Migration paths

Deliverable 3.3
February 2010

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 3 leader**

RATP

Michel Barjansky (Work package leader)
Phone: +33 1 58 77 93 85
E-mail: Michel.Barjansky@ratp.fr

**Main authors**

Michel Barjansky, RATP
François GUILLAUME, RATP
Gilles de Chantérac, SNCF
Jean-Philippe Amiel, Nextendis

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 65035 111
Fax +49 221 65035 115
E-mail: oliver.althoff@de.tuv.com

Visit the webpage [www.ifm-project.eu](http://www.ifm-project.eu)
Table of content

1 Introduction ................................................................................................................................. 4
  1.1 The IFM project .......................................................................................................................... 4
  1.2 Application and interoperable media work package ................................................................. 4
2 Version Control .......................................................................................................................... 5
3 Reference documents ..................................................................................................................... 5
4 Glossary ......................................................................................................................................... 6
5 Preliminary agreements and organisational consideration ............................................................ 7
6 Inventory of existing media & applications .................................................................................. 7
   6.1 MIFARE templates .................................................................................................................... 8
   6.2 VDV Core application template .............................................................................................. 9
   6.3 Calypso templates .................................................................................................................. 10
   6.4 Application Templates used by ITSO ...................................................................................... 11
7 Gap Analysis between existing applications and IFM requirements ........................................... 13
   7.1.1 Portability to JAVA CARD environment: ........................................................................... 13
   7.1.2 Manageability with GlobalPlatform: .................................................................................. 15
8 Migration paths to the introduction of multi-application media .................................................. 18
   8.1 Migration paths for Customer media ...................................................................................... 18
   8.1.1 Migration paths from MIFARE templates .......................................................................... 18
   8.1.2 Migration paths from VDV KA templates .......................................................................... 18
   8.1.3 Migration paths from Calypso templates ........................................................................... 18
   8.2 Migration paths for Front Office equipment .......................................................................... 19
   8.3 Impacts on Back office IT system ............................................................................................ 19
9 Conclusions ..................................................................................................................................... 21

Table of illustration

Fig. 6-1: 7 layers of Calypso environment (source CNA) ................................................................. 10
Fig. 7-1: Comparison table for portability to JAVA CARD environment ........................................ 14
Fig. 7-2: Comparison table for manageability with GlobalPlatform ............................................. 16
Fig. 8-1: Integration of Application Download server ..................................................................... 20
1 Introduction

1.1 The IFM project

The IFM project aims to make public transport more user-friendly by facilitating seamless accessibility to different public transport networks. The objective of the "Interoperable Fare Management Project (IFM Project)" is to provide travellers with common styles of contactless media throughout Europe which can be used for multiple transport products in different geographic areas and for sustainable modal switching, such as the use of "Park and Ride"—unlike existing smart cards which are restricted to specific city or regional geographies.

A number of Public Transport Operators have joint IFMs and commenced the path towards the vision of seamless travel. It requires common business rules and organisations, and involves linked or hierarchical back offices with structured cooperation between transport authorities and operators to share security and privacy issues, and eventually create common products and organize their settlement when the market needs it and can afford it. The customer can therefore only use his smartcard media in the networks that have already joined these agreements and use common or joined back-office ICT systems.

IFM project has a long term vision where common products will help each customer finding exactly the same interface and processes through his journey all over Europe for purchasing and using his transport fare products. In this work package, we will focus on a first step based on the usage of interoperable media that can be accepted by any IFM scheme and on which customers can download the local ticketing applications they need as they move, should it be an existing local transit application or a future common EU application when available.

1.2 Application and interoperable media work package

The application and interoperable media work package (WP3) aims to:

- Identify the common requirements for transport contactless media
- Identify the benefits of multi-application media to enlarge interoperability
- Define common requirements on interoperable contactless media and multi-application management for Public Transport
- Issue recommendations for migration path to multi-application media

The first deliverable of this work package ([R14]) has provided a state of the art vision of the benefits for multi application media for end users and a description of multi application management functions.

The EU IFM project vision for interoperable Customer Media has also been defined in the second delivery of this work package ([R15]).

The present document aims at defining recommendations for migration paths to the introduction of interoperable and multi-application media, and will cover the following items:

- Inventory of media currently supported in the main existing IFM schemes in EU
- Gap analysis between existing media and media requirements issued by the IFM project
- Recommendations on how to migrate
2 Version Control

1.0 First version circulated between members. November 24th, 2009
1.2 Reviewed version following member comments. January 25th, 2010
1.3 Final version for publication. February 5th, 2010

3 Reference documents

[R3] ISO 14443: Identification cards — Contactless integrated circuit(s) cards — Proximity Cards – April 2000
[R5] ETSI TS 102 225 Smart Cards; Secured packet structure for UICC based applications (Release 7) (2006-04)
[R6] ETSI TS 102 226 Smart Cards; Remote APDU structure for UICC based applications (Release 7) (2007-07)
[R7] ETSI TS 102 613 UICC CLF interface – Part 1 Physical and data link layer characteristics (Release 7 2007-11)
[R8] ETSI TS 102 622 Smart Cards; UICC - Contactless Front-end (CLF) interface; Host Controller Interface (HCI) (Release 7 2008-02)
[R13] JCP - Java Card Platform Specification 2.1
[R15] IFM Project - Common requirements and recommendations on interoperable media and multi-application management - Deliverable 3.2 – September 2009
[R16] IFM Project - Development of Cooperative Organisational Models - Deliverable 4.3
[R18] Intercode - ref. AFNOR XP 99-405
[R19] Calypso – Specifications release 3.1
[R20] VDV-Kernapplikation/VDV Core Application for Interoperable Electronic Fare
4 Glossary

Definitions referring to the IFM specifications ([R1]) are marked with [IFM]. Definitions referring to the Global Platform specifications ([R2]) are marked with [GP].

Application A software program designed to perform some tasks or functions by proceeding data. In many cases, a set of data is associated to the application program.

[IFM] Implemented and initialised Application Template on a Customer Medium. It is identified by a unique identifier. The Application houses Products and other optional Customer information (Customer details, Customer preferences).

[GP] Instance of an Executable Module after it has been installed and made selectable.

Application Provider [GP] Entity that owns an application and is responsible for the application's behaviour.

(Card) Issuer [GP] Entity that owns the card and is ultimately responsible for the behaviour of the card.

ICT Information and Communication Technologies

Customer Medium (CM) [IFM] Medium initialised with one or more Applications through an Application Contract

Medium Access Device [IFM] A device with the necessary facilities (hardware and software) to communicate with a Customer Medium. The Medium Access Device is in fact a “reader” or a “coupling reader” and the term reader is also used in this document.

Product [IFM] Instance of a Product Template on a Medium stored in an Application issued by a Product Retailer. It is identified by a unique identifier. Enables the customer to benefit from a service provided by a Service Operator.

SAM Secure Application Module, used to store and manage the distribution of transport application keys.

Secure Channel [GlobalPlatform] A communication mechanism between an off-card entity and a card that provides a level of assurance, to one or both entities

Security Domain (SD) [GlobalPlatform] On-card entity providing support for the control, security, and communication requirements of an off-card entity (e.g. the Card Issuer, an Application Provider or a Controlling Authority)
5 Preliminary agreements and organisational consideration

The aim of the present document is to focus only on the functional and technical aspects of the migration paths from existing media to interoperable and multi application media.

The business and commercial aspects regarding the set up of the necessary agreements between the public transport application owner and the owner of the Secure Element (SE) of the media onto which the application may be stored, should not be forgotten or underestimated.

Most generally, the PT Operators must define and have to agree with SE owners on the business and commercial terms and conditions for downloading of a public transport application onto an IFM compliant SE before starting technical migrations in their EFM system.

These organisational impacts are described in the IFM project document D4.3 “Development of Cooperative Organisational Models” ([R16]).

6 Inventory of existing media & applications

In the previous document ([R15]), common requirements have been defined for interoperable and multi application Customer Media. Such media must meet a set of common requirements to offer interoperability for application loading and personalisation. JAVA Card ([R13]) and GlobalPlatform ([R9] to [R12]) have been agreed as the best available technologies to rely on today for fulfilling these interoperability and multi application management expectations.

To summarize, an interoperable and multi application media shall comply with the following list of requirements & standards:

1. Microprocessor based device
2. Java Card 2.1 or later as open multi application OS
3. Global Platform Specifications 2.2 for interoperable application management
4. ISO/IEC 7816-4 as APDU interfaces to the microprocessor
5. ISO/IEC 14443 type A or B as contactless communication protocols (and their NFC adaptations),
6. Support of standard crypto algorithms needed by the transport applications and GlobalPlatform downloading process which are at least: DES, 3DES, RSA (1024 bit till 2014), HMAC-SHA1, ISO 9797 MAC. This list may evolve in the future with the publication of new GP amendments or versions. The EU IFM group (see WP4) will agree collectively on protocols suitable for Public Transport enabled by GP.

Not surprisingly, existing Customer Media are not compliant yet in Europe with all these features. A first analysis has been conducted by a questionnaire inquiry sent to the IFM project members and through IFM Forum exchanges to collect a vision about the main types of customer media and applications presently in use across the main EFM schemes in Europe.
Existing customer media are mostly native and specifically designed to support only one ticketing application. The current CALYPSO media could be natively instantiated to support different applications, including the TRIANGLE bridging one, but this technical possibility has only recently been envisaged by some application owners and no effective use of it yet exists.

All media will need anyway to be replaced by Java Card and GlobalPlatform compliant media to fulfill the interoperable and multi application media objectives of the IFM project, or they will be provided by third parties like Mobile Network Operators that will propose to host contactless applications on their already deployed media.

Hence, the focus has been set on the existing ticketing applications rather than on the media itself and on how the existing applications can be ported into an IFM interoperable and multi application media.

Four main types of applications and ticketing templates are currently in use in Europe:

- MIFARE templates used in Netherlands, UK, Austria, Czech Rep., ...
- VDV-KA templates used in Germany and Austria;
- Calypso templates used in France, Belgium, Italy, Portugal, Latvia ,...
- ITSO templates used in UK.

The following chapters describe the main characteristic for each type of applications.

### 6.1 MIFARE templates

MIFARE technology is a proprietary technology from NXP, formerly Philips Semiconductors ([http://mifare.net/](http://mifare.net/)). It applies to a range of NXP memory card products that allow the hosting of a structured set of data organized in blocks and sectors. Exchanges between the Mifare card and the reader rely on a MIFARE proprietary set of commands that allow to select, login, write, read, increment or decrement (for store value) a block of data. Data exchanges are secured using an NXP proprietary algorithm (NXP-Crypto1), or using standard DES or 3DES depending on each MIFARE product, and a different keyset can be used to protect each data sector.

A Mifare template requires a MIFARE reader (supporting the MIFARE command set and cryptographic algorithm) in the front end equipment.

The mostly used MIFARE templates are MIFARE Classic (1K or 4K) and MIFARE DESFire memory cards.

An application developed on a MIFARE template is then the combination of data blocks and sectors mapping, the assignment of one or several keyset to protect the data block including data sectors access and the related security rules defining how the key sets are derived from card specific data and from Master keys.

MIFARE Classic templates are used for example by OV-chipkaart, the largely deployed transport application in the Netherlands by Translink (more than 6 M units), by Oyster Card in Greater London by Transport for London (more than 10 M units) and by some ITSO cards deployed in UK.

A Security flaw has been unveiled in 2008 about the proprietary NXP Crypto-1 algorithm[^1] and even if the security of an AFC system cannot be reduced only to the security of its ticketing

[^1]: [“Dismantling MIFARE Classic”](http://www.dismantlingmifare.com) by Institute for Computing and Information Sciences, Radboud University Nijmegen, The Netherlands

Page 8 to 21

This report is a result from the IFM Project - a project funded through the 7th EU Framework Program
card, most of the Transport organizations using MIFARE Classics are scaffolding a card migration plan. Some ongoing migration plans are already converging with some of the requirements of the IFM Project and then reducing the initial gap between existing cards and IFM project media requirements:

- Usage of standard algorithm such as 3DES in replacement of proprietary NXP Crypto-1,
- Usage of microprocessor card relying on Java Card OS in replacement of memory card,
- Progressive giving up of MIFARE data structure avoiding the need for hardware support of proprietary MIFARE emulation.

In UK for example, ITSO has decided to migrate as a first transition step towards MIFARE DESFire card, which appears as a first step towards IFM requirements with the usage of the 3-DES standard algorithm, but still makes problem for interoperability because of the need for MIFARE specific data structure, not compliant to ISO 7816-4.

In the Netherlands, Translink has made the decision to migrate the entire base of MIFARE Classic cards in the field because of security risks associated with the Mifare Classic media platform. As a first phase, new cards will be JAVA Cards and the Translink ticketing application OV-chipkaart initially designed for Mifare Classic will be developed as an OV Applet.

### 6.2 VDV Core application template

The aim of the VDV Kernapplikation (VDV-KA) project was to provide a standardised basis for a national electronic fare management in Germany, called ((eTicket systems (http://www.vdv-ka.org/).

VDV Core Application is a data and interface standard that forms the basis for implementing the interoperable electronic fare management system in Germany. VDV KA specifications have been designed to be used as a secure application on different multi application able electronic media, such as smart card or mobile phones. To facilitate this, the customer media must fulfil the security and interface requirements: contactless and contact interfaces according to ISO/IEC 14443 (support for type A and B) resp. ISO/IEC 7816 part 1 through part 3; card OS, file structures and commands according to ISO/IEC 7816 part 4; data structures according to EN 1545; support of RSA, SHA-1 and 3-DES standard algorithms as defined in the VDV-KA user medium specification. Security mechanisms and command interfaces are described in the KA specifications (current specification version 1.106). The core application includes a common Public Key Infrastructure (PKI) which forms an inherent basis for interoperability between all core application systems and media without for example the need to share or exchange keys.

Existing VDV KA implementation are available mainly on Java cards (JAVA Card applet of different suppliers are available), but also native cards of the German banking industry - dual interface card with two other independent applications - are in use. It has already been implemented on NFC phones.

((eTicket systems are implemented by several authorities in North Rhine-Westphalia, Saarbrücken, Ostalb mobil, Kreisverkehr Schwäbisch-Hall, MDV (Leipzig, Halle), prospectively in RMV (Hesse), VBB (Berlin-Brandenburg), VVO (Saxonia), HVV, Hamburg, Schleswig-Holstein..
Each application instantiated on a VDV media is given a unique VDV-KA ID number, which validates the “VDV-KA Application”. The VDV-KA standard guarantees both the creation of a secure ticketing transaction between a medium and a terminal and the transfer of data with end to end security between media and different eTicket systems of different operators.

### 6.3 Calypso templates

Calypso templates are based on Calypso specifications defined by the Calypso Network Association ([http://www.calypsonet-asso.org/](http://www.calypsonet-asso.org/)).

These specifications, originally defined by the so-called Calypso European project, allow for the development of applications between a card and a terminal relying on existing standards for all layers 1 to 7. They complement the existing standards to create a secure ticketing transaction between a card and a terminal.

<table>
<thead>
<tr>
<th>Layer</th>
<th>International Standard</th>
<th>Calypso Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Security Management and Architecture</td>
<td>Calypso Security Architecture</td>
</tr>
<tr>
<td>6</td>
<td>Terminal Applicative Software</td>
<td>Calypso API</td>
</tr>
<tr>
<td>5</td>
<td>Data Model</td>
<td>INTERCODE compliant</td>
</tr>
<tr>
<td>4</td>
<td>Card and SAM Security Mechanisms</td>
<td>Calypso card application</td>
</tr>
<tr>
<td>3</td>
<td>Card Data structure</td>
<td>EN 1545</td>
</tr>
<tr>
<td>2</td>
<td>Card OS and Files structure &amp; Commands</td>
<td>ISO/IEC 7816-4</td>
</tr>
<tr>
<td>1</td>
<td>Contact and Contactless Communication Interface</td>
<td>ISO/IEC 7816 1-3, ISO/IEC 14443 A/B 1-4</td>
</tr>
</tbody>
</table>

Fig. 6-1: 7 layers of Calypso environment (source CNA)

The development of a ticketing application on a Calypso template is therefore based on the international standards (layer 1 to 3 in compliance with IFM project recommendations):

- **Contactless communication** ISO/IEC 14443 A/B which defines the radio signal and protocol for a high frequency induction transmission at 13.56 MHz.

- **Card OS and file architecture**: ISO/IEC 7816-4, which defines the card data organisation in files and basic card commands

- **Card data structure**: based upon EN 1545, which defines the codification of data elements used for public transport (such as the date, time, validation event, transport contract, etc.)

- **Security Management and security mechanisms**: which describe the management of the data security for a ticketing system, and indicate the choices available for transport networks. In addition, CALYPSO specifies with precision the card and SAM
commands and files used during the ticketing transaction. These mechanisms are optimised for ticketing (fast, secure) and include such innovative patents as the Session and Ratification systems, used with security cryptogram algorithms.

- Data Model, which allows to describe the definition and the interpretation of the data in the card’s file. Calypso supplies a user friendly generic data model for all ticketing systems which is compliant with Intercode ([R18]) and supports any type of transport product from ticket to store value.

- Terminal Applicative Software, which ensures that the applications are managed in the same way by all the terminals, and allows an easier evolution of all kinds of terminals.

Each application instantiated on a Calypso media receives a unique Calypso ID number, which validates the concept of “Calypso Application”.

Access to the Calypso application is secure with applicative keys and relies on standard algorithm. Depending on the willingness and agreement between transport authorities, the same Calypso keys can be shared to provide access to the same Calypso application, allowing to build local or regional interoperability. Another possibility is to define some shared elementary files between different Calypso applications, for instance to share a common purse.

The current version of Calypso specifications described in this chapter in Calypso Release 3.1 ([R19]). Most Calypso applications today in the field are still based on Calypso Release 1 which used some proprietary algorithm and pre-normative contactless interface. Calypso Release 3 applets already exist and have been experimented in multi application smart card and NFC phones.

Some example of Calypso applications are the Navigo card for the Ile de France Region, including Paris metro area, Lisboa, the OùRAI card for Rhones Alpes region in France, the Mobib card in Brussels, … Calypso applications are in use in 21 countries, more than 80 cities, for more than 39 million contactless cards.

### 6.4 Application Templates used by ITSO

ITSO Limited (www.itso.org.uk) is a company limited by guarantee, a non-profit distributing organisation, whose membership covers transport operators (bus, tram, ferry and train operating companies), suppliers to the industry, local authorities and integrated transport authorities. Supported by the UK Department for Transport, ITSO’s objective is to maintain and develop the ITSO Specification, operate and manage an interoperable smart media environment, and facilitate and support development of interoperable smart ticketing schemes that comply with the ITSO Specification.

The ITSO Specification is a technical platform on which interoperable smart ticketing schemes can be built. It defines the key technical items and interfaces that are required to deliver interoperability between all components of a smart ticketing system –Customer Media (CM), points of service terminals (POSTs) and back offices - and separate ticketing systems. The ITSO Specification is an open specification. It is UK Government Copyright and available to all.

To be compliant with the ITSO Specification requirements, a CM shall support a contactless interface that complies with the relevant parts of ISO/IEC 14443 (support for Types A and B). Other data interfaces may be present on the CM, but are not covered by the scope of ITSO.
This means that an ITSO Application can support multiple Products or an ITSO Product (within an ITSO Shell) can stand alone in someone else's Application space. Furthermore, a CM platform may be dedicated to the ITSO Application, or the ITSO Application may be added alongside others on a multi-application CM platform.

The current ITSO Specification supports Mifare Classic (1k and 4k), Mifare DESfire, Calypso and Java cards; it also supports small memory media such as Innovision Jewel or Mifare Ultralite, but these are not relevant to this paper. ITSO supports Message transfer (between CM and the POST's CM reader) with relevant media, secured by use of a MAC that is generated using a triple-DES session key derived during mutual authentication. The ITSO File structure complies with ISO 7816-4.

**Note:** The migration of ITSO templates is addressed in this document through the analysis of the Mifare Classic, Mifare DESfire, native microprocessor and Calypso migration paths.
7 Gap Analysis between existing applications and IFM requirements

Two main aspects must be investigated in existing ticketing application in order to establish the migration effort towards a compliance to the IFM projects common requirements for interoperable and multi application media:

- The portability of existing application to JAVA Card environment,
- The manageability of existing application with GlobalPlatform,
- To allow a mutual application download all media must meet the highest requirements set by the individual PT specifications regarding the security and technical platform.

The following chapters give the result of the gap analysis made on existing applications regarding these aspects.

7.1.1 Portability to JAVA CARD environment

For porting local applications onto a JAVA card /GP environment, the first thing is to develop the ticketing application as a JAVA Card applet. The applet can then be loaded and executed onto any JAVA Card platform, this is the JAVA promise of “Develop once, run everywhere”.

Nevertheless, some verification may apply to ensure that an application is able to be developed and ported into a fully interoperable JAVA Card environment. These checks shall include that the application will only use:

- Standard algorithms,
- Standardized contactless communication,
- Standardized Card OS & file structure.

**Standard algorithms:**

Most smart media today are implementing standard cryptographic library including DES, 3DES, AES, SHA-1, ISO MAC and RSA capabilities when a crypto processor is part of the chip design. Those features are implemented in the hardware design of the chip to provide state of the art tamper proof security and acceptable performance.

Applications requiring non standard algorithms may need either to implement software emulation of the algorithm which leads both to poorer performance and lower level of security, or to restrict their portability to card platform implementing those proprietary algorithms.

**Standardized Card OS and file architecture (ISO/IEC 7816-4):**

Most of the smart cards in the industry are relying on a well established standard which is the ISO/IEC 7816-4 to provide APDU command interoperability, and this is used in all industry sectors: UICC or SIM for the telecoms industry, payment card for the banking and retailing sectors, health care and e-government cards, ...

As a consequence, IFM project recommended that ticketing application for interoperable and multi application media shall be able to send and receive APDU command compliant to ISO/IEC 7816-4 format. Obviously, the contents and data structure of these ISO/IEC 7816-4
APDUs are application dependent and can be secured thanks to media or application related security mechanisms.

Such compliance may be an issue for templates relying on memory cards and especially the MIFARE Classic and MIFARE DESFire implementations requiring a proprietary DESFire command set as the organization of the data file structure is not fully compliant to the ISO/IEC 7816-4.

**Standard Contactless communication (ISO/IEC 14443):**

One of the key points also highlighted in the IFM project requirements for media is the ability to rely on ISO/IEC 14443 standard for contactless communication as multi application devices will not be dedicated solely to the transportation industry. NFC phones for example or any multi application media willing to support payment application will have to strictly comply to ISO 14443 Type A or Type B protocol.

The support of additional contactless protocol for legacy reasons may either slow down the performance of the ticketing transaction as the validation reader will have to poll on type A, type B and any additional protocols that need to be supported. This shall have also an additional cost for the front equipment upgrade if the introduction of the support of ISO/IEC 14443 has not been anticipated in most of the current equipments.

The following table summarises the compliance of the main types of ticketing templates with the above listed requirements in order to be able to roll out ticketing application as a dematerialized JAVA Card applet.

<table>
<thead>
<tr>
<th>Application template specification</th>
<th>Standard Algorithms</th>
<th>Non standard algorithms</th>
<th>ISO 14443 RF protocol</th>
<th>ISO 7816 –4</th>
<th>Applet available</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NXP Proprietary MIFARE environment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mifare Classic</td>
<td>-</td>
<td>NXP’s Crypto-1</td>
<td>A - part 1 to 3 + Mifare proprietary layer</td>
<td>Not supported Mifare Command Set</td>
<td>No</td>
</tr>
<tr>
<td>Mifare Plus</td>
<td>AES</td>
<td>NXP’s Crypto-1 (optional)</td>
<td>A</td>
<td>Not supported Mifare Command Set</td>
<td></td>
</tr>
<tr>
<td>Mifare Desfire</td>
<td>DES, 3DES, AES</td>
<td>NXP’s Crypto-1 (optional)</td>
<td>A</td>
<td>Supported + Mifare Command Set</td>
<td></td>
</tr>
<tr>
<td><strong>VDV KA</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V1.106</td>
<td>3DES, SHA-1, RSA</td>
<td>-</td>
<td>A &amp; B</td>
<td>Supported</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NFC</td>
<td>Supported</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>CNA Specifications</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calypso V1</td>
<td>DES</td>
<td>Innovatron Hash</td>
<td>Bv0 Innovatron</td>
<td>Supported</td>
<td>No</td>
</tr>
<tr>
<td>Calypso V2</td>
<td>DES-X</td>
<td>Innovatron Hash</td>
<td>B or Bv0 Innovatron</td>
<td>Supported</td>
<td>No</td>
</tr>
<tr>
<td>Calypso V3</td>
<td>3DES ISO 9797-1 (MAC) RSA (activation)</td>
<td>-</td>
<td>A &amp; B</td>
<td>Supported</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NFC</td>
<td>Supported</td>
<td>Java Card 2.1 &amp; 2.2</td>
</tr>
</tbody>
</table>

Fig. 7-1: Comparison table for portability to JAVA CARD environment

Latest specifications for VDV-KA and Calypso applications are already compliant to the IFM requirements and some applets already exist for smart card and NFC environments in both cases.
Regarding the migration of the older versions of Calypso applications, the migration of existing front end equipment should not be a concern as most of the ticketing equipment providers are providing since several years equipment supporting also the ISO/IEC 1443 type A and B protocols in addition to the type B Innovatron, as required by the standard.

The migration of an application implemented on a MIFARE template is more concerning as today it’s not possible to emulate a MIFARE template outside a MIFARE environment. Even if the newest MIFARE products are progressively integrating some conformance to the ISO/IEC 14443 and ISO/IEC 7816-4 standard, there is no way to implement a MIFARE application as an applet. Some chips include some MIFARE emulation allowing to combine MIFARE application and standardized applet but this is only applicable to some NXP chips such as SmartMX or to some chips from MIFARE licenced chip manufacturers. This may not represent the largest majority of the smart card market and there is no certainty that bank or mobile operators are willing to integrate MIFARE technology and to bear the related inherent licensing costs for integrating this technology into their media.

Temporarily, in order to work around the limits of MIFARE templates, some application owners in France and UK opted for operating two types of templates:
- A MIFARE one used for purely urban needs, continuing the existing template as it is
- A Calypso one used for interoperable urban and regional products.

Implementing the support of a second ticketing application can be a possible migration path to European interoperability to circumvent MIFARE limitations, should this second ticketing application be the future EU IFM application or an already existing ticketing application compliant to the EU IFM media requirements defined in [R15].

### 7.1.2 Manageability with GlobalPlatform:

Having a dematerialized ticketing application in a JAVA Card applet format is a necessary but not sufficient step for the usage of interoperable and multi application media. The process to load, install and personalize each transport application must be defined in a secure and interoperable way and this is the reason why the IFM project is relying on GlobalPlatform technology as a basis for fulfilling this requirement.

This implies to have media compliant to GlobalPlatform specifications but it also requires that the ticketing application must able to be loaded, installed and personalized using GlobalPlatform commands as described in chapter 7 of “D3.2 Common requirements and recommendations on interoperable media and multi-application management” [R15]. Each application specification must then include the description of a GlobalPlatform compliant personalisation process.

Loading and installing an application with GlobalPlatform commands does not require specific adaptations to ticketing application once they exist as a JAVA Card applet. For the personalisation of an application, the process & security rules which are defined at application level can be implemented using GlobalPlatform secure channel & commands. That requires to have defined the way the application parameters must be split and passed on to the applet with GlobalPlatform commands and the applet must be of course designed in order to be able to process those GlobalPlatform personalisation commands.
This installation and personalisation process is ensuring full interworking and interoperability when issuing the application on any GlobalPlatform device. It also provides a high level of security inherent to GlobalPlatform technology to transmit all the application parameters including the application keys over any type of connection between the personalisation device and the media. This is highly beneficial when using non-trusted remote link over the Internet or any wireless network to personalize a ticketing application into a NFC phone or into a smart card connected to the cardholder’s PC at home. This may allow the personalisation server to use the same perso script whatever the type of link (remote/local – trusted/non trusted) is used to communicate with the media, the end to end security of the link (from the perso server till inside the media) being provided by GlobalPlatform secure channel.

The following table summarizes the compliance of the 3 main types of templates with the above listed requirements in order to be able to issue a ticketing application in an interoperable way on any IFM compliant interoperable and multi application media.

<table>
<thead>
<tr>
<th>Application template specification</th>
<th>Application loading</th>
<th>Application Personalization</th>
<th>GP personalization process specified</th>
</tr>
</thead>
<tbody>
<tr>
<td>NXP Proprietary MIFARE environment</td>
<td>Mifare Classic</td>
<td>Not applicable – A MIFARE emulation shall exist in the media.</td>
<td>Proprietary (non GP based) except for NFC UICC implementing Mifare4Mobile</td>
</tr>
<tr>
<td></td>
<td>Mifare Plus</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mifare Desfire</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VDV KA</td>
<td>V1.106</td>
<td>Supported</td>
<td>Proprietary (non GP based). Will be supported in next version.</td>
</tr>
<tr>
<td>CNA Specifications</td>
<td>Calypso V1</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Calypso V2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Calypso V3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Fig. 7-2: Comparison table for manageability with GlobalPlatform**

MIFARE and DESFire templates are fundamentally different from JavaCard. They have a dedicated application OS with applications in a form of static data which are by definition not executable. Therefore the JavaCard/GP concept of application loading is not applicable as such.

- To bring together JavaCard and MIFARE / DESFire technologies in the same device i.e. NFC UICC and phone and in order to offer to provide the Service Provider with processes and security mechanisms to personalize and manage MIFARE in NFC mobile phones, NXP proposed a specification called MIFARE4Mobile for interacting with MIFARE from a JavaCard / GP environment. It consists in using an applet (called MIFARE4Mobile service manager) that is used as a proxy for MIFARE personalization and management. Service Providers will then use GP secure channel protocols to dialog with the MIFARE4Mobile service manager applet and to provision the MIFARE application.
Even if GlobalPlatform compliant personalization of MIFARE Application via a proxy applet can be applicable to others SE than NFC UICC, we’re not aware about initiatives to extend this process to non UICC smart card with MIFARE emulation.

Regarding VDV KA application, the applet can be loaded, instantiated, activated and personalized with GP commands although these steps are not currently defined in detail in the standard. In the terminology of the core application the term “initialization” is usually used for the process referred to as “personalization” in the documents of IFM WP3 and it covers the following steps: generation and registering of the application ID, on board generation of a private/public key pair, and the request and loading in the card of the public key certificate.
Following the completion of this “initialization” a VDV KA application is ready to run according to the specifications of the core application and contains its own secure end-to-end mechanisms for the operational phase of the application based on PKI, RSA and 3DES.
During the “operative life” of the application only specific entitlements and possibly the name of the customer are loaded into the application using the ISO/IEC 7816-4 compliant commands of the core application.

VDV KA specifications are going to be updated so that the “initialization process” (i.e. the personalization as commented above) will be specified as a GlobalPlatform process. As for today, a VDV KA applet can be loaded and installed with GP commands but needs a proprietary but secure process for initialization and personalization. Once new VDV KA specifications will be available, the full loading and personalization process will be GP compliant.

Calypso V3 applications can be loaded and personalized using GlobalPlatform process as it is.
8 Migration paths to the introduction of multi-application media

8.1 Migration paths for Customer media

8.1.1 Migration paths from MIFARE templates

The migration path for MIFARE applications towards IFM interoperable and multi application media requires some important and structuring changes. By priority and importance order the following changes should be considered in order to pave the way towards IFM media interoperability:

- Giving up of Crypto-1 NXP proprietary algorithm, but this is even a recommendation from NXP not to deploy anymore MIFARE Classic media for new implementations,
- Adoption of full standard ISO 14443 Type A communication protocols
- Renunciation to the MIFARE proprietary data and file structure which requires MIFARE emulation and will not be available on all JAVA cards.

Among those three migration steps, the last one is the most impacting one as MIFARE application are by definition based on the specific MIFARE file and data structure. As already indicated at the end of §7.1.1, this 3rd step can be achieved by the replacement of local MIFARE application by the future EU IFM application or by one of the existing ticketing applications.

8.1.2 Migration paths from VDV KA templates

The migration path for VDV KA application is quite straight forward as VDV KA applications exist as an applet even though the personalisation with GlobalPlatform is not yet described in the KA standard.

As GP personalisation process is not yet available, this would currently require the PTO to specify one personalisation processes per distribution channels.

The next release of VDV KA specification for GlobalPlatform personalisation will avoid this roll out and implementation of specific personalisation processes.

8.1.3 Migration paths from Calypso templates

Regarding Calypso application the latest Calypso Release 3 specifications are already fulfilling all the requirements for using Calypso applet on IFM media.

Very logically, existing Calypso V1 application shall be migrated into Calypso V3. Because, the product data structure in Calypso application is based on separate specifications (EN1545 and Intercode in France), the same generic Calypso V3 applet will be able to host any type of ticketing product and shall fulfil the need for all Calypso networks.

The personalisation process will only need one adaptation as its GP compliance can allow the same personalisation script to address media over all the possible channels and whatever the media form factor.
8.2 *Migration paths for Front Office equipment*

The migration of existing ticketing applications may impact the contactless Front End equipment for validation, control or product sales.

Front Office equipment must be made fully compliant to ISO/IEC 14443 Type A and B for EFM scheme that were using MIFARE applications with MIFARE specific contactless level 4 layer and Calypso V1 applications relying on type B Innovatron protocol.

This effort is not only linked to IFM interoperability as the migration of front end equipment towards standard contactless protocols has been already anticipated and forecasted on some networks to prepare either the introduction of new MIFARE or Calypso media, or to support NFC phone or direct payment with contactless banking card at the gates.

The usage of standard algorithm in Calypso 3.1 templates may also require replacing the existing SAM in the Front End equipments or adding a new SAM.

Similarly, for networks that will decide to implement an additional ticketing application in lieu and place of MIFARE applications to fulfill IFM interoperability requirements, very likely a new SAM will be needed to store the new ticketing credentials related to this application.

VDV-KA Front Office equipment already supports the ISO/IEC 14443 Type A and B, which must be demonstrated in a “Terminal Certification Procedure”.

8.3 *Impacts on Back office IT system*

The migration of existing media towards interoperable and multi application media should only slightly impact the back office systems of EFM schemes as long as local application are used and comply to the previously enounced JAVA Card portability and GP manageability requirements.

The main impact will be the set up of an application download and personalisation server and its connection to the different distribution channels, to the different application management systems of SE owners to retrieve the media keys needed prior to be entitled to download the PTO application on 3rd party media, and to the customer database and personalization server to get the necessary operator and customer data for application personalization.
The integration of the application server can be managed step by step with the gradual introduction of distribution channels and set up of agreements with SE Owners.

Again, the benefit of relying on GlobalPlatform technology is to easily fulfil the highest constraint for application personalisation which is certainly to have a transaction management secure enough to be processed in a remote mode over a non trusted network. This is what GP technology provides with end to end secure channel communication with mutual authentication between Application server and the SE, integrity and confidentiality protection for the transferred data, and confidential key distribution or generation process for the Application Owner.
9 Conclusions

The migration paths from existing media and applications towards IFM recommended interoperable and multi application media is quite different according to the type of legacy ticketing application in place.

Whereas migration for network using either VDV KA or Calypso templates is quite seamless by following up the specification evolution of VDV KA and Calypso, the situation is more is much less easy to handle for networks only using MIFARE templates.

Unfortunately there is today no solution to port applications defined for MIFARE templates on non specific device, i.e. without a MIFARE HW emulation. This may likely lead PT networks relying on MIFARE templates to progressively introduce an alternative application as Translink is for instance currently considering in its migration plan.

This may also be seen as an opportunity to promote and foster the introduction of an EU IFM application.

--------- End of the report -----------