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

File name:	EG 11 - DSRC Transaction - Issue 1 - 6feb06
Status:	Final. Issued to EFC Expert Group
Document nature:	Draft report endorsed by DG TREN
Dissemination level:	EFC Expert Group
Date of issue:	6 February 2006
Contact persons:	Bernhard Oehry Rapp Trans AG, Basel, Switzerland Tel: +41 61 335 7846 Fax: +41 61 335 7700 Email: bernhard.oehry@rapp.ch Philippe Hamet DG TREN Tel : +32.2.295.18.61 Fax : +32.2.296.53.72 Philippe.hamet@cec.eu.int

CONTENTS

1. OBJECTIVES AND SCOPE

1.1 MOTIVATION AND BACKGROUND

Article 2.2 of Directive 2004/52 on The European Electronic Toll Service asks for a service that enables a road user to travel on all tolled highways in Europe and only require one OBE. It states:

> "2. (…) Operators shall make available to interested users on-board equipment which is suitable for use with all electronic toll systems in service in the Member States using the technologies referred to in paragraph 1 and which is suitable for use in all types of vehicle, in accordance with the timetable set out in Article 3(4). This equipment shall at least be interoperable and capable of communicating with all the systems operating in the Member States using one or more of the technologies listed in paragraph 1. The detailed arrangements in this respect shall be determined by the Committee referred to in Article 5(1), including arrangements for the availability of on-board equipment to meet the demand of interested users."

For DSRC based charging systems most aspects of the data exchange between road side equipment and on-board equipment have already been harmonised by initiatives including CESARE, PISTA, CARDME and MEDIA. All these specifications are based on the 5.8GHz DSRC standards produced by CEN TC278. However, some choices still remain open and it is also a requirement of the Commission that the EETS accommodates the Italian Telepass system.

This document provides a common definition of the data exchange over the DSRC interface for central account based charging. The document is intended to provide a basis for agreement of this definition between Member States for inclusion in the EETS.

1.2 TASK OF EXPERT GROUP 11

Expert Group 11 has received the following task description from the Commission:

> Expert Group 1 has promoted the idea of a single European EFC application for the European EFC service based on microwave technologies. This idea seems to be well accepted by the majority of the EFC Expert Group.
>
> The basic aim of the EG 11 is now to define the general specifications for this Application. It might start from the achievements of such European projects as CARDME, MEDIA, CESARE. Its report will be submitted to the Regulatory Committee created by the Directive 2004/52/EC, thru the "EFC Expert Group". It should coordinate its work with the project CESARE III.
>
> Furthermore, it will study the requirements for security of the transactions, and especially the question of security keys.

1.3 OBJECTIVES

The tariffs applied to road users and the rules for their application differ between EFC operators across Europe. For example, some charge on the basis of the number of axles while others do not. A key role for this specification is to set out all the data required in an OBE to enable it to exchange data that will satisfy every European operator.

Expert Group 11 covers two objectives:

Create the basis for discussion and agreement by Member States

The document is intended for a consensus finding process. Hence all proposed specification elements shall be explained and motivated.

Make a complete specification for charging on DSRC

The proposed specification shall be complete in the sense that it contains a full definition of the DSRC interface of the EETS for DSRC based charging systems.

The first objective is covered by the step-by-step development of the specification in the main body of the report, and the second objective is covered by the specification of the EETS DSRC transaction in Annex A.

1.4 SCOPE

This document specifies the DSRC interface of EETS compatible on-board equipment regarding charging and enforcement:

- The specification is intended for DSRC–based charging systems. Other uses of the DSRC interface, e.g. for enforcement in GNSS/CN systems or for value added services, are not covered.
- For DSRC-based systems the specification covers the DSRC data transfer for both charging and enforcement purposes.
- The specification is for the EETS. The EETS is considered to be an additional service that is not intended to replace national services or specifications.

1.5 RELATION TO OTHER WORK

EG 11 has used the following projects and documents as basis for its proposal:

- The requirements stemming from the Interoperability Directive 2004/52/EC
- European projects CARDME, PISTA, CESARE (which include the results of previous projects, such as A1 and MOVEit)
- The interoperability initiative MEDIA
- National EFC specifications
- The CEN TC 278 DSRC standards (Layer 1, Layer 2, Layer 7 and Profiles)
- The UNI DSRC standards (UNI 10607-1/2/3/4:2006)
- The CEN TC 278 standards on EFC: EFC Application Interface Definition, [EN 14906], and the draft standard on an Interoperable Application Profile for DSRC, [EFC IAP]

The output of EG 11 is intended to be used:

- for discussion and agreement in Comité Télépéage to become annexed to Directive 2004/52/EC as part of the EETS service definition
- as an input to CEN TC278/WG1 for the ongoing work on the Interoperable Application Profile standard in order to harmonise the two documents and for enabling a common European implementation

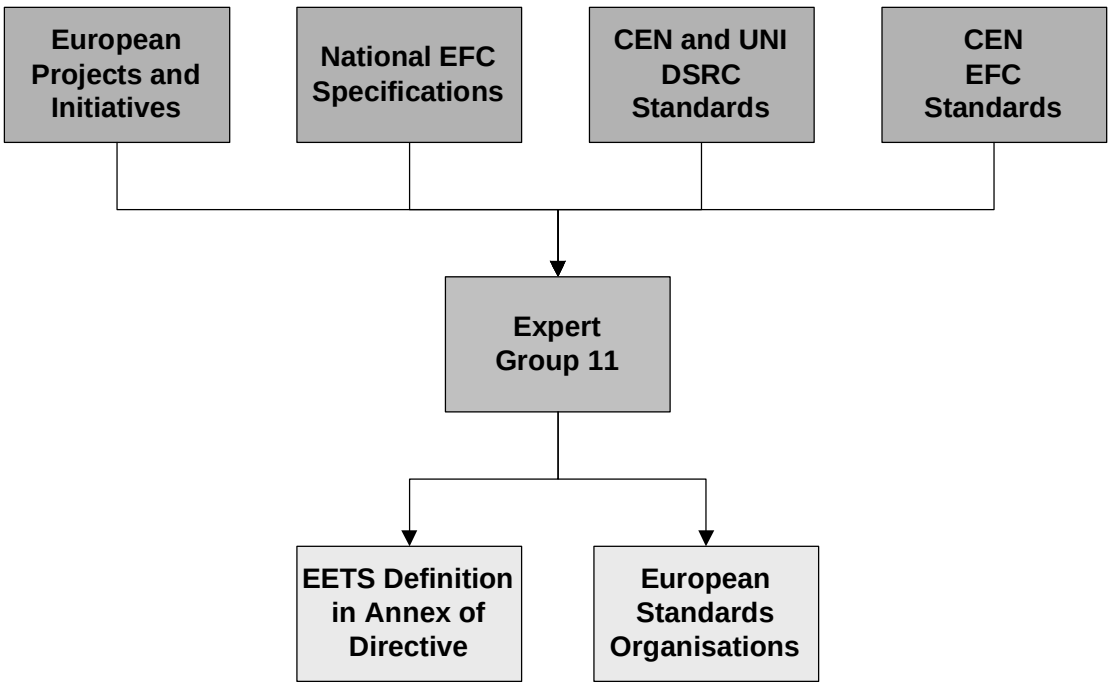

Figure 1: Relation of EG 11 to other work

The output of EG 11, i.e. the DSRC transaction specification, is given in ANNEX A.

[R 1] The specification given in Annex A of this document should be accepted as the technical basis of the EETS for DSRC based charging systems.

[R 2] This specification should be forwarded as input to European Standardisation.

2. PRINCIPLES

2.1 HIGH LEVEL REQUIREMENTS

General Framework

Vehicles using infrastructures and services subject to toll charging are equipped with an OBE able to manage a “single European application”. OBEs are delivered to the service user by European EETS Providers in the frame of a contract binding service user and EETS Provider.

A contractual framework is to be set up between EETS Providers (or Contract Issuers) and Toll Chargers (or EFC Operators) in Europe. In this frame OBEs are accepted by the Toll Chargers for payment of toll charges.

The amount of toll may depend on the used toll section (or bridge, tunnel, parking, …), on the time of its usage, and on the measured and/or declared vehicle data (weight limits, height, number of axles, Euro Class, …).

Toll charges are calculated by the roadside system using information received from the vehicle’s OBE through the DSRC interface. The OBE does not calculate the fee. It provides stored information to the roadside equipment.

DSRC transactions (entry transaction, transit transaction, payment transaction, enforcement transaction, etc.) can be performed for all types of vehicles (private cars, light commercial vehicles, motorcycles, trucks, busses) in various contexts:

- EFC lanes with or without barriers
- Free flow context (beacons on gantries or on road side supports)
- Motorways in open and closed toll system configuration
- Tunnels, bridges, ferries
- Parkings
- ….

Interoperability Issues

The DSRC application for the EETS shall cover all national requirements.

EETS OBE shall support a single EETS DSRC application on two radio interfaces, according to

- the CEN DSRC 5.8 GHz standards and
- the UNI DSRC standard (for Italy only).

The DSRC application shall enable equal treatment and non discrimination between EETS users and national users.

The DSRC application shall cover all situations when a vehicle equipped with an EETS OBE is driving on a tolling infrastructure.

The EETS DSRC application shall require minimal change to existing RSE equipment and central systems. However, software upgrades will be necessary in some systems.

The performance, especially regarding transaction time, shall be suitable for all existing DSRC contexts.

The application shall be able to cope with the scale of the EETS service, which might be very large, with a high number of actors in Europe (hundreds of Toll Chargers, tens of EETS Providers, tens of millions of vehicles).

The application security shall be adapted to the increased threats arising from a European-scale service.

2.2 CESARE MODEL FOR INTEROPERABILITY

CESARE III is a European project that develops the contractual and procedural aspects of the EETS. CESARE III works from the following abstract model of actors regarding interoperable fee collection:

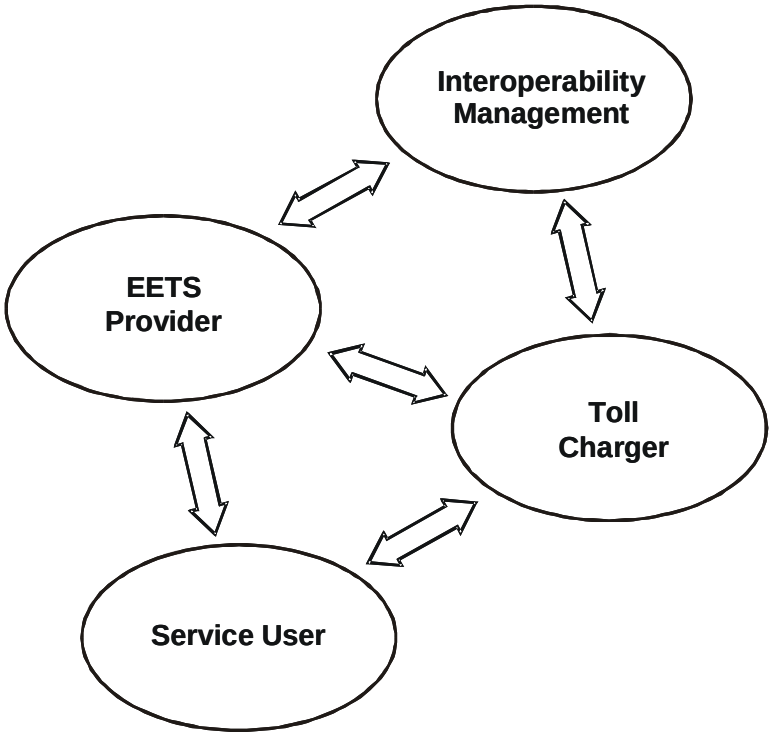

Figure 2: The CESARE model

The abstract actors in the CESARE model consist of several sub-actors and roles, e.g.

- the Service User domain contains the Driver, the Haulier, and the Vehicle Owner
- the Toll Charger contains the EFC Operator and the Transport Service Provider
- the EETS Provider contains the Contract Issuer and the Payment Means Provider
- the Interoperability Management contains laws and regulations, the EFC Expert Group, standardisation, framework agreements, and the management of system-wide identifiers and security keys.

Internal details of these actor domains are not important for the purpose of this specification. It is sufficient to know the interaction between the actor domains, i.e. the basic processes and the contents of the information exchanges. EG 11 uses the CESARE model and the associated processes for its definition of attributes and security provisions.

3. PROCESSES

The following process descriptions define the requirements of the DSRC transaction. Only processes that influence the information exchange on the DSRC are described. The processes are based on draft material from the projects CESARE III (WP 2 and WP3), RCI (WP1 and WP3), and MEDIA.

3.1 OBE PROVISION

- The EETS Provider obtains OBEs compatible with this specification from the open market. The OBEs shall be certified for EETS compliance. It is assumed that European Standards Organisations will create a test suite that accompanies the IAP [EFC IAP] and also provide tests for the complete DSRC stack including electromagnetic compatibility. Certification for EETS compliance will make use of these standards. It is expected that other groups and projects will define the details of the EETS certification process and also define further requirements, like environmental conditions for OBE (temperature and humidity range, vibrations, etc.).
- The user enters a contract with the EETS Provider. The EETS Provider sets up a user account that is identified by a unique Personal Account Number, PAN. Service User and EETS Provider agree on the mode and conditions of payment.
- The EETS Provider personalises the OBE with the required Contract, Payment, Vehicle, Equipment and Security data. The personalisation interface is not defined in this specification and is left to the EETS Provider to define.
- The user is responsible for the correctness of the Vehicle data given to the EETS provider for personalisation of the OBE.
- The EETS Provider must guarantee that personalisation data can only be changed by persons authorised by him. The EETS Provider is responsible for this against the Toll Charger. Ideally, compliance testing for the EETS includes certification of the personalisation interface with a given level of access protection. Note that personalisation might also make use of the DSRC interface.
- The EETS Provider provides the OBU to the Service User

[R 3] The European Commission (DG TREN and DG ENTR) intend to establish a mechanism to maintain this specification in harmony with European Standards.

[R 4] The European Commission intends to establish a mechanism that defines test procedures for conformity evaluation of EETS equipment in the frame of the European Network of Certification Centers. The test procedures should at least contain a test strategy and a test plan.

3.2 CHARGING

- An approaching OBE is detected by the road-side equipment (RSE).
- The RSE reads basic contract information and checks whether the OBE has a valid EETS contract from an EETS Provider that is recognised by the Toll Charger.
- In case the OBE has a valid contract the RSE reads data from the OBE, e.g. regarding the payment means, the vehicle classification, the equipment, and possibly past receipts.

- The RSE checks the validity of the data against the black-list and the expiry date of the payment means. It may also check the validity of some security elements (Authenticators).
- In case of valid data the RSE registers the charging transaction, writes a receipt to the OBE and signals to the user that the transaction was OK.
- In case of invalid data the toll station signals to the user that a problem has occurred.

3.3 PAYMENT

- For valid transactions the Toll Charger calculates the fee from the tariff table with information obtained from measuring vehicle data and/or with the data received from the on-board equipment.
- The Toll Charger sends all data from a valid transaction as a claim to the EETS Provider. The Toll Charger must provide all data required by the EETS Provider to produce a complete invoice for the Service User.
- The EETS Provider checks the completeness and consistency of the data and security elements.
- In case the data are valid the EETS Provider pays the contractually agreed amount to the Toll Charger.
- The EETS Provider invoices the Service User.

3.4 ENFORCEMENT

- Enforcement is under control of the Toll Charger. The Toll Charger defines his enforcement strategy. The Toll Charger may use fixed, portable or mobile equipment and/or inspection by personnel.
- The enforcement may encompass reading OBE data via DSRC and comparing them with data observed or measured from the vehicle.
- As part of the enforcement the Toll Charger may check whether the OBE or the payment means of the user is blacklisted.
- In case of a suspected non-compliance (enforcement condition) the Toll Charger stores all relevant data, possibly including DSRC transaction data, measured data, observed data and pictures of the vehicle.
- Arrangements for prosecution are considered outside the scope of EG 11.

3.5 SYSTEM MANAGEMENT

The EETS Provider regularly sends to Toll Chargers

- a list of acceptable contract types (i.e. acceptable EFC Context Marks)
- blacklists for the payment means and for the OBE

A trusted entity in the Interoperability Management domain shall manage the exchange of secret keys used by Toll Chargers for OBE authentication and for Access Credentials (if necessary).

[R 5] EG 11 and DG TREN recommend that the process for key management for keys common to Toll Chargers are defined as part of the CESARE work.

4. PROPOSED SOLUTION

Our solution for the EETS defines a single harmonised set of data, functions and security elements that enables all Toll Chargers to perform DSRC transactions according to their requirements.

Different charging systems require different data. As a principle our proposed approach requires that all data that are needed by the different systems in Europe shall be available on the OBE such that every Toll Charger can read and write the data he needs in his local context. The Toll Charger is free to read on the DSRC link just a few or all data, as he requires. The requirements of the Toll Charger will be given by local needs and by agreements with the EETS Providers.

According to our specification the Toll Charger can only modify data regarding the OBE status and write receipts. All other data, regarding the Contract, the Payment Means or the Vehicle, are read only on the DSRC and can only be modified by the EETS Provider (except for a declaration of trailer presence by the Service User).

Expert Group 11 proposes a flexible “pick what you need” approach. Our specification gives a common definition for a set of data that can be read and written in flexible way by any party that has the required security elements to access the OBE.

Our approach requires that the following items are specified:

- DSRC Requirements: A specification of the radio link, i.e. of the lower layers of the DSRC stack. Both CEN DSRC and the Italian UNI DSRC are covered.
- DSRC Functions: Defines how the data in the OBE can be retrieved or modified.
- Data Requirements: A list of data that must be present in every EETS-compliant OBE.
- Security Requirements: The security elements that allow only authorised parties access to the data plus security elements that prove that data are genuine and not being tampered.
- Transaction and Process Requirements: Some minimal requirements for EETS system processes, e.g. regarding key distribution.
- OBE Requirements: Some minimal requirements regarding the OBE, e.g. regarding the security of the personalisation interface.

4.1 DSRC REQUIREMENTS

Both CEN DSRC and the UNI DSRC shall be supported in the EETS. The principle shall be “Dual DSRC Stacks / Common EFC Application” (Option 2a of Expert Group 1, see [EG1 Report]).

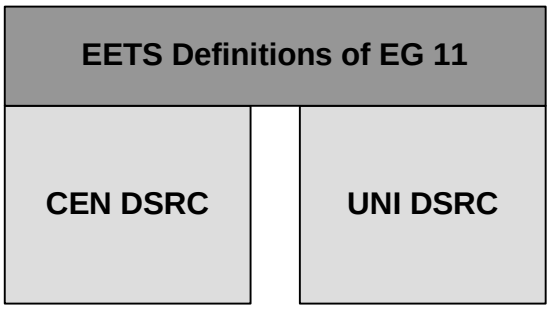

Figure 3: Dual DSRC Stack / Common EFC Application

OBE that work in all European DSRC systems will need to support both stacks. Products that support only one stack may be offered on the market.

Regarding the CEN DSRC, the specification allows for both parameter sets of Layer 1 (L1-A and L1-B) to be used such that no changes to existing RSE are required. For the OBE, additional restrictions apply regarding L1-A in order to make it compatible with all installations. Details are defined in [EFC IAP].

Regarding UNI DSRC, currently draft English versions of the standard documents are available, [UNI DSRC1] to [UNI DSRC4]. According to Italian experts the contents of these documents are stable. The standardisation process in UNI is advanced and the documents will soon be formally issued as UNI standards (in Italian). EG11 has checked the basic validity of the proposed solution, but lacking final documents and lacking the required resources, formal references to standards and full scrutiny of details of the solution cannot be provided.

4.2 DSRC FUNCTIONS

Our specification is based on the functions of [EN 14906] that are most commonly used in Europe. In accordance with CESARE III only functions required for central account are provided. On-board accounts (DEBIT and CREDIT functions) are considered outside the scope of EG 11.

4.3 DATA REQUIREMENTS

Charging and enforcement on the DSRC require data regarding

- contract,
- payment,
- vehicle,
- equipment, and
- receipts.

The items in this list correspond to Data Groups defined in [EN 14906].

4.3.1 Contract

The road side requires information regarding the contract that is contained in the OBE of the passing vehicle, especially whether it can recognise the contract as an EETS one.

EFC-ContextMark and Service Identification

According to CEN standards a contract is identified by the EFC-ContextMark that is contained in the VST. The VST is a data structure that is sent by the OBE in the initialisation phase of a DSRC communication, see [EN 14906]. The EFC-ContextMark contains the elements:

- ContractProvider
- TypeOfContract
- ContextVersion

The element ContractProvider identifies the EETS Provider. Procedures are in place for a EETS Provider to apply for a unique identifier that shall be transmitted in the element ContractProvider. The identifier consists of a country code and of a number that is assigned on a national basis.

TypeOfContract and ContextVersion are elements that identify certain contractual or technical choices that are available with a certain ContractProvider.

In a DSRC transaction every RSE first reads and interprets the EFC-ContextMark. The RSE then decides whether it can accept the contract, i.e. whether there is a relationship with the ContractProvider and whether the TypeOfContract and the ContextVersion are acceptable.

The RSE needs to learn from the EFC-ContextMark whether or not the Contract is an EETS contract. The group has discussed several alternatives how this can be achieved:

- Agree in all Europe on a specific coding for TypeOfContract and Context Version to say “EETS Contract”. This solution was discarded by EG 11 since there might be collisions with existing coding in national contexts.
- Define a new country code for “Europe” and issue identifiers for EETS Providers on a European basis. This is an attractive solution in principle since it would allow registering certified EETS Providers in a simple and unique way without collisions with existing numbering schemes. EG 11 has discarded this solution since current standards do not foresee such a procedure and coding.
- Do not prescribe a specific coding but use look-up tables for accepted EFC-ContextMarks in the RSE. This solution does not create conflicts with existing implementations and also allows equipment to be accepted that already is EETS-compliant. The disadvantage of this solution is that it requires management of the look-up tables which requires constant updating in the RSE.

The first and the second solution had to be discarded also for a management reason, since they do not allow for invalidating contracts from an EETS Provider that is no longer EETS compliant. OBE coded by a certain EETS Provider would remain valid even if the EETS Provider has ceased to be active or has been excluded from the service, e.g. for not fulfilling contractual obligations or because of bankruptcy. (OBE from the invalid EETS Provider would need to be blacklisted on an individual basis).

In the proposed solution all RSE have to carry look-up tables of accepted EFC-ContextMarks. Toll Chargers have to update their lists as soon they have entered a contractual agreement with a new EETS Provider.

ContractSerialNumber

Earlier DSRC specifications have used a Contract Serial Number as an identification of an account of the service user at the service issuer (e.g. in Swiss LSVA). Since the work of CESARE II and CARDME this data element is no longer used, see the comparison tables in Annex B. The identifier now used for this purpose is PersonalAccountNumber (PAN), which does not identify a contract, but rather an account. (PersonalAccountNumber is contained in the attribute PaymentMeans.)

ContractValidity

EG 11 proposes to use PersonalAccountNumber as an identifier of a user contract instead of ContractSerialNumber. Hence also the associated ContractValidity becomes obsolete. It is replaced by PaymentMeansExpiryDate that by standard is part of the attribute PaymentMeans.

ContractAuthenticator

ContractAuthenticator is intended to carry a signature over the contract data such that false or changed contracts can be identified by the Toll Charger or EETS Provider. It is contained in the CESARE II and PISTA specification, but no details are given as to its calculation and its practical use.

EG 11 has decided not to support this data element since

- currently no installation makes use of this data element

- according to CEN standards, [EN14906], ContractAuthenticator shall be calculated over the data Group Contract. Since in our specification Contract Serial Number is no longer used, the Data Group Contract contains no critical information that requires protection
- it is weak since it is a static element that can be copied by a fraudulent user
- it is functionally replaced by much stronger dynamic authenticators that are calculated over the Payment Means.

4.3.2 Payment

In accordance with current practice EG 11 proposes to use PaymentMeans as the attribute that identifies an account of the Service User at an EETS Provider. PaymentMeans is coded in a way to be compatible with the identification scheme for credit cards. PaymentMeans contains the elements

- PersonalAccountNumber (PAN): Contains an issuer identifier (IIN) and an account number. The account number is encompassing Customer ID (contract is signed between customer and EETS Provider) and user ID (one or several for a given customer).
- PaymentMeansExpiryDate: Limits the temporal validity of the payment means. It is expected that EETS Providers will give sufficient validity time since upon expiry OBE become invalid and have to be exchanged or retrieved and re-personalised in order to prolong validity. However, a limited validity period allows a reduction of the size of the black lists.
- PaymentMeansUsageControl: Credit card issuers use this field to give usage restrictions for their cards. EG 11 proposes not to use this field for the EETS.

4.3.3 Vehicle

Vehicle Classification Data

Expert Group 2 has proposed a list of vehicle data for classification in the EETS. Our proposal simply accommodates this list.

VehicleAuthenticator

As can be seen in the comparative table in Annex B some specifications foresee the use of an authenticator that is calculated over the vehicle classification data, but as far we know the authenticator is not actually used in practice.

The purpose of the Authenticator would be that the Toll Charger can detect whether the vehicle data in the OBE are unchanged since it was personalised. This is not practical in our approach since it requires the Toll Charger to read all Vehicle Classification Data to calculate the Authenticator. This does not fit with our “pick what you need” approach, and in addition would make the data transmission so long that two DSRC frames would be required.

EG 11 proposes not to use VehicleAuthenticator. Instead the Toll Charger shall send the Vehicle Classification Data he has read and used to determine the tariff to the EETS Provider. The EETS Provider can check whether the data match with his records from personalisation and can detect any fraudulent changes.

4.3.4 Equipment

EquipmentOBUId

EquipmentOBUId uniquely identifies an OBE. It is required by some systems for blacklisting on-board equipment.

Operational issues like blacklist content are outside the scope of EG 11. In their discussions, EG 11 members have expressed the opinion that PAN rather than

EquipmentOBUId should be used for blacklisting. It should also be noted that some EFC systems assume that every OBE (i.e. every EquipmentOBUId) is linked to a single PAN. These systems might run into difficulties if their local one-to-one correspondence of PAN and EquipmentOBUId does not hold in the EETS. It should also be noted that in some systems the PAN stored in an OBE can be updated via a card read by the OBE.

Several systems have is no possibility for managing a black list based on EquipmentOBUId. Moreover, a given OBE may be reused by the EETS Provider after its PAN has been black listed by writing a new PAN without changing EquipmentOBUId.

EG 11 recommends that these important operational issues are looked into.

[R 6] EG 11 and DG TREN recommend that blacklist content and the relation between PAN and EquipmentOBUId is addressed from an operational point of view by the project CESARE III.

EquipmentStatus

EquipmentStatus is a field that can be read and written. According to CEN standards [EN 14906] it is intended to carry “operator-specific EFC application-related information pertaining to the status of the equipment”. According to the comparative table in Annex B, EquipmentStatus is already commonly used, but not everywhere with the same contents. We propose that EquipmentStatus shall contain a transaction counter as a security element, see the section on Security Requirements below. Besides the transaction counter there is room left in EquipmentStatus for use by the individual Toll Charger.

4.3.5 Receipt

ReceiptData1 and ReceiptData2

ReceiptData1 and Receiptdata2 are read/write attributes and carry the receipts of the last transaction and of the one before that. The data usually serve as entry tickets in closed tolling systems.

EG 11 proposes that the use of these attributes shall remain fully at the discretion of the individual Toll Charger. When a vehicle enters a tolling context, the Toll Charger normally cannot expect that the ReceiptData fields contain useful data, except in case of interconnected networks.

The ReceiptData attributes contain a ReceiptAuthenticator as a security element. Its use by a Toll Charger is voluntary.

ReceiptText

Receipt Text may optionally be used to transfer text information to OBE which are able to display text, e.g. in order to communicate information about transaction. This feature is not currently supported by OBE on the market, but will most likely become more common with multi-technology OBE such as the EETS-compliant ones.

4.4 Security Requirements

EG 11 proposes a security framework that is adapted to the environment of the EETS. It is recognised that the threats in a multi-actor environment are larger and different to the threats encountered in local or national systems.

EG 11 recognises that some existing road-side installations lack the possibility to store cryptographic keys in a secure way. Hence, security solutions have to be found that can accommodate such installations, at least for a certain period of time.

The Table below addresses important threats and the proposed countermeasures.

Threats	Measures
Service User uses a manipulated or non-genuine OBE, i.e. with data not issued by an EETS Provider	- All critical data are read-only on the DSRC - OBE Authentication to the RSE (Stamping) - Payment Authentication to the EETS Provider (Stamping)
Service User alters receipt data	- Receipt Authenticator and/or Access Credentials
User charged wrongly (e.g. for a passage that did not occur)	- Payment Authentication to the EETS Provider (Stamping)
OBEs are being cloned	- Transaction Counter
Incorrect payment claims by the Toll Charger	- Payment Authentication to the EETS Provider (Stamping) - Transaction Counter
Genuine payment claims not accepted by the EETS Provider	- OBE Authentication to the RSE (Stamping) - Payment Authentication to the EETS Provider (Stamping)
Infringement of a users privacy by unauthorised parties reading his OBE data	- OBE Access Credentials
Third parties making unauthorised use of EETS OBE for other purposes	- OBE Access Credentials
Protect the EETS Provider against counterfeit (or manipulated) transactions by Users.	- OBE Authentication to the EETS Provider (Stamping) - Receipt Authenticator - Transaction Counter

Table 1: Security threats and measures

4.4.1 Dynamic Authenticators (Stamping)

Dynamic Authenticators use the GET_STAMPED action of [EN 14906]. Details of the cryptographic calculations are not given here and can be found, e.g. in [EFC IAP].

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 our specification foresees the use of an Authenticator that is calculated by the OBE using a challenge-response mechanism and diversified keys. This mechanism is used in many European EFC transactions. The keys are entered by the EETS Provider into the OBE upon personalisation and shall not be known by any other party.

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 provides for high security and is essential for the operation of the CESARE model. In addition it requires no cryptographic provisions on the RSE of the Toll Charger. Hence, EG 11 proposes to make the Payment Authenticator a mandatory element of EETS DSRC transactions.

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. In order to enable 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 Toll Chargers using this mechanism (for a given EETS Provider). These keys have to be managed and distributed by a central body, see Recommendation [R5].

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.

4.4.2 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.

Toll Chargers have the option to protect the entry tickets by using the element ReceiptAuthenticator which by standard is part of the attributes ReceiptData1 and ReceiptData2. When reading out the tickets at the exit, the tickets can be checked with the Authenticators.

This security feature is not an integral part of the operation of the EETS since correct charging stays within the responsibility of the individual Toll Charger. Hence EG 11 recommends making the use of the Receipt Authenticator an optional part of the EETS. Toll Chargers shall remain free whether or not to use this element, and which algorithms to apply for its calculation.

4.4.3 Transaction Counter

The Transaction Counter is a simple counter based on a concept in [CARDME]. The counter is 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 the only means to identify the most massive breach of system security, namely the appearance of cloned OBE.

4.4.4 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 considers 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. Moreover, existing RSE in Europe presently have no provisions (such as SAMs) able to safely store the required keys.

Hence EG 11 proposes not to foresee Access Credentials as part of the EETS for the time being, and at the same time encourages Toll Chargers to develop a migration strategy to enable a later introduction.

It should be noted that later introduction of Access Credentials will require OBE that has access restrictions implemented. This means that new OBE has to be introduced or, where possible, old OBE has to be re-personalised.

It should also be noted that existing deployed OBE with Access Credentials that would otherwise be EETS compliant can not be used in the EETS when Access Credentials are not supported.

[R 7] The specification does not foresee the use of OBE Access Credentials for the time being. It is recommended that Toll Chargers make ready their equipment for key handling and the dynamic calculation of Access Credentials when they replace or update RSE. Introduction of Access Credentials on a mandatory basis shall be decided at a later point in time.

[R 8] EETS security issues should be investigated in detail, e.g. by an Expert Group to be launched in 2006 (EG 12 or 13). A proper threat analysis should be undertaken and a system-wide coherent and comprehensive security framework be proposed. Migration issues, like the co-existence of different security levels, should also be looked into.

4.5 Transaction and Process Requirements

The specification does not prescribe a certain sequence of transaction steps. Every Toll Charger is free to read and write any attributes in any order as long as he can provide to the EETS Provider the data that are required for a valid claim (including the mandatory security elements), and as long the basic transaction model remains compliant with European Standards, especially [EN 14906].

Mandatory elements of charging transaction are

- reading the PaymentMeans and the EquipmentOBUId (if part of the blacklist, see [R6]) and checking them against the blacklist
- obtaining an Authenticator for the EETS Provider, calculated over the PaymentMeans
- increasing the transaction counter for valid charging transactions
- signalling the success of the transaction to the user. The success can be signalled by a SET_MMI command and/or by installations on road side (barrier or signal lights)

Since enforcement is fully in the responsibility of the Toll Charger, transactions that are only used for enforcement, i.e. without simultaneous charging, have no mandatory elements. The Toll Charger is free to read any data for enforcement purposes.

For the Toll Charger to be able to perform a charging transaction, processes need to be in place that ensure that

- accepted EETS Providers are known to the RSE of the Toll Charger (list of accepted ContractProviders in the EFC-ContextMark)
- all RSE contain a list of which key number to use for which EETS provider for calculating the Payment Authenticator
- all Toll Chargers that require them have the keys needed to verify the OBE Authenticator

4.6 Personalisation and Mounting Requirements

The specification does not prescribe any features of the OBE besides mounting conditions, its behaviour on the DSRC interface and a few relevant aspects on other interfaces:

- In passenger cars, OBEs (or the DSRC antenna) shall be mounted behind the rear-view mirror, i.e. in the central upper part of the windshield. For metallized windshields, the non metallized window behind the rear-view mirror shall be used, if available.
- In HGVs, OBEs shall be mounted with the corresponding HGV's OBE support, in the central lower part of the windshield.
- The EETS Provider must ensure that no other party than himself can change OBE data via the personalisation interface.
- The EETS Provider must generate (diversify) and store the 4+4 Authentication keys in every OBE he issues. The keys must be stored in secure access modules.
- The OBE must be able to signal to the user the success of a transaction with an acoustical or optical signal.

5. IMPLEMENTATION / MIGRATION

Already today most DSRC installations will be able to perform valid transactions with OBE according to this specification. This can be seen from the comparison table in Annex B. In practice, however, transactions will not occur since current road-side installations recognise only a limited number of contract issuers.

Hence, in a first step Toll Chargers and EETS Providers will need to set up contracts. Besides financial issues these contracts will also detail the data exchange format between the Toll Charger and the EETS Provider. In most cases the Toll Charger will have to make some adaptations to his back office system in order to provide data to the EETS Provider in the agreed format. At the same time, the road-side equipment of the Toll Charger will need a software update or at least some parameterisation in order to recognise the contracts from the EETS Provider (via the EFC Context Mark) and to handle the blacklists provided.

Regarding security, matters depend on the contract between EETS Provider and Toll Charger. In case the Toll Charger does not yet use a GET_STAMPED command to produce a Payment Authenticator, he might agree with the EETS Provider to start the service without this security measure.

In a second step Toll Chargers might wish to become fully compliant with this specification and read out the Payment Authenticator from the OBE using a GET_STAMPED command. This will require a minor upgrade of road-side equipment software and of the data exchange format with the EETS Provider. The Toll Charger will pass the Payment Authenticator unchanged to the EETS Provider. There is no need for the Toll Charger to do any cryptographic calculations at all. The Toll Charger simply reads the Payment Authenticator from the passing OBE and sends it on to the EETS Provider. This will give the EETS Provider an excellent proof of passage that he can use in case of customer complaints.

In later steps Toll Chargers might wish to make use of the OBE Authenticator. This measure will give the Toll Charger better security and control over his system. This will require cryptographic checking, either online in the road-side equipment, or offline in the back office system. Toll Chargers are free whether and when to introduce this security feature, according to their own policy and technology decisions.

According to recommendation [R7] EG 11 suggests that Toll Chargers foresee in their maintenance and replacement strategy to make their equipment ready for the dynamic calculation of Access Credentials. Introduction of Access Credentials on a mandatory basis for a new generation of OBEs (to be accepted by the RSEs in parallel with existing OBEs) shall be decided at a later point in time.

6. SUMMARY OF RECOMMENDATIONS

[R 1] The specification in Annex A of this document should be accepted as the technical basis of the EETS for DSRC based charging systems.

[R 2] This specification should be forwarded as input to European Standardisation.

[R 3] The European Commission intends to establish a mechanism to maintain this specification in harmony with European Standards.

[R 4] The European Commission intends to establish a mechanism that defines test procedures for conformity evaluation of EETS equipment inside the European Network of Certification Centers. The test procedures should at least contain a test strategy and a test plan.

[R 5] The processes for key management for keys common to Toll Chargers should be defined as part of the CESARE work.

[R 6] Blacklist content and the relation between PAN and EquipmentOBUId should be addressed from an operational point of view, e.g. by the project CESARE III.

[R 7] The specification does not foresee the use of OBE Access Credentials for the time being. It is recommended that Toll Chargers make ready their equipment for key handling and the dynamic calculation of Access Credentials when they replace or update RSE. Introduction of Access Credentials on a mandatory basis shall be decided at a later point in time.

[R 8] EETS security issues should be investigated in detail, e.g. by an Expert Group. A proper threat analysis should be undertaken and a system-wide coherent and comprehensive security framework be proposed. Migration issues, like the co-existence of different security levels, should also be looked into.

ANNEX A
DSRC TRANSACTION SPECIFICATION

This Annex gives the complete proposed specification of EG 11. The specification is given on a high level. Detailed definitions can be found in the underlying standards and in [EFC IAP].

Regarding the UNI DSRC part of the specification, currently draft English versions of the standard documents ([UNI DSRC1] to [UNI DSRC4]) are available. The standardisation process in UNI is advanced and the documents will soon be issued as UNI standards (in Italian). Hence, EG11 cannot make formal reference to the UNI standards and cannot guarantee for every detail of the specification.

DSRC Requirements

The EETS supports two DSRC communication stacks for the OBE, according to the CEN and the UNI specifications. The functions, data and security shall be the same for both stacks.

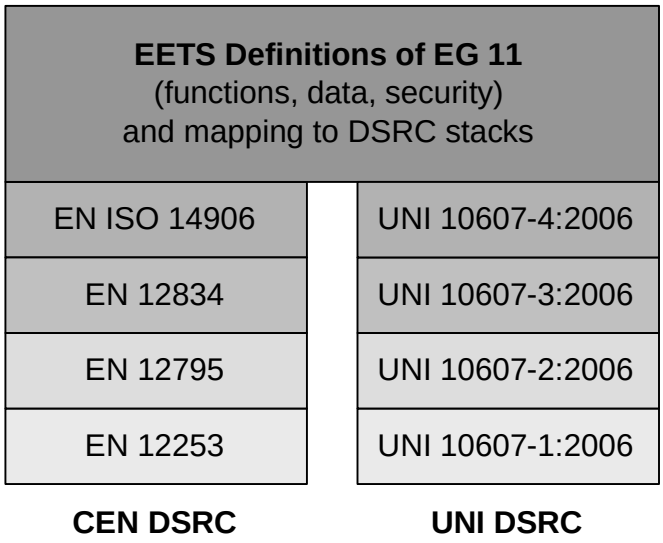

Figure 4: Structure of the EETS

CEN DSRC

The CEN DSRC stack shall comply with EN 13372 [EN Profiles], DSRC Profiles P0/P1 according to detail defined in [EFC IAP], and with EN ISO 14906 [EN 14906].

Note that compliance with [EN Profiles] includes compliance with the other DSRC standard documents for Layer 1, Layer 2, and Layer 7 ([EN Layer 1], [EN Layer 2], [EN Layer 7]).

UNI DSRC

The UNI DSRC stack shall comply with [UNI DSRC1], [UNI DSRC2], [UNI DSRC3], and [UNI DSRC4], respectively with the corresponding final UNI standards.

EETS Functions

The OBE shall support the DSRC services and EFC functions listed in the Table below and defined in [EN 12834] and [EN 14906].

Function	Remarks
INITIALISATION	Establishes communication, selects the application and contract.
GET	Retrieves data from the OBE.
SET	Writes data to the OBE.
GET_STAMPED	Retrieves data with a dynamic authenticator from the OBE.
SET_MMI	Invokes an MMI function (e.g. signal "OK" via buzzer). All SetMMIRq values (i.e. 0, 1, 2 and 255) defined in Annex A in [EN 14906] shall be supported.
ECHO	OBE echoes received data
EVENT-REPORT RELEASE	Terminates communication

Table 2: EETS functions

Functions correspondences

The following table shows the correspondences between EETS functions and primitives defined in the CEN and UNI stacks. Different UNI service primitives are used to access data that are located in different memory regions.

EETS Function	CEN primitive	UNI primitive
INITIALISATION	see EN 12834, section 7	A-Associate, [UNI DSRC3]
GET	GET, [EN 12834]	*Data location* — *Service primitive* Master core — Get_Context, [UNI DSRC3] Master record — Get_Context_Record, [UNI DSRC4] Application core — Get_ASO_Context, [UNI DSRC3] Application record — GET [UNI DSRC3]
SET	SET, [EN 12834]	*Data location* — *Service primitive* Application core — Set_ASO_Context, [UNI DSRC3] Application record — SET, [UNI DSRC3]
GET_STAMPED	GET_STAMPED, [EN 14906]	Concatenation of: 1. Get_Credentials, [UNI DSRC4] 2. A Get operation (according to the requested data, see GET above in this table)
SET_MMI	SET_MMI, [EN 14906]	A-Alert_Extrn, [UNI DSRC4]
ECHO	ECHO, [EN 14906]	A-SLT, [UNI DSRC3]
EVENT-REPORT RELEASE	EVENT-REPORT, [EN 12834]	A-Release, [UNI DSRC3]

Table 3: Functions correspondences

EETS Data

The following data attributes according to [EN 14906] shall be implemented in the OBE:

ATTRIBUTES	AttrId	Read	Write	Remarks
CONTRACT				Information associated with the service rights of the issuer of the EFC service.
EFC Context Mark	0	Yes	No	Transmitted as part of the VST.
PAYMENT				Data identifying the Payment means and its validity
PaymentMeans	32	Yes	No	Includes PAN and Expiry Date
VEHICLE				Identification and characteristics of the vehicle.
VehicleLicencePlateNumber	16	Yes	No	see Expert Group 2 [EG2 Report]
VehicleClass	17	Yes	No	- - - " - - -
VehicleAxles	19	Yes	No	- - - " - - -
VehicleWeightLimits	20	Yes	No	- - - " - - -
VehicleSpecificCharacteristics	22	Yes	No	- - - " - - - (Include Euro Class)
VehicleSuspensionType	-	Yes	No	Not in EN 14906. Added by Expert Group 2
EQUIPMENT				Identification of the OBE and general status information
EquipmentOBUId	24	Yes	No	
EquipmentStatus	26	Yes	Yes	Includes transaction counter
RECEIPT				Financial and operational information associated with a specific session.
ReceiptData1 (last)	33	Yes	Yes	Used as entry ticket in closed systems
ReceiptData2 (penultimate)	34	Yes	Yes	Used as transit ticket
ReceiptText	12	Yes	Yes	Optional text for OBE with display

Table 4: OBE data

The EETS Provider shall ensure that all read-only data (data in the Table above with Write "No") are personalised when the OBE is provided to the user.

Data belonging to "Vehicle" shall be implemented according to [EG2 Report], latest version. Only data that are relevant according to the Vehicle Group of the vehicle need to be personalised.

Data correspondences

The main difference between data defined in the CEN standards and data defined in the UNI standards is their addressing. CEN-based data are addressed by reference, i.e., by using data identifiers. UNI-based data are addressed by position, i.e., by specifying their location in OBE memory.

The following table specifies the mapping of the defined data in the UNI memory structure (see also [UNI DSRC4]). In the table, field names are the same as parameter names. The optional parameter ReceiptText is not supported for UNI conformant implementations, and is not mapped.

Application context / Field			Field length (octets)	Description
Master	header	core-len	1	Core length = 5
		record-len	1	Record length = 11 octets
		record-number	1	There is 1 record (in case of only EETS application present in the OBE)
		current-record	1	The current record (addressed application) is the first one
	core		5	OBE-specific (manufacturer) information (reserved)
	record 1	application-id	2	This is the EETS Application identifier
		reserved	1	
		EFC-ContextMark	6	EN ISO 14906, AttrId 0
		AC_CR-KeyReference	2	Reserved for key reference for AC-CR, see [EFC IAP]
EETS Application	header	core-len	1	Core length = 40 + n (VehicleSuspensionType length)
		record-len	1	Record length = 58 octets
		record-number	1	There is 1 record
		current-record	1	The current record is the first one
	core	VehicleLicence PlateNumber	9	EN ISO 14906, AttrId 16
		VehicleClass	1	EN ISO 14906, AttrId 17
		VehicleAxles	2	EN ISO 14906, AttrId 19
		VehicleWeightLimits	6	EN ISO 14906, AttrId 20
		VehicleSpecificCharacteristics	4	EN ISO 14906, AttrId 22
		VehicleSuspensionType	n	Not in EN 14906. Added by Expert Group 2
		PaymentMeans	14	EN ISO 14906, AttrId 32
		EquipmentOBUId	4	EN ISO 14906, AttrId 24
	record 1	EquipmentStatus	2	EN ISO 14906, AttrId 26
		ReceiptData1	28	EN ISO 14906, AttrId 33
		ReceiptData2	28	EN ISO 14906, AttrId 34

Table 5: UNI addressing of EETS data

Reading or writing of the above data is performed by a set of functions that is specific for each identified memory region, namely, Master Core, Master Record, Application Core, and Application Record (see [UNI DSRC3] and [UNI DSRC4]). The way to access the above data is specified in the next section on function correspondences.

Data access

The following table shows how to access data with the functions defined above.

EETS Attribute	CEN access	UNI access
EFC Context Mark	**Get** (AttributeId=0)	**Get_Master_Record** (Offset=3, Length=6)
	Set not allowed	
PaymentMeans	**Get** (AttributeId=32)	**Get_ASO_Context** (Offset=22+m, Length=14)
	Set not allowed	
VehicleLicencePlateNumber	**Get** (AttributeId=16)	**Get_ASO_Context** (Offset=0, Length=9)
	Set not allowed	
VehicleClass	**Get** (AttributeId=17)	**Get_ASO_Context** (Offset=9, Length=1)
	Set not allowed	
VehicleAxles	**Get** (AttributeId=19)	**Get_ASO_Context** (Offset=10, Length=2)
	Set not allowed	
VehicleWeightLimits	**Get** (AttributeId=20)	**Get_ASO_Context** (Offset=12, Length=6)
	Set not allowed	
VehicleSpecific Characteristics	**Get** (AttributeId=22)	**Get_ASO_Context** (Offset=18, Length=4)
	Set not allowed	
VehicleSuspensionType	**Get** (AttributeId=?)	**Get_ASO_Context** (Offset=22, Length=n)
	Set not allowed	
EquipmentOBUId	**Get** (AttributeId=24)	**Get_ASO_Context** (Offset=36+n, Length=4)
	Set not allowed	
EquipmentStatus	**Get** (AttributeId=26)	**Get** (Offset=0, Length=2)
	Set (AttributeId=26)	**Set** (Where=Current, Offset=0, Length=2)
ReceiptData1	**Get** (AttributeId=33)	**Get** (Offset=2, Length=28)
	Set (AttributeId=33)	**Set** (Where=Current, Offset=2, Length=28
ReceiptData2	**Get** (AttributeId=34)	**Get** (Offset=30, Length=28)
	Set (AttributeId=34)	**Set** (Where=Current, Offset=30, Length=28)

Table 6: Data access

Reading or writing multiple attributes in a single instance of a service primitive (Get or Set) is possible in the UNI case for attributes that are stored sequentially in the same memory region. This can be accomplished by specifying a displacement corresponding to first attribute to be read or written, and a length equal to the sum of the attributes' lengths.

Example: Get(ting) EquipmentStatus and ReceiptData1 can be accomplished by:

- the CEN interface by means of a GET (AttributeList(26,33))
- the UNI interface by means of a Get (Where=Current, Offset=0, Length=30).

Security Requirements

Dynamic Authenticators (Stamping)

The OBE shall support dynamic authentication of the Payment Means (i.e. GET_STAMPED for the attribute PaymentMeans).

The OBE shall contain 4 keys reserved for the Toll Charger domain and 4 keys reserved for the EETS Provider domain.

Toll Chargers shall execute a GET_STAMPED on the attribute PaymentMeans with a specified key number from the EETS Provider and transmit the result to the EETS Provider as part of the claim, if mutually agreed between the Toll Charger and the EETS Provider.

Toll Chargers are free to execute an additional GET_STAMPED on the attribute PaymentMeans with a key number from the Toll Charger domain in order to authenticate the passing OBE.

Receipt Authenticator

Toll Chargers may use the element ReceiptAuthenticator in the attribute ReceiptData to authenticate receipts given by beacons. There is no prescribed use regarding the EETS.

Transaction Counter

The RSE of the Toll Charger shall use parts of the attribute EquipmentStatus as a transaction counter. The attribute shall be read and written back to the OBE with the counter incremented for every transaction that leads to transaction data being sent to the EETS Provider.

Access Credentials

The use of OBE Access Credentials is not foreseen in this specification. Toll Chargers are encouraged to ready their road-side equipment for a later introduction of Access Credentials.

Transaction and Process Requirements

The specification does not prescribe a certain sequence of transaction steps. Mandatory elements of charging transaction are

1. reading PaymentMeans and EquipmentOBUId (if part of the blacklist) and checking them against the blacklist
2. obtaining an Authenticator for the EETS Provider, calculated over the PaymentMeans
3. increasing the transaction counter for valid transactions
4. signalling the success of the transaction to the user. The success can be signalled by a SET_MMI command or by installations in the lane (barrier or signal lights)

The following table gives examples of use of CEN and UNI primitives for the mandatory transaction elements.

Transaction element	CEN primitive(s)	UNI primitive(s)
1	Get (AttributeIDList (AttributeID=32,AttributeID=24))	Get_ASO_Context (Offset=22+m, Length=12) Get_ASO_Context (Offset=34+m, Length=5)
2	GetStamped (AttributeIdList(AttributeID=32), nonce, keyRef)	Get_Credentials (Offset=22+m, Length=12, Noncelen, Nonce, key) clause 6.1.2) Get_ASO_Context (Offset=22+m, Length=12)
3	Set (AttributeId=26)	Set (Where=Current, Offset=0, Length=2)
4	Set_MMI (ok)	A-Alert_Extrn (Video=ok, Audio=ok, Time=1, Count=2)

Table 7: CEN and UNI primitives for the mandatory transaction elements

Transactions that are not used for charging (e.g. for enforcement without simultaneous charging) have no mandatory elements.

EETS Providers and Interoperability Management shall install processes that ensure that

- Toll Chargers have current lists of accepted ContractProviders and specific parameters associated to them, like e.g. the key number to use when requesting OBE to produce a Payment Authenticator
- the security keys for verification of the OBE Authenticator are available to Toll Chargers

OBE Requirements

- EETS compliant OBE shall be protected on all interfaces such that attributes that are read-only on the DSRC interface cannot be changed by any party unless authorised by the EETS Provider.
- EETS compliant OBE shall have 8 diversified keys stored in secure access modules. It is the responsibility of the EETS Provider to diversify and store these keys.
- EETS compliant OBE shall be able to signal to the user the success of a transaction with an acoustical or optical signal.

ANNEX B
COMPATIBILITY WITH OTHER SPECIFICATIONS

ATTRIBUTES	Attr ID	PISTA / CESARE	CARDME	Austria	OMISS UK	EFC Sweden	TIS PL France	MEDIA	Telepass	EG 11
Contract										
EFCContextMark (VST)	0	X	X	X	X	X	X	X		**X**
ContractSerialNumber	1									
ContractValidity	2									
ContractAuthenticator (R)	4	X				X	X			
Telepass Id	-								X	
Payment										
Payment Means (R)	32	X	X	X	X	X	X	X		**X**
Vehicle										
VehicleLicencePlateNumber (R)	16		X	X	X	X	X	X		**X**
VehicleClass (R)	17	X	X	X	X	X	X	X		**X**
VehicleDimensions (R)	18	X	X			X	X			
VehicleAxles (R)	19	X	X	X	X	X	X	X		**X**
VehicleWeightLimits (R)	20		X		X	X	X	X		**X**
VehicleSpecificCharacteristics (R)	22		X	X	X	X	X	X		**X**
VehicleAuthenticator (R)	23	X				X	X	X		
Receipt										
ReceiptData1 (R/W)	33	X	X	X	X	X	X	X		**X**
ReceiptData2 (R/W)	34	X	X	X	X	X	X	X		**X**
ReceiptText (W / display)	12		X				X	X		**X**
Equipment										
EquipmentOBUId (R)	24	X		X		X	X	X		**X**
EquipmentStatus (R/W)	26	X	X	X	X	X	X	X		**X**
Private Attributes										
TransactionLog (W)	99			X						
D-PASS (Journey following)	124						X			
D-GES (Grey list management)	116						X			
D-EVE (Data of OBE)	125						X			

"X" means that according to specification the RSE reads or writes the attribute if required and if present in the OBE.

Table: Comparison of application data

Security feature	PISTA/ CESARE	CARDME	Austria	OMISS UK	EFC Sweden	TIS PL France	MEDIA	Telepass	EG 11
Transaction Counter	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Data Access protection (Access Credentials):									
Static password	No	Option	Yes		Option	Yes	Option	No	No
Dynamic cryptogram	No	Option	Option	Yes	Option	yes	Option	No	Future
Static Authenticator (Data attributes):									
Contract Authenticator	Yes	No	No	No	Yes	Yes.	Yes	No	No
Vehicle Authenticator	Yes	No	No	No	Yes	Yes.	Yes	No	No
Receipt Authenticator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Dynamic Authenticator (Stamping):									
Charging Transaction Authenticator for Issuer	No	Yes	No	Yes	Yes	Yes.	Yes	No	Yes
Transaction Authenticator for Operator	Yes	Yes	Yes	Yes	Yes	Yes.	Yes	No	Yes

"Yes" means that according to specification the corresponding mechanism is implemented in OBE and can be activated by RSE if required.

Table: Comparison of supported security elements

ANNEX C REFERENCES

General References

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

[CESARE] Detailed CESARE Technical Specification, EC Project CESARE II, Deliverable 032.1

[EG1 Report] Recommendations on Microwave DSRC Technologies at 5.8 GHz to Be Used for the European Electronic Toll Service, Report of Expert Group 1, European Commission, 2005

[EG2 Report] Recommendations on Parameters to Be Stored in On-board Equipment Designed for Use with the European Electronic Toll Service, Report of Expert Group 2, European Commission, 2005

[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

Referenced Standards

[EFC IAP] Draft prEN on Road Transport and Traffic Telematics — Electronic Fee Collection — Interoperability Application Profile for DSRC, CEN TC278 WG1, WG1N859

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

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

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

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

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

[UNI DSRC1] UNI10607-1:2006, Road Traffic and Transport Telematics - Automatic Dynamic Debiting Systems and Automatic Access Control Systems Using Dedicated Short-range Communication at 5.8 GHz Part 1: Physical Layer (English draft of the UNI standard to be issued in 2006)

[UNI DSRC2] UNI10607-2:2006, Road Traffic and Transport Telematics - Automatic Dynamic Debiting Systems and Automatic Access Control Systems Using Dedicated Short-range Communication at 5.8 GHz Part 2: Data Link Layer (English draft of the UNI standard to be issued in 2006)

[UNI DSRC3] UNI10607-3:2006, Road Traffic and Transport Telematics - Automatic Dynamic Debiting Systems and Automatic Access Control Systems Using Dedicated Short-range Communication at 5.8 GHz Part 3: Application Layer (English draft of the UNI standard to be issued in 2006)

[UNI DSRC4] UNI10607-4:2006, Road Traffic and Transport Telematics - Automatic Dynamic Debiting Systems and Automatic Access Control Systems Using Dedicated Short-range Communication at 5.8 GHz Part 4: The Electronic Fee Collection Service Object (English draft of the UNI standard to be issued in 2006)

ANNEX D GLOSSARY OF TERMS

CARDME	Concerted Action for Research on Demand Management in Europe
CESARE	Study for a Common EFC system for an ASECAP Road Tolling Service
CEN	European Committee for Standardization (Comité Européen de Normalisation)
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)
GNSS/CN	Global Navigation and Satellite System / Cellular Network (for example GPS/GSM)
Layer 1	Layer 1 of DSRC (Physical Layer)
Layer 2	Layer 2 of DSRC (Data Link Layer)
Layer 7	Layer 7 of DSRC (Application Layer)
MEDIA	Management of EFC DSRC Interoperability in the Alpine Region
OBE	On-Board Equipment
PAN	Personal Account Number
PISTA	Pilot on Interoperable Systems for Tolling Applications
RSE	Road-Side Equipment
SAM	Secure Access Module
UNI	Italian Standards Organization (Ente Italiano di Normazione)
VST	Vehicle Service Table

ANNEX E
EXPERT GROUP MEMBERS

The members of the Expert Group were appointed by the European Commission.

Name	Company/Organisation
Bernhard Oehry (Lead)	Rapp Trans (Switzerland)
Paolo Giorgi	Autostrade per l'Italia (Italy)
Johan Hedin	Hybris Konsult AB (Sweden)
François Malbrunot	Logma (France)
Paulo Marques	Via Verde (Portugal)
Joan Marti Riola	ServiAbertis (Spain)
Anton Sieber	ASFINAG (Austria)
Simon Smith	PA Consulting (UK)
Bjarne Olav Tveit	Self employed consultant (Norway)