
2. The OBE sends a usage message to the Trusted Element periodically[7]. The usage message will contain a timestamp, incremental usage/charge data or (sampled) position data.
3. Any errors/anomalies detected by the OBE will lead to an error message to the TE. The TE generates an internal error (stored in the event log) in case subsequent status messages are inconsistent or obviously incorrect[8].
4. The TE assigns a sequence number to each message, generates a digital signature over each message and sends it back to the OBE. The OBE may store the signed usage messages to maintain a detailed user log with proof of integrity. This user log is meant for the EETS service user (contract holder) and may be used in case of a dispute.
5. The TE stores the usage messages or aggregates these into the information required for the declaration to the backoffice. A number of last usage messages is always kept in a cyclic spot check log. A separate event log is kept for error messages and other events that may relate to fraud or defects.
6. In case of a spot check (by fixed, transportable or mobile enforcement equipment) the OBE submits the following information:
   - spot check log
   - event log
   - vehicle registration number
   - time and date.

---

[6] The toll charger may in this case still require the full OBE declarations as standard supporting information or may request this information occasionally for enforcement/monitoring/auditing purposes.

[7] Once in a certain period of time, after traveling a certain distance or a combination of these.

[8] The TE may e.g. check that time is always increasing, that the change in position between two messages is realistic given the difference in time etc.

This information is signed by the TE. For reasons of performance, the digital signature for the spot check response may be generated periodically, i.e. not using a challenge from the spot check RSE. The use of the VRN and time and date counters replay, man-in-the-middle and impersonation attacks.

7. The following types of checks can be performed using the data retrieved by the enforcement equipment:
   - do the data indicate that the OBE does not function properly or that there has been erroneous behaviour before? This can be concluded from the spot check log and the event log.
   - is the vehicle registration number in the data retrieved from the OBE identical to the vehicle registration number observed visually (by ANPR) ?
   - are the spot checking data consistent with declaration data (this will usually not be possible in real time)
   - are spot checking data from different spot checks consistent?

It is noted that several variants of the described procedure are possible and further analysis and elaboration is required.

[R 24] The concept of secure monitoring and spot checking is regarded important to achieve a sufficient level of protection against fraud in GNSS/CN based EETS. It is recommended that the concept is further analysed and elaborated e.g. by CEN/ISO.

7.4.4 CN Communication

The GNSS OBE relies heavily on the communication channel provided by a Cellular Network. Access to this communication channel must be protected as well as the integrity and confidentiality of the transported data.

CN access is generally protected by the network operators. There are several configuration options required by the GSM standards and supported by all network operators that can further limit access to the network, hereby limiting access to the communication interface from third party GSM users.

The communication channel between the OBE and the EETS Provider needs further protection to establish a secure channel:

- Asymmetric cryptography for authentication and initial key exchange
- Symmetric cryptography for high performance encryption or resource-limited encryption
- An Integrity protection algorithm.

There are several well established cryptographic protocols that accomplish the required integrity and confidentiality on the link.

[R 25] A comprehensive technical security concept with particular consideration of the points mentioned in this report should be developed to be used in the EETS context. A substantial amount of work has already been done in drafts for CEN/ISO 17575 and MISTER. It is recommended that the concept is further analysed and elaborated.

8 SPECIFIC SECURITY ISSUES

This section contains remaining specific security issues that were discussed in EG12.

8.1 BLACKLISTS

When examined in detail, CESARE III proposes several blacklists to counter fraud and handle cases of withdrawn licenses and guarantees. The trust relation analysis (see E.4.3) covers them in more detail. CESARE III does not address the management and maintenance of the blacklists and places the responsibility at the Interoperability Management role. On a contractual level it may simply be arranged that a Toll Charger is liable for applying blacklist information within a certain period after delivery by the EETS Provider.

It should be noted that the management of blacklists is difficult in large systems with multiple actors/nodes. As an example, adequate management of certificate revocation lists (a specific type of blacklist) is one of the major issues in PKIs (Public Key Infrastructures), where lists tend to grow continuously over time. This may lead to increasing demands on storage and network, as well as deterioration of availability and performance for consultation of the lists.

Although the use of blacklists seems unavoidable for the EETS, the complexity of managing blacklists in the EETS context should not be underestimated. This approach to exclusion should be investigated in more detail and revised:

[R 26] In order to arrive at a secure, fast and reliable mechanism for distributing and using revocation information for the EETS:

- Measures for efficient implementation of blacklists and alternative approaches for distribution of revocation information are to be further elaborated.
- For OBE blacklists, requiring a periodic OBE update by the EETS provider to keep it in operational status seems a valid approach, as effectively disabled OBEs do not have to be kept on any blacklist. EETS providers should maintain OBE blacklists without need for central co-ordination.

9 SUMMARY OF RECOMMENDATIONS

The list below summarizes the recommendations from this document. Some recommendations only apply to DSRC-based toll systems. This is indicated by <<DSRC>>. Some requirements only relate to GNSS/CN based toll systems. This is indicated by <<GNSS/CN>>. All other recommendations apply to the EETS in general.

1. An EETS Data Protection Policy should be developed as an anchor for the further elaboration of EETS security:
   - The EETS Data Protection Policy shall have its main focus on the On-Board Equipment (OBE) and the interfaces between the OBE and the equipment operated by the Toll Chargers and the EETS Providers.
   - The EETS Data Protection Policy shall enable a flexible, multi-level and stepwise implementation of the data protection policy.
   - The EETS Data Protection Policy shall lead to EETS Protection Profiles for the OBE and the interfaces between the OBE and the equipment operated by the Toll Chargers and the EETS Providers following the guidelines given in CEN ISO/TS 17474 RTTT – EFC – Guidelines for EFC security protection profiles.
2. A future EETS Management Board shall initiate additional research into an adequate trust model for the EETS.
3. The actors in the Cesare III Model should be treated as non-trusted partners with a variety of trust relations that should be secured. The complexity of the relations implies that standard measures should be developed for protecting them. The protection should be based on a peer to peer trust model, so that trust can be established between two actors without requiring a third party.
4. The EETS OBE shall be subject to type approval procedures, comprising security features as well as accuracy and availability.
5. In GNSS/CN based systems, the correctness of toll declarations depends on the complete data processing by the EETS provider. Therefore, the related operations of the EETS Provider shall be subject to certification and audit procedures. <<GNSS/CN>>
6. The EETS will involve handling of data that are to be regarded as personal data by the definition of 95/46/EC. The individual entity controlling such data will have to comply with national privacy legislation derived from 95/46/EC. A central coordination on EETS/EMB level is not required.
7. The EETS Provider is responsible for protection of the personalisation interface. Certification of OBE for the EETS shall include requirements and tests regarding this protection.
8. Certification of OBE shall require and test for safe storage of keys.
9. EETS Providers shall check PAN, Payment Authenticator and Transaction Counter for every transaction as quickly as possible. Security Processes of the EETS Provider shall be part of the approval process. <<DSRC>>
10. For all keys used in the EETS a set of system-wide known test keys shall be foreseen.
11. EETS Providers should only deliver OBE Authentication Master Keys to Toll Chargers that have a certified secure key storage at the roadside or in the central system. <<DSRC>>
12. The Master Keys distributed to Toll Chargers for OBE Authentication on the DSRC link shall be controlled by each EETS Provider and be different from one EETS Provider to the other. <<DSRC>>

13. The EETS Provider is responsible for key distribution and for the distribution strategy. No central body is required for key management.
14. Toll Chargers should develop a phased security strategy that allows fast migration to higher protection levels as the need arises. <<DSRC>>
15. EETS Providers and Toll Chargers shall cooperatively step-by-step prepare for online authorisation of OBE. As part of the preparation for this, the necessary data exchange protocols and processes need to be defined. <<DSRC>>
16. It is recommended to move towards the use of Access Credentials as quickly as possible. EETS Providers have to decide when to issue OBE that require Access Credentials. <<DSRC>>
17. The EETS as a whole, and the DSRC-solution in particular, needs to be continuously monitored for its security status. Risks and security strategy need to be reassessed on a regular basis.
18. A second generation DSRC-transaction should be further investigated. It should be integrated in the overall crypto-concept for the EETS. The second generation transaction should offer enhanced security, exploiting the capabilities of the EETS OBE. <<DSRC>>
19. For ensuring an appropriate level of security while keeping OBE cost to a minimum, the EETS OBE shall contain a Trusted Element (TE), e.g. crypto processor smart card or built-in processor with internal security kernel.
20. The implementation of a cryptographic concept for GNSS systems should rely on a suitable combination of asymmetric and symmetric algorithms. Every cryptographic entity should be equipped with an individual key or key pair that has a limited validity and can be revoked under well defined circumstances. <<GNSS/CN>>
21. For establishing trust between multiple entities, a peer to peer trust model should be used, e.g. as described by ISO/CD 20828. While a number of operational aspects of this standards need to be considered more deeply when applied in a large scale scenario, it is recommended that the ISO 20828 standard should be supplemented by a standard profile which describes an implementation in more detail. <<GNSS/CN>>
22. The EETS technical security concept should cover operational aspects such as flexibility, performance, cost, roll-out and migration, multi-client support, emergency procedures and revocability.
23. The declaration of usage from an OBE has to be provided with integrity, authenticity and non-repudiation measures. This security service can be realised with a digital signature. <<GNSS/CN>>
24. The concept of secure monitoring and spot checking is regarded important to achieve a sufficient level of protection against fraud in GNSS/CN based EETS. It is recommended that the concept is further analysed and elaborated e.g. by CEN/ISO. <<GNSS/CN>>
25. A comprehensive technical security concept with particular consideration of the points mentioned in this report should be developed to be used in the EETS context. A substantial amount of work has already been done in drafts for CEN/ISO 17575 and MISTER. It is recommended that the concept is further analysed and elaborated. <<GNSS/CN>>
26. In order to arrive at a secure, fast and reliable mechanism for distributing and using revocation information for the EETS:
    - Measures for efficient implementation of blacklists and alternative approaches for distribution of revocation information are to be further elaborated.
    - For OBE blacklists, requiring a periodic OBE update by the EETS provider to keep it in operational status seems a valid approach, as effectively disabled OBEs do

not have to be kept on any blacklist. EETS providers should maintain OBE blacklists without need for central co-ordination.

ANNEX A RELEVANT INPUTS

A.1 STANDARDISATION, CEN/TC278/WG1

Background

Standardisation of EFC started in the beginning of the 1990s in the CEN Technical Committee TC278. On a global level the corresponding standardisation is handled by ISO TC204 (these two working in co-operation since the mid 1990s) The working group standardising the EFC-application is called CEN/TC278/WG1 (& ISO/TC204/WG5) [9]

WG1 has delivered several standards supporting interoperable EFC over the years (see list below). It is currently (April 2007) working on the following work items of interest for the EETS:

- 15509 Interoperable Application Profile for DSRC-EFC.
- Conformance evaluation for 15509.
- 17575 Application Interface Definition for GNSS/CN-EFC.
- 17573 EFC Architecture (under revision)
- Information flows between operators

The more technical standardisation issues concerning e.g. DSRC-communication are handled by other working groups.

There are also other, more general, issues regarding IT-security that are standardised by other groups.

Scope

WG1 basically covers all of the EFC area, including all technologies, all services and everything being "inside" of the EFC-community. WG1 is dealing with; clearing, architecture, IC-cards, security, EFC-DSRC application interface, test procedures and EFC-GNSS application interface.

However, WG1 only deals with concrete work items (within the scope) decided by the parent standardisation body. Thus WG1 has never had the task to define "full" interoperable solutions, neither for DRSC-EFC nor for autonomous systems. The focus has been on making framework and toolbox standards, enabling and supporting interoperability between EFC-systems.

Abstract of security parts

17574

For some 5 years in the mid 1990s WG1 included a special sub-group, SG4, dealing with security issues. The first task of SG4 was to make a summary of security issues in an Internal Technical Report (ITR) finalised in 1997. The report goes through possible threats and security services.

[9] For short this group is called WG1 below.

The next step was to provide a framework standard called ISO TS 17574:2004 "Road transport and traffic telematics - Electronic Fee Collection (EFC) - Guidelines for EFC security protection profiles ". This standard is basically a set of guidelines for the preparation and evaluation of security requirements specifications called Protection Profiles (PP). The standard defines the outline and contents of a PP and give examples of how this may be done. Its scope it limited to the User, Service provider and the interface between them (i.e. not the entire EFC chain). The approach in 17574 is based on the following general IT-security standards:

- ISO/IEC 15408-1/2/3:1999 "Information technology - Security techniques - Evaluation criteria for IT security" (in three parts).
- ISO/IEC PDTR 15446 "*Guide for the production of protection profiles and security target*".

14906

The DSRC-application toolbox standard, 14906, also includes some security related EFC-functions, such as GET_STAMPED, GET_SECURE and a brief security framework.

15509

A more detailed security definition is done in the Interoperable Application Profile standard, 15509[10], that provides for a full set of security measures for DSRC-EFC transactions. This includes: security data elements, calculation of dynamic authenticators, transaction counter and the option of using access credentials (AC_CR)[11]. prEN 15509 uses a set of general standards for calculation of DES, triple-DES, MAC-calculation, i.e.: ANSI X3.92, ANSI X9.52, ISO/IEC 9797-1.

The access credentials issue is of special importance as there are different implementations and requirements over Europe (and between CARDME and CESARE). WG1 has done a discussion paper to highlight these issues (WG1 N971). As it is not up to WG1 to decide on security implementation, EN 15509 allows for both having and not having support for access credentials by defining two security levels.

17575

The GNSS/CN-application toolbox standard, 17575, is not finalised yet, but will provide for some basic security tools for GNSS-based EFC.

20828

This draft standard specifies how trust between devices from different security domains, with different entities responsible, can be established and managed in a cost-effective way. It uses public key certificates. It addresses the role and responsibilities of the Certification Authority relating to certificate issuing and distribution, specifies how to handle certificate validity and certificate policies and defines a certificate format. This draft standard is not finalised yet.

[10] 15509 was approved unanimously after a formal vote in February 2007, it is now in the process of being published (April 2007).

[11] Thus, using the lower of the two security levels makes the specification in 15509 fully in line with [EG11 report] (i.e. with no support for AC_CR).

A.2 CARDME

Background

The CARDME-initiative started in 1993 by the EU-commission as a “concerted action” for enabling interoperability between EFC-systems in Europe. After a few years CARDME changed its organisational structure and became a series of Framework projects (CARDME-2, 3 and 4) with a loosely connected CARDME-Steering Committee (SC) consisting of member states and other countries in the EEC. CARDME-SC that had no formal role in the CARDME-project, but served as a feedback forum for CARDME and information exchange between member states.

The final report of CARDME-4 (2002) provided a very concrete specification for interoperability between DSRC-based EFC-systems in Europe and became the foundation for several EFC-specifications nationally. The CARDME-4 solution is also provided as an informative example in the 14906 standard.

Scope

CARDME deals mainly with DSRC-based EFC. Its main focus lies in the interface between OBE and RSE. It defines (fully) a transaction for the communication between OBE/RSE. It supports payment using central account in an interoperable environment.

CARDME does not explicitly deal with other parts of interoperability; legal issues, procedures, organisation and communication between operators.

Abstract of security parts

The final CARDME report provides for a full security solution for an interoperable DSRC-EFC transaction. There are sections in the report specifically dealing with security issues and measures (3.2.4, 3.3.1, 3.3.2).

CARDME has four "security services":

- Integrity service providing protection against unauthorised modification or deletion of information
- Authentication service providing confirmation that the identity of a source of data received is as claimed
- Confidentiality service providing protection against unauthorised disclosure of information
- Access control service providing protection against unauthorised operations on information or processes in the system.

The concrete set of security tools includes: definition of security data elements, calculation of dynamic authenticators, static authenticator, transaction counter and the use of access credentials (AC_CR).

A.3 CESARE & PISTA

Background

CESARE was started in 1998 by ASECAP[12] as an effort to achieve interoperability among national systems with the objective to allow common users to make use of their own on-board unit (OBE) throughout Europe. The initiative was intended from the start to be a multi-phase project. In 1999 CESARE-1 produced a draft definition of such an interoperable solution.

CESARE-2 started in the year 2001 and was completed in spring 2002. The objective of this phase of the project was the development of a Memorandum of Understanding defining all technical, organisational and operational rules upon which contractual interoperability among ASECAP members might be established. The PISTA-project (see below) is largely based in the findings of the CESARE-2 project.

In the next step, CESARE-3, the ASECAP members were joined in equal shares by non-ASECAP countries represented by the so-called "Stockholm-group". CESARE-3 was to include a wider range of services, including GNSS-based systems and HGV-taxation schemes. It was to provide direct support for the EETS-definition. The final results were provided in October 2006 divided into parts on: revised model, service definition, national organisational impacts, legal issues and procedures.

Scope

CESARE-1 and 2 were mainly focusing on DSRC-based EFC for tolled motorways. It aimed at post-payment using central account between the ASECAP members. CESARE also had a strong procedural and legal focus defining all the interfaces necessary for interoperable EFC in this context. Thus it complemented the more technically oriented CARDME-project with the non-technical parts of interoperable DSRC-EFC.

CESARE-3 had a much wider scope than before, dealing also with; new schemes (e.g. taxation) and new technology (autonomous systems). The focus remained on procedural and legal issues (leaving the details on technology to other projects).

Abstract of security parts

CESARE-2 and PISTA

CESARE-2 and PISTA provides for a full security solution for an interoperable DSRC-EFC transaction to be used within the ASECAP-group.

The CESARE-2 and PISTA set of security tools includes: definition of security data elements, optional calculation of dynamic authenticators and static authenticators.

Note: Although CESARE-2 and PISTA have two security levels the overall security functionality is set at a lower level than in CARDME (naturally this also means less costly upgrades to be made in Roadsides in ASECAP-countries).

CESARE-3

[12] ASECAP is an association of road toll facility operators in European countries.

The CESARE-3 deliverables does not deal explicitly with security, except on an overall level. The CESARE-3 service definition provides room for security services, but leaves to other projects to define those in detail (e.g. WG1, EG11, EG12, etc).

ANNEX B REFERENCES

General References

[CARDME] CARDME-4 – The CARDME Concept (Final, 1 June 2002), EC Project IST-1999-29053, Deliverable 4.1

[CESARE-II] Detailed CESARE Technical Specification, EC Project CESARE II, Deliverable 032.1, 2002-02-27.

[CESARE-III] CESARE III Project – D2.1 Detailed Service Definition", Final, Validated by project Steering Committee, 9 October 2006

[EG9 Report] Specification of the EFC application based on satellite technologies, Version 3.2, Report of Expert Group 9, European Commission, 2006.

[EG10 Report] Functional requirements and technologies for enforcement of violations in non-stop environment, Report of Expert Group 10, European Commission, 2006.

[EG11 Report] Definition of the EFC Application for the EETS Based on Microwave Technologies - Prepared by Expert Group 11 - Working to support the European Commission on the work on Directive 2004/52/EC (2006-06).

[IO Directive] Directive 2004/52/EC of the European Parliament and of the Council of 29 April 2004 on the Interoperability of Electronic Road Toll Systems in the Community

[PISTA] PISTA – Transaction Model, EC Project IST-2000-28597, Deliverable 3.4

PISTA: Agreement on Security, D3.7 v4, 2002-10-24.

Referenced Standards

EN ISO 14906:2004, Road Transport and Traffic Telematics (RTTT) – Electronic Fee Collection (EFC) – Application Interfaces Definition for Dedicated Short-Range Communication (DSRC)

EN ISO 12253:2004, Road Transport and Traffic Telematics (RTTT) – Dedicated Short Range Communication (DSRC) – Physical layer using microwave at 5.8 GHz (DSRC Layer 1 standard).

EN ISO 12795:2002, Road Transport and Traffic Telematics (RTTT) – Dedicated Short Range Communication (DSRC) – Medium access and logical link control (DSRC Layer 2 standard).

EN ISO 12834:2002, Road Transport and Traffic Telematics (RTTT) – Dedicated Short-Range Communication (DSRC) – Application Layer (DSRC Layer 7 standard)

EN ISO 13372:2004, Road Transport and Traffic Telematics (RTTT) – Dedicated Short-Range Communication (DSRC) – DSRC profiles for RTTT applications (DSRC Profiles standard).

ISO/IEC 15408-1/2/3:1999; Information technology - Security techniques - Evaluation criteria for IT security.

ISO/IEC PDTR 15446; Guide for the production of protection profiles and security target.

CEN/ISO TS 17573:2003; Road Transport and Traffic Telematics (RTTT) – Electronic Fee Collection (EFC) – System architecture for vehicle related transport services.

ISO TS 17574:2004; Road Transport and Traffic Telematics – Electronic Fee Collection (EFC) – Guidelines for EFC security protection profiles.

EN ISO 15509:2007; Road Transport and Traffic Telematics — Electronic Fee Collection — Interoperability Application Profile for DSRC (also called the 'IAP standard', approved in 2007-02, under publication 2007-04).

Not yet published Standards and internal technical reports

prTS 17575; Road Transport and Traffic Telematics (RTTT) – Electronic Fee Collection (EFC) – Application Interface Definition for GNSS and CN (under development by WG1, 2007-04).

ISO/CD 20828; Road Vehicles – Security Certificate Management (under development by ISO TC22/SC3/WG1, 2004-01).

CEN/TC278/WG1/SG2: Access Credentials discussion paper, 2006 (WG1 N971).

ITR: Definition of threats and security controls for the charging interface in EFC, 1997 (WG1 N418).

ANNEX C ABBREVIATIONS

AC_CR	Access Credentials
ATM	Asynchronous Transfer Mode
CA	Certification Authority
CARDME	Concerted Action for Research on Demand Management in Europe
CEN	European Committee for Standardization (Comité Européen de Normalisation)
CESARE	Study for a Common EFC system for an ASECAP Road Tolling Service
CM	Customer Media
CN	Cellular Network (for example GPS/GSM)
DES	Data Encryption Standard
DSRC	Dedicated Short-Range Communication
EETS	European Electronic Toll Service
EFC	Electronic Fee Collection
EG1	Expert Group 1 (on microwave technologies at 5.8 GHz)
EG7	Expert Group 7 (The role of financial institutions - payment and contractual aspects of EETS
EG9	Expert Group 9 (Specification of the EFC application based on satellite technologies)
EG10	Expert Group 10 (Enforcement specifications and technologies for the EETS)
EG11	Expert Group 11 (Definition of the EFC Application for the EETS Based on Microwave Technologies)
EG12	Expert Group 12 (Security aspects of the EETS)
EMB	EETS Management Body
EMV	Europay, Mastercard, Visa (Standard for credit cards with chip)
EP	EETS Provider
GNSS/CN	Global Navigation and Satellite System / Cellular Network (for example GPS/GSM)
IFM	Interoperable Fare Management
IM	Interoperability Management
ISO	International Organization for Standardization
ISO	International Standards Organisation
MAD	Media Accepting Device

MEDIA	Management of EFC DSRC Interoperability in the Alpine Region
MISTER	Minimum Interoperability Specification for Tolling on European Roads
OBE	On-Board Equipment
PAN	Personal Account Number
PISTA	Pilot on Interoperable Systems for Tolling Applications
PKI	Public Key Infrastructure
PP	Protection Profile
PT	Public Transport
RSA	Asymmetrical Cryptographical technique
RSE	Road-Side Equipment
RTTT	Road Transport and Traffic Telematics
SAM	Secure Access Module
SC	Steering Comittee
SU	Service User
TC	Toll Charger
TE	Trusted Element
TOE	Target of Evaluation
VST	Vehicle Service Table

ANNEX D EXPERT GROUP MEMBERS

The following members of Expert Group 12 were appointed by the European Commission:

Name	Company/Organisation
Stefan Eisses (Lead)	Rapp Trans NL / Get ID (Netherlands)
Erich Erker	Siemens (Austria)
Rafael Fando	Cintra (Spain)
Trond Foss	Sintef (Norway)
Jean-Marc Gautier	Isis (France)
Karl-Heinz Goebbels	Toll Collect (Germany)
Heinz Haderer	Asfinag (Austria)
Johan Hedin	Hybris Konsult AB (Sweden)
Uwe Leinberger	T-Systems (Germany)
Bernhard Oehry	Rapp Trans (Switzerland)
Simon Smith	PA Consulting (UK)

Informal participation in the expert group by:

- Fausto Caneschi, Lecit Consulting, Italy
- Daniel Ohst, Toll Collect, Germany.

Other inputs from:

- Ilse van der Giessen, Collis b.v. (EMV)
- Jan Blonk and Lex Schoonen, Brightsight b.v. (ANNEX H)

ANNEX E ENTITIES AND TRUST RELATIONS IN THE CESARE III MODEL

E.1 INTRODUCTION

A correct and detailed trust model is the basis for any serious consideration of required, optional and superficies protection mechanisms. Security decisions based on too abstract models have historically resulted in easy security breaches or inelegant security designs since they neglected the complexity arising from the higher level of detail in the real world. Building a detailed trust model allows verifying decisions and directions against the model in future work, hereby providing great flexibility and a safe ground to operate on. Alternatively, threat and risk analysis would operate either on the basis of current, non-EETS compliant scenarios or on no basis at all.

The approach should be understood as fundamental research towards a correct model of higher abstraction. By dissecting the entities and trust relations to a fine granular representation, it is possible to show that an entity is entirely under the control of a underlying entity. In other cases, the detailed model can be used to show that a sub-entity extends or receives trust relations the higher-level entity is not concerned with, hereby showing that the sub-entity cannot be abstracted in the higher-level entity.

The model presented represents a top-down first, bottom-up last approach in contrast to historical or arbitrary classification. It provides base research to a more abstract and compact representation of the entities while it can already be used to distill the less obvious but never less essential trust relations.

Based on the detailed trust model, multiple possible bottom-up abstractions and groupings can be evaluated, which allows to balance protection needs for trust relations against business needs. For example, each trust relation to a sub-entity can be evaluated in terms of its impact if the sub-entity becomes a legally separate company, which helps to determine outsourcing potential. The same approach can be taken towards required agreements and management.

To build a trust model from CESARE III, all entities in the documents must be identified. The CESARE III model is mainly a behavioural approach to an interoperable EFC structure which centers on the four roles and their interaction. Analyzing [CESARE-III] allowed capturing the explicitly mentioned entities in the model but also to deduce entities only implicitly assumed to exist by the CESARE III authors. The trust relations between the entities were extracted from the Detailed Service Description or deduced from the requirements the service description imposed.

The analysis showed that in an interoperable EFC system according to [CESARE III], there are two distinct trust relation types or trust layers. The organizational trust layer covers the trust relations between organizational entities, namely natural persons and corporate bodies. The second layer involves technical entities, namely devices such as OBE, RSE and central systems of the participants. The two layers can be cleanly separated with interfaces at the operational sub-entities of the major roles.

Maybe they can be clearly distinguished, but both are complementary and should be analysed in conjunction. What counts are secure interactions between EETS Providers and Toll Chargers as legal entities including secure interactions between equipment configurations acting on their behalf).

To secure the trust relations in the two trust layers, different approaches can and should be taken. The organizational trust layer will involve legal measures such as placing of contracts and service level agreements. The technical trust layer must use technical means to protect trust relations such as security protocols using strong

cryptography as well as clearly defined interfaces with logging and monitoring. Both should be audited on a regular basis, preferably achieving or confirming certifications.

On the other hand, the trust analysis showed that [CESARE III] does not go into sufficient detail of its entities and their relations. But describing the trust between entities is the basis for any detailed threat and risk analysis. Therefore, additional research by the EMB into this area is highly recommended.

E.2 SUITABLE MODELS

Based on the trust model analysis and the role interaction specified by [CESARE-III], it becomes obvious that any protection of trust relationships between entities, technical or organizational, must scale with the number of expected participants. The following key points regarding the scale of the resulting system must be considered:

- [CESARE III] requires any-to-any relationships between any EETS Provider and any Toll Charger in the participating countries.
- The resulting number of direct links is large and grows over time.
- It should be noted that the trust relation diagrams in B.6 includes only one EETS Provider and one Toll Charger, but already contains fifty-seven trust links.

Not every EETS Provider will trust every Toll Charger at the same level. In fact, the different actors and business model combinations suggested by [CESARE III] clearly indicate a network of non-trusted partners. Participants will initially not trust any other participant; they have to establish trust on a basis of organizational and technical measures to a level that is sufficient for both.

The above facts lead to the following requirements for the model:

- A set of strong standard measures per relation is needed.
- The standard measures must be applicable individually to a trust relation.
- A peer-to-peer model is required to prevent extensive organizational overhead.

Two participants would be able to set up a trust relation independent from the entire remaining system. Central or hierarchical models do not allow for such flexibility. They also require that every potential trust relation is known beforehand and catered to, which appears not achievable given the expected complexity of the system.

The actors of the CESARE-III Model should be treated as non trusted partners with a variety of trust relations that should be secured. The complexity of the relations implies that standard measures should be developed for protecting them. The protection should be based on a peer to peer trust model, so that trust can be established between two actors without requiring a third party.

E.3 ANALYSIS APPROACH

To identify entities in the CESARE III model, the available documentation from the CESARE III working group was studied. First, the entire documentation was reviewed to understand the global concept and the level of detail provided in it. Only a complete study of the documentation allowed understanding of the granularity of specifications.

A detailed analysis was performed on [CESARE]. The document was selected, since a detailed service definition includes the finest granular descriptions of actual services performed and the requirements of the major actors regarding said services. Analyzing this document not only allowed to capture the explicitly mentioned entities in the model but also to deduce entities only implicitly assumed to exist by the authors.

The identified entities are listed in section E.4. The identified trust relations are discussed in section E.5.

E.4 ENTITIES IN CESARE III

E.4.1 Well Defined Entities

The CESARE III documents define the following four roles in interoperable EFC

- The Service User is the one taking advantage of the EETS for payment of tolls in toll domains.
- The Toll Charger provides the transport service (road usage) to the Service User and charges the Service User a fee for use of the service.
- The EETS Provider provides equipment (OBE), contract and payment means to the Service User. The EETS Provider claims money from the user and pays the Toll Charger for legitimate claims of service usage.
- The Interoperability Management defines the functionality that deals with the overall management of interoperable EFC. This includes rules for interoperability, ID schemes, certifications and common specifications. The Interoperability Management is the regulatory entity in the model.

While the definition of abstract roles is required to define a model, the granularity is not well suited for the analysis of trust relations. By decomposing the roles defined in CESARE III, a organizational and physical architecture with a number of entities is developed. These entities and their relations are the basis for a substantial trust analysis which leads to trust classes that can be implemented by organizational and technical measures.

E.4.2 Decomposition of the Well Defined Roles

To analyze the trust relations between roles, the CESARE III definitions are too broad. Each of the roles is composed of several entities that have different trust relations and requirements against each other and third parties. Additionally, [CESARE-III], section 2, clearly states that:

> "A generic representative of a role is NOT by all means always one organisation or one entity. There can be different organisations or entities representing the role depending on the interface function between the roles."

Therefore, the entities defined in [CESARE-III] are decomposed as follows:

- Service User
  - Private Service User
  - Registered vehicle owner
  - Vehicle user (at the time of tolled road usage)
  - Business Service User
  - EETS contractual partner
  - Registered vehicle owner
- Toll Charger
  - Legal Toll Charger
    (legally entitled to charge for road usage by government / legislation)

    - Legal Executive Toll Charger
      (legally entitled to charge for road usage by the Legal Toll Charger)
    - Fiscal Toll Charger
      (entitled by the Legal Executive Toll Charger with handling of financial transactions)
    - Technical Toll Charger
      (provides and maintains the technology required for interoperable EETS)
    - Operational Toll Charger
      (operates the core services required by the Toll Charger role)
- EETS Provider
    - Legal EETS Provider
      (also called “Contract Issuer” in [CESARE-III], the contractual partner of the respective Service User)
    - Fiscal EETS Provider
      (entitled by the Legal EETS Provider with handling of the financial transactions)
    - Technical EETS Provider
      (provides and maintains the technology required by the EETS role)
    - Operational EETS Provider
      (operates the technical core services required by the EETS Provider role)
- EETS Management
  (according to [CESARE-III], page 57, responsible for EETS service quality assurance)
    - EETS Distribution Agents
      (in-house or third party agents for the distribution of the EETS equipment and contracts)
    - EETS Distribution Partner
      (Third parties acting on behalf of EETS Distribution Agents)
    - Interoperability Management
    - Arbitration
      (settles disputes between EETS Provider and Toll Charger roles)
    - Registration Authority
      (maintains the required lists of authorized EETS Providers and Toll Chargers)
    - Contract Model Provider
      (creates and provides model contracts for Legal EETS Providers and Legal Executive Toll Chargers)
    - Trust Center
      (defines ID schemes and supports the issuing the IDs)
    - Technical Certification Authority
      (certifies equipment according to he interoperability requirements)

The decomposition of the roles allows a fine granular reference when only a leaf entity is used while still allowing the use of the broad roles defined in the original document.

E.4.3 Additional Entities

This section deals with the entities that are not mentioned explicitly in [CESARE III]. These additional entities are not listed in the CESARE III documentation but are

required for trust relation analysis. Entities in this context are all elements of the EFC system where initial trust among these entities is not initially presumed.

The entities are presented together with the rationale behind their inclusion in Table E1. There is no particular order in which the entities are listed. Classification and grouping are handled in section E.5. Each entity listed may have a single or multiple instances in the entire European system.

Table E1 Identified Entities

Entity	Rationale
Bank	Since pre- and post payment are required and [CESARE-III] assumes a connection between a bank account with an EETS account, the financial institutes involved become entities. The bank must in some payment scenarios manage the relations between the account owner and the EETS contract, since the EETS Provider may not be able to identify the source of a payment transaction. Additionally, the bank may need to associate an ATM transaction with an EETS contract.
Central EETS Blacklist Authority	Protection against fraud and verification of active contracts relies in [CESARE-III] heavily on the use of blacklists. Since all blacklists must be available in real time, distribution of them in any-to-any fashion is complex. Accordingly, there must be a central authority managing and distributing the blacklists. The blacklists identified are: • OBE Rejection Blacklist This blacklist covers OBEs that failed to correctly communicate with either the TC RSE or their EETS Provider. • Toll Charger Blacklist This blacklist is mentioned in [CESARE-III] to include Toll Chargers that repeatedly charged EETS Providers incorrectly or whose license was withdrawn from Interoperability Management. • EETS Customer Rejection Blacklist Since [CESARE-III], 4.3 requires that changing the EETS must not allow evasion of blacklists, a list of customers rejected by one EETS Provider must be available for other EETS Providers. • EETS Withdrawn payment guarantee list An EETS Provider may, under certain circumstances, withdraw the payment guarantee to Toll Chargers or may loose certification from Interoperability Management as an EETS Provider.

Entity	Rationale
Certified Vehicle Inspection Center	[CESARE-III], 4.3 requires in CI.04 a Certified Vehicle Inspection Center. The Certified Vehicle Inspection Center is needed in regions, where the toll tariff depends on certain properties of the vehicle such as the emission class.
EFC Logo Placement Provider	Some countries require road signs to be installed by government or accredited institutions. Accordingly, the required EFC Logos that are to be placed on EFC conform tolling roads will be required to be installed by an EFC Logo Placement Provider who is allowed post road signs on roads. Since this would be an additional party, it must be considered as entity in the trust model
Electronic Map Material Supplier	Independent of the technical system specifications, both TC and EETS Provider require solid map data for charge calculation or respective verification purposes. Such map material is usually bought from a Geo data company specializing in road map material. While the EETS Provider will most likely obtain the material from the Toll Charger, the later will at least use some third party data, potentially just as a basis for its own material.
Email Hosting Provider	[CESARE-III], 3.2.2 requires communication from the EETS Provider to the Service User (and vice versa) via Email. Although [CESARE-III] seems to only consider this requirement for the purpose of higher acceptance of the EFC system, it introduces the Email Hosting Providers of both the Service User and the EETS Provider as trust entities. Unrelated attackers may use the Email system to modify messages between the EETS Provider and the Service User, causing misinformation and potentially legal issues.
Fuel Card Issuer	[CESARE-III], 3.2.3 requires the possibility to use a Fuel Card to pay the EFC fees. Since fuel cards are issued by separate legal entities (for example fleet management companies), the Fuel Card Issuer becomes an entity.
Crossborder Enforcement	[CESARE-III], 3.2.5: The OBE is required to contain enforcement data, which is not accessible to all entities. Crossborder Enforcement must obey the same limits in terms of data access as National Enforcement, but has a different trust model position since it allows cross-border enforcement.
National Data Protection Agency	The National Data Protection Agency is required to register the EETS use of personal data. [CESARE-III] explicitly mentions it and several European countries require such an agency to sign off massive use of personal data.

Entity	Rationale
National Enforcement	Based on the legal requirements of enforcement, it will in most cases be national. Since this represents a significant difference to the data access requirements of the Multinational Enforcement, the National Enforcement is introduced as entity. It is additionally required that enforcement will only have access to data that is relevant for enforcement purposes and not to personal information or value added services data on the OBE. Therefore, the enforcement entity has significantly different trust relations to the OBE than other communication partners.
National License Plate Database	According to [CESARE-III], 4.7, the Toll Charger has access to a license plate database of all participating countries. Currently, such database would in all cases be maintained by the national government. Access to such database may reveal a host of personal data about the registered owner of the vehicle in question and must therefore considered separately.
National TC	Since [CESARE-III], 3.2.1 requires the contract for EETS to extend and/or include the national contract, the National TC is an entity in the European system. There is the theoretical possibility that an already existing National TC will not part take in the EFC system while an EFC compliant Toll Charger provides the same services for EFC customers. This would mean that more than one Toll Chargers are covering the same road segment. In such a case, there are trust relations from the National TC to the EFC TC to allow for the National TC to continue its operation in the same fashion.
Newspapers and Magazines	Newspapers and Magazines are used for publishing important information in the promotion process according to [CESARE-III], 4.8. Therefore, Newspapers are an entity in the trust model, since invalid or inaccurate information would lead to users taking incorrect decisions.
OBE Hardware Vendor	This is the supplier of an OBE conforming to interoperable EFC requirements. Several other entities rely on the hardware vendor for protection of their data and secrets while these are being stored on the OBE. Additionally, the technical security of the hardware solution has important consequences for any protection and authentication mechanisms used by the software.

Entity	Rationale
OBE Installation and Personalization	[CESARE-III], 4.3 requires OBE Installation and Personalization, which may, from a security requirement point of view, be different than OBE Replacement and Repair, since the initial personalization will include access permissions to information stored at the EETS Provider that a repair station should not have. Also, personalization is required to be real time, which the OBE Replacement Service may not be able to provide due to its international distribution. Additionally, the Interoperability Management must certify the OBE Installation and Personalization entity, which is not a documented requirement for repair.
OBE Repair Service	[CESARE-III], 3.2.3 requires OBE repair and replacement in all participating countries. Therefore, the OBE Repair Service is its own entity. The OBE Repair Service will need access to the OBE using special equipment and potentially access credentials not available to other parties.
OBE Replacement Service	[CESARE-III], 3.2.3 requires OBE repair and replacement in all participating countries. OBE Repair Service is different than OBE Replacement Service due to the OBE belonging to the EETS Provider, therefore it is its own entity.
OBE Service Helpdesk	[CESARE-III] refers to a Service Helpdesk for OBE users. Apparently, the helpdesk is foreseen per EETS Provider, but may be a third party or entirely different. Any Helpdesk in EFC will require extensive access to personal data of the Service User stored at the EETS Provider. It may also need to access information about transactions from the Toll Charger to the EETS Provider regarding the Service User currently serviced. This implies additional trust relations.
OBE Smartcard Vendor	[CESARE-III], 3.2.1 mentions Smartcards for some types of OBE. The possibility to associate a Smartcard with a Service User is a spelled out requirement in the document. Since smartcards use their own operating system and hardware designs, the vendor is an important entity.
OBE Software Vendor	The supplier of an interoperable EFC conform OBE software. Much like the OBE hardware Vendor, several security methods will rely on the OBE Software, including but not limited to: • Key Storage • Remote Data Access Limitations • Technical Security Accordingly, the OBE Software Vendor has a number of trust relations to other entities in the model.
RSE Vendor	The supplier of any Road Side Equipment is, similar to the OBE Hardware and Software Vendors, responsible for important parts of the security architecture.

Entity	Rationale
Service User GSM Provider	[CESARE-III], 3.2.2 requires notification of Service Users via SMS, which introduces the GSM Provider of the Service User as an entity. Although GNSS implementations of EFC will require the GSM Provider as communication network carrier, such role is not foreseen in [CESARE-III].
SSL Certificate Authority	Based on the observation of the Web Hosting Provider, at least one SSL Certificate Authority is required so the users can validate the identity of the WWW server. SSL Certificate Authorities are well established entities in the current Internet infrastructure. They become an important part of the EFC trust model once the Service User is allowed to perform contractual binding transactions via the required WWW server offerings of the EETS Provider.
Toll Charger Local Database	According to [CESARE-III], SU-DSRC 2.3, specifies a local database containing all EETS data from all EETS Providers, blacklist information and security keys. While this is in total contrast to other requirements, it needs to be considered.
Web Hosting Provider	[CESARE-III], 3.2.1 requires communication of the Service User to the EETS Provider via WWW[13]. Therefore, the infrastructure for Internet based communication with the user must be maintained, which is commonly performed by a Web Hosting Provider. The technical security of the infrastructure in question will be important once the Service User is allowed to use this interface for contractual binding transactions.

Table E2 lists the trust entities in the technical trust model.

Table E2 Technical Trust Entities

Entity	Rationale
OBE	The OBE is a core element trusting and being trusted.
EETS Datacenter	The EETS Datacenter describes all technical entities in the computing centre of the EETS Provider.
TC Datacenter	The TC Datacenter describes all technical entities in the computing centre of the Toll Charger.
RSE	Road Side Equipment is a core trusting and trusted element in the EFC model.
Enforcement RSE	Enforcement Road Side Equipment has several trust relations with the OBE on the technical plane.
OBE Service Equipment	Service equipment located at entities dealing with OBE service is a trust entity in the model.

[13] [Error! Reference source not found.] uses the term WWW. For this document, we consider WWW representing a HTTP or HTTPS based web service offerings.

E.5 TRUST RELATIONS

Discussing all trust relations arising from the requirements in [CESARE-III] alone would not aid the understanding of the main relations. However, [CESARE-III] indicates the following obvious trust relations between these entities.

- Service User
  - Trusts EETS Provider with personal/business data
  - Trusts TC to charge the correct fee
- EETS Provider
  - Trusts the Toll Charger to correctly claim fees based on actual use by a Service User under his contract
  - Trusts the Interoperability Management to guarantee reasonable requirements as well as fair arbitration
- Toll Charger
  - Trusts a not well defined entity (this document refers to a “Central EETS Blacklist Authority”) to have a well-known list of allowed and not allowed Service Users in real time
  - Trusts the EETS Provider to receive payment for any claimed fees

To approach the complex task of trust relations in the interoperable EFC based on CESARE III and the entities listed in E.4, this section relies on Figure 4 and Figure 5. Table E3 lists the general trust relation classes and explains their meaning. Table E5 then maps the classes to the captions of all edges in Figure 4, since the captions define the objects the trust relation is concerned with.

The tables blow use the abbreviations “T” for the trustee (a.k.a. the one being trusted) and “C” for creditor, the one trusting. In Figure 4, this relation is displayed by a directed edge originating at the creditor and terminating (pointing to) the trustee.

Table E3 Trust Classes

Class	Meaning
Secure Key Trust	C trusts T that key material generated, handled and exposed by T is secure and cannot be compromised via an attack on T. This applies to asymmetric key material depending on T’s secret keys as well as symmetric key material shared between T and C.
Data Integrity Trust	C trusts T with the protection of the data integrity. This applies to data T provides and C operates on as well as data the C provides for T to operates on.
Data Confidentiality Trust	C trusts T to maintain confidentiality of the data or information that C provides to T.
Functional Reliability Trust	C depends on the functional correctness and reliability (including availability) of a product or service provided by T. C trusts T that T will maintain a reliable and functional product or service in the fashion that C requires.
Remote Access Trust	C trusts T with access to resources under the control of C and requires that T neither abuses the granted access nor extend it to third parties.
Authenticity Trust	C trusts T that any communication from or to T is

Class	Meaning
	proven to originate from the respective sender and cannot be generated by a third party.
Non Repudiation Trust	C trusts T that neither T nor C can deny data sent or received. The proof can be archived for future use.
Minimum Latency Trust	C depends on a functionality operated by T that requires minimum latency. C therefore trusts T to make sure there are only minimal delays.
Technical Security Trust	C trusts T with securing an infrastructure T operates providing services for C and making sure the infrastructure stays secure.

Table E4 Description of the Trust Relations

Object	Description
Access Keys	These trust relations are concerned with passing-on a copy of an access key of some sort. T is trusted with a key to allow T access to a cryptographically protected entity or communication.
Business Data	Business Data describes trust relations that require T to maintain confidentiality of data provided by C, since leaking this data would provide competitors of C with business intelligence usually not available.
Charged Tariff	The Charges Tariff object describes the dependency of the Service User on the correctness of the claimed tariffs from the EETS Provider. Apart from the EETS Provider's invoice and publicly communicated tariffs, the Service User has no possibility to validate the claims, which produces a trust relationship.
EETS Customer Rejection Blacklist	The EETS Customer Rejection Blacklist contains all EETS Customers that were rejected from one or more EETS Providers. [CESARE-III] explicitly requires that such customers cannot sign up with a different EETS Provider repeatedly. Therefore, a blacklist must be maintained and be trusted by all EETS Providers.
EETS Network	Several entities in the trust model are trusted with different extends of access to the EETS Network to access EETS internal services.
EETS Withdrawn Guarantees	According to [CESARE-III], an EETS Provider can withdraw his payment guarantees to a single Toll Charger until a settlement is reached. Toll Chargers need to look up potentially withdrawn

Object	Description
	payment guarantees when a Service User of an EETS Provider enters their road network and must trust the lookup result.
Email Platform	Email communication for Service Users is explicitly required by [CESARE-III]. Each email communication involves at least two Email service providers, whose infrastructure must be trusted if contractual binding activities are performed using email.
Intellectual Property Protection	Several entities (C) will open intellectual property to other entities (T) in the process provisioning or compliance certification. T must be trusted with the confidentiality of the intellectual property.
Legal Correctness	This trust object relates to the Contract Model Provider or the Interoperability Management group. Users of the model contracts must trust in the legal correctness of the same in order to use them.
Legal Execution	This trust object applies to all entities that outsource or sub-contract parts of the EFC operation.
Map Data	Electronic map data must be relied upon but cannot be easily verified, which makes C trust T with the correctness of said data.
Non-Interference	In the case of a pure National TC, the same must trust all EFC implementations on the road network as well as OBEs to not interfere with his system, since he has no influence in the EFC side.
OBE Compliance Detection	OBE Compliance Detection is a feature required by [CESARE-III] to be present in RSE and Enforcement equipment. This compliance detection must be relied upon to work correctly, which introduces a trust relationship covering this object.
OBE Hardware	The OBE Hardware needs to be trusted by several entities in the model.
OBE Hardware and Software	OBE Hardware and Software is a differing trust object to pure OBE Hardware, since it describes the functional unit as a whole. This unit is trusted by several entities in the model.
OBE Rejection Blacklist	Toll Chargers are according to [CESARE-III] able to reject OBEs that were found non-compliant or malfunctioning. [CESARE-III] also requires a blacklist mechanism to deal with such cases,

Object	Description
	which makes this blacklist an important trusted object.
OBE Vehicle Data	Several mechanisms for toll charge calculation rely on the vehicle data declared by the OBE.
Payment guarantee without prior transaction	This trust object is required by [CESARE-III] and guarantees the Toll Charger payment even if he cannot prove road network usage due to missing transaction records. This is a huge trust from the EETS Providers towards the Toll Charger, since it would allow massive fraud from the later.
Personalization Issue Prevention	This is a trust object extended by the EETS Provider towards its peers performing personalization of an OBE, since [CESARE-III] requires that the EETS Provider is responsible for any loss of revenue that would affect Toll Chargers due to incorrectly personalized OBEs.
Protection Mechanisms	Several data protection mechanisms are used in the EFC model. These mechanisms are to be trusted by most entities in the model.
RSE Functionality	Correctly functioning Road Side Equipment is one of the base trusts in the EFC model.
SMS Delivery	[CESARE-III] requires communication from the EETS Provider towards his Service Users using SMS. The integrity of the delivery mechanism as well as timely delivery must be trusted.
SSL Certificate Security	All entities using standard Internet technology protection mechanisms will rely on the security of their SSL Certificates.
Service Payment	This is a special trust object in the case of an independent National TC, who cannot verify the service use by EFC users and must trust the EFC Toll Charger to actually pay for his share.
Settlement	Parties requiring settlement from the Interoperability Management must trust in the same to perform fair arbitration.
Smart Card	[CESARE-III] explicitly requires Smart Cards as an option for Service User identification towards the OBE. Therefore, the Smart Card is a highly trusted object.
Standard Compliance	Compliance with the standards set forth for EFC is one of the basic assumptions of the EFC model and therefore a base trust

Object	Description
	object.
TC Registration List	Several entities must trust their current understanding of registered and EFC compliant Toll Chargers. Every Toll Charger appearing in this list automatically has in example a payment guarantee from all EETS Providers.
Tariff Data	Tariff data and settings are one of the central trust objects in the EFC model.
Transaction Source	This object must be trusted in from EETS Providers fulfilling the requirements of [CESARE-III] regarding anonymous ATM payments.
User Data	User Data is an object the Service User initially trusts the EETS Provider with, who in turn will pass user data partially on to other entities.
Vehicle Data	This trust object describes vehicle data before it is implemented in the OBE by personalization.
Web Platform	[CESARE-III] requires the entities to allow communication to the Service User via WWW. Therefore, the web platform must be trusted.

The identified trust relations between the organizational entities are shown in graphical form in Figure 4.

The identified trust relations are assigned to Trust Classes which helps to reduce complexity of the process to identify adequate organizational and technical measures to establish the trust.

Table E5 Caption to Class Mapping

Object	Class
Access Keys	Secure Key Trust
Business Data	Data Confidentiality Trust Authenticity Trust
Charged Tariff	Minimum Latency Trust Non Repudiation Trust
EETS Customer Rejection Blacklist	Minimum Latency Trust Data Integrity Trust Authenticity Trust
EETS Network	Remote Access Trust Technical Security Trust
EETS Withdrawn Guarantees	Data Integrity Trust Minimum Latency Trust Authenticity Trust

Object	Class
Email Platform	Data Integrity Trust Technical Security Trust
Intellectual Property Protection	Data Confidentiality Trust
Legal Correctness	Non Repudiation Trust
Legal Execution	Function Reliability Trust
Map Data	Data Integrity Trust
Non-Interference	Functional Reliability Trust
OBE Compliance Detection	Functional Reliability Trust
OBE Hardware	Functional Reliability Trust
OBE Hardware and Software	Data Integrity Trust Data Confidentiality Trust
OBE Rejection Blacklist	Data Integrity Trust Minimum Latency Trust Authenticity Trust
OBE Vehicle Data	Data Integrity Trust Data Confidentiality Trust
Payment guarantee without prior transaction	Non Repudiation Trust
Personalization Issue Prevention	Functional Reliability Trust
Protection Mechanisms	Functional Reliability Trust Data Integrity Trust
RSE Functionality	Functional Reliability Trust
SMS Delivery	Minimum Latency Trust Data Integrity Trust
SSL Certificate Security	Data Integrity Trust Secure Key Trust
Service Payment	Non Repudiation Trust
Settlement	-
Smart Card	Technical Security Trust Secure Key Trust
Standard Compliance	-
TC Registration List	Data Integrity Trust Minimum Latency Trust Authenticity Trust
Tariff Data	Data Integrity Trust Non Repudiation Trust
Transaction Source	Functional Reliability Trust Data Integrity Trust
User Data	Data Confidentiality Trust Data Integrity Trust
Vehicle Data	Data Confidentiality Trust Data Integrity Trust Functional Reliability Trust

Object	Class
Web Platform	Technical Security Trust Functional Reliability Trust

Table E6 describes the trust relations between technical entities of a assumed physical architecture as shown in.Figure 5.

Table E6 Description of Technical Trust Relations

Object	Description
Access Keys	In the technical trust model, entities trust each other with master- or derived access keys, which become a trust object.
Enforcement Data	Enforcement Data must be relied upon and the trust put into it must be secured in the technical model.
Map Data	Map Data is essential to be trusted upon for EFC operation.
OBE Config Data	OBE configurations are essential to be trusted upon for EFC operation.
OBE Payment Transactions	The OBE Payment Transactions are the most important trusted object.
OBE Position Reporting	OBE Position Reporting is a trust object in GNSS operations of EFC.
OBE Software	The OBE Software must be trustworthy and integrity protected.
OBE Status	OBE Status messages must be trusted.
RSE Config Data	Configuration Data transmitted by the RSE must be trusted.
Service User Data	Service User Data falls under data protection and privacy considerations and is therefore a trust object.
Tariff Data	Tariff Data must be relied upon by participating EFC entities.
Vehicle Data	Vehicle Data must be trusted for EFC operation to work correctly.

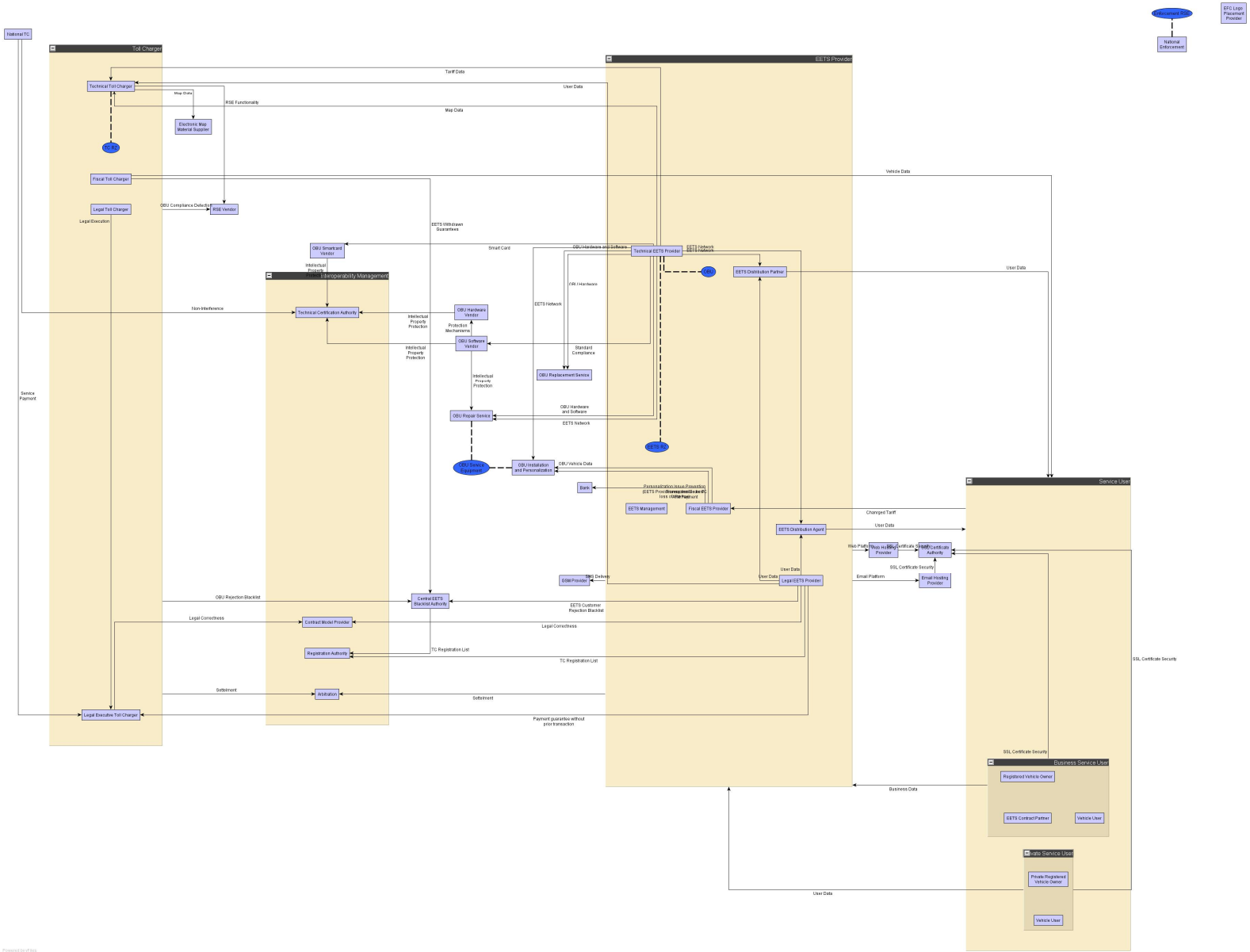

Figure 4 Trust Entities and Relations

(Print this graph on A3 or enlarge on-screen to view details)

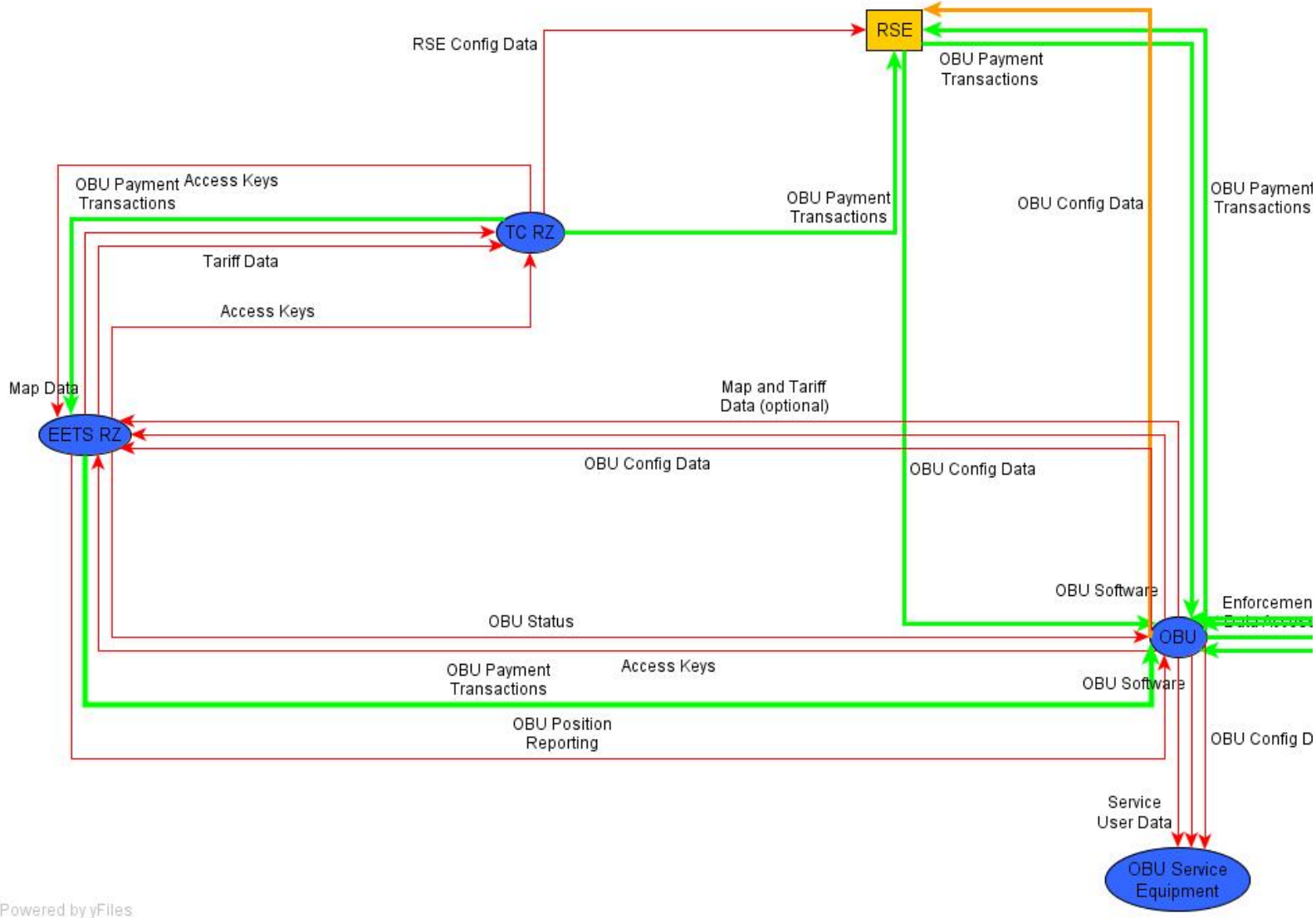

Figure 5 Technical Trust Entities and Relations

ANNEX F EMV

F.1 INTRODUCTION

EMV is a global standard describing the use of chip technology for payment cards (debit cards, credit cards, and ATM cards). As a result, payment cards will become less susceptible to fraud through skimming, hence reducing fraud costs and maintaining customer confidence in electronic payments. EMV leads to further standardisation of interfaces, chip platforms and interchange models will lead to more open payment infrastructures and therefore more open specifications.

This is comparable to one of the challenges the EC will face when specifying an open infrastructure for pan-European automatic toll collection. An open infrastructure from this respect means a situation where multiple Toll Chargers can securely offer their services to customers of different EETS Providers.

For compliancy reasons, it is important that transactions are traceable and digitally signed in case of disputes. Within an EMV payment scheme, key management principles and policies have been defined carefully as part of the security architecture. An automatic toll collection environment has similarities with an EMV payment environment regarding the need for (identification) transactions being traceable and genuine, and the large number of parties involved. This annex describes the roles and responsibilities involved in an EMV payment scheme and the basic elements of the security architecture.

F.2 EMV PAYMENT SCHEME IN GENERAL

F.2.1 Layers in the EMV-scheme

In a nutshell an EMV payment can be described as a cardholder inserting his card in a merchant's terminal in order to perform a payment transaction. During this transaction, data is exchanged between the chip on the card and the terminal of the merchant to verify each other's identity using certificates and corresponding keys (offline data authentication using asymmetric cryptographic functions, to be explained later on). Part of this chip data including a digital signature based on transaction details is send to another party involved in the scheme (e.g. the bank that issued the card) for verification and authentication purposes (online data authentication using symmetric cryptographic functions, to be explained later on). This party either authorises or declines the transaction, and sends this result back to the terminal. Afterwards, for example end of the day, the transaction data are sent to the banks involved for clearing and settlement purposes.

Taking a closer look at this EMV payment, it shows that it can be divided into separate layers, as illustrated in figure 1. Each layer handles different aspects of the above described payment transaction. These layers are:

- Physical layer, where the actual (physical) transaction takes place. The card is inserted in the terminal, and goods or services are being handed over.
- Technical layer, where the authorisation en authentication messages are being send.
- Financial layer, where clearing and settlement of all transactions takes place.

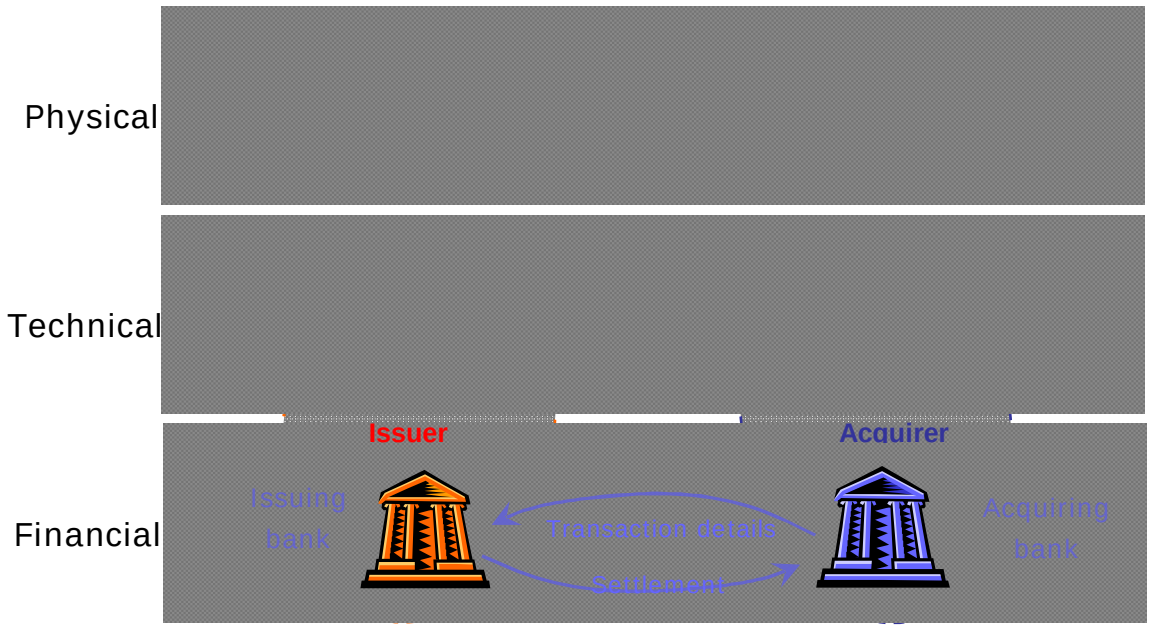

Figure 1 EMV payment scheme

Within this scheme, several parties are involved. These parties, their roles and responsibilities within the EMV scheme are discussed in the next chapter.

F.2.2 EMV Actors

F.2.2.1 Roles & Responsibilities

As depicted in figure 1, the roles within the EMV payment scheme are:

- Cardholder
- Issuing bank
- Card Processor / Authorisation of transactions
- Merchant
- Acquirer / Switching of transactions
- Acquiring bank
- Scheme operator

Parties involved in the scheme can have more than one role. On the other hand, one role can be fulfilled by one or more parties at the same time.

Cardholder & Merchant

The role and responsibilities of these actors are trivial and therefore not discussed here.

Issuing bank

- issues cards that comply to the rules of the scheme provider to cardholders
- contracts and bills cardholders
- pays a fee to the scheme operator that licences the issuer to issue scheme branded cards to his cardholders

Card Processor / Authorisation

- verifies payment authorisation requests
- authorises payment transaction

Acquirer / Switching

- contracts merchants for accepting scheme transactions
- is responsible for providing Card Acceptance Devices (CAD's, referred to as terminals) with CA public keys to merchants
- guarantees payment to the merchant of the transactions using this CAD
- pays a fee to scheme operators which licence the acquirer's acquiring bank to accept their scheme transactions
- sends clearing information to card processor

Acquiring bank

- maintains merchant accounts for his merchants

Scheme operator (e.g. Visa, MasterCard)

- Responsible for
  - Maintaining network infrastructure
  - Financial clearing & settlement (clearing house and / or settlement bank)
  - Member and vendor relations
  - Product specifications
  - Marketing of brand

F.2.2.2 Liabilities

Whenever one of the parties involved is not EMV-compliant, or does not act according to the rules and standards provided by the scheme operator when performing a transaction, this non-compliant party is accountable (liable) for this particular transaction.

F.2.3 Security architecture of EMV

F.2.3.1 Used cryptographic functions

Several types of cryptographic functions exist. Two types of functions are of interest in this memo. These two types of cryptographic functions are:

- Symmetrical functions, where the key of the sender and receiver is the same key, and the same key is used for encipherment and decipherment.
- Asymmetrical functions, where the key of the sender and receiver are different keys. Different keys are used for encipherment and decipherment (private key and public key known as key pair). Storing a public key is inexpensive.

Both types of functions can be used for encryption / decryption and digital signatures. However, both types have different characteristics for use in different environments.

EMV supports these two types in its two methods for authenticating that a card is valid and that the data on the card has not been altered. These authentication methods are online data authentication and offline card authentication.

Online data authentication takes place in the technical layer. During online data authentication, the digital signature over an EMV authorisation request is generated by the card using symmetrical cryptography, using a symmetric (TDES) key. This key must be distributed to all parties using the algorithm, before it can be used. Within EMV, the parties in need of this key are the issuer and the card only. The EMV terminal, acquiring host, and acquiring network are fully transparent for this data. However, for successful transactions the terminal should also store this signature generated by the card that can be verified by the issuer as evidence of the validity of the completed transaction (e.g. in case of disputes).

Offline card authentication takes place in the technical layer. During offline card authentication asymmetrical cryptography (RSA) is used. The terminal verifies the issuer certificate stored on the card, using the scheme operator's (CA) public key. Certain cards are also capable of creating RSA signatures using their own private key and corresponding certificate. This allows dynamic offline card authentication, which provides a much higher level of security than a static proof (signature over fixed data). In the case of dynamic authentication however, the card should contain a (crypto-)processor capable of RSA calculations.

A third cryptographic function type is "one way" functions, like SHA-1. This results in a check sum. From this check sum, the original message can not be derived. If the message used as input for the checksum is altered, the check sum calculated from the original message will not be valid anymore. EMV makes use of this third type of function as well.

F.2.4 Justification for PKI solution

As mentioned above, EMV uses both symmetric and asymmetric cryptographic functions. Symmetric keys are easy to generate and can be used to encipher large amounts of data. However, they are not easy to distribute, since every party shares the same key. Therefore, there is no distinction between parties, and thus no absolute confidentiality and authenticity. For symmetric keys, parties really need to know and trust each other. Each communicating pair of entities is to have its own key. This results in complex key management when many parties are involved.

Within the EMV payment scheme a lot of parties are involved that are not always familiar with each other. For these parties it is necessary to have certainty on the identity and solvency of parties and on the integrity, confidentiality, origin and receipt of a message.

A Public Key Infrastructure (PKI) is a solution to provide this certainty. It is a combination of techniques used, standards, legislation, and procedures/policies that apply (roles and responsibilities)

Therefore, EMV uses a PKI solution (based on RSA) as well due to its less complex key management:

- Keys are easy to distribute
- Public keys are always available
- Public keys do not require to remain secret
- Each party has its own key pair. Obviously, the private key has to be kept secret by the owner.

The disadvantage is that keys are less easy to generate and they are not suitable for large amounts of data.

Within an EMV scheme, symmetric keys are only used for signing en encrypting data exchanged between the card and the issuer.

F.2.5 How does it work?

In a PKI, keys come in pairs, a public one which can be widely distributed, and the other one, the private key, needs to be kept secret by its owner. Although the public does not need to be kept confidential, the receiver of the public key must have some certainty that this key indeed belongs to whom it claims to belong to. This problem is usually solved by using certificates.

A certificate consists of a public key and related data (including the name or identifier of a party and a validity period) with a digital signature attached. This digital signature is generated by an overall trusted party, the Certification Authority (CA). This CA distributes its public key to other parties. Any party having a copy of the CA public key can then verify all certificates generated by that CA.

The EMV public key certification scheme is illustrated in figure 2. Within the EMV scheme, the scheme provider will act as the CA. It creates certificates for each issuer by signing the issuer public keys with the CA public key. This process of certificate generation must be reliable, since identity and key pairs are coupled by means of certificates.

The CA public keys will be distributed to the terminals through the acquirers in order to verify the issuer certificates. Verifying the issuer certificate provides the issuer public key and assurance about the origin and authenticity of the card.

If the card is equipped with asymmetric capabilities, it may contain a card public key certificate (and the corresponding key pair). This certificate is signed by the issuer with the issuer private key. When the terminal retrieved the issuer public key by verifying the issuer certificate, the terminal can validate the card's certificate as well and can obtain the card's public key.

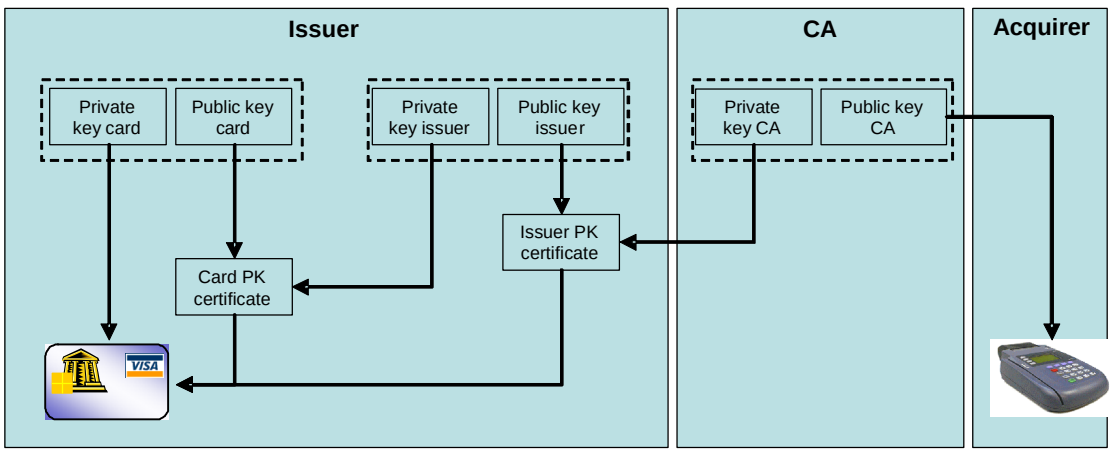

Figure 2 EMV public key certification scheme.

F.2.6 Processes involved

Within the security architecture, various key and certificate-related processes are involved. Key management is the process of:

- verifying an identity
- creating keys (DES, TDES, RSA pairs)

- generating certificates
- distributing keys
- revoking keys

Several roles within the EMV scheme are responsible for these key management processes.

Scheme operators

- verify the identity of issuers and acquirers
- manage the CA public key pairs:
    - create CA secret key and store it in a HSM (host security module)
    - make public key available to acquirers
- sign issuer public key certificates

Acquirers

- distribute CA public keys to terminals
- manage symmetric keys for PIN encryption, PIN decryption, and PIN re-encryption

Issuers

- asymmetrical keys
    - manage issuer public key pair:
        - create issuer key pair
        - store issuer private key in HSM
        - obtain issuer public key certificate from scheme operator
        - sign card data with issuer private key
    - manage card key pairs
        - create unique public key pair for each card
        - create card public key certificates for each card asymmetrical keys
- generate and manage and store (issuer and card) symmetrical keys

Parties have to make sure that they have systems and processes in place to prevent compromising private RSA and DES keys and systems, and processes involved.

ANNEX G HIGH-LEVEL RISK ANALYSIS

G.1 INTRODUCTION

This threat analysis is performed at a high level of abstrac tion, to keep away from implementation aspects that are yet unknown and that will strongly influence the way in which certain attacks can be realised, their likelihood, resulting possible damage and possible countermeasures. Threats are described in a way that they are largely independent of a specific system concept. The drawback of this approach is that a balanced assessment of the severity of risks is not possible. Identified items tend to refer to vulnerabilities rather than concrete threats.

Some threats do not need to be catered for on an EETS level, but are suggested to be left to the responsibility of individual actors (EPs or TCs). This is explicitly indicated in the tables.

Threats are grouped by the domain in which they occur. The domain does n ot in all cases coincide with the responsible party. Service User and EETS Provider risks are combined in one table.

An explanation of the fields in the tables is given below.

Nr	Description of damage	Possible attacks causing the damage (not exhaustive)	To be addressed in EETS definition ?	Severity	Countermeasures (not exhaustive)	Comments
Identifier of threat (domain abbreviation + sequence number)	Damage that may result.	Attacks corresponding to the threat	Yes or No. This classification	High/Low/Medium. This is a rude estimation for the product of likelihood and damage of a threat.	Countermeasures that will help to reduce the risk.	Any further remarks relating to the threat or its environment.

G.2 RISKS IN THE EP AND SU DOMAIN

Notes:

- The role Ser vice User aggregates different roles:

  - Vehicle Registration Holder
  - One Liable for Toll
  - Driver
  - EETS Contract Holder.
- Toll declaration: report of usage sent to the TC, signed by the EP/OBE. In case the OBE reports to the TC directly, the Toll declaration is equal to the OBE declaration.
  - OBE declaration: charge related data as sent by the OBE to a back office, (TC or EP).

Nr	Description of damage	Possible attacks causing the damage (not exhaustive)	To be addressed in EETS definition ?	Severity	Possible measures (not exhaustive)	Comments
EP1	Fees cannot be collected from SU – loss of income	SU does/can not pay his bill, and follow up ineffective.	No	Medium	EP may require certain guarantees from new customers	Responsibility of individual EP.
EP2	Toll Charger is overcharging – EP suffers loss of income or has disputes with SU	TC sends (on purpose) false/erroneous payment claims to EP	Yes	Medium	• Backoffice charging process subject to certification and audit. • OBE declaration provided with proof of integrity, authenticity and non-repudation. • EP should have access to OBE declaration data (always or on request).	
EP3	Wrong fixed vehicle characteristics declared (characteristics in OBE do not match vehicle in which it is used) – loss of income or enforcement	• EP Personnel enters erroneous data in personalisation process. • OBE used in wrong vehicle.	Yes	Medium	To be implemented by EP • Entry of vehicle characteristics in OBE only by authorised personnel, entry protected with data origin authentication measures. • EP data entry process subject to certification and audit.	One Liable for Toll is in the end responsible to declare the right vehicle characteristics. The EP is however responsible for vehicle characteristics entry. Measures to safeguard integrity of OBE resident data, and to ensure correct entry are EP responsibility.
EP4	Wrong dynamic vehicle characteristic used	SU uses manual indication (e.g. trailer presence)	No	Medium	Check on vehicle characteristics is part of individual TC responsibility for enforcement.	SU is responsible for correct declaration of vehicle characteristics.

Nr	Description of damage	Possible attacks causing the damage (not exhaustive)	To be addressed in EETS definition ?	Severity	Possible measures (not exhaustive)	Comments
	- possibly loss of income to TC or enforcement event.	incorrectly.				
EP5	Unauthorised disclosure or use of customer/travel-related data – privacy infringement	Interception of declaration data from OBE or Payment claim from TC or stored data at EP premises.	No	High	• Encryption of personal data exchanged over open networks. • Separation of processing domains. • No more data kept than necessary for the purpose – and no longer than necessary. • Access to personal data only by authorised personnel on need-to-know basis. • Access to personal data subject to audit trail.	The proper handling of personal data is the responsibility of the entity who is to be seen as the 'controller' of these data, as defined in 95/46/EC. Each controller will have to comply with applicable national legislation on processing of personal data. EP's will obviously qualify as controllers of personal data.
EP6	Non-available or incorrect raw data from OBE sensors – loss of income to TC.	E.g. GPS shielding or spoofing. Sabotage of sensors or modification of data from sensors.	Partly	High	• EETS OBE requirements should include detective measures against manipulation of sensors. • Enforcement / spot check policy is responsibility of TC – but the mechanisms are to be facilitated by EP / OBE.	This applies to autonomous OBE concepts (GNSS/CN) only.
EP7	Recording or declaration of incorrect data by the OBE – loss of income, complaints from SU or TCs	Modification of software or stored data in OBE, modification of declaration data or toll context data	Partly	High	• EETS OBE requirements shall include measures to maintain integrity and authenticity of all data and software.	
EP8	OBE malfunction because toll context data not available or incorrect – loss of income or	Communication of toll context data is obstructed, modified or made unavailable	No / Partly	Medium	• Basically this is a matter between EP and his Contract Holder, yet: • Minimum service levels should be part of EETS requirements on EPs	In the end, the one liable for toll is responsible for an accurate declaration / functioning equipment.

Nr	Description of damage	Possible attacks causing the damage (not exhaustive)	To be addressed in EETS definition ?	Severity	Possible measures (not exhaustive)	Comments
	enforcement of 'honest user'					
EP9A	False OBE – unjustified charges to existing SU or loss of income	OBE/SAM cloned, or fake OBE used	Yes	High	• EETS OBE requirements shall include measures to maintain integrity, confidentiality and authenticity of data and software. • Blacklisting.	
EP9B	Use of stolen OBE – unjustified charges to EETS contract holder.	OBE/SAM stolen and used by other person.	Partly		• Blacklisting. • A periodic on-line reactivation mechanism can be used to make an OBE dysfunctional within a certain time after reported loss.	Procedures to report OBE loss to EP can be left to individual EPs. A global rule on dealing with blacklists by EPs/TCs is important.
EP10	EETS not available for SU – SU dissatisfied	OBE is broken or power failure	Partly	High	• Basically this is a matter between EP and his Contract Holder, SLA included in the service contract between EP and Contract Holder, yet • Minimum service level requirements shall be part of EETS certification requirements on EPs	
EP11	EP systems not available for receiving claims – delay of clearing process	Attack on EP back-office systems (from outside or by personnel)	Partly	Low	• Basic service levels shall be part of EETS certification requirements on EPs	In case charging/position data are routed through EP Central Equipment.
EP12	Secret keys compromised – may lead to loss of income to Toll Chargers and or EPs	Several types of attack on devices storing keys, encrypted text exchanged and in generation process.	Partly	High	• Crypto-concept should require no or minimum central co-ordination. • Avoid sharing of secret keys between parties. • Storage of secret/private keys only in protected environment. Avoid sharing of secret keys between parties.	

Nr	Description of damage	Possible attacks causing the damage (not exhaustive)	To be addressed in EETS definition ?	Severity	Possible measures (not exhaustive)	Comments
					• Asymmetric crypto where possible. • Measures to limit damage and recover after compromise of keys.	

G.3 RISKS IN THE TC DOMAIN

Nr	Description of threat and damage	Possible causes (not exhaustive)	To be addressed in EETS definition ?	Severity	Possible measures (not exhaustive)	Comments
TC1	Fees cannot be collected from EP – loss of income	EP bankrupt	Yes	Medium	• Certification requirements on EPs should include financial stability.	This issue is not related to security, but has to be addressed.
TC2	No toll declarations received from OBE or EP – loss of income	Sabotage of communication, OBE or RSE	Partly	Medium	• EP Backoffice charging process subject to certification and audit. • EETS OBE requirements should include measures to maintain integrity of data and software. Data may be delayed but not lost before arriving correctly in backoffice.	TC enforcement should cater for the situation that a correctly operating OBE may not send an OBE declaration at a later time.
TC3	No/wrong recording of movement data – loss of income and/or enforcement of	Local GNSS jamming.	Partly	Medium	• EETS OBE requirements should include detective measures against manipulation of sensors or anomalous sensor input. • EETS OBE requirements may include additional sensors for dead-reckoning / detecting erroneous GNSS input.	To be covered by TC enforcement policy.

Nr	Description of threat and damage	Possible causes (not exhaustive)	To be addressed in EETS definition ?	Severity	Possible measures (not exhaustive)	Comments
	honest users					
TC4	Unauthorised disclosure of customer/travel-related data – privacy infringement	Interception of data exchange or disclosure of stored data at TC (by outsiders or personnel)	No	High	• Encryption of personal data exchanged over open networks. • Separation of processing domains. • No more data kept than necessary for the purpose – and no longer than necessary. • Access to personal data only by authorised personnel. • Access to personal data subject to audit.	The proper handling of personal data is the responsibility of the entity processing these data. This entity (here: a TC)will have to comply with national legislation on processing of personal data.
TC5	Loss of income due to TC's RSE or CE failure	Attack on TC RSE or back-office systems (from outside or by personnel)	No	High	Responsibility of TC	

G.4 RISKS IN THE IM DOMAIN

Nr	Description of threat and damage	Possible causes (not exhaustive)	To be addressed in EETS definition ?	Severity	Possible measures (not exhaustive)	Comments
IM1	Loss of income for Toll Chargers – because EETS Provider bankrupt	• Insufficient requirements on EETS Providers. • Errors in auditing or certification of EPs.	Yes	High	• Certification and audit process of EPs should include financial stability.	

Nr	Description of threat and damage	Possible causes (not exhaustive)	To be addressed in EETS definition ?	Severity	Possible measures (not exhaustive)	Comments
IM3	Erroneous OBE declarations – loss of income for TCs, complaints from SUs, or enforcement of honest users	EETS certified OBE incapable of fulfilling TC requirements (insufficient accuracy or functionality) as a result of insufficient or erroneous certification.	Yes	High	• EETS OBE requirements shall include accuracy/performance aspects to assert that required accuracy for a variety of toll environments is sufficient.	This is primarily an issue for the respective EP but listed here as it is caused by deficiencies of the EETS certification.

ANNEX H EVALUATION CARDME TRANSACTION BY BRIGHTSIGHT

Review of CARDME-4 for application in EETS

By

Jan Blonk, Lex Schoonen
Brightsight
The Netherlands

Date
February 8, 2007
Our reference
07-MEM-001

Brightsight has been asked by the Dutch Ministry of Transport AVV to review the suitability of the security part in the CARDME-4 version 3.0 (and systems based upon this specification, e.g. the WG11 system) for a pan European EETS. From this review it is concluded that in the opinion of Brightsight the CARDME-4 version 3.0 is not well suited for this purpose. To explain this a number of scenarios are described for which the CARDME-4 specification will not be adequate.

1 Introduction

The CARDME-4 version 3.0 has been designed to support Electronic Fee Collection (EFC) in a multi OBE-issuer environment, in which an OBE can communicate with roadside DSRC stations of different toll operators. The basis for the security of payment information is a symmetric cryptographic algorithm (DES), which is used to calculate "Issuer Authenticator" data and "Operator Authenticator" data.
The CARDME-4 version 3 security has been designed to support integrity in an environment in which a few 'loyal' and 'forgiving' issuer and operator organisations inter-operate. In the next paragraphs it is argued that CARDME-4 is not designed to operate in a larger pan European network.

2 What if an OBE is compromised

Lessons learned from the banking domain show that it is difficult to protect the OBE keys and that in spite of system security requirements and certification schemes system hacks do happen. Experience show that it is near impossible to design cost-effective equipment that offers complete protection for keys located inside the equipment. Due to this, it is imperative to consider keys that are physically located in untrustworthy domains - such as OBE's under control of civilians - to be vulnerable, and in result always ensure a realistic strategy is in place to detect key compromise and to mitigate the effects when such compromise occurs. Mature key management in the banking domain typically allow for scenarios in which network operators can replace keys in compromised systems.

Furthermore, keys are usually generated in such a way that compromise of a single key does not lead to compromise of the whole key base (so no system-wide replacement of equipment is required). In order to achieve said property it is difficult to imagine a strategy in which the four available key slots in the CARDMe-4 OBE are sufficient (see also the following under 4). A point worth noting is that compromise of a single OBE typically means compromise of more OBEs is imminent: most modern classes of attacks require a fair amount of effort, and investment, to achieve a first successful attack, but require significantly less effort for subsequent reproductions of the attack on other devices.

In a pan European environment it must be accepted that OBEs of different quality (with respect to security) will be issued in different regions. Again the banking domain is where this lesson is learned. In spite of the existence of a central agency for security requirement definition and certification, factors such as price competition, national interests, evaluating skills, certification periods versus periodically upgraded security requirements that lead to legacy issues, will cause an installed base in which OBEs of different security quality will be used. In a CARDME -4 version 3 network the risk of a low quality OBE will affect not just the issuer of that particular OBE but also all other parties. If the keys inside of the OBE can be compromised it becomes easy to create duplicates or derivatives of the OBE in question. Those duplicates or derivatives cannot directly be distinguished from bona fide OBE's, and as such will be accepted in all systems all over Europe. We foresee the potential development of a large pan-european market in hacked devices. The absence of an efficient key replacement mechanism greatly increases the potential damage related to this threat.

3 Is CARDME-4's dependency on mutual trust between parties a problem for the migration path?

This is where non-repudiation between the partners becomes an issue. The main reasoning here is that an attacker from country A that obtains the EFC Operator keys will be able to pass all toll gates in country B while pretending to travel under a contract issued in coun try C. This weakness provides the contract issuer from country C an excuse to never honor any transactions from operators in country B; the operator will claim they could have all been generated by fraudulent citizens from another country. Since the operat or has no access to the keys of the issuer, which, in itself, in a symmetric system, is a necessary requirement to obtain any meaningful level of security, the operator will not be able to prove this contract issuer wrong.
Given the fact that this property is system-wide, the above reasoning holds between all the partners in the system.
Furthermore, the CARDME system requires all operators to share a common set of master keys. In the symmetric cryptographic context used for CARDME this implies that each operator will be able to forge any set of data by impersonating any of the other operators. This renders the non-repudiation issues even more serious. Furthermore, it raises the required mutual trust between operators to unrealistic levels.

4 How helpful are the 4 keys stored in the OBE?

Each OBE can store 4 “Contract Issuer keys” and 4 “EFC Operator keys”. In the current specification these keys are in fact 4 different versions of the Issuer Key and the Operator Key. They allow for some flexibility in key m anagement. The actual keys to be used are selected by the roadside equipment by referring to the location of the key in the OBE’s key storage. As such this mechanism allows for gradual replacement of keys when a key has been compromised, but it does in no way improve security or limit a risk. Furthermore, the number of stored keys (4) is so low, that any scheme for gradual replacement of keys will suffer severe time constraints. Support for any replacement scheme will require sacrificing at least one key slot in order to maintain the service as the keys are replaced. Furthermore, in the most optimal implementation possible the card base is still only partitioned in four segments, which means any master key compromise will result in the forced (key or card) replacement of at least one quarter of the installed card base (apart from the obvious action of replacing keys in all road side equipment).
The fact that in this system the keys in all components throughout Europe have to be replaced when fraud is detected anywhere in the Communityputs an extremely serious strain on the entire system, which should be carefully considered by EETS decision makers.

5 Quality of he roadside systems

In addition to the previous, all of the observations considering the security quality of OBE’s also hold for the road side equipment. It seems unlikely that all the road side equipment will be sufficiently tamper proof to prevent compromise of one or more keys that are located in

that equipment. Since those keys are used to check al l passing traffic, and the fact that they are symmetric, a successful attack on those keys will provide the attacker the possibility to emulate all the data that allows him to pass road side equipment in all countries in the manner explained earlier preten ding to travel under contract of a foreign issuer. Essentially, this means that compromise of a single unit results in a system -wide security breakdown.
In the EETS context, there is the additional concern that the chain is as strong as the weakest link: t he security level achieved is as high as that of the least tamper -proof road side device. Due to this, it is highly advisable to consider public key solutions, where the road side equipment does not have to contain extremely sensitive information such as s ymmetric master keys. (note that using public key solutions does not imply that the road side equipment need no security at all; it is probably still interesting to sabotage the equipment)

6 How to improve the system security

The dominant security princi ple for a secure pan European EETS should be that poor quality OBEs issued by one Issuer, or poor quality roadside equipment in use by one Toll Operator, should not lead to increased risk for all other actors. This leads to the requirement that each actor should be protected by his own secret key, with no need to share those keys with other parties. To master the complexity of the resultantly required key management, solutions based on asymmetric cryptography should be adopted in a CARDME -4 improved system .