European Commission - DG INFSO
Telematics Application Programme
Transport Sector

Concerted **A**ction for **R**esearch on **D**emand **M**anagement in **E**urope

FINAL REPORT OF THE FOURTH PHASE OF THE

CARDME

CONCERTED ACTION

IST PROGRAMME

Thematic Networks
Contract IST-1999-29053

Coordinator - Orchidnote Limited

Editor - Brian Bourne

Version 1

February 2002

CONTRACT IST-1999-29503 CARDME-4

Since 1993 the CARDME concerted action has provided a forum at government level for the discussion of cross-border interoperability of motorway tolling systems. The project team has identified obstacles to interoperability and proposed solutions. A Steering Committee of national representatives chaired jointly by DG INFSO and DG TREN has reviewed and approved the work.

Background

In this fourth and final phase of the action the emphasis has been on further development of the specification of a common payment service which was proposed in the previous phase of the project. In achieving this the CARDME team has worked closely with other projects in the field including DELTA and CESARE. Close cooperation with the working groups of CEN has also been possible as a result of common membership of all these groups.

Approach

Initial attempts at overcoming obstacles to interoperability between EFC systems were focussed on harmonising the different approaches. However, it was recognised that the different objectives of each system lead to different requirements. The approach adopted by the CARDME project is to accept that the different requirements and priorities of national and local systems will lead to different technical solutions. The project considers the minimum additional requirements for an interoperable payment service. The project has designed a transaction which meets these requirements.

Key features of the service

The proposed service can provide interoperable operation by the addition of a single interoperable application in addition to any applications which existing local operators may already provide. It is suitable for use in open or closed systems in mono-lane or multi-lane mode and for both passenger cars and HGVs.

In existing mono-lane systems it can provide a “stop and pay” capability with an IC card which may also be used with the on-board unit. In the case of systems using monolithic tags the card will replicate the contract and vehicle data held in the tag.

The DSRC transaction used has been developed in close cooperation with the CESARE project of ASECAP and both transactions are compliant with CEN standard prEN ISO 14906.

Significant differences between the CARDME and CESARE transactions are confined to two aspects.

[1] On the question of security features the ASECAP members have taken the view that the present method of operation which uses no cryptographic security will be able to continue even when extensive interoperability is available. CARDME, on the other hand takes the view that cryptographic security would be expensive and inappropriate at the present time but provision can be made in the OBUs at negligible cost. Thus operators who wish to introduce greater security on their own networks can do so at any time.

[2] ASECAP has retained the simple classification of vehicles based on dimensions. CARDME has made provision for possible Commission requirements for an extended set of characteristics taking account of such things as engine emissions.

Neither of these differences presents any serious obstacle to interoperability of the two transactions since the roadside equipment is able to recognise the type of system a vehicle is using as it approaches and can very simply switch between them.

Management of payments

Both CARDME and CESARE make use of a central account system normally with post payment. CARDME provides a mechanism for roaming in which the “foreign” operator can claim toll charges directly from the “home” operator. of operators. Alternatively claims can be made via a clearing system. The CESARE project has undertaken the design of an MoU to enable this mode of operation.

Other ways of paying

It was noted in earlier phases of the project that the existing stop and pay method of operation allows users to pay with credit cards. The use of a credit car over a DSRC link remains unacceptable to the issuers at least in the short term. With single lane toll systems users will usually have the option of stopping to pay manually but this will not be possible if multi-lane free-flow systems without any toll booths become the norm.

There is also pressure from those countries which put unusual emphasis on civil liberties for a system which will allow payment with electronic purses. This possibility has again been investigated but the obstacles noted above remain together with the fact that there are no international purses available at present.

Contract details

Project Name: CARDME-4
Research Area: Transport Telematics
Timescale: 2000-2001
Overall cost €360,626
EC contribution €282,169

Key Words: Tolling, Interoperability, electronic fee collection, standardisation.

Key Project Participants:-

Orchidnote Ltd [Coordinator]	[GB]
Lisitt	[E]
Transport Research Laboratory	[GB]
ISIS	[F]
Rapp Ingenieure+Planer	[CH]
Statcraft Grøner A/S	[N]
TCL	[D]
Intercai	[NL]

Project Coordinator Brian Bourne
Fax: +44 1428 717 012
E-mail: CARDME@btinternet.com

CONTENTS

1 INTRODUCTION

1.1 The CARDME project

The CARDME project was initiated in 1993 and has consisted of four phases. Initial attempts at overcoming obstacles to interoperability between EFC systems were focussed on harmonising the different approaches. However, it was recognised early on in the project that the different objectives of each system lead to different requirements. The approach which has been taken is to accept that the different requirements and priority of those requirements for local systems will lead to different technical solutions. The approach adopted has been to consider the minimum additional requirements for an interoperable payment service. This has resulted in a specification for a common interoperable payment service which can be offered alongside existing EFC systems.

The project has defined a single new EFC application which can be added to existing systems or can provide the basis for new systems. The intention is that each system would be enlarged to accommodate the common system without affecting the functionality of the local systems.

A detailed design of a transaction for use in DSRC systems has been completed and is specified down to bit-level. The system as proposed uses a central account. The use of electronic purses has been suggested but their use in interoperable tolling systems is not currently feasible.

The possibility of payment by means of a cellular device has been investigated and may be feasible in the medium term although motorway operators do not generally favour arrangements whereby the collection of money lies in the hands of a communications company.

1.2 Scope of the report

This report presents a condensed version of the results of the final phase of the CARDME project. It includes a review of developments in technology for payment of toll charges and describes the CARDME concept for a common interoperable payment service.

Full details of the recent work are presented in two deliverables which are freely available:

Deliverable 4.1 issue 2 December 2001 – The CARDME concept

Deliverable 4.3 issue 1 December 2001 - Technology developments

Extracts from these deliverables are included in this report.

Note that there is no Deliverable 4.2. This is the project web site **www.cardme.org**

1.3 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 prEN ISO 14906 will present a powerful force in favour of universal adoption of interoperable systems.

1.4 CARDME OBJECTIVES

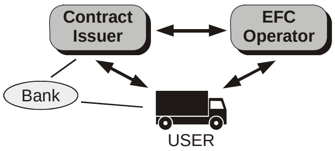
CARDME has two objectives:

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.

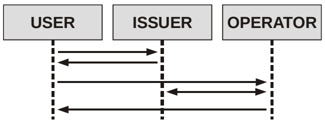
In addition, the CARDME service is defined in such a way that it may also serve as a template for concessions or countries that newly introduce an EFC service. The CARDME-Concept can be used to introduce EFC services that are designed for interoperability from the very beginning and enjoy maximum industry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

The definition of the CARDME service comprises

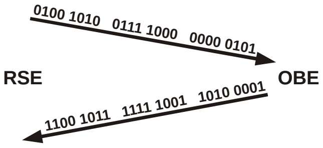
– the ***system architecture***, describing the basic model of the CARDME Concept, the involved parties, their roles and their relationships.



– 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.



1.5 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

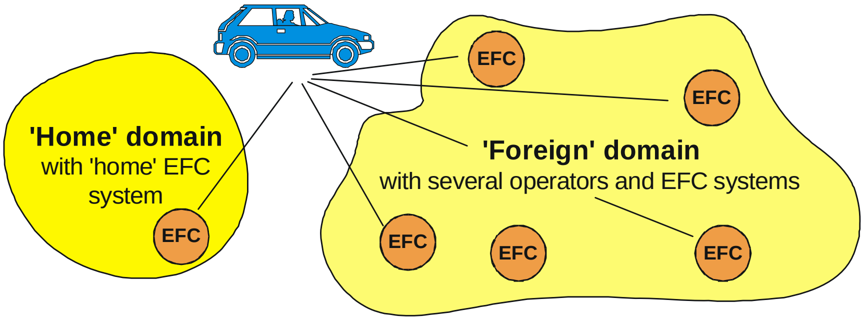
The CARDME Concept is based upon

- 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

2. 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.



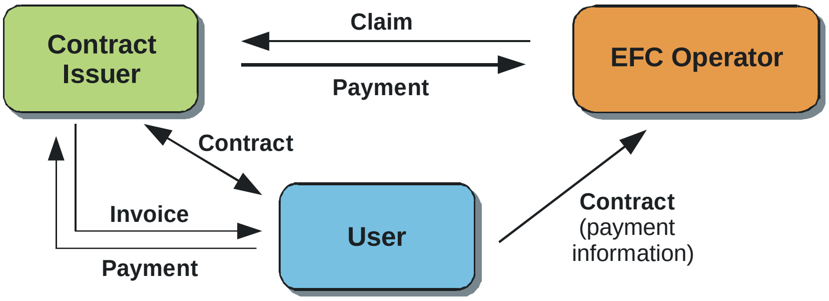
The CARDME domains

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

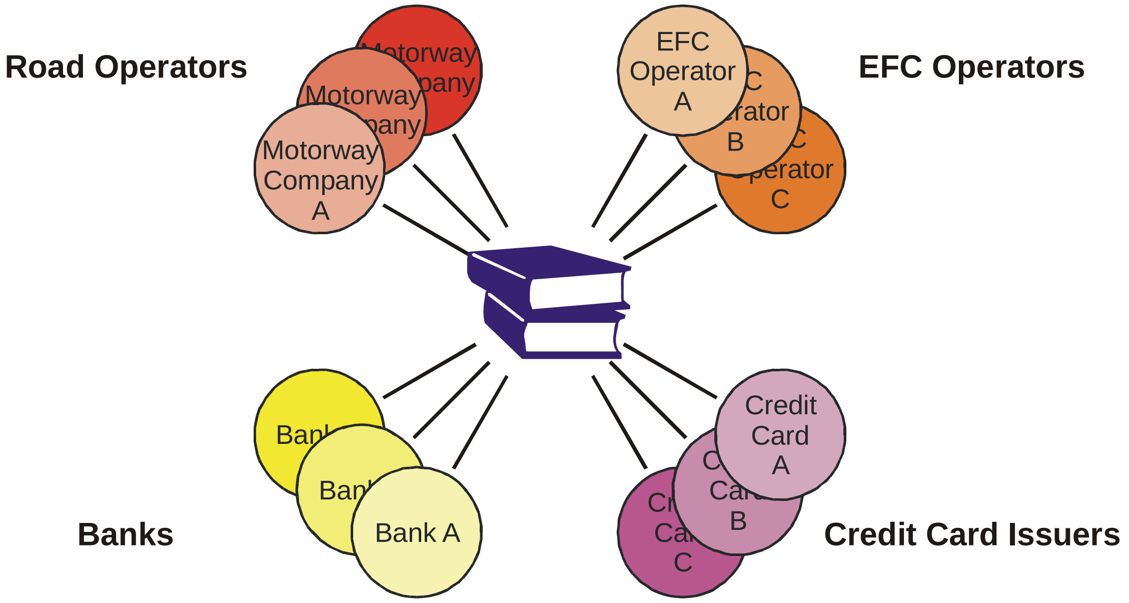
CARDME does not influence the ‘home’ systems, which can be EFC systems with totally different constraints and requirements. CARDME is an additional service co-existing with the ‘home’ EFC service. However, the claims from the foreign EFC systems will be merged with the claims from the home system. The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

3. 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-initialised ‘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.

3.1 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 DSRC communication 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.



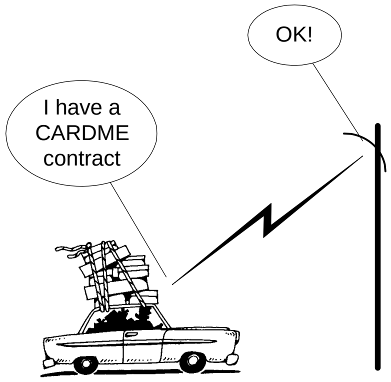
The MoU Partners

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.

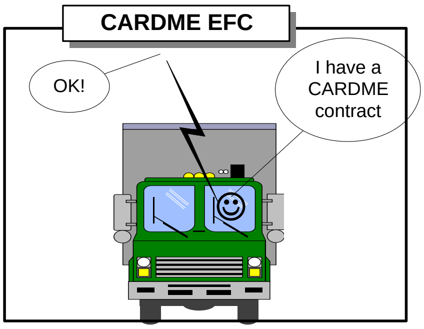
He has heard about the new CARDME interoperable EFC service and decides to call the operator of his local system for Liverpool Road User Charges, LRUC, in order to investigate how to benefit from this new service.

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 initialised 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.

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 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 petrol 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 initialisation 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.

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-initialised 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.

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.

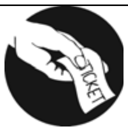
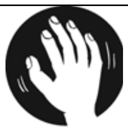
Mrs. Dulac looks down on the toll plaza to see a family going on holiday passing through the EFC lane. From the licence plate she can see it is a car from the UK. ‘Have a nice trip’, she thinks, ‘we will send a claim to your Contract Issuer’.

4 How is it done – CARDME Transaction

4.1 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.

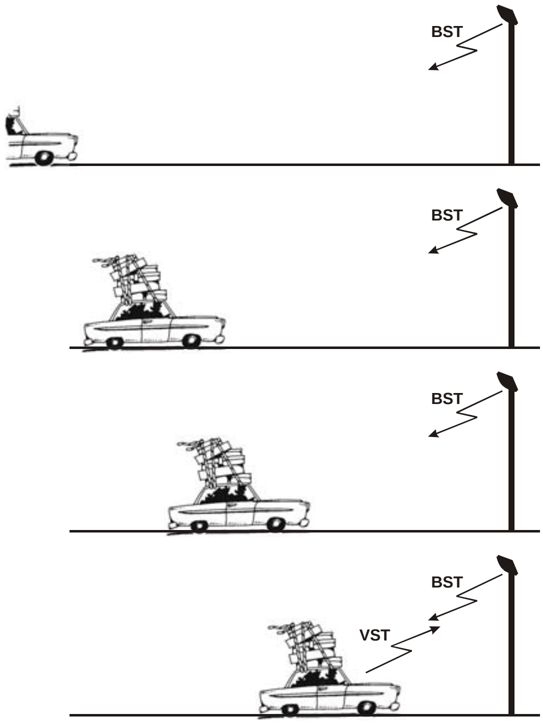
Phase 1. Say Hello - Initialisation

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: *'Hello, here is an EFC Station'*	
BST: *'Hello, here is an EFC Station'*	
BST: *'Hello, here is an EFC Station'*	(A vehicle is approaching. OBE wakes up and replies)
	VST: *'Hello, I can offer the following EFC contracts and transactions:'* *1. Transaction type 'AUTOPASS'* *Central account with the Operator 'NorwegTrans'* 2. *Transaction type 'CARDME'* *Central account with the Operator 'NorwegTrans'* 3. *Transaction type 'SPECIAL/LOCAL'* *Yearly pass from the Operator 'CityParking'*
The roadside thinking: According to my tables, I have the following transaction available and recognise the accounts with the following operators: *Transaction* *Operator* TIS transaction AREA COFIROUTE ESCOTA SANEF .... CARDME transaction AustroToll BelgiaPay NorwegTrans PagaMadrid .... 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'	

Phase 2 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

'Please give me the following information about your CARDME contract with NorwegTrans: - your personal account number (with signature) - your previous receipts - your vehicle classification details '	
	'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* - 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:

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 calculate 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 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 road-side 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.

Phase 3. 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
'Please store the following information in your memory: - transaction receipt (entry ticket) *Inform the user about the success of the transaction'*	
	'I confirm. *I have stored the ticket and I have given the user a signal'.*

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 will be capable 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.

Phase 4 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.

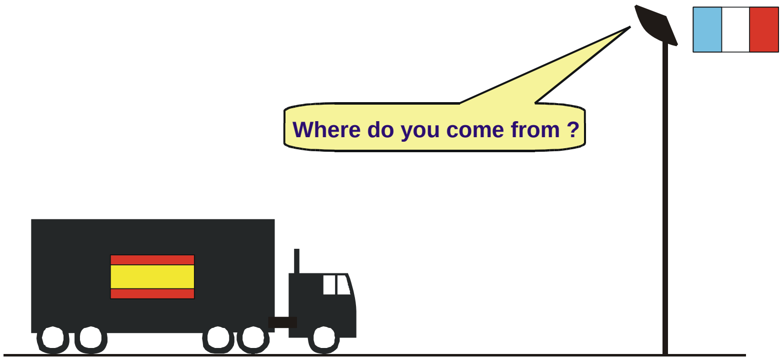
Some technical house-keeping tasks are required, namely to track the vehicle through the communication zone (mainly required in free-flow installations with video-enforcement) and/or to formally close the transaction, i.e. telling the OBE that there is no more to come.

4.2 Transaction Data

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

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.

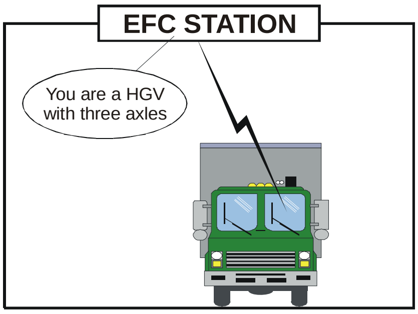
Measured and Declared Classification

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

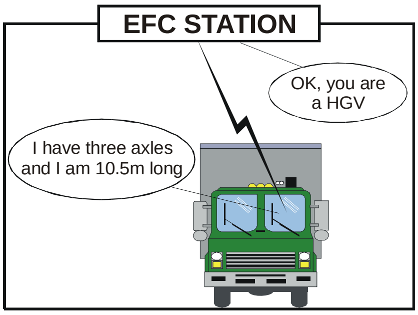
   Sensor arrays are installed to measure specific vehicle characteristics in order to determine the class. In mono-lane systems it is possible to measure a wide range of physical characteristics, e.g. number of axles, presence of dual tyres, length, height, etc. In a multi-lane environment sensor technology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

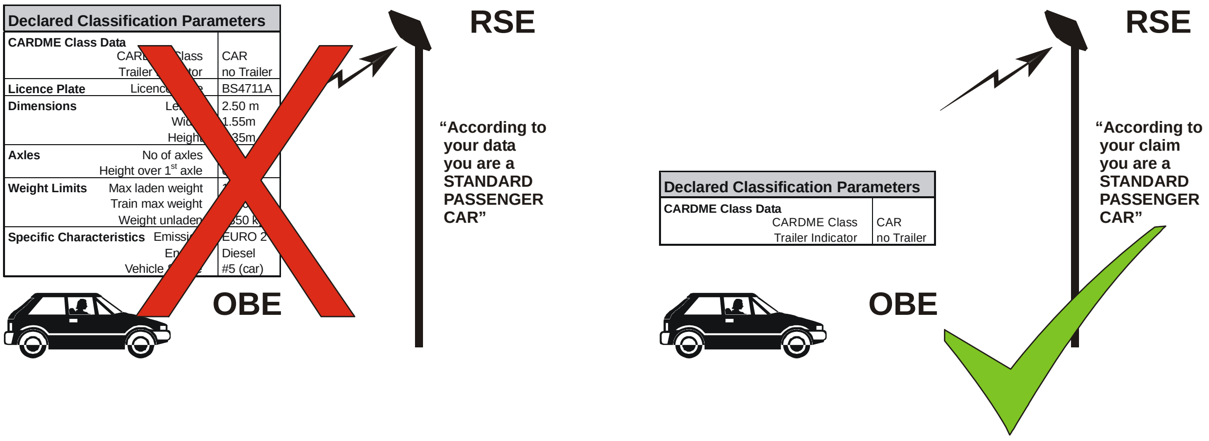
A **normal passenger car** falls into the ‘car’ class in practically every European tolling system. Thus it is not required for a car to have a lengthy list of vehicle characteristics entered into its OBE. CARDME believes that it is possible to find **common European interoperable classes for clear-cut 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.

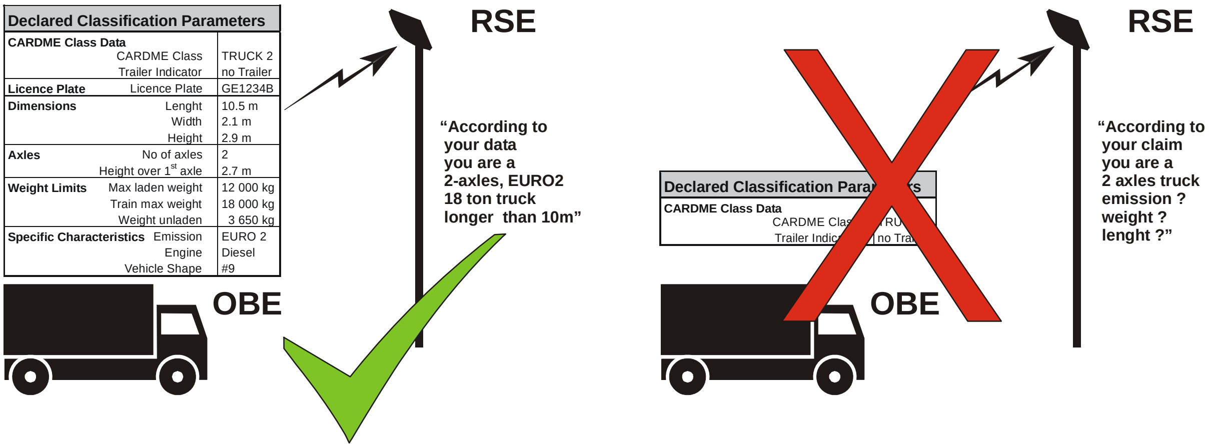
user friendly. Since they only carry a general class information and no vehicle specific details, pre-configured OBE fit any ‘similar’ vehicle. The user may move his OBE from one vehicle to another.

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 and supervised personnel with specialised equipment at dedicated 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.**



Declared Classification Parameters		
CARDME Class Data	CARDME Class	TRUCK 2
	Trailer Indicator	no Trailer
Licence Plate	Licence Plate	GE1234B
Dimensions	Lenght	10.5 m
	Width	2.1 m
	Height	2.9 m
Axles	No of axles	2
	Height over 1st axle	2.7 m
Weight Limits	Max laden weight	12 000 kg
	Train max weight	18 000 kg
	Weight unladen	3 650 kg
Specific Characteristics	Emission	EURO 2
	Engine	Diesel
	Vehicle Shape	#9

RSE
OBE
"According to your data you are a 2-axles, EURO2 18 ton truck longer than 10m"
RSE
OBE
Declared Classification Para rs
CARDME Class Data
CARDME Clas RU
Trailer Indic no Tra
"According to your claim you are a 2 axles truck emission ? weight ? lenght ?"

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.

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.

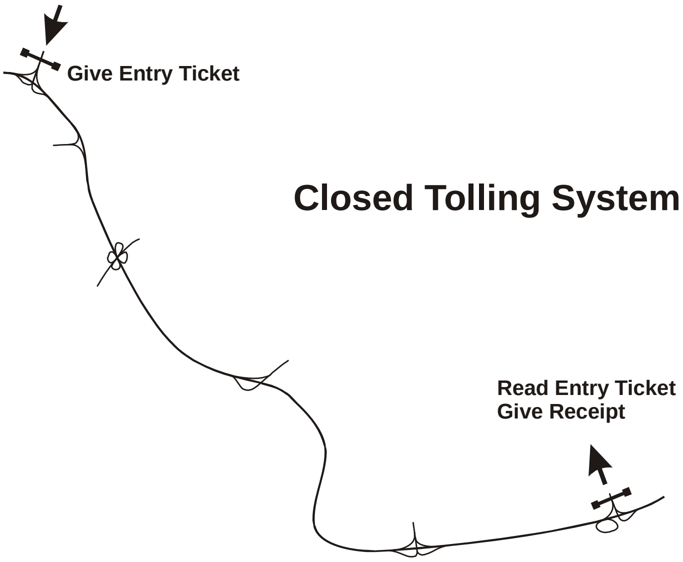
In every CARDME Transaction a 'Receipt' is read from the OBE and then written again. In other words, the road-side always reads the Receipt given at the last station and then writes a new one for the next station. This way information is carried from one station to the next.

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:

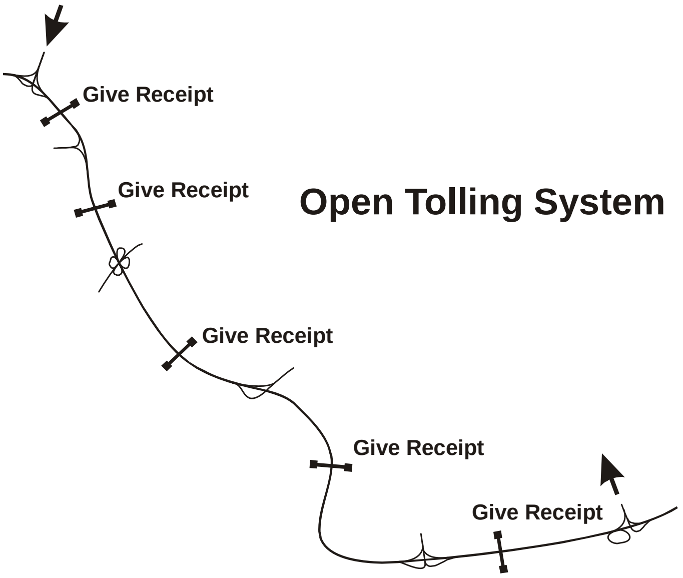
In a Closed Tolling System the tolling stations are at the entries and exits of the highway. There are no stations on the highway. On entering the highway one receives an 'entry ticket' which is then used at the exit to determine the origin of the trip.

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.

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.

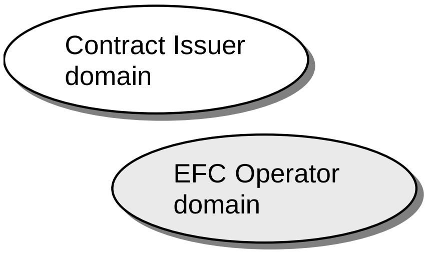
The flexibility of the CARDME security architecture enables the EFC operators and Contract Issuers to choose their own level of security from a wide range. It can be adapted to the threats perceived by each EFC operator. What's more, it allows them to choose the most suitable time for smooth migration 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 a fair 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 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.

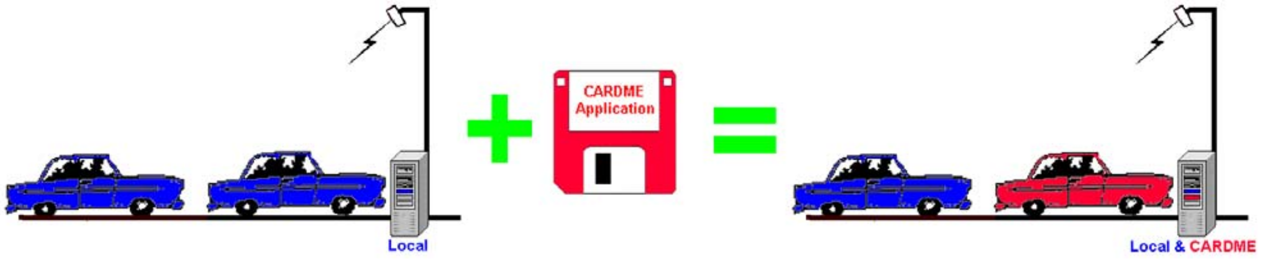
A ***GOOD*** sequence of Transaction Counter value in claims	A ***BAD*** sequence of Transaction Counter value in claims	A ***BAD*** sequence of Transaction Counter value in claims
1	1	1
2	2	2
3	3	2
4		3
5	5	4
6	6	4
7	7	5
8		6
9	9	6

4.3 Transaction implementation

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.

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-initialised '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.

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 a option that can be chosen by the user
- The Contract Issuer cannot disclose this 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. There 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.

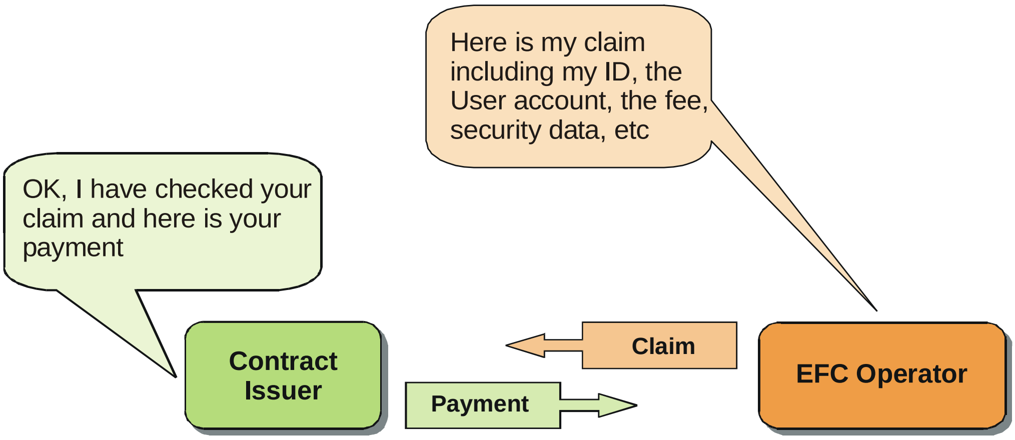
The EFC Operator can offer the user the opportunity to have an itemised bill by providing him access to trip information via internet or by including in the data sent to the Contract Issuer truncated trip data containing only enough detail for the user to identify the trip. Hence neither the Contract 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.

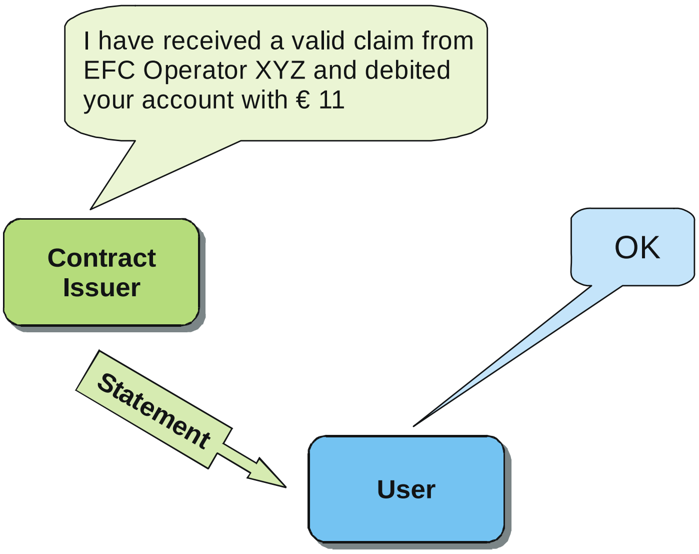
How to Get Paid for a CARDME Transaction

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.


Here is my claim including my ID, the User account, the fee, security data, etc
OK, I have checked your claim and here is your payment
Contract Issuer
Claim
Payment
EFC Operator

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


I have received a valid claim from EFC Operator XYZ and debited your account with € 11
Contract Issuer
OK
Statement
User

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:

Initialisation		▪ Non equipped user ▪ Contract not accepted
Presentation		▪ 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 assistance 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 violating against 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.

5. TECHNOLOGY DEVELOPMENTS

5.1 Introduction

In the CARDME-3 project the possible use of credit cards and electronic purses for toll payment using a DSRC link was investigated. The motivation for this method of payment rather than the use of a central account as proposed by CARDME and CESARE was the alleged desire of users in some countries for greater privacy than is offered by the central account method of payment. This applies mainly to those countries which have not traditionally charged for the use of motorways and which do not have toll plazas. The ASECAP counties do not have a problem of privacy where single lane systems with barriers are available. In these countries users feel that suitable anonymity is maintained by paying in cash at a toll booth.

The conclusions of CARDME-3 were not optimistic for the short term. While some progress has been made since the publication of the earlier report the situation remains essentially unchanged.

This report summarises the position with regard to electronic purses, credit cards and commercial fuel cards.

In the case of the electronic purse the security needed for the transfer of real money over a DSRC link is costly and difficult for operators to justify as an alternative method of payment for EFC alone. The processing speed of IC cards of the present generation remains at a level which requires a second or two to complete a transaction. This is feasible only for single lane systems with barriers where the barrier can remain closed until a transaction is complete or alternatively for free flow systems with an extra gantry to provide a second communication zone for completion of the transaction.

In the case of credit cards the situation regarding processing time is similar but the main restraining factor stems from the fact that the issuers are the financial institutions who feel no particular pressure to offer cards with faster chips. The credit card market is overwhelmingly dominated by retail transactions in which a processing time of a second or two is perfectly acceptable. Even with a high speed chip there remains the problem of reading the credit card details. With an EFC system integrated into the vehicle electronics as is presently being studied by the DELTA project a means of reading cards may be possible but it is unlikely that a contact reader would be recommended for a vehicular environment. The use of an arrangement in which a card is inserted momentarily at the beginning of a journey has been ruled out on grounds of security. A solution involving a monolithic OBU with a credit card account number installed either permanently or by personalising via a DSRC link after agreement of the contract would provide the necessary transaction speed for free flow operation but this does not provide the flexibility to use different cards and in any case is not what most users would regard as “using a credit card” to pay. Both CARDME and CESARE have adopted a 19 digit personal account number for their normal transactions and this would make the monolithic solution easy to implement.

Freight vehicles have more need than others for a flexible payment system as incentives are offered by card issuers which differ among the European countries. Equally the equipment fitted in heavy goods vehicles can be much more capable than that which drivers of passenger cars might be prepared to pay for and the ability to select one of several payment methods is easily provided. This means that slow or non-existent chips on cards are not a problem

The use of commercial fuel cards has also been investigated in this document. The situation is technically similar to that which exists with credit cards but with the advantage that the issuers see provision for toll payment as part of the service they offer.

A complexity for freight transport companies which does not affect passenger cars is the payment of VAT. A preliminary investigation has been made and the findings are reported here. No firm conclusions can be drawn about how VAT for international traffic will be calculated when using a system of the type proposed by CARDME. A general rule seems to be that tax is payable at the rate prevailing for the country in which the service is received but when a single invoice is provided by the users home operator it is not clear how this would apply. It is possible that the procedure could be similar to that used by telephone companies for roaming users. A much more comprehensive investigation of these matters is being undertaken by ASECAP as part of the CESARE project

The project team has worked with the DELTA project to ensure that their recommendations are consistent with those of CARDME. Members of the CARDME team have taken part in the DELTA workshops to ensure this. It is the intention of DELTA to demonstrate support of the A1 transaction and thus vehicles equipped with a DELTA system should be able to use the CARDME transaction.

Finally, this document introduces the subject of the use of a hand-held cellular telephone as a payment device. This is a possibility for the future with DELTA type integrated systems and may enable an extension of a market already saturated in countries such as Italy by allowing users who do not wish to subscribe with an established EFC operator. Further work will be needed on the definition of a suitable contractual framework.

5.2 PAYMENT WITH CARDS

Most deployments of Electronic Fee Collection throughout Europe make use of payment by Central Account: in case of a toll passage the RSE and the OBE exchange data that identify a contract with a toll operator or his agent. The exchanged data enables the operator to charge the amount to either a pre-paid or post-paid account. Typically, the user receives an invoice for the accumulated toll passages of a fixed period. In order to achieve interoperability countries and operators need to agree on a common transaction specification and the involved security measures.

However in countries which are considering the introduction new of EFC systems and where paying for the use of roads is not usually the case, national institutions are concerned with issues regarding user privacy.

In traditional systems if users wish to remain anonymous then they have the option to pay using cash at traditional toll booths. However, in many of these envisaged new systems it is not possible to install traditional toll plazas due to space constraints and the effect on traffic throughput. Therefore there have been significant efforts in the investigation of anonymous payment methods.

The table below summarises the differences between these payment methods:

	COMMERCIAL CARD (so called petrol cards)	**CREDIT CARD**	**ELECTRONIC PURSE**
Specifications body	Proprietary	EMV	CEPS (and 20 proprietary ones)
Availability on a large scale	Yes	No	No
Data available for EFC application	Yes	No	No
Security Scheme	Organisational (magstripe)	Yes	Yes
Transaction Type	Contract Details with authentication	Secure Exchange of Contact Details with authentication	Secure Financial Transaction
Transaction time			
Issuer	10 major international issuers	1000 issuers	1000 issuers
Options		100	100
Transaction mode	Off-line	Off Line On Line	Off Line
Chip type	No smartcard in place	Microprocessor	Microprocessor

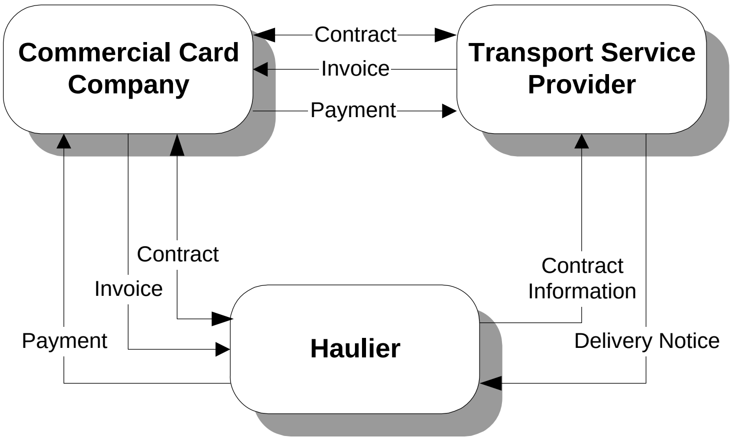
Comparison between Cards

The perceived advantages of using a user's existing payment method with an existing payment service provider is that the user already has a contractual relationship for payment for goods and services. This potentially means that the user does not have to have an explicit contractual relationship with the operator of the toll system.

5.3 Commercial cards

Several companies offer freight haulage firms the possibility for their drivers to purchase transport services across Europe without using cash (e.g. DKV, Euroshell, Routex, UTA). The drivers are issued with payment cards (at present in the form of magnetic stripe cards) which may be used for the purchase of (diesel) fuel, servicing and related services. It should be taken into account that tolls may only represent approximately 2-5% of the running costs of a truck.

These card issuing companies may be termed Payment Service Providers (PSPs). They have the legal status of retailers and, in effect, buy and resell the transport services. shows the relationships between Hauliers, PSPs and TSPs in the commercial card world.



Relationships in the Commercial Card Sector

The Commercial Card Company sets up individual contractual relationships with Transport Service Providers across Europe which guarantee payment for goods and services when a valid credit card is presented.

At the time of purchase the driver presents the contractual details for the vehicle i.e. mag stripe card, and in return receives a delivery note for the goods received. The Transport Service Provider invoices the Commercial Card Company for the goods purchased, which is paid by the CCC according to the contractual regulations. Every 2 weeks the CCC invoices the Haulier for the goods and services consumed for each country in Europe which are paid for by the haulier in one single payment.

At present this is a very commercially competitive market within which Commercial Card companies offer incentives to hauliers/drivers to use their card, there therefore is a requirement for EFC that the driver should be able to dynamically change the payment service provider depending on the current incentives that are on offer although (not necessarily linked directly to EFC).

the following table details the data that (in the magstripe world) is currently needed to be passed from a transport service provider to the commercial card company for payment to be made:

Data Element	Description	Added by Point Of Sale	Held on Card
Account Number (Issuer, Customer No, Card No)	Vehicle Related account number		X
Vehicle Registration Number	Registration Number of vehicle for which the card is valid		X
Card Expiry Date	Expiry date of the card		X
Transaction processing details	Data requirements of the issuer i.e. Mileage, PIN etc	X	X
Restriction Code	Products or countries for which the card is valid		X
Date and Time	Date and time of transaction	X	
Service Provider	Identifier of TSP	X	
Location Identifier	Location of transaction TSP specific	X	

Product Code	Identifier of product type i.e. Fuel workshop etc	X	
Quantity (fuel)	Amount of fuel purchased (litres)	X	
Price per litre (fuel)	Price per litre	X	
Amount	Value of transaction	X	
Version No. of blacklist file	Version of Issuers blacklist checked	X	

Transaction Data Element Requirements

The table below shows how the data elements carried on the Commercial Card can be mapped to data elements within the CARDME transaction.

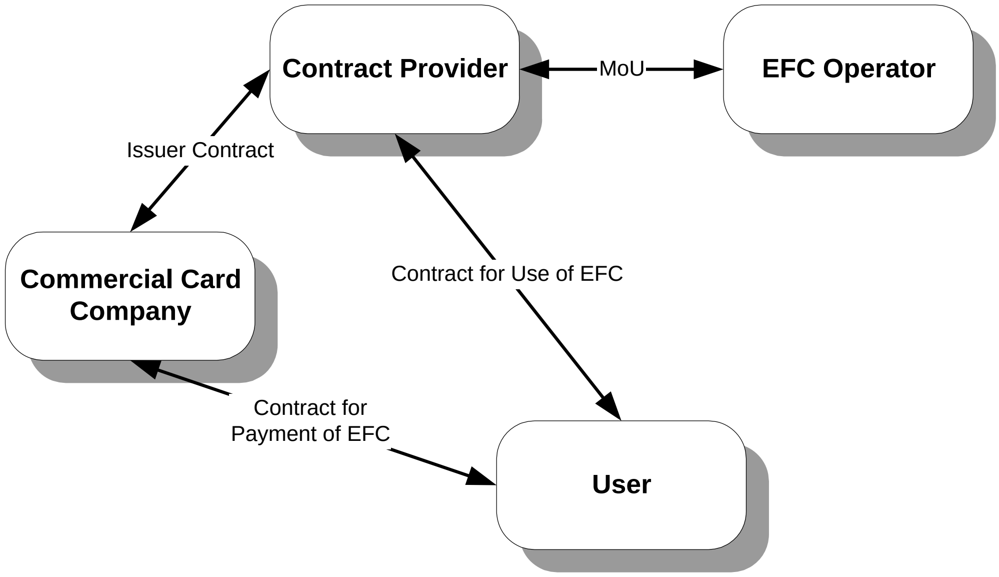
Data Element	**Mapping onto CARDME Data Element**
Account Number	PersonalAccountNumber
Vehicle Registration Number	VehicleLicencePlateNumber
Expiry Date	ContractExpiryDate
Transaction Processing Details	TypeofContract
Restriction Code	ContractRestrictions

Mapping of Data Elements

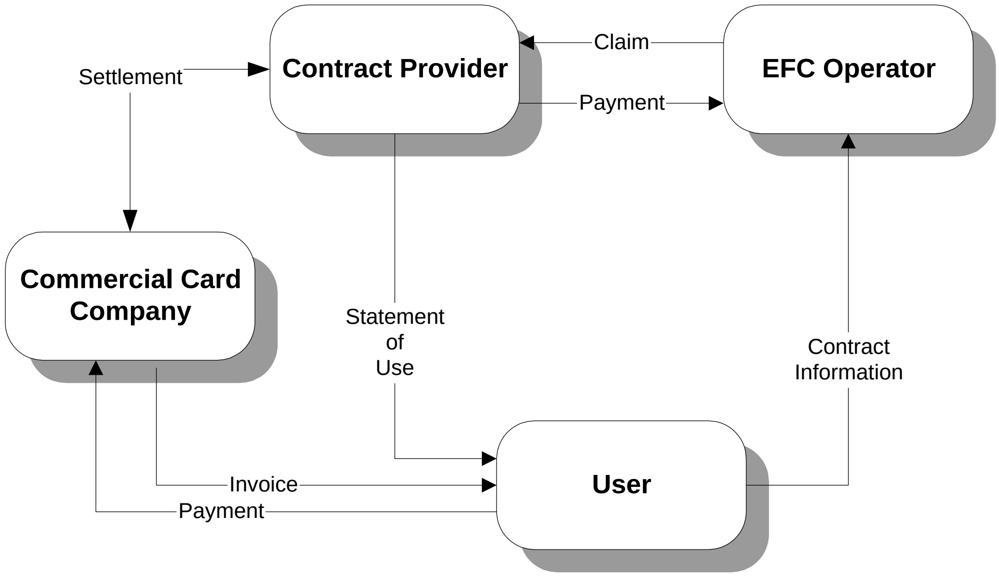
Organisational Implications

In the established scenario for many systems within Europe users sign a contract with their local toll collection company in order to use EFC. If the user has a contract with a Commercial Card Company which is an accepted issuer for the Toll Operator the arrangements shown below will exist. The user has a central account with the 'home' operator which is settled by the user's commercial card account.

Within this scenario it is the 'home operator' which signs up to the CARDME MoU, the commercial card company does not need to have contractual relationships with other operators as it will be viewed as part of the local system.



Contractual Relationships



Information Exchange and Payment

A possible future alternative scenario can be envisaged in which the Commercial card company is itself the contract issuer.

5.4 Recommendations for Commercial Cards

The commercial card sector is a very competitive market, the card issuers source of income is directly linked to the number of transactions carried out with their cards. As a result these companies offer incentives to hauliers to chose their card over other competitors. These companies are able to offer discounts/rebates to hauliers due to the commercial terms of the contractual relationships the card companies negotiate with the various transport service providers across Europe.

Commercial Card Companies have already established contractual relationships with toll operators across Europe in order to offer to hauliers a pan European payment method which allows for payment of all transactions effected within one single invoice and the recovery of VAT from all countries (if indicated in EFC environment).

Currently the Commercial Card Companies issue mag-stripe based cards to hauliers however it could be predicted that this sector may also have to switch to chip based cards in the future in order to combat increasing levels of fraud.

The data exchanged at the point of sale in the current mag-stripe situation is very similar to the information that is exchanged during the CARDME transaction only contractual identification and authentication presented by the haulier at the point of sale.

It is technically feasible for Card issuers to issue monolithic OBUs which replicate the contractual information held on the Mag-stripe card which would be valid in the CARDME interoperable service. It would require no alterations to the business practices in this sector, however, single issuer OBUs conflicts with the requirement from hauliers to be able to dynamically select the payment method.

It is unlikely that until Commercial Card companies issue chip based cards that it will be feasible for hauliers to dynamically change the payment service provider for EFC.

The demand of chip based cards maybe accelerated by the integration of the OBU into the vehicle. Integral DSRC Communications in cars is being investigated within the DELTA project. Two options for the personalisation of the equipment have been identified within the project:

- Personalisation via the air-link
- Personalisation via the On-board computer possibly via chip-card

At present it has not been decided which of these options will be implemented. In CARDME-3 it was indicated that HGV manufacturers may provide standard integrated OBUs as optional equipment as the cost would be marginal in relation to the equipment already installed in such vehicles. Such OBUs could have a chip-card reader to enable the hauliers to dynamically change the contractual details for payment of EFC.

First Stage of Implementation

In the short term it is believed that there are two possible options for the inclusion of Commercial Card Companies within the CARDME scheme:

- Option 1 A Haulier signs a contract with a local CARDME Contract Issuer and this account is settled with the haulier's Commercial Card Account - the monolithic OBU only contains information relating to the contract with the local Contract Issuer.
- Option 2 The Commercial Card Company signs up to be a CARDME Contract Issuer and therefore can issue CARDME OBUs to hauliers that require them. It is likely that due to the commercial environment that these monolithic OBUs will be related to a single card issuer i.e. DKV or Euroshell OBU. As the same information is stored in the OBU as in the Commercial Credit Card there are no implications on the current services offered to hauliers.

However both of these options conflict with the requirement from hauliers to be able to choose with which Commercial Card the toll is paid with unless either multiple OBUs are held or the haulier uses the Stop and Pay method as an alternative to EFC.

In addition Option 1 may have implications on the VAT recovery service offered by the Commercial Card Companies as the contractual situation between the EFC operators will be different to that currently in the commercial mag-stripe card world. For further explanation of the problems see section 5.

Requirements for Future Implementations

In order to implement the flexibility required by hauliers within the EFC world it will be necessary for Commercial Card Issuers to issue chip based cards. However there are a number of issues which are likely to have an impact on this process:

- Commercial Card companies do not own the infrastructure at the Points of Sale, this means that they cannot influence the deployment of the smartcard infrastructure required
- The EMV standards for smart cards are applicable to the financial sector however it is not clear whether the standard meets the requirements of the commercial card world
- If smartcards are to be issued by Commercial Card Companies a decision needs to be made as to whether there will be a common standard for these cards. If not every issuer will have to update terminals with new software and OBUs with common smartcard interfaces could not be developed.

6. CREDIT and DEBIT CARDS

Credit cards like VISA, Eurocard/Mastercard and American Express are well-known examples of widely used ‘internationally interoperable’ payment instruments. The question whether these payment instruments could be the basis for interoperable EFC has been explored before in previous CARDME projects. On-going developments in the field of credit card payment deserve further attention in the context of EFC.

Credit cards are seen as an attractive payment method for the private motorist for the following reasons:

- Credit cards are already accepted for payment of tolls in most stop and pay situations
- Users already have a contractual relationship with the card Issuer
- It is perceived that there is privacy - operators cannot trace individuals and the credit card companies do not know the exact details of where the user has travelled
- The ability to switch cards enable the easy distinction between business and private journeys
- International Payment infrastructure is already in place

However it is believed that there may be a number of drawbacks to the involvement of credit card issuers in EFC.

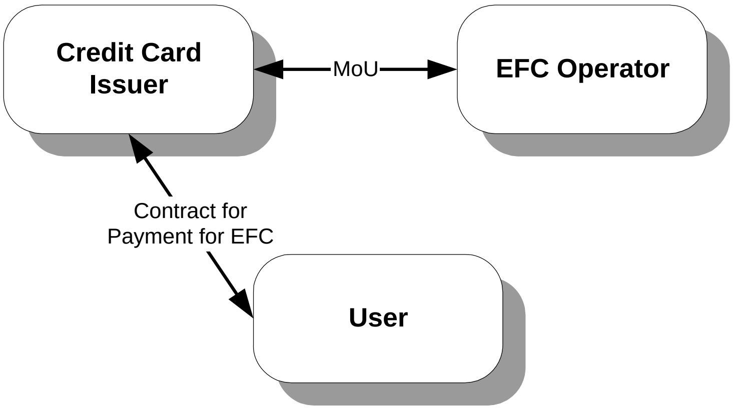
Current credit cards are based on magnetic stripe technology. Both for technical – magnetic stripe reader in the OBU - and security reasons - conventional magnetic stripe based credit cards are not suitable for EFC.

However, Europay, Mastercard and VISA (the ‘EMV’ parties) are now taking on the migration towards chipcard-based credit and debit payments. This chipcard-based scheme is generally simply referred to as ‘EMV’. Card, terminal and transaction requirements for EMV are stable and form the basis for the first implementations (UK). Although it will take several years from now before all terminals and credit cards will be EMV-compliant, there is little doubt that EMV will be the future for credit/debit cards throughout Europe (and beyond).

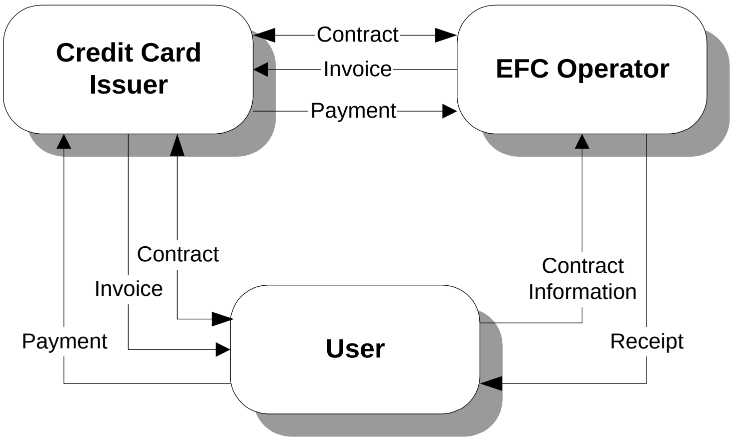
6.1 Incorporating Credit Card Issuers in the CARDME Concept

Within the CARDME Concept it is envisaged that participating financial institutions may act as contract issuers to users. Within this scenario the user signs a contract with the financial institution which allows payment by EFC. The diagrams below show the contractual relationships and the exchange of information of use and payment. All charges are accrued directly onto the user's credit card account.

Within this scenario the Credit Card Issuer will have to be a member of the CARDME MoU and by being so can issue contracts and OBUs to users to enable payment by EFC. The user will only have implicit contracts with the toll operators providing the service.



Contractual relationships



Information exchange and payment

6.2 Technical issues

Main characteristics of the EMV standards for chip cards

Europay, Mastercard and Visa have been working on the specifications for credit and debit payments by chip card since 1995. There are basically three reasons for the intended migration:

- Fraud reduction. Current magnetic stripe bank cards are sensitive to fraud. During the last 10 years credit and debit card fraud has been steadily increasing, especially the counterfeit and so-called ‘card not present’ fraud. The chipcard is expected to be an effective countermeasure.
- Reducing processing costs: with a chip a significant part of the transactions could be executed off-line. This will reduce communication and processing costs.

- New functionality: New applications and functions can be offered on the same card because of the chips´ ability to communicate actively and to store data in secure way.

Europay, Mastercard and Visa co-operated for the development of the EMV standard in order to reduce implementation costs and to maximise the chances of success. Many other financial institutions now follow EMV as the standard for future credit and debit payments (e.g. American Express and Cartes Bancaires). The current version (4.0) of the specifications was issued in December 2000.

Visa and Europay have set a timeframe in which the migration to EMV has to be completed by the member institutions. Europay and Visa EU & CEMEA have adopted the policy that from summer 1999 all new chip card programs shall be EMV-compliant. Starting mid 2000 new cheaper rates are charged to issuers for EMV transactions. During the coming couple of years all new terminals must be EMV compliant and the back-office systems must be made ready for EMV. In nearly all European countries projects have started to prepare for migration of magnetic stripe products to EMV chip based products. Actual roll-out has started in a few countries.

In the United Kingdom, where the first major EMV implementation started in 1998, more than 20% of the banking cards contained an UKIS EMV chip by the end of 2000. Because of security problems with the existing B0' chipcard, the French banks also have a relatively fast path of migration to EMV. According to current plans, B0' will no longer be supported after 2003.

It is expected that EMV will be the dominant standard for Credit and Debit payment in most European countries from 2006.

Capability to support European IOEFC

The main issues to apply the EMV transaction in EFC seem to be the following:

1. *Only off-line transactions are feasible*; online authorisation would lead to unacceptable response times. Individual card issuer policy may require online handling in specific cases. For a terminal without online capability this would lead to a transaction decline.
2. *A cardholder verification method (CVM) should be excluded*. A PIN pad to enter a PIN-code would add to the complexity and cost of the OBU, seems unpractical and may affect traffic safety. The same holds for biometric CVM. EMV specifications (as well as the Europay specifications) do not exclude terminals without CVM capabilities.
3. *Transaction time*. A normal EMV transaction without optimisation may take some 1-2 seconds, depending on the IC-card used. This may be acceptable for EFC-installations with barriers and low-speed single lane systems. For high-speed configurations a 2-zone solution seems feasible. However, the envisaged route to an interoperable EFC-transaction should avoid major hardware modifications in existing EFC-systems. A complicating factor is that the EMV specifications do not specify any performance requirements. For the terminal this does not cause major concerns, as terminal processing time can be reduced without much difficulty given the processing power in computer hardware available in a typical RSE. Bottleneck is the IC-card. Issuers are allowed to make their own decisions on make and types of cards issued. As a result, there may be a great variety in response times between EMV branded cards.

6.3 Procedural issues

EMV will have many card issuers which make their individual choices for card technology. Cards will differ strongly as to response times. It is therefore a challenge to guarantee that any given EFC-system supporting EMV would work with all existing varieties of EMV-cards.

Apart from variations in response times, other differences have to be taken into account. In order to offer a solution that is suited for a wide variety of countries, banks and merchants in different environments, the EMV specification offers options for several functions.

Some of the options can be selected by the merchant/terminal or acquirer, others depend on the card issuer’s policy and the capabilities of the card type issued. The options selected by the issuer can lead to complications if the EFC-system has to deal with (EMV-cards from) various issuers from all over the world.

The EMV specifications do not set performance requirements for EMV transactions. However, it seems plausible that cards will be developed in such a way that a transaction will take at most 2 seconds. In those 2 seconds communication with the card takes place, card processing and terminal processing.

The terminal processing can be done very quickly in an advanced terminal as could be developed for remote EFC.

The card communication mainly consists of Read Record commands-responses. Between 5 and 10 Read Record commands will be send to the card. In an offline transaction with SDA or Combined DDA/Generate AC and without offline PIN verification only three other commands are required.

On basis of this we may assume that on average a command will not take more than 200 ms to be handled (communication to the card, card processing and card response). By increasing the frequency and baud rate, which is allowed according to the ISO specifications, this time may even be reduced to something like 100 ms per command.

Since for a remote EFC transaction the Read Record commands can be performed before the card reaches the payment zone, it seems possible that the other commands can be handled in the available time assuming a wake-up signal and two communication zones. Note however, that card performance may differ a lot from one card to the other and agreements have to be made with the issuers about card performance.

6.4 Recommendations for Credit Cards

One of the main reasons for the introduction of EMV based credit cards is due to the unacceptable levels of fraud currently being experienced due to the use of mag-stripe cards. Due to the large scale nature of these payment methods, approximately 20,000 card issuers worldwide, the potential for fraud is high and so the importance of scheme integrity is important the card issuing organisations. The introduction of EMV based cards has allowed for the use of cryptographic measures in the transaction between the card and the terminal. However the use of cryptographic techniques means that the transaction times for EMV payments are currently longer than the time frame allowed for EFC.

Whilst it maybe possible to develop terminal equipment which is optimised for the time constraints within EFC it is highly unlikely that the EFC community will be able to influence the cards that are issued to users. In the future as card processing power increases then the time required for EMV transactions will decrease, however the EMV standards do not cover the technical performance specifications for the cards which means that there is likely to be a significant difference in EMV transaction times between card issuers.

It is technically feasible to overcome this problem for multi-lane systems through the use of two DSRC communication zones over which the transaction is split, approach adopted in the

Rekeningrijden project, however this is an unacceptable solution as it would imply the installation of additional equipment at every toll point in Europe.

A more viable solution would be for credit card issuers to issue 'standard' CARDME monolithic OBUs to users which are linked to the user's credit card account. The identification within the OBU would point to the users account but be different to the actual account number so that the security of the credit card scheme could be maintained.

1. *No need for hardware modifications*. This condition would not be met for multi-lane configurations as multiple communication zones are necessary to accommodate an EMV-transaction.
2. *Applicable for single and multi-lane*. A 1s transaction time is expected to be feasible with some enhancements. For single-lane with barrier this will not cause difficulties. A free-flow multi-lane solution seems technically feasible but would require specific development.
3. *Feasibility within 5 years*. By 2006 the majority of European credit cards are expected to be EMV-compliant. Some deviations from the specifications would be necessary for EFC. Specific arrangements would have to be made with the acquirer(s)

7 ELECTRONIC PURSE CARDS

An Electronic Purse is essentially an account held in a secure module, typically an IC-Card or smart card. The payment scope of the purse can be limited to a limited number of services or service providers, in which case it is generally referred to as a ‘closed purse’ (e.g. a telephone card). It can also have a broader scope and have the status of a generally accepted payment means: an ‘open’ or ‘intersector electronic purse’. This type of purse is generally issued by banks.

Since the mid-90’s several national open purse schemes have emerged in Europe and some other countries. Examples with millions of cards issued are the German ‘Geldkarte’ and the Dutch ‘Chipknip’. As was reported already in CARDME-3, these purse schemes currently have little potential of being used as a Europe-wide interoperable payment means as a result of their national scope.

Recent developments in Electronic Purse Schemes

Recent initiatives concerning electronic purse schemes with an international (or at least Euro-) scope however deserve renewed attention in the context of CARDME.

The European Committee for Banking Standards (ECBS) produced the first outline for an 'Interoperable Financial Sector Electronic Purse’ in June 98. The specifications define the requirements and roughly describe the application protocols and key management.

Just after deliverance of the ECBS specifications, the birth of the Common Electronic Purse Specification (CEPS) was announced (18 June 1998). CEPS [4,5,6] can be regarded as the next step on the path taken by ECBS. The specifications were completed in 1999.

The CEPS specifications were released by:

- VISA España / SERMEPA
- VISA International
- ZKA (Zentraler Kredietausschuss, Geldkarte)

The CEPS-supporting parties are now united in ‘CEPSCO’.

The specifications describe a minimum functionality that is required for interoperability. VISA international (‘VisaCash’) and Europay (‘Clip’) each have further elaborated these specifications to the detail required for implementation.

Implementation status

Officially Visa, ZKA, Europay and many other European financial institutions have committed themselves to CEPS as THE standard for future electronic purse schemes. Several small-scale pilots have been carried out.with card and terminal implementations according to CEPS.

At this moment a larger-scale CEPS project is done by Banksys, Europay International, Interpay, Proton World, Sermepa, Sistema 4B and Visa International and Cartes Bancaires. The project is named "Ducato" and has the following objectives: 'to validate the CEPS-related technology in a real, international environment, and to demonstrate interoperability, between different countries and different e-purse technologies, schemes, brands, clearing systems and hardware. The project will show that CEPS are reliable, ready for implementation and supported by industry-leading vendors and financial institutions.'

Obviously CEPS is not yet ready for mass roll out. A factor that may speed up deployment is that several domestic e-purse schemes will need an update within the next few years. CEPS could be offered as an application on EMV-cards and may break through after the implementation of EMV. One of the critical success factors will be a convincing business case for electronic purses. Current domestic schemes suffer from disappointing transaction volumes.

Issues Surrounding Electronic Money

Electronic purses are intended by the issuers to be primarily a replacement for notes and coins. Cards can be bought with a preloaded value, or they can be loaded from a bank account, then used at retail outlets with suitable terminal equipment, or at vending machines, payphones and car parks.

However public acceptance of these schemes and uptake have been relatively poor to date even with the advertised benefits such as:

- the convenience of not having to carry and find change;
- Electronic Purses are more secure hygienic than carrying cash
- The ability to change currencies easily.

It is feared by sectors of the public that banks are able to monitor all transactions carried out with an electronic purse and so be able to determine the habit of individuals, but at the same time users have the requirement that if the card is lost or stolen that the monetary values stored on the card be retrievable,

Banks like electronic purse schemes because it usually gives them a "float" value relating to the unused balance on the card, on which they can earn interest. For retailers, there is evidence people spend 15/20% more with SVCs because of the higher propensity to make impulse purchases and never running out of change. Because electronic cash does not have to be manufactured, transported around or counted, it is cheaper for banks and retailers to administer.

Because it is actual money that is contained in an electronic purse, the means of transferring money to and from a purse must be done in a secure manner. Naturally financial institutions are concerned with the security of money and the banking regulators are concerned over the rules that govern the issuing of electronic purse schemes. The banking regulators ensure the soundness of the money in circulation in their countries, regulate institutions which issue money, fight fraud, and monitor money supply.

There is currently a debate as to what organisations are able to issue purse schemes - credit institutions are required to be regulated by their Central Banks and to satisfy these regulators on the capital stability of the institution. Thus, a consumer depositing money with such an institution can have a degree of confidence his money is safe and there is a lender of last resort if the bank should fail. If unregulated institutions are allowed to issue electronic money, it might be like turning the clock back to mid-19th century America, and the issuing of unsupported greenbacks

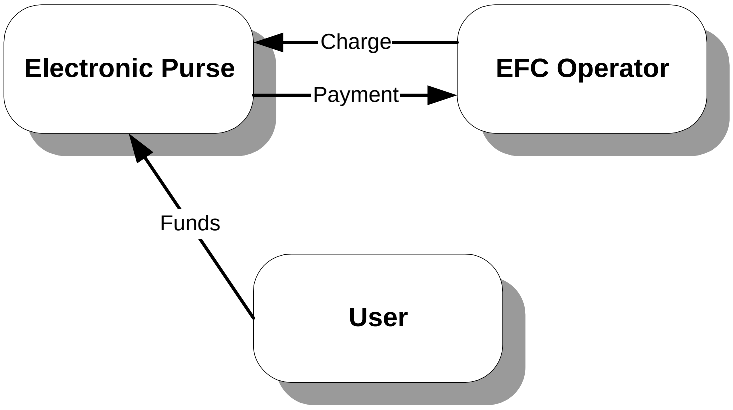
7.1 Incorporating Electronic Purses in the CARDME Concept

Organisational Implications

The main driving factor for the inclusion of electronic purses in CARDME is the anonymity which is offered to users through such schemes.

The CARDME scheme has been set up on the assumption that the user has a contract with an entity for the payment of EFC. This issuer maintains a central account to which all charges incurred by the user are accumulated and settled via a post payment invoice. There is currently no provision within the CARDME CONCEPT for financial transactions to be carried out over the air link, currently on the exchange of contract identification is proposed.

Electronic purses offer immediate anonymous payment, removing the requirement for the identification of the user to enable post event billing. As no user information is provided to the operator it is likely that unless a VAT receipt can be stored in the vehicle it will not be possible for the user to obtain a VAT receipt after the event as with current central account processes.



Exchange of Money with Electronic Purse

Potential Technical Implementations

As the money contained in an electronic purse is contained within the chip on a smartcard the OBU will require a smartcard reader. The OBU must be transparent to the purse so that the transaction with the terminal at the roadside can be completed in a secure manner. The exact nature of this transaction is likely to be determined by the scheme issuer.

7.2 Technical Issues

Main characteristics of CEPS

A CEPS payment transaction requires a smart card with a CEPS purse application on one side, and a payment terminal with a CEPS Purchase Secure Application Module (PSAM) on the side of the merchant. The transaction results in the debiting of an amount from the purse and the generation of transaction data on the PSAM/terminal that provide proof for reimbursement by the acquirer. The amount to be debited is either sent by the cash register or entered manually on the terminal's keypad by the merchant. Typical for electronic purses is that the transaction can always be executed without online communication to the issuing and/or acquiring bank. This has the advantage of fast and potentially low cost transactions.

Most existing e-purse schemes are based on symmetric cryptography essentially based on shared secret keys between purses and SAMs. This architecture is not suited for a multiple-issuer environment. In practice, a multiple-issuer support is a prerequisite to achieve international interoperability in a practical way. CEPS is therefore based on public key cryptography (using RSA). RSA however, is rather computation-intensive. Given the limited computing power of a smart card, short transaction times are still a challenge for CEPS implementations.

Standard CEPS Transaction

A CEPS purchase or payment transaction (which is not optimized for EFC) consists of the following steps:

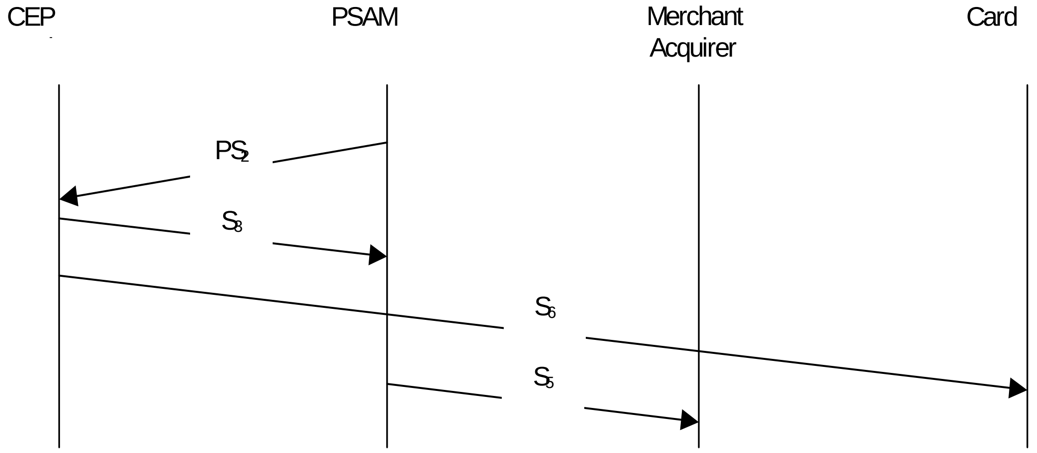
1) the initialization of the card & exchange of certificates

2) the debiting of the card

3) the transaction record signing process.

During the initialisation of the card the right currency slot is selected on the user card. This is done through an 'Initialise for Purchase' command. Further the terminal has to check whether a card of this (regional) issuer is supported by the PSAM or not. The terminal also checks whether the issuer public key is already in the PSAM. When not, the issuer certificate and the regional issuer certificate are read out from the user card. (The last occurs e.g. when an American pays in a European terminal).

During the debiting of the card both symmetric and asymmetric cryptography is used. Authentication of the PSAM to the card is done with RSA certificate called PS_2 (algorithm and certificate versions specified by the card). This certificate contains a DES key that is encrypted with the Private key of the PSAM and with the public key of the card. The card decrypts this DES key and uses it as a session key, to authenticate itself to the PSAM (S_3). Actually the dynamic authentication of the card to the PSAM is done with the 'Response to Debit for Purchase' command. During the debit of the card also the signing of the transaction record is done (S_6). So the Debit for Purchase command has three functions: to debit the card, to authenticate the card to the PSAM and to sign the debit transaction. The transaction data is signed by both the card (using a card issuer's DES key: S_3) and the PSAM (using a merchant acquirer's DES key: S_5).



Flow of signatures for a CEPS purchase transaction

CEPS for EFC

Electronic purses are attractive for Electronic Fee Collection. Payments are always anonymous. Moreover clearing and settlement is always done batch-wise, which may reduce the transaction costs. Apart from that the risk is less because electronic purses are ´pre-paid´.

The CEPS protocol however, has not been designed for EFC (fast) payments. This is clear from the lack of performance requirements and also from the protocol between card and terminal (PSAM).

Having a closer look to the first part of the protocol between card and terminal, it seems that both first have to exchange data and that the Terminal/PSAM (at the road side) than has to send the PS_2 cryptogram. It seems that this technically can be solved by reading out the CEPS card upon insertion in an On Board Unit (OBU), and by sending over the required data to the terminal/PSAM (at the road side) at a first DSRC zone (1st gantry). During that communication the terminal/PSAM than can send the PS2 cryptogram to debit the card.

During the debit of the CEPS card, the card needs time. At least one RSA calculation needs to be done and two T-DES cryptograms need to be calculated.

In the specifications of CEPS no performance requirements are put. These requirements could be given in the brand specifications (VisaCash and Clip), but the authors of this document do not know whether this is done.

An estimate is that the debit will take at maximum 1 second for a transaction as normal baud rates and chip clock frequencies. When the debit would take longer, the percentage of ´unsure debits´ would increase (when customers take out their card during debiting the card). This means that at increased baud rates and clock frequencies we expect the debit to take at maximum 0.5 second (estimation). This gives a restriction to the distance between two DSRC zones (1st and 2nd gantry).

At the second gantry the OBU will send the essential information (mainly the cryptograms) to the road side. The PSAM will sign the transaction and the data can be send (batch wise) to the acquirer and issuer for clearing and settlement.

To be sure about all this the protocol needs to be worked out more precise. However, for the moment we conclude that it seems that CEPS can be used for EFC in a two gantry DSRC set-up.

Capability to support European IOEFC

A few problems may arise when applying CEPS for EFC:

Transaction approval.

In a normal purse transaction the user has to explicitly approve a debit to his card. After the transaction amount is displayed, a YES or OK key is to be pressed. Given time constraints, given the minimum user interface requirements to an OBU, and given the fact that the user should not be distracted from his driving task, such an explicit approval is not feasible for EFC. A possible solution is that the insertion of the card into the OBU at the start of the trip implies approval for an EFC transaction. Some limitations to the transaction amount may have to be defined for implicit approval.

Transaction time.

No card performance requirements are defined in the CEPS specifications. Nevertheless, for any practical deployment a transaction duration of more than a few seconds is unlikely and undesired even in a retail environment (risk of early withdrawal of the card). As was discussed in the introduction of this Section for single lane EFC-installations with barrier a transaction time of a few seconds may be acceptable. Free-flow multi-lane systems may offer a DSRC connection time of only some 130 ms at high speeds (leaving e.g. some 70 ms 'net' for the payment transaction). Both the IC-Card and the PSAM processing are an obstacle to achieve such short transaction times. The debiting process on the card typically requires one RSA calculation and two 3-DES calculations. For a state-of-the-art IC-Card without dedicated crypto-hardware this may take some 500 – 1000 ms[1]. Optimisation of clock rate and bit rate will help to reduce this figure by a factor of 2.

It seems that free-flow high-speed transactions with CEPS are possible in an EFC-setup with two DSRC-zones. As the CARDME interoperable EFC-transaction should work in any EFC-system without the need for major modifications, a two zone solution is currently only of theoretical possibility.

Schemes with one zone only would be forced to upgrade to 2 zone systems for free flow operation unless card speeds are increased

7.3 Procedural Issues

Obviously CEPS is not yet ready for mass roll out. A factor that may speed up deployment is that several domestic e-purse schemes need will need an update within the next five years. CEPS may follow the Europe-wide implementation of EMV. One of the critical success factors will be a convincing business case for electronic purses as current national schemes still suffer from disappointing transaction volumes. A substantial installed base for CEPS is unlikely before 2007.

As is the case for EMV, a future CEPS-scheme may have many card issuers which make their individual choices for card technology. The CEPS card specifications currently don't define any requirements regarding transaction duration. It is therefore difficult to guarantee that any given EFC-system supporting CEPS would work with all existing varieties of CEPS purses.

On the side of the PSAM and EFC-terminal performance is also critical, but easier to deal with as these can be influenced by the EFC-operator. In addition, the RSE will have far stronger processing resources than the IC-Card. The standard PSAM however may also be IC-Card based and require performance enhancement to be applicable for EFC.

7.4 Recommendations for Electronic Purses

The Common Electronic Purse Standard (CEPS) has serious potential to become the basis for an internationally interoperable open electronic purse. Whether such a scheme will be realised is however still an unanswered question. It is unlikely that CEPS will be operational on a large scale before 2007.

If CEPS will be realised on a European scale, it could be the basis for an interoperable EFC-transaction. Analysis of the specifications indicate that with state-of-the-art card technology, a CEPS transaction will generally take too much time to be applicable in free-flow EFC-systems with one DSRC zone. It would probably fulfil for single lane systems with barrier.

CEPS does not specify any performance requirements. For the potential benefit of EFC and other applications, it is recommended to discuss the possibility of performance requirements in a future issue with the parties responsible (CEPSCO).

1. *Feasibility within 5 years*. Unlikely. Both CEPS and the banks are not ready for large-scale roll-out. The business case for a European purse has not convinced all financial parties (yet).
2. *Applicable for single and multi-lane*. A 1 s transaction time is expected to be feasible with some enhancements. For single-lane + barrier this will not cause difficulties. A free-flow multi-lane solution seems technically feasible but would require specific development.
3. *No need for hardware modifications*. This condition would not be met for multi-lane configurations as multiple communication zones are necessary to accommodate the EMV-transaction.

8 VAT AND INTEROPERABLE EFC

8.1 Background

Users of tolled motorways across Europe are offered many different payment methods at each toll plaza. While most users initially paid using cash, multi-trip magnetic cards, credit/debit cards and local account cards are now accepted.

Most operators are introducing non-stop payment methods which make use of microwave communications between roadside beacons and on-board equipment. Users with suitable on-board equipment drive through the toll lane without stopping. Unfortunately currently most of these systems are not interoperable and users wishing to make long-distance cross border trips may be faced with the need to have multiple on-board equipment.

The CARDME project has been working since 1994 on overcoming the potential problems caused by incompatibilities between electronic charging systems for non-stop payment of motorway tolls. This is a particular problem for the long-distance movement of freight.

CARDME has proposed a solution to the problem. This involves use of the CEN standards to achieve technical and procedural interoperability (using 5.8 GHz microwave communication). CARDME has defined a minimum common inter-operable transaction which it is hoped can be implemented by all tolled motorway operators across Europe.

Several initiatives (MOVE-it, CARDME, CESARE) have worked on the contractual framework to support interoperable Electronic Fee Collection (EFC). The contractual framework proposes that users sign contracts with "local" issuers (i.e. in their own country). These issuers will provide on-board equipment which can be used throughout Europe.

Unfortunately, tolls are becoming increasingly subject to VAT, with different rates applied in different countries, this may introduce further potential obstacles to the realisation of the inter-operable service for commercial users. Commercial users need a VAT receipt in order to reclaim VAT from the appropriate VAT authority.

An outline of the potential issues is presented within this section and existing solutions within other sectors are presented for consideration. Due to the complexity of this issue no attempt has been made to draw conclusions on potential solutions, however, CESARE II is conducting an investigation into the resolution of this problem.

8.2 VAT Issues

There are a number of issues associated with VAT for interoperable services:

- Across Europe the levels of VAT differ

- Commercial Users need to be able to recover the VAT that they are charged

In traditional stop and pay situations commercial drivers could receive a legal VAT receipt at the time of payment for the services, however most current non-stop payment methods are based on post payment. As these services are currently restricted to single system operations users are supplied with a monthly VAT legal invoice from the operator of the EFC service.

However the VAT situation is complicated when dealing with interoperable systems and especially cross border interoperable systems where different VAT rules apply.

The key issue is that VAT is charged at the appropriate rate where the service is consumed. A possible procedure is to set up an agency to act as a VAT clearing house which would then charge all users at the VAT rate applicable in the country in which the agency is established.

In the GSM world the problem of cross-border VAT has been solved in the definition of the service provided to users.

It has been defined that wherever the user uses the GSM service it is an extension of the local service provided by his contract issuer that is being consumed and as a result VAT is charged at the ‘home’ VAT rate.

More detail on existing VAT procedures is to be found in Deliverable 4.3

9 OBU INTEGRATION BY VEHICLE MANUFACTURERS

The trend in Europe by most car manufacturers to include air conditioning as first fit equipment is still very positive. To improve the efficiency of the air conditioning system, car manufacturers have introduced metallic windscreens. The metal coating on the glass of the windscreen creates a large attenuation for radio signals, especially for signals at 5.8 GHz used by DSRC equipment. Hence, a large part of the car market, like the high segment, is faced with overwhelming problems when the question of mounting an OBU is raised.

To help the car industry to solve this issue with the DSRC community, the DELTA project has been set-up during the 5th Framework. The objective of the project is to integrate the DSRC communication link as basic equipment in any vehicle. This will be done by establishing a standardised interface between CEN compliant DSRC units and the in-vehicle electronics (DELTA will fully comply with the current DSRC ENVs as well as with future ENs). Apart from standardisation proposals on the overall architecture and common interface specifications, the project will also produce recommendations on related issues such as antenna position and design. This will allow a range of DSRC applications such as EFC and TTI to be combined with a view to being offered on the mass market whilst ensuring the correct functioning of transponders operating behind metallic or heated windscreens.

As the intent of DELTA is to have the specified OBU mounted in all vehicles in the near future, this raises questions of the compatibility of this project with the results obtained during the different phases of CARDME. The introduction of OBU in each car in future is seen by CARDME as a great help in promoting an IOEFC service across Europe. The following sections summarise the main results obtained until now by the DELTA project and look at how the CARDME IOEFC service could be supported by such devices. At the present time CARDME is compatible with the products available on the second fit market.

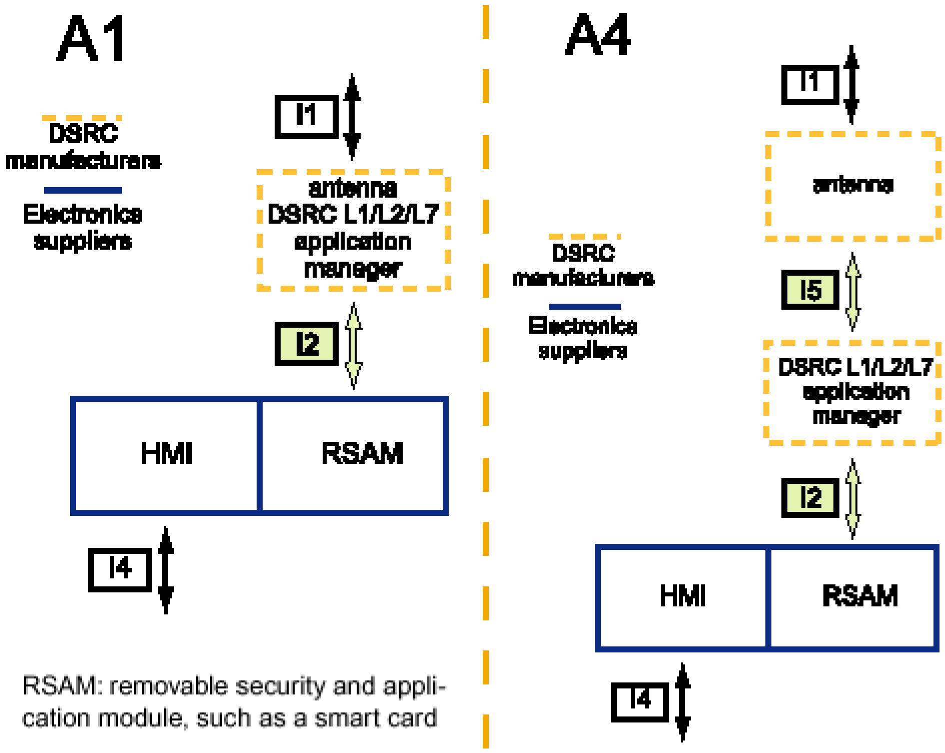
10 THE DELTA PROJECT

10.1 DELTA Architecture

The DELTA consortium has developed several functional and physical architecture proposals. The functional architecture pays particular attention to the applications that will be tested in DELTA, including electronic fee collection. Apart from EFC and TTI, many other applications have been investigated and will be supported, such as in-vehicle signing to assist with safe driving, parking garage fee payment, MP3 music download while fuelling, vehicle status, software installation, mission planning, floating car data, multimodal transport information, vehicle control, service subscription and diagnostics.

The DELTA consortium has considered five physical architectures. Using an extensive evaluation framework derived from the project's user needs, the consortium has selected two very related architectures (shown below).

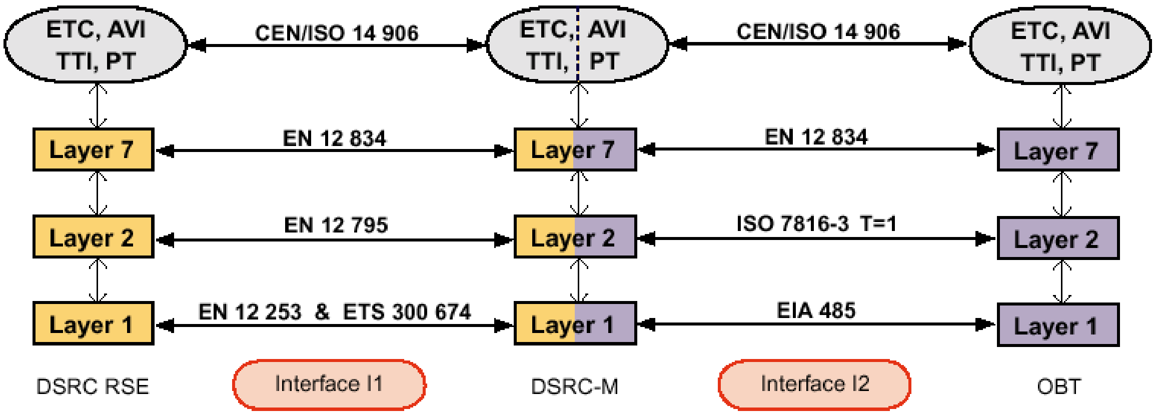
Architecture A1 is proposed for test purposes within DELTA whilst both architectures A1 and A4 are proposed for mass-market deployment. The compelling arguments for architecture A1 are high performance, low cost and good time to market. Architecture A 4, on the other hand, is highly modular and therefore very flexible. It also allows optimal integration of the DSRC antenna.



RSAM: removable security and application module, such as a smart card

DELTA is also addressing the interface between the on-board terminal which can also be distributed equipment and the DSRC unit. Key aspects considered when specifying this interface were the ability to execute different demanding applications in real-time, the ability to perform new applications and to configure and upgrade these applications whilst at all times respecting a high level of security. Also, maximum use was made of existing standards when developing the specification. The result of this is the selection of EIA-485 as a reliable, high-speed and widely available cheap connection at the physical level; ISO 7816-3 T=1, or a widely used and robust smart card interface at the data link level; and prEN ISO 14906, or the existing DSRC standard at the application interface level.

The DELTA specifications also cover key issues such as communication activation, HMI (human-machine interface) functions on the interface such as data entry via a keyboard or presentation of information via a buzzer or screen, data security focusing on the management of the security keys, key communication scenarios such as system and application configuration, application initialisation and random number generation, and finally, reliability through support for degraded modes and flexibility offered by the interface to car manufacturers, for instance by allowing different DSRC units to be connected to the on-board terminal.



10.2 Support of CARDME concept by a DELTA OBU

The DELTA project will conduct tests on the different equipment developed according to the scope of the project. The equipment will be able to demonstrate different applications from the EFC and the TTI domains.

For EFC applications, DELTA should be able to support the following transactions:

- TIS,
- Autopass,
- A1.

The transaction specified in detail by CARDME in the Deliverable D 4.1 fulfils the requirements of the CARDME concept. It is specified by using the tools provided by the A1 project and can thus be regarded as one instantiation of the A1 transaction model.

Therefore the CARDME transaction can be supported by DELTA. The transaction should be entered in the programmable area of the DSRC module offering to the User the functionality and the service provided by CARDME.

10.3 Initialisation of the OBU with Contract Issuer data

Presentation of the problem

The target of the DELTA project is to implement directly as a first fit a DSRC interface in each car manufactured and sold in Europe in the coming years. Any car could be sold anywhere in Europe by the manufacturer.

This car will have also its own life cycle: multiple owners, owners could also move from place to place. Therefore it will be a very complex and tedious task for the car manufacturer to enter into the DSRC module the data provided by a contract issuer.

The car manufacturer must provide a way for the car owner to allow an authorised organisation to enter the data into the DSRC module. Depending on the architecture of the on-board computer of the car, two main categories of data initialisation are possible: direct initialisation or via a removable support.

Direct initialisation means that the data will be directly entered into the DSRC device as is done at the present time with most DSRC OBUs. The removable support is a device able to carry all the data required by the Contract Issuer to enable a user to benefit from the service. This device will be read by the On-board Computer to personalise the DSRC module.

Direct initialisation

The direct initialisation could take different means for the transfer of the data from the Contract Issuer inside the DSRC OBU. The direct initialisation proposal is a very attractive one, because it relies only on existing solutions and products. Therefore, it could be implemented as soon as the DELTA module is available on the market.

The mains solutions are:

- Microwave link
- Access through the on-board computer

The microwave link is already used by several manufacturers for the personalisation of their OBU. In this case, these OBUs do not have any external access for the reception of the data. All the mechanisms required to ensure security for the personalisation are already defined by the manufacturers. To ease the interoperability of the equipment from different sources, the DSRC module manufacturers should defined a common procedure for the personalisation of the DSRC module through the microwave link.

The access through the on-board computer is only possible if a port is provided by the car manufacturer for entering data by external parties. There is also a lack of standardisation in this area to ensure the Contract Issuer to have only one equipment and software for the configuration of the DSRC module of their subscribers. Therefore this solution does not seem to be a viable one for the near future.

A difficulty with the direct initialisation solution is the management of the data during the life cycle of the car. The car life cycle could lead a User to close his contract with the Contract Issuer for many reasons like the sale of his car. Hence, the data written inside the DSRC interface must be erased to avoid any trouble for the relationship between the User and the Contract Issuer (wrong charging, violation, etc…). The Contract Issuer could do the removal of the data in the same manner as the writing of the data. This will imply that the User will have to stop at a point of sale to have the operation done. It is also possible to allow the On Board Computer to do it at the request of the User. This solution is very convenient for the User who does not need to go anywhere to have this task done. But it will never assure the Contract Issuer or the User that the data have been properly erased from the DSRC interface.

An other issue will be the need for the User to go to a point of sale of the Contract Issuer to get his vehicle personalised with his own data. This drawback is counterbalanced by the fact that it enables the Contract Issuer to keep a direct link with his customer. This is a major part of a security scheme.

If the Contract Issuer wishes to avoid the User having to come to a point of sale to obtain the personalisation of his DSRC module, there are other possibilities: EFC lane or car dealer.

The EFC lane solution is based on the fact that for most users the issue to subscribe is the need to stop at a point of sale. The points of sale are mainly located at toll plazas and the users are not keen to stop for subscribing. It could be envisaged that the Contract Issuer could offer a new service to the users by subscribing on the Web. The users would be able to open a contract on-line by providing to the Contract Issuer all the data needed to open an account, as part of the data set is included the DSRC module identifier. When the driver goes through an EFC lane, he is recognised as a new subscriber and the relevant data are written into the DSRC module. The issue to be solved is around the security required to ensure the correctness of the data entered.

The car dealer solution relies on the fact that the user could subscribe to an EFC service directly when he orders his new car. This solution will need an agreement between Contract Issuer and car dealer on the procedures to enable the car dealer to distribute EFC contract with all the relevant security concerns.

Removable support

The removable solution offers more flexibility because there is no need to have a physical link between the subscription act and the initialisation act.

The removable support could take different technical solutions to cope with the constraints relative to the car environment. The removable support is personalised by the Contract Issuer and delivered to the User. After being connected to the corresponding device in the car, the data will be transferred to the DSRC interface via the on-board Computer.

Two possibilities will be offered for the data transfer:

- Once from the removable device to the DSRC module via the On-Board Computer,
- at each insertion of the removable device.

The first possibility will ensure the Contract Issuer and the User that the data are always present inside the DSRC module. Only the DSRC module will be involved later in the process and the same level of security is provided as with the direct initialisation. To improve the security the data inside the removable device could be destroyed or removed to avoid the use of it in a different car.

The second possibility is more convenient for the User. When the device is removed from the car, the data are also removed from the DSRC interface. The account number identifying the User and other data need to be removed to avoid any wrong charging of the User when he moved the support. The security will be reduced because all data will be permanently exchanged between the removable device and the DSRC module through the On-Board Computer.

They are multiple devices, which could provide a good solution for the implementation of this technique:

- Smart card,
- Micro-SIM card like in a GSM phone,
- Contactless smart card,
- Security module.

All these devices offer the same level of capacity and security to fulfil the requirements for an EFC application. The selection of one technology instead an other will be influenced by many different criteria like maturity of the technology, risk of obsolescence, reliability in the car environment, cost… All these criteria are controlled by the car manufacturers and not by the EFC Operator because this interface could be used for other applications not related to the DSRC module like automatic guidance.

11 USE OF A CELLULAR HANDHELD DEVICE FOR FINANCIAL TRANSACTIONS

11.1 Introduction

The cellular handheld device is one of the most popular electronic devices introduced in the daily life of a huge quantity of people in recent years. The cellular penetration rate in many European countries is very high, around 50% or even more for some European countries. It is also possible that in the near future all cars could be equipped by the manufacturers with a cellular device targeted for ITS applications requiring a link between the car and its driver and the infrastructure.

This could be completed by the use of localisation functions using GPS or/and cell_ID and/or network based localisation. Therefore, it could be very interesting to use the cellular device for tolling applications. The envisaged solution will assume that the tolling application does not need a dedicated infrastructure within the tolled area for collecting the fees. All that is required is enough computation power inside the vehicle to continuously determine whether the vehicle is subject to tolling.

This hypothesis has directed development in the area of autonomous systems based on GNSS/CN. This kind of system has been analysed by CARDME during the previous phase of the project and has continued in CARDME-4. Research is still going on in the project INITIATIVE involving many partners across Europe. This type of solution without dedicated infrastructure appeals to several countries in Europe for their road tolling projects.

But the cellular handheld device is also envisaged as solving a different problem that the operators have to face - how to reduce their operating costs. For existing operators, the solution is to introduce an EFC system in their tolling plaza. The efficiency of such a solution is built on the willingness of users to subscribe to this service. Hence, after a given period of growth, all the frequent users are equipped and the attractiveness of the service to new users becomes very low. The number of subscribers, which could be relatively large (millions of users in a country like Italy), represents only a proportion of the total potential users. The issue to be solved is how to automate the transaction at tolling lanes without the need to use dedicated OBUs. Again, the handheld cellular device is seen as a potential candidate for this application.

The technology like GSM, GPRS or UMTS behind the handheld device is not the key element in determining the possibility of offering this service in the toll plaza. The amount of data needed to realise the transaction is so limited that the high capacity offered by the next generation like UMTS is not required. The most important thing is the capability of the handheld device to support m-commerce for local payment applications.

11.2 Use of a cellular handheld device for tolling applications

What is m-commerce?

E-commerce can be defined as electronic shopping via Internet. M-commerce, on the other hand, refers to mobile e-commerce, transactions with monetary value using a mobile terminal, for instance. M-commerce can be divided into online shopping and local payment. In online shopping, a subscriber purchases something remotely. In other words, he is not able to test or touch the product when purchasing it. Local payment, instead, refers to local activity. Thus, the subscriber can, for instance, pay for goods at the cashier’s desk of a store, with a mobile phone. These two types of m-commerce can complement each other, for example, when the subscriber books cinema tickets by online m-commerce, and pays for them locally at the theatre using a mobile terminal. One of the differences between these two types of m-commerce is that online shopping uses GSM, GPRS or UMTS networks and mostly WAP technology, whereas local payment can utilise either Bluetooth or Wireless LAN technologies in addition to SMS, for instance.

In local payment the user's SIM card in his mobile phone functions as an electronic purse. Technically this can be implemented either in the SIM card in the phone or in the network server. When using local payment, the payer is close to the service. The service can be manned, at kiosks, grocery stores or petrol stations, or unmanned with vending machines, ticket readers or a parking house. One of the main benefits of local payment is the riddance of different cards and tickets, and coins in some cases.

11.3 Applications to Road Tolling

Cellular handheld device alone

For road tolling application on existing toll plazas, the cellular handheld device could have two functions: identification of the vehicle to be tolled and the settlement of the transaction.

The identification of the vehicle to be tolled raise some technical problems difficult to be solved by using cellular handheld device only:

- Localisation,
- Number of cell phones in a car,
- Classification,

The localisation of the vehicle could not be done by the cellular handheld device alone. A handheld device could provide its position to the network in different ways. The most classical way is to include a GPS receiver in the handheld device. The vehicle should be located in the proper lane to avoid problems with the enforcement of users. The accuracy of the GPS is not sufficient (between 5 and 40 metres) to locate the mobile without ambiguity in a toll plaza.

The others possibilities are to use the capabilities of the cellular and the network itself to locate the mobile:

- TOA (Time Of Arrival), the localisation is done by the infrastructure.
- TDOA (Time Difference Of Arrival), the localisation is also done by the infrastructure by measuring time differential between a signal's arrival at one cell site vs. another site.
- AOA (Angle Of Arrival), derives "bearing" data from the phase characteristics of radio waves.
- E-OTD (Enhanced-Observed Time Difference), the mobile computes the position by measuring time differences between signals received from different base stations.

These technologies offer a limited accuracy (between 10 and 150 metres).

The use of cellular techniques could bring also a lot of concern if there is more than one cellular phone active in a vehicle arriving in the toll lanes. In this case, it will be impossible to determine which handheld device is owned by the User, who should be charged (in most cases the driver).

The cellular solution is envisaged as an alternative to an OBU, so it will be impossible to obtain from the handheld device information for the classification of the vehicle like claimed class or claimed characteristics. Only automatic classification equipment inside the lane could properly classify the vehicle.

But the main drawback of cellular handheld devices for the EFC operators is that the control of the system is in the hands of the cellular operators and not the EFC operator. This implies that the EFC operator should have agreement with all cellular operators covering the toll plaza to have access to the localisation data. Also, since the cellular networks are not designed for this application, the quality of the localisation data will not be consistent from one operator to the other, depending on the choice of the technology selected and the performance of the handheld device.

So, the difficulties seem too great to be overcome easily, at the time being, using the cellular handheld device alone as a replacement to a DSRC OBU.

Cellular handheld device associated with a DSRC OBU

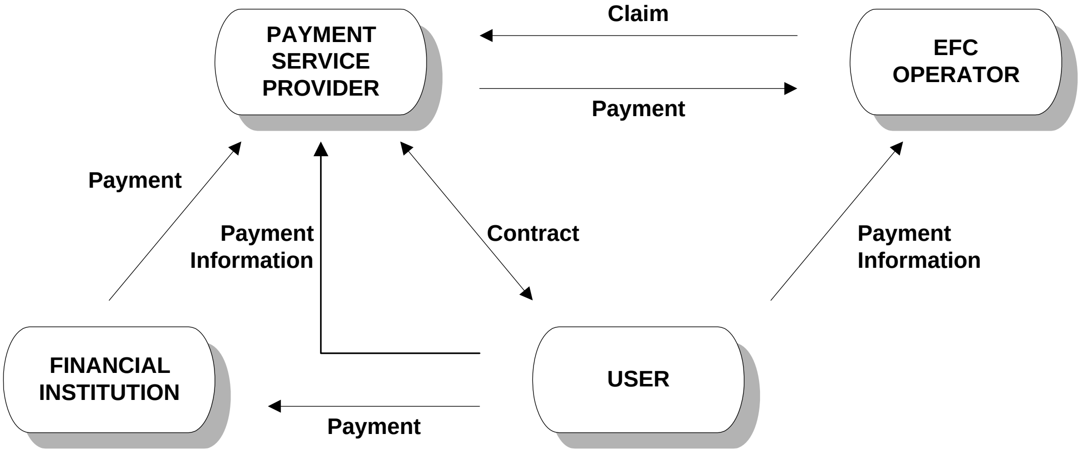
A solution could be a link between a DSRC OBU already installed in the car (DELTA device) and the cellular phone as a payment means. The DSRC OBU will be used to determine the precise location of the vehicle and to correctly match vehicle and the toll to be charged to it.

When the vehicle arrives in a tolling lane, a DSRC transaction will start and a minimum data set will be transmitted to the EFC operator. This data will be sufficient to enable the EFC operator to make a claim to the Payment Service Provider corresponding to the service consumption. The data should enable the identification of PSP, User and proof of service consumption if the application is not based on electronic purse.

At the same time, the handheld device will send information to the PSP to allow him to pay the EFC Operator. Depending of the amount of data to be transferred, the type of transaction and the security level, the vehicle could leave the toll lane while the transaction is still going on in the air. For electronic purses, this will solve the performance issue of this kind of application as seen previously.

The link between the DSRC OBU and the cellular handheld device could be made in a different way. If the cellular is also integrated with the car like the DSRC OBU, the on-board computer will be in charge of the management of data flow between both devices. If the handheld device is not attached to the vehicle, a wireless link between the on-board computer and the handheld device could enable the proper transfer of data via the cellular link. For example, the wireless link could be a Bluetooth link.

A possible functional model for such concept could be the following:



This model involves the same entities as the proposed model for EFC in Deliverable 4.1 for interoperability between EFC operators. The main difference in this model is that the User is transmitting Payment Information both to the EFC Operator and the Payment Service Provider. The transfer of the information to the EFC Operator is to enable the PSP to check the genuineness of the claim of the EFC Operator; and to enable the EFC Operator to start enforcement procedures if he does not receive the corresponding payment.

The role of PSP could be played by different kinds of organisation: commercial card issuer, cellular operator, banks providing credit card or electronic purse, etc… The role of the PSP is to collect data from the User and the EFC Operator to enable the money flow between the User and the EFC Operator.

This solution enables the introduction of the electronic purse for tolling applications without some of the limitations seen in the Part I of this document. The handheld device holds a virtual account for each registered user, which can be used to settle payments. This will particularly reduce the cost of processing micro-payments (a few Euros). These micro-payments are encountered mostly for open systems or road charging schemes.

Availability for interoperable EFC

In this model, interoperability is provided by the acceptance by the EFC Operators of a new payment means issuer. There is a need for an agreement between the PSP and the EFC Operators. This solution could gain acceptance only if most EFC Operators accept most PSP providing such payment solution. In this case an MoU between all involved parties across Europe will help to solve the different issues depending on how the PSP will offer an m-commerce facility to the User: central account, electronic purse, credit card,….

As in the case of commercial cards, the interoperability is supported by the relationship of EFC Operators with PSPs, and not by the contract between EFC Operators. This means that this solution will be feasible only after a significant deployment of m-commerce by the PSP. As with other payment means, the EFC Operator needs to wait for the market to select the best offers for him and his customer.

11.4 Recommendations for use of cellular hand held devices

It has been shown that a package consisting of DSRC OBU and cellular handheld device could provide an EFC solution for users who do not want to subscribe to an EFC Operator. This solution could be introduced in the market after the fulfilment of these conditions:

- availability of DRSC OBU integrated in the car,
- availability of m-commerce solution toward EFC operator,
- large base of equipped users.

Some difficulties in the schedule of introduction of this solution could be foreseen:

- for the time being at least, the carriers remain the keepers of the keys when it comes to m- commerce.
- in order to market m-commerce successfully, major effort needs to be put into convincing the customers about the security and reliability of the service, mainly for the case of application of electronic purses.

The feasibility of the use of cellular handheld device associated with a DSRC OBU as an alternative to the subscription of a contract with an EFC Operator will need further work on definition of contractual frameworks between the involved parties.