



Project IST-1999-29053

Deliverable 4.1

(Final)

1 June 2002

THE CARDME CONCEPT

ABSTRACT

The CARDME Electronic Fee Collection concept provides users with an interoperable payment service in the concession areas of all European participating operators.

The use of central accounts enables users to receive a single monthly invoice for their tolls. A high degree of privacy for users is offered. The CARDME DSRC transaction follows the EN ISO 14906 Standard and is similar to the transaction proposed by the CESARE project.

The system is independent of hardware and is suitable for open and closed systems with free flow multi-lane operation as well as for single lane operation with or without barriers. The interoperable application can be added to existing local applications without prejudice to their operation.

Provision is made for an extended set of vehicle characteristics for classification and a variety of security measures is available for use if required.

Keyword list: Tolling, Electronic Fee Collection, Standards, Transaction, Roaming, Classification, Privacy, Security

Document number: D4.1 CARDME-4 Deliverable 1
Document version: Issue 3 (Deliverable Version 3.0)
Status: Final
Document nature: Project Deliverable
Dissemination level: Public
Date of issue: 1 June 2002
Activity: WP1
Author(s): Bernhard OEHRY RAPP
Trond FOSS GRØNER
Brian BOURNE Orchidnote
Jesper ENGD AHL RAPP
Jean-François JOUEN ISIS
Francisco SORIANO LISITT
Stefan EISSES INTERCAI
Mark WEDLOCK TRL

Contact person: *Bernhard Oehry*
RAPP Ltd, Basel, Switzerland
Phone +41-61-335 78 46
Fax +41-61-335 77 00
bernhard.oehry@rapp.ch

Executive Summary

Background

In a previous phase of this project [CARDME-3] a concept for an interoperable toll payment system using central accounts was established and was described in Deliverable 3.3 issue 3 'Specification of an interoperable European EFC service' published in May 2000.

CARDME-4 builds on the principles established in that deliverable and progresses further in terms of refinement of the concept and convergence with related projects. Advantage has been taken of the coincidence of the timescales of CARDME-4 and CESARE-II which has made it possible to ensure a close agreement between the recommendations of the two projects.

Document structure and readership

The format of this document differs from that of the previous deliverable and provides descriptions of the CARDME concept and processes at levels of complexity designed to accommodate the needs of policy makers, operators, and system implementers.

The Introduction explains the motivation, objectives and scope of CARDME and is relevant to all readers.

Part 1 is intended for readers who wish to understand the concept but do not have the time to delve into the technical detail. It describes the concept in terms of the parties involved, what happens in various situations and how the transaction is done. It also covers matters such as adding the CARDME application to an existing installation, how to protect privacy and how to ensure payment by foreign users.

Part 2 covers the same ground in greater depth. 'Operators' who need to be familiar with the operational aspects of a system will wish to read parts 1 and 2.

Part 3 is a technical annex dealing in depth with the transaction, security, attributes and data elements etc. It is envisaged that only those charged with implementation of new systems will need to study the annex in detail.

Convergence with other projects

The CARDME-3 project coincided in time scale with the work of MÅNS, the implementation of the Autopass system in Norway and the development of an EFC toolbox by the A1 project. As a result of active co-operation between the projects the CARDME transaction was demonstrated to be fully compatible with the toolbox. Although the first phase of the ASECAP project CESARE I was active at the time, its ideas were not then fully formulated and while the projects co-operated in matters of general philosophy it was not possible to attempt an agreement on compatibility of the transactions.

The time scale of CARDME-4 has coincided closely with that of CESARE II and a much more vigorous level of co-operation has been possible partly due to participation of some CARDME members in the CESARE project. The transactions proposed by the two projects are now extremely close. There are some differences in the approach to security and to declared vehicle characteristics. With regard to security the projects agree that it will be expensive for operators to implement but CARDME believes that it is prudent to make provision in the on-board equipments for a possible future requirement at little cost. The CARDME transaction makes provision for the extended set of characteristics required for heavy goods vehicles and which are not included in the CESARE specification. Neither of these differences is irreconcilable as the roadside equipment will be able to determine which system a vehicle is using and can process the data accordingly.

Standardisation

Another important aspect of the work has been the promotion of a revision of the application interface standard EN ISO 14906 in which the CARDME and CESARE transactions are fully compatible with the Standard. This objective has been achieved at the CEN TC278 WG1 level, again in some measure due to CARDME membership of the working group and is expected to be confirmed in 2002.

PAGE INTENTIONALLY LEFT BLANK

Table of Contents

INTRODUCTION	8
1 MOTIVATION FOR CARDME	8
2 CARDME OBJECTIVES	8
3 SCOPE	9
4 PROPERTIES OF THE CARDME-CONCEPT	9
5 DOCUMENT STRUCTURE	10
5.1 Organisation of the Document	10
5.2 Reading Guidelines	10
PART ONE: THE CARDME CONCEPT	11
1 THE INVOLVED PARTIES - CARDME ARCHITECTURE	11
2 WHAT HAPPENS WHEN – CARDME PROCEDURES	12
2.1 The MoU Partners	12
2.2 A User Obtains an OBE for a Holiday Trip	13
2.3 A Driver Acquires a Personalised OBE for a Truck	13
2.4 An Operator Handles His Local Customers	14
2.5 An Operator Handles Roaming Customers	14
3 HOW IS IT DONE – CARDME TRANSACTION	15
3.1 Transaction Phases	15
3.1.1 The Four Phases of the DSRC Communication	15
3.1.2 Say Hello - Initialisation	15
3.1.3 Read OBE Data - Presentation	17
3.1.4 Write New OBE Data - Receipt	18
3.1.5 End the Transaction - Tracking and Closing	18
3.2 Transaction Data	19
3.2.1 Contract - From Which MoU Partner do You Come ?	19
3.2.2 Classification - What Type of Vehicle do You Have ?	20
3.2.3 Receipt - Where did You Enter the Highway ?	22
3.2.4 Security - Can I Trust You ?	23
3.3 Transaction Implementation	25
3.3.1 How to Add CARDME to Existing Installations	25
3.3.2 How to Protect Privacy	26
3.3.3 How to Get Paid for a CARDME Transaction	28
3.3.4 How to Proceed when an Exception Occurs	29

PART TWO: THE CARDME SPECIFICATION -----30

1 CARDME ARCHITECTURE	30
1.1 Introduction.....	30
1.2 Organisations in the CARDME Architecture.....	32
2 CARDME PROCEDURES	34
2.1 MoU Management and Implementation	34
2.2 Contract Issuing.....	35
2.3 Charging.....	38
2.4 Payment	40
3 CARDME TRANSACTION	42
3.1 Transaction Phases	42
3.1.1 Transaction Overview	42
3.1.2 Initialisation Phase	44
3.1.3 Presentation Phase	46
3.1.4 Receipt Phase	50
3.1.5 Tracking / Closing Phases	51
3.2 Transaction Data	52
3.2.1 Contract and Context Mark	52
3.2.2 Classification in CARDME	54
3.2.3 Entry Ticket and Receipt	58
3.2.4 Security and Authenticators	60
3.3 Transaction Implementation	62
3.3.1 Implementing CARDME	62
3.3.2 Protecting Privacy	65
3.3.3 Clearing and Exchanging Claims	67
3.3.4 Exception Handling	69
4 REFERENCES	72

TECHNICAL ANNEX-----73

1 TERMS, DEFINITIONS AND ABBREVIATIONS	73
1.1 Terms and Definitions.....	73
1.2 Abbreviations.....	79
2 TRANSACTION	80
2.1 Initialisation.....	80
2.1.1 Initialisation request (BST)	80
2.1.2 Private window request	80
2.1.3 Private window allocation	80
2.1.4 Initialisation response (VST)	81
2.2 Presentation	82
2.2.1 Presentation request	82
2.2.2 Presentation response	83
2.3 Optional Presentation	85
2.3.1 Optional presentation request	85
2.3.2 Optional presentation response	86
2.4 Receipt	87

2.4.1 Set receipt request	87
2.4.2 Set receipt response	88
2.5 Tracking and Closing	89
2.5.1 Tracking request (Echo.request)	89
2.5.2 Tracking response (Echo.response)	89
2.5.3 Closing	89
3 ATTRIBUTES AND DATA ELEMENTS	91
4 SECURITY	97
4.1 Introduction	97
4.2 Security Requirements	98
4.3 CARDME Security Services and Mechanisms	99
4.3.1 Integrity	99
4.3.2 Authentication	100
4.3.3 Confidentiality	101
4.3.4 Access control	101
4.4 Key Management	102
4.4.1 Authentication keys	102
4.4.2 Access keys	103
4.5 Key Generation	103
4.5.1 Masterkeys	103
4.5.2 OBE-specific keys	104
4.6 Computation of Authenticators	106
4.6.1 Issuer Authenticator (Auth_Iss)	106
4.6.2 Operator Authenticator (Auth_Op)	107
4.6.3 Receipt Authenticator	107
4.7 Access Credentials	108
4.7.1 OBE computation of AC_CR	108
4.7.2 RSE computation of AC_CR	109
4.8 Transaction Counter	109
4.9 IMPLEMENTATION EXAMPLES	110
4.9.1 Key derivation – Authenticator Keys	110
4.9.2 Key derivation – Access Credentials key	110
4.9.3 Computation of authenticators	111
4.9.4 Computation of Access Credentials	112

INTRODUCTION

1 MOTIVATION FOR CARDME

The CARDME system is independent of hardware and is suitable for open and closed systems with free flow multi-lane operation as well as for single lane operation with or without barriers. It is a central account system and users receive a single 'monthly invoice' for all the transactions whether in their home region or while travelling outside their own region or country.

An essential feature of the CARDME concept is that the interoperable application can be added to any existing local applications and only those users who wish to take advantage of cross-border interoperability need to have the application installed in their OBEs. In practice this means that the take up among private car users will be greatest in areas where cross border travel is frequent. For freight hauliers the advantages are generally greater and a much higher level of installation may be expected.

The use of EFC systems is widespread in those countries which have a tradition of manual charging tolls for the use of motorways – in France there were over 1 billion transactions in 2000 resulting in the collection of € 5 billion.

The objectives of different governments and operators vary. In some cases the aim is to provide better services funded by tolls while, at the other extreme, tolls may be used to discourage the use of roads particularly in urban areas. The take-up in northern European countries has generally been slower than among the ASECAP countries due to conflicting requirements and the fact that, where tolling has not been an established practice there are frequently no toll plazas. The take-up would almost certainly be more rapid if a consistent approach offering a realistic possibility of Europe-wide interoperability for applications with free-flow operation as well as single lane operation could be seen to exist.

The CARDME project has addressed these concerns and with active co-operation among emerging projects over the past several years this is now a real possibility and the alignment of the approaches of CARDME and CESARE, in conformity with the revised Standard EN ISO 14906 will present a powerful force in favour of universal adoption of interoperable systems.

2 CARDME OBJECTIVES

CARDME has two objectives:

CARDME defines the framework for **an interoperable European EFC service** based on central account. This service is intended for use **in addition to any existing local EFC services**. All procedures of existing systems can remain as they are today. Users who want to have the convenience of an interoperable service are offered the option to have an on-board equipment and an associated contract that enables them to travel through all concession areas that support the CARDME Concept. For users who do not want or need the CARDME roaming service nothing changes – they keep their local on-board equipment and contracts.

**Add an option for interoperation
BUT
Don't change proven procedures**

In addition, the CARDME service is defined in such a way that it may also serve as **a template for concessions or countries that newly introduce an EFC service**. The CARDME-Concept can be used to introduce EFC services that are designed for interoperability from the very beginning and enjoy maximum industry support. The CARDME transaction can easily meet local requirements.

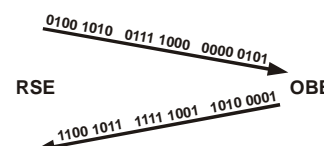
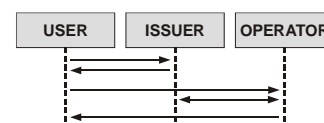
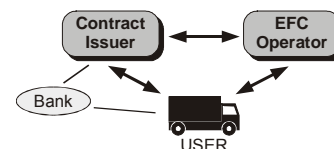
**Avoid inventing the wheel afresh each time
BUT
Go for standardised, low cost equipment**

3 SCOPE

The scope of this document is to define the interoperable CARDME service in sufficient detail to enable implementations to be based directly on this document.

The definition of the CARDME service comprises

- the **system architecture**, describing the basic model of the CARDME Concept, the involved parties, their roles and their relationships.
- the **detailed procedures** for all important processes in the system, like ‘a user acquires an OBE’, like ‘a user passes a foreign tolling station’ or like ‘the operators settle their mutual claims’.
- the **complete technical specification** for the DSRC transaction, including a bit-level specification of the frames exchanged on the DSRC link, detailed specifications of all data elements and their contents plus a specification of the transaction record and claims exchanged between operators.



4 PROPERTIES OF THE CARDME-CONCEPT

The CARDME-Concept enables the operator

- to introduce an interoperable service within existing installations without affecting local EFC services
- to enter agreements with other operators while keeping full control over the local system
- to procure equipment at prices that benefit from true mass production

The CARDME-Concept offers to the user

- the convenience of a seamless non-stop EFC service across concession areas or countries
- the comfort of having a single invoice for all tolls
- the choice to obtain the basic local or the enhanced interoperable equipment according to his needs

The CARDME-Concept has the technical features

- extension of the scope of the local payment means into a Europe-wide payment service
- full support for all vehicle types and for all classification schemes
- separated local and roaming security domains which gives the operator full control and flexibility

The CARDME-Concept is based upon

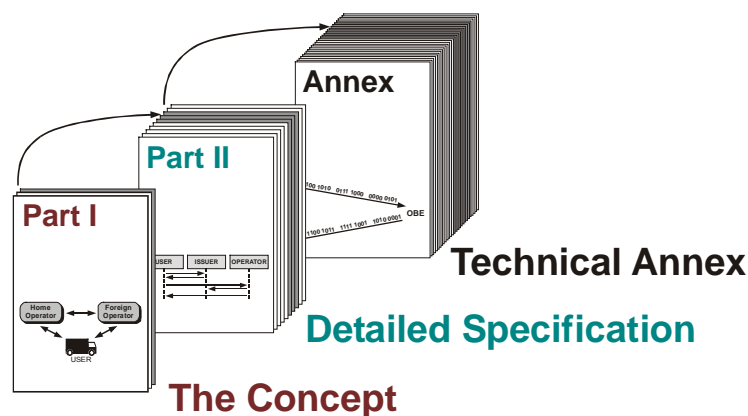
- direct input from operators, from national EFC Projects, and from previous EC research projects
- the set of CEN DSRC standards
- available mature industrial products from several suppliers

5 DOCUMENT STRUCTURE

5.1 ORGANISATION OF THE DOCUMENT

The document has *three sections* that treat the same content at *three levels of detail*:

- **PART ONE** introduces the basic concepts. It defines the **conceptual core** of the system architecture and of the operational procedures. Part One is self-contained and gives the complete picture in a non-technical way, focusing on procedural aspects.
- **PART TWO** is structured **completely parallel to Part One**. In case you need more information on a certain topic in a certain chapter of Part One, you will find **more detail in Part Two under the same chapter number**. Part Two again tries to avoid technical detail and focuses on precise definitions of procedures and data exchanges instead.
- **ANNEX**. All **detailed technical specifications** are provided in the Annex. Whereas technical detail was avoided in the main body of the document, here the contrary becomes true: Data elements and transaction steps are defined in full unambiguous detail down to bit-level so that implementations can directly be based on the specifications of the Annex.



5.2 READING GUIDELINES

It is recommended that all readers first go completely through **Part 1**, which introduces all essential concepts and is kept as short as possible. It is written with the intention of giving **policy makers, company management and generally interested persons** the complete picture without need to read through lengthy detail.

Part 2 is structured completely parallel to Part 1 but treats each of the subjects in more depth. If you want more detail for a certain subject, you can simply jump from a topic in Part 1 to the same topic in Part 2 without need to read the full document. Reading the whole **Part 2** is recommended **for the technically interested, for the EFC expert, for people in related research projects and for similar readership**.

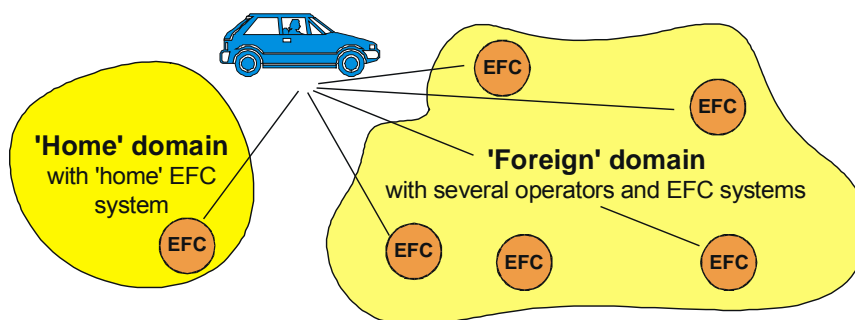
The Annex is intended for reference purposes. It is assumed that **except for implementing engineers, few will have the need to consult material in the Annex**.

PART ONE: THE CARDME CONCEPT

1 THE INVOLVED PARTIES - CARDME ARCHITECTURE

In the CARDME Architecture the EFC user travels in two different domains. In the 'home' domain the user benefits from services in a local EFC system. In the 'foreign' domain he benefits from services in several 'foreign' EFC systems.

It is the vision of CARDME that eventually all European EFC systems are in the CARDME domain where the user is able to use his home payment means and medium in all foreign EFC systems.



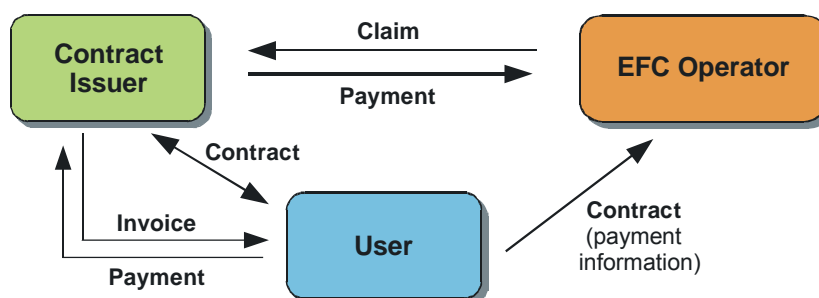
The CARDME domains

There will be someone in the 'Home' domain who provides the user with a contract to be used in the foreign domain. In CARDME this 'someone' is called the **Contract Issuer**. This may be a toll collection company that operates the 'home' EFC system. A financial institution may also be involved.

The operators in the 'foreign' domain are usually operators of toll collection systems. However, to be more generic allowing for other types of service providers, e.g. road pricing schemes, access control systems and parking lots the term **EFC operator** is used from now on and in the Part 2 specification.

When a user passes through a 'foreign' EFC system he presents his contract with his Contract Issuer. Based on the information presented, the 'foreign' EFC operator sends a claim to the Contract Issuer with the information required to collect the money from the user. This claim will include the data identifying the contract, the fee to be paid and some other data from the use of the service, such as the classification data.

The Contract Issuer will check the claim for its content. If the claim is genuine he will pay for it and the User will be charged for the transport service that has been used via his normal 'home' payment procedures. The figure below shows the basic entities and their relationships.



Basic entities in CARDME

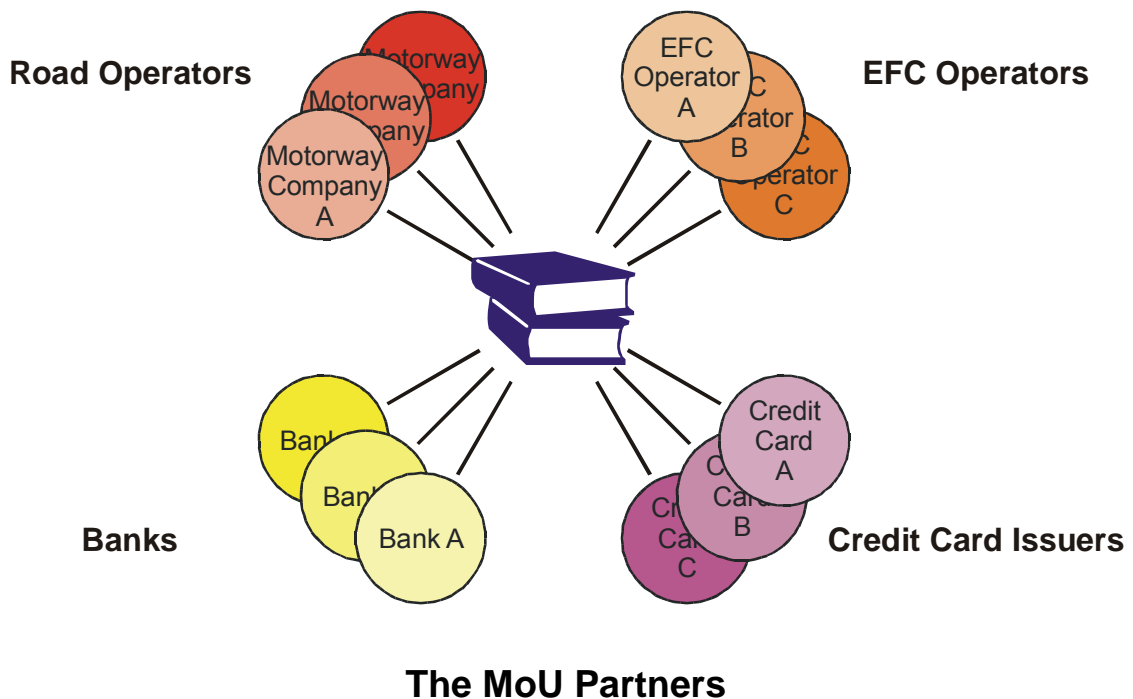
CARDME does not influence the 'home' systems, which can be EFC systems with totally different constraints and requirements. CARDME is an additional service co-existing with the 'home' EFC service. However, the claims from the foreign EFC systems will be merged with the claims from the home system. The User will experience one continuous and seamless service concerning both the use of transport services such as tolled roads, and the payment for use.

2 WHAT HAPPENS WHEN – CARDME PROCEDURES

The following scenarios describe the CARDME procedures. We meet two drivers who have different starting points for acquiring the contract and the On-Board Equipment (OBE) used for EFC. The first person we meet is a driver who has a pre-personalised ‘off-the-shelf’ OBE going on holiday in Europe. The other person is a truck driver who acquires a personalised OBE for the heavy goods vehicle he is driving. We also meet two people from the operators where one is providing the contract and the OBE and the other person is providing the transport service. In section 2.2 we have a scenario for the establishment of the contract between the EFC Operators and Contract Issuers.

2.1 THE MOU PARTNERS

Several European companies related to EFC agree on the basis for a common EFC payment service. This includes contracts between themselves, a standardised contract between the Contract Issuer and the User, a technical specification for the OBE, RSE and the wireless communication (Dedicated Short-Range Communication, DSRC) and a security architecture. Everything is included in the Memorandum of Understanding (MoU) signed by all the partners. Amongst the partners there are motorway operators, toll collection operators, banks and credit card institutions. Some are Contract Issuers, some are EFC Operators and some are both.

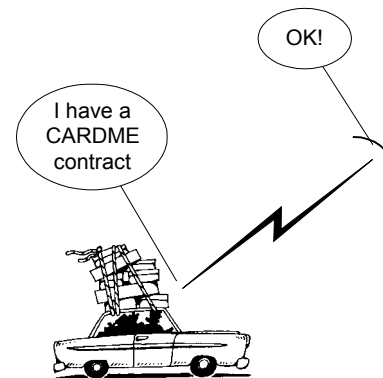


2.2 A USER OBTAINS AN OBE FOR A HOLIDAY TRIP

Mr. Harrison from Liverpool is preparing his summer holidays in the south of France. Last time he went there he had spent some time in the French toll collection systems paying manually but this time he wants to be better prepared.

He has heard about the new CARDME interoperable EFC service and decides to call the operator of his local system for Liverpool Road User Charges, LRUC, in order to investigate how to benefit from this new service.

Apparently the only thing he has to do is to wait for a new OBE that is sent to him by mail. The new OBE has the CARDME contract already implemented and he has only to return his old OBE that is customised with the LRUC contract only. Together with the new OBE he will receive some information on how to pass through foreign toll stations with the interoperable EFC services. His contract with the LRUC will be upgraded also covering the CARDME EFC service. The passages in French EFC systems will be added to his usual monthly invoice for the LRUC. Mr. Harrison is very happy with this solution.



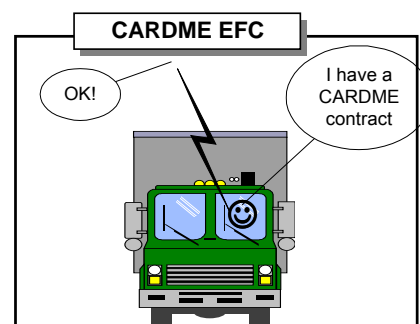
2.3 A DRIVER ACQUIRES A PERSONALISED OBE FOR A TRUCK

Mr. Carreras drives his truck transporting goods between Barcelona and the United Kingdom. He is tired of all the stops in toll collection systems. But there is hope. His commercial card issuer (often called petrol card issuer) has informed him about the new CARDME interoperable EFC service. The only two things he needs is an extended contract with the card issuer and an interoperable OBE installed in his truck.

Mr. Carreras calls the commercial card company and the next day he finds a contract form in his mailbox. He also gets information on how to proceed including a list of authorised OBE installation companies.

Mr. Carreras calls one of the authorised companies and makes an appointment the following day concerning the installation and personalisation of the OBE. He has learned that this has to be done as part of the security scheme to protect him and the operators from fraudulent use. Especially the detailed characteristics of his vehicle have to be entered into the OBE by a knowledgeable and trustworthy party since vehicle characteristics determine the tolling tariffs.

Having installed the OBE with the CARDME contract and the specific vehicle characteristics he goes for a trip to Liverpool. He is surprised to see just how continuous the use of tolled roads has become. He knows that next month there will be an invoice with all the fees from his passages through the toll stations to Liverpool and back.



2.4 AN OPERATOR HANDLES HIS LOCAL CUSTOMERS

Mr. Jarret works in the company operating the Liverpool Road User Charges system, LRUC. His company has joined the CARDME MoU on EFC. They have a lot of customers that are interested in the new interoperable EFC service, both private and commercial users. Yesterday he had a call from Mr. Harrison, one of his subscribers going on holiday in France. He wanted to have the upgraded OBE enabling him to drive through toll stations without stopping for manual payment.

This is an straightforward case to handle. Mr. Jarret takes one of the pre-personalised OBE for private cars, registers the OBE contract information in his central system and sends the OBE to Mr. Harrison requesting him to return the old one that only had the LRUC contract.

Mr. Jarret knows that he will receive some claims from French operators at the end of next week. This is according to the agreement between the operators that have joined the MoU. He, or rather his computers, will check the claims to see whether they are genuine. That is done automatically as prescribed by the security scheme they follow. Any claim that is not in line with the security specifications and measures is not accepted.

From his office window Mr. Jarret looks down on a charging point of LRUC. He spots a truck from Barcelona going through the lane for interoperable EFC, which means that a contract issuer in Barcelona will receive a claim for a truck passing the LRUC cordon around Liverpool.



2.5 AN OPERATOR HANDLES ROAMING CUSTOMERS

Mrs Dulac watches the traffic flows through the toll station. She is in charge of the daily operation of one of the toll stations on E15. Things have really improved the last years since the CARDME interoperable EFC service was established. Before that there used to be long queues with vehicles waiting to pay manually but now there are only queues at the beginning of the summer holidays. The company was able to reduce the operational cost due to the shift from manual attended lanes to EFC lanes. The charging of the fees is not a problem any more. The toll company she is working for joined the Memorandum of Understanding (MoU) three years ago and now all the EFC lanes in the toll station are upgraded to handle OBEs from a lot of other foreign EFC systems.

Mrs Dulac is a member of the General Assembly of the MoU. There is a small secretariat handling the administrative matters forming the 'body' of the MoU. The only external party is the company dealing with the security scheme. So far there was only one case of attempted fraud, a student from the university trying to communicate with the EFC equipment via a self-made OBE and his PC. The communication failed due to the security measures and he was enforced and fined for his fraud attempt.

Mrs. Dulac looks down on the toll plaza to see a family going on holiday passing through the EFC lane. From the licence plate she can see it is a car from the UK. 'Have a nice trip', she thinks, 'we will send a claim to your Contract Issuer'.

We will send a claim to your Contract Issuer







3 HOW IS IT DONE – CARDME TRANSACTION

3.1 TRANSACTION PHASES

3.1.1 The Four Phases of the DSRC Communication

When a user enters a manual tolling station, four phases can be discerned. The electronic CARDME transaction consists of the same four phases:

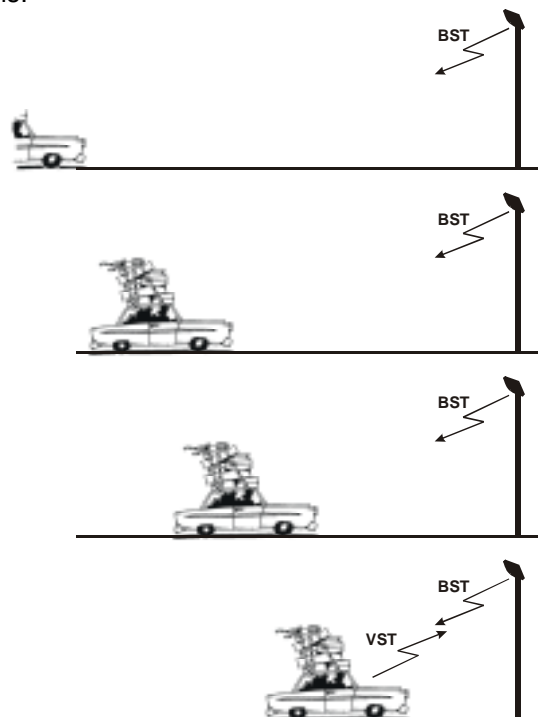
Initialisation		‘Hello, welcome, where do you come from, how do you want to pay’ Negotiation of the EFC contract to use
Presentation		‘Please give me your payment details and your entry ticket’ The RSE reads OBE data (details on contract, account, vehicle classification, last transaction, etc.)
Receipt		‘Here is your receipt’ The RSE writes an electronic receipt (which may also serve as an entry ticket)
Tracking and Closing		‘Thank you and good bye’ The RSE tracks the vehicle through the communication zone and eventually closes the transaction.

Irrespective of EFC station type (passage in an open system, entry or exit in a closed system) the transaction performed is always the same. Although the functionality of the different station types is quite different, there is a single CARDME transaction which is identical at all locations.

3.1.2 Say Hello - Initialisation

EFC beacons continually emit a signal in order to make contact with newly approaching vehicles. The data in this periodic signal is called the **Beacon Service Table, BST**.

As soon as a vehicle receives a BST, it answers with its **Vehicle Service Table, VST**. The **VST contains a list of all EFC-contracts** present in the OBE.



Upon reception of the VST the RSE analyses its contents and **decides whether it can accept one of the EFC contracts** presented by the OBE.

In case the RSE recognises a contract, **it knows exactly what to do from then on**. The RSE knows which organisation has issued the contract and, hence, where to send the claim and which transaction type is supported by the OBE. Although the RSE may have software available for several different EFC applications (e.g., software routines for the local EFC application and the CARDME application) only one piece of software is executed at a time. The Initialisation Phase can be seen as a switch where the RSE decides which path to follow. From the initialisation onwards, the RSE will (for a certain OBE) address a single EFC contract only. If however, the RSE cannot accept one of the EFC contracts presented by the OBE, the transaction will be terminated. As no information regarding the identity of the user has been exchanged at this point, the local exception handling procedures will need to be initiated.

An example of such an information exchange in the Initialisation Phase is given below for a beacon at a **French tolling station** communicating with an OBE in a **Norwegian vehicle**.



Road Side Equipment	On-Board Equipment						
BST: <i>'Hello, here is an EFC Station'</i>							
BST: <i>'Hello, here is an EFC Station'</i>							
BST: <i>'Hello, here is an EFC Station'</i>	(A vehicle is approaching. OBE wakes up and replies)						
	VST: <i>'Hello, I can offer the following EFC contracts and transactions:'</i> 1. <i>Transaction type 'AUTOPASS' Central account with the Operator 'NorwegTrans'</i> 2. <i>Transaction type 'CARDME' Central account with the Operator 'NorwegTrans'</i> 3. <i>Transaction type 'SPECIAL/LOCAL' Yearly pass from the Operator 'CityParking'</i>						
The roadside is thinking: According to my tables, I have the following transactions available and recognise the accounts with the following operators: <table style="margin-left: 20px;"> <tr> <td><i>Transaction</i></td> <td><i>Operator</i></td> </tr> <tr> <td>TIS transaction</td> <td>AREA COFIROUTE ESCOTA SANEF</td> </tr> <tr> <td>CARDME transaction</td> <td>AustroToll BelgiaPay NorwegTrans PagaMadrid</td> </tr> </table> When I compare my table with the VST, I see that I can recognise the second option offered by the OBE and, hence, will from now on use 'CARDME / NorwegTrans'	<i>Transaction</i>	<i>Operator</i>	TIS transaction	AREA COFIROUTE ESCOTA SANEF	CARDME transaction	AustroToll BelgiaPay NorwegTrans PagaMadrid	
<i>Transaction</i>	<i>Operator</i>						
TIS transaction	AREA COFIROUTE ESCOTA SANEF						
CARDME transaction	AustroToll BelgiaPay NorwegTrans PagaMadrid						

3.1.3 Read OBE Data - Presentation

In order to know which tariff to apply and which account to charge, the RSE needs to have some information from the passing vehicle. The RSE obtains this information via read commands sent over the DSRC link.



Note that the RSE addresses only data from the contract that it has chosen to use in the preceding Initialisation Phase ('NorwegTrans' in our example).

Road Side Equipment	On-Board Equipment
<p><i>'Please give me the following information about your CARDME contract with NorwegTrans:</i></p> <ul style="list-style-type: none"> - your personal account number (with signature) - your previous receipts - your vehicle classification details' 	
	<p><i>'With pleasure, here are the data you have asked for. I have added my signature to show that my data are correct and that you can trust to receive money</i></p> <ul style="list-style-type: none"> - my personal account number, with signature - my previous receipts (entry ticket) - my vehicle classification details'

The RSE uses the received data for the following purposes:

- **Payment means** including the **personal account number**. The account held at the issuer of the contract is identified through the Personal Account Number. Personal Account Number points to exactly one customer account held with a Contract Issuer in Europe. This information enables the EFC Operator to draw money from the account of a local user or to claim money from the Contract Issuer of a foreign user.
- **Previous receipts**. Two receipts, associated with the two most recent passages through EFC CARDME stations, are read from the OBE memory. (When an OBE passes an EFC station, a new Receipt is written into the OBE memory. See also the explanation of the Write-Phase below).
 - In a classical manual closed tolling system a user takes a ticket from an automatic ticket dispensing machine when he enters the motorway. At the exit the user shows this ticket to the tolling personnel, who calculates the fee from the distance matrix entry-exit. The same thing happens electronically. Some systems also require the last but one receipt to determine the fee. This is especially the case when there are alternative routes through the (motorway) network.
 - In an open toll system, where one pays per passage of a bridge, a mountain pass or a stretch of motorway, reading the last receipt is of little use to the RSE. In CARDME it is done anyway, in order to have the same transaction everywhere, regardless of station type.
- **Vehicle classification details**. In some systems, the applicable tariff is determined from the vehicle class measured at the tolling station. In other systems, vehicle class is determined from the data in OBE (the so called 'declared classification'). These OBE-declared vehicle-related data are read out here. The declared vehicle characteristics are sufficient for any RSE to determine the applicable tariff. Systems that measure class can ignore these data.
- **Signature**. The OBE adds several security-related data to the tolling data, here simply called 'Signature'. CARDME foresees several different such security data, and even an optional second read-command for roaming users, in order to cover all security needs. These security measures are discussed in a separate chapter. In CARDME it is mandatory for OBEs to produce these security-related data. It is important to note, however, that **using the security data is optional** in the sense that the roadside may simply ignore them. From a technical point of view, every operator is free to decide which of the security data he wants to check, when and where he wants to check them, or whether he wants to check them at all.

3.1.4 Write New OBE Data - Receipt

In the previous phases the RSE has read all data that are required to charge the user (either directly for local users or indirectly for roaming users, who are charged via their contract issuers).



The receipt phase is used to write all data to the OBE that will be carried to the next tolling station ('you can only read what you have written before'). It is also time to inform the user about the success of the tolling transaction.

Road Side Equipment	On-Board Equipment
<p><i>'Please store the following information in your memory:</i></p> <ul style="list-style-type: none"> - Transaction receipt (entry ticket) <p><i>Inform the user about the success of the transaction'</i></p>	
	<p><i>'I confirm. I have stored the ticket and I have given the user a signal'.</i></p>

The most important data that have to be written into the OBE is the **entry ticket**. In closed tolling systems it is essential that this information is carried from one tolling station to the next. Also for other system types it makes sense to give an **electronic receipt**. This receipt is not primarily intended as direct information for the user since very few OBEs currently have the capability of displaying the rather complex receipt information. The receipt rather serves as a record of past transactions in case a dispute arises.

The two latest receipts will be stored in the OBE. These are transmitted over the DSRC link as 'ReceiptData1' and 'ReceiptData2'. The RSE and not the OBE keeps track of what is old and what is new, in order to have a simple OBE design. The RSE always reads and writes both receipts. When writing, the RSE writes the new receipt to ReceiptData1 and it copies the data just read under ReceiptData1 (in the presentation phase) to ReceiptData2.

The information in the receipt or in the entry ticket, respectively, comprises:

- Passage data and time
- Passage location (EFC operator, station number, lane number, station type)
- Passage result (OK / not OK, wrong class, blacklisted, security error, etc.)
- Applied vehicle/tariff class
- Used contract

In addition, **the user is informed** about the success of the transaction. The OBE signals the user one of three messages 'OK', 'not OK' and 'Contact Operator'.

Also in the Write-Phase there is security-related information added to the data. These security data do not influence the tolling functionality and are treated in Chapter 3.2.4.

3.1.5 End the Transaction - Tracking and Closing

At this stage in the transaction all tolling-related data exchange is done. A communication failure which could affect the transaction is no longer possible.



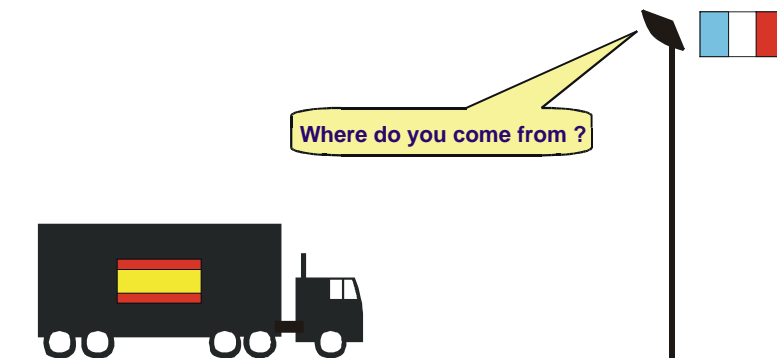
Some technical house-keeping tasks are required, namely to track the vehicle through the communication zone (mainly required in free-flow installations with video-enforcement) and/or to formally close the transaction, i.e. telling the OBE that there is no more to come.

3.2 TRANSACTION DATA

3.2.1 Contract - From Which MoU Partner do You Come ?

When a vehicle approaches an EFC station, the RSE must, at the very beginning of the transaction, obtain some basic information from the passing vehicle. This fundamental information tells the roadside how to proceed with the transaction. The OBE sends the required information in the first block of data transmitted over the radio link in the Vehicle Service Table, VST (see Chapter 3.1.2 on the Initialisation).

A user may have several EFC contracts in his OBE at the same time, e.g., the standard local EFC contract which he uses every day when commuting to work, plus a CARDME contract for use when he is travelling to other EFC systems, plus a yearly pass for the garage where he has a fixed parking space. The OBE presents all available contracts in the VST so that the RSE can decide which one is applicable.



From the first data transmitted the RSE must know whether it can recognise a contract ('where do you come from' – is the contract provider known to me, i.e. part of the MoU). Naturally different contracts use different data and may also have different transaction types (e.g. Autopass transaction, TIS transaction or CARDME transaction). The RSE has to store a table that lists all contract types that it can recognise. The MoU partners have to install procedures to exchange and regularly update the list of accepted Contract Issuers and Types of Contract.

For every contract the VST contains the following information (which is called the 'Context Mark' of the contract):

Name of data element	Content with example	Meaning for the road side with example
Contract Provider	Country code and contract issuer code <i>Norway, NorwegTrans</i>	Contract issuer. If the issuer is part of the MoU, the EFC operator will understand all the rest of the data, otherwise not. <i>The EFC operator will send his claim to NorwegTrans of Norway, who is part of the MoU.</i>
Type of Contract	Code for type of contract. <i>CARDME transaction, international contract, pre-personalised OBE</i>	A code with a meaning that is agreed by all MoU partners (otherwise it has only local meaning). <i>In this case the RSE has to use the software for the CARDME central account transaction. Only the pre-personalised class information is available. The extended class information cannot be read.</i>
Context Version	Version number <i>Version code 3</i>	A number that says according to which version of the transaction specification the OBE has been produced. <i>CARDME transaction version 2002.</i>

3.2.2 Classification - What Type of Vehicle do You Have ?

For the majority of tolling systems within Europe the level of charge incurred for a given passage is dependent on the type of vehicle used. Heavy goods vehicles, HGVs, usually pay more than passenger cars. In traditional stop-and-pay systems this vehicle categorisation is done by exchanges between the toll booth attendant and the driver.

Measured and Declared Classification

In an EFC system there is no toll booth attendant present so an alternative method must be employed. Two different approaches have been adopted:

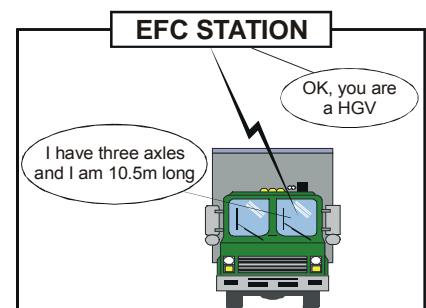
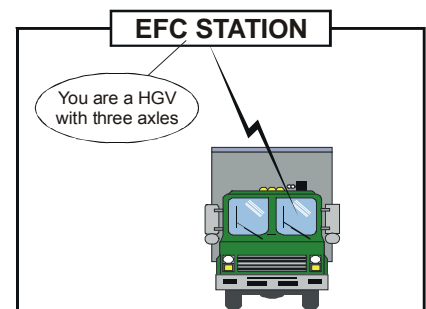
1. Measured Vehicle Parameters

Sensor arrays are installed to measure specific vehicle characteristics in order to determine the class. In mono-lane systems it is possible to measure a wide range of physical characteristics, e.g. number of axles, presence of dual tyres, length, height, etc. In a multi-lane environment sensor technology usually restricts the measurable parameters to length, height and width.

It is not possible to measure non-physical characteristics of vehicles such as Maximum Laden Weight or Euro emission class.

2. Declared Vehicle Parameters

Vehicle details are stored in the OBE and read out during the transaction. The details stored can either be a simple vehicle class ('Passenger Car') or a set of vehicle parameters from which the RSE determines the correct vehicle category. In a single operator environment it is feasible to just declare a system specific vehicle class. In a multi-operator environment, however, unless there is a harmonised classification system, an agreed set of vehicle parameters must be declared.



Flexibility for Operators: The CARDME Concept offers a high degree of flexibility in the approach to classification adopted by toll operators across Europe. Both measured and declared characteristics are supported. However, in order to deliver this flexibility across Europe, it is mandatory that all OBEs carry declared vehicle data. Entering detailed vehicle classification data into the OBE requires skilled and trustworthy personnel, some special equipment for data entry into the OBE, and makes OBE distribution considerably more complicated and costly. With an OBE that is personalised with detailed vehicle characteristics it has also to be assured that the OBE is not moved from vehicle to vehicle. CARDME offers a solution to this, see below.

Naturally, in systems relying on measured characteristics, the declared characteristics can either simply be ignored or be used to check the plausibility of the automatic measurement.

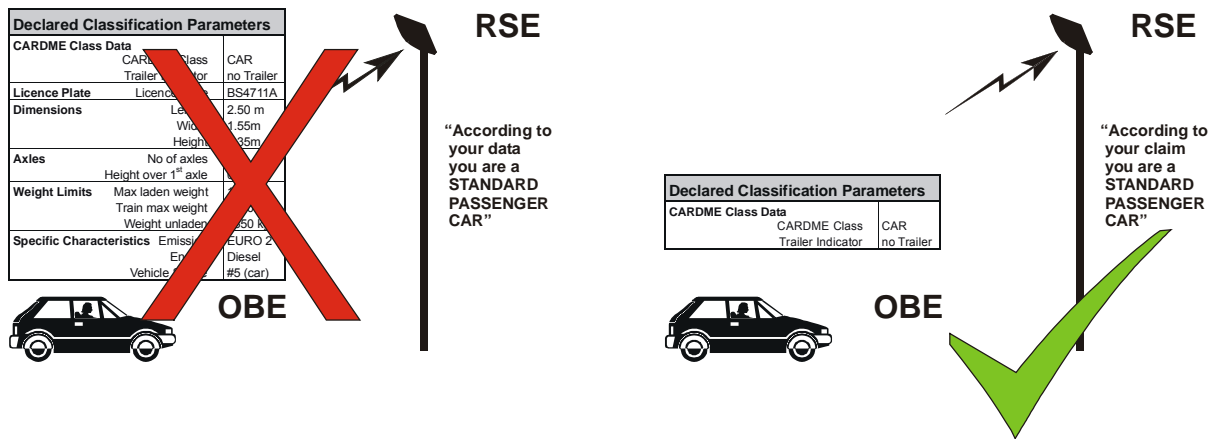
Support for Pre-Configured and for Personalised OBE

Passenger cars and heavy goods vehicles have very different needs:

A **normal passenger car** falls into the 'car' class in practically every European tolling system. Thus it is not required for a car to have a lengthy list of vehicle characteristics entered into its OBE. CARDME believes that it is possible to find **common European interoperable classes for clear-cut cases**. Probably 80% to 90% of all vehicles are clear cases. For them, pre-configured OBE can be produced.

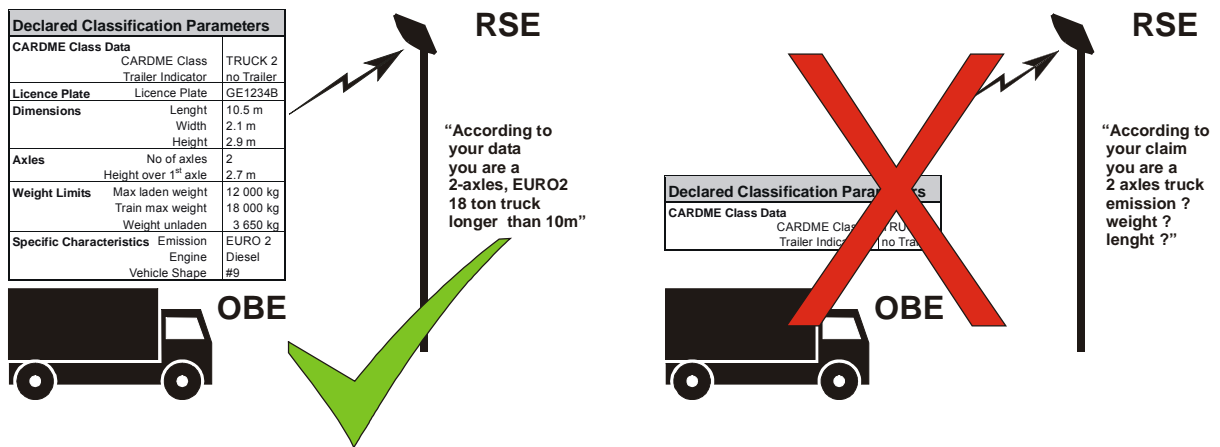
Pre-configured OBE are

- **easy to distribute.** There is no need to enter complex vehicle specific data. The OBE can be issued on signature of a contract at any convenient outlet, such as a petrol station.
- **user friendly.** Since they only carry a general class information and no vehicle specific details, pre-configured OBE fit any 'similar' vehicle. The user may move his OBE from one vehicle to another.
- **low cost.** Pre-configured OBE can be personalised at the time of manufacture. There is no need to have costly individual personalisation done by skilled personnel with specialised equipment in a trusted environment at customer service centres. A pre-configured OBE constitutes an off-the-shelf product.



For a standard passenger car:
 Personalised OBE is too complicated Pre-configured OBE is preferred

A heavy goods vehicle will rarely fall into a clear cut interoperable class. Many countries are introducing heavy vehicle fees with rather complex classification, where tariff depends amongst other on maximum laden weight of truck and trailer and on emission values. A simple class-concept is unlikely to be able to fit the classification needs for commercial vehicles.



For a heavy vehicle:
 Personalised OBE is often required Pre-configured OBE is rarely sufficient

Clearly, it would be ideal to serve both needs.

CARDME offers exactly this flexibility. CARDME supports both pre-configured OBE and OBE carrying detailed classification information.

For clear cut cases, i.e. when one of the common European interoperable classes is applicable, there is no need for further data. OBEs with pre-configured class information can be produced and distributed.

For all other cases, such as most heavy commercial vehicles, CARDME provides a comprehensive list of vehicle classification parameters that supports all known tariffing policies.

3.2.3 Receipt - Where did You Enter the Highway ?

At every tolling station the same CARDME Transaction is performed, regardless of tolling system – open or closed. One and the same CARDME transaction is used for all systems under all circumstances.

In every CARDME Transaction a ‘Receipt’ is read from the OBE and then written again. In other words, the roadside always reads the Receipt given at the last station and then writes a new one for the next station. This way information is carried from one station to the next.

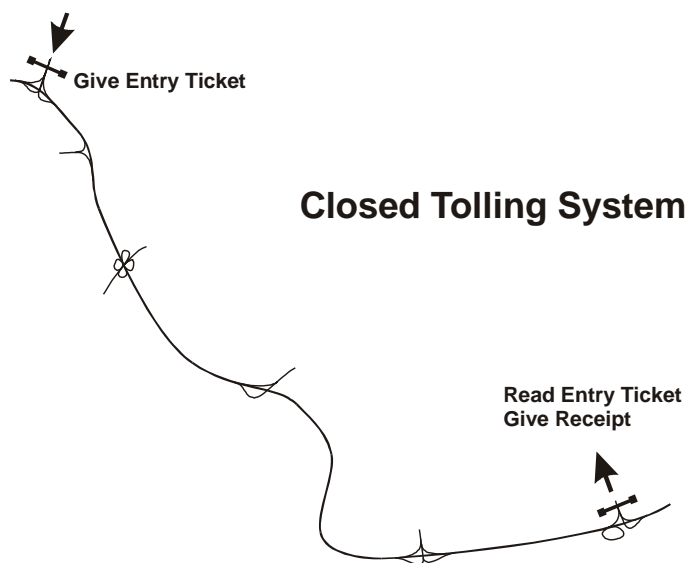
In fact even two receipts are read: the last and the last but one. All CARDME OBEs store two receipts in order to have some record of travel history in the OBE in case a dispute arises.

For tolling purposes, normally only the last receipt is required. Although the same receipt data are always read and written, their function differs for the different tolling systems:

In a **Closed Tolling System** the tolling stations are at the entries and exits of the highway. There are no stations on the highway. On entering the highway one receives an ‘entry ticket’ which is then used at the exit to determine the origin of the trip.

The same is done in CARDME. All necessary entry information is stored in the ‘Receipt’ given on entry. (Note that on entry automatically also an old Receipt – presumably from the last trip - is read. This ticket is ignored by the entry station.)

This ‘Receipt’ is then read out at the exit, the fee is calculated, and a new Receipt is given. This Receipt serves the same purpose as its manual counterpart: it is a proof of payment. Note that ‘entry operator’ and ‘exit operator’ can also be different parties that have a roaming agreement.

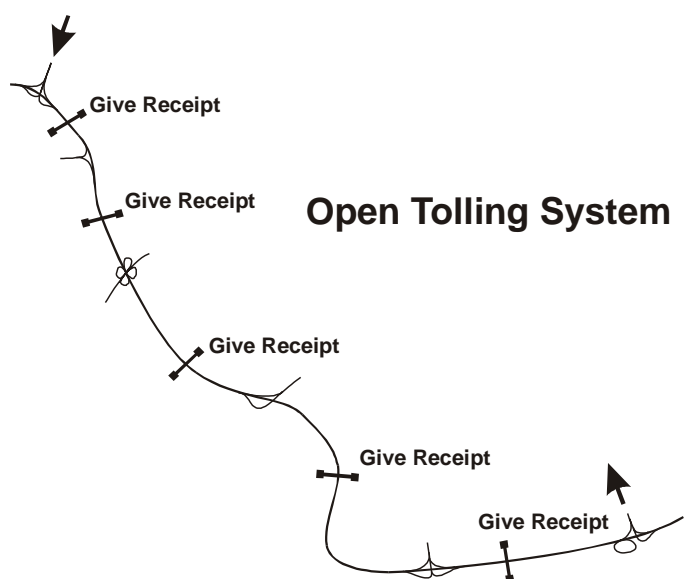


In an **Open Tolling System** the ‘Receipt’ has a totally different meaning. In an open system one pays a fee for passing a tolling station. As shown on the picture to the right, these stations could be on different segments of a highway, but pay-per-passage stations are also found on bridges, at tunnels, and on mountain passes.

For these stations it is irrelevant to know the history of the vehicle passing. There is no such thing as an ‘entry ticket’.

In order to have a single transaction type applicable for all stations, in CARDME the old ‘Receipt’ is read anyway. It is simply ignored by the open tolling station.

Analogous to the Closed System, a new Receipt is written at every station. It simply serves as a proof of passage and of payment.



3.2.4 Security - Can I Trust You ?

In any EFC-system there will be users who will try to find ways to use the transport service without paying for it. They may attempt to achieve this e.g. by:

- declaring wrong class info (trailer switch)
- changing data (account information, vehicle classification info) stored in the OBE
- engineering a fake-OBE that produces the required messages using an existing valid account number, or one that replays recorded messages of an old transaction with another OBE
- jamming the RSE-transceivers with a powerful RF-source in the environment.

The actual risks of fraud depend on a number of system characteristics, e.g. the local 'cultural environment', the typical transaction amounts, the number of users and the scope of the service (e.g. a single regional service provider or an international scheme with multiple-service providers).

In most EFC systems some measures are taken to prevent and detect fraud. The strength and complexity (=costs) of these 'security measures' however differs widely from implementation to implementation. In some cases sophisticated cryptographic integrity and authentication services are used to protect the data exchanged between OBE and RSE, in other cases a blacklist is regarded sufficient. In general the level of security implemented is balanced with the perceived risk level the system is exposed to.

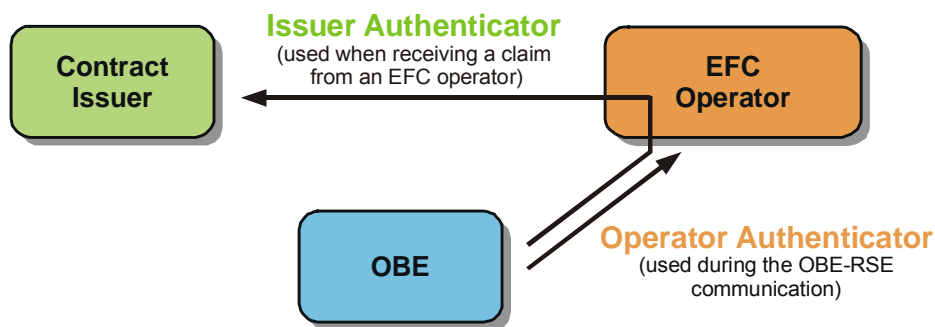
The flexibility of the CARDME security architecture enables the EFC operators and Contract Issuers to choose their own level of security from a wide range. It can be adapted over time to the threats perceived by each EFC operator. Moreover, it allows them to choose the most suitable time for smooth migration to stronger security provisions, if desired. To make such migration practically feasible, all CARDME-compliant OBEs are capable of supporting all security options 'on-board'.

The generic security services available in CARDME are the following:

- **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 available security services provide an adequate level of protection against all the threats foreseen in a widespread and large-scale network of interoperable EFC systems.

One of the main features is that the CARDME security architecture is built on two different domains concerning security key management. One domain is strictly controlled by the entity that issues the payment means (Contract Issuer) and one domain is common for all the entities (EFC Operators) that collect payment information from the users passing through a toll station paying by means of EFC. Hence, a disclosure of one or more secret keys in the most vulnerable domain, which is the one common for all EFC Operators, will not harm the Contract Issuer domain.



The payment information authenticators associated with the two security domains

The EFC Operators verify by means of the Operator Authenticator, associated with a secret key managed by the EFC Operators, whether the OBE is genuine and whether the payment information it has transmitted during the transaction is as stored by the Contract Issuer at the time of OBE-RSE communication. The Contract Issuer verifies at a later stage by means of the Issuer Authenticator, associated with a secret key managed by the Contract Issuer, whether the OBE is an OBE personalised by Contract issuer and whether the claim from an EFC Operator is a genuine one.

The CARDME security architecture also includes a Transaction Counter. When an EFC transaction is completed the value of a counter in the OBE is increased with 1. The value of the Transaction Counter is sent to the Contract Issuer as part of the claim and enables the Contract Issuer to monitor the performance of the OBE and other EFC systems. It also enables the Contract Issuer to detect fraudulent users who have changed the functionality or data in the OBE or EFC Operators sending more than one claim for the same transaction.

A GOOD sequence of Transaction Counter values in claims	A BAD sequence of Transaction Counter values in claims	A BAD sequence of Transaction Counter values in claims
1	1	1
2	2	2
3	3	2
4		3
5	5	4
6	6	4
7	7	5
8		6
9	9	6

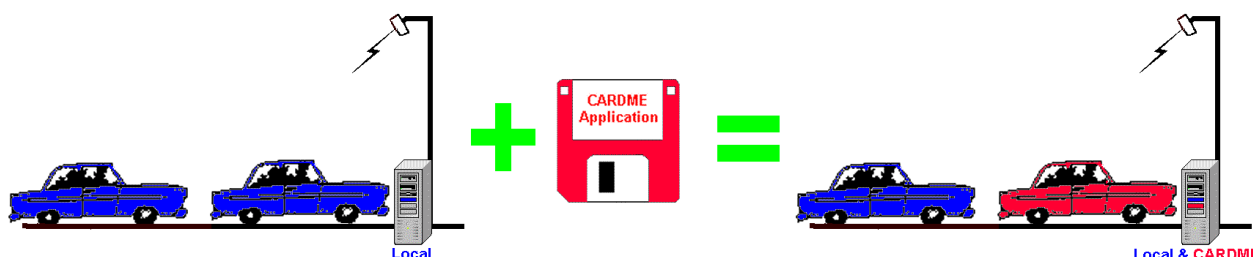
Examples of sequences of Transaction Counter value received by the Contract Issuer

3.3 TRANSACTION IMPLEMENTATION

3.3.1 How to Add CARDME to Existing Installations

Staged Implementation Path for Roadside Equipment

CARDME offers a staged implementation path for operators adopting the new service. It is intended that CARDME is offered as additional service alongside any existing systems. It is possible for any standards compliant beacon to operate both the CARDME service and the local system at the same time without affecting system reliability or performance. All that is needed is a “software” update in each beacon to handle the new service.



Based on the BST/VST exchange of information in the initialisation phase the Road Side Equipment switches to the appropriate software - local or CARDME application - for the current session.

Whilst the CARDME Concept can offer operators a high degree of security due to the flexible approach it can be implemented initially without the need for dynamic security across the air link. It is up to the operator to decide the degree of security that is employed within his system. If necessary this level can be increased with time by implementing additional security features at the roadside equipment.

CARDME on-board equipment

Once an operator has signed up to the CARDME service it is likely that some of his existing users will wish to benefit from the new European Service. For these users a new OBE will need to be issued, containing the CARDME transaction and contract, plus the local transaction and/or contract.

For private car users this is a relatively straight forward process, the user's contract details will need to be entered into a pre-personalised 'CARDME car' OBE and sent to the user along with information relevant to the new service.

For all other vehicles the OBE will need to contain a defined set of vehicle specific measurements as well as the user's contract details. The vehicle details can either be obtained as part of the contract or the vehicle measurements can be entered into the OBE by an approved outlet.

Links to other Systems

In order to receive reimbursement from 'foreign' Users it will be necessary to form links to the Contract Issuers so that claims can be sent to the appropriate entity and payment recovered. Through this link claims for roaming local users in other schemes will also be received as well as updated lists of invalid OBEs from other systems.

3.3.2 How to Protect Privacy

Privacy and Electronic Fee Collection

International and European regulations impose restrictions on the collecting, storage, processing and dissemination of data relating to individuals and their behaviour. Individual national legislation is based on these principles. As information relating to movement of individuals is used in EFC applications these regulations impose obligations on EFC Operators and Contract Issuers.

The need for **anonymity is seldom a strong requirement** from users. However, most **users require the protection of their privacy** by the Contract Issuer and/or EFC Operator.

The privacy of the user is maintained if the following conditions are met:

- Only relevant personal data needed for the opening of an account is requested from the user
- The itemised disclosure of the service consumption on the invoice is an option that can be chosen by the user
- The Contract Issuer cannot disclose the personal related information to third parties

It is possible to meet these conditions with a central account in an EFC system.

In some countries legislation requires that the option of a fully anonymous usage of the infrastructure is provided. In these countries the user has to be offered the choice between a true anonymous payment means like cash or taking an alternative non-tolled route. At present time total anonymity in interoperable EFC systems cannot be ensured. In the future, international electronic purses may offer anonymity in these systems.

Privacy and Central Accounts

Electronic fee collection using Central Accounts generally involves the collection of data relating to individuals, such as the identification number of the contract, which is exchanged in each transaction. In principle this identification number can be linked to the name of the customer. In the case of post-payment the connection is obvious: the Contract Issuer needs to invoice the customer in accordance with the actual consumption of the service.

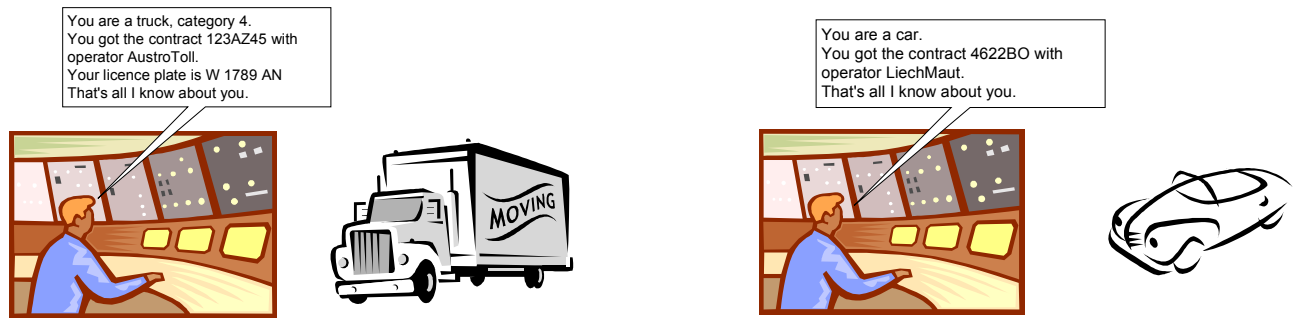
It is conceivable that users could be offered pre-paid central accounts which are not directly linked to an individual. As long as the balance associated with the account is sufficient, the EFC Operator is guaranteed payment by the Contract Issuer. If insufficient balance occurs, the account can simply be blacklisted.

However, it is not feasible to offer such a service on a European scale. In order to be guaranteed payment each RSE would need up-to-date information to decide whether there is sufficient balance on the account, which would require 'online' access to the Contract Issuer. Typically EFC Operator and Contract Issuer exchange data once a day.

Privacy and CARDME

As CARDME is based on central accounts, the previous subsection fully applies. In addition a few specific remarks can be made.

The messages exchanged between an ordinary passenger car OBE and the RSE do not contain any information that can be linked directly to a person, not even to a vehicle licence number or bank account. The Personal Account Number (PAN) is declared in the data exchange between RSE and OBE, however, only the Contract Issuer can relate this identifier to an individual. As a consequence the foreign EFC Operator cannot relate passages to the contract holder / user.



For heavy goods vehicles a mandatory set of vehicle parameters is exchanged which includes the licence plate number. However, as with the PAN, the database linking the licence plate number to the vehicle keeper is held by an organisation other than the foreign EFC operator. In addition it should also be noted that in most cases for commercial vehicles the vehicle registers do not link licence plate numbers to individuals but to companies.

A possible option to increase the level of privacy protection in CARDME is to implement a formal and procedural division between Contract Issuer and (home) EFC Operator. The Contract Issuer is now the only party with access to the customer database. The EFC Operator is the only party with access to passage details. The EFC Operator could only forward accumulated amounts to the Contract Issuer for invoicing.

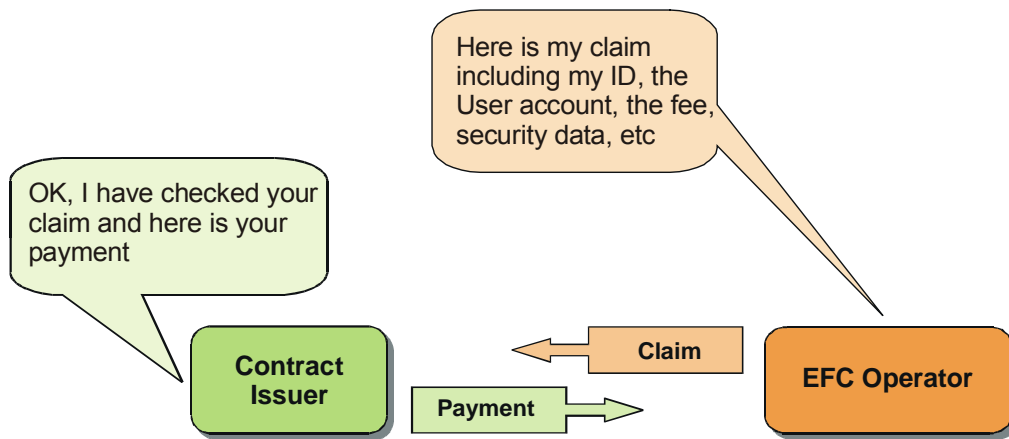
The EFC Operator can offer the user the opportunity to have an itemised bill by providing him access to trip information via internet or by including in the data sent to the Contract Issuer truncated trip data containing only enough detail for the user to identify the trip. Hence neither the Contract Issuer nor the EFC Operator can link detailed passage data to individuals.

In summary, several legal requirements on the handling of data relating to individuals gathered by an EFC implementation have to be fulfilled. The CARDME Central Account is an acceptable basis to provide privacy protection to the users. When the user is roaming in a 'foreign' network, a high level of privacy is ensured. The EFC Operator is only able to obtain information relating to the identification of a contract and not about the user.

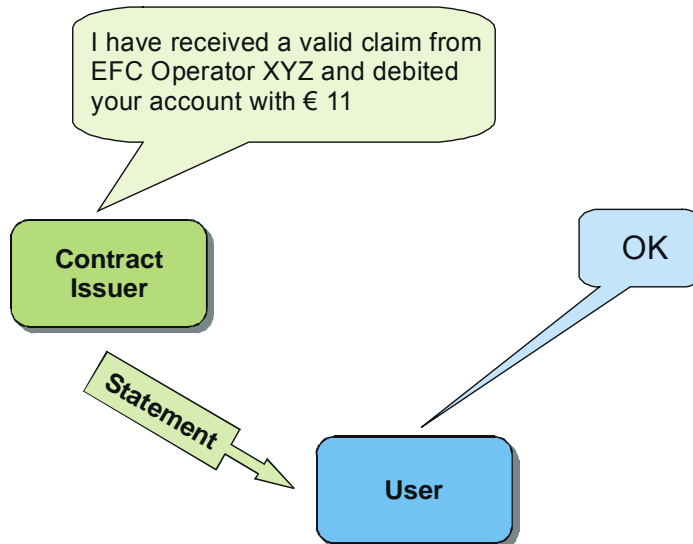
3.3.3 How to Get Paid for a CARDME Transaction

The EFC operator providing the transport service, e.g. the use of a tolled road, will issue a claim to the Contract Issuer, i.e. the entity that issued the CARDME contract to the user. The claim will be based on the information collected at the use of the service. The most crucial information will be the identity of the EFC Operator, the Personal Account Number, the fee that has been charged and security data.

The Contract Issuer may check the validity of the claim using the security data included. Any valid claim will be reimbursed by the Contract Issuer according to the MoU.





The Contract Issuer will then send the user an invoice or debit his account and send a statement.



3.3.4 How to Proceed when an Exception Occurs

There are a number of points during the transaction phases when exceptions can occur which will need to be handled by the RSE.

The following table indicates the types of exception that can occur during the Initialisation and Presentation phases of the transaction:

<p>Initialisation</p>		<ul style="list-style-type: none"> ▪ Non equipped user ▪ Contract not accepted
<p>Presentation</p>		<ul style="list-style-type: none"> ▪ OBE blacklisted ▪ Contract validity expired ▪ Transaction failure ▪ Sequencing error (missing entry ticket)

In all these cases it will be necessary for the local exception handling procedures to be initiated. For all systems without barriers this will initially involve capturing 'proof of passage'.

The MoU will define the procedures for the exchange and updating of blacklists. EFC Operators will be guaranteed payment for passages for non-blacklisted contracts, for other cases the EFC Operator is responsible for the recovery of payment.



The MoU could be extended to include possible support for co-operative exception handling, where the Contract Issuer of the user has been identified. For other cases the standard local exception handling and enforcement procedure will have to be applied, without support from the MoU.

The increasing number of free-flow multi-lane EFC systems require exception systems which do not stop the vehicle and have a deferred identification processes. Consequently, exceptions are only identified after the use of the tolled road and the proof of passage has to be presented to recover payment.

The main issue concerning cross-border enforcement and assistance in the case of violation of fee collection rules is the legal jurisdiction. The legal jurisdiction defines the competence of the courts of law.

In Europe, no common legislation exists for minor offences. The jurisdiction for a minor offence is generally bound to the court of the area where the offence has been committed. The highest level where decisions of these courts can be appealed is within national borders.

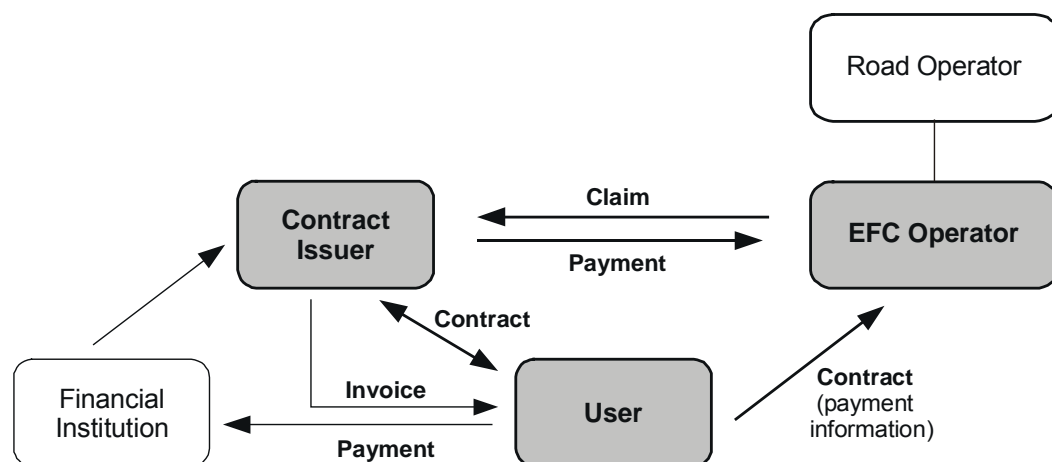
Until common European legislation is established defining the legal jurisdiction for cross-border enforcement, the legal responsibility of vehicle owner and the requirements for proof of evidence, Enforcement will not be an issue of interoperability but has to be handled locally.

PART TWO: THE CARDME SPECIFICATION

1 CARDME ARCHITECTURE

1.1 INTRODUCTION

The figure below shows the CARDME Architecture. The three crucial entities are the User, the Contract Issuer and the EFC Operator. An overall and simplified description of the CARDME concept is given in Part One. This chapter gives a more detailed description of the concept including all its entities and their roles. A certain degree of abstraction is needed to cover any scenario but some practical examples are given to make it more like 'real-life'.



The CARDME Architecture

In an *interoperable* environment there has to be an entity that gives the User the rights to benefit from transport services provided, e.g. in other countries, using the same payment means (Central Account) and payment medium (OBE) as the User does in his local environment. These rights are based on a contractual relationship, i.e. the MoU, between the entity giving the rights to the User and the entities providing a transport service, e.g. the use of a tolled road.

In the CARDME architecture the **Contract Issuer** is responsible for giving the rights to the users who want to benefit from transport services paying via the interoperable EFC system.

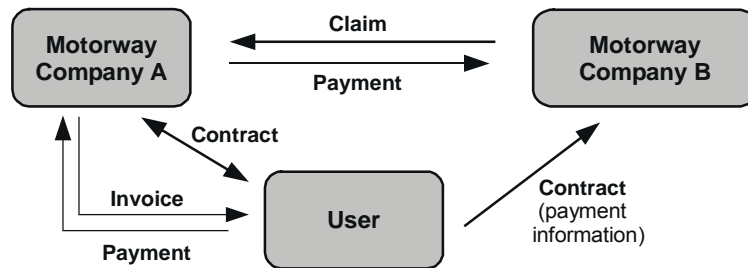
The entities that provide EFC payment services are the **EFC Operators**.

CARDME is concentrating on the payment systems and not on the different transport services themselves. The **Road Operator** manages and maintains the road.

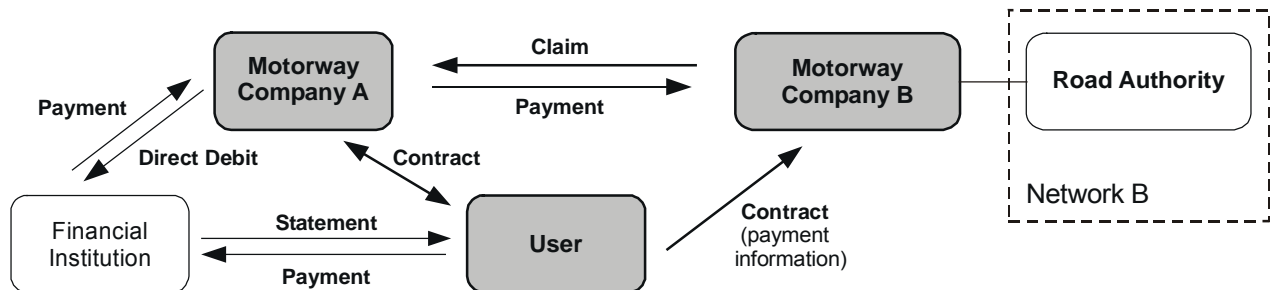
CARDME focuses on the interoperability aspects of the payment system. This service will usually be added to an existing payment relationship between User and Contract Issuer which in most cases will involve a **Financial Institution**, e.g. the bank of the User or his Credit Card company.

A single organisation can in practice encompass more than one functional entity of the CARDME architecture. For example a motorway concession holder is often the Road Operator, EFC Operator and Contract Issuer. The figures below show two examples of how the abstract entities above may become real entities or companies.

In the first example the User has a contract in one motorway company (network A) and use the network operated by another motorway company (network B).



In the second example a road authority owns and operates the network B while the EFC payment service is provided by a toll collection company acting on behalf of the road authority providing the transport service. As in the first example motorway company A has issued the contract. This time the user does not pay the motorway company directly. He has given the motorway company the permission to debit his bank account directly. The bank will send the user a statement, an 'advice of debit'.



1.2 ORGANISATIONS IN THE CARDME ARCHITECTURE

Name	Contract Issuer
<i>CESARE term</i>	Issuer
<i>14906 term</i>	Contract Provider
<i>Definition</i>	Identifies the organisation that issued the service rights to the User, either implicit or explicit.
<i>Main tasks</i>	<ul style="list-style-type: none"> • User information • Initialise OBE with contract data (could also be done by an agent, e.g. the supplier of the OBE or a company installing the OBE) • Receive and handle claims from EFC operators • Pay for transport services provided by Road Operators • Charge Users for their use of 'foreign' transport services
<i>'Real-life'</i>	Toll operators, financial institutions (e.g. banks or credit card companies)

Name	EFC Operator
<i>CESARE term</i>	EFC Operator
<i>14906 term</i>	Session Service Provider
<i>Definition</i>	Identifies the organisation that provides an EFC payment service to the User.
<i>Main tasks</i>	<ul style="list-style-type: none"> • Implement the CARDME application • Provide an EFC payment service to the User • Communicate with OBE and calculate a fee • Send claims to Contract Issuers • Receive payments from Contract Issuers
<i>'Real-life'</i>	Toll operators, operators of parking houses, operators of access control systems, operators of road user charges systems

Name	Road Operator
<i>CESARE term</i>	Road Operator
<i>14906 term</i>	- (no equivalent)
<i>Definition</i>	Identifies the organisation that provides a transport service to the User.
<i>Main tasks</i>	<ul style="list-style-type: none"> • Provide a transport service to the User • Provide constraints, requirements and other working conditions for EFC operators collecting fee for transport services provided. • Receive payment from EFC operators
<i>'Real-life'</i>	Motorway companies, road authorities, infrastructure owners

<i>Name</i>	Financial Institution
<i>CESARE term</i>	User's Bank
<i>14906 term</i>	-
<i>Definition</i>	Organisation that manages the user's account and credits the Contract Issuer in relation to passages made by the user
<i>Main tasks</i>	<ul style="list-style-type: none"> • Acts as link between the user and the Contract Issuer
<i>'Real-life'</i>	Banks, credit card companies

<i>Name</i>	MoU Secretariat
<i>CESARE term</i>	Central Organisation
<i>14906 term</i>	-
<i>Definition</i>	Identifies the organisation that manages the MoU
<i>Main tasks</i>	<ul style="list-style-type: none"> • Management of crucial EFC information like EFC-ContextMarks, Key generations, Personal Account Numbers and black lists • Management of marketing and user/public information • Secretariat for MoU General Assemblies and MoU Technical committees
<i>'Real-life'</i>	Organisation owned and paid by the Contract Issuers and Road Operators, one of the major toll operators, toll operator association

<i>Name</i>	Trusted Third Party
<i>CESARE term</i>	-
<i>14906 term</i>	-
<i>Definition</i>	Identifies the organisation that manages the CARDME security scheme
<i>Main tasks</i>	<ul style="list-style-type: none"> • Secret key management including generation, storage, distribution, installation, registration and destruction of secret keys • Audits of organisations handling secret keys, e.g. the EFC Operators.
<i>'Real-life'</i>	Organisation separate from MoU secretariat owned and paid by the Contract Issuers and EFC Operators, financial institutions or their subsidiaries

The two last organisations are not shown in the architecture figures in order to make the figures as simple as possible.

2 CARDME PROCEDURES

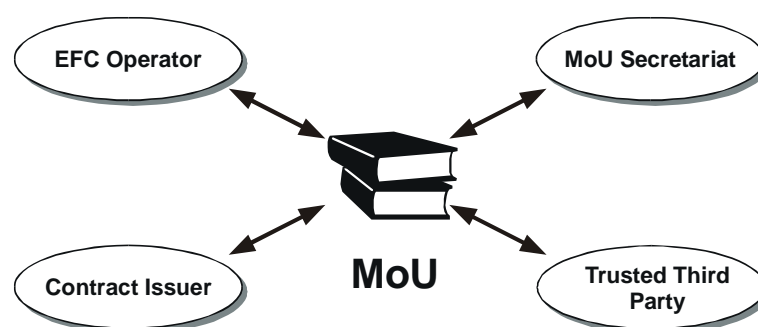
The CARDME procedures are described by four scenarios or use cases:

- MoU management and implementation
- Contract Issuing
- Charging
- Payment

The first use case is described by a simplified entity-relationship figure as it is not a sequential procedure as the three others. For the last three use cases several sequence diagrams are used. The sequence diagrams only show the *information* flows.

2.1 MoU MANAGEMENT AND IMPLEMENTATION

The figure below gives an overview of the organisations involved in the MoU management and implementation. It should be kept separate from the matter of who signs the MoU.



The **EFC Operator**, e.g. a toll operator, implements the MoU both in an organisational and technical way. The technical matters will be the implementation of the MoU requirements for:

- Roadside Equipment
- Central system
- Security scheme including installation, storage, protection and use of security keys
- Communication protocols between equipment held by User, EFC Operators, Contract Issuers and Trusted Third Party.

The **Contract Issuer**, e.g. a toll operator, also implements the organisational and technical requirements of the MoU. In addition to that, one important task will be to act as an agent for the MoU secretariat concerning marketing, PR and User information. As concerns the Contract Issuer, the technical aspects of the MoU are:

- Use of EFC-ContextMarks, Contract Issuer identification, Personal Account Numbers, Classification principles (vehicle classes and vehicle characteristics)
- On-Board Equipment
- Central system
- Security scheme including installation, storage, protection and use of security keys
- Communication protocols between equipment held by User, EFC Operators, Contract Issuers and Trusted Third Party.

The **Trusted Third Party** is responsible for the key management including but not limited to the generation, registration, distribution, storage, protection and destruction of secret keys. The main contribution to the MoU implementation will be to provide a security architecture that fulfils the MoU security requirements.

The **MoU secretariat** is acting as an administrator and manager of the MoU on behalf of and in line with the guidelines from the group of companies having joined the MoU. The management and implementation of the MoU will involve the following:

- Management of critical EFC information like EFC-ContextMarks, Key generations, Personal Account Numbers and black lists
- Management of marketing and user/public information
- Secretariat for MoU General Assemblies and MoU Technical committees

2.2 CONTRACT ISSUING

Two use cases are used to describe two completely different scenarios for issuing a contract:

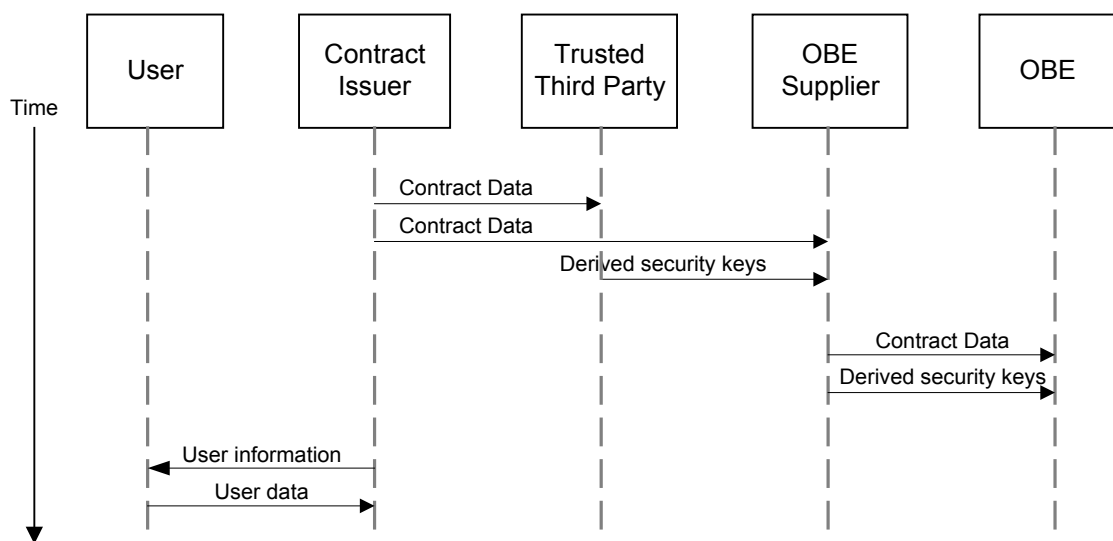
- Acquire an ‘off-the-shelf’ OBE
- Acquire a personalised OBE

The CARDME architecture allows for both scenarios as well as every applicable and feasible scenario between the two scenarios below.

NOTE: The ‘off-the-shelf’ use case is used for scenarios where there is no need for storing vehicle characteristics in the OBE, i.e. the OBE is used for vehicles with certain vehicle characteristics, e.g. a total permissible weight of 3500 kg (light vehicle) or length less than 6,00 meters. This implies that the owners of light vehicles have an easy access to the OBE as it can be sold pre-personalised in a widespread distribution network, e.g. petrol stations, car-dealers and supermarkets. It also enables the owners to move the OBE from one vehicle to another, for instance when the owner changes his car and wants to have the same OBE and contract for the new car. The ‘off-the-shelf’ scenario could be used for about 90% of the vehicles on the road.

Acquire an ‘off-the-shelf’ OBE

The sequence diagram below shows the use case where a user acquires a pre-personalised OBE from the Contract Issuer or from an agent acting on behalf of the Contract Issuer such as a supermarket or a petrol station.

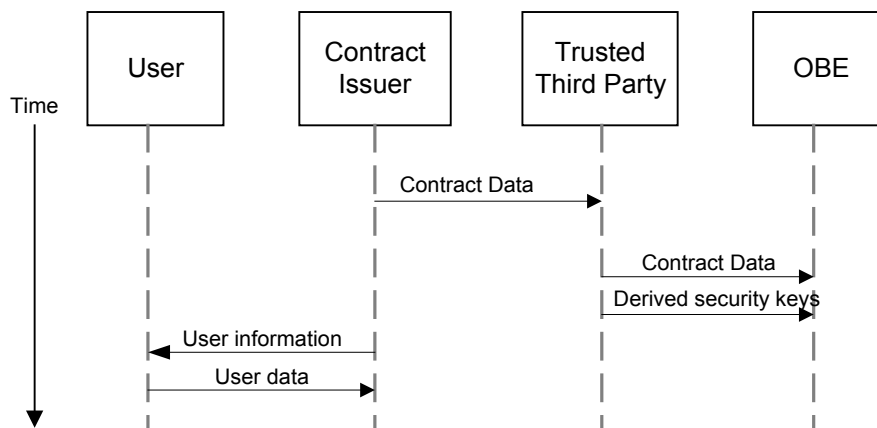


Sequence diagram for Contract Issuing for an ‘Off-the-shelf’ OBE

The Contract Issuer, being responsible for the contract including the OBE, gives the Contract data (no personal information of the User) to the Trusted Third Party (TTP) and the OBE supplier. The TTP uses the information for deriving the OBE-specific keys to be installed in the OBE. The OBE supplier uses the contract data and the derived security keys for personalisation of the OBE. The OBEs are delivered to the Contract Issuer or his agents for distribution to the users.

The User is informed by the Contract Issuer or his agent about the CARDME interoperable EFC systems and conditions for use. Depending on the requirement of the Contract Issuer the User gives some information to the Contract Issuer, e.g. name and address for invoicing or bank account details for automatic debiting.

The figure below shows an alternative solution that is better for security. The TTP initialises the OBEs and deliver them to the Contract Issuer or his agents for distribution to the users.

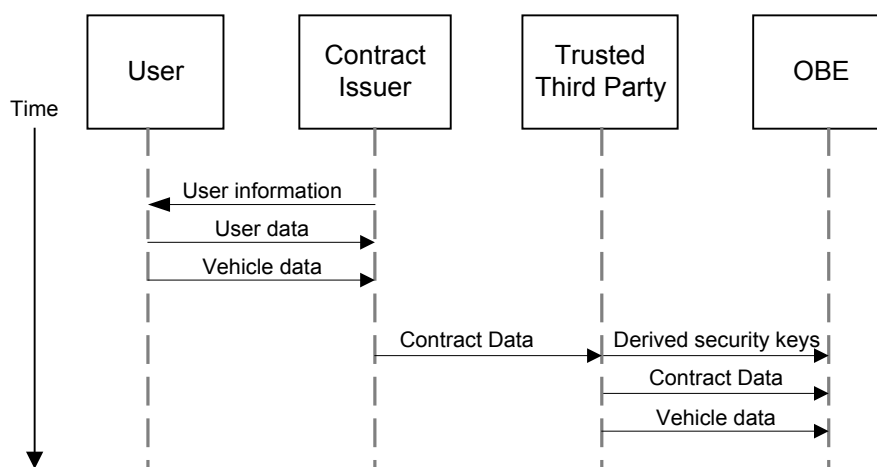


Alternative personalisation

Acquire a personalised OBE

The figure below shows the sequence diagram for the use case where a user acquires a personalised OBE from the Contract Issuer or an agent acting on behalf of the Contract Issuer, e.g. an authorised workshop or petrol station.

The Contract Issuer, a toll operator for example, or his agent, informs the User about the CARDME interoperable EFC systems and conditions for use. The User then gives the required information to the Contract Issuer including for instance name and address for invoicing and the characteristics of the vehicle where the OBE shall be installed.

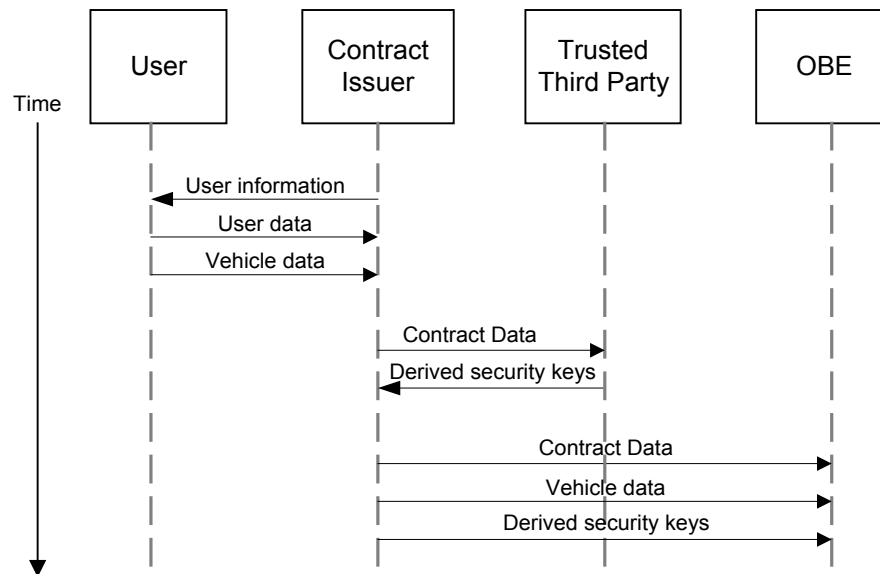


Sequence diagram for Contract Issuing for a personalised OBE

The Contract Issuer, being responsible for the contract including the OBE, gives the Contract data to the Trusted Third Party (TTP). The TTP uses the information for deriving the OBE-specific keys to be installed in the OBE and then stores all data in the OBE. The OBE is then delivered to the Contract Issuer or his agents for installation in the vehicle.

The next figure shows an alternative procedure for acquiring a personalised OBE. The TTP receives the Contract data used for deriving the secret keys and returns the keys within a secure application module to be installed in the OBE by the Contract Issuer or its agent, e.g. an authorised workshop.

NOTE: Within the CARDME scheme each operator can choose his own procedure of contract issuing and OBE distribution and/or installation allowing an adaptation of the local constraints and requirements. The only requirements are that the data shall be according to the CARDME specification and the procedure is done a secure way protecting the sensitive and secret data.



Alternative procedure for acquiring an OBE

Data stored in the OBE upon issuing

The following information must be stored in the OBE to enable the CARDME interoperable EFC system:

- Identification of the entity (Contract Issuer) issuing the contract for the use of the transport service (service rights)
- Identification of the Type of Contract and Context Version
- Identification of the contract (Payment means including the Personal Account Number and the associated expiry date and validity restrictions). It is assumed that one Personal Account Number is always associated with exactly one OBE. This enables for instance blacklisting of a specific OBE.
- Security keys both for the Contract issuer and the EFC Operator authenticators. The keys belonging to the Contract Issuer are only known by the Contract Issuer while the keys for the EFC Operators are shared between the EFC Operators.
- Identification of Access Credentials references. The CARDME scheme enables both the use and non-use of access control of data stored in the OBE. The CARDME default value is no access control.
- Initial values for Transaction Counter and Equipment status
- For pre-configured 'off-the-shelf' OBEs: Vehicle class information according to a classification scheme agreed amongst the interoperable EFC operators (simplified classification according to the common European interoperable classes with no individual, vehicle-specific characteristics)
For personalised OBEs: Vehicle characteristics data (list of vehicle classification parameters)

2.3 CHARGING

The use case Charging is the scenario where a user benefits from a transport service and the EFC Operator collects enough information to charge the user for the transport service provided, typically charging a vehicle that passes through a toll station. The User is able to use the transport service with the contract he has with the Contract Issuer.

The use case Charging can be divided into the following procedures:

- Detection of vehicle
- Classification of vehicle
- Communication with the OBE (interoperable EFC transaction)
- Calculation of the fee
- Handling of Exceptions

Detection of the vehicle is a matter of Roadside system implementation and is not an issue related to interoperability. The same goes for calculation of the fee and handling of exceptions. It is assumed that each EFC Operator defines and implements his own solutions independently of other EFC Operators.

Communication with the OBE is a crucial matter for interoperability. Classification is also a crucial matter in those cases where the vehicle class or vehicle characteristics are stored in the OBE. However, classification by reading data from the OBE is in this document defined being part of the Communication with the OBE.

The use case Charging is shown on the next page.

NOTE: The figure shows just one of many examples of roadside implementations. Within the CARDME scheme each EFC Operator is free to implement any solution as long as he fulfils the specification for the communication in the shaded area of the use case figure. The specification of the communication is given in Chapter 3 'CARDME Transaction' and Chapter 2 of the Annex 'Transaction'.

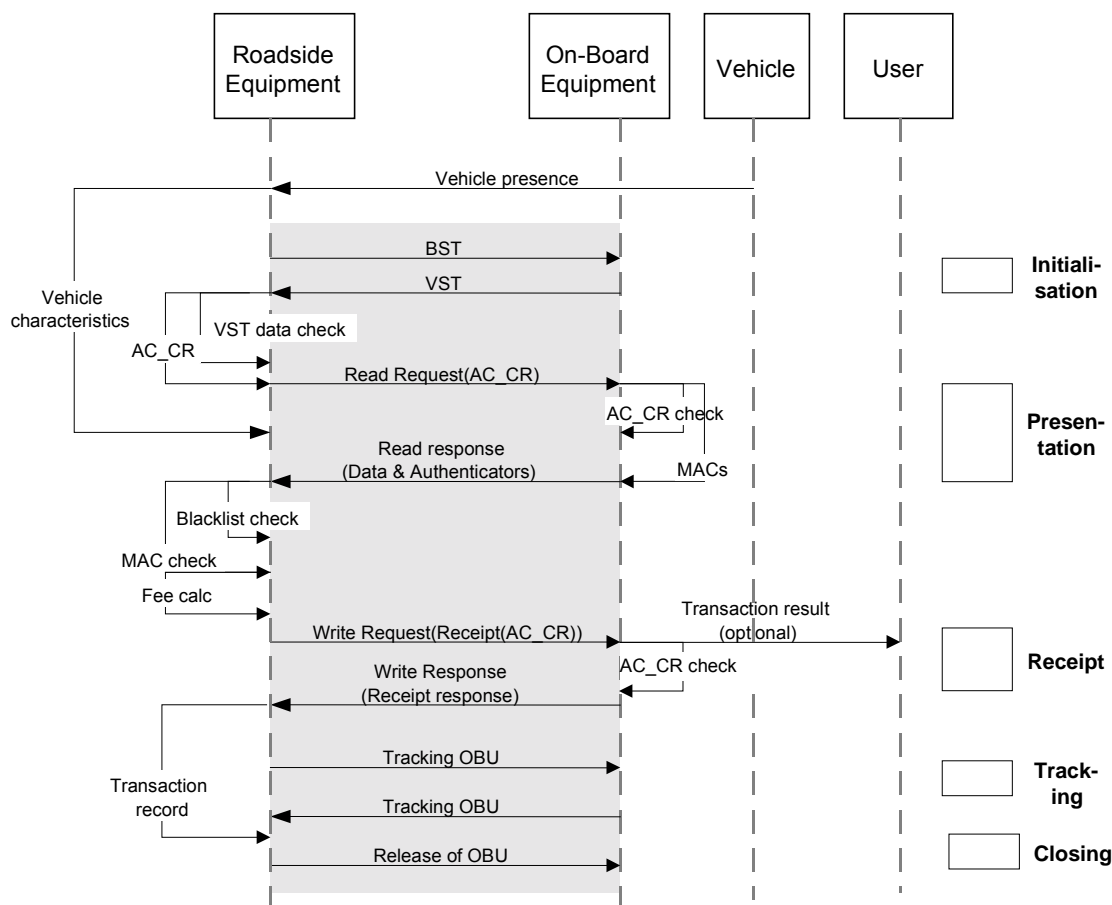
A vehicle presence is detected by the Roadside Equipment. A picture (or pictures) of the licence plate may be stored for later enforcement or proof of transaction. Also the vehicle characteristics may be measured for fee calculation or verification of declared characteristics (data stored in OBE).

The Initialisation phase (BST-VST) covers the standardised exchange of information that shall always precede the exchange of payment-related information between the On-Board Equipment (OBE) and the Roadside Equipment (RSE). By transmitting the Beacon Service Table (BST), the RSE informs any OBE entering the communication zone that it is within a charging zone for electronic fee collection. The BST is received by the OBE and triggers an answer, the Vehicle Service Table (VST), which includes some information about the OBE and the information it is carrying, e.g. EFC Contract provider and type of EFC Contract.

The RSE checks the information from the OBE, principally the Contract Issuer and the context version, and calculates the Access Credentials (if required).

The Presentation phase includes a set of EN ISO 14906 commands used by the RSE to get the information needed to calculate the fee to be charged in a secure way (Read request). The request for information will always be followed by an answer from the OBE after the OBE having checked the Access Credentials (if requested). The answer (Read response) will include the requested information and two authenticators enabling both the EFC operator and the Contract Issuer individually to check that the OBE is genuine and that the EFC information presented is authentic. In the figure "Vehicle Characteristics" indicates verification of the declared vehicle against measured characteristics. Note that this is just an implementation example.

The Receipt phase includes the EN ISO 14906 command used by the RSE to write a receipt to the OBE after the information from the OBE has been accepted and processed. This will consist of several data elements describing the operational and financial result of the handling of the information given in the Presentation phase. The writing of the information to the OBE is done in a non-secure way (Write Request), as the threats can be overcome by other security measures, for example a receipt authenticator. This is also the phase where the RSE informs the OBE to give a signal to the driver that the transaction was successful by writing text to a display, or a beep or a visible signal such as a green LED. The OBE responds to the request by a confirmation that the writing has been done and the information to the user has been given by returning the message (Write response). The whole session is recorded (Transaction record) and will be part of the claim from the EFC Operator to the Contract Issuer.



Use case Charging – implementation example

The Tracking phase includes the phase where the RSE keeps track of the OBE in the communication zone. This may be needed depending on the operational environment, e.g. when the communication zone covers several lanes (multi-lane situation).

The Closing phase is just the release of the OBE from the session.

The following data will be retrieved from the OBE during the EFC transaction:

- Identification of the entity (Contract Issuer) issuing the contract for the use of the transport service (service rights)
- Identification of the Type of Contract and Context version
- Identification of the contract (Payment means including the Personal Account Number and the associated expiry date and validity restrictions)
- Vehicle class or vehicle characteristics data
- Equipment Status (includes a transaction counter value)
- Receipt from last transaction
- Receipt from second last transaction
- Authenticators calculated with a key known only by the Contract Issuer and a key known by all EFC Operators having signed the MoU

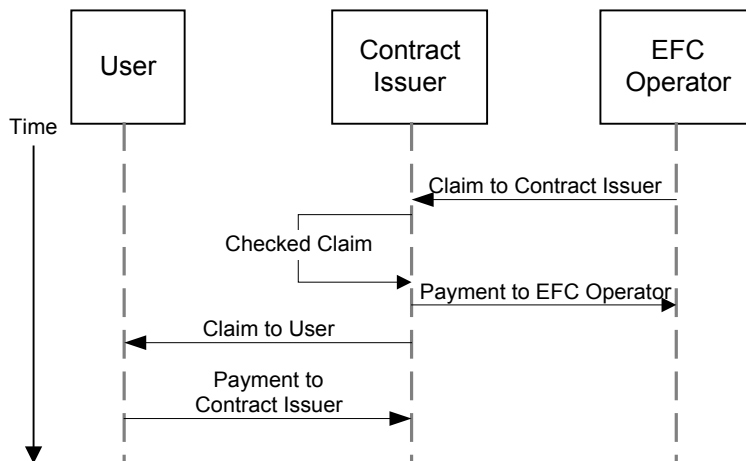
The following data will be written to the OBE during the transaction:

- Receipt from this transaction
- Receipt from the previous transaction
- Receipt Text, which is any message to be written to an OBE display (MMI)
- Equipment Status, including the transaction counter (previously read value + 1)

2.4 PAYMENT

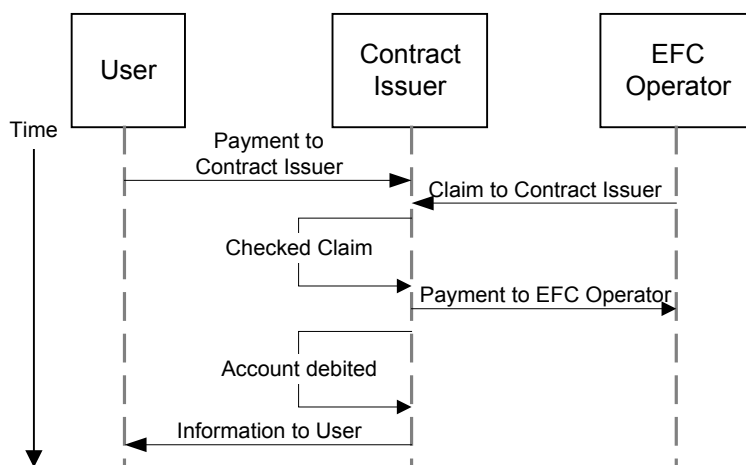
The sequence diagram for the use case Paying for the use of services is shown below. The EFC Operator, acting on behalf of the Road Operator who has provided the transport service, such as the use of a tolled road, sends a claim to the Contract Issuer based on the Transaction record. The Claim is checked by the Contract Issuer depending on the security level implemented. If the claim is found to be valid the Contract Issuer pays the EFC Operator.

The Contract Issuer sends an explicit (e.g. an invoice) or an implicit claim (e.g. automatic withdrawal from an account) to the User. The user pays the Contract Issuer depending on the payment method and agreed type of money transfer, e.g. via the bank of the User.



Sequence diagram for paying for the use of services – (post-payment)

The sequence diagram shown above is one of several alternatives. The sequence describes a system where the User pays after he has used the service having received an invoice from his Contract Issuer. Another example is shown below where the User has a pre-paid Central Account kept by the Contract Issuer. Any accepted claim leads to a debiting of the account and the user is informed that so has been done on a regular basis.



Sequence diagram for paying for the use of services – (pre-payment)

The 'Claim to User', the 'Information to User' and the 'Payment to Contract Issuer' are outside the scope of the CARDME interoperable EFC systems being a matter between the User and the Contract Issuer. This can be done by invoices, bank account withdrawals with an information note from the bank, cash payment and any possible payment arrangement.

The 'Claim to Contract issuer' is a crucial issue for interoperability, as the claim has to fulfil certain requirements in order to be accepted by the Contract Issuers.

The claim shall contain the following information:

- Session Service Provider, i.e. the identity of the EFC Operator providing the payment service
- A unique Claim ID
- Contract Issuer and Payment means including the Personal Account Number
- Place and time, i.e. the session location (e.g. toll plaza number) and session time
- Session Fee
- Information on whether VAT is included or not
- Equipment Status including the value of the transaction counter in the OBE
- An Authenticator (using the secret key of the Contract Issuer) enabling the Contract Issuer to check whether the claim is genuine as well as the integrity of the claim.
- The key reference used by the OBE to calculate the authenticator in the previous bullet point
- Unique reference(s) to the file(s) with picture(s) linked to the transaction.

The 'Payment to EFC Operator' must, as a minimum, include a unique reference to the original claim enabling the EFC Operator to settle his accounts when receiving the payment.

3 CARDME TRANSACTION

3.1 TRANSACTION PHASES

3.1.1 Transaction Overview

Phase	Roadside Equipment		On-board Equipment	Remarks
Initialisation (BST - VST)	INITIALISATION.request (BST)	→		The RSE periodically sends BST in order to probe for newly arriving vehicles
		←	INITIALISATION.response (VST) <ul style="list-style-type: none"> EFC-ContextMark AC_CR-Reference RndOBE 	A newly arrived vehicle answers with standardised VST EFC-ContextMark consists of ContractProvider, TypeOfContract, and ContextVersion Gives the reference for the Access Credential Keys to use by the roadside RndOBE is a Random Number the RSE uses when calculating the Access Credentials
Presentation (GET)	GET_STAMPED.request AC_CR <ul style="list-style-type: none"> Payment Means including PersonalAccountNumber (RndRSE, KeyRef_Op) GET.request AC_CR <ul style="list-style-type: none"> ReceiptData1 ReceiptData2 EquipmentStatus Classification data: <ul style="list-style-type: none"> VehicleClass VehicleDimensions VehicleAxles VehicleLicencePlateNumber VehicleWeightLimits VehicleSpecificCharacteristics 	→		GET, and ask OBE to calculate an Authenticator that proves 'OBE is genuine' OBE will give access only when RSE provides the correct Access Credentials AC_CR Personal Account Number, pointing to the user contract/account at the contract issuer Random number and key reference for the authenticator that the OBE calculates
		←	GET_STAMPED.response <ul style="list-style-type: none"> Operator_Authenticator (Auth_Op) GET.response	Read whether Contract is still valid Read last receipt (entry ticket or last transaction) Read next to last receipt Read the equipment status (which includes a transaction counter) Read declared classification data Vehicle Class also gives information on trailer presence Vehicle Axles includes information on presence of dual tyres VehicleSpecificCharacterisitcs include information on emission class, engine type, etc.
				OBE responds with the data asked for, plus an Authenticator calculated with the 'interoperable key', i.e. with a key known to all EFC Operators

Phase	Roadside Equipment		On-board Equipment	Remarks
Optional Presentation for Foreign OBEs	GET_STAMPED.request AC_CR • Payment Means including PersonalAccountNumber (RndRSE, KeyRef_Iss)	→		For OBEs from a foreign Contract Issuer, the RSE asks for the calculation of an additional authenticator over the Payment Means (incl. Personal Account Number) with keys only known to the Contract Issuer, so that one can prove that the vehicle actually has passed.
		←	GET_STAMPED.response • Issuer_Authenticator (Auth_Iss)	
Receipt (SET)	SET.request AC_CR • ReceiptData1 • ReceiptData2 • EquipmentStatus • ReceiptText	→		Write new receipts (or entry ticket) Write new status information and increment transaction counter (Optionally) Write some textual information to display to the user
	SET_MMI.request			Give an 'OK' indication to the user (normally the OBE will beep)
		←	SET.response Set_MMI.response	
Tracking	ECHO.request	→		Track OBE by exchanging dummy information
	Etc...	←	ECHO.response	
Closing	EVENT_REPORT.request (Release)	→		RSE closes transaction and releases OBE

The table above gives the CARDME-Transaction in terms of the sequence of data that is exchanged between roadside and onboard equipment. A detailed, bit-level technical specification is given in Chapter 2 of the Annex.

3.1.2 Initialisation Phase

<i>Phase</i>	<i>RSE</i>		<i>OBE</i>
<i>Initialisation</i>	INITIALISATION.request (BST)	→	
		←	INITIALISATION.response (VST) Data for EFC Contract #1 (e.g. from local EFC system): <ul style="list-style-type: none"> • EFC-ContextMark <ul style="list-style-type: none"> – ContractProvider – TypeOfContract – ContextVersion • (optional additional data) Data for EFC Contract #2 (e.g. CARDME European Service) <ul style="list-style-type: none"> • EFC-ContextMark <ul style="list-style-type: none"> – ContractProvider – TypeOfContract – ContextVersion • AC_CR-Reference <ul style="list-style-type: none"> – AC_CR-MasterKeyRef – AC_CR-Diversifier • RndOBE Data for EFC Contract #3 <ul style="list-style-type: none"> •
<i>Presentation</i>	GET_STAMPED.request GET.request	→ ←	GET_STAMPED.response GET.response
<i>Optional Presentation</i>	GET_STAMPED.request	→ ←	GET_STAMPED.response
<i>Receipt</i>	SET.request SET_MMI.request	→ ←	SET.response Set_MMI.response
<i>Tracking</i>	ECHO.request	→ ←	ECHO.response
<i>Closing</i>	EVENT_REPORT.request (Release)	→	

Purpose of the Initialisation Phase

An EFC beacon continually emits a signal in order to make contact with newly approaching vehicles. This periodic signal is called **Beacon Service Table, BST**. The BST contains no other application related information than **'here is an EFC station'**. The BST gives no indication on country, operator, transaction type, etc.

As soon as a vehicle with an EFC OBE receives a BST, it answers with its Vehicle Service Table, VST. The **VST contains a list of all EFC-contracts** present in the OBE. An EFC contract is identified by its **EFC-Context-Mark**. According to the relevant standards, the VST may in addition to the Context Mark contain further information required by the individual EFC contracts (e.g. Security key references, random challenges or OBE serial number). The VST also contains the address that the OBE chooses for the communication with the current beacon.

Upon reception of the VST the road side equipment analyses its contents. The **RSE decides whether it can accept one of the EFC contracts** represented by the EFC Context Marks of the VST.

In case the RSE recognises a contract, it will from this step onwards address only data pertaining to this contract. A read-command issued by the RSE in the subsequent Presentation Phase, hence, will contain the following information: 'from contract number 2, I want to GET the data element *vehicle class*'.

When the RSE recognises a certain EFC-ContextMark in the Initialisation Phase it knows exactly what to do from then on. The EFC-ContextMark contains information on the issuer of the contract (e.g. the 'home operator'), on the type of contract (e.g. 'CARDME European EFC Service') and on a context version (CARDME-4 Specification, Version 1, with 3rd Security Key Generation). Issuer and type of contract also

determine transaction type (say TIS French national specification or AUTOPASS Norwegian national specification or CARDME European specification). With transaction type we mean the exact sequence of steps to be performed during the DSRC communication session.

Note: The above data exchange is described on the application level. There are also more technical negotiations going on between RSE and OBE, e.g. in order to arrive at a mutually agreed DSRC communication profile, determining amongst other parameters which subcarrier frequency the OBE shall use on the up-link.

CARDME Data in the Initialisation Phase

RSE periodically broadcasts the Beacon Service Table, BST

The RSE indicates its presence to passing OBE by periodically sending out its Beacon Service Table (BST). The BST details which application(s) the RSE supports. For EFC, the application identification code (AID) equals 1. The BST is fully standardised and contains nothing CARDME-specific.

OBE answers with the Vehicle Service Table, VST

The OBE, having detected the presence of the RSE and gathered what application(s) it wants to execute, sends a return signal by means of its Vehicle Service Table (VST).

In our case, the OBE wants to (or rather has to) execute an EFC application. In its VST the OBE sends a list of all EFC transactions it supports. Every EFC transaction supported by the OBE is represented by a data element called the 'EFC-Context Mark'. An EFC-Context Mark indicates which operator issued the contract in the OBE, the type of contract and a version number (context version, i.e. application/software/key versions).

The CARDME Context Mark

For CARDME the ContextMark contains the standardised EFC context mark defined by EN ISO 14906:

- ContractProvider: A code standing for the Contract Issuer (the code contains the country of residence of the Contract Issuer and a nationally assigned number identifying the individual issuer)
- TypeOfContract: A data element that gives the RSE basic information on the EFC contract residing in the OBE (for example: central account or on-board purse; pre- or post-paid; unlimited or restricted to a certain concession area; discount tariff applies; etc.). Within CARDME currently only one type of contract is defined, namely the 'CARDME European central account transaction'.
- ContextVersion: This data element is used by the OBE to tell the RSE the Version of some data it contains. For CARDME it says something like 'I am built according to CARDME-4 Specification V1.0, and I have been personalised using interoperable Security Key Version 3'.

In addition to mandatory contents above, according to the standard (EN ISO 14906) the ContextMark may contain further information. CARDME makes use of this feature and has defined the following additional data as part of the OBE response in the CARDME ContextMark.

- AC_CR-Reference: A reference number that tells the RSE which keys to use when calculating the Access Credentials. CARDME supports both key generations and key diversification (see Chapter 4 of the Annex for details).
- RndOBE: This data element contains a number that is freely chosen by the OBE and not predictable by the RSE (hence RndOBE, which stands for 'random number generated by the OBE'). The number has to be used by the RSE when calculating the Access Credentials. This guarantees that the RSE has to calculate the Access Credentials afresh for each session. This avoids someone erecting an unauthorised beacon using Access Credentials he has obtained through listening to correct EFC transactions.

The VST contains no data that might have privacy implications. The VST is accessible to any standards-conformant beacon. No interested party can either be forbidden or technically prevented from reading VST information. Hence, in CARDME the VST contains no information that allows identification of the vehicle.

Note: BST and VST include further standardised content like time information, EquipmentClass, ManufacturerID, and OBStatus which may be used for technical management purposes but are of no relevance for the EFC application itself.

3.1.3 Presentation Phase

<i>Phase</i>	<i>RSE</i>		<i>OBE</i>
<i>Initialisation</i>	INITIALISATION.request (BST)	→ ←	INITIALISATION.response (VST)
<i>Presentation</i>	GET_STAMPED.request AC_CR <ul style="list-style-type: none"> • Payment means including PersonalAccountNumber (RndRSE, KeyRef_Op) GET.request AC_CR <ul style="list-style-type: none"> • ReceiptData1 • ReceiptData2 • EquipmentStatus • Classification data: <ul style="list-style-type: none"> – VehicleClass – VehicleDimensions – VehicleAxles – VehicleLicencePlateNumber – VehicleWeightLimits – VehicleSpecificCharacteristics 	→	
		←	GET_STAMPED.response <ul style="list-style-type: none"> • Operator_Authenticator (Auth_Op) GET.response
<i>Optional Presentation</i>	GET_STAMPED.request	→ ←	GET_STAMPED.response
<i>Receipt</i>	SET.request SET_MMI.request	→ ←	SET.response Set_MMI.response
<i>Tracking</i>	ECHO.request	→ ←	ECHO.response
<i>Closing</i>	EVENT_REPORT.request (Release)	→	

Purpose of the Presentation Phase

In the Presentation Phase the roadside equipment reads data from the OBE. In the previous Initialisation Phase the RSE has established which contract to use during the transaction. The RSE will now address data pertaining to the selected contract, reading both static data that have been entered into the OBE upon issuing or personalisation, and dynamic data that have been written during the last transaction. Functionally, four groups of data can be discerned:

1. **Account information - static.** Data that allow the EFC Operator to claim money from a user account held with a financial institution or with a Contract Issuer.
2. **Information about the last passage - dynamic.** The RSE reads data that have been written at the last tolling station. At the exit of a closed tolling system these data constitute the entry ticket, which was written by the DSRC beacon on entry. On other stations the data are normally ignored.
3. **Vehicle classification information - static.** In tolling systems which rely on declared classification to determine tariff, vehicle classification information has to be read from the OBE. Also in systems relying on measured parameters, classification data read from the OBE is sometimes used for verification.
4. **Security related information – dynamic.** The CARDME Transaction enables several security mechanisms, without making them mandatory to by the RSE. The different mechanisms address different security requirements. If it is decided not to use some of the mechanisms, the related security data can simply be ignored by the RSE, or dummy data can be transferred.

CARDME Data in the Presentation Phase

Account and contract information

Account related information is contained in the following attributes:

- Payment means including PersonalAccountNumber: Points to a user account held at the Contract Issuer (which is already known from the Initialisation Phase). The EFC Operator will send his claim to this account. It also contains use restrictions and the end date of the validity of the payment means.

Information about the last passage

Information about the last passage is mainly required when exiting a closed tolling system. In this case the information sent by the OBE is the 'entry ticket' written when the vehicle entered the tolled system. For the details see the separate section on 'Entry Ticket and Receipt' (Chapter 3.2.3).

- ReceiptData1: The 'Ticket' written by the last beacon passed. For details see the special Chapter 3.2.3. This attribute also contains both the class that was declared at the last transaction and the class that was actually used (e.g. measured). When used as part of an entry ticket, this information enables the exit station to find out whether the class has changed during the trip. The attribute ReceiptData1 also contains the data element ReceiptAuthenticator, which contains data that have been calculated by the last beacon in order to 'sign' the ticket given. The RSE may use this authenticator to check that the (entry-)ticket has not been manipulated, especially that the entry point has not been changed. In addition the authenticator can be used as a kind of 'indirect authentication of the previous beacon'. The Receipt Authenticator is both produced and checked with a local algorithm and with local keys, i.e. with keys that are not distributed to any third party. The procedure is fully in the realm of an EFC operator's local system, and the authenticators are both calculated and checked by his own beacons only. The OBE merely transports this authenticator from one beacon to the next. Operators are free to use this security service, simply ignore it (i.e. by writing empty authenticators in the Receipt Phase and not checking the authenticators read in the Presentation Phase) or even use it for other purposes. In this use, the Receipt Authenticator serves as a free field where an EFC Operator may transport some local data from one beacon to the next.
- ReceiptData2: The 'Ticket' of the penultimate beacon (last but one). In some systems two receipts are required to find which of two alternative routes the vehicles has passed.

Vehicle classification information

CARDME foresees a list of declared classification data that tries to cover a maximum of needs while remaining as short as possible. Keeping the list of classification data short is not required for technical reasons – a few bytes more or less over the DSRC link make little difference – but for cost reasons upon personalisation of the OBE. In order to be as flexible as possible, CARDME has devised an adaptable concept to treat classification – see the separate chapter devoted to this concept (Chapter 3.2.2).

- VehicleClass: Vehicle Class is a very simple and well known data element which in CARDME is used in a clever new way: Vehicle Class covers three purposes: (1) it gives the local class in the 'home system' of the Contract Issuer; (2) for clear-cut cases it gives simple 'European harmonised classes', to avoid having the more complex extended declared characteristics present; (3) it states whether a trailer is present or not. For more details see the special section on classification, Chapter 3.2.2.
- VehicleDimensions, VehicleAxles, VehicleLicencePlateNumber, VehicleWeightLimits, VehicleSpecificCharacteristics: These extended declared vehicle characteristics are only present if required by the contract or when the vehicle does not fall into a 'European harmonised class'. All classification data are standards conformant, i.e. according to the definitions of EN ISO 14906. For further details see 3.2.2. The RSE may read only those classification data it requires.
- There is no longer a 'VehicleAuthenticator'. In a previous phase of the project, [CARDME-3], it was proposed that a Vehicle Authenticator is added to the classification data. The idea was that the organisation which enters the vehicle classification data shall sign them to prevent the data being altered. The Authenticator had to be calculated with 'interoperable keys', i.e. with keys known to all participants of the MoU, since all EFC operators would have the need to check them. Because of the wide distribution of this key, problems in diversifying the key, and the difficulty of having new keys from time to time, CARDME-4 has opted to delete this data element. Instead proper access control conditions must be implemented in the OBEs to prevent manipulation.

Security related information

CARDME enables several security mechanisms, which are designed to protect the individual security requirements of the different entities in the CARDME architecture. The security level is fully adaptable from the RSE's point of view – all security measures can either be used or be disregarded by the RSE.

- AccessCredentials: In CARDME all access to OBE data (both read and write) is protected with Access Credentials (AC_CR). The RSE has to send the right Access Credentials before the OBE accepts a command. The RSE calculates the Access Credentials dynamically using a challenge produced by the OBE (see Initialisation Phase). The required keys need to be known by all partners of the MoU. Because of the wide distribution of the keys, it is indispensable that these keys are diversified (different OBE have different keys) and that there are key generations (new keys are used from time to time). Details of the calculation and of diversification can be found in Chapter 4 of the Annex.
How to do without AccessCredentials: CARDME foresees one generation of Access Credentials ('Generation 0') which is openly known to all. OBEs or rather contracts with these Access Credentials can be read by everybody. It is left to the Contract Issuer's policy (and presumably to agreements in the MoU) whether he issues such OBEs or not.
- Operator Authenticator: The CARDME Transaction uses a GET_STAMPED command to retrieve the Contract Identifier. The purpose of this command is to ask the OBE to 'stamp' the data it sends back with an Authenticator. We call this special Authenticator the Operator_Authenticator since it can be interpreted by any Operator. The Authenticator can be checked to make sure that the OBE passing is a 'true one', i.e. part of the interoperability scheme (and not a forged one). It is dynamically calculated by the OBE with the interoperable keys, i.e. with keys known to all EFC operators (KeyRef_Op).
How to do without Operator Authenticator: There is no technical need to check this Authenticator. It is automatically produced by the OBE, but EFC Operators that do not wish to perform such a security check are free not to check the authenticator in their RSE (at least from a technical viewpoint – they might be obliged to do so contractually, say through contracts with associated issuers or through the interoperability MoU). One possible reason why an operator does not want check this authenticator is when he adds the CARDME Transaction onto his existing RSE which has no appropriate key storage and security handling facilities. At some point in time, e.g. when he routinely replaces some of his older equipment, he may then decide to go for higher security.
- ReceiptAuthenticator (contained in the ReceiptData-attributes): This RSE signature under the receipt has already been treated above under 'Information about the last passage'.
- EquipmentStatus: In CARDME this data element serves as a very simple but effective security measure, namely as a simple transaction counter. According to the EFC application standard EN ISO 14906 the coding of the data element 'EquipmentStatus' is left to the operator (it says 'operator-specific EFC-application information pertaining to the status of the equipment'). The data element provides for 16 bits. CARDME recommends that operators agree to reserve 4 bits for their private local use (e.g. for management of the transaction in their own system, containing information like 'next suitably equipped gantry should take an enforcement picture'), and to leave 12 bits for a **transaction counter** (0...4095). CARDME proposes that each communication between RSE and OBE should be counted and a record of this maintained in the OBE, thereby increasing the practicalities of proving some instance of fraud (e.g. on the part of an operator by duplicating transactions at RSE, especially when he makes use of the low-security mode of operation optionally allowed for in CARDME. The transaction counter also helps to identify instances when cryptographic security is broken). The use of this transaction counter provides a very important facility for monitoring system performance.
The RSE of every EFC operator signed up to the MoU reads the Equipment Status in the Presentation Phase, increments the counter, and writes the new value back to the OBE in the Receipt Phase.

Optional Presentation Phase

Phase	RSE		OBE
Initialisation	INITIALISATION.request (BST)	→ ←	INITIALISATION.response (VST)
Presentation	GET_STAMPED.request GET.request	→ ←	GET_STAMPED.response GET.response
Optional Presentation	GET_STAMPED.request AC_CR • Payment means including PersonalAccountNumber (RndRSE, KeyRef_Iss)	→	
		←	GET_STAMPED.response • Issuer Authenticator (Auth_Iss)
Receipt	SET.request SET_MMI.request	→ ←	SET.response Set_MMI.response
Tracking	ECHO.request	→ ←	ECHO.response
Closing	EVENT_REPORT.request (Release)	→	

Nowadays it is very often the case that the EFC Operator and the Contract Issuer is one and the same organisation. Very often the operator issues the OBE with the contract inside. In this case, the security information passed in the previous Presentation Phase is sufficient.

In case these two organisations are different, and especially when they are organisationally strongly separated, e.g. reside in different countries (which is normal in a roaming environment) or are totally different entities (a tolling operator and a bank perhaps) a new security requirement arises. In the Presentation Phase, the EFC Operator was able to check through the Operator_Authenticator that the OBE (or rather the Contract in the OBE) is a genuine one, i.e. from an organisation belonging to the MoU. He will then send a claim to the Contract Issuer requesting payment. The Contract Issuer now has no means to really check this claim. He also has no clear proof for his customer, the user that drove the vehicle, that the money is correctly requested for a passage somewhere.

Every RSE knows from the data element 'ContractProvider' in the ContextMark of the VST, whether it is communicating with a local or a foreign vehicle. Only for foreign vehicles the RSE executes this optional presentation phase. The sole purpose of this phase is to obtain a Authenticator from the OBE. This Authenticator is calculated by the OBE with keys only known to the Contract Issuer. The (foreign) EFC Operator, where the vehicle passes, can neither check nor forge this authenticator. The EFC Operator simply adds this authenticator to the transaction record he sends as a claim to the Contract Issuer in order to be reimbursed. The Contract Issuer checks the Issuer_Authenticator in order to have proof that a vehicle for which he is obliged to pay has actually passed a certain (foreign) EFC station. This both serves as proof against users trying to deny the passage and checks for a correct claim made by the foreign operator.

Note: The challenge sent by the roadside (RndRSE) may not be a number to be freely chosen by the roadside. It has to be prescribed and constructed in such a way that the roadside cannot influence its value. A concatenation of Date and Time of passage (i.e. session time) would serve this purpose perfectly. This challenge has to be passed to the Contract Issuer in the transaction record, together with the authenticator calculated by the OBE, in order to enable the Contract Issuer to check the authenticator.

3.1.4 Receipt Phase

<i>Phase</i>	<i>RSE</i>		<i>OBE</i>
<i>Initialisation</i>	INITIALISATION.request (BST)	→	INITIALISATION.response (VST)
<i>Presentation</i>	GET_STAMPED.request	→	GET_STAMPED.response
	GET.request	←	GET.response
<i>Optional Presentation</i>	GET_STAMPED.request	→	GET_STAMPED.response
<i>Receipt</i>	SET.request AC_CR • ReceiptData1 • ReceiptData2 • EquipmentStatus • ReceiptText	→	
	SET_MMI.request	←	SET.response Set_MMI.response
<i>Tracking</i>	ECHO.request	→	ECHO.response
<i>Closing</i>	EVENT_REPORT.request (Release)	→	

In the Receipt Phase, the RSE writes the details of the transaction to the OBE. This includes information such as the location of the EFC station, the date and time of passage, and the success of the transaction. In addition, the RSE sends an MMI command to the OBE, to indicate to the user the success of the EFC transaction (e.g. different beeps for 'OK' and 'not OK').

For most data there is no need to go into detail, since they have been treated already in the Presentation Phase. Data written to the OBE in the Receipt Phase are:

- ReceiptData1: The 'Ticket' given by the RSE. See Presentation Phase.
- ReceiptData2: The data read in ReceiptData1 in the presentation phase are now written as ReceiptData2 ('old ticket'). See Presentation Phase.
- EquipmentStatus: Includes a transaction counter. For details see Presentation Phase.

In addition, **the user is informed** about the success of the transaction. This is done in two ways:

1. **ReceiptText**: The RSE may use this data element to send a short text message to the passing OBE (maximum length 12 characters). The Standard does not prescribe what the RSE shall say. The text might contain some cost information ('EURO 2.00'), some station information ('ENTRY 24'), added value information ('A55 CLOSED'), or may even be left blank.
Nowadays few OBEs have a display, and very few OBEs will have the possibility to display this text information, so normally OBEs will simply disregard the information. CARDME believes nevertheless that in many emerging systems it will be increasingly important to have the option to send at least a short text message, consisting of a few text characters. Especially in systems with complex, time-dependent tariffs for demand management purposes it may be important for the user to be informed of the actual cost of the current passage to make variable charging meaningful.
2. **SET_MMI**: With this command the RSE instructs the OBE to use its man-machine interface (MMI), to signal the user one of three pre-defined messages, namely 'OK', 'not OK' and 'Contact Operator'. It is up to the OBE how to signal these messages. Depending on OBE make, the OBE may beep, light a signal lamp or even write something onto a display.

3.1.5 Tracking / Closing Phases

Phase	RSE		OBE
Initialisation	INITIALISATION.request (BST)	→ ←	INITIALISATION.response (VST)
Presentation	GET_STAMPED.request GET.request	→ ←	GET_STAMPED.response GET.response
Optional Presentation	GET_STAMPED.request	→ ←	GET_STAMPED.response
Receipt	SET.request SET_MMI.request	→ ←	SET.response Set_MMI.response
Tracking	ECHO.request	→	
	Etc...	←	ECHO.response
Closing	EVENT_REPORT.request (Release)	→	

In full multi-lane systems, a Tracking Phase is usually used to keep track of the vehicle after the EFC transaction is finished (using the Echo service, which may be used several times). In systems requiring no tracking, the session is closed with an explicit release in the Closing Phase.

Tracking and Closing are optional and used by RSE where required locally. All OBEs need to support these functionalities.

3.2 TRANSACTION DATA

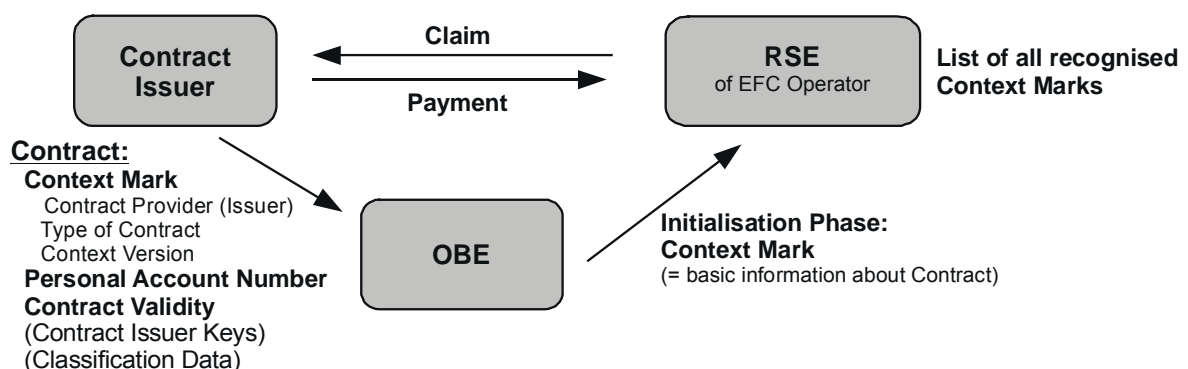
3.2.1 Contract and Context Mark

The Contract Issuer initialises the OBE with all data pertaining to the Contract:

- Contract Issuer Informs the EFC Operator, where the user account is kept, i.e. where to send the claim
- Type of Contract Basic information about the contract, for CARDME saying something like "CARDME interoperable contract for central account"
- Payment means including Identification of the user's account held with the Contract Issuer, the
Personal Account Number associated expiry date and possibly other validity restrictions

In addition the Contract Issuer will enter some further data:

- Context Version Housekeeping data for system maintenance, giving version numbers for transaction specification version, software version, security key versions, etc.
- Contract Issuer Keys In case the Contract Issuer makes use of the security service "Issuer Authenticator" he has to diversify his Master keys and store individual secret keys in the OBE.
- Classification Data In the CARDME architecture it is not explicitly required that the Contract Issuer enters the classification data, but it is normally the case. Classification data have strong contractual implications and should therefore be entered under control of the Contract Issuer.



The Context Mark gives essential information about the Contract

When the user's OBE passes an EFC station, the RSE must **from the first data transmitted** know whether it can recognise a contract. It cannot wait until all contract data are transmitted. Hence, for every contract available (there might be several), the OBE must transmit some basic information very early in the communication. The OBE does so in the Initialisation Phase by sending the Vehicle Service Table, VST, which for every available EFC contract contains the basic information required by the RSE to decide whether or not it can accept the contract. This basic information is contained in the EFC Context Mark, which is a data attribute defined in the standard ENV ISO 14906.

The EFC Context Mark summarises the Contract Information. The Context Mark is transmitted in the Initialisation Phase of the transaction. From its contents the EFC Operator learns whether he can accept the contract. For this purpose the RSE of the EFC Operator has to contain a list of all EFC Context Marks that are recognised by the MoU.

Context Mark	Contract Provider
	Type of Contract
	Contract Version

Data contained in the EFC Context Mark attribute

The RSE has to store a table that lists all Context Marks that it can recognise. The MoU partners have to install procedures to exchange and regularly update the list of accepted Contract Issuers, Types of Contract and Contract Versions.

The MoU secretariat has to keep a list of value assignments for the data elements of the Context Mark. Such a list might look as follows:

Name of data element	Content	List of Value Assignments and example																		
Contract Provider	Country code and national issuer identifier	<p>Value assignment is defined by standards (Data type CS1 in ENV ISO 14816). List of Contract Providers (Contract Issuers in CARDME terminology) is kept at www.nni.nl/cen278/.</p> <p><i>Example:</i></p> <table border="1"> <thead> <tr> <th>Country</th> <th>Issuer</th> <th>Country Code</th> <th>Issuer Identifier</th> </tr> </thead> <tbody> <tr> <td>Sweden</td> <td>Öresundskonsortiet</td> <td>1010 0100 00</td> <td>00 0000 0000 0001</td> </tr> <tr> <td>--- " ---</td> <td>EuroPark Sevenska AB</td> <td>---- " ----</td> <td>00 0000 0000 0011</td> </tr> <tr> <td>Switzerland</td> <td>Customs Authority</td> <td>0111 0001 01</td> <td>00 0000 0000 0001</td> </tr> </tbody> </table>	Country	Issuer	Country Code	Issuer Identifier	Sweden	Öresundskonsortiet	1010 0100 00	00 0000 0000 0001	--- " ---	EuroPark Sevenska AB	---- " ----	00 0000 0000 0011	Switzerland	Customs Authority	0111 0001 01	00 0000 0000 0001		
Country	Issuer	Country Code	Issuer Identifier																	
Sweden	Öresundskonsortiet	1010 0100 00	00 0000 0000 0001																	
--- " ---	EuroPark Sevenska AB	---- " ----	00 0000 0000 0011																	
Switzerland	Customs Authority	0111 0001 01	00 0000 0000 0001																	
Type of Contract	Code for type of contract.	<p>A code with a meaning that is agreed by all MoU partners (otherwise it has only local meaning).</p> <p><i>Example:</i></p> <table border="1"> <tbody> <tr> <td>0000 0000</td> <td>CARDME-4, Central Account; Personalised OBE</td> </tr> <tr> <td>0000 0001</td> <td>CARDME-4; Central Account; Pre-configured OBE</td> </tr> <tr> <td>0001 0000</td> <td>CESARE, Central Account</td> </tr> <tr> <td>1xxx xxxx</td> <td>Local Contract; Coding only known by Contract Issuer</td> </tr> </tbody> </table>	0000 0000	CARDME-4, Central Account; Personalised OBE	0000 0001	CARDME-4; Central Account; Pre-configured OBE	0001 0000	CESARE, Central Account	1xxx xxxx	Local Contract; Coding only known by Contract Issuer										
0000 0000	CARDME-4, Central Account; Personalised OBE																			
0000 0001	CARDME-4; Central Account; Pre-configured OBE																			
0001 0000	CESARE, Central Account																			
1xxx xxxx	Local Contract; Coding only known by Contract Issuer																			
Context Version	Version number	<p>A number that says according to which version of the transaction specification the OBE has been produced. Has to be seen together with Type of Contact:</p> <p><i>Example:</i></p> <p><i>For Type of Contract = 0000 0000 and 000 0001 (CARDME)</i></p> <table border="1"> <tbody> <tr> <td>Context Version 0000 0000</td> <td>CARDME version 2002; 1st Key Generation</td> </tr> <tr> <td>Context Version 0000 0001</td> <td>CARDME version 2002; 2nd Key Generation</td> </tr> <tr> <td>Context Version 0000 0010</td> <td>CARDME version 2002; 3rd Key Generation</td> </tr> <tr> <td>....</td> <td>....</td> </tr> <tr> <td>Context Version 0001 0000</td> <td>CARDME version 2010; 1st Key Generation</td> </tr> <tr> <td>Context Version 0001 0001</td> <td>CARDME version 2010; 2nd Key Generation</td> </tr> <tr> <td>Context Version 0001 0010</td> <td>CARDME version 2010; 3rd Key Generation</td> </tr> </tbody> </table> <p><i>for Type of Contract = 0001 0000 (CESARE)</i></p> <table border="1"> <tbody> <tr> <td>Context Version 0000 0000</td> <td>CESARE V1.0</td> </tr> <tr> <td>Context Version 0000 0001</td> <td>CESARE V2.0</td> </tr> </tbody> </table>	Context Version 0000 0000	CARDME version 2002; 1 st Key Generation	Context Version 0000 0001	CARDME version 2002; 2 nd Key Generation	Context Version 0000 0010	CARDME version 2002; 3 rd Key Generation	Context Version 0001 0000	CARDME version 2010; 1 st Key Generation	Context Version 0001 0001	CARDME version 2010; 2 nd Key Generation	Context Version 0001 0010	CARDME version 2010; 3 rd Key Generation	Context Version 0000 0000	CESARE V1.0	Context Version 0000 0001	CESARE V2.0
Context Version 0000 0000	CARDME version 2002; 1 st Key Generation																			
Context Version 0000 0001	CARDME version 2002; 2 nd Key Generation																			
Context Version 0000 0010	CARDME version 2002; 3 rd Key Generation																			
....																			
Context Version 0001 0000	CARDME version 2010; 1 st Key Generation																			
Context Version 0001 0001	CARDME version 2010; 2 nd Key Generation																			
Context Version 0001 0010	CARDME version 2010; 3 rd Key Generation																			
Context Version 0000 0000	CESARE V1.0																			
Context Version 0000 0001	CESARE V2.0																			

3.2.2 Classification in CARDME

In order to determine the correct tariff for a given passage the EFC Operator must be able to determine the classification of the vehicle, in traditional Stop-and-Pay Toll Plazas this classification is determined by the operator in the toll booth.

In an EFC system automatic classification methods must be employed. Two approaches have been adopted across Europe:

Measured Characteristics

Sensor arrays are installed to measure specific vehicle characteristics in order to determine the class. In mono-lane systems it is possible to measure a wide range of physical characteristics, e.g. length, width, height, number of axles, weight, etc. However, in a multi-lane environment due to sensor technology limitations the parameters are usually restricted to length, width and height. It is not possible to measure non-physical characteristics of vehicles e.g. Euro class, Max Laden Weight.

Declared Characteristics

Vehicle classification data is either stored in the OBE and declared during the transaction or is retrieved from a central database via a unique identifier. There are two possible approaches, either a vehicle class is declared or the Roadside Equipment determines the correct classification from a set of declared vehicle characteristics. In a single system environment it is feasible to just to declare a system specific vehicle class however in a multi-system environment unless there is a harmonised classification system an agreed set of vehicle parameters must be declared.

The CARDME Concept supports both approaches towards classification. However, it is a requirement that every OBE with an interoperable contract must contain declared classification data for the vehicle that it is installed in, so that the declared characteristics can be presented in systems that require them. In systems where measured characteristics are used, the declared characteristics are ignored in the calculation of the tariff. For such systems the requirement of having to store vehicle characteristics that are not used locally means a burden that has to be carried for the sake of interoperability. The cost associated with the need to have declared characteristics will most probably be passed on to the customers who want interoperable contracts rather than basic, local ones. CARDME offers a way to reduce cost in some cases by offering the opportunity to have pre-configured OBEs for certain vehicle types, see below.

Support for Pre-Configured and for Personalised OBE

When using declared vehicle classification parameters, we face a **dilemma**:

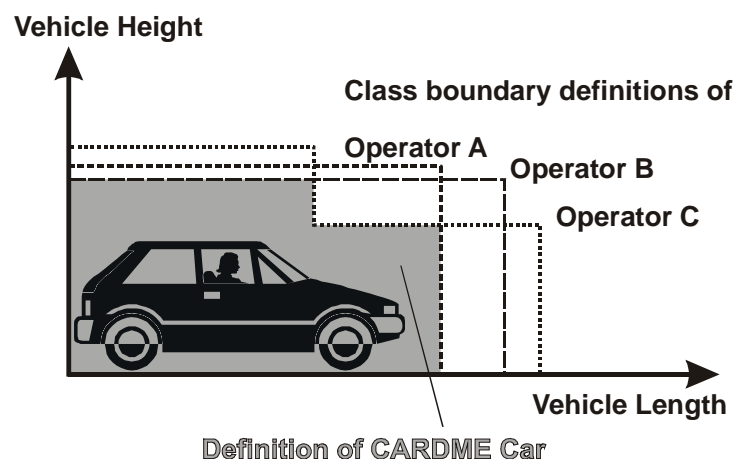
On the one hand it is a well known fact that it is illusory to try to harmonise vehicle class definitions throughout Europe. Hence, instead of storing in the OBE the simple but non-interoperable vehicle class, the concept of vehicle classification parameters was invented. In each OBE a set of vehicle parameters is stored upon OBE personalisation (e.g. number of axles, length, height). These classification parameters are read out at every EFC transaction, which allows every operator to deduce the local class from the detailed parameters. The concept of using detailed **vehicle classification parameters** instead of system specific classes is a workable solution for making declared classification interoperable, but it comes at a price. When a user wants to obtain a contract, his OBE has to be personalised with the specific data of his vehicle. In CARDME these data are the vehicle dimensions (length, height and width), number of axles and height above the first axle, the licence plate number, the weight limits, and some engine and emission related data.

Clearly entering these data bears rather **high financial and operational costs**:

- OBE distribution becomes laborious since it requires personnel. OBEs cannot be distributed in a pre-configured way.
- The personnel have to be trained and supervised (classification data are sensitive data since they determine tariff - cheating pays off)
- All customer service counters have to be equipped with personalisation equipment (at least a PC for entering the data, an interface to enter the data into the OBE, and possibly a photo-copier to take copies of the vehicle licence document in order to have proof of the data in case of later dispute).
- All OBE need a personalisation interface and appropriate access control mechanisms that allow only authorised service centres to enter or change the vehicle data.
- There has to be a security key distribution scheme and procedures where the keys required to access the OBE via the personalisation interface are distributed in a safe way.

- The user has to visit a customer service centre when he wants to obtain an OBE. It is not possible to buy OBEs or rather to establish a contract at un-authorised outlets. This makes OBE distribution via petrol stations, automobile clubs or mail-ordering practically impossible.
- OBEs cannot be moved between vehicles. Since the detailed vehicle classification parameters only fit a specific vehicle, moving OBE between vehicles cannot be allowed.

On the other hand it is also obvious that only comparatively few vehicles will need the detailed vehicle characteristics. A normal passenger car will be in the 'car' class in all tolling systems. For such a normal car there is no need to have more detailed vehicle classification data available in the OBE, a **single simple class indication** would be sufficient. Only 'borderline cases', i.e. vehicles that are a car in some systems, but a different category in other systems, will need the whole list of detailed vehicle classification parameters (examples for such vehicles could be large mini-vans, small passenger buses or vans, cars with small trailer, etc.). All other cars, i.e. probably **80% to 90% of all vehicles**, can use a **simple pre-configured OBE** with low distribution cost. This requires that European interoperable classes are defined. The CARDME project does not have the necessary resources to do so, but the operators joining an MoU could easily collect the required base information on class definitions in their respective countries and filter out some clear cut **common European interoperable classes**, thus defining the 'CARDME Car' and probably the 'CARDME two axles truck' and so on. The sketch below shows the basic idea.



For the large number of vehicles that are clear cut cases and fall into one of the 'MoU Vehicle Classes' pre-configured OBE can be produced. Class information can be entered already before distribution. This would bring the following advantages:

- Easier distribution. Since there is no need to enter complex vehicle specific data, the OBE can simply be bought 'off-the-shelf' at any convenient outlet, such as a petrol station. There is no need for the user to call at a customer service centre. OBEs for different classes can be made distinguishable with different external markings (e.g. different colour fabrication labels).
- Pre-configured OBEs are transferable. Pre-configured OBEs only carry a general class information and no vehicle specific details. Hence such OBEs fit any 'similar' vehicle. The user may move his OBE from one vehicle to another.
- Lower cost. Pre-configured OBEs can be personalised at manufacture. There is no need to have costly individual personalisation done by skilled personnel with specialised equipment in a trusted environment at customer service centres.

Clearly, it would be ideal to serve both needs. CARDME offers exactly this flexibility.

CARDME allows for a comprehensive list of vehicle classification parameters for those who need it. For others that do not need the extended characteristics because they are simple, standard cases, CARDME proposes to use the vehicle class information stored in the OBE in a specific way.

Pre-Configured OBE

Previous phases of the CARDME project have highlighted the fact that there is a requirement for OBEs to be transferable within the passenger car market. This can be achieved in a local system through the storage of a vehicle class in the OBE. However, to implement this on a European scale could imply the harmonisation of vehicle class across Europe.

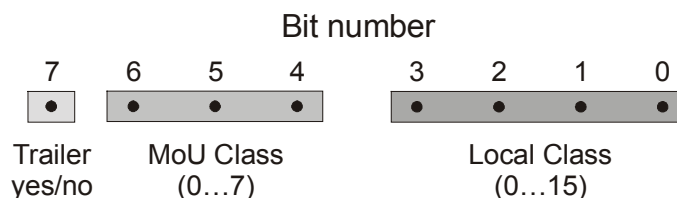
Within CARDME an analysis of existing toll classification systems across Europe showed that whilst there were significant differences in the number of classes used and the boundaries between classes, it would be feasible to define a class of vehicle which would be considered a car in all systems. The same is also true for HGVs, if a HGV is above a certain weight or number of axles then it will always pay the highest tariff.

CARDME is not in a position to define such interoperable vehicle classes. The definition of such MoU Vehicle Classes has to be left to the operators preparing the MoU. The table shows how such a definition might look.

EXAMPLE for a possible definition of MoU Vehicle Class	
European Class	Definition
0 'undefined'	Not a clear cut case. Does not fit into any fixed class. Extended vehicle characteristics are required (and present).
1 'Motorbike'	2 axles vehicle; length less than 2 metres; width less than 1 metre
2 'Car'	2 axles; length less than x metres, height less than y metres; height over 1 st axle less than z metres; has rear windows; maximum laden weight less than 3.5 tonnes
3 'bus'
4 '2 axles truck'	2 axles vehicle; maximum laden weight between 3.5 tonnes and 12 tonnes; length between xx and yy metres,
5 '3 axles truck'
6 '4 axles truck'
7 'maximum permitted vehicle'

Vehicles that fall into one of the MoU Vehicle Classes do not need the extended characteristics. Those vehicles can make use of pre-configured OBE. The attributes for the extended vehicle characteristics are left empty (carrying dummy values). In case an RSE recognises from the Type Of Contract in the VST that the passing vehicle has a contract associated with a pre-configured OBE, it may even decide not to read those data fields in the Presentation Phase of the transaction. Another valid practical implementation is to always read all data, even the dummy entries.

For pre-configured OBE, CARDME proposes to handle the 'MoU Vehicle Class' by using the vehicle class information stored in the OBE in a specific way. According to the standard EN ISO 14906, class information shall be carried in the attribute 'VehicleClass' (data type Integer of one octet length) which is defined in the standard as an operator specific vehicle class allowing up to local 256 classes to be discerned. CARDME proposes that the 8 bits of this data element shall be interpreted in the following way:



CARDME use of the 8 bits contained in the attribute VehicleClass

The 4 least significant bits are reserved for local operator use allowing 16 local classes to be defined which can be combined with the Most Significant Bit to indicate the presence of a trailer. It is up to the Contract Issuer what use he makes of this field. The idea behind reserving this field is to allow local procedures to remain the same, untouched by the introduction of a new interoperable service. The remaining 3 bits are available to define up to 8 interoperable classes, the 'MoU Vehicle Classes' which if agreed would allow OBEs to be transferable within these classes.

Personalised OBE

Especially heavy commercial vehicles cannot do without an extensive list of vehicle classification parameters. Many countries are introducing heavy vehicle fees that use rather complex classification in order to have a better match between the external cost incurred by a vehicle and the fee levied for its use.

OBE for heavy vehicles used in such systems have to be personalised, as previously described. Because the vehicle data are fully vehicle-specific and do not match any other vehicle, **such OBEs are non-transferable**. Such OBEs are said to be 'logically bound to a vehicle' by their data content (e.g the licence plate number). Ideally the OBE should also physically be bound to the vehicle in order to avoid accidental exchanges or intentional cheating.

Entering these lengthy list of vehicle data is costly. It is expected, however, that heavy vehicle manufacturers would support their customers with individually configured OBEs built-in at delivery of a new vehicle in case a Europe-wide harmonised EFC transaction should be widely used.

The table below details the vehicle characteristics supported by the CARDME transaction:

Attribute [EN ISO 14906]	Data Element	Description
Vehicle Class	VehicleClass	The vehicle class field as defined by CARDME
Vehicle Dimensions	VehicleLengthOverall	Nominal maximum overall length, in dm.
	VehicleHeightOverall	Nominal overall unladen height, in dm.
	VehicleWidthOverall	Nominal overall width, in dm
Vehicle Axles	VehicleFirstAxleHeight	Bonnet height, measured over the front axle, in dm.
	VehicleAxlesNumber	Number of axles (including drop axles) plus presence of dual tyres
Vehicle Licence Plate Number	VehicleLicencePlateNumber	Declared licence plate of the vehicle
Vehicle Weight Limits	VehicleMaxLadenWeight	Maximum permissible total weight including payload in 100kg units.
	VehicleTrainMaximumWeight	Maximum permissible weight of the complete vehicle train.
	VehicleWeightUnladen	Nominal unladen weight.
Vehicle Specific Characteristics	VehicleSpecificCharacteristics	EnvironmentalCharacteristics: EuroClass (Euro Emission Class) CopValue (COP-Emission Code) EngineCharacteristics (leaded/unleaded Petrol, Diesel, LPG, ..) DescriptiveCharacteristics (Vehicle shape).

Vehicle Characteristics supported by CARDME

Handling of trailers

In practically all EFC systems, tariff class changes when a trailer is attached to a vehicle. This does not pose any problems in systems employing measured characteristics.

With the appearance of free-flow systems, with fully electronic systems, and with EFC systems that also charge according to environmental characteristics comes the need to have declared characteristics. In such systems **there is no other way than to have trailers declared by the OBE**, i.e. in fact by the driver.

Interoperable system concepts such as CARDME have to support both measured and declared classification. Hence all OBE for vehicles that may or may not have trailers **need a possibility for the driver to declare trailer presence** (e.g. with a trailer switch). Naturally, such a feature is not required for vehicles that either cannot pull a trailer or that do not intend to ever pull a trailer.

3.2.3 Entry Ticket and Receipt

Regardless of station type (entry, exit or passage) the same CARDME Transaction is performed everywhere. At every station the same data are read and written.

Some of the data that are read out are of a static nature, i.e. they are entered and changed at special locations and occasions, but never altered through a transaction. Examples of such data are the Personal Account Number and the classification parameters.

One data element is write only: The data element Receipt Text is sent by the RSE after each transaction. It is text to be displayed by the OBE if it is capable of doing so.

Other OBE data are dynamic. These data are read out and re-written at each transaction. The OBE carries them in its read-write memory from one tolling station to the next one. The dynamic data in the CARDME transaction are the following:

Dynamic data in CARDME (read/write at every station)		
Attribute Name	Data Elements Contained	Meaning / Purpose
ReceiptData1	Session Time	Data and time of the transaction
	Session Service Provider	EFC Operator that has provided the service
	Station Location	Toll plaza number
	Session Location	Lane number
	Type Of Session	Station type (entry, exit, passage, etc.)
	Session Result	'OK', 'not OK', 'Vehicle Class incorrect', ...
	Session Tariff Class	Class applied in the session
	Session Claimed Class	Class declared in the session
	Session Fee	Amount paid for the service (includes currency)
	Session Contract Provider	-- The three elements give the Context Mark used
	Session Type Of Contract	--
	Session Context Version	--
	Receipt Authenticator	Signature of the tolling station giving the receipt
ReceiptData2	(same as above)	Previous receipt
Equipment Status	Equipment Status	Transaction counter and some free bits

ReceiptData1 contains all operationally relevant information regarding the passage of the vehicle. Hence, this information block can both serve as the 'Entry Ticket' in a closed system and as the 'Receipt' on exit in a closed system, respectively on passage in an open system.

Session Class contains both information about the class declared at the transaction and about the class actually applied (which might be different, e.g. because it was measured). The receipt also contains information on which one (of possibly several) contracts in the OBE was used. For that purpose, the Context Mark selected by the RSE is part of the receipt (comprising the elements Session Contract Provider, Session Type Of Contract and Session Context Version)

Receipt Authenticator is a very simple local security means. Every beacon may give a kind of signature which may be checked at the next beacon. This signature can be used to protect the entry ticket against forgery. This security element is designed for local usage and there is no need for a harmonised approach of all EFC operators. The Authenticator is meant to be carried only from entry to exit. After leaving a system it loses its relevance. EFC Operators are free to use this security feature or not. Operators may even use the data element for other local purposes.

ReceiptData2 repeats has the same structure as ReceiptData1, but contains the next older receipt. Having two receipts facilitates reconstructing a trip in case of disputes. In addition, some closed systems may need to read two receipts (entry ticket and checkpoint) on exit in order to distinguish between possible alternative paths through the network.

In order to have a simple OBE design, not the OBE but the RSE keeps track of what is old and what is new: The RSE always reads and writes both receipts. It writes the new receipt to ReceiptData1 and copies the read old ReceiptData1 to ReceiptData2.

Equipment Status serves a similar purpose. CARDME reserves part of this data element for a mandatory transaction counter (12 bits, corresponding to counter readings from 0 to 4095). Every beacon reads this counter, increases its value by one, and writes it back to the OBE. This counter is **a very simple but excellent quality control and security monitoring instrument**. Since in the CARDME Architecture all transactions are finally collected at the Contract Issuer, he should for every user have a consecutively numbered sequence of transactions – without missing numbers and without double numbers.

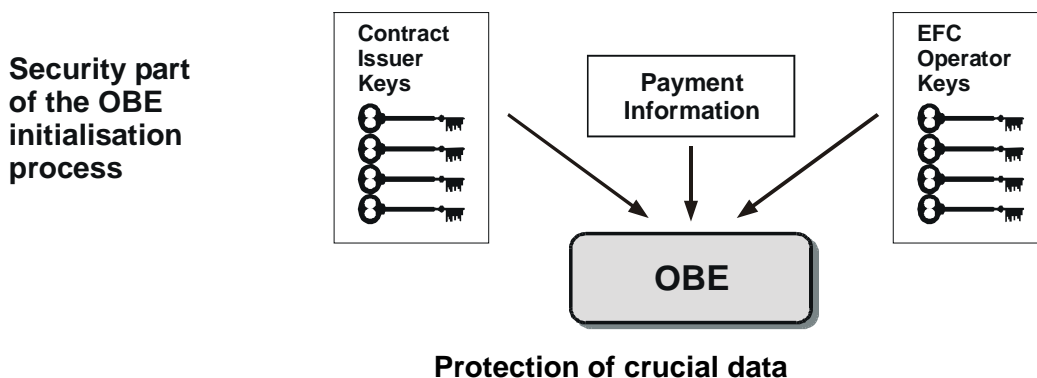
For tolling purposes, normally only the last receipt is required. Although always the same receipt data are read and written, their function differs for the different tolling systems:

Station type	Meaning of READ data	Meaning of WRITE data
CLOSED ENTRY	Ignore	write Entry Ticket
CLOSED EXIT	read Entry Ticket	write Transaction Receipt
OPEN PASSAGE	ignore	write Transaction Receipt

3.2.4 Security and Authenticators

Whenever an OBE performs the CARDME EFC transaction it will calculate some security data (authenticators) used for authentication of the equipment and the information it is carrying and transmitting to the Roadside Equipment (RSE). The authenticators are calculated using an international banking standard for authentication of a message. Crucial input for the calculation is the payment information (Contract Issuer and Personal Account Number) and the security keys stored in the OBE at the time of OBE personalisation.

Two sets of security keys, and amongst others, the payment information are stored in the OBE during the personalisation of the OBE. It is a strong requirement that both the keys as well as the payment information are well protected in the OBE. The Contract Issuer keys are only known and used by the Contract Issuer. The EFC Operator keys are distributed (one by one) to all the EFC operators having signed the MoU and having implemented the authentication service.

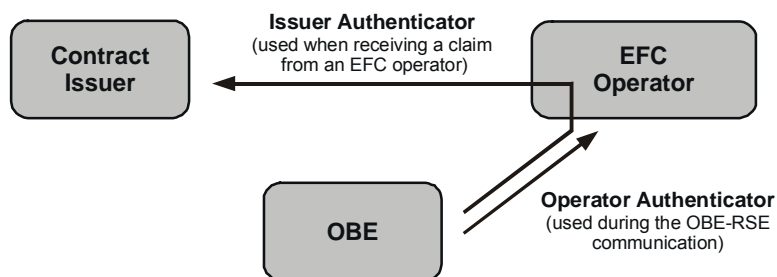


Two authenticators are calculated by the OBE:

- Operator Authenticator (Auth_Operator) using the EFC Operator keys
- Issuer Authenticator (Auth_Issuer) using the Contract Issuer keys

The EFC Operators use the Auth_Operator at the time of OBE-RSE communication verifying whether the OBE is genuine and whether the payment information it has transmitted during the transaction is as stored by the Contract Issuer.

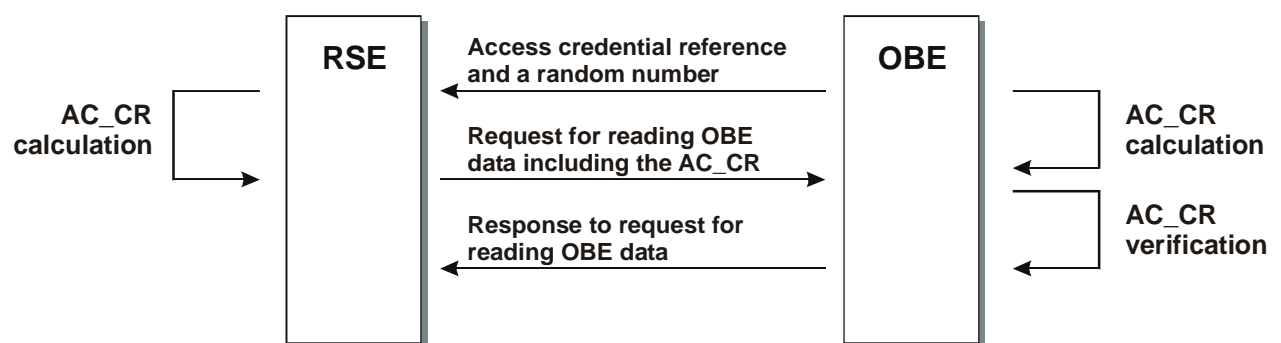
The Auth_Issuer is used by the Contract Issuer at a later stage verifying whether the OBE is an OBE personalised by Contract issuer and whether the claim from an EFC Operator is a genuine one. The Auth_Issuer is sent to the Contract Issuer as part of the claim from the EFC operator to the Contract Issuer. The EFC operator can read the Auth_Issuer but he can not use it for verification as only the Contract Issuer has the secret key used for the calculation of the Auth_Issuer.



The payment information authenticators

One of the measures to protect the payment information is the use of access control to OBE data. This implies that the OBE does not allow any RSE to read or write information in the OBE without having authenticated itself by so-called access credentials ('access control password'). The CARDME transaction enables the use of such mechanisms but as default the mechanisms is not used. That means that as default any RSE is able to read the payment information as well as other data stored in the OBE, e.g. vehicle characteristics stored by the Contract Issuer or the last receipts stored by the last EFC operator(s). It is the Contract Issuer who initialises the OBE and who controls the use of access control. However, the use of access control also means that the Contract Issuer has to distribute a secret key to all operators that are allowed to read the payment information and all the EFC operators have to implement the use of it. If not they will not be able to read the payment information and there will be no interoperability as for EFC.

The principle of access control to the payment information is shown below. When an OBE, having entered the communication zone, responds to a polling message from the RSE, it returns an Access Credential Reference and a random number (RndOBE). The Access Credential Reference includes the data AC_CR-MasterKeyReference and AC_CR-Diversifier. The data are the diversifier and a reference to a secret key (MasterKey for Access Credentials) that shall be used for the computation of the secret key AC_CRKey. This key is used for the computation of the Access credential (AC_CR) using the RndOBE number as input. The RSE returns the access credentials calculated and the OBE compares the access credentials with its own calculation. In case they are equal the OBE accepts the RSE as a genuine RSE and reading data from the OBE is allowed.



The principle of access control to the OBE data

The CARDME solution in its first version is that Access Credential Reference refers to a certain value that is used by the RSE as access credentials and acknowledged by the OBE as a valid 'access control password'. Hence, in practice reading of OBE data will always be allowed.

The CARDME security also includes measures to protect the information written to the OBE during a transaction, i.e. the receipt. This enables for instance an EFC Operator verifying that an entry ticket in a closed EFC system has not been changed during the entry and exit point.

It is assumed that agreements about the periodicity and maximum delay in submitting claims form part of the MoU.

The complete CARDME security specification is given in Chapter 4 of the Annex.

3.3 TRANSACTION IMPLEMENTATION

3.3.1 Implementing CARDME

Suitability of CARDME Transaction

The CARDME transaction has been developed so that it is suitable for:

- Open and Closed systems
- Free Flow or Barrier systems
- Mono or Multi-Lane
- Claimed or Measured classification

It is intended that the CARDME application is installed alongside existing systems and can be customised to match the specific requirements of any existing local system. By doing this it is possible for the EFC operator to receive the information necessary to charge users equipped with CARDME OBEs.

For EFC operators with standards compliant DSRC equipment there is no need to modify the hardware in the roadside equipment at each tolling point, all that is needed is a “software” upgrade in each beacon. The beacon is able to determine which application should be used for a given session following the BST-VST interaction and should be able to support sessions of the local and CARDME applications at the same time with no adverse effect on system performance or reliability.

The CARDME application is also suitable for new EFC operators or for operators considering an upgrade to an existing system. It is possible to set-up both a local application and the interoperable service using the one CARDME application enabling the setting up of local contracts which have the possibility of offering local subscribers preferential rates.

Operators using Measured Characteristics

The CARDME transaction includes the provision for the use of claimed characteristics by operators in order to determine the appropriate class, for EFC operators which already have roadside equipment capable of determining the vehicle class of a vehicle independent of information in the EFC transaction there are two possible options:

1. The characteristics claimed during the transaction by the passing vehicle can be ignored and the class determined using information retrieved from the measurement system.
2. The characteristics claimed during the transaction can be used to verify the measured class or vice versa

Operators using Claimed Characteristics

Currently in Europe there are a number of systems in which the tariff applied is dependent on the class claimed by the passing vehicle. This method is suitable for single systems but due to the difference in class boundaries unless there is a harmonised class structure across Europe it is necessary for vehicles to carry a list of vehicle parameters from which the roadside system can determine the appropriate class.

For operators which are currently using a simple claimed class structure, it will be necessary to determine the boundaries between classes based on the list of claimed characteristics available within the CARDME OBEs. In addition software routines will need to be added to the RSE which are able to interpret these list of characteristics claimed by the vehicles and determine the appropriate class to be applied.

In some current systems where claimed class is used very little information is exchanged over the air link regarding the class of the vehicle, instead a unique ID is passed by the vehicle which allows the class/characteristics of the vehicle to be retrieved from a central database. In these systems software routines will also need to be added to the RSE to interpret the claimed characteristics and determine the appropriate tariff.

Tariffing and discount policies

The CARDME Concept has been developed on the basis that users travelling in the domains of foreign EFC operators are not eligible for any discount schemes available to local users of a particular system. However, it is still possible for EFC operator to offer to local CARDME subscribers preferential contract conditions for EFC use within the local system.

Security Level Implementation

The CARDME Concept offers an optimum in security choices for the individual operator whilst maintaining the overall integrity of the CARDME Service.

It is recognized at present that most existing EFC operators within Europe do not employ cryptographic security. It was therefore considered necessary to offer an implementation path which does not require security measures that imply RSE upgrades from the start.

However, it is also recognised that due to the wider scope of the CARDME Service, potentially entire Europe, the potential benefits from fraud and consequently the risks involved are greatly increased. For that reason the CARDME service has been designed to enable a high level of security if required.

For operators which have existing RSE not capable of performing dynamic security measures across the air-link, the CARDME Service can be implemented without any changes to the existing equipment but if required at a later date, a migration to higher security levels is possible.

A step wise implementation scenario could be as follows:

- **Phase 0.** Operators have their own different EFC-applications that are mostly non-interoperable, or interoperable only on a regional/national scale.
- **Phase 1.** A number of operators sign up to a CARDME MoU. Each operator has to implement the CARDME application in all RSE. This does not affect existing local/national applications and does generally not require any hardware modification. It is up to the individual operator to issue new CARDME-compliant OBE to new customers and/or to customers who wish to be able to use their OBE also abroad. The OBE is loaded with different generations of Operator and Issuer keys from the start. Operator A does not wish to check the Operator Authenticator for foreign transactions. Due to the limited scope of the MoU at this stage, Operator A accepts the - expectedly marginal - risk that a claim sent to Operator B will be rejected because the Issuer Authenticator of a transaction proves to be incorrect (e.g. as a result of fraud using a fake OBE). For claims sent to Operator A, he can decide for himself whether he wishes to check the Issuer Authenticator. If so he has to implement a claim verification application in the back-office, including a sufficiently secure storage of the Issuer Key. This is the exclusive responsibility of Operator A. Operator A further checks the transaction counter sequence for each OBU.
- **Phase 2.** The number of operators that signed the MoU has increased, and the perceived fraud risks accordingly. Some operators - Operator A is one of them - have lots of 'foreign' transactions and decide it is time to check the Operator Authenticator to protect themselves against false 'foreign' transactions. In order to support this functionality all RSEs have to be extended with functionality for secure key storage and cryptographic calculations. This may require additional hardware. It is the primary responsibility of the TTP to maintain the integrity of the EFC-Operator keys. The TTP may therefore verify that certain facilities and procedures are in place before the key is exchanged.
- **Phase 3.** MoU Parties agree that it is necessary to enhance provisions against unauthorised access to OBE data, e.g. by parties who wish to use these data for their own business without permission from the Contract Issuer. Up till this stage access to the Contract Data was possible with a static 'password' as access credentials. The writing of receipt is from now on also access protected, by the access credentials, as a measure against sabotage. From now on the dynamic access control function will be implemented by all EFC-Operators. This implies that an access credentials master key, associated with the Contract Issuer, is to be distributed by the TTP to all EFC-Operators. Comparable provisions as for checking the Operator Authenticator are required in the RSE. For parties that have these facilities already in place - like Operator A - no further hardware modifications are necessary. It should be noted that, whilst the existing OBE's can still be used without any restriction, the enhanced provisions against unauthorised access only apply to newly issued OBEs with AC_CR-MasterKeyReference > 0. (Instead of the "dummy" AC_CR-MasterKeyReference = 0 used in the earlier issued OBEs).

The migration example is summarised in the table below.

Phase	Description	Impact on OBE	Impact on RSE	Security features implemented by Operator A	Remarks
0	Local EFC applications only	-	-	?	Situation before CARDME
1	CARDME MoU in place	New OBEs issued support CARDME transaction. All OBEs issued with AC_CR-MasterKeyRef. = 0	Additional SW loaded to support CARDME transaction.	- Transaction counter - Iss Auth check (optional) - AC_CR password	No need to replace OBE for local use.
2	Operator Authenticator checked at RSE.	None.	Crypto-facilities required.	- Transaction counter - Iss Auth check - AC_CR password - Op Auth check	Operators can migrate on individual basis.
3	Cryptographic Access Credentials implemented.	New OBEs issued with AC_CR-MasterKeyRef. > 0	Crypto-facilities required for all operators.	- Transaction counter - Iss Auth check - Crypto AC_CR - Op Auth check	All operators have to join. Crypto access protection only for new OBE.

Demand for CARDME Service from Local Subscribers

Once an EFC Operator has signed up to the CARDME Service and is offering the service to foreign users it is likely that there will be a demand from existing local subscribers to benefit from this payment service for tolls across Europe.

In order to benefit from this additional service it will be necessary for subscribers to sign a CARDME Contract for which additional information is likely to be required e.g. Specific vehicle details. The information relating to the vehicle and contract will need to be personalised in a 'Standard' CARDME OBE and issued to the user. Having signed the contract it will be necessary for the local EFC Operator to inform the user about the service including how to recognise when the CARDME Service is a valid payment method.

For users with vehicles that fit into the CARDME Car Class the only vehicle related information that is necessary is the Vehicle Licence Plate Number which is entered along with the contract information into a pre-personalised 'CARDME car' OBE.

For all other vehicles the OBE will need to contain a defined set of vehicle specific measurements as well as the user's contract details. The vehicle details can either be obtained as part of the contract or the vehicle measurements can be entered into the OBE by an approved outlet.

For most existing users it is likely that the demand for the interoperable service will be low, however, for vehicles which frequently travel in other EFC systems (e.g. HGVs) offered the demand is likely to be high. It could be expected that the demand from local users for the additional roaming service is likely to increase before vacation periods.

By providing new subscribers to the local system with CARDME based OBEs it will be possible to migrate the local system to a CARDME based system, with its inherent advantages, so that in the future there will be no need to support the separate local system in addition to the CARDME service.

3.3.2 Protecting Privacy

Privacy and Electronic Toll Collection

International and European regulations¹ impose restrictions on the gathering, storage, processing and dissemination of data relating to individuals and their behaviour. Additional - in detail differing - national regulations exist in most of the EU member states. In general the following guidelines apply:

1. data relating to individuals shall only be gathered and stored for a specific purpose and only as far and as long as needed for the execution of that purpose
2. data relating to individuals shall only be gathered in case no 'reasonable' alternative exists that achieves this purpose without the need to gather (the extent of) data relating to individuals
3. *proportionality*: in case data relating to individuals are gathered for the execution of a public task, the importance of this task needs to justify the infringement on privacy it incorporates
4. organisations responsible for the gathering of data relating to individuals shall inform the individuals concerned about the fact that such data are collected, and the nature of these data
5. such organisations have the obligation to enable individuals to inspect all information kept on them (some conditions apply).

The requirements for rules 2 and 3, are less stringent if the individual gives his explicit consent to the collection of these data and in case this consent is the result of a 'free choice'. It should be noted that driving a car and the associated use of public road infrastructure is generally perceived to be a basic need, rather than a luxury service one can choose to use.

In order to assess the impact of privacy regulations on EFC systems and schemes, one could differentiate between three cases:

1. EFC is introduced on new or existing tolled infrastructure, as a more convenient alternative to manual payment at a toll booth. The user is free to choose.
2. EFC is introduced on existing infrastructure to implement demand management policies. No manual payment is possible.
3. EFC is used for new complementary infrastructure, e.g. paylanes. No manual payment is possible. An almost similar alternative for the tolled infrastructure is available (although the quality of service will be different, e.g. free lanes vs. paylanes).

Case 1 is the most common today. Non-anonymous Central Account based schemes prove to be perfectly acceptable for this case, provided that appropriate procedures for the handling and protection of personal data are in place. These include measures to make sure personal data are no longer kept than necessary, restricted access to these data and a possibility to provide customers with non-itemised bills.

Case 3 is not yet seen much in Europe, but several examples in the U.S. exist. As to privacy, it seems to resemble case 1: the user has a reasonable alternative that provides full anonymity and can make a free and explicit choice.

Very few cases of type 2 are realised, although demand management using EFC has been considered in different EU countries for over 10 years now. Privacy requirements for case 2 are certainly more severe than for cases 1 and 3 as there is no free choice to make use of the EFC-system. Data protection authorities may - and will - argue that an anonymous payment method should be offered as such is technically and 'reasonably' possible. Whether the price to pay for EFC with full anonymity - e.g. in terms of costs, user convenience, security - is acceptable, will depend on details of the context and mostly be determined by a political judgement. Anonymous EFC can be realised through On-Board Accounts, e.g. using pre-paid IC-cards. Less straightforward, but certainly viable is to provide anonymity with tag-based Central Account systems, see discussion below.

¹ This basically concerns the International Covenant on Civil and Political Rights (esp art 8), the Convention for the Protection of Human Rights and Fundamental Freedoms (esp art 17) and the European Directive 95/46/EC on data protection. The directive can be regarded as a more specific elaboration of the 1981 Strasbourg Treaty on data protection.

Privacy and Central Accounts

Electronic toll collection using Central Accounts generally involves the collection of data relating to individuals, as the identification number of the tag which is exchanged in each transaction can be linked to the name of the customer. In case of post-payment the connection is obvious: the contract issuer needs to invoice the customer in accordance with the actual consumption of the service.

A system using pre-paid Central Accounts is well conceivable in which accounts are not directly linked to an individual. As long as the centrally-held balance associated with the tag number is sufficient, payment is guaranteed for operator and issuer. When insufficient balance occurs, the tag number can simply be blacklisted. Full anonymity can only be provided however, if also the loading/reloading of accounts can be done in an anonymous way. This could be achieved by e.g. cash deposits at a bank or post office, by a system based on a 'recycling' system of non-user-rechargeable tags, or by using pre-paid cards to recharge the account by telephone - analogue to pre-paid arrangements for mobile phones. Such fully anonymous payment facilities do generally not offer the optimum in user convenience, costs of exploitation and fraud prevention. If full anonymity necessary, it may be sufficient to offer an anonymous payment facility as one of the options. In practice, the majority of users will value convenience much higher than privacy protection.

Also in fully anonymous systems users may wish to have a specification of their usage. This can e.g. be realised in the form of a call-centre or a web-interface where users can get access to their passage details using their anonymous account identifier in combination with a PIN-code or alike.

Privacy and CARDME

As CARDME is Central-Account based, the previous subsection fully applies to the CARDME model. In addition a few specific remarks can be made.

The messages exchanged between an ordinary passenger car OBE and the RSE do not contain any information that can directly be linked to a person, not even to a vehicle licence number or bank account. Of course a unique contract identifier is sent, yet only the contract issuer can relate this identifier to an individual. As a consequence also the foreign EFC-operator cannot relate passages to the contract holder / user.

For heavy goods vehicles a mandatory set of vehicle parameters is exchanged that includes the licence plate number. It should be noted however that for commercial vehicles, vehicle registers do not link licence plate numbers to individuals but only to companies. In addition, access to national vehicle registers is generally restricted and subject to specific conditions.

An interesting option to increase the level of privacy protection in the CARDME model is to implement a formal and procedural division between contract issuer and (home) EFC operator. The contract issuer is now the only party with access to the customer database. The EFC operator is the only party with access to passage details. The EFC operator only forwards accumulated amounts to the contract issuer for invoicing. No single party is hence able to link detailed passage data to individuals. In special cases, e.g. a dispute on the amount on the bill, it will be necessary to establish the exchange of detailed data to issuer. A procedural framework can be established that safeguards that this can only be done with explicit permission of the contract holder. The contract holder can be provided with a means to inspect his passage details in an anonymous way (see previous subsection).

Conclusions

- If an EFC implementation gathers data relating to individuals, several legal requirements on the handling of these data have to be fulfilled.
- Measures needed in an EFC implementation to fulfil legal requirements on data protection depend on situation details: e.g. is a reasonable non-paid alternative or a manual payment possibility provided? If not, an anonymous electronic payment facility may have to be realised.
- In practice, the Central Account based CARDME model in post-payment mode will be an acceptable basis for the majority of cases.
- A possibility to increase privacy protection in the CARDME model is to implement a formal and procedural division between contract issuer and (home) EFC operator.
- The CARDME model can be used for anonymous EFC using anonymous pre-paid accounts with anonymous recharging facilities.

3.3.3 Clearing and Exchanging Claims

When a vehicle equipped with an OBE uses a toll motorway, the EFC Operator keeps a record of some data from the transaction. These data will be used for the claim, i.e. for the request for toll payment from the Contract Issuer. Details of the claim exchange procedure are to be laid down in the MoU.

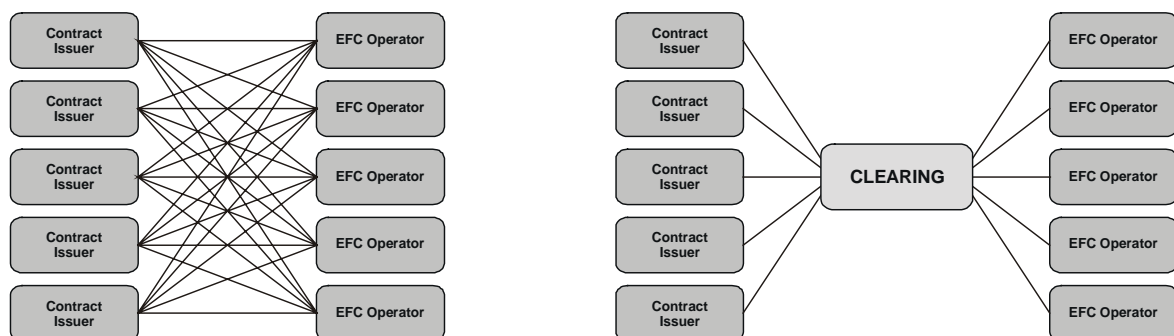
The EFC Operator collects information during the transaction process and stores it in his database. These data shall be kept in the database only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued.

After some period of time the EFC Operator regularly extracts the essential passage information into claims which he sends to the individual Contract Issuers. In case the MoU encompasses many Contract Issuers, a central clearing functionality may be offered in order to simplify the process. Note that the basic clearing functionality in the CARDME Architecture need to encompass only data re-routing plus some house-keeping tasks, without any further services (like, e.g., payment guarantee, immediate reimbursement etc.).

A straightforward approach towards clearing can be realised with a simple central data store with secure web access. EFC Operators put their claims via Internet into the clearing server. Likewise every Contract Issuer regularly retrieves his respective claims and reimburses all EFC Operators directly. In more sophisticated schemes, there is a central pool and distribution not only for the claims (data sets from EFC Operators), but also for the reimbursement (money to the EFC Operators). The central clearing may also offer additional data processing services, like

- checking of claims for consistency, integrity and authenticity on behalf of the Contract Issuers,
- stripping the claims from privacy-sensitive information but keeping the full transaction records on store (acting as an organisational and institutional 'fire wall' in order to protect the user's privacy),
- system quality monitoring (e.g. by checking for continuity of Transaction Counters, by checking Authenticators for breaks of security, checking for trip logic, etc.)
- keeping system statistics of the whole interoperable system (MoU data warehouse)

The clearing functions may be extended by the MoU up to any convenient level up to full Clearing House functionality and ultimately also include financial services associated with payment guarantee and risk-sharing.



A clearing intermediate can reduce complexity

Note that in the basic CARDME architecture, clearing encompasses only EFC Operators and Contract Issuers, and not the Financial Institutions, which are considered external (at least as long as they do not also take the role of Contract Issuer). Theoretically the clearing could be extended to also include Financial Institutions. This might be very useful in case of Commercial Credit Card companies (also called Petrol Card companies), which are international and traffic oriented and will probably sign the MoU. It has to be noted, though, that in this case the Card Company already partially slips into the role of Contract Issuer. The relationship to the user becomes more than mere pay and invoice. For example, for a Commercial Credit Card that is part of the MoU, the account in the OBE points directly to a Credit Card account, without an account with the Contract Issuer serving as an intermediate.

In contrast, for a user account held with a local bank, clearing will always solely remain on the level of the Contract Issuers - it is exactly the great advantage of the CARDME Architecture that the scope of the local payment means is extended over all Europe, without the need for all Financial Institutions to join the MoU.

The **contents of the claim** must ensure that the EFC operator providing the transport service is paid for the service he has provided and it shall enable the Contract Issuer to check the validity of the claim. The table below shows the (minimum) contents of a claim.

Data element	Definition	CARDME usage	Length in octets
SessionService Provider	As in EN ISO 14906	The identity of the EFC operator that has provided the transport service and that is sending the claim	3
ClaimID	A unique identity of the claim	A serial number defined by the EFC operator to have a unique reference for the claim sent to that specific Contract Issuer	4
Contract Issuer	As ContractProvider in EN ISO 14906	Usage according to EN ISO 14906. Identifying the receiver of the claim.	3
PaymentMeans	As in EN ISO 14906	Identifying the Contract/Central Account of the user that has benefited from a transport service. It also includes the expiry date and restrictions on the geographic usage and services allowed.	14
StationLocation	As in EN ISO 14906	The place where the EFC transaction took place	2
SessionTime	As in EN ISO 14906	The time when the EFC transaction took place	4
SessionFee	As in EN ISO 14906	The fee that was charged for the transport service	3
SessionTariffClass	As in EN ISO 14906	The session class applied for the fee calculation	1
ClaimedClass	As in EN ISO 14906	The class claimed by the OBE. See also Annex 2.	1
VATIncluded	Data informing whether or not VAT has been included in the fee	To inform the Contract Issuer on the VAT regulations applied: 0 = VAT not applicable 1 = VAT included 2 = VAT not included	1
Equipment Status	The value of the last 12 bits in the EFC Attribute EquipmentStatus is used as a Transaction Counter	Value read from the OBE enabling the Contract Issuer to keep track of the transactions performed by the OBE enabling the issuer	2
Issuer Authenticator	An authenticator computed with the secret key of the Contract Issuer	Used by the Contract Issuer to check the validity of the claim	4
RndRSE	Random number sent by the RSE to the OBE.	Random number to be used for the computation of the Issuer Authenticator	4
KeyRef	Key reference	Key reference for the Contract Issuer specific secret key used for computation of the Issuer Authenticator	1
PictureRef	A unique reference to a picture taken of the vehicle being linked to the EFC transaction	Used by the Contract Issuer and EFC operators to solve disputes between the User and/or the EFC operator and/or the Contract Issuer. StationLocation = 2 bytes SessionLocation = 1 byte SessionTime = 4 bytes ReasonFor StoringPicture = 1 byte	8



The Contract Issuer checks the validity of the claim. He primarily checks for a valid contract (valid Personal Account Number, contract not expired). He may also check some security elements, like the Transaction Counter and the Issuer Authenticator. Especially the Issuer Authenticator gives the Contract Issuer high confidence, since he is the only one in possession of the keys used to calculate it (he also needs the data KeyRef and RndRSE from the claim for the calculation).

The Contract Issuer has to reimburse the EFC Operator for correct claims, irrespective whether the user pays or not. 'Payment reminders' and debt collection in general is to be handled locally.

The MoU has to contain detailed rules about how to proceed with invalid claims.

3.3.4 Exception Handling

There are a number of points during the transaction phases where exceptions can occur which will need to be handled by the RSE. In all cases it will be necessary for the local enforcement procedures to be initiated which will in most cases start with the 'capture of proof of passage'. The table indicates the exceptions that can occur during the Initialisation and Presentation phases:

Initialisation		<ul style="list-style-type: none"> ▪ Non equipped user ▪ Contract not accepted
Presentation		<ul style="list-style-type: none"> ▪ OBE blacklisted ▪ Contract validity expired ▪ Transaction failure (incomplete transaction, security failure, data format errors) ▪ Sequencing error (missing entry ticket)

Initialisation Phase

In the Initialisation phase an equipped vehicle will present the following information in the VST:

<i>Phase</i>	<i>Roadside Equipment</i>		<i>On-board Equipment</i>
Initialisation (BST - VST)	INITIALISATION.request (BST)	→	
		←	INITIALISATION.response (VST) <ul style="list-style-type: none"> • EFC-ContextMark • AC_CR-Reference • RndOBE

The EFC-ContextMark contains the following information:

- Contract Provider
- Type of Contract
- Context Version

The RSE is required to check this information against the list of accepted MoU Contract Issuers and related contract types. The EFC Operator will only receive payment for valid contracts. If the RSE cannot accept one of the EFC contracts presented by the OBE, the transaction will be terminated. As no information regarding the identity of the user has been exchanged at this point, the local enforcement procedures will need to be initiated as is the case for non-equipped users.

Presentation Phase

Following the Initialisation phase in which the contract provider is identified it is necessary for the RSE to determine whether the contract presented by the OBE is valid for reimbursement of the users fee for passage by the Contract Issuer. In the Presentation phase the following information is presented by the OBE:

<i>Phase</i>	<i>RSE</i>		<i>OBE</i>
Presentation	GET_STAMPED.request AC_CR [Element Access Key] <ul style="list-style-type: none"> • Payment means including PersonalAccountNumber (RndRSE, KeyRef_Op) GET.request AC_CR [Element Access Key] <ul style="list-style-type: none"> • ReceiptData1 • ReceiptData2 • EquipmentStatus • Classification data 	→	
		←	GET_STAMPED.response <ul style="list-style-type: none"> • Operator_Authenticator (Auth_Op) GET.response

In order to be able to request data from the OBE the RSE is required to generate the appropriate access credentials using the random number RndOBE and key reference AC_CR-Reference (AC_CR-MasterKeyRef. and AC_CR-Diversifier) supplied by the OBE. If there is an error in the generation of the access credentials the RSE will not be able to obtain any further information form the OBE and the transaction will be terminated.

Following the receipt of this data the RSE is required to perform a number of checks to ensure that the contract is valid:

- Check the Personal Account Number (PAN) is of recognisable format
- Check the static period of validity of the contract
- Check the Blacklist for the PAN

The MoU will define the procedures for the exchange and updating of blacklists. EFC Operators will be guaranteed payment for passages for non-blacklisted contracts, for other cases the EFC Operator is responsible for the recovery of payment.

The rest of the information presented by the OBE during this phase maybe used by the RSE to calculate the charge for the passage, any errors encountered will mean that the RSE may not be able to calculate the correct charge applicable. In these cases it may be possible for the RSE to enter a default charge which can be corrected through back office procedures.

Optional presentation Phase

The optional presentation Phase is used to obtain the Issuer_Authenticator from the OBE.

<i>Phase</i>	<i>RSE</i>		<i>OBE</i>
<i>Optional Presentation</i>	GET_STAMPED.request AC_CR • Payment means including PersonalAccountNumber (RndRSE, KeyRef_Iss)	→	
		←	GET_STAMPED.response ▪ Issuer_Authenticator (Auth_Iss)

Receipt Phase

During the receipt phase the following information is written back to the OBE:

<i>Phase</i>	<i>RSE</i>		<i>OBE</i>
<i>Receipt</i>	SET.request • ReceiptData1 • ReceiptData2 • EquipmentStatus • ReceiptText SET_MMI.request	→	
		←	SET.response Set_MMI.response

At this stage all the information necessary to charge the user has been exchanged and a record of the transaction is written to the OBE. Whilst it may appear that errors at this stage would have little impact on the operation of the system there can be significant operational effects in closed systems. If such an error occurs at an entry station, and the receipt is not written to the OBE, the exit station will not have the information required to calculate the exit fee as the details of the entry station are carried in the OBE via the receipt.

Implications

As mentioned at the start of this section if an exception occurs then the local exception/enforcement procedures will have to be initiated by the RSE. In systems where a barrier is present this could simply involve not opening the barrier and asking the driver for an alternative payment means. However with the

increasing use of free-flow systems it is necessary for the RSE to capture 'proof of passage which can be used as evidence to recover payment.

At present there exists no common European legislation for the recovery of payment and as a result the evidence captured is determined by the local evidence requirements.

If errors occur after the Initialisation phase it may be possible for the EFC Operator to ask for assistance from the Contract Issuer in the identification of the user if bilateral agreements or MoU Procedures for co-operative enforcement have been put in place. If these agreements do not exist then the standard procedures for identifying non-equipped users on the local system will have to be followed.

4 REFERENCES

ENV ISO 14816:	2000	Road Transport and Traffic Telematics (RTTT) – Automatic Vehicle and Equipment Identification – Numbering and Data Structures
ENV ISO 14904:	2002	Road Transport and Traffic Telematics (RTTT) – Electronic Fee Collection (EFC) – Interface specification for clearing between operators
PrEN ISO 14906:	2002	Road Transport and Traffic Telematics (RTTT) – Electronic Fee Collection (EFC) – Application interface definition for dedicated short range communications
ENV ISO 14907-1:	1999	Road Transport and Traffic Telematics (RTTT) – Electronic Fee Collection (EFC) – Test Procedures for User and Fixed Equipment – Part 1: Description of test procedures
PrENV ISO 17573:	2002	Road Transport and Traffic Telematics (RTTT) – Electronic Fee Collection (EFC) – System architecture for vehicle related services
PrENV ISO 17574:	2002	Road Transport and Traffic Telematics (RTTT) – Electronic Fee Collection (EFC) – Security service framework – Guidelines for Protection Profiles
ISO 8731-1:	1987	Banking – Approved Algorithms for Message Authentication – Part1: DEA
ANSI X3.92	1998	Data Encryption Algorithm

TECHNICAL ANNEX

1 TERMS, DEFINITIONS AND ABBREVIATIONS

1.1 TERMS AND DEFINITIONS

This section covers the Terms and Definitions used during through this document, they have been extracted from the different standards available in the EFC field:

- ENV ISO 14904: 2002
- prEN ISO 14906: 2002
- ENV ISO 14907-1: 1999
- prENV ISO 14907-2
- prENV ISO 17573: 2002
- prENV ISO 17574:2002

with some inputs from the MANS terminology.

Access Control

The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.

Access Credentials

Data that is transferred to On-Board Equipment, in order to establish the claimed identity of an RSE.

NOTE: The access credentials carries information needed to fulfil access conditions in order to perform the operation on the addressed element in the OBE. The access credentials can carry passwords as well as cryptographic based information such as authenticators.

Attribute

Application information formed by one or by a sequence of data elements, and is managed by different actions used for implementation of a transaction.

Authentication

The provision of assurance of the claimed identity of an entity. Process performed to check if the presented information or equipment is valid and genuine, e.g. a payment contract for use in EFC

Authenticator

Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and/or the integrity of the data unit and protect against forgery.

Black List

A list of issued contracts and related payment means, which are not valid for payment in a payment system.

Central Account

A transport account which is administrated by the issuer of the payment means or by an entity acting on behalf of the issuer.

Certification

Action by a third party, demonstrating that adequate confidence is provided that a duly identified product, process or service is in conformity with a specific standard or other normative document.

Charging Operator (Roaming Operator)

A payment system operator that according to an agreement between the operators, accepts a payment based on a contract between the user and his/her home operator

Charging Point

The physical point or zone where the use of the transport service is registered. In case of a DSRC based system the communication between the OBE/OBU and RSU takes place to exchange the information

needed to charge the user by EFC. Charging point also covers the physical point or zone where a fee is collected manually.

Charging Point Equipment

The equipment installed at a charging point, e.g. a toll station, enabling the operator to collect the fee by the different payment methods offered to the users.

Classification

The process of dividing vehicles into various classes according to certain classification parameters (e.g. weight, length, purpose of use, engine type, number of axles, actual number of passengers).

Clearing

The operation of re-allocating value generated in the payment system(s) between the various operators in a payment system or between payment systems. This operation reflects commercial agreements existing between those parties. An example of such an operation is the exchange of information between Service Providers and an Issuer which enables the transfer of money from the Issuer, collecting the money from the User, to the Service Provider.

Clearing Operator

The entity that collects and possibly aggregates transactions from one or more Transport Service Providers for delivery to the Issuer(s). The Clearing Operator can also handle the Apportionment between the Transport Service Providers. In the financial world this operator is equivalent to an Acquirer. The entity responsible for selling, reloading or delivering the Payment Means to the

Collection Agent

The entity responsible for selling, reloading or delivering the Payment Means to the User and collecting the payment from the User on behalf of the Issuer. The Collection Agent can also collect user related application specific data from the User.

Compatibility

Suitability of products, processes or services to be used together under specific conditions to fulfil relevant requirements without causing unacceptable interactions

Confidentiality

The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Contract

The expression of an agreement between two or more parties in a payment system or between payment systems. An example of a contract is the specific relationship between a User and an Issuer in a payment system where the contract may be explicit or implicit.

Contract Issuer

See Home Operator

Contractual Interoperability

The intention of operators to co-operate recorded in a contractual agreement.

Cryptography

The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification or/and prevent its unauthorised use [ISO/IEC 7498-2].

Data Integrity

The property that data has not been altered or destroyed in an unauthorised manner.

Data Origin Authentication

The confirmation that the source of the data received is as claimed.

Declared Vehicle

A data set stored in the OBE/OBU containing vehicle characteristics of the vehicle Characteristics the OBU is related to.

EFC Equipment

EFC Equipment consists of Roadside Equipment (RSE) and On-Board Equipment (OBE).

EFC Operator

See Transport Service Provider

EFC Operator Authenticator

An authenticator calculated using the secret key known by the EFC Operators having signed the MoU and having implemented the Authentication service.

EFC System

A system that enables electronic debiting, i.e. paying for a transport service, without any action from the user at the moment of the use of the service.

Electronic Fee Collection

The collection of a fee for a transport service where the fee is collected via the exchange of data, e.g. via an air-link communication, enabling the user to pay for the transport service with electronic values, e.g. an electronic purse or values stored in a central account.

Electronic Purse

An application on an IC-card (integrated circuit card) or a similar device that can store, credit, debit and protect electronic values having their equivalent in money.

Enforcement

Measures or actions performed by enforcement authorities or other organisations to achieve compliance with laws, rules and regulations

Enforcement Operator

The entity responsible for prosecution on the basis of violation information provided by the Service Providers. Very often the Service Provider will be the Enforcement Operator.

Equipped User

A user that is in possession of accepted payment means and mediums necessary for payment of the service at the charging point

Exception

A user or system behaviour not conforming to the normal behaviour

External User

A user presenting appropriate payment means issued for his/her home payment system in another payment system to pay for the service in question (roaming)

Grey List

A part of the white list containing issued contracts and/or related payment means, which financial status is under consideration by the issuer

Home Operator

The payment system operator, with whom the user has signed a payment contract

Human-Machine Interface (HMI) (Man-Machine Interface (MMI))

The human-machine interaction mechanism, including the set of inputs, outputs, and dialogue procedures

Immediate Payment

Payment mode in which the funds are transferred from the user when a transport service is used

Integrated Payment Systems

A common framework of payment methods and information exchange between operators or payment systems that makes transfer of money from one payment system or operator to another possible (Clearing/Apportionment).

Interchangeability

The ability of one product, process or service to be used in place of another to fulfil the same requirements

Interoperability

The ability of systems to provide services to and accept services from other systems and to use these services to enable the systems to operate effectively together (see contractual, procedural and technical interoperability).

Issuer

The entity responsible for the payment system and responsible for issuing the Payment Means to the User.

Issuer Authenticator

An authenticator calculated using the secret key known only by the Contract Issuer

Key Management

The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

Non-Equipped User

A user that is not in possession of accepted payment means and mediums necessary for payment of the service at the charging point

Non-Repudiation

Protection against the denial, by one of the parties involved in the communication through the interface, of having participated in all or part of the communications.

On-Board Equipment (OBE)

Equipment located within the vehicle and supporting the information exchange with the Road Side Unit or the Central Communication Unit. It is composed of the On-Board Unit and other sub-units whose presence has to be considered optional for the execution of a Transaction.

OBE Customisation

Loading of issuer (operator) specific data and structures, i.e. creation of the EFC element and attributes including the writing of issuer specific data (e.g. EFC-ContextMark), in the OBE.

OBE Initialisation

Loading of issuer (operator) independent data and structures, such as the system element and manufacturing serial number, in the OBE.

OBE Personalisation

Loading of user specific data and structures, e.g. the OBE-specific keys (AuKes_Iss) and vehicle data, in the OBE.

OBE Programming

The whole process of OBE initialisation, customisation and personalisation.

On-Board Unit

Minimum component of an On-Board Equipment, whose functionality always includes at least the support of the DSRC interface or/and the Central Communication Unit and the protection of the data stored in the OBU.

Operator

Generic term for the entities Issuer, Clearing Operator, Collection Agent, Transport Service Provider, Enforcement Operator or Trusted Third Party.

Payment Means

The expression of a Contract between the User and the Issuer (or via a Collection Agent) that allows the User to access the transport services available in the Payment System, e.g. an account in a credit card system or an Electronic Purse.

Payment Medium

The carrier of payment means (such as ticket, card or on-board unit).

Payment Method

A combination of a Payment Means, a Payment Mode and a Payment Scope.

Payment Mode

Parameter defining the time dimension in payment by the User, e.g. Pre-payment or Post-payment.

Payment Scope

The application extent of the Payment Method, e.g. national transport or inter-sector.

Payment System

A financial system that includes the complete process of issuing and use of payment means, clearing and settlement of transactions.

Post Payment

Payment mode in which the funds are transferred from the user after the use of a transport service

Pre-Payment

Payment mode in which the funds are transferred from the user prior to the use of a transport service

Privacy

The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Procedural Interoperability

The existence of common data element definitions, the same working procedures and data delivery and common format of presentation in different sets of equipment required to communicate.

Random Number

A parameter whose value is unpredictable by the receiving party.

Road Side Equipment

Equipment located at a fixed position along the road transport network, for the purpose of communication and data exchanges with the On-Board Equipment of passing vehicles.

Roadside Unit

The DSRC part of the Roadside Equipment whose functionality is to communicate and exchange data with vehicles passing the charging point.

Secret Key

A key used with symmetric cryptographic techniques and usable only by a set of specified entities.

Secure Application Module

A module intended to contain algorithm(s), related keys, security procedures and information to protect an application in such a way that unauthorized access is not possible. In order to achieve this the module shall be physically, electrically and logically protected.

Security Policy

A set of rules that regulate how to cope with security threats or what degree of security levels should be kept.

Security Threat

A potential action or manner to violate security systems.

Service

Road transport related facility provided by a Service Provider. Normally a type of infrastructure, the use of which is offered to the User for which the User may be requested to pay.

Service Provider

The person, company, authority or abstract entity offering a service to the User for which the user has to pay a fee (the fee will in some cases be zero, e.g. emergency vehicles).

Settlement

Transfer of funds from one Operator to another according to the Clearing rules.

Technical Interoperability

The capability of different sets of equipment to work together through interconnection, co-ordinated execution or sharing of resources.

Toll Collection System

The equipment and functions enabling the collection of a fee for the use of road infrastructure.

Toll Plaza

See Charging point

Toll Station

See Charging point

Transaction

The whole of the exchange of information between the Roadside Equipment and the On-Board Equipment necessary for the completion of an Electronic Fee Collection operation over the DSRC.

NOTE: A transaction may require more than one session in order to be achieved, e.g. an entry session and an exit session.

Transaction Model

Functional model describing the general structure of Electronic Fee Collection transactions.

Transport Service

Road transport related facility provided by a Transport service Provider. Normally a type of infrastructure, e.g. a toll road or a road network inside a toll ring, the use of which is offered to the User for which the User is requested to pay.

Transport Service Provider

The person, company, authority or abstract entity offering a transport service to the User for which the user has to pay a fee (the fee will in some cases be zero, e.g. emergency vehicles).

Transport Service Provider Equipment

All equipment installed at the Charging point being used for EFC, e.g. communication equipment, classification systems, vehicle detection systems and signs and signals to the User.

Trusted Third Party

A security authority, or its agent, trusted by other entities with respect to security related activities. The entity who might be responsible for operation monitoring, system and security assessment (including security key management) as well as granting licences.

User (Client, Customer, Consumer)

The entity that uses a transport service provided by the Transport service Provider according to the terms of an agreement. The User may also be described as the subscriber of an EFC contract, the vehicle owner and the driver in those cases where these are not the same person or company.

User Equipment

Any equipment held by the User enabling him to communicate with the collection agent updating his service rights, e.g. with a PC and a modem.

Violator

A user who disregards laws, regulations and/or rules

White List

A list of issued contracts and related payment means, which are valid for payment in a payment system.

1.2 ABBREVIATIONS

Abbreviation	Definition
ASN.1	Abstract Syntax Notation One [ISO/IEC 8824]
Auth_Issuer	Issuer Authenticator
Auth_Operator	EFC Operator Authenticator
BST	Beacon Service Table [prEN 12834]
CEN	European Committee for Standardization (Comité Européen de Normalisation)
DEA	Data Encryption Algorithm [ISO 8731-1]
DES	Data Encryption Standard [ANSI X3.92]
DSRC	Dedicated Short-Range Communication
EFC	Electronic Fee Collection
EID	Element ID [prEN 12834]
EMC	Electromagnetic Compatibility
ETC	Electronic Toll Collection System
HMI	Human Machine Interface
HGV	Heavy Goods Vehicle
ICC	Integrated Circuit(s) Card
ID	Identification
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
L1	DSRC - Physical layer using microwave at 5.8 GHz (prEN 12253 : 2002)
L2	DSRC - Data link layer: MAC and LLC (prEN 12795 : 2002)
L7	DSRC - Application layer (prEN 12834 : 2002)
MAC	Message Authentication Code
MMI	Man-Machine Interface
MoU	Memorandum of Understanding
OBE	On-Board Equipment
OBU	On-Board Unit
RndOBE	Random number generated by the OBE
RndRSE	Random number generated by the RSE
RSE	Roadside Equipment
RSU	Roadside Unit
RTTT	Road Transport and Traffic Telematics
SAM	Secure Application Module
UML	Unified Modelling Language
VST	Vehicle Service Table [prEN 12834]

2 TRANSACTION

This chapter provides for the bit-level specification of the CARDME transaction. The specification accounts for the complete frame content (excluding the zero-bit insertions) of the data exchanged, including protocol information related to DSRC-L1, -L2 and -L7 in order to ensure a minimum ambiguity of the CARDME transaction specification. The data that are associated with the application level are highlighted in grey.

2.1 INITIALISATION

2.1.1 Initialisation request (BST)

Octet #	Attribute / Field	Bits in Octet b ₇ b ₀	Description
1	FLAG	0111 1110	Start Flag
2	Broadcast LID	1111 1111	Link address for broadcast
3	MAC control field	1010 0000	The frame contains a command LPDU
4	LLC control field	0000 0011	UI command
5	Fragmentation header	1xxxx x001	No fragmentation. PDU no shall never be set to 0000 ₂ or 0001 ₂ .
6	BST SEQUENCE {	1000	INITIALISATION.request
	OPTION indicator	0	NonmandApplications not present.
	BeaconId.ManufacturerId INTEGER (0..65535)	000	Manufacturer identifier. Example :1 (=Kapsch). See ENV ISO 14816 Register at www.nen.nl/cen278 for value assignment.
7		0000 0000	
8	BeaconId.IndividualId INTEGER (0..2 ²⁷ -1)	0000 1	27 bit ID available for manufacturer. Example: Id=1052
9		0000 0000	
10		0000 0100	
11		0001 1100	
12	Time TimeReal	0100 0001	32 bit UNIX System Time, the number of seconds passed since 1st January 1970, 00:00 (UTC). Example: 1103790512 ₁₀
13		1100 1010	
14		1000 0001	
15		1011 0000	
16	Profile INTEGER (0..127,...)	0000 0000	No extension, Profile p, (p=0 ₁₀ : 1,5 MHz subcarrier p=1 ₁₀ : 2,0 MHz subcarrier). Example: Profile 0
17	MandApplications SEQUENCE (0..127,...) OF {	0000 0001	No extension, Number of mandApplications= 1
18	OPTION indicator	0	EID not present
	OPTION indicator	0	Parameter not present
	AID DSRCApplicationEntityID }	00 0001	No extension. AID = 1 ₁₀ =EFC
19	ProfileList SEQUENCE (0..127,...) OF Profile }	0000 0000	No extension, number of profiles in list = 0.
20	FCS	xxxx xxxx	Frame check sequence
21		Xxxx xxxx	
22	FLAG	0111 1110	End Flag

2.1.2 Private window request

1	FLAG	0111 1110	Start Flag
2	Private LID	Xxxx xxx0	Link address of a specific OBE
3		Xxxx xxx0	
4		Xxxx xxx0	
5		Xxxx xxx1	
6	MAC control field	0110 0000	Private window request
7	FCS	Xxxx xxxx	Frame check sequence
8		Xxxx xxxx	
9	FLAG	0111 1110	End Flag

2.1.3 Private window allocation

1	FLAG	0111 1110	Start Flag
2	Private LID	Xxxx xxx0	Link address of a specific OBE
3		Xxxx xxx0	
4		Xxxx xxx0	
5		Xxxx xxx1	
6	MAC control field	0010 s000	Private window allocation
7	FCS	Xxxx xxxx	Frame check sequence
8		xxxx xxxx	
9	FLAG	0111 1110	End Flag

2.1.4 Initialisation response (VST)

Octet #	Attribute / Field	Bits in Octet b ₇ b ₀	Description
1	FLAG	0111 1110	Start Flag
2	Private LID	xxxx xxx0	Link address of a specific OBE
3		xxxx xxx0	
4		xxxx xxx0	
5		xxxx xxx1	
6	MAC control field	1100 0000	The frame contains a command LPDU
7	LLC control field	0000 0011	UI command
8	Fragmentation header	1xxx x001	No fragmentation. PDU no shall never be set to 0000 ₂ or 0001 ₂ .
9	VST SEQUENCE {	1001	INITIALISATION.response
	Fill BIT STRING (SIZE(4))	0000	Set to 0
10	Profile INTEGER (0..127,...)	0000 0000	No extension, profile p. Example : 0 ₁₀
11	Applications SEQUENCE (0..127,...) OF {	0000 0010	No extension, 2 applications
12	OPTION indicator	1	EID present
	OPTION indicator	1	Parameter present
	AID DSRCAApplicationEntityID	00 0001	No extension, AID = 1 (EFC)
13	EID	0000 0010	Associated with a context mark. Example : 2 ₁₀
14	Parameter CONTAINER	0000 0010	Choice 2 = Octet string
15		0000 0110	No extension, octet string length = 6 ₁₀
16	EFC-ContextMark SEQUENCE {		
	ContractProvider SEQUENCE {		
17	CountryCode BIT STRING (SIZE(10))	0011 0000	10 bit country code according to ISO 3166 with ITA2
	IssuerIdentifier INTEGER (0..16383) }	11 00 0000	Binary encoding based on ISO 14816. Example : NO 14 bits issuer identifier. Example 2 ₁₀
18		0000 0010	
19	TypeOfContract OCTET STRING (SIZE(2))	0000 0000	Type of contract. Example : 1
20		0000 0001	
21	ContextVersion INTEGER (0..127,...) }	0000 0010	No extension, context version. Example : 2 ₁₀
22	OPTION indicator	1	EID present
	OPTION indicator	1	Parameter present
	AID DSRCAApplicationEntityID	00 0001	No extension, AID = 1 (EFC)
23	EID	0000 0101	Associated with a context mark.
24	Parameter CONTAINER {	0000 0010	Choice 2 = Octet string
25		0001 0000	No extension, octet string length = 16 ₁₀
26	EFC-ContextMark SEQUENCE {		
	ContractProvider SEQUENCE {		
27	CountryCode BIT STRING (SIZE(10))	1010 0100	10 bit country code according to ISO 3166 with ITA2 binary
	IssuerIdentifier INTEGER (0..16383) }	00 00 0000	Encoding based on ISO 14816. Example : SE 14 bits issuer identifier. Example : 1 ₁₀ (Öresundskonsortiet)
28		0000 0001	
29	TypeOfContract OCTET STRING (SIZE(2))	0000 0000	Type of contract. Example 2
30		0000 0010	
31	ContextVersion INTEGER (0..127,...) }	0000 0001	No extension, context version. Example : 1 ₁₀
32	CONTAINER	0000 0010	Choice 2 = Octet string
33	OCTET STRING	0000 0010	No extension, field length 2 ₁₀
34	AC_CR-Reference SEQUENCE {		
	AC-MasterKeyRef Int1, AC_CR-Diversifier Int1}	0000 0001 0000 0001	AC_CR-Reference to, consisting of AC_CR-MasterKeyRef and AC_CR-Diversifier, used for the computation of AC_CRKey and AC_CR.
35		0000 0010	Choice 2 = Octet string
36	CONTAINER	0000 0010	Choice 2 = Octet string
37	OCTET STRING	0000 0100	No extension, field length 4 ₁₀
38	rndOBE Int4	0000 0000	Random Number (nonce) used together with AC_CRKey to
39		0000 0000	calculate AC_CR. Example : 640 ₁₀
40		0000 0010	
41		1000 0000	
42	ObeConfiguration SEQUENCE {		
	OPTION indicator	1	ObeStatus present
	EquipmentClass INTEGER (0..32767)	000 0000 0000 0011	Example : 3 ₁₀
43		0000 0000	
44	ManufacturerId INTEGER (0..65535)	0000 0000	Manufacturer identifier. See ENV ISO 14816 Register at
45		0000 0010	www.nen.nl/cen278 for value assignment. Example : 2 ₁₀ .
46	ObeStatus INTEGER(0..65535)	0000 0011	Example : 768 ₁₀
47		0000 0000	
48	FCS	Xxxx xxxx	Frame check sequence
49		Xxxx xxxx	
50	FLAG	0111 1110	End Flag

2.2 PRESENTATION

2.2.1 Presentation request

Octet #	Attribute / Field	Bits in Octet b ₇ b ₀	Description
1	FLAG	0111 1110	Start Flag
2	Private LID	xxxx xxx0	Link address of a specific OBE
3		xxxx xxx0	
4		xxxx xxx0	
5		xxxx xxx1	
6	MAC control field	1010 S000	The frame contains a command LPDU
7	LLC control field	N111 0111	Polled ACn command, n bit
8	Fragmentation header	1xxx x001	No fragmentation. First service of chain.
9	GET_STAMPED.request SEQUENCE {	0000 1101	ACTION.request (GET Stamped, AccessCredential and ActionParamert present, IID not present and Reply expected)
10	EID INTEGER(0..127,...)	0000 0101	Element EID, uniquely related to a Context mark within the OBE
11	ActionType INTEGER(0..127,...)	0000 0000	No extension, GET_STAMPED.request = 0
12	AccessCredential OCTET STRING {	0000 0100	No extension, octet string length = 4 ₁₀
13	AC_CR	aaaa aaaa	Access credential calculated by RSE using RndOBE and the Access Credential Key AC_CRKey.
14		aaaa aaaa	
15		aaaa aaaa	
16		aaaa aaaa	
17	ActionParameter CONTAINER {	0001 0001	No extension, Choice 17 ₁₀ = GetStampedRq
18	AttributeldList SEQUENCE (0..127,...) OF { INTEGER (0..127,...) Attributeld {	0000 0001	No extension, number of attribute IDs = 1
19	PaymentMeans } }	0010 0000	Attributeld = 32 ₁₀ = PaymentMeans
20	Nonce OCTET STRING {	0000 0100	No extension, octet string length = 4 ₁₀
21	RndRSE	rrrr rrrr	Random number from RSE, containing SessionTime, needed to calculate OperatorAuthenticator
22		rrrr rrrr	
23		rrrr rrrr	
24		rrrr rrrr	
25	KeyRef_Op(h) } }	xxxx xxxx	h = Reference to AuKey_Op used for the computation of Operator Authenticator.
26	Fragmentation header	1xxx x001	No fragmentation. Same PDU no as before (concatenation).
27	GET.request SEQUENCE {	0110	GET.request
	OPTION indicator	1	AccessCredential present
	OPTION indicator	0	IID not present
	OPTION indicator	1	AttributeldList present
	Fill BIT STRING(SIZE(1))	0	Set to 0
28	EID INTEGER(0..127,...)	0000 0101	No extension, EID
29	AccessCredential OCTET STRING {	0000 0100	No extension, octet string length = 4 ₁₀
30	AC_CR	aaaa aaaa	Access credential calculated by RSE using RndOBE and the Access Credential Key AC_CRKey.
31		aaaa aaaa	
32		aaaa aaaa	
33		aaaa aaaa	
34	AttributeldList SEQUENCE (0..127,...) OF { INTEGER (0..127,...) Attributeld {	0000 0110	No extension, number of attribute lds = 6 ₁₀
35	VehicleLicencePlateNumber	0001 0000	Attributeld = 16 ₁₀ = VehicleLicencePlateNr
36	VehicleClass	0001 0001	Attributeld = 17 ₁₀ = VehicleClass
37	VehicleWeightLimits	0001 0100	Attributeld = 20 ₁₀ = VehicleWeightLimits
38	EquipmentStatus	0001 1010	Attributeld = 26 ₁₀ = EquipmentStatus
39	ReceiptData1	0010 0001	Attributeld = 33 ₁₀ = ReceiptData1
40	ReceiptData2 } } }	0010 0010	Attributeld = 34 ₁₀ = ReceiptData2
41	FCS	xxxx xxxx	Frame check sequence
42		xxxx xxxx	
43	FLAG	0111 1110	End Flag

Remark: VehicleSpecificCharacteristics, VehicleDimensions and VehicleAxles are not included in the above example.

2.2.2 Presentation response

Octet #	Attribute / Field	Bits in Octet b ₇ b ₀	Description
1	FLAG	0111 1110	Start Flag
2	Private LID	xxxx xxx0	Link address of a specific OBE
3		xxxx xxx0	
4		xxxx xxx0	
5		xxxx xxx1	
6	MAC control field	1101 0000	The frame contains a response LPDU
7	LLC control field	N111 0111	Response available, ACn command n bit
8	LLC status field	0000 0000	Response available and command accepted
9	Fragmentation header	1xxx x001	No fragmentation. First service of chain.
10	GET_STAMPED.response SEQUENCE {	0001 0100	ACTION.response (Get Stamped rs)
11	EID INTEGER (0..127,...)	0000 0101	No extension, EID
12	ResponseParameter CONTAINER {	0001 0010	No extension. Choice 18 ₁₀ = GetStampedRs
13	AttributeList SEQUENCE (0..127,...) OF {	0000 0001	No extension, number of attributes: 1
14	Attributes SEQUENCE { AttributeId	0010 0000	PaymentMeans = 32 ₁₀
15	AttributeValue CONTAINER {	0100 0000	Container Choice: 64 ₁₀ = PaymentMeans
16	PersonalAccountNumber	xxxx xxxx	PersonalAccountNumber
17		xxxx xxxx	
18		xxxx xxxx	
19		xxxx xxxx	
20		xxxx xxxx	
21		xxxx xxxx	
22		xxxx xxxx	
23		xxxx xxxx	
24		xxxx xxxx	
25		xxxx xxxx	
26	PaymentMeansExpiryDate	0001 1110	DateCompact. Example : 2005-03-01
27		0110 0001	
28	PaymentMeansUsageControl	0000 0000	Example : 1
29		0000 0001	
30	Authenticator OCTET STRING {	0000 0100	No extension, octet string size = 4 ₁₀
31	OperatorAuthenticator	xxxx xxxx	Operator Authenticator over AttributeList (containing PaymentMeans) and RndRSE (containing SessionTime) calculated using AuKey_Op(h).
32		xxxx xxxx	
33		xxxx xxxx	
34		xxxx xxxx	
35	Fragmentation header	1xxx x001	No fragmentation. Same PDU no as before (concatenation).
36	GET.response SEQUENCE	0111 0100	GET.response
37	EID INTEGER(0..127,...)	0000 0101	No extension, EID
38	AttributeList SEQUENCE (0..127,...) OF {	0000 0110	No extension, 6 attributes in list.
39	AttributeId INTEGER(0..127,...)	0001 0000	AttributeId = 16 ₁₀ = VehicleLicencePlateNo
40	Attribute Value CONTAINER {	0010 1111	Container choice = 47 ₁₀
41	Vehlpn {SEQUENCE countryCode,	1010 0100	VehicleLicencePlateNumber. Example : SE, alphabet indicator no 1 OCD560
42		00	
43	AlphabetIndicator,	00 0000	
44	LicencePlateNumber	0000 0110	
45		0100 1111	
46		0100 0011	
47		0100 0100	
48		0011 0101	
49		0011 0110	
49		0011 0000	
50	AttributeId INTEGER(0..127,...)	0001 0001	AttributeId = 17 ₁₀ = VehicleClass
51	Attribute Value CONTAINER {	0011 0001	Container choice = 49 ₁₀
52	VehicleClass	xxxx xxxx	VehicleClass value
53	AttributeId INTEGER(0..127,...)	0001 0100	AttributeId = 20 ₁₀ = VehicleWeightLimits
54	Attribute Value CONTAINER {	0011 0100	Container choice = 52 ₁₀
55	VehicleWeightLimits	xxxx xxxx	VehicleWeightLimits.VehicleMaxLadenWeight
56		xxxx xxxx	VehicleWeightLimits.VehicleTrainMaxWeight
57		xxxx xxxx	
58		xxxx xxxx	VehicleWeightLimits.VehicleWeightUnladen
59		xxxx xxxx	
60		xxxx xxxx	

Octet #	Attribute / Field	Bits in Octet b ₇ b ₀	Description
61	Attributeld INTEGER(0..127,...)	0001 1010	Attributeld = 26 ₁₀ = EquipmentStatus
62	Attribute Value CONTAINER {	0011 1010	Container choice = 58 ₁₀
63	EquipmentStatus	0000 0000	EquipmentStatus
64	} }	0000 0001	
65	Attributeld INTEGER(0..127,...)	0010 0001	Attributeld = 33 ₁₀ = ReceiptData1
66	Attribute Value CONTAINER {	0100 0001	Container choice = 65 ₁₀
67	ReceiptData1	Xxxx xxxx	ReceiptData1.SessionTime
68		Xxxx xxxx	
69		Xxxx xxxx	
70		Xxxx xxxx	
71		Xxxx xxxx	ReceiptData1.SessionServiceProvider
72		Xxxx xxxx	
73		Xxxx xxxx	
74		Xxxx xxxx	ReceiptData1.StationLocation
75		Xxxx xxxx	
76		Xxxx xxxx	ReceiptData1.SessionLocation
77		Xxxx xxxx	ReceiptData1.TypeOfSession
78		Xxxx xxxx	ReceiptData1.SessionResult
79		Xxxx xxxx	ReceiptData1.SessionTariffClass
80		Xxxx xxxx	ReceiptData1.ClaimedClass
81		Xxxx xxxx	ReceiptData1.SessionFee
82		Xxxx xxxx	
83		Xxxx xxxx	
84		Xxxx xxxx	
85		Xxxx xxxx	ReceiptData1.SessionContractProvider
86		Xxxx xxxx	
87		Xxxx xxxx	
88		Xxxx xxxx	ReceiptData1.SessionTypeOfContract
89		Xxxx xxxx	
90		Xxxx xxxx	ReceiptData1.SessionContextVersion
91		Xxxx xxxx	ReceiptData1.Authenticator
92		Xxxx xxxx	
93		Xxxx xxxx	
94	}	Xxxx xxxx	
95	Attributeld INTEGER(0..127,...)	0010 0010	Attributeld = 34 ₁₀ = ReceiptData2
96	Attribute Value CONTAINER {	0100 0010	Container choice = 66 ₁₀
97	ReceiptData2	Xxxx xxxx	ReceiptData2. Same format as ReceiptData1 (see octets # 67-94)
....		Xxxx xxxx	
124	}	Xxxx xxxx	
125	FCS	Xxxx xxxx	Frame check sequence
126		Xxxx xxxx	
127	FLAG	0111 1110	End Flag

Remark: VehicleSpecificCharacteristics, VehicleDimensions and VehicleAxles are not included in the above example.

2.3 OPTIONAL PRESENTATION

2.3.1 Optional presentation request

Octet #	Attribute / Field	Bits in Octet b ₇ b ₀	Description
1	FLAG	0111 1110	Start Flag
2	Private LID	xxxx xxx0	Link address of a specific OBE
3		xxxx xxx0	
4		xxxx xxx0	
5		xxxx xxx1	
6	MAC control field	1010 S000	The frame contains a command LPDU
7	LLC control field	N111 0111	Polled ACn command n bit
8	Fragmentation header	1xxx x001	No fragmentation. First service of chain.
9	GET_STAMPED.request SEQUENCE {	0000 1101	ACTION.request (GET Stamped, AccessCredential and ActionParamert present, IID not present and Reply expected)
10	EID INTEGER(0..127,...)	0000 0101	Element EID, uniquely related to a Context mark within the OBE
11	ActionType INTEGER(0..127,...)	0000 0000	No extension, GET_STAMPED.request = 0
12	AccessCredential OCTET STRING {	0000 0100	No extension, octet string length = 4 ₁₀
13	AC_CR	aaaa aaaa	Access credential calculated by RSE using RndOBE and the
14		aaaa aaaa	Access Credential Key AC_CRKey.
15		aaaa aaaa	
16		aaaa aaaa	
17	ActionParameter CONTAINER {	0001 0001	No extension, Choice 17 ₁₀ = GetStampedRq
	AttributeldList SEQUENCE (0..127,...) OF		
18	{ INTEGER (0..127,...) Attributeld {	0000 0001	No extension, number of attribute IDs = 1
19	PaymentMeans } }	0010 0000	Attributeld = 32 ₁₀ = PaymentMeans
20	Nonce OCTET STRING {	0000 0100	No extension, octet string length = 4 ₁₀
21	RndRSE	Rrrr rrrr	Random number from RSE, containing Session Time, needed to
22		Rrrr rrrr	calculate IssuerAuthenticator
23		Rrrr rrrr	
24		Rrrr rrrr	
25	KeyRef_Iss(i) }	Xxxx xxxx	i = Reference to AuKey_Iss used in the computation of Issuer Authenticator.
26	FCS	Xxxx xxxx	Frame check sequence
27		xxxx xxxx	
28	FLAG	0111 1110	End Flag

2.3.2 Optional presentation response

Octet #	Attribute / Field	Bits in Octet b ₇ b ₀	Description
1	FLAG	0111 1110	Start Flag
2	Private LID	xxxx xxx0	Link address of a specific OBE
3		xxxx xxx0	
4		xxxx xxx0	
5		xxxx xxx1	
6	MAC control field	1101 0000	The frame contains a response LPDU
7	LLC control field	N111 0111	ACn command n bit
8	LLC status field	0000 0000	Response available and command accepted
9	Fragmentation header	1xxx x001	No fragmentation. First service of chain.
10	GET_STAMPED.response SEQUENCE {	0001 0100	ACTION.response (Get Stamped rs)
11	EID INTEGER (0..127,...)	0000 0101	No extension, EID
12	ResponseParameter CONTAINER {	0001 0010	No extension. Choice 18 ₁₀ = GetStampedRs
13	AttributeList SEQUENCE (0..127,...) OF {	0000 0001	No extension, number of attributes: 1
14	Attributes SEQUENCE { AttributeId	0010 0000	PaymentMeans = 32 ₁₀
15	AttributeValue CONTAINER {	0100 0000	Container Choice: 64 ₁₀ = PaymentMeans
16	PaymentMeans	xxxx xxxx	PaymentMeans
17		xxxx xxxx	
18		xxxx xxxx	
19		xxxx xxxx	
20		xxxx xxxx	
21		xxxx xxxx	
22		xxxx xxxx	
23		xxxx xxxx	
24		xxxx xxxx	
25		xxxx xxxx	
26	PaymentMeansExpiryDate	0001 1110	DateCompact. Example : 2005-03-01
27	PaymentMeansUsageControl	0110 0001	Example : 1
28	} }	0000 0000	
29		0000 0001	
30		Authenticator OCTET STRING {	
31	IssuerAuthenticator	xxxx xxxx	Issuer Authenticator over AttributeList (containing PaymentMeans) and RndRSE (containing SessionTime) calculated using AuKey_Iss(i).
32		xxxx xxxx	
33		xxxx xxxx	
34		xxxx xxxx	
35	FCS	xxxx xxxx	Frame check sequence
36		xxxx xxxx	
37	FLAG	0111 1110	End Flag

2.4 RECEIPT

2.4.1 Set receipt request

Octet#	Attribute / Field	Bits in Octet b ₇ b ₀	Description
1	FLAG	0111 1110	Start Flag
2	Private LID	xxxx xxx0	Link address of a specific OBE
3		xxxx xxx0	
4		xxxx xxx0	
5		xxxx xxx1	
6	MAC control field	1010 S000	The frame contains a command LPDU
7	LLC control field	N111 0111	Polled ACn command n bit
8	Fragmentation header	1xxx x001	No fragmentation. First service of chain.
9	SET.request SEQUENCE {	0100 1001	SET.request (AccessCredential, no IID, fill, reply expected)
10	EID INTEGER(0..127,...)	0000 0101	No extension, EID
11	AccessCredentials OCTET STRING {	0000 0100	No extension, octet string length = 4 ₁₀
12	AC_CR	aaaa aaaa	Access credential calculated by RSE using RndOBE and the Access Credential Key AC_CRKey.
13		aaaa aaaa	
14		aaaa aaaa	
15	}	aaaa aaaa	
16	AttributeList SEQUENCE ((0..127,...) OF {		
	Attributes SEQUENCE {	0000 0100	No extension, number of attributes in list = 4 ₁₀
17	Attributeld INTEGER(0..127,...)	0000 1100	Attributeld = 12 ₁₀ = ReceiptText
18	Attribute Value CONTAINER {	0010 1100	Container choice = 44 ₁₀
19	Length indicator	0000 1010	10 octets
20	ReceiptText	xxxx xxxx	ReceiptText value
21		xxxx xxxx	
22		xxxx xxxx	
23		xxxx xxxx	
24		xxxx xxxx	
25		xxxx xxxx	
26		xxxx xxxx	
27		xxxx xxxx	
28		xxxx xxxx	
29	}	xxxx xxxx	
30	Attributeld INTEGER(0..127,...)	0001 1010	Attributeld = 26 ₁₀ = EquipmentStatus
31	Attribute Value CONTAINER {	0011 1010	Container choice = 58 ₁₀
32	EquipmentStatus	xxxx xxxx	EquipmentStatus value
33	}	xxxx xxxx	
34	Attributeld INTEGER(0..127,...)	0010 0001	Attributeld = 33 ₁₀ = ReceiptData 1
35	Attribute Value CONTAINER {	0100 0001	Container choice = 65 ₁₀
36	ReceiptData1	xxxx xxxx	ReceiptData1.SessionTime
37		xxxx xxxx	
38		xxxx xxxx	ReceiptData1.SessionServiceProvider
39		xxxx xxxx	
40		xxxx xxxx	
41		xxxx xxxx	ReceiptData1.StationLocation
42		xxxx xxxx	
43		xxxx xxxx	ReceiptData1.SessionLocation
44		xxxx xxxx	
45		xxxx xxxx	ReceiptData1.TypeOfSession
46		xxxx xxxx	ReceiptData1.SessionResult
47		xxxx xxxx	ReceiptData1.SessionTariffClass
48		xxxx xxxx	ReceiptData1.ClaimedClass
49		xxxx xxxx	ReceiptData1.SessionFee
50		xxxx xxxx	
51		xxxx xxxx	
52		xxxx xxxx	ReceiptData1.SessionContractProvider
53		xxxx xxxx	
54		xxxx xxxx	
55		xxxx xxxx	ReceiptData1.SessionTypeOfContract
56		xxxx xxxx	
57		xxxx xxxx	ReceiptData1.SessionContextVersion
58		xxxx xxxx	
59		xxxx xxxx	

Octet #	Attribute / Field	Bits in Octet		Description
		b ₇	b ₀	
60	}	xxxx	xxxx	ReceiptData1.Authenticator
61		xxxx	xxxx	
62		xxxx	xxxx	
63		xxxx	xxxx	
64	Attributeld INTEGER(0..127,...)	0010	0010	Attributeld = 34 ₁₀ = ReceiptData2
65	Attribute Value CONTAINER {	0100	0010	Container choice = 66 ₁₀
66	ReceiptData2	xxxx	xxxx	ReceiptData2. Same format as ReceiptData1 (see octets #31-58)
....		
93		xxxx	xxxx	
94		Fragmentation header	1xxx	
95	SET_MMI.request SEQUENCE {	0000		ACTION.request
	OPTION indicator		0	AccessCredential not present
	OPTION indicator		1	ActionParameter present
	OPTION indicator		0	IID not present
	Mode BOOLEAN		1	Confirmed mode, reply expected
96	EID INTEGER(0..127,...)	0000	0000	No extension, EID = 0 (system element)
97	ActionType INTEGER(0..127,...)	0000	1010	No extension, SET_MMI.request = 10 ₁₀
98	ActionParameter CONTAINER	0000	0000	No extension, Type 0 = INTEGER
99	SetMMI INTEGER }	0000	0000	Example : ok (0 ₁₀)
100	FCS	xxxx	xxxx	Frame check sequence
101		xxxx	xxxx	
102	FLAG	0111	1110	End Flag

2.4.2 Set receipt response

Octet #	Attribute / Field	Bits in Octet		Description
		b ₇	b ₀	
1	FLAG	0111	1110	Start Flag
2	Private LID	xxxx	xxx0	Link address of a specific OBE
3		xxxx	xxx0	
4		xxxx	xxx0	
5		xxxx	xxx1	
6	MAC control field	1101	0000	The frame contains a response LPDU
7	LLC control field	N111	0111	ACn command n bit
8	LLC status field	0000	0000	Response available and command accepted
9	Fragmentation header	1xxx	x001	No fragmentation. First service of chain.
10	SET.response SEQUENCE {	0101		SET.response
	OPTION indicator		0	IID not present
	OPTION indicator		0	ResponseStatus not present
	Fill BIT STRING (SIZE(2))		00	Set to 0
11	EID INTEGER (0..127,...) }	0000	0101	No extension, EID
12	Fragmentation header	1xxx	x001	No fragmentation.
13	ACTION.response SEQUENCE {	0001		SET_MMI.response
	OPTION indicator		0	IID not present
	OPTION indicator		0	ResponseParameter not present
	OPTION indicator		0	ResponseStatus not present
	Fill BIT STRING (SIZE(1))		0	Set to 0
14	EID INTEGER (0..127,...) }	0000	0000	No extension, System Element EID = 0
15	FCS	xxxx	xxxx	Frame check sequence
16		xxxx	xxxx	
17	FLAG	0111	1110	End Flag

2.5 TRACKING AND CLOSING

2.5.1 Tracking request (Echo.request)

Octet #	Attribute / Field	Bits in Octet b ₇ b ₀	Description
1	FLAG	0111 1110	Start Flag
2	Private LID	xxxx xxx0	Link address of a specific OBE
3		xxxx xxx0	
4		xxxx xxx0	
5		xxxx xxx1	
6	MAC control field	1010 0000	
7	LLC control field	N111 0111	Polled ACn command n bit
8	Fragmentation header	1xxx x001	No fragmentation.
9		0000	ACTION.request
	ECHO.request SEQUENCE {		
	OPTION indicator	0	No Access Credentials
	OPTION indicator	1	ActionParameter present
	OPTION indicator	0	IID not present
	Mode BOOLEAN	1	Reply expected
10	EID INTEGER (0..127,...)	0000 0000	No extension, EID = 0
11	ActionType INTEGER (0..127,...)	0000 1111	No extension, ECHO.request = 15
12	ActionParameter CONTAINER	0000 0010	No extension, Choice 2 = Octet string
13	}	0000 0000	No extension. String length = 0 octets
14	FCS	xxxx xxxx	Frame check sequence
15		xxxx xxxx	
16	FLAG	0111 1110	End Flag

2.5.2 Tracking response (Echo.response)

1	FLAG	0111 1110	Start Flag
2	Private LID	xxxx xxx0	Link address of a specific OBE
3		Xxxx xxx0	
4		Xxxx xxx0	
5		xxxx xxx1	
6	MAC control field	1101 0000	
7	LLC control field	N111 0111	ACn command n bit
8	LLC status field	0000 0000	Response available and command accepted
9	Fragmentation header	1xxx x001	No fragmentation.
10		0001	ACTION.response
	ECHO.response SEQUENCE {		
	OPTION indicator	0	No IID
	OPTION indicator	1	ResponseParameter present
	OPTION indicator	0	ReturnStatus not present
	FILL BIT STRING (SIZE(1))	0	Set to 0.
11	EID INTEGER (0..127,...)	0000 0000	No extension, EID = 0
12	ResponseParameter CONTAINER	0000 0010	No extension, Choice 2 = Octet string
13	}	0000 0000	No extension. String length = 0 octets
14	FCS	xxxx xxxx	Frame check sequence
15		xxxx xxxx	
16	FLAG	0111 1110	End Flag

2.5.3 Closing

1	FLAG	0111 1110	Start Flag
2	Private LID	xxxx xxx0	Link address of a specific OBE
3		xxxx xxx0	
4		xxxx xxx0	
5		xxxx xxx1	
6	MAC control field	1000 0000	
7	LLC control field	0000 0011	UI command
8	Fragmentation header	1xxx x001	No fragmentation.
9	RELEASE.request SEQUENCE {	0010	EVENT_REPORT.request
	OPTION indicator	0	AccessCredential not present
	OPTION indicator	0	EventParameter not present
	OPTION indicator	0	IID not present
	Mode BOOLEAN	0	No reply expected
10	EID INTEGER (0..127,...)	0000 0000	No extension, EID = 0 (system element)
11	EventType INTEGER (0..127,...)	0000 0000	No extension, RELEASE = 0.
12	FCS	xxxx xxxx	Frame check sequence
13		xxxx xxxx	
14	FLAG	0111 1110	End Flag

3 ATTRIBUTES AND DATA ELEMENTS

This chapter defines the attributes and data elements used in the CARDME transaction, by referring to the definitions in prEN ISO 14906 and by provision of precision of CARDME's usage when necessary. Examples are given to facilitate the reading.

The following abbreviations are used in the table:

M / O = Mandatory / Optional

- R = Read (access conditions)
- W = Write (access conditions)

Attribute Id / Name Data element	Definition & remarks according to prEN ISO 14906	CARDME usage	Length in octets	M/O	Access conditions	Responsible
0 / EFC-ContextMark			6	M	R	Issuer
ContractProvider	Identifies the organisation that issued the service rights given in the Contract. Numbers shall be assigned on a national basis. The ContractProvider might, e.g., be a single operator or a group of operators holding an inter-company agreement.	Usage according to prEN ISO 14906 : Country code (10 bits) + Issuer Identifier (14 bits). Example : <ul style="list-style-type: none"> • Sweden = 1010010000'B • Öresundskonsortiet = 00 0000 0000 0001'B See also ENV ISO 14816 Register at www.nen.nl/cen278 .	3			
TypeOfContract	ContractProvider-specific designation of the rules that apply to the Contract. Allows, e.g., for the determination of the tariff or designating the type of purse associated with the contract.	A two octet value identifying the EFC contract residing in the OBE (e.g. central account or on-board purse). CARDME's European central held account transaction is assigned the value 0000 0000 0000 0001'B.	2			
ContextVersion	ContextVersion denotes the implementation version of the concerned contract within the context of the given ContractProvider, value assigned at the discretion of the ContractProvider. The ContextVersion may also be used as a security key reference.	Identification of the version residing in the OBE. 0sss vvvv'B, where <ul style="list-style-type: none"> • sss identifies the personalisation security key used. 000'B identifies Security Key version 0 etc. • vvvv identifies the version of the CARDME transaction. 0000'B identifies CARDME-4, version 1.0 	1			

Attribute Id / Name Data element	Definition & remarks according to prEN ISO 14906	CARDME usage	Length in octets	M/O	Access conditions	Responsible
32 / PaymentMeans			14	M	R	Issuer
Personal Account Number	Coded according to financial institutions.	Usage according to prEN ISO 14906	10			
PaymentMeans ExpiryDate	Expiring date of payment means. Payment means expires at 24h of PaymentMeans ExpiryDate	DateCompact	2			
PaymentMeans UsageControl	Indicates issuer's specified restrictions on the geographic usage and services allowed for the applications	OCTET STRING (SIZE(2))	2			
12 / ReceiptText					W	Operator
ReceiptText	Plain text decodeable by the OBU. May be used to display session information to user (e.g. session location).	An octet string containing a maximum of 13 characters – 1 octet for the length indicator and 12 octets with receipt text characters. The semantics of what the RSE shall transmit is not prescribed. Example : EURO 2.00, <ul style="list-style-type: none"> length indicator = 0000 1000'B EURO 2.00 	Variable (CARD ME, max 13)			
16 / Vehicle License Plate Number					R	Issuer
VehicleLicence PlateNumber	Claimed licence plate of the vehicle	Usage according to prEN ISO 14906. Example : SE, LatinAlphabethNo1, OCD560 <ul style="list-style-type: none"> Country code = SE = 1010010000'B Alphabet indicator = LatinAlphabethNo1 = 000000'B Length indicator = 6 octets = 00000110'B LPN = OCD560 = 4F 43 44 35 36 30'H 	Variable	O		

Attribute Id / Name Data element	Definition & remarks according to prEN ISO 14906	CARDME usage	Length in octets	M/O	Access conditions	Responsible
17/ Vehicle Class Vehicle Class	Service provider specific information pertaining to the vehicle.	Vehicle class' substructure TCCC LLLL, where <ul style="list-style-type: none"> • T (trailer indicator) : • 0'B = no trailer • 1'B = trailer present • CCC (MoU) • LLLL (Local vehicle classes) : value assignments at the discretion of the contract issuer. 	1	M	R(W)	Issuer (/User)
18 / VehicleDimensions			3	O	R	Issuer
VehicleLengthOverall	Nominal maximum overall length of the vehicle according to ISO 612, in dm, rounded to the next dm.	Usage according to prEN ISO 14906. Example : a 6.15 m long vehicle is coded as 0011 1101'B.	1			
VehicleHeightOverall	Nominal overall unladen height, according to ISO 612, in dm, rounded to the next dm.	Usage according to prEN ISO 14906. Example : a 2.43 m high vehicle is coded as 0001 1000'B.	1			
VehicleWidthOverall	Nominal overall width, according to ISO 612, in dm, rounded to the next dm	Usage according to prEN ISO 14906. Example : a 1.87 m wide vehicle is coded as 0001 0010'B.	1			
19 / VehicleAxles VehicleAxles	Tyre type and number of axles, including drop axles. / Also gives information on the usage of dual tyres.	Usage according to prEN ISO 14906 : hhhh hhhh ttaa aaaa, where <ul style="list-style-type: none"> • hhhh hhhh : Vehicle first axle height (8 bits). Example : a bonnet height of 115 cm is coded as 0000 1011'B. • tt : Tyre type (2 bits) : • 00'B = not specified; • 01'B = single tyre per axle; • 10'B = dual tyres per axle; • 11'B = reserved for future CEN use, • aa aaaa: number of Axles (6 bits). Example : 2 axles is coded as 00 0010'B. 	2	O	R(W)	Issuer (/User)

Attribute Id / Name Data element	Definition & remarks according to prEN ISO 14906	CARDME usage	Length in octets	M/O	Access conditions	Responsible
20 / VehicleWeightLimits			6	O	R	Issuer
VehicleMaxLaden Weight	Maximum permissible total weight including payload, according to ISO 1176. 10kg units, rounded down to the next 10kg step.	Usage according to prEN ISO 14906. Example: a weight of 16'801 kg is coded as 0000 0110 1001 0000'B.	2			
VehicleTrainMaximum Weight	Maximum permissible weight of the complete vehicle train, as defined in ISO 1176. 10kg units, rounded down to the next 10kg step. / ISO 1176 Code ISO-M18 maximum design mass of vehicle combination	Usage according to prEN ISO 14906. Example: a weight of 16'801 kg is coded as 0000 0110 1001 0000'B.	2			
VehicleWeightUnladen	Nominal unladen weight, according to ISO 1176 in 10kg units, rounded down to the next 10kg step.	Usage according to prEN ISO 14906. Example: a weight of 3'530 kg is coded as 0000 0001 0110 0001'B.	2			
22 / VehicleSpecific Characteristics VehicleSpecific Characteristics	Further vehicle characteristics. Each enumerated value has a specific meaning assigned. The meaning of some values are defined in this standard, others are reserved for future needs. / Assignment of meaning to the unassigned enumerated values is subject to registration according to the registration procedure specified in EN 12834.	Usage according to prEN ISO 14906. <ul style="list-style-type: none"> Euro type (4 bits). As defined in EC directive 88/77/EEC annex 1, and in 91/542/EEC <ul style="list-style-type: none"> 0000'B = no entry 0001'B = euro 1 0010'B = euro 2 0011'B = euro 3 Cop type (4 bits) : 0000'B = no entry Engine characteristics (8 bits) : <ul style="list-style-type: none"> 0000 0000'B = no entry 0000 0001'B = no engine 0000 0010'B = petrol unleaded 0000 0011'B = petrol Leaded 0000 0100'B = diesel 0000 0101'B = LPG 0000 0110'B = battery 0000 0111'B = solar reservedForFutureCENUse (8-255) Descriptive characteristics (8 bits) : as defined in prENV/278/8/1/5 <ul style="list-style-type: none"> 0000 0000'B = no entry 0000 0001'B = vehicle shape 1. Etc. FutureCharacteristicsType (8 bits) : 0000 0000'B = no entry 	4	O	R	Issuer

Attribute Id / Name Data element	Definition & remarks according to prEN ISO 14906	CARDME usage	Length in octets	M/O	Access conditions	Responsible
26 / EquipmentStatus EquipmentStatus	Operator-specific EFC application-related information pertaining to the status of the equipment. Boolean information to support an operator's handling of an OBU on application level. (E.g. 'next suitably equipped gantry should take an enforcement picture')	LLLL CCCC CCCC CCCC, where <ul style="list-style-type: none"> LLLL'B : Local use (4 bits), coding and use at the discretion of the operator; CCCC CCCC CCCC'B : sequential transaction counter (12 bits). 	2	M	R/W	Operator
33 / ReceiptData1	Latest receipt.		28	M	R/W	Operator
SessionTime	Date and Time of session with a two-seconds resolution. Time Easy to decode into a displayable format by OBE. Date and time value assignment – Octet Aligned[01.01.1990, 00:00:00]... [31.12.2116, 21:59:58], then rollover.	Usage according to prEN ISO 14906 : <i>Example : 1st of March 2003, 21:12:10 is encoded as</i> year (1997..2117); 0110'B month (0..12); 0011'B date (0..31); 0001'B hours (0..23); 10101'B minutes (0..59); 001100'B double-secs, 2 s resolution (0..30); 00101'B	4			
SessionService Provider	Operator that provides the service of the session. Provider Identifier of an operator.	See ContractProvider in the EFC-ContextMark	3			
StationLocation	Service provider specific coding of the station location. Toll plaza code defined by country organisation.	Usage according to prEN ISO 14906.	2			
SessionLocation	INT1 Travel direction + Lane Code0/1 + 0..127	Usage according to prEN ISO 14906.	1			
TypeOfSession	Designates the type of service station.	Usage according to prEN ISO 14906.	1			
SessionResult	Code designating whether a session has been completed successfully or not.	Usage according to prEN ISO 14906.	1			
SessionTariffClass	Service provider specific tariff class applied in the session. Enables to reproduce the price calculation (e.g. claimed or measured vehicle class that was applied.)	Usage according to prEN ISO 14906.	1			
SessionClaimedClass	Service provider specific vehicle class derived from claimed characteristics in the data group Vehicle. Claimed class and applied class (tariff class) may differ.	See Vehicle Class.	1			
SessionFee	The amount paid for the service. Contains a currency designation plus a multiplier.	0 .. 999.999,99 €	4			
SessionContract Provider	Organisation that provides the contract (Issuer).	See ContractProvider in the EFC-ContextMark	3			

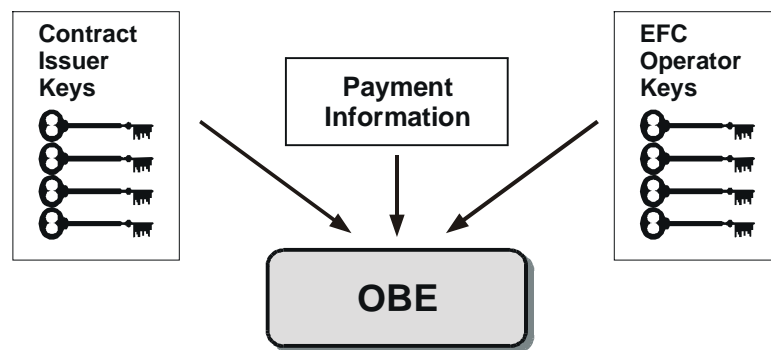
SessionTypeOf Contract	ContractProvider-specific designation of the rules that apply to the Contract.	See TypeOfContract in the EFC-ContextMark	2			
SessionContext Version	It identifies the version of the transaction model used for formatting the data.	See ContextVersion in the EFC-ContextMark	1			
Receipt Authenticator	Authenticator over all the Attributes of the data group Receipt, calculated by the SessionServiceProvider.		4			
34 / ReceiptData2	Penultimate receipt.	See ReceiptData1.	24	M	R/W	Operator
AC_CR	Access credentials calculated by the RSE and the OBE using RndOBE and the Access Key AC_CRKey.	Integer (0..4'294'967'295). (4 octets)	4	M	R/W	
AC_CR- KeyReference	Reference to the key generation and the Diversifier for the computation of AC_CRKey.	<ul style="list-style-type: none"> • Key reference (k): Integer (0..255) (8 bits) • Diversifier: Integer (0..255). (8 bits) Example : Key reference (# 1) and Diversifier # 2 : <ul style="list-style-type: none"> • 0000 0001'B (Key reference (1)): • 0000 0010'B (Diversifier(2)). 	2	M	R/W	
RndOBE	Random number (nonce) used together with AC_CR-KeyRef to calculate the access credential (AC_CR).	Integer (0..4'294'967'295). (4 octets)	4	M	R/W	
RndRSE	Random number, containing SessionTime, from RSE used for the computation of Operator and Issuer Authenticator	See ReceiptData1.SessionTime above	4	M	R/W	
KeyRef_Op	Reference to AuKey_Op used for the computation of Operator Authenticator.	Integer (0..255). (1 octet)	1	M	R/W	
KeyRef_Iss	Reference to AuKey_Iss used for the computation of Issuer Authenticator.	Integer (0..255). (1 octet)	1	M	R/W	
Operator Authenticator	Operator Authenticator over PaymentMeans (including Personal Account Number) and RndRSE (containing SessionTime) calculated using AuKey_Op(h). Used by the Operator to check the validity of the user. See also Ch. 4.4.1.	OCTET STRING (SIZE(4))	4	M	R/W	
Issuer Authenticator	Issuer Authenticator over PaymentMeans (including Personal Account Number) and RndRSE (containing SessionTime) calculated using AuKey_Iss(i). Used by the Contract Issuer to check the validity of the claim. See also Ch. 4.4.1.	OCTET STRING (SIZE(4))	4	M	R/W	

4 SECURITY

4.1 INTRODUCTION

Whenever an OBE performs the CARDME EFC transaction it will calculate some security data (authenticators) used for authentication of the equipment and the information it is carrying and transmitting to the Roadside Equipment. The authenticators are calculated using an international banking standard for authentication of a message. Crucial input for the calculation is the payment information (Contract Issuer and Personal Account Number) and the security keys stored in the OBE at the time of OBE personalisation.

Two sets of security keys and, amongst others, the payment information are stored in the OBE during the personalisation of the OBE. It is a strong requirement that both the keys as well as the payment information are well protected in the OBE. The Contract Issuer keys are only known and used by the Contract Issuer. The EFC Operator keys are distributed (one by one) to all the EFC operators having signed the MoU and having implemented the authentication service.



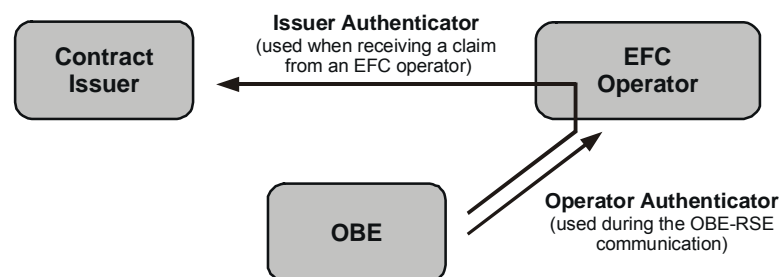
Security part of the OBE personalisation process

Two authenticators are calculated by the OBE:

- (EFC) Operator Authenticator (Auth_Operator) using the EFC Operator keys
- Issuer Authenticator (Auth_Issuer) using the Contract Issuer keys

The EFC Operators use the Auth_Operator at the time of OBE-RSE communication verifying whether the OBE is genuine and whether the payment information it has transmitted during the transaction is as stored by the Contract Issuer.

The Auth_Issuer is used by the Contract Issuer at a later stage verifying whether the OBE is an OBE personalised by Contract Issuer and whether the claim from an EFC Operator is a genuine one. The Auth_Issuer is sent to the Contract Issuer as part of the claim from the EFC operator to the Contract Issuer. The EFC operator can read the Auth_Issuer but he can not use it for verification as only the Contract Issuer has got the secret key used for the calculation of the Auth_Issuer.



The payment information authenticators

One of the measures to protect the payment information is the use of access control to OBE data. This implies that the OBE does not allow any RSE to read and write information in the OBE without having authenticated itself by so-called access credentials (access control 'password'). The CARDME transaction enables the use of such mechanisms but as default the mechanisms is not used. That means that as default any RSE is able to read the payment information as well as other data stored in the OBE, e.g. vehicle characteristics stored by the Contract Issuer or the last receipts stored by the last EFC operator(s). It is the Contract Issuer who initialises the OBE controlling the use of access control. However, the use of access control also means that the Contract Issuer has to distribute a secret key to all operators that are allowed to read the payment information and all the EFC operators have to implement the use of it. If not they will not be able to read the payment information and there will be no interoperability as for EFC.

The CARDME security also includes measures to protect the information written to the OBE during a transaction, i.e. the receipt. This enables for instance an EFC Operator verifying that an entry ticket in a closed EFC system has not been changed during the entry and exit point.

With respect to security, the CARDME concept specifies :

- the messages, data elements and associated cryptographic measures (Issuer and Operator Authenticators, Access Credentials) for the CARDME transaction in detail;
- how authenticators and access credentials are to be computed in OBU and RSE using the appropriate keys;
- key hierarchy and key derivation for the authenticator- and access keys;
- the (optional) transaction counter mechanism.

The CARDME concept does not include the following items, which are deemed to be closely related to the terms and conditions of the MoU:

- The implementation of the (optional) Receipt Authenticator;
- Procedural/practical key management issues;
- The exact role and responsibilities of the TTP, issuers and operators;
- Detailed contractual issues (MoU) concerning security.

4.2 SECURITY REQUIREMENTS

The CARDME security architecture is based upon the following guiding principles:

1. The CARDME security architecture shall enable an EFC Operator to verify whether the payment information sent by an OBE is genuine.
2. The CARDME security architecture shall enable a Contract Issuer to verify whether a claim from an EFC Operator is genuine. (Any claim verified as genuine is to be reimbursed by the Contract Issuer.)
3. The CARDME security architecture shall impose only a basic minimum of security provisions on the EFC Operator and provide optional features for enhancement.

In the CARDME concept a number of minimum security requirements apply to the Contract Issuer and the OBE. The most important requirements are listed below:

1. All Contract Issuers shall be registered in national registers as defined by EN ISO 14906 EFC - Application interface definition for DSRC.
2. The Contract Issuer and Personal Account Number data stored in the OBE shall be protected against unauthorised modification (e.g. by the use of a secure application module).
3. The OBE shall store the following types of keys:
 - OBE-specific authentication keys derived from Contract Issuer Masterkeys (MAuKey_Iss)
 - OBE-specific authentication keys derived from EFC Operator Masterkeys (MAuKey_Op)
4. The keys stored in the OBE shall be protected against disclosure and unauthorised modification.
5. The OBE shall store 4 generations of each type of OBE-specific keys.
6. The OBE shall support the computation of authenticators according to subsection 4.6 of this Annex.
7. The OBE shall support random number generation.
8. The OBE shall have a transaction counter as part of the EquipmentStatus. This transaction counter is initialised during the manufacturing and incremented by the RSE each time an EFC transaction is completed.

9. The OBE shall support one of the Access Control mechanisms as defined in 4.7.1: either the dynamic computation or the static AC_CR(0) shall be implemented.

In addition, a number of security requirements apply to EFC Operator and RSE. The most important ones are listed below:

1. All EFC Operators shall be of type Provider defined in Annex A in EN ISO 14906 EFC -Application interface definition for DSRC including a CountryCode and a ProviderIdentifier. The ProviderIdentifier should be registered on a national level in the same way as Contract Issuers avoiding ambiguity in claim identification.
2. In case authentication or access control keys are stored in the RSE, they shall be protected against disclosure and unauthorised modification.
3. In case the MoU partners agree to enable the security level with the dynamic Access Credentials (i.e. phase 3 according to the implementation scenario in Chapter 3.3.1 in Part 2), all RSE shall support computation of the AC_CR-Key according to 4.5.2 and computation of the AC_CR according to 4.7.2. This requires capabilities for TripleDES computation and random number generation.

4.3 CARDME SECURITY SERVICES AND MECHANISMS

The security services used in CARDME are the following:

- **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

4.3.1 Integrity

The most sensitive information – apart from the cryptographic keys - in the CARDME interoperable scheme is the information stored in the OBE related to the payment, i.e. the payment information consisting of the Contract Issuer data and the Personal Account Number data. A User may want to impersonate another User by using fake payment information. Hence, it is very important to protect the data that are stored in the OBE at the time of OBE personalisation as well as during the communication between the OBE and the RSE. This is done by the following mechanisms:

- Derivation of the OBE-specific secret keys from the Masterkeys and the payment information
- Calculation and verification of authenticators

The OBE-specific keys are stored in the OBE and are derived using the payment information, the MAuKey_Op and MAuKey_Iss as input. The OBE-specific keys used by the EFC Operators are also calculated by the RSE when it receives the payment information from the OBE using the relevant MasterKey stored in the RSE. Hence, any attempt of changing the payment information stored in the OBE, e.g. by trying to re-initialise the OBE writing new data for Contract Issuer and/or Personal Account Number, will result in the RSE deriving different OBE-specific keys than those stored in the OBE. This will again result in the RSE calculating a different authenticator than the OBE, the transaction will be stopped and the User will be treated as an exception, which may lead to enforcement. Assuming that the secret keys are securely protected by the OBE, e.g. by Secure Application Modules (SAM), the integrity service provides for the following:

The CARDME security architecture assures that the payment information, i.e. Contract Issuer data and the Personal Account Number data, is protected against unauthorised modification or deletion during storage in the OBE and transmission from the OBE to the RSE.

4.3.2 Authentication

The authentication service can be divided in Peer entity authentication and Data Origin authentication. The Peer entity authentication confirms that the identity of a peer entity in an association is as claimed, e.g. the identity of the OBE is genuine. The Data Origin authentication confirms that the identity of a source of data received is as claimed, e.g. the payment information sent from the OBE is the data that were stored by the Contract Issuer or the agent acting on behalf of him.

The objective of Peer authentication is to prove that a peer entity in an association is a genuine one. The main threat as for EFC is false OBEs. In CARDME the origin of the payment information is authenticated. Hence, the threat of having false OBEs with genuine data is minimal because a false OBE does not cause any loss to the EFC Operator or the Contract Issuer. To be accepted in an EFC system the OBE has to carry genuine information and an EFC Operator may always check this. There may also be false OBEs carrying genuine information but this is very unlikely unless some users are very interested in building their own OBE. However, under certain assumptions the CARDME also provides a kind of Peer entity authentication:

The CARDME security services provides an authentication of the OBE in those cases where the secret keys are protected by a SAM and where any attempt of removing the SAM from an OBE will be detected and the keys destroyed. Under such circumstances only genuine OBEs will send a correct Auth_Issuer and Auth_Operator. The secret keys are derived from the payment information and any attempt of splitting the payment information from the secret keys will cause incorrect authenticators. Hence, an OBE carrying the correct keys and sending correct authenticators has to be genuine.

Concerning the Data origin authentication the main threat will be that the Payment Information is coming from a false Contract Issuer and that the claim from a EFC Operator will not have a genuine Contract Issuer to be sent to. Hence, this represents a loss for the EFC Operator and a gain for the User having incorrect data in his OBE. The security mechanism used as countermeasure for such threats is the authenticators.

The CARDME security services provide Data Origin authentication of the Payment information sent by an OBE. Assuming that the MAuKey_Op is kept secret and protected and always only in the possession of the EFC Operators and Contract Issuers, only Contract Issuers with access to the MAuKey_Op will be able to initialise an OBE with payment information that together with the OBE-specific keys will present a Auth_Operator that will be accepted by the RSE of an EFC Operator.

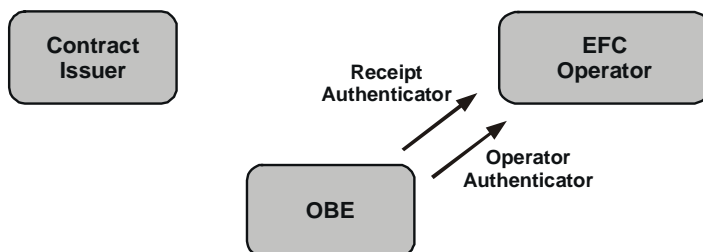
Another threat is that a Contract Issuer receives a claim from a false EFC Operator. It is assumed that this type of threats is met by secure communication between EFC Operators and Contract Issuers. A false EFC Operator will first of all not be in the list of accepted EFC Operators and secondly he will not have the secret keys used for the secure communication between the EFC Operators and the Contract Issuer. The (secure) communication between EFC Operators and Contractor Issuers is outside the scope of CARDME.

A third threat is that a claim from a true EFC Operator is not genuine, e.g. the EFC Operator has made his own transactions with the payment information read from different OBEs. The Data origin authentication service assures by means of the Auth_Operator that such threats are met:

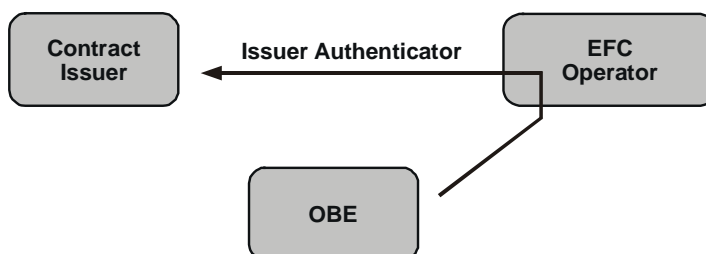
The CARDME security services provide a Data Origin authentication of the claim sent by an EFC Operator. Assuming that the MAuKey_Iss is kept secret and protected and always only in the possession of the Contract Issuer, only OBEs carrying the OBE-specific key derived from MAuKey_Iss will be able to generate a transaction record with a Auth_Issuer that will be accepted by the Contract Issuer. The EFC Operator has not access to the MAuKey_Iss and will not be able to generate a genuine Auth_Issuer.

Authentication is also used meeting the threat of a user denying having used a transport service. By using the Transaction Counter in the calculation of the Auth_Issuer the Contract Issuer will receive a claim including a Auth_Issuer that is calculated by using the unique OBE-specific keys, the unique Payment information and the TransactionCounter. The location of the use of the transport service is not included in the Auth_Issuer but the User can not deny that only his OBE is able to calculate the Auth_Issuer included in the claim from the EFC Operator.

Finally, authentication is used to protect the data in the receipt by means of Data Origin authentication. When a receipt is written to the OBE, e.g. an entry ticket in a closed system, the RSE writes a Receipt Authenticator to the OBE. The algorithm and secret key to be used is the choice of the EFC Operator writing the receipt. He can use his own algorithm and secret key or he can use an algorithm and secret key that are shared between some EFC Operators, e.g. toll collection companies operating a toll road network. The Receipt Authenticator provides the proof of the data origin as only EFC Operators with knowledge of the algorithm and access to the secret key can write a genuine receipt to the OBE.



Authentication at the charging point, e.g. a toll station



Authentication done by the Contract Issuer

4.3.3 Confidentiality

Providing protection against unauthorised disclosure of information is part of a security architecture. For the User it is important that all the EFC Operators providing a transport service do not know his identity. The CARDME scheme provides the required level of confidentiality and privacy via the way a transport service is paid for. An EFC Operator will collect the Payment information, which will consist of two numbers, the Contract Issuer ID and the Personal Account Number. The Contract Issuer ID will in most cases reveal the 'home' operator of the User but there will not be any other information enabling the EFC Operator to link the payment information to a certain User. The claim will be sent to the Contract Issuer who will reimburse a correct claim without revealing the identity of the User.

4.3.4 Access control

The CARDME security services and the CARDME transaction enables the use of Access Control of data stored on the OBE but as default this service is not used in the CARDME transaction.

CARDME has as a requirement that the level of security should be the matter of each EFC Operator within the MoU framework. The use of access control requires that all EFC Operators implement the use of this service. Otherwise they will not be able to read any Payment information from the OBE and there will be no interoperability between the EFC systems. This implies that all EFC Operators have to comply with the secret key management as for key handling, installation, protection etc and this has to be done by all EFC Operators from day one if the interoperability shall work. From a practical and strategically point of view this seems not feasible. The implementation of the security architecture should be flexible enough allowing a stepwise introduction from a level of almost no security services to the full level of services. The CARDME scheme can work from day one without the integrity and authentication services and the services can be put into operation and implemented when the EFC Operator sees the need for them.

4.4 KEY MANAGEMENT

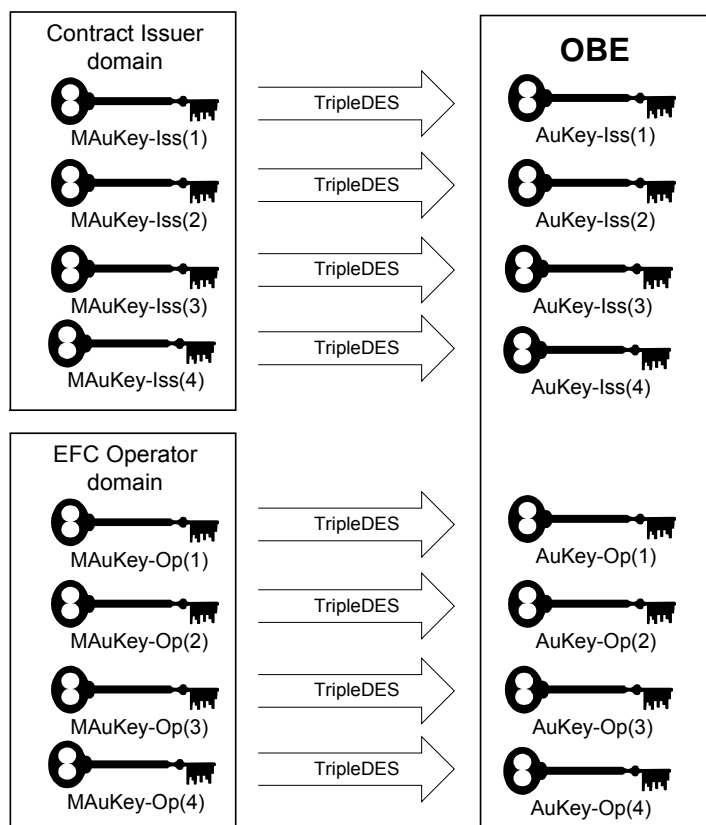
4.4.1 Authentication keys

The CARDME security architecture is based on the following secret key hierarchy:

- Each Contract Issuer has a set of Masterkeys called MAuKey_Iss_(i) where (i) denotes the generation 1-4.
- All EFC Operators share a set of Masterkeys called MAuKey_Op_(h) where (h) denotes the generation 1-4.
- Each OBE has a set of OBE-specific keys called AuKey_Iss(i) where (i) denotes the generation 1 to 4. The AuKeys_Iss are derived from the MAuKey_Iss_(i) by Triple-DES.
- Each OBE has a set of OBE-specific keys called AuKey_Op(h) where (h) denotes the range 1 to 4. The AuKeys_Op are derived from the MAuKey_Op_(h) by Triple-DES.

This implies that each **OBE** has 4 secret keys known and used by the Contract Issuer and 4 secret keys known and used by all EFC Operators. However, only one MAuKey_Op_(h) is distributed and used at the time by the operators. This reduces the risk of revealing the secret keys.

Authentication keys

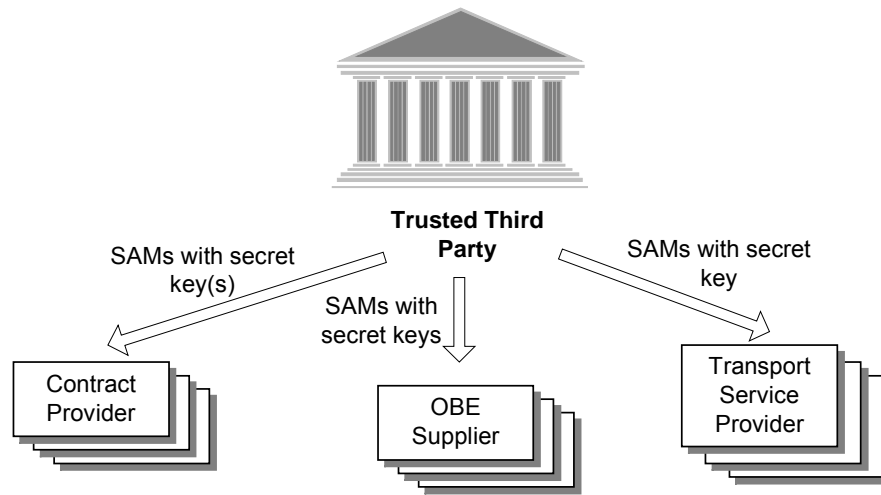


The Contract Issuers keep their keys within their own domains enabling them to protect and use their own secret keys although the common EFC Operator keys should be broken and revealed.

One of several possible solutions for key management is shown in the figure below. A Trusted Third Party (TTP) is responsible for the key management which covers the administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with the CARDME security policy. It is assumed that the MoU also includes the CARDME security policy.

The secret keys are distributed from the TTP whenever requested by the Contract Issuers, the EFC Operators and the OBE suppliers according to the MoU. One of the main ideas behind the scheme proposed below is that as few secret keys as possible are outside the domain of TTP. For instance could only one generation of the MAuKey_Iss be implemented in the central system of a Contract Issuer as well as only one generation of the common MAuKey_Op to be implemented in the RSEs of the EFC Operators. The distribution and installation of the derived OBE-specific keys in the OBE should also be done in a very secure and restricted way.

The detailed specification for the security key management is outside the scope of this document.



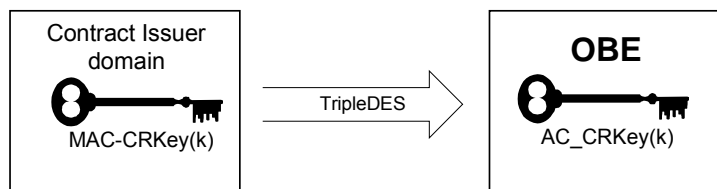
A possible scheme for key management

4.4.2 Access keys

The Issuers and the EFC operators will decide whether the use of Access Credentials is to be enabled and how the implementation costs should be shared between the Issuers and EFC operators. If the Issuers and the EFC operators decide to use Access Credentials, then the Master Access Credential Key is to be distributed by the TTP to all Issuers (for OBE personalisation) and EFC Operators (for access to the protected OBU data).

The secret key for access control ($AC_CRKey(k)$ where k denotes the key reference) is derived from the Master Access Credential key, $MAC_CRKey(k)$, generated and kept by the Issuer.

The $AC_CRMasteKeyRef(k)$ and an $AC_CR-Diversifier$ is used for diversification of the key to avoid that the same AC_CRKey is stored in all OBEs. The $AC_CR-Diversifier$ is the choice of the Issuer and could for instance be a serial number or certain combinations of parts of the PersonalAccountNumber.



In case of no deployment of dynamic Access Credentials, then $AC_CR-MasteKeyRef(k) = 0$ and $MAC_CRKey = 0$ and AC_CR is fixed to '04 94 F8 97' for $k=0$ (corresponding to $AC_CR-Diversifier = 0$ and $RndOBE = 0$. See also Chapter 4.7.1 in the Annex). This fixed value is used in the initial phases of the security level implementation (see Chapter 3.3.1 in Part 2).

4.5 KEY GENERATION

4.5.1 Masterkeys

The following requirements should be fulfilled concerning secret key generation:

- [Reqm 1] The MasterKey shall be randomly or pseudo-randomly generated.
- [Reqm 2] The mechanism used to generate masterkeys shall be such that knowledge of one key shall not enable the disclosure any other key.
- [Reqm 3] Each generation of keys shall be generated independently from the other generations of keys (meaning that knowledge of the keys corresponding to one generation shall not enable the disclosure of the keys of another generation).
- [Reqm 4] During the generation of the master keys used to derive the keys stored in the OBUs, a check for weak keys shall be performed in order to prevent their use.
- [Reqm 5] The MasterKeys shall be protected from unauthorised parties throughout its active life.

4.5.2 OBE-specific keys

The OBE-specific keys are derived from the Master keys by TripleDES. The **ede[Key] (VAL) syntax** is used below for description of the TripleDES operations, where

- 'ede' denotes encryption, decryption and encryption according to the TripleDES algorithm;
- '[Key]' denotes the applied key;
- '(VAL)' denotes the input value to the TripleDES operations.

Contract Issuer keys

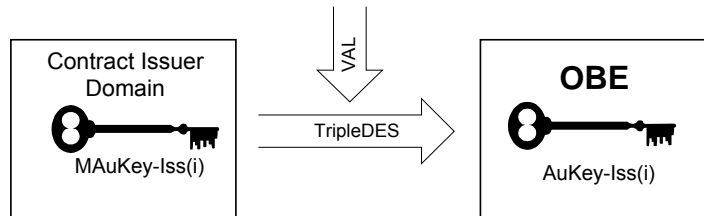
Use the following procedure to compute the AuKey_Iss(i) for a given generation (i):

1. Get the attribute Compact_PersonalAccountNumber by truncating the first 64 bits in the PaymentMeans attribute to 32 bits with the following algorithm:
 $Compact_PersonalAccountNumber = [HighDWord32(PAN)] XOR [LowDWord32(PAN)]$
2. Get the first 3 octets of EFC-ContextMark, i.e. the ContractProvider
3. Pad left the concatenation of Compact_PersonalAccountNumber || ContractProvider with '00' to obtain an 8 bytes value VAL:

$$VAL = 'Compact_PersonalAccountNumber || ContractProvider || 00'$$

4. Compute the AuKey_Iss(i) as follows:

$$AuKey_Iss(i) = ede[MAuKey_Iss(i)] (VAL)$$



EFC Operator keys

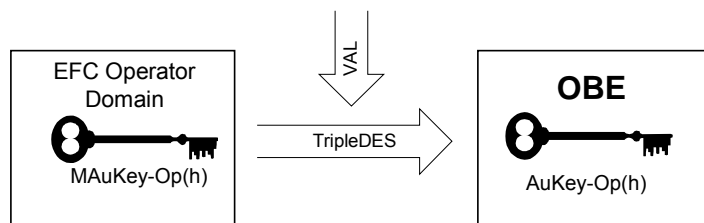
Use the following procedure to compute the key AuKey_Op(h) for a given generation (h):

1. Get the attribute Compact_PersonalAccountNumber by truncating the first 64 bits in the PaymentMeans attribute to 32 bits with the following algorithm:
 $Compact_PersonalAccountNumber = [HighDWord32(PAN)] XOR [LowDWord32(PAN)]$
2. Get the first 3 octets of EFC-ContextMark, i.e. the ContractProvider
3. Pad left the concatenation of Compact_PersonalAccountNumber || ContractProvider with '00' to obtain an 8 bytes value VAL:

$$VAL = 'Compact_PersonalAccountNumber || ContractProvider || 00'$$

4. Compute the AuKey_Op(h) as follows:

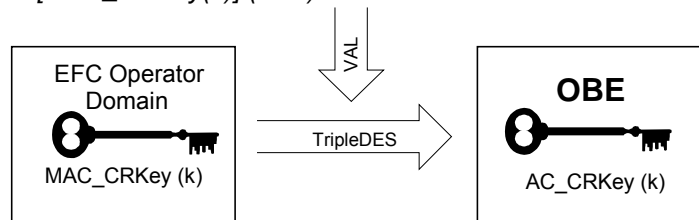
$$AuKey_Op(h) = ede[MAuKey_Op(h)] (VAL)$$



Access Credentials key

Use the following procedure to compute the AC_CRKey(k) for a given AC_CR-MasterKeyReference. (k):

1. Set AC_CR-Reference = 'AC_CR-MasterKeyRef || AC_CR-Diversifier' (2 octets)
2. Make the concatenation of AC_CR-Reference || AC_CR-Reference || AC_CR-Reference || AC_CR-Reference to obtain an 8 bytes value VAL:
 $VAL = 'AC_CR_Reference || AC_CR_Reference || AC_CR_Reference || AC_CR_Reference'$
3. Compute the AC_CRKey(k) as follows:
 $AC_CRKey(k) = edef[MAC_CRKey(k)] (VAL)$



For calculation of the AC_CRKey(0) to be used to calculate the fixed “password” in the initial phases of the security level implementations, the value MAC_AKey(0) = 0, AC_CR-MasterKeyRef. = 0 and AC_CR-Diversifier = 0 shall be used.

This will give the fixed value of the AC_CRKey(0) = '8C A6 4D E9 C1 B1 23 A7'

4.6 COMPUTATION OF AUTHENTICATORS

The computation of authenticators is done according to ISO 8731-1 Banking – Approved algorithms for message authentication – Part 1: DEA.

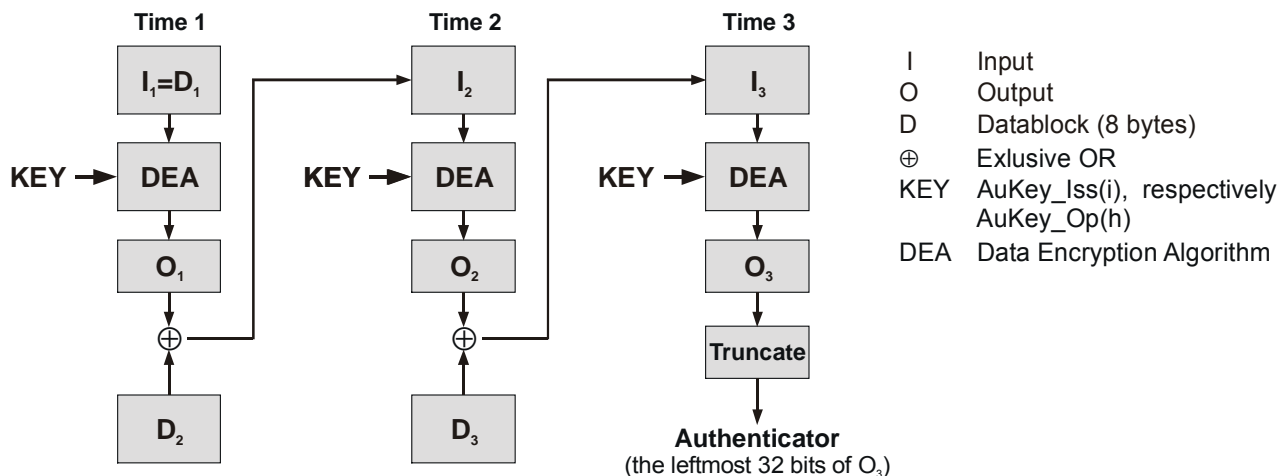
4.6.1 Issuer Authenticator (Auth_Iss)

Use the following procedure to compute the Issuer Authenticator (Auth_Iss) for a given key generation (i):

- Let M be the Attribute List in the GET_STAMPED response containing the single attribute PaymentMeans (including Personal Account Number), concatenated by the octet string containing the RndRSE sent by the RSE in the GET_STAMPED request. M will now have the following content:

Octet #	Attribute / Field	Bits in Octet		Description
		b ₇	b ₀	
1	AttributeList SEQUENCE (0..127,...) OF {	0000	0001	No extension, number of attributes: 1
2	Attributes SEQUENCE { Attributeld	0010	0000	PaymentMeans = 32 ₁₀
3	AttributeValue CONTAINER {	0100	0000	Container Choice: 64 ₁₀ = PaymentMeans
4	PaymentMeans	xxxx	xxxx	PaymentMeans
5		xxxx	xxxx	
6		xxxx	xxxx	
7		xxxx	xxxx	
7		xxxx	xxxx	
9		xxxx	xxxx	
10		xxxx	xxxx	
11		xxxx	xxxx	
12		xxxx	xxxx	
13		xxxx	xxxx	
14	PaymentMeansExpiryDate	0001	1110	DateCompact. Example : 2005-03-01
15	PaymentMeansUsageControl	0110	0001	Example : 1
16		0000	0000	
17	}	0000	0001	
18	Nonce OCTET STRING {	0000	0100	No extension, octet string length = 4 ₁₀
19	RndRSE	rrrr	rrrr	Random number from RSE, containing the SessionTime
20		rrrr	rrrr	
21		rrrr	rrrr	
22		rrrr	rrrr	
23	Padding	0000	0000	Padding to obtain even 8-octet blocks
24		0000	0000	

- Let D₁ be the first 8 bytes, D₂ be 9-16 bytes and let D₃ be the last 8 bytes of the message M
- Let Key in the figure below be the Aukey-Iss(i) where (i) is the KeyRef_Iss sent by the RSE
- Compute the Issuer Authenticator (Auth_Iss) according to the DES algorithm ISO 8731-1



4.6.2 Operator Authenticator (Auth_Op)

Use the following procedure to compute the Operator Authenticator (Auth_Op) for a given key generation (h):

- Let M be the Attribute List in the GET_STAMPED response containing the single attribute PaymentMeans (including Personal Account Number), concatenated by the octet string containing the RndRSE sent by the RSE in the GET_STAMPED request. M will now have the following content:

Octet #	Attribute / Field	Bits in Octet		Description
		b ₇	b ₀	
1	AttributeList SEQUENCE (0..127,...) OF {	0000	0001	No extension, number of attributes: 1
2	Attributes SEQUENCE { AttributeId	0010	0000	PaymentMeans = 32 ₁₀
3	AttributeValue CONTAINER {	0100	0000	Container Choice: 64 ₁₀ = PaymentMeans
4	PaymentMeans	xxxx	xxxx	PaymentMeans
5		xxxx	xxxx	
6		xxxx	xxxx	
7		xxxx	xxxx	
7		xxxx	xxxx	
9		xxxx	xxxx	
10		xxxx	xxxx	
11		xxxx	xxxx	
12		xxxx	xxxx	
13		xxxx	xxxx	
14	PaymentMeansExpiryDate	0001	1110	DateCompact. Example : 2005-03-01
15	PaymentMeansUsageControl	0110	0001	Example : 1
16	} Nonce OCTET STRING {	0000	0000	No extension, octet string length = 4 ₁₀
17		0000	0001	
18	RndRSE	ffff	ffff	Random number from RSE, containing the SessionTime
19		ffff	ffff	
20		ffff	ffff	
21		ffff	ffff	
22	}	ffff	ffff	
23	Padding	0000	0000	Padding to obtain even 8-octet blocks
24		0000	0000	

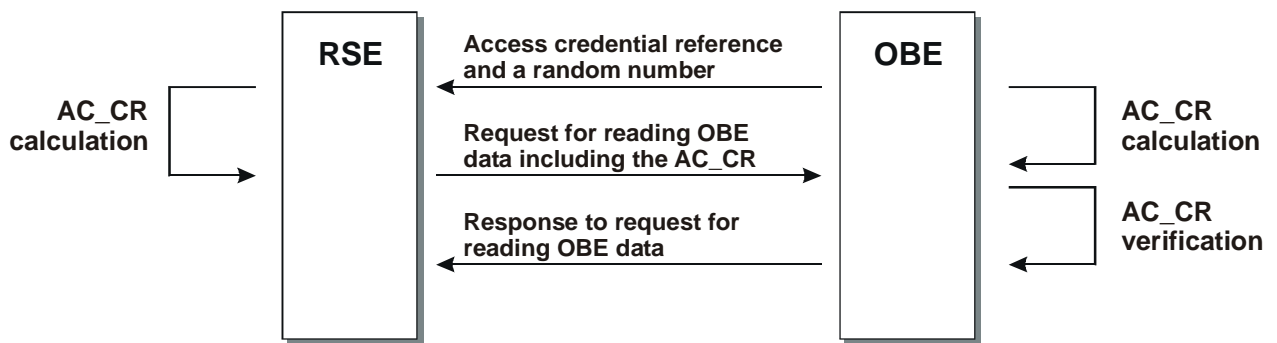
- Let D₁ be the first 8 bytes, D₂ be 9-16 bytes and let D₃ be the last 8 bytes of the message M
- Let Key in the figure in 4.6.1 be the Aukey-Op(h) where (h) is the KeyRef_Op sent by the RSE
- Compute the Operator Authenticator (Auth_Op) according to the DES algorithm ISO 8731-1

4.6.3 Receipt Authenticator

The use of the Receipt Authenticator is the choice of each operator and is outside the scope of the CARDME EFC specification.

4.7 ACCESS CREDENTIALS

The principle of access control to the payment information is shown below. When an OBE, having entered the communication zone, responds to a polling message (BST) from the RSE, it returns a VST that for each available Contract contains information about an Access Credential Reference (AC_CR-Reference) and a random number (RndOBE). The AC_CR_Reference includes the data AC_CR-MasterKeyReference and AC_CR-Diversifier. The data are the diversifier and a reference to a secret key (MasterKey for Access Credentials) that shall be used for the computation of the secret key AC_CRKey. This key is used for the computation of the Access credential (AC_CR) using the RndOBE number as input. The RSE returns the access credential calculated and the OBE compares the access credential with its own calculation. In case they are equal the OBE accepts the RSE as a genuine RSE and reading data from the OBE is allowed.

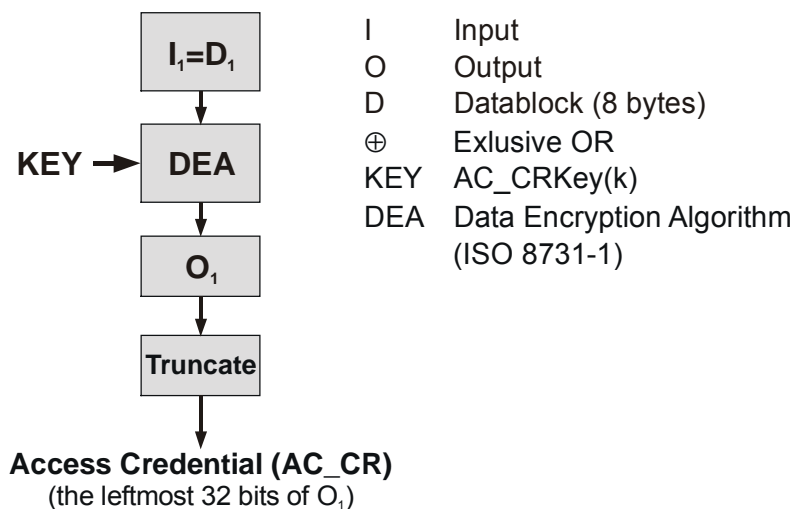


The principle of access control to the OBE data

4.7.1 OBE computation of AC_CR

Use the following procedure for the **OBE** computation of the AC_CR for a given key reference (k):

1. Get the RndOBE
2. Make the concatenation of 'RndOBE || 00 00 00 00' to obtain an 8 bytes value VAL:
 $VAL = 'RndOBE || 00\ 00\ 00\ 00'$
3. Let VAL be D_1
4. Compute the $AC_CR(k)$ according to the DES algorithm ISO 8731-1:



OBE and RSE computation of Access Credentials

For the first version of CARDME (see also Chapter 3.3.1 in Part 2), i.e. $k = 0$, the OBE shall use the following procedure for the AC_CR calculation with the key reference (0):

1. Let RndOBE = '00 00 00 00'.
2. Make the concatenation of 'RndOBE || 00 00 00 00' to obtain an 8 bytes value $VAL = \text{'RndOBE || 00 00 00 00'}$
3. Let VAL be D_1
4. Let AC_CRKey(0) be '8C A6 4D E9 C1 B1 23 A7'
5. Compute the AC_CR(0) according to the DES algorithm ISO 8731-1

Or

1. Let AC_CR(0) be '04 94 F8 97'

Note that for $k=0$, RndOBE may be different from '00 00 00 00' but AC_CR shall invariably equal '04 94 F8 97'. This means that the RSE, for $k=0$, shall not make use of the RndOBE.

The values selected for $k = 0$ enable EFC operators who have not implemented TripleDES functionality and/or facilities for storage and protection of the MasterKey for AC_CR calculation to just send a predefined value for AC_CR enabling them to read the data carried by the OBE.

4.7.2 RSE computation of AC_CR

Use the following procedure for the **RSE** computation of the AC_CR for a given key reference (k):

1. Set $k = \text{AC_CR-MasterkeyReference}$ (sent by the OBE in VST)
2. Get the MAC_CRKey(k) (stored in the RSE)
3. Get the AC_CR-Reference (2 octets sent by the OBE in VST)
4. Make the concatenation of AC_CR-Reference || AC_CR-Reference || AC_CR-Reference || AC_CR-Reference to obtain an 8 bytes value VAL1:

$$VAL1 = \text{'AC_CR-Reference || AC_CR-Reference || AC_CR-Reference || AC_CR-Reference'}$$
5. Compute the AC_CRKey(k) as follows:

$$AC_CRKey(k) = \text{ede}[\text{MAC_CRKey}(k)](VAL1)$$
6. Get the RndOBE sent by the OBE in VST
7. Make the concatenation of 'RndOBE || 00 00 00 00' to obtain an 8 bytes value $VAL2 = \text{'RndOBE || 00 00 00 00'}$
8. Let VAL2 be D_1
9. Compute the AC_CR(k) according to the DES algorithm ISO 8731-1

For the first version of CARDME, i.e. $k = 0$, the AC_CR (0) shall be '04 94 F8 97'.

4.8 TRANSACTION COUNTER

Use the following procedure for the **RSE** computation of the Transaction Counter:

1. Get the EFC attribute EquipmentStatus (sent by the OBE in the Presentation Phase)
2. Let the Transaction Counter be the value of the last 12 bits in EquipmentStatus (0...4095)
3. Increase the Transaction Counter by 1
4. Insert the changed Transaction Counter into the last 12 bits of EquipmentStatus

The updated EquipmentStatus is sent to the OBE in the Receipt Phase (SET.Request).

4.9 IMPLEMENTATION EXAMPLES

This paragraph illustrates the cryptographic mechanisms defined in chapters 4.5 to 4.7 by means of a few numerical examples. Numeric values in the examples below are in hexadecimal.

4.9.1 Key derivation – Authenticator Keys

In this example we use the following application data and Master Key values:

PaymentMeans:

- PersonalAccountNumber, PAN: '52 75 12 34 56 78 90 12 FF FF' (16 characters PAN, padding with '1' bits)
- PaymentMeansExpiryDate: '21 21' (2006-09-01)
- PaymentMeansUsageControl: '00 00'

ContractProvider: 'A4 00 01' (Sweden (SE), Issuer #1 (Öresundskonsortiet))

MAuKey_Iss : '13 13 13 13 13 13 13 13 AB AB AB AB AB AB AB';

MAuKey_Op : '34 34 34 34 34 34 34 34 CD CD CD CD CD CD CD CD';

The CompactPAN is calculated as:

CompactPAN = Sub(PAN, 0, 4) xor Sub(PAN, 4, 4) = '04 0D 82 26'

{Sub(PAN,0,4) = HighDWord32(PAN), Sub(PAN, 4,4) is LowDWord32(PAN)}

The input data (VAL) follow from:

VAL = 'CompactPAN || ContractProvider || 00' = '04 0D 82 26 A4 00 01 00'

With ISO 8731-1 defining the Initial Chaining Value ICV:

ICV : '00 00 00 00 00 00 00 00',

this gives the following value for the Issuer Authenticator Key:

AuKey_Iss = ede[MAuKey_Iss](VAL) = '26 BF 3D F3 BC E3 65 6B'

where the formula above denotes the Triple-DES operation using MAUKey_Iss over the data string VAL.

Similarly the value for the EFC Operator key can be calculated:

AuKey_Op = ede[MAuKey_Op](VAL) = '19 11 91 F2 F8 97 42 53'.

With a different value for the PAN the derived key will be different. As an example, with a PAN = '58 61 12 34 56 78 90 12 FF FF', and the same Contract Provider and Master Keys as above we find the following derived keys:

AuKey_Iss = 'A7 AD C3 82 44 1C 1D 00'

AuKey_Op = '4A C2 F9 50 A2 49 02 D9'.

4.9.2 Key derivation – Access Credentials key

The derivation of the Access Credentials key is quite similar to the derivation of the Authenticators keys. Instead of the PAN the AC_CR-Reference (consisting of the AC_CR-MasterKeyRef. and AC_CR-Diversifier) is used.

We use the following application data values and Master Key:

AC_CR-Reference:

- AC_CR-MasterKeyRef.: '12'
- AC_CR-Diversifier: '34'

MAC_CRKey : '57 57 57 57 57 57 57 57 EF EF EF EF EF EF EF EF'

This gives:

VAL = 'AC_CR-Reference || AC_CR-Reference || AC_CR-Reference || AC_CR-Reference' = '12 34 12 34 12 34 12 34'

And:

AC_CRKey = ede[MAC_CRKey](VAL) = '9B 48 AA E0 7A 7B C0 08'

Again, a different AC_CR-Reference or Master Key will produce a completely different Access Credentials Key.

4.9.3 Computation of authenticators

The computation of authenticators is performed according to the standard ISO 8731-1.

We use the following values:

PaymentMeans = '52 75 12 34 56 78 90 12 FF FF 21 21 00 00'

RndRSE: '1A 61 A9 85' (1th of March 2003, 21:12:10)

AuKey_Iss = '26 BF 3D F3 BC E3 65 6B'

AuKey_Op = '19 11 91 F2 F8 97 42 53'

The message M (the input data) is then equal to:

M = 'AttributeList (including PaymentMeans) || RndRSE (octet string) || Padding' = '01 20 40 52 75 12 34 56 78 90 12 FF FF 21 21 00 00 04 1A 61 A9 85 00 00'

and

$D_1 = I_1 = \text{Sub}(M, 0, 8) = '01 20 40 52 75 12 34 56'$

$D_2 = \text{Sub}(M, 8, 8) = '78 90 12 FF FF 21 21 00'$

$D_3 = \text{Sub}(M, 16, 8) = '00 04 1A 61 A9 85 00 00'$

With ICV : '00 00 00 00 00 00 00 00': the Input $I_1 = \text{ICV} \text{ xor } D_1 = '01 20 40 52 75 12 34 56'$

$O_1 = e[\text{AuKey_Iss}](I_1) = '45 1F F4 A9 72 9B CE 58'$

and

$I_2 = O_1 \text{ xor } D_2 = '45 1F F4 A9 72 9B CE 58' \text{ xor } '78 90 12 FF FF 21 21 00' = '3D 8F E6 56 8D BA EF 58'$

Calculation of O_2 gives:

$O_2 = e[\text{AuKey_Iss}](I_2) = '4F BB E8 C6 4B 0B EF A5'$

and

$I_3 = O_2 \text{ xor } D_3 = '4F BB E8 C6 4B 0B EF A5' \text{ xor } '00 04 1A 61 A9 85 00 00' = '4F BF F2 A7 E2 8E EF A5'$

Calculation of O_3 gives:

$O_3 = e[\text{AuKey_Iss}](I_3) = 'BF 87 5F F0 90 AD BF E0'$

The leftmost 32 bits represent the Issuer Authenticator:

Auth_Iss = Sub(O_3 , 0, 4) = 'BF 87 5F F0'

In a similar way the Operator Authenticator is calculated. This leads to equal values for D_1 , D_2 , D_3 and I_1 . Hence,

$O_1 = e[\text{AuKey_Op}](I_1) = '5D 20 33 E4 DB 95 22 31'$,

$I_2 = O_1 \text{ xor } D_2 = '5D 20 33 E4 DB 95 22 31' \text{ xor } '78 90 12 FF FF 21 21 00' = '25 B0 21 1B 24 B4 03 31'$,

$O_2 = e[\text{AuKey_Op}](I_2) = '2D 62 88 F4 DB FD AC 82'$,

$I_3 = O_2 \text{ xor } D_3 = '2D 62 88 F4 DB FD AC 82' \text{ xor } '00 04 1A 61 A9 85 00 00' = '2D 66 92 95 72 78 AC 82'$,

$O_3 = e[\text{AuKey_Op}](I_3) = 'D3 FA D4 CD 97 B4 22 88'$ and

Auth_Op = Sub(O_3 , 0, 4) = 'D3 FA D4 CD'

A change in the input parameters will completely change the Authenticators. To illustrate this we calculate the Authenticator for a different value of RndRSE, without changing the values for the other parameters.

With:

RndRSE: '1A 61 A9 86' (1th of March 2003, 21:12:12)

we find:

Auth_Iss = '23 98 AA 8D' and

Auth_Op = '04 FE 63 DC'.

4.9.4 Computation of Access Credentials

We use the AC_CRKey = '9B 48 AA E0 7A 7B C0 08' derived above.

Assuming

RndOBE = '97 86 75 64'

gives

VAL = 'RndOBE || 00 00 00 00' = '97 86 75 64 00 00 00 00'.

Calculation gives:

$O_1 = e[AC_CRKey](VAL) = 'E0 55 EA 12 1F 5C 97 D7'$

and hence:

$AC_CR = Sub(O_1, 0, 4) = 'E0 55 EA 12'$

For the first version of CARDME (AC_CRMasterKeyRef.= k =0) a fixed AC_CR value is used (see also Chapter 4.7.1 in the Annex).

This value may also be calculated by first deriving the AC_CRKey from the MAC_CRKey and the AC_CR-Reference as shown below:

MAC_CRKey(0) = '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00' and

VAL = 'AC_CR-Reference || AC_CR-Reference || AC_CR-Reference || AC_CR-Reference' = '00 00 00 00 00 00 00 00'

this gives:

$AC_CRKey = ede[MAC_CRKey](VAL) = '8C A6 4D E9 C1 B1 23 A7'$

Then the Access Credentials can be calculated with RndOBE = '00 00 00 00' which gives:

VAL = 'RndOBE || 00 00 00 00' = '00 00 00 00 00 00 00 00' and

$O_1 = e[AC_CRKey](VAL) = '04 94 F8 97 08 87 1D 3F'$ and hence:

AC_CR(0) = '04 94 F8 97'

- - - END - - -