



IFM
PROJECT
INTEROPERABLE FARE MANAGEMENT

Inventory of functions, organisational models and economic issues of existing IFM-Systems

Deliverable 4.1

March 2009

Grant Agreement number:	IST-2007-214787
Project acronym:	IFM PROJECT
Project title:	INTEROPERABLE FARE MANAGEMENT PROJECT
Funding Scheme:	Support Action
Project Coordinator:	John Graham Verity Head of Compliance ITSO Limited, United Kingdom
Tel:	+44 121 634 3700
Fax:	+44 121 634 3737
E-mail:	compliance@itso.org.uk
Project website address:	http://www.ifm-project.eu

For further information please contact:

Work package 4 leader

VDV-Kernapplikations GmbH & Co. KG

Elke Fischer (Work package leader)

Phone +49 30 3999322

E-mail: e.fischer@vdv.de

Main authors

VDV-Kernapplikations GmbH & Co. KG

Elke Fischer

Phone +49 30 39993222

Fax +49 221 57979 8222

E-mail: e.fischer@vdv.de

Dr. Joseph Lutgen

Phone +49 221 57979162

Fax +49 221 57979 8162

E-mail: lutgen@vdv.de

For further information on the IFM Project please contact:

Coordination

ITSO Ltd.

Phone +44 121 634 3700

Fax +44 121 634 3737

E-mail: compliance@itso.org.uk

Secretariat

TÜV Rheinland Consulting GmbH

Phone +49 221 806 4165

Fax +49 221 806 3496

E-mail: oliver.althoff@de.tuv.com

Visit the webpage www.ifm-project.eu

List of abbreviations

AFC	Automated Fare Collection
CALYPSO	Electronic Ticketing Standard for (microprocessor) contactless Smartcard, designed by a group of European transit operators
CBO	Central Back Office
CRL	Certificate Revocation Lists
EFM	Electronic Fare Management
EN	European Norm
FM	Fare Management
HOPS	ITSO Back office system
HSM	Cryptographic "Hardware Security Module" it is the secure central element of the Security Management System that generates (and holds) the key pairs and certificates.
IFM	Interoperable Fare Management
ISO	International Organization of Standardization
ITSO	Integrated Transport Smartcard Organisation; UK Standard for nationwide Interoperable Electronic Fare Management
MO	mobile operators
PT	public transport
OTLIS	Consortium of Operators that Specify, Build and Operate the Interoperable Fare Collection System which manages the LisboaViva, 7 Colinas, Viva Viagem and Lisboa Card contactless cards (Lisbon wide Region)
PTO	public transport operator
RKF	Resekortsföreningen i Norden ekonomisk förening, from January 2007 it is Resekortet i Norden AB
TA	Transport Authority
TO	Transport operator
VDV-KA	VDV Core Application, German Standard for nationwide Interoperable Electronic Fare Management
VDV-KA KG	VDV-Kernapplikations GmbH & Co. KG
UITP	International Association of Public Transport

Table of contents

I. Introduction.....	5
I.1 Focus of Analysis.....	5
I.2 Objective.....	6
I.3 Approach.....	6
II. IFM System Architecture.....	8
II.1 Application of National System Standards.....	8
II.1.1 Administration of the standard.....	10
II.1.2 Availability of the specification documents.....	10
II.2 System Architecture.....	11
II.2.1 Realised Roles in the National Systems.....	11
II.2.2 Content of national specifications.....	13
II.2.3 Implementation of Use Cases from the IFM System Architecture Standard.....	16
III. System concept.....	20
III.1 Types of customer media.....	20
III.2 Types of products.....	22
III.3 Interoperability.....	23
IV. Security.....	26
IV.1 Security measures for customer media and their applications.....	26
IV.2 End-to-End Security.....	30
IV.2.1 Authenticity and integrity of data.....	30
IV.2.2 Confidentiality of data.....	31
IV.2.3 Employment of Secure Application Modules.....	31
IV.3 Security management.....	33
IV.3.1 Mechanisms and procedures.....	33
IV.3.2 Monitoring and revocation of rights.....	34
IV.4 Realisation of an IFM wide revocation list management.....	35
IV.5 Liability.....	35
V. General organisational conditions.....	37
V.1 Central Organisations in the National IFM System.....	37
V.2 Legal framework.....	39

I. Introduction

I.1 Focus of Analysis

The objective of the IFM project is to show opportunities how it is possible to get an interoperable ticketing for EU citizens in Europe based on the nationally more or less interoperable working or even set up separate electronic fare management systems (EFM systems).

Of course the fact was also considered, that world wide great EFM systems exist, which handle millions of passengers daily. Such systems are known especially in Asia e.g. from Hong Kong, Singapore, Seoul, Tokyo and in America e.g. from New York and San Francisco.

These systems have been realized by different suppliers e.g. Cubic Transportation Systems, ERG Group and Samsung Group.

These suppliers use different technical smart card platforms like nxp Mifare standard, the Sony standard FeliCa ore ISO/IEC 14443-Type A or B based chips. The running transport applications on the smart card platforms are also different.

Some of them are only used to pay on different transport systems cashless. The different transport systems use their own tariffs independent of the others with different kinds of tariff calculation like uniform tariff or automated fare calculation with check in and check out on gates. An interoperable use of the same "pay card" in different EFM systems in different regions does not exist nowhere, as well as the sale and supply of interoperable electronic tickets for different transport systems in different regions.

The systems in Singapore, New York, Hong Kong and Tokyo have the advantage that they cover particular metropolitan areas with transport usage by millions of passengers per day. The use in sparsely populated regions with a low-developed transportation network is rather absent.

Here's an example from the region of Tokyo where two different chip card systems are in use:

Since 2007, the Tokyo-area private railways, bus companies, and subways implemented PASMO, a smart card solution to replace the existing Passnet magnetic card system. Through collaboration with JR East, passengers can use SUICA cards interchangeably with PASMO cards to ride any railway or bus in the Tokyo metropolitan area. SUICA cards can be used on JR West's ICOCA system as well, whereas PASMO cards cannot. Monthly passes for JR East lines can only be on SUICA cards, while monthly passes for Tokyo Metro can only be on PASMO cards but otherwise, the cards are functionally identical for commuters.

From discussions with representatives of the Japanese Ministry of Transport was expressed that the problem of non-interoperable systems in Japan and other Asian cities also perceived as a disadvantage and that they wants to develop concepts to solve this.

Thus one can conclude that all those problems analyzed in Europe as part of the IFM project which preclude the interoperable use of the relevant European systems, and which in the EU are to be resolved in long term, in these regions of the world generally also exist. This conclusion also UITP pronounced in the position paper "Everybody Local Eeverywhere" dated April 2007 with the statement:

“The vision Everybody Local Everywhere expresses the idea that public transport customers should feel welcome and comfortable anywhere they travel. They should be delivered coherent service with simplified interchanges, thorough information and hassle-free ticketing. When abroad, the travel experience should be as easy as for local travellers. The vision is one of seamless travel and seamless fares, as outlined below.”¹

I.2 Objective

It is intended in this work package to apply an analysis of functions, organisational models and economic issues for the following European fare management systems:

- France
- Germany
- The Netherlands
- Portugal/Lisbon wide Region
- Sweden
- United Kingdom

Representatives of France, Germany, The Netherlands and UK are involved in the IFM project. Sweden and Lisbon were additively included in the analysis, so that a relatively large area of Europe could be considered.

All of them have answered the questionnaire for their national system deserve the thanks of the project.

I.3 Approach

The questions for the analysis were categorised into the following four groups:

- Criteria Group 1: IFM System Architecture
- Criteria Group 2: System Concept
- Criteria Group 3: Security
- Criteria Group 4: General Conditions / Legal Framework

The recipients of this document were asked to give brief descriptions to each of the topics respectively answers to the specific questions contained in it.

In all of the analysed systems there exist Specific National Standards for IFM/EFM. So a good common basis for a migration to an European IFM is given.

The basis for all of the various systems is more or less the common IFM System Architecture described in the standard ISO EN 24014-1 (shown in Figure 1). In particular the role model defines therein which system participant complies which role and who describes the central functions like IFM Manager, Security Manager or registrar.

In Sweden it is planned to confirm with ISO EN 21014-1 in 2009.

¹ Citation UITP position paper Everybody Local Everywhere Electronic Ticketing Interoperability and Fare Management Cooperation, April 2007

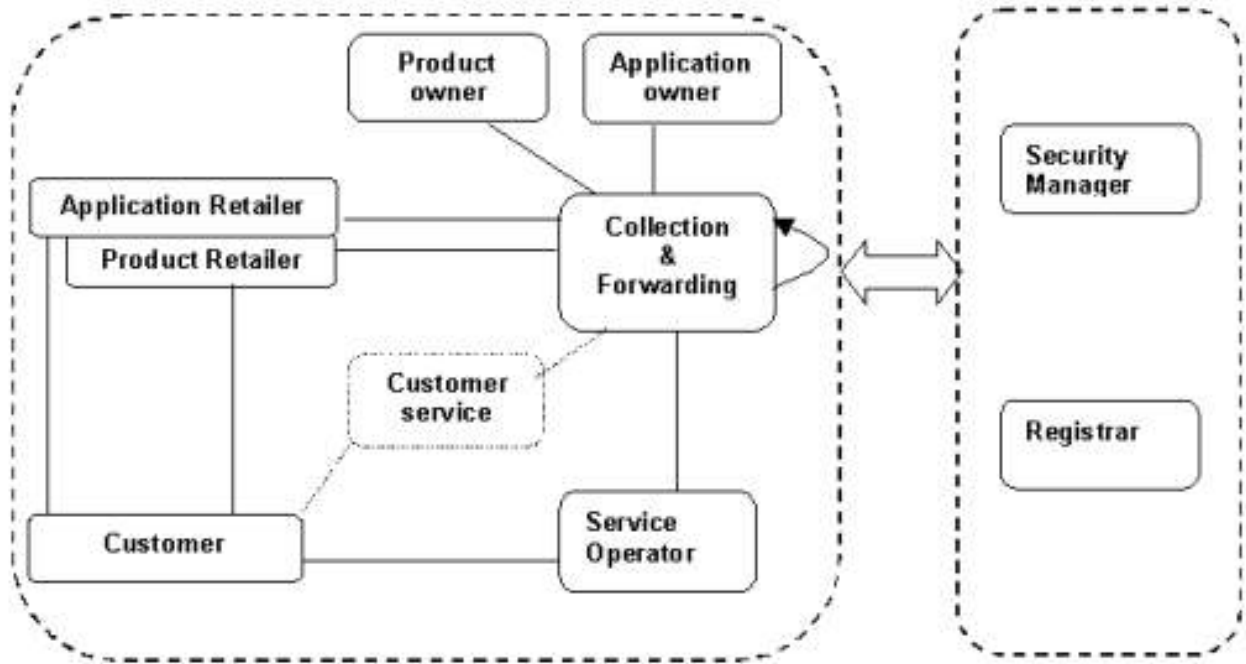


Figure 1 – The two IFM domains (operational and management Entities)²

ISO 24014 has not inspired the existing organisations in France, but the existing organisations could be analysed with ISO 24014.

The Portuguese specification follows the core concepts of IFM ISO EN 24014-1, because it has been designed along the years based on some other specifications, which are also from IFM background (ISO-14904, EN-1545), but they would not say that it follows strictly the IFM since the IFM was only released on 2007Q2.

For the implementation of the VDV Core Application the tasks of the companies in an EFM system will be analysed. Based on this analysis the roles will be classified. So it may be that one company has to take up more than one role. In the national implementation of the VDV Core Application the Security Manager and also the Registrar are assigned to the Application Owner. The security function of blocking list management is also defined as a separate role attributed to the VDV-Kernapplikations GmbH & Co. KG. The Customer Service is seen as part of the Retailer because he rules the payment with the Customer and holds the Payment contracts. The Collection & Forwarding is seen as a part of the reference systems of every separate role.

² Source: ISO/EN 24014-1:2005

II. IFM System Architecture

II.1 Application of National System Standards

In all of the analysed systems of the different countries there exist Specific National Standards for IFM/EFM. So a good common basis for a migration to a European IFM is given. Only the Portuguese one is described rather as an International standard, following the ISO-14904 (Road transport and traffic telematics. Automated fare collection (AFC). Interface specification for the clearing between the operators) with an open implementation of "Enhanced ISO-14904" messages on top of an open source platform which allows any intervenient to interface to the system by this MessIAS Messaging software. It is complemented by EN-1545, Transmodel, INTERCODE, Intertick, etc.

The French systems are termed as regional interoperable applications.

In Germany EFM has started in several regions based on VDV Core application specification. They work together interoperable. The customer can use his medium with application and entitlement also in order to travel within other systems and regions. So interoperability is a matter of migration. Interoperability in one region with more than one participant and more than one back office system is technically the same matter as interoperability between systems in different regions.

The titles of the standard are:

- INTERCODE; ref. AFNOR XP 99-405 (France)
- VDV-Kernapplikation/VDV Core Application for Interoperable Electronic Fare management - ((eTicket Deutschland (Germany)
- Open ticketing Standard (SDOA, Open architecture) for Trans Link Systems (The Netherlands)
- No official title - set of "Regional specifications so called „OTLIS LisboaViva Specification" (Lisbon wide Region)
- RFK-specification (Sweden)
- ITSO (United Kingdom of Great Britain and Northern Ireland)

The development of the standard was funded in part or in full in every country as follows:

- in France by Federal Government Agencies and Transport Operators or their Associations
- in Germany by Federal Government Agencies, Transport Operators or their Associations and industry
- in the Netherlands by Transport Operators or their Associations
- in Portugal/Lisbon by OTLIS Consortium/Association of Transport Operators in partnership with Link Consulting
- in Sweden by Federal Government Agencies and Transport Operators or their Associations
- in the United Kingdom by Federal Government Agencies, Transport Operators or their Associations and industry

Different entities were directly involved in the work on the standards, like members of transport operators or their associations, consultants, members of industry and suppliers.

In France also CERTU (Government research body for urban transport) taken part in the work, in the Netherlands TLS was involved.

This shows, that the work out of the national standards was not only on behalf of the transport operators and authorities.

The leadership structure behind the development of the standard was:

- in France:
steering committee, instituted by agreement between Ministry of Transport, GART (association of transport authorities) and UTP (Association of transport operators)
- in Germany:
Association of German Transport Undertakings - VDV, the organization for Germany's public transport undertakings and rail freight transport companies
- in the Netherlands:
TRANS Link Systems (TLS)
- in Portugal/Lisbon:
OTLIS, Transport Operators Consortium of the Lisbon wide Region (after European projects participation such as ICARE and CALYPSO)
- in Sweden:
RKF (Resekortsföreningen i Norden ekonomisk förening, from January 2007 it is Resekortet i Norden AB)
- in the United Kingdom:
ITSO

The specifications include:

- INTERCODE:
no information
- VDV Core Application (VDV-KA):
 - 1) technical (mostly interface specifications and sequence descriptions at the interface user medium - terminals),
 - 2) security (conception, SAM-specification, PKI, key management within order processes and order forms) ,
 - 3) organization - legal (role model, contract schemes for participants in EFM based on VDV-KA
 - 4) Common Customer interface for self-service processes
- Open ticketing Standard in the Netherlands:
 - 1) SDOA (technical specifications),
 - 2) HRP (rules and regulations),
 - 3) CCHS (Clearing and Settlement)
- OTLIS LisboaViva Specification:
several (non-formalised) work packages existed, Link and the OLIS consortium, involving for example:
 - 1) card data models,
 - 2) security,
 - 3) interfaces between ticketing systems and service centre, 4) service centre functionalities,
 - 4) business plan,
 - 5) card management and issuance,

- 6) customer service and commercial procedures,
 - 7) financial and clearing,
 - 8) reloading over external agents (ATM, Payshop, internet, mobile),
 - 9) certification of new products (cards, readers) and new applications (sub-systems)
- Resekortet:
Today it does not work like an IFM model but hopefully it can be implemented in this model during 2009
- ITSO:
- 1) Technical;
 - 2) Security;
 - 3) Legal

II.1.1 Administration of the standard

The role of the application owner is realized for ITSO, Open ticketing Standard, for Resekortet i Norden AB, the Lisbon wide Region systems and the VDV Core Application. There is also a specific organisation responsible for the maintenance and the continuous development of the national standard. It is ITSO on behalf of UK Government who owns the copyright for the specification. It is TLS in the Netherlands, Resekortet i Norden AB, OTLIS who hold the rights for the specification, and VDV-Kernapplikations GmbH &Co. KG, who holds the rights for the VDV Core Application.

In case of the VDV Core Application a working group of operators respectively consultants and also a Change Request group of manufacturers have been constituted. They discuss changes or complements for the specifications of the VDV Core Application.

In France, the question about a national application owner is not relevant, because France has no national application. Maintenance and continuous development are identified issues, which have not been answered yet.

II.1.2 Availability of the specification documents

LisboaViva Specification is not public, but it is delivered to suppliers who are awarded to implement systems or sub-system implementations. There you do not have to pay an initial fee or license fees for the use of the standard.

In order to get all VDV Core Application specifications it is necessary to order it from the VDV KA KG. A nominal fee is charged by the VDV KA KG. Information about the available documents, the relevant version, and about relevant CRs is available on <http://www.vdv-ka.org>. You do not have to pay an initial fee or license fees for the use of the standard.

In the Netherlands the documents are only available after qualification. During qualification (free of charge) TLS verifies that the applicant has a solid financial background, and is capable of producing for the Dutch market (http://www.translink.nl/media/bijlagen/Qualification_KC3.1.pdf). For transport organisations outside the Netherlands, a comparable procedure is on the way. Additionally, the Security Architecture is only available after signing a NDA.

The OTLIS under conditions to be discussed. An initial fee and license fees for the use of the LisboaViva management system are charged (not to use the specification, but to use the card issuing, management, clearing etc).

There are certain parts on the website of the RFK specification for Resekortet i Norden AB. Administrative regulations, transaction protocols and key management documents are not

public. An initial fee has to be paid. It depends on the users size, volume of transactions etc. (from 2.500 Euro to 10.000 Euro). License fees are also charged for the use of the standard (from 2.500 Euro up to 40.000 Euro).

All the ITS0 specification documents are publicly available. The security part requires a signed NDA. There has not to be paid an initial fee or license fees for the use of the standard.

II.2 System Architecture

The architecture of FM system (in case of France regional interoperable applications) is based on the standard ISO EN 24014-1. In Sweden it is only planned yet to implement the Standard. There are no organisations , which fulfil the roles of the IFM role model today.

II.2.1 Realised Roles in the National Systems

The following roles are realised:

- Application Owner
In France these are TAs, who agree to interoperate the same application and sign a "charte d'interopérabilité", in which they agree on the objectives and on the common rules to manage the application.
In Germany it is the VDV-KA KG.
In Netherlands it is TLS.
In Portugal/Lisbon region currently the only application owner is OTLIS (negotiations with Parking operators, municipalities, mobile operators and banks are going in the direction of additional application owners).
In the UK it is ITS0.
- Application Retailer
In France these are mostly TOs. It can be a special entity, (i.e. joint venture of transport operators for NAVIGO). It can also be the local government as TA for concessionary cards. (e.g. Midi-Pyrénées)
In Germany these are different TAs or PT companies.
In the Netherlands exists one.
In Portugal/Lisbon this concept is foreseen, but not implemented today, except for some functions of an Application Retailer, Product Retailers can provide it based on an on-line application from the Application Owner.
In the UK there are many; a lot of transport operators, but also banks.
- Product Owner
In France, products owners are TAs, when the product is a fare (solely or in common depending upon the product). When the product is not a fare but a payment facility (i.e. bank account orders - we have no stored value), the Product Owner can be a TO or more generally a product retailer.
In Germany these are different TAs or PT companies.
In the Netherlands these are TLS or PTOs.
In Portugal/Lisbon the Product Owner concept is implemented. In that case there are

20 operators, combinations of 2, 3, 4 or any of these 20 operators are in fact the Product Owners.

In the UK there exist 300+ to date; the government for concession scheme; transport operator for commercial scheme; local authority for private application (e.g. library).

- **Product** **Retailer**
 In France, these are TOs, for Navigo annual passes a joint venture of TO. Independent retailers are generally subcontractors of TOs. For departmental networks (coaches), the product retailer often is a different firm from TOs, linked to a TA.
 In Germany these are different TAs or PT companies.
 In the Netherlands these are PTOs.
 Any of the 20 operators in Lisbon region is a Product Retailer, additionally SIBS (ATM banking entity), Payshop (POS operating entity), Link/OTLIS (Internet reloading service operating entity) and also Lisbon Tourism ATX (Lisbon Region tourism agency).
 In UK many work; can include shops.

- **Service** **Operator**
 In France, there may be a difference between the product acceptor and the service operator in some cases. In the case of departmental coaches for example, the ticketing operator (which operates the driver's POS, the validators, the back-office, etc.) and the TO (which operates the coaches) can be different. In Germany these are different PT companies or private transport companies. In German TAs it is possible that a service provider is responsible for the ticket control. In the Netherlands these are the PTOs.
 All the PT operators in Lisbon region and in the future the Parking operators and others being negotiated (not counting on some partners that allow the usage of the card to get discounts: e.g. Zoos, Cinemas).
 in the UK these are many bus, rail, tram operators.

- **Collecting** **&** **Forwarding**
 In France, the function exists, but it is generally decentralised between the different stakeholders.
 It is integrated as part of the several systems in VDV Core application basic systems. All connected PTOs in the Netherlands and M-com play the C&F role. Additionally TLS serves as the central C&F party.
 In the Lisbon region system the concept exists, but it is always part of the role of the Application Owner (OTLIS), with software agents installed in the entities, which perform the previously mentioned roles.
 In the UK these are scheme operators such as local authorities and large transport operators.

- **Registrar**
 The function is realised through the "interoperability charter" and is controlled by the steering committee in France.

Die VDV KA KG realises the role of the Registrar combined with the application management.

TLS also realises the role of the Registrar. This role is still merged with the Application Owner and Security Manager and performed by OTLIS consortium. ITSO realises the role of the Registrar.

- Security Manager

The interoperability charters specify the security agreements. In Ile de France a special contract defines the rules applicable to security management and in case of security crashes according to that contract. TOs are jointly responsible and TA decides, if TOs don't come to an agreement.

In Germany the VDV-KA KG is responsible for the security management. The T-Systems trust centre operates it.

TLS also realises the role of the security manager.

This role today is still merged with the Application Owner and Registrar and is performed by OTLIS consortium.

ITSO also realises the role of the security manager.

The enforcement of the role model is very similar in all the analysed systems/standards. A migration to an European Application standard should be possible without problems.

II.2.2 Content of national specifications

The national standards encompass also data exchange interfaces between reference systems of various roles in France, Germany, the Netherlands, Portugal/Lisbon, Sweden and the UK.

National Standards for data exchange interfaces in the different EFM systems of the EFM participants, independent of their roles in the EFM system, exist within INTERCODE, VDV Core Application, TLS, Resekortet and ITSO, but not within OTLIS LisboaViva Specification (although it follows standards such as ISO-14904, INTERCODE, EN-1545, etc, to build a data exchange specification).

Within ITSO manufacturer standards are used for media interfaces such as Mifare and JCOP.

In France, there do not exist component specifications at a national level; with exception for card/reader subsystem: INTERCODE is only compliant with microprocessor cards and is CALYPSO-compliant.

Within the VDV Core Application exist

- specifications for interfaces between system components using interoperable user media,
- specifications for user medium and SAM
- run charts for the interfaces between terminals and user medium.
- interfaces are also specified between PKI, Key management and component manufacturer
- a back office system specification is planned as complement to the interface specifications for them.

Within TLS exist specifications for:

- Central Clearing House System,
- Fare Media Layout,
- Security Architecture,
- Functional specifications for all Media Access Devices,
- Interface Specifications for: messaging, action listing, reconciliation

Within OTLIS LisboaViva Specification are some technical descriptions and certification guidelines that may be included either in tenders or in system specification. There are no component specifications within ITSO and Resekortet.

ITSO TS 1000 defines the key technical items and interfaces that are required to deliver interoperability, defined in detail as follows

- the end-to-end security system and
- shell layout;
- other elements (e.g. terminals, back office databases) are described only in terms of their interfaces. The business rules that supplement the technical requirements are defined elsewhere.

Based on VDV Core Application, interoperable CiCo systems work between Kreisverkehr Schwäbisch Hall and Nahverkehr Hohenlohe prospectively in Ostalb mobil (authorities in Baden-Württemberg), eTicket systems are implemented in several authorities in North Rhine-Westphalia, Saarbrücken, Ostalb mobil, prospectively in RMV (Hesse), VBB /Berlin-Brandenburg), VVO (Saxonia), HVV, Hamburg, Schleswig-Holstein), MDV (Leipzig, Halle). Interoperability is today regional limited; the interoperability will be managed with extension of new or existing systems.

In the OTLIS LisboaViva Specification only one back end system for IFM management is implemented (and secured messaging system to connect the several operator sub-systems), which is used by the transport authority and all transport companies, who in turn only own the terminals, data pooling systems and some local specific back-offices to manage its network of terminals, account and financial issues and in fact all the operator level issues, but not the overall smartcard and transaction issues. The system is in fact a basis for improving the concept of IFM within the region, with already 2 million cards issued. Improving the concept includes several steps, such as expanding to several other service providers, application and product retailers, and even the way to model banking and mobile phone players into the IFM concept (which we somehow already support). The issue is not so much about changing the concept in future, but contribute and get contributions so that the existing IFM system (and necessary evolutions) gets close to the IFM ISO standard and its evolutions.

ITSO covers only those aspects of the Back Office that impact upon interoperability between HOPS. ITSO has defined the following HOPS functional requirements:

- Loss less communications management (the Message Processor);
- Message data storage;
- ITSO Shell and IPE account management, including Hot list and Action list Processing;
- Asset management;
- Services:

- · Audit trail + Journal,
- · Rule Compliance,
- · Security Monitoring,
- · Backup,
- · Archive.

ITSO, TLS and VDV-KA are applied similarly. They use one application for different systems, which includes products (normally regional, but in case of using payment systems, system wide).

OTLIS is a regional standard.

INTERCODE is a regional standard with various applications in a technically identical user medium. Here we have to verify, to which extent the regional application concept is compatible to the system wide application.

II.2.3 Implementation of Use Cases from the IFM System Architecture Standard

- Certification of Organisations:
It is implemented in ITSO, OTLIS and TLS.
Organisations, which will use VDV-KA, have to be accredited.
No certification is executed in INTERCODE and Resekortet.

- Certification of Application Specifications and Templates.
It is implemented in ITSO and TLS.
The application template is firmly defined in the VDV-KA specification. A Test suite is used to verify the functions of user media and SAMs; a certification laboratory, which will execute tests for all components, is planned.
No certification is executed in OTLIS, Resekortet and generally in INTERCODE. Only in the case of NAVIGO a certification process exists for the card/reader subsystem.

- Certification of Product Specifications and Templates
It is implemented in ITSO, OTLIS and TLS.
No certification is executed in VDV-KA, Resekortet and generally in INTERCODE.

- Registration of Organisations
It is executed in INTERCODE, VDV-KA, ITSO, OTLIS and TLS, not in Resekortet.

- Registration of Components
It is implemented in OTLIS, INTERCODE, TLS, and ITSO. Within VDV-KA only for user media applications and SAMs, terminals only within the organisations.
No registration is executed within Resekortet.

- Registration of Application Templates
It is implemented in INTERCODE and ITSO.
No registration is executed within Resekortet, TLS, OTLIS and VDV-KA.

- Registration of Applications
It is implemented in INTERCODE, TLS, VDV-KA and ITSO.
No registration is executed within Resekortet and OTLIS.

- Registration of Product Templates
It is implemented in INTERCODE, TLS, VDV-KA, OTLIS and ITSO.
No registration is executed within Resekortet.

- Registration of Products
It is implemented in, TLS, VDV-KA, OTLIS and ITSO.

It isn't executed within Resekortet, INTERCODE.

- Dissemination of Application Templates
It is implemented in INTERCODE, TLS and ITSO.
No registration is executed within Resekortet, VDV-KA, OTLIS and VDV-KA.
- Acquisition of Applications
It is implemented in, TLS, VDV-KA, OTLIS and ITSO.
It isn't executed within Resekortet, INTERCODE.
- Termination of Application Templates (regular and forced termination of Application Templates)
It is implemented in ITSO.
It is not implemented in TLS, Resekortet, OTLIS, not yet in VDV-KA (specification is planned in connection with Mobile Ticketing).
For INTERCODE currently only one application template exists per medium. ULYSSE group is defining on a national level the processes for these use cases with multi-application media.
- Termination of Applications
It is implemented in ITSO, TLS, VDV-KA, and OTLIS.
It is not implemented in INTERCODE and Resekortet.
- Management of Products
 - Dissemination of Product Templates
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, and OTLIS, not in Resekortet.
 - Termination of Product Templates (regular and forced termination of Product Templates)
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, OTLIS, not in Resekortet.
 - Management of Action Lists
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, and OTLIS, not in Resekortet.
 - Acquisition of Products
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, and OTLIS, not in Resekortet.
 - Modification of product parameters
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, OTLIS, not in Resekortet.
 - Termination of Products (regular and forced termination of Products)
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, OTLIS, not in Resekortet.

- Use and Inspection of Products
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, and OTLIS, not in Resekortet.

- Collection of data
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, OTLIS, not in Resekortet.

- Forwarding data
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, OTLIS, not in Resekortet.

- Generation and distribution of clearing reports
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, OTLIS, not in Resekortet.

- Monitoring of IFM processes and IFM data life cycle
It is implemented in ITSO, TLS and VDV-KA, not in INTERCODE, OTLIS and Resekortet.

- Management of IFM security keys
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, OTLIS, not in Resekortet.

- Management of security lists
 - It is implemented in INTERCODE, ITSO, TLS, VDV-KA, and OTLIS, not in Resekortet.

 - Updating security list data
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, not in Resekortet.

 - Add or remove a component to/from security list
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, not in OTLIS and Resekortet.

 - Add or remove an application template to/from security list
It is implemented in INTERCODE and ITSO, not in VDV-KA, TLS, OTLIS and Resekortet.

 - Add or remove an application to/from security list
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, not in, OTLIS and Resekortet.

 - Add or remove a product template to/from security list
It is implemented in INTERCODE, TLS and ITSO, not in VDV-KA, OTLIS and Resekortet.

 - Add or remove a product to/from security list
It is implemented in INTERCODE, ITSO, TLS, VDV-KA, not in OTLIS and Resekortet.

- Management of Customer Service

It is implemented in INTERCODE, ITSO, TLS, VDV-KA, not in OTLIS and Resekortet.

The realisation of the use cases is very similarly in all the analysed systems/standards. A migration to a European Application standard should be possible without problems.

In France a national standard to register TAs has been defined; for other objects, registration is made on a regional level. The community administrates documents that register the products (REFOCO, referential functional common) and their business rules (DMO document de mise en oeuvre) and the corresponding technical specifications (Instanciations). Depending upon the case, these documents are administrated by SNCF or by independent companies.

In Germany are all organisations/entities which are operating in the system or which are taking up a role get a unique identity. The numbering system for components, applications, products/entitlements/SAMs behind the Organisation_ID is administrated by the entities on their own.

III. System concept

III.1 Types of customer media

- INTERCODE
 - For interoperability only **micro-processor cryptographic media** are accepted. Memory cards can complement them as non-interoperable media, if one partner decides so. Most cards are dual interface cards, but single contactless interface cards now appear. Global Platform Multi-application media are not used yet, but the process defined by ULYSSE group could apply to it. Calypso BMS (Billettique monetique service) cards can be used. They contain a bank-operated e-purse, and can host different applications.
 - Experiments with mobiles are on-going in different IFMs, according to the organisation scheme defined by the ULYSSE group joining TOs and MOs (mobile operators), Technically: using SIM card as secure element, CALYPSO interface, NFC and Global platform standards
 - dual interface contactless & USB devices have been tested

- VDV-KA
 - **Micro-processor cards with crypto-co-processor**
 - Multi application possible (GeldKarte with VDV-KA in use)
 - Dual Interface cards possible (only contactless IF is used)
 - NFC-Mobiles in preparation (specification for application download is to define, KA-specifications to OTA download eTickets are available)
 - PDA may be

- TLS
 - Simple memory cards
 - Micro-processor personalized cards (Dual Interface) for regular customers (using both contactless and contact interfaces. E.g. contact interface is used to reload the card over ATM network)
 - Only Mifare Classic 4k and Mifare UltraLight are currently supported

- OTLIS
 - Simple memory cards , for interoperable products for occasional customers and tourists
 - Micro-processor cards
 - multiapplication possible
 - In the near future NFC mobile phones, individual radio-frequency based parking devices, Paypass + multi-services cards, etc. Only a prototype OTA system for the moment, going for pilot
 - In the future individual RF parking devices should be used.

- Resekortet
 - Simple memory cards

- ITSO
 - Simple memory cards
 - Micro-processor cards
 - **Micro-processor cards with crypto-co-processor**
 - multiapplication possible
 - Dual Interface cards possible (only contactless IF is used)
 - NFC-Mobiles may be use as customer medium (no OTA use case)

In none of the different systems all card types are used.

In order to guarantee interoperable applications it is necessary to use micro processor media with crypto-co-processors. Elementary memory cards are chosen for media, which are used only regional.

Multiple types of media are supported in operation within INTERCODE, ITSO, TLS, VDV-KA, and OTLIS, not in Resekortet.

In VDV-KA they have to fulfil the Testsuite tests and it is postulated to contribute a hardware certification and manufacturer declaration.

In TLS the implementation of the applications on the Contactless Smart Card is defined.

In OTLIS in addition to the common data model, as a basis for interoperability, also the concept of Interoperability Embedded Framework stack is used as a way to quickly adapt each component to use either a new type of customer media, reader or even application data / rules and each system/component must be submitted to a "Cross-test and certification process".

Multiple applications are supported in operation within OTLIS and ITSO.

All EFM participants within INTERCODE, ITSO, TLS, VDV-KA, OTLIS, not in Resekortet, support the technologies of the customer media.

Customers can use their media in all kinds of transportation in the EFM area.

Within VDV-KA: If it is defined so - normally for interoperable product templates and for any product template in a region.

The customer media and its public transportation applications can be used in future in connection with the Internet:

- The OTA process defined by ULYSSE group could also be used for remote processing of other media via the internet (e.g., via USB interface)
- The use of PC with reader is planned, the use of ACTION Lists for selected EFS-Product templates is in discussion within VDV-KA
- The most relevant use case in place is the reloading of the customer media via the internet, by using a contact or contactless reader connected to the browser or even without reader by receiving the product by green list (similar to ACTION LIST) within OTLIS
- Internet retailer creates ACTION LIST which is sent to selected Point of Service Terminal to load media on next presentation within ITSO

- Action Listing: products or e-purse top-up can (end 2009) be bought on the Internet, and picked up at devices. Website can also be used to see status of medium, products and last 10 transactions within TLS
- Action list can be use for loading values and products on the card in Resekortet.

All of this type should be also possible within a European solution.

Customer Media and Applications are issued of

- Public transport authorities within:
VDV-KA, INTERCODE, OTLIS, ITSO, Resekortet
- Public transport companies within
TLS, VDV-KA, OTLIS, INTERCODE, ITSO, Resekortet
- Local communities
INTERCODE, ITSO, Resekortet
- Others within
INTERCODE (joint ventures of TAs), OTLIS (Tourism Agency), TLS (TLS), ITSO (any Licensed Operator holding commercial agreement with Operator or Authority)

All of these types of issuing should be also possible within an European solution.

Usually customers request their media at transport operators' desks or via PTA's sales organisations (may be also via internet service).

- There is a business model and clearing model that the OTLIS application owner processes giving the adequate income to each transport operator. Customers can request theirs card and pick it up at the station later, or at home or even get it on the moment.
- It can be issued as personalised or anonymous card at any Point of Service set up to load ITSO onto cards.

III.2 Types of products

- Electronic Tickets (issuing of all relevant ticket data)
 - single tickets within
VDV-KA, INTERCODE, OTLIS, ITSO, Resekortet, TLS
 - different types of season tickets within
VDV-KA, INTERCODE, OTLIS, ITSO, Resekortet, TLS
 - subscription season tickets within
VDV-KA, INTERCODE, OTLIS, ITSO, Resekortet, TLS
 - Control must be possible electronically within
VDV-KA, INTERCODE, OTLIS, ITSO, Resekortet, TLS

Also: Zonal, km-based, flat fee, subscription fee+discount, time+discount, km+discount, stored value, charge to account, loyalty, area ticket, carnet, voucher, tolling, multi-journey

- Electronic Tickets with Check-In within VDV-KA possible, INTERCODE, OTLIS, ITSO, Resekortet, TLS
 - transaction "stamps" are generated in every case in terminals and with exception of ITSO and TLS also in the medium
 - the "stamps" are stored in the medium, in terminals and back office in every case

- Entitlements for automatic electronic fare calculation within VDV-KA and ITSO (stored value, charge to account), OTLIS (generic electronic purse for PT, charge to credit card is being implemented), Resekortet and TLS
 - transaction "stamps" are generated in every case in terminals and with exception of ITSO and TLS also in the medium
 - the "stamps" are stored in the medium, in terminals and back office in every case

Multiple products (electronic tickets, electronic tickets with check-In, entitlements for automatic electronic fare calculation) are supported in single customer media or at individual terminals in operation in every case with exception of INTERCODE.

The product information is stored in the media structured in accordance with EN 1545-1/-2 with exception of Resekortet.

The following methods of payment are supported:

- cash within VDV-KA, INTERCODE, OTLIS, Resekortet, TLS
- electronic payment (credit, debit cards) within VDV-KA, INTERCODE, OTLIS, Resekortet, TLS
- use of national electronic purses within VDV-KA, INTERCODE, ITSO, Resekortet, TLS
- use of procedures for PT account settlement within VDV-KA, OTLIS, ITSO, Resekortet, TLS
- use of stored travel values in the PT application in the medium within VDV-KA, OTLIS, ITSO, Resekortet

Public transport accounts or stored travel values are accepted nationwide within VDV-KA, ITSO, Resekortet, and TLS.

Different modes of payment have been implemented: not everywhere PT proprietary modes and not everywhere nation wide accepted modes.

Topic: The customer's payment mode is not realisable Europe wide.

III.3 Interoperability

Data are generated in the processes, which allow or support the clearing of transport services delivered by possibly multiple transport operators during individual trips of customers. Validation data help adjusting periodically the relevant part of the fare that goes to each operator.

There exist products, which can be used in all means of transportation in the whole IFM system in all cases with exception of Resekortet.

Different tariff systems exist in all of the IFM systems.

Stored travel values are usable at and can be loaded by all EFM participants in all cases with exception of INTERCODE.

PT accounts are usable for all EFM participants in all cases with exception of INTERCODE and Resekortet.

There is, or it is planned to have uniform Man-Machine-Interfaces (MMI) nationwide within ITSO, TLS and VDV-KA.

Information and service supported by all EFM participants within ITSO, INTERCODE, Resekortet, TLS and VDV-KA.

Interoperability between local and long-distance traffic is supported within ITSO, TLS and VDV-KA and it is starting to be addressed currently in OTLIS.

For INTERCODE the general answer is NO, because long distance usually requires seat-reservation, and media that are readable by the customer, exception can exist (e.g., regional season tickets can be accepted in long distance trains with no seat reservation at all or with only the seat reservation added).

System implementations

The following types of systems are implemented:

- Manual pre-selection, i.e. storage of predefined, complete tickets in Germany, France, Portugal/Lisbon, UK, Sweden and the Netherlands
- Automated fare collection, e.g. Check-In / Check-Out or Check-In only in Germany, Portugal/Lisbon, UK, Sweden and the Netherlands
- Combinations of the above in Germany, Portugal/Lisbon, UK, Sweden and the Netherlands
- Systems with entry gates in France (partial), Portugal/Lisbon, UK, Sweden and the Netherlands

Other variants are implemented in Portugal/Lisbon in form of some special pre-selections, which are defined for suburban and national railways and in the Netherlands in form of open-closed hybrid entries and validators on vehicle or platform.

IV. Security

Security management, except for key management, is decentralised in French systems based on the standard INTERCODE. Details are not described.

In general it is to determine, that the security concept of the national systems based on very different concepts.

Security (signature) by the medium itself is only realised in the VDV KA. The signature of the medium supports an audit of transactions over all different system components and systems to the last recipient of this transaction, who has to evaluate and profit in its system.

The authentication between system components the other hand, is postulated in different execution in more or less all of the systems.

IV.1 Security measures for customer media and their applications

Identification

The unique identification of all objects and participating entities (including transactions between terminals and media/applications) is guaranteed within VDV-KA, OTLIS, ITSO and TLS

Note:

Unique identifiers are may be generated decentralized!

In Lisbon unique identifiers are also generated decentralized, but they are still unique because they are build based on structuring identifiers based on registration data fields (different for each card, SAM, terminal, operator, etc, and complemented by date/time stamps.

INTERCODE and Resekortet are working decentralise.

Access rights

Ownership and access rights of the data stored in the customer medium and application are clearly defined in each specification.

Following access rights are reserved for the different roles and participants:

- CALYPSO-SAM:
 - keys are used to authorise the card modification or to generate and verify data authenticity or to limit the number of operations up to a „reload“ ,
 - keys are used to manage
 - Calypso card transaction (e.g. reloading card, or validation card)
 - Data certificates used in contactless tickets
- VDV-KA:
 - read media data always,
 - read customer profile and PIN with asymmetric authentication or PIN
 - write static data only by object (application/products) owner ,
 - write transaction data with symmetric authentication

role specific and functional depending access rights to the back office data is not defined by VDV-KA

- OTLIS:
The system is based on an extension of CALYPSO SAM principles (see above), which besides all the Calypso security features, includes also specific keys to sign data certificates in side cards and also transactions sent to the central system.
There are 3 levels of access rights: load, validate, control.
Besides that at the central system / service centre other security features exist: there is a concept named Entity Mks which defines one bit for each entity, and allows this entity to perform that action when it's bit is set to 1.
Additionally also there is a set of rules to access data, depending on being source, owner or viewer of data.
- ITSO:
Access rights are all passed to Operator; defined by Commercial / Legal constraints of each operator. Not defined by ITSO
- Resekortet:
The electronic purse is accessible to all participants.
All other accesses are defined by each PTA.
- TLS:
The Card Issuer (TLS) can initialise and personalise the cards; no differentiation between participants.

The access to personal customer data in public transport applications in customer media is protected by:

- VDV-KA:
PIN or asymmetric authentication
- OTLIS:
Calypso based PIN with 3 retries
- ITSO:
Access rights are all passed to Operator; defined by Commercial / Legal constraints of each operator. Not defined by ITSO.
- Resekortet:
Only accessible for participants who possess the security keys.
- TLS:
No customer data available in the application. (only birth date and Holder Profile as trait)

In the case of multi-application customer media the following mechanisms are realised to prevent unauthorized access of other applications to the public transport application:

- VDV-KA:
PT application has an own security access condition with own certificates and keys.
- OTLIS:
There are sets of different keys for different applications, although the "other applications" are still not rolled out.
- ITSO:
Media Issuer is responsible and must provide customer interface.
- Resekortet:
not relevant
- TLS:
Each application has its own set of keys and physical location in the medium.

Access rights are used very different in the systems. The Owners have written access rights in every system. Keys certificates specify the access conditions.

Authentication

A mutual authentication between customer media and terminals based on a cryptographic challenge-response algorithm is realised in every case.

- CALYPSO-SAM:
keys are used to authorise the card modification or to generate and verify data authenticity.
- VDV-KA:
 - RSA (to issue objects with keys or to change static data by owners)
 - 3DES (to read objects authentically and execute transactions)
 - PIN is defined, to read customer profile data
- OTLIS:
It follows the CALYPSO security protocols.
- ITSO:
For relevant media only; 3-DES and RSA.
- Resekortet:
DES
- TLS:
CRYPTO1 (Mifare)

Authentication is used in every specification. There are different methods used from CRYPTO1 (which is broken) to 3 DES and RSA.

Data integrity

Following mechanisms are implemented to ensure the integrity of data exchanged between customer media and terminals:

- VDV-KA:
 - Each Transaction is signed by user medium with two MACs (Retailer/Product owner/Application owner).
 - Each service operator Transaction is signed by SAM with MAC to prove it during the next transaction
 - Data exchange between back office systems is executed with standard procedures

- OTLIS:

Besides the ratification mechanisms supported by CALYPSO protocols and cards, for memory cards there are BACKUP and CERTIFICATE zones in the cards and software on the Interoperability Embedded Framework that guarantee the integrity of data both from the security perspective but also from the transactional point of view (i.e. allowing that a card in which the transaction was interrupted comes to a stable status for the next transaction at any terminal).

Each service operator Transaction is signed by SAM with MAC

- ITSO:

Each Transaction is signed by SAM (equivalent to MAC)

- Resekortet:

Implemented by each PTA/suppliers system.

- TLS:

ISO-14443-A

The mechanisms implemented to ensure the integrity of data exchanged between customer media and terminals are different in every specification.

Evaluation of customer media

The components used for customer media possess evaluations according to ITSEC-Criteria or Common Criteria in

- VDV-KA:
 - User medium EAL4+(compliance declaration of the manufacturer)
 - SAM EAL5

- OTLIS:

No information

The components used for customer media do not possess evaluations according to ITSEC-Criteria or Common Criteria in

- ITSO, Resekortet, TLS

IV.2 End-to-End Security

IV.2.1 Authenticity and integrity of data

Role specific protection of the authenticity and integrity of the data generated and transported in the system implemented for each participating organisation is intended in

- VDV-KA by MAC verification with master keys (Mac is executed by role specific application and product keys in the medium)
- OTLIS by MAC creation on de terminals based on the SAMs and verification on de service centre SAMs using special keys of the SAMs, which allow the full tracking of the transactions generated in terminals + cards at the service centre
- ITSO by signed transactions by SAM and encrypted. Certificates used as applicable.
- Resekortet by implemented methods by each PTA/supplier's system
- TLS by PKI for authenticity and integrity of messaging, role based authenticity is implemented in CBO

It is ensured that objects of value (e.g. transactions) can only be generated in cooperation with an authentic customer medium by mutual authentication between NM an SAM in terminals/ by checking directory seal on media directory/check for authentic customer medium in CBO.

Counterfeited, manipulated or repeated messages or transaction in the system cab are identified and filtered out by methods like:

- use and check of different counters and MAC sign
- detection of repeated messages and counterfeit and manipulated messages due to the fact that ALL the messages/transactions are signed. These are put in quarantine.
- checking seal; analysing back office transaction records for trends
- CBO

The authenticity of transactions can be secured independently by all entities involved in the data processing through

- use and check of different counters and MAC sign
- all transactions signed by SAM and with a sequence number generated by SAM.

The authenticity of transactions can be secured in other cases through

- the SAM and transaction signing mechanism global and independent from the role managed by the service centre (application owner, today).

Secure processes (authentication, Keys, MAC verification) for the inspection of transactions (e.g. validation of tickets, In-Out transactions) are implemented within VDV-KA, OTLIS, ITSO, Resekortet, and TLS.

The transactions are securely stored until confirmation of receipt by receiver back office systems in every case through

- collection and forward mechanisms involving protocols (based on the ISO-14904 framework) and software that guarantees the delivery of messages until they are confirmed by
- resenting until ACK (or NACK) received

The completeness of transmitted data (e.g. sets of transactions) can be verified by authorised entities through

- detecting mechanism/fraud detection mechanisms,
- SAM summed and signed transactions (even photos!),
- audit register and transaction and file sequence numbers checked in CBO, reconciliation via interfaces between CBO and PTO BO.

IV.2.2 Confidentiality of data

Following mechanisms or procedures are implemented to assure the confidentiality of data transported between the following entities:

- Terminals and back office systems:
Not specified (security via end-to-end security of transactions).
- Different back office systems
 - Messages between back-offices and service centre, are transmitted via MessIAS (which implements the ISO-14904) and for that several mechanisms are implemented from authenticity, integrity, confidentiality and non-repudiation, and also authentication (between components)
 - Secure messaging using certificates
- Customer media and terminals
RSA, 3DES, secure messaging using certificates; with media only those media supporting secure messaging

IV.2.3 Employment of Secure Application Modules

SAM Deployment

Secure Application Modules (SAMs) in shape of a micro-processor smart card used in VDV-KA (KA-SAM), INTERCODE (Calypso SAM), TLS, not in Resekortet.

In OTLIS the SAM is a Calypso SAM, complemented by an Embedded Software Agent which acts as the proxy of the SAM to the service centre.

SAMs are employed in different terminal types like

- Personalization/ issuing terminals (Card production environment)
- Selling/ vending machines
- Reloading terminals
- Validators
- Check Terminals with fare calculation
- Control terminals

The SAMs are employed only in terminals within VDV-KA. The Terminal can be divided (terminal component, OTA or Internet). They are valid for 5 years. Keys and key counter are reloadable. Retailer SAMs need activation with an operator key after they were without current.

The SAMs are employed in terminals within OTLIS and also on the service centre to verify transactions. The Terminal can be divided (terminal component, OTA or Internet). The SAMs may have a temporal validity period (configurable) but in particular they have a "ceiling" which limits the number of transactions/products which can be loaded on cards in an off-line mode, after which the ceiling value must be reset, by the service centre (security management role).

It includes 4 types of SAM: Initialisation, Issuing, Reloading, and Validation. Based on those SAMs (which have counters), one can generate SAMs to install in equipments. All the SAMs are registered, or, if not, after first transaction received, a blocking protocol is activated, until security manager accepts. Keys and limits can be updated by using service centre SAMs to generate cryptograms, which are sent to terminal SAMs to perform these updates. Also central SAMs are used to verify transactions and to perform reloading (or debiting) transactions for ATM or Internet

The SAMs are employed in all point of service and back office modules within ITSO. They are warranted for 5 years; operator can set parameter (>90days) where SAM will shut down and lock if not connected to its own back office. (Normally set for 2-7days).

The SAMs are employed in front-end devices, PTO back office systems, CBO within TLS. They are limited # of authentication sets and configurable, CRL.

Evaluation of SAMs

The components used for SAMs possess following evaluations according to ITSEC-Criteria or Common Criteria:

KA SAM: EAL5+ by BSI PP-0002
ITSO SAM: CC EAL4+, profile 9911

The others aren't evaluated.

SAM security mechanisms and features

All SAMs support the following features:

- secure storage and usage of all cryptographic keys
- cryptographic protection of the communication between customer media and terminals
- Processes for the loading of certificates and cryptographic keys (e.g. secure distribution of new keys to SAMs already in the field)
- storage and usage of security relevant counters in connection with the usage of cryptographic keys.

As measures against the unauthorised removal of a fully functional SAM from a system component are realized:

- usage of an operator activation key after removal of a SAM out of his place (KA SAM)
- Blacklisting SAMs
- Usage of parameter (>90days) where SAM will shut down and lock if not connected to its own back office. (Normally set for 2-7days) (ISAM).

Procurement

Standard ordering processes for the delivery of SAMs according to the configuration of individual participants are implemented within VDV-KA, OTLIS, ITSO, and TLS, not within Resekortet.

No information about INTERCODE.

IV.3 Security management

IV.3.1 Mechanisms and procedures

Security services are carried out by certified Trust Centres only within

- VDV-KA: T-Systems
- ITSO: UK secure site to Banking Regulations.

Public key infrastructure implemented only within

- VDV-KA: for the issuance of cryptographic keys, for the purposes of authentication
- Resekortet: Managed by Resekortet i Norden
- TLS for data integrity of data to and from front end devices (i.e. Blacklist, transactions, audit registers).

Key management systems for the generation, archiving and distribution of cryptographic keys are realized within:

- VDV-KA: operators purchase role specific keys from T-Systems HSM system
- OTLIS: The Security Management is a kind of CALYPSO enhanced architecture. The keys generation (half-master keys) are generated according to CALYPSO security architecture specification and stored in "SAM for generation of SAMs".
- ITSO: bespoke Registrar system linked to HSM
- TLS: HSM and management system around it.

Migration strategies for cryptographic keys and, in case employed, for the public key infrastructure are implemented only within:

- VDV-KA: back-up keys, key changes, Root CA
- TLS: Key rollover for 3 different generations

Measures implemented to guarantee the secure loading of keys into the system out of the key management system within:

- VDV-KA: Masterkeys are available only in the Key Management System and at the discretion of the key owner; numbering Keys are delivered from the Key Management System to the SAMs by way of unique, non-reusable, SAM-specific encrypted messages implementing end-to-end security.
- OTLIS: the master keys are stored in safes in separate halves and access is governed by a protocol
- ITSO: SAM confirms transaction and signs
- TLS: There are multiple layers of symmetric keys for key distribution

Ordering and distribution of cryptographic keys are only possible by entities specifically authorised by a central security management for these processes

- VDV-KA: Only companies, accredited by the KA KG, get keys according to their contractual roles, after signing a contract with the Key manager T Systems. Asset Managers are allowed by T-systems to get cryptograms.
- OTLIS: The service centre functionalities as "SAM management" are only accessible by some parties, with all the activities being monitored, and which allows performing this kind of key management transactions.
- ITSO: Asset Managers are validated by Banking Regulations and have own SAMs.
- TLS: It will be authorised by the Scheme provider, executed by the security officer.

Measures employed to minimise the impact of possible compromise of cryptographic keys within

- VDV-KA through: key diversification and groups of keys (key generations and back-up keys, key region), different keys for different functionalities and roles, different CA authorities
- OTLIS through: implemented mechanisms, being that all the keys are used in a diversified way based on SAM and card serial number.
- ITSO through: Multiple diversification including random number generation and sequence
- TLS through: key diversification and different keys for different functionality

IV.3.2 Monitoring and revocation of rights

Transactions are logged and monitored for possible unauthorised activity:

- VDV-KA: The product owner has to do it for every product specific entitlement; the retailer has to do it for his retailed entitlements.
- OTLIS: Card transaction at terminals is collected. Back-office transactions (or "activities") at service centre are all logged and associated to entity and person, and no data is deleted on the system; everything goes into historical data after modifying.
- ITSO: All transactions held for >12 months for operators to implement monitoring.
- Resekortet: It is implemented by each PTA/suppliers system
- TLS: Validation rules at CBO

The possibility to revoke certificates within the PKI is executed within:

- VDV-KA with a blocking procedure
- ITSO: with a centrally generated key roll-over
- TLS: CRL pushed from CBO to PTOs.

The possibility to revoke individual cryptographic keys is executed only within:

- VDV-KA: with a blocking list and termination of the keys and activation of back-up keys
- ITSO: with an instruction to SAM; also protected by original key roll-over

The possibility to block individual SAMs is executed within:

- VDV-KA: with a blocking list - all objects created with this SAM will be blocked
- OTLIS: The SAM Management functions detect transaction by transaction the SAM status, giving alerts, and based on this error status it is possible for the security manager to perform action on a specific SAM or groups of SAMs, either to update keys, issue new keys, block SAM, etc
- ITSO: with instruction to SAM; also protected by original key roll-over
- TLS: with a device blacklisting and CRL

IV.4 Realisation of an IFM wide revocation list management

For the following objects revocation lists are implemented:

- No information about INTERCODE.
- Customer Media: within OTLIS, ITSO, TLS
- Application templates within ITSO,
- Applications: within VDV-KA, ITSO, TLS
- Product templates: within OTLIS, ITSO
- Products: within VDV-KA, OTLIS, ITSO, TLS
- Cryptographic keys: within VDV-KA, ITSO, Resekortet, TLS
- Certificates: within VDV-KA, ITSO, TLS
- SAMs within VDV-KA, OTLIS, ITSO, TLS
- Organisations (EFM participants): within VDV-KA, ITSO, Resekortet, TLS
- Terminals: within OTLIS, ITSO, TLS

In all systems are blocking mechanism are available. The reasons are to find out in the different systems why object is blocked or not blocked.

IV.5 Liability

There are liability agreements regarding the Security Management within:

- VDV-KA by a basic agreement between VDV-KA KG and the Security management operator; single supply contracts made with operators and security management operator
- ITSO, by an Operator License, requires that all operators share liability

- Resekortet: draft is available

Following parties takes over the liability:

- VDV-KA: security management operator T-Systems
- ITSO: Operators

V. General organisational conditions

V.1 Central Organisations in the National FM System

- No national FM System in France; FMs are regional; Two discussion platforms: PREDIM (plateforme de recherche et d'expérimentation intermodale) and CN03 (commission de normalisation)
- VDV-KA KG as Application owner, registrar, responsible as security manager, Security list operator in preparation
- OTLIS with some relation with governmental department (secretary of state)
- ITSO: specification, SAM, security management, Registrar
- SLTF Resekortet i Sverige AB. Provision of the Technical Specification, granting a licence for the brand name "Resekortet", implementation of the "e-purse", conducting a survey of clearing systems, setting up and administering an advisory body for the Travel Card Co-operation
- TLS: Security, Registrar, Scheme Provider, Certification, Clearing and Settlement, Specification development, Card Issuer, Float manager, Customer Service

Conditions of participation in the National FM System are:

- VDV-KA: i to sign a participation contract with VDV-KA KG (role specific)
- ITSO: Government mandated for Concession Travel, and National Rail; otherwise commercial decisions
- Resekortet: participants have to fulfil the implementation of the agreement requirements
- TLS: Check-to-Connect

Central certification procedures for EFM components are implemented within:

- VDV-KA: a certification lab for all component is planned, existing: user medium and SAM functional tests with test suite, Terminal tests over prepared user media
- OTLIS: all system components from cards to complete terminal solutions are implemented and certificated in a "certification lab", which procedures still need to be better formalised eventually aligned with standards
- ITSO: All media, point of services and back office systems interfacing to ITSO must be certificated to spec and tested for interoperability.
- TLS: All components are certified against the Openticketing Standard.

Obligations to certify components for participation in the IFM system exist within:

- VDV-KA not yet
- OTLIS: PT operators consortium
- ITSO
- TLS

Initiators for the IFM System are

- In Germany: transport authorities, larger transport companies, regional PTOs

- In France: transport authorities will decide, often upon suggestion of transport operators
- In Portugal/Lisbon: OTLIS: PT operators consortium
- In UK: government, transport operators, suppliers
- In Sweden: The Swedish PTA's and SJ
- In the Netherlands: larger transport companies. Ease of use, security, reporting and resource management

Who obligates companies to take part in the IFM System?

- VDV-KA: decision of PT authorities, PT companies
- INTERCODE: transport authorities
- OTLIS: in fact operators are not obliged, but instead they only have to choose or not to follow the "recommendation" and specifications from OTLIS, as a basic requirement to be part of the interoperable fare solution (because intermodal fares are an unavoidable reality!)
- ITSO: Government mandated for Concession Travel, and National Rail; otherwise commercial decisions
- Resekortet: each of the participants
- TLS: Transport authorities. They can demand the concessionaire to take part in the IFM. The national transport authority (minister) ultimately decides on the abolishment of the paper ticket based system.

Who decides about possible migration steps?

- VDV-KA KG with their limited partners
- INTERCODE steering committee where all implied transport authorities stand. This steering committee may be chaired by the regional authority or by the capital city.
- OTLIS in agreement with Operators, sometimes co-financed by the government
- ITSO: commercial decision by operator or public transport authority, often based on franchise obligations
- Resekortet i Norden
- TLS: transport authorities.
They can demand the concessionaire to take part in the IFM. The national transport authority (minister) ultimately decides on the abolishment of the paper ticket based system.

Possible migration steps are:

- VDV-KA: issue limited kind of product templates, issuing limited kind of payment methods and according technical equipment
- INTERCODE: technical steps, acceptance of new stakeholders, new fares
- ITSO: existing ISO14443 schemes may migrate but require media to be re-initialised
- OTLIS: follow an "Enterprise Architecture Methodology" to evaluate the current status (e.g. no system, magnetic system, etc) and "where-to-go", which results in a definition of the system for the operator, but aligned to the interoperable system specification.
- Resekortet: Technical specification and administrative regulations
- TLS: Paper based -- paper and smart card -- smart card

Following entities are liable for possible losses incurred in the case of interoperable products:

- VDV-KA: every product retailer (customer contract provider) for his products
- INTERCODE: Would be examined by juridical courts if one stakeholder were proofed to be solely responsible. (which may not be the case for successful hacking for example)
- OTLIS: operators with the co-solidarity of OTLIS
- ITSO: depends on commercial agreement; ITSO requires all operators to sign license accepting risk
- Resekortet: Not regulated yet
- TLS: No product clearing yet. As soon as it gets in scope, agreements will be made

Economic basis for the implementation of the IFM is within:

- VDV-KA: secure against forgery, minimisation of sales costs
- INTERCODE: decision is mostly not economic, but political (multimode policies), technical (renewal of systems) or commercial (new services to customers)
- OTLIS: First of all what we could call the "card issuing and management business case" (sharing the costs - and the incomes - for card issuing and management), but also the sharing of costs for third party sales networks (e.g. ATM, Internet, Payshop)
- ITSO: government funding to support countrywide interoperability across bus, tram, metro, rail and ferry
- Resekortet: Entrance and annually fees
- TLS: Public safety, customer convenience, optimisation of operations

Calculations concerning profitability of the system are available only within OTLIS.

The revenue apportionment for interoperable products (used in different transport companies) between the IFM participants are solved within

- VDV-KA: revenue apportionment contracts at most based on number of travellers today
- INTERCODE: Depending from scheme to scheme. A percentage may be given to the retailer. (i.e. for Navigo in Ile de France) The rest is cleared according to fixed rates adjusted periodically from surveys or from validations.
- OTLIS: All the transactions are processed at OTLIS service centre and clearing maps issued every day, and every month in a consolidated mode. The clearing statements are then settled by the operators between themselves and the system keeps a tracking record of the real funds transfers.
- ITSO: commercial agreements between operators; bi and multi-lateral; ITSO not involved but supports transactions necessary
- TLS: No product clearing yet, but will be part of services provided by TLS. Apportionment will be according to agreements between product owners and service providers.

Revenue apportionment is executed only in exceptional cases, depending on the use of covered transactions!

V.2 Legal framework

Relevant contracts for the national IFM are:

- VDV-KA; Participation contracts for Retailer/Customer contract partner, Product Owner, Service Operator, IOP Clearing, issuing (application/entitlements to customer) contracts, conditions of carriage, Regional PT contracts
- ITSO: membership agreement; licensed operator agreement; registered supplier agreement
- Resekortet: Co-operation agreement
- TLS: contracts between TLS (as Scheme Provider) and IFM participants: Framework agreement, participant agreement, load agent agreement. Part of the participant agreement is the services portfolio

Uniform, centrally defined Rules & Regulations for participation in the IFM System exist for VDV-KA, OTLIS, ITSO, Resekortet and TLS.

Within VDV-KA there exist specific central agreements between VDV-KA KG and KA-EFM participants, between security management operator T-Systems and VDV-KA KG, single contracts between security management operator and companies.

Within ITSO all individual parties have a contract with ITSO.

Within Resekortet exist Contracts between each PTA and Resekortet i Sverige and bilateral and multilateral contracts between PTA's and operators.

Within TLS exist bilateral contracts belong to the central agreements between the parties and TLS.

There are relevant requirements stemming from data protection acts

- in Germany: Federal Data Protection Act (Bundesdatenschutzgesetz/Landesdatenschutzgesetze), EFM Guideline
- in France: privacy requirements from CNIL (national privacy authority)
- in Portugal: imposed by the National Data Protection Agency (please consult with OTLIS)
- in UK: ITSO makes very limited requirements; up to individual operators to comply with legislation
- in the Netherlands; Dutch privacy law is applicable

There are relevant requirements stemming from data protection acts in every European country!

Open procurement and standardised solutions are mandatory for public bodies. References to other legal and political requirements may be company laws and obligations stemming from monetary regulations (E-Money Directive, banking law (Credit Transaction Law))