Common requirements and recommendations on interoperable media and multi-application management

Deliverable 3.2
September 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**

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

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
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** .

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Table of content

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Table of illustration

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

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 cities or regional geographies.

A number of Public Transport Operators have commenced path towards the vision of seamless travel and the creation of IFMs. It requires common business rules and organisations, and involves linked or hierarchical back offices with structure 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

Additionally, customers should be able to benefit from their status all over Europe, allowing them to benefit from specific rights linked to its status all across Europe.

1.2 Application and interoperable media work package

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

- Identify the benefits of multi-application media to enlarge interoperability (D3.1 - [R14])
- Define common requirements on interoperable contactless media and multi-application management for Public Transport (D3.2 - present document)
- Issue recommendations for migration path to multi-application media (D3.3 -

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 previous delivery of this work package ([R14]). To sum up, an interoperable Customer Media is a device able to host several transport applications on demand of the customer from distinct IFM schemes. In a second phase, a nucleus EU IFM application will need to be standardized to host EU citizen status, to offer a common template for hosting local product and to ultimately host common products.

This proposal will enable multiple transport applications from separate IFM schemes to be replaced by a single EU-application in the future.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

1.3 Application and interoperable media work package

The present deliverable will address the following items:

- Listing the common requirements for Customer Media
- Clarifying the relationship between IFM roles and multi application customer media stakeholders
- Listing the common requirements for multi application management
- Giving some common requirements for EU status application

It focuses 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 applications they need as they move, should it be an existing local transit application or a future common EU application when available.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

2 Version Control

0.5	First draft for internal review.	February 27th 2009
1.0	First version circulated between members.	March 6th, 2009
1.6	Revised version including ITSO and VDV comments.	May 4th, 2009
2.0	Revised version based on outputs of WP3.2 workshop	June 18th, 2009
2.2	Integration of VDV, SNCF and Newcastle University comments	June 30th, 2009
2.3	Integration of Newcastle University comments on §5.1, §5.5 & §5.6	July 17th 2009
2.4	Integration of comments collectively redacted during September IFM Workshop – Approved version	Sept. 3rd , 2009

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

3 Reference documents

[R1] ISO 24014-1:2007 - Public transport - Interoperable fare management system - Part 1: Architecture (IFMS)

[R2] ISO 24014-2: [Working draft] -Public Transport - Interoperable Fare Management System - Part 2: Recommended Business Practice for Set of Rules

[R3] ISO 14443: Identification cards — Contactless integrated circuit(s) cards — Proximity Cards – April 2000

[R4] ISO 7816: Integrated circuit cards with contacts

[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)

[R9] GlobalPlatform Card Specification 2.2 – March 2006

[R10] GlobalPlatform Card Specifications 2.2 – Amendment A: Confidential Card Content Management v1.0 – October 2007

[R11] GlobalPlatform UICC Configuration 1.0 – October 2008

[R12] GlobalPlatform Messaging Specification 1.0 – October 2003

[R13] JCP - Java Card Platform Specification 2.1

[R14] IFM Project - State of the art on interoperable media and multi-application management - Deliverable 3.1- February 2009

[R15] IFM Project – Migration Paths - Deliverable 3.3- December 2009

[R16] EMVCo - EMV Contactless Specifications for Payment Systems, EMV Contactless Communication Protocol Specification 2.0 – August 2007

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

4 Glossary and definitions

4.1 Glossary

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

APDU	Application Protocol Data Unit – Unit of data exchanged between a smartcard and a smartcard reader. The structure of an APDU is defined by the ISO 7816 standards ([R4]).
Application	[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.
Validation Authority	[GP] A Validation Authority is an entity independent from the Issuer, represented on the card and responsible for the verification of applications signatures (mandated DAP) during the loading process.
Controlling Authority	[GP] A Controlling Authority is an entity independent from the Issuer, represented on the card and responsible for securing the keys creation and personalization of the Application Provider Security Domain (APSD)..
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.
Portable Object (PO)	A portable object with an ISO14443 interface that hosts a SE. A SE is usually embedded in a smartcard but not always. Some Portable Objects use a fixed SE soldered to a motherboard (like USB Keys and some mobile phones) while others use removable SE (a mobile phone with a UICC that serves as a SE). Examples: • A contactless smartcard, • A mobile phone with a NFC interface,

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

- An USB key with a NFC interface (also called a "Smart Key").

Product	[IFM] Instance of a Product Template on a Medium stored in an Application. 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
Secure Channel Protocol (SCP)	[GlobalPlatform] Protocol used to secure a Secure Channel. SCPs can ensure the confidentiality and the integrity of the application code during application loading and and of the application data during personalisation. GlobalPlatform SCPs can also provide authentication and/or mutual authentication between the Secure Element and an off card entity (Application Owner, SE Owner, …).
Security Domain (SD)	[GlobalPlatform] On-card entity representing an off-card entity (e.g. the Card Issuer, an Application Provider or a Controlling Authority) and supporting security services for their providers' applications (holding keys for encryption, decryption, signature verification, off card authority authentication, …. and used for application management)
Secure Element (SE)	A secure microprocessor that stores and executes the contactless applications. It is typically accessed through the ISO7816 interface but may support additional interfaces (USB, SWP, ISO14443, ...).
Uniform Resource Identifier (URI)	A string of characters used to identify or name a resource on the Internet. Such identification enables interaction with representations of the resource over a network, typically the World Wide Web, using specific protocols. URIs are defined in schemes specifying a specific syntax and associated protocols.
Universal Integrated Circuit Card (UICC)	Chip card used in mobile phones in GSM (2G) and UMTS (3G) networks. It contains a SIM application for GSM networks and a USIM application for UMTS networks. UICC designed for NFC phones are generally able to host third party applications for transport ticketing, payment, loyalty, access control, …

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

4.2 Reminder on role mapping between GlobalPlatform and IFM model

There are some correspondences between GP and IFM Conceptual models. The following table is an update of the version given in WP3.1 ([R14]):

IFM Definition	*Global Platform Definition*
SE Owner	**(Card) Issuer**
SE Retailer	**(Card) Issuer (partially)**
SE Loader	**(Card) Loader & Card Enabler & Collator/Decollator**
Application Owner	**Application Provider & Application Owner**
Application Retailer	**Application Provider (partially)**
Application Template	**Application (instance)**
Customer	**Cardholder**
Collection & Forwarding	n.a.
Product Owner	n.a. - Product management is not addressed by GP
Product Retailer	n.a. - Product management is not addressed by GP
Service Operator	n.a.
Registrar	n.a.
Security Manager	**Validation Authority** (partially)
Controlling Authority	**Controlling Authority**
n.a.	**Application Developer**
n.a.	**Card Manufacturer**
n.a.	**IC Manufacturer**
n.a.	**Platform Developer**
n.a.	**Platform Owner**

Some roles are out of scope of the GP Messaging conceptual model which only describes a technical solution. They are then indicated as not applicable (n.a.).

Similarly, some GP roles are out of scope of the IFM conceptual model as they do not impact the IFM ecosystem.

IFM definitions in red are new definitions in the draft version of ISO24014-2 ([R2]).
IFM definitions in blue are new IFM roles introduced through the present IFM project.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

5 Common requirements for customer media

The following requirements define the functional and technical characteristics of an interoperable Customer Media used in an IFM transport network as seen today.

Most of the present requirements are based on Java Card and GP technologies. Should furthers standards meeting the same criteria being available in the future and widely accepted by the transport and related card industry, It is important the EU IFM group (see WP4) remains open to consider any substitute or extension of the present referenced standards as the market develops.
The same approach remains valid considering extension or new version of JavaCard and GlobalPlatform standards. The EU IFM group may revise and complement the present requirements at the time the first EU IFM implementation will be rolled out.

As an important remark, it should be noted that most of the following requirements are not specific to transport application. They apply to any type of media able to host contactless applications should it be for transport ticketing but also for payment, loyalty program, access control …

5.1 Functional characteristics

The following functional requirements must be fulfilled by multi application Customer Media (CM):

[Req1]: The customer can load and manage several (transport) applications in the same device.

[Req2]: Customer media shall enable customers to select, buy and load a transport product through the existing product retailing channels.

[Req3]: Customer media shall enable customers to select, buy and load a transport product remotely, at the user's chosen place and time (using a mobile phone or a media connected to a PC with internet connection).

[Req4]: The customer shall access the transport network directly with the media.

[Req5]: When the media provides a user interface, the customer shall be able to select the transport product or the transport application he wants to use.

The capability for some CM types to be interactive (like NFC phones for example) can allow a more important mix of applications or products on it which are secured against each other.

[Req6]: Customer media should ensure an absolute data tightness between applications to guarantee application code & data privacy.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

5.2 Technical characteristics

Customer media must rely on the open industry standards widely used for contactless multi application devices.

[Req7]: The Customer Medium shall hold a Secure Element which is a Microprocessor based component.

[Req8]: Application (and products) shall be stored and executed in the Secure Element of the Customer Medium.

Important note:
The term Secure Element will be used when requirements only apply to the Secure Element which is part of the Customer Media.
The term Customer Media will be used when requirements apply to the Customer Media as a whole device, regardless of the implementation of the required features inside the Secure Element or not.

[Req9]: The Secure Element shall comply with GlobalPlatform Card Specification 2.2 (and amendments) or higher for content management ([R9] & [R10]).

GlobalPlatform is an application management standard in the banking industry since end of 1990's, is field proven for multi application management and provide cards ([R9],[R10]) and system specifications ([R12]) to support application issuance into a multi application environment.

[Req10]: The Secure Element OS shall be compliant to Java Card 2.1 or higher ([R13]).

Java Card is one of the most used standards in the smart card industry for contactless device. Java Card technology is offering limited development and seamless deployment for application providers, thanks to the "Develop once, Run everywhere" Java promise.

In addition to the security mechanism provided by GP for the application loading and personalization, Java Card environment is also providing a security framework that offers application firewalling.

[Req11]: The Secure Element shall support a set of standard algorithms to offer the cryptographic capabilities required by the existing transport applications.

The complete list of required algorithms will be specified in the WP3.3 deliverable based on the inventory of existing transport application among the different EU public transport networks.

[Req12]: The management of transport applications on the Secure Element shall be secured by the Secure Channel Protocols (SCP) defined in GlobalPlatform specifications.

Such SCPs can ensure the confidentiality and the integrity of the application code and of the application data during application loading and personalisation. GlobalPlatform SCPs can also provide authentication and/or mutual authentication between the Secure Element and an off card entity (Application Owner, SE Owner, …).

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

[Req13]: The Secure Element shall support the set of crypto algorithms used for content management defined by GlobalPlatform Card specifications ([R9] & [R10]).

The list of algorithms used by GlobalPlatform 2.2. is : DES, 3DES, RSA, 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 those protocols suitable for Public Transport enabled by GP.

5.3 Customer Media 's form factors

Customer Media's can have different form factors. The list hereafter gives a non exhaustive view of possible form factors for Customer Media:

1) Contactless smart card
2) Dual (contact & contactless) smart card
3) NFC mobile phone with application stored in the UICC
4) Contactless USB key
5) …

The different form factors may introduce different requirements for Secure Element. For smart cards or contactless USB keys, the Secure Element – which is the card or token microcontroller chip - will implement the RF protocol stack. For a NFC mobile phone using the UICC as the Secure Element, the RF protocol stack may be implemented in the mobile phone and not by the Secure Element (UICC),

5.4 Customer Media Interfaces

Customer Media must support proximity exchanges in contactless mode but may also provide a contact interface depending on its form factor.

When a contact interface is available, remote access through the contact interface should be possible to offer remote content management to the Application Provider (via a card reader connected to a PC, via an USB interface, …).

5.4.1 Contact & contactless interfaces

[Req14]: Customer media shall support ISO 14443 types A & B RF communication protocols.

[Req15]: Customer media shall behave like a regular contactless card from a transport network reader point of view for application transactions (validation at the turnstile, ticket top up, control operation on the train, …).

To improve interoperability between contactless cards and readers, EMVCo has defined additional requirements for implementing ISO 14443 communication protocol ([R16]). It's premature to evaluate if such recommendations are applicable to public transport Fare Management systems, but this evaluation should be done by the transport industry as:

- Multi application devices like NFC phones will have both to comply with EMVCo RF specifications and to communicate with transport network contactless readers.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

- RF protocol interoperability is not required across distinct IFM schemes and some common rules for ISO 14443 implementation may be needed.

Additional RF requirements may then be needed for reaching RF interoperability across the distinct EU transport networks.

[Req16]: The implementation of a contact interface to access to the SE remains optional.

[Req17]: APDU communication according to ISO/IEC 7816-4 shall be possible over the contact & contactless interfaces of the Secure Element.

5.4.2 Remote access and secure communication

The objective of this section is to identify the mechanisms that meet the security requirements for remote access. Those mechanisms must provide the means to secure from end to end the exchange of content management commands (i.e. GlobalPlatform commands) between an off card entity and a Security Domain.

[Req18]: The information exchanged between an off card entity and the corresponding Security Domain in the Secure Element must be secured by a GlobalPlatform Secure Channel Protocol, independently of the transport layer.

[Req19]: The support of SCP02 is mandatory to secure communication between the Application Provider and the corresponding Application Provider Security Domain (APSD) in the SE.

[Req20]: Others Secure Channel Protocols may be supported.

Remark: The usage of GP security scheme does not overlap with the possibility for each Application Provider to use its own security scheme when exchanging commands directly with its application (see §7 for more details on combining GP and application command flows).

Java contactless cards are used to simplify the life of their users, and to dematerialise product. The use of USB keys and mobile phones actually deliver more functions than full sized smartcards.

New possibilities with a USB key or mobiles phones are:

- To communicate remotely with an off card entity to download application or products for example.
- To appear as a regular smartcard when presented to a contactless reader such as a validation gate.

Furthermore, the remote mechanism would entice nothing but standard protocols:

- For USB key or smart card connected via a PC reader : HTTP and SSL to communicate with the user's browser or a proxy application in the PC,
- For mobile phones : wireless data connection to communicate with a proxy application in the mobile or OTA connection to communicate directly with the UICC,
- The GlobalPlatform protocols to load and personalise a new application,

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

- The applicative APDUs to load product in the application

That's why, for remote communication, the standard mechanism to communicate securely with a Secure Element is to use a Secure Channel Protocol (SCP). A SCP ensures the mutual authentication of both the Secure Element and the off card entity and protects the APDUs exchanged between them (over a logical channel) by encrypting and/or signing each APDU.

SCPs are specified by GlobalPlatform and different SCPs have been defined according to history and different needs:

- SCP02 with i="15" synchronous protocol based on 3DES,
- SCP02 with i="55" asynchronous protocol based on 3DES,
- SCP03 based on AES,
- SCP10 based on public keys,
- SCP80 which is the ETSI defined 102.225 OTA protocol.

Except SCP80, every SCP can be used independently of the transport layer and the communication technologies.

SCP80 provides end to end secure communicate between an off card server and the UICC. Mobile phone, being a always connected CM, SCP80 allows to manage transparently SE contents without end user interaction

SCP02 with i="55" is nowadays the preferred option for securing remote communication:

- Its asynchronous mode allows to send script of commands that can cope with low bandwidth and high latency of wireless networks,
- SCP02 is currently supported by a large range of Secure Elements.

Recommendation for SCP02 may change in the future if newer protocol such as SCP03 based on AES becomes more widely spread within the smart card industry.

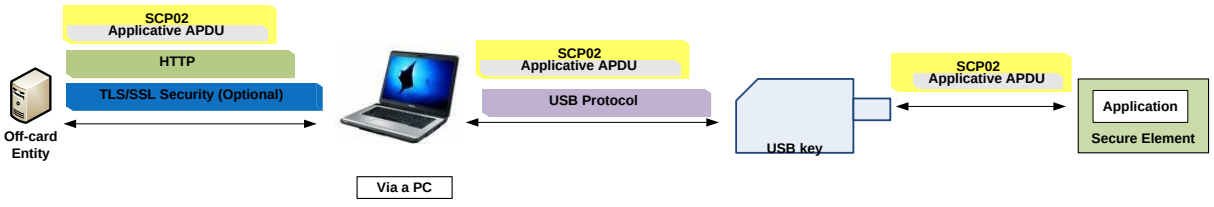
SCP02 provides the three followings levels of security that can be used independently of each other:

- Entity authentication
- Integrity and Data origin authentication
- Confidentiality

It is recommended from a security perspective that all the three levels are available for use at the convenience of each Application Owner for its application download.

The following figures describe the way to establish secure communication between an off card entity (like an application download server) and the corresponding SD in the Secure Element:

1. Secure communication via internet for a USB key plugged to a PC:



This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Fig. 5-1: Secure communication via internet for a USB key plugged to a PC

2. Secure communication with a smart card connected via contact or contactless reader to a PC:

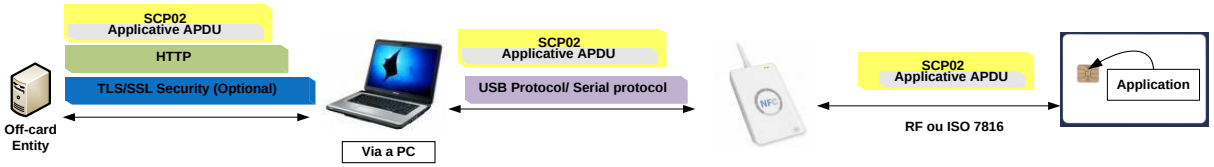


Fig. 5-2: Secure communication with a smart card connected via contact or contactless reader to a PC

3. Secure communication with a NFC phone with SIM centric architecture: [Req21]:

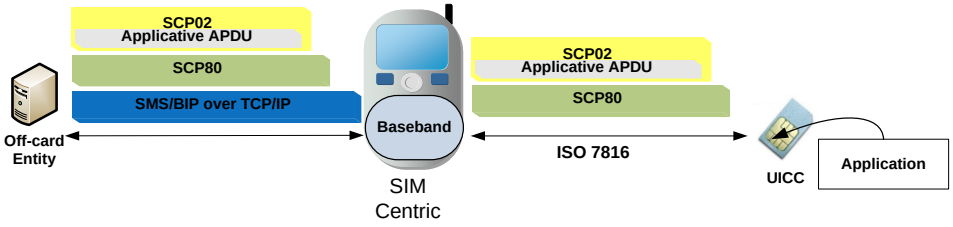


Fig. 5-3: Secure communication with a NFC phone - SIM centric architecture

For remote PC connection (1&2), a proxy application is needed in the PC to communicate with the Secure Element.

The case of SIM centric mobile (3) is a bit specific as SCP80 allows sending GP commands directly to the UICC as defined in ETSI TS102.225. The lists of available commands are defined by GP and ETSI TS 102.226. The SCP80 can be used over SMS or BIP transport protocols. In this case SCP02 is used to encrypt the message destined to the APSD and SCP80 is used to protect the OTA communication. No proxy application is required in the phone in this case to access to the Secure Element.

The following scheme summarizes the possible ways of setting up a secure remote communication with a Secure Element in order to load and personalise an application.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

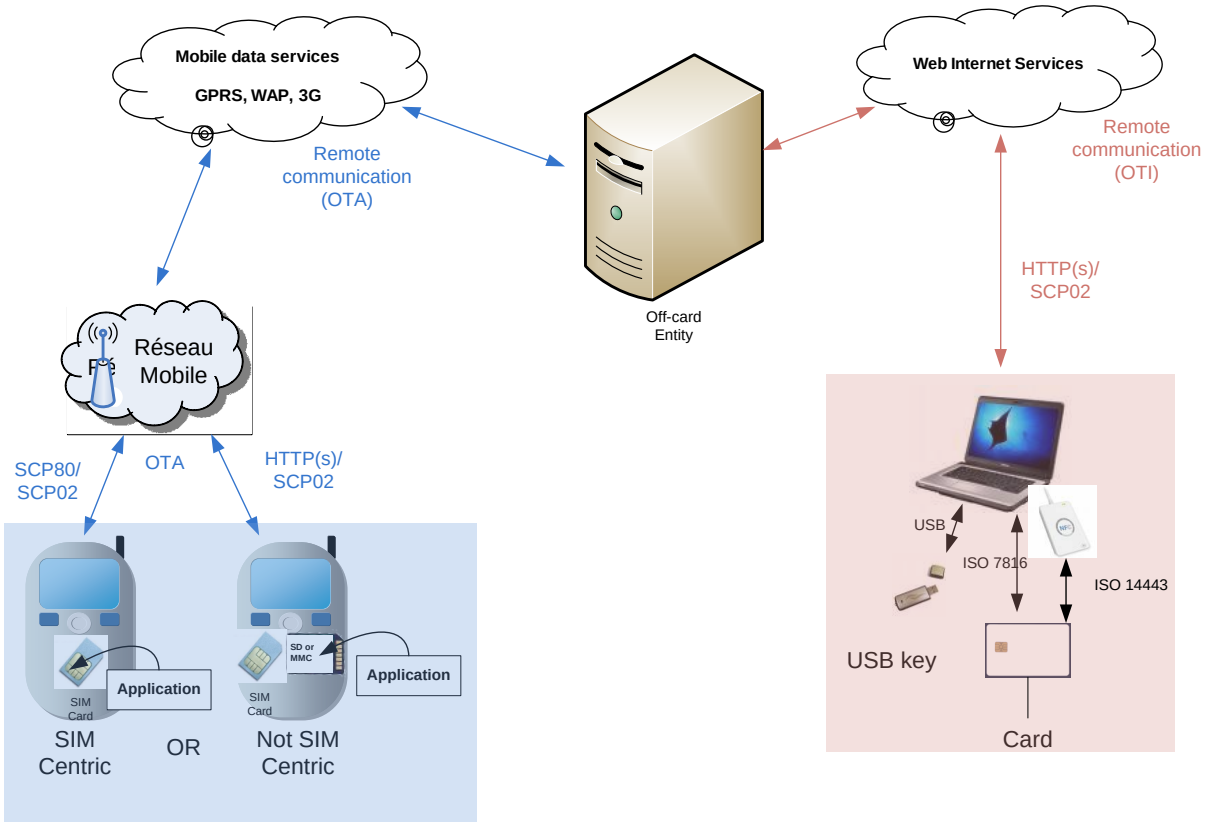


Fig. 5-4: Different scenarios of remote communication with a Secure Element

The following table summarizes the available standardized interfaces per type of Customer Media;

Type of Customer Media	*SE*	*SE Contact Interface*	*SE Contactless Interface*
Contactless smart card	IC Chip	None	ISO 14443 ([R3])
Dual (contact & contactless) smart card	IC chip	ISO 7816 ([R4])	ISO 14443 ([R3])
NFC mobile phone with application stored in the UICC	UICC	ISO 7816 ([R4])	None (*)
Contactless USB key	IC chip	ISO 7816 ([R4]) over USB protocol	ISO 14443 ([R3])

(*) The UICC is connected via a single wire interface (ETSI HCI data protocol [R8] over SWP link [R7]) to a NFC chip that provide mobile phone with an ISO 14443 interface.

5.5 Customer Media ‘s profile

In addition to the functional and technical requirements, each customer media will have its own characteristics in terms of supported features, available memory size and execution performance.

Such characteristics are known by the SE Owner, but not necessarily communicated in a standardized way to the Application owner.

These characteristics are important for the Application Owner to determine if a 3rd party Customer Media can be eligible for hosting its application and there is a need for exchanging such information in a standardized way.

[Req22]: Each customer media shall be assigned a “SE profile” by the SE Owner.

[Req23]: The SE profile shall include a set of information including:

- List of supported RF protocols
- List of supported algorithms
- Available memory size
- Performance class

The way performance class is assigned to a SE shall be defined through a universal method. This can be based on the usage of a public test application providing execution times for elementary operations (read/ write/crypto computation / etc …) and from which different performance classes should be derived according to results.

[Req24]: The SE profile data will be held on the media. The SE profile shall be freely accessible in read mode over the air or through the contact/contactless interface of the SE.

5.6 Customer Media certification

For mono application media, certification process was generally a monolithic process including the test of the chip, of the operating system and of the application.

In a multi application and dynamic environment where applications can be pre loaded or loaded post issuance, such a certification is not adapted anymore as the introduction of a new application cannot imply the full retesting of the complete media.

Based on recent works aiming at targeting UICC certification in the NFC ecosystem, a new approach has been proposed, named “Composite evaluation”.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

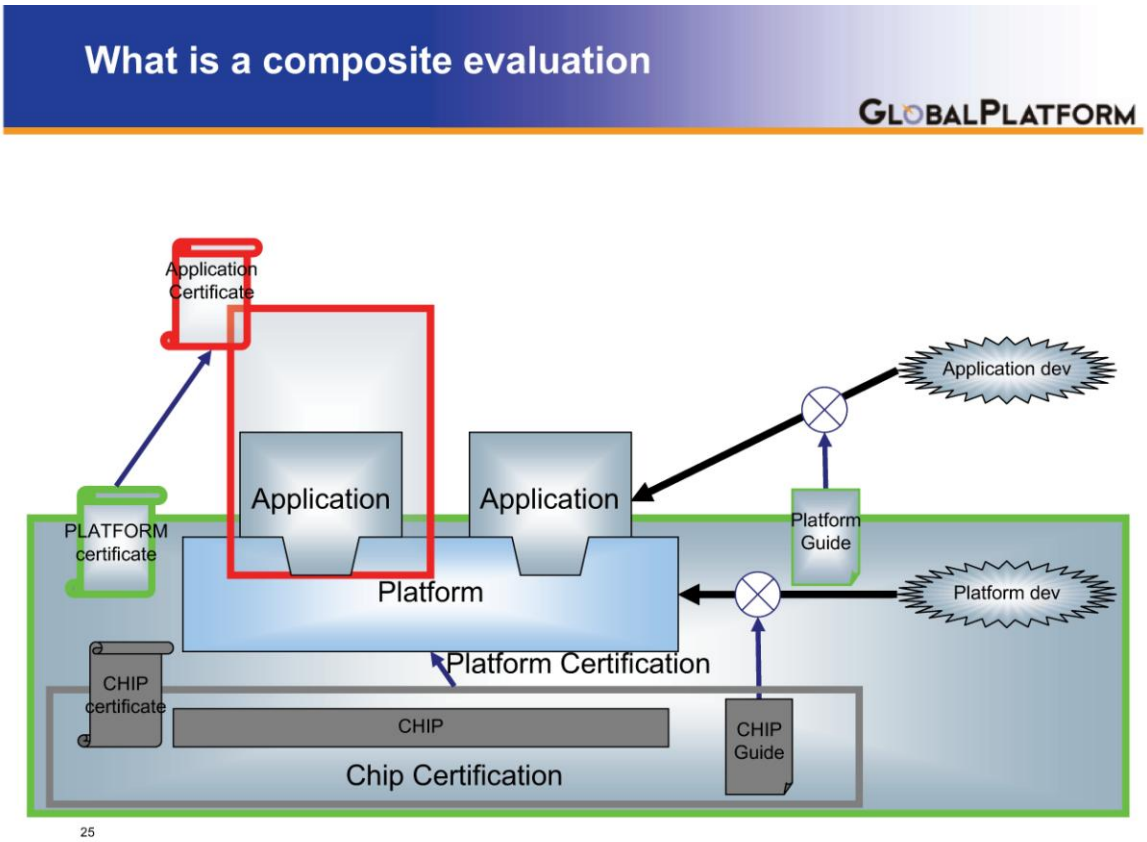


Fig. 5-5: Composite Certification of Customer Media *(source GlobalPlatfom)*

The aim of this new evolutionary certification scheme is to make more cost and time effective application certification by going through a composite certification process:

- **Chip certification:**
  Chip certification shall be achieved nearly as usual via standard Common Criteria certification. Generally the most demanding industry (payment) is requiring an EAL4+ certification for IC Chip. The public transport industry may very likely cope with a lower level of EAL chip certification such as EAL1+. The definition of the minimum threshold for chip certification is not crucial anyway, knowing that cross industry media will need finally to reach EAL4+ to match the payment industry requirements,
  Chip certification shall be managed by chip manufacturer.

- **OS certification:**
  OS certification shall be specified for a new defined perimeter excluding applications. The OS certification shall check in particular compliance with Java Card and GlobalPlatform mechanisms. This certification shall be managed with media manufacturer and shall require cross industry players to agree on a new Protection Profile per type of media. Initiatives are on going in EU to define a UICC Protection Profile for the NFC use case with the involvement of GlobalPlatform, EMVCo, Mobile Network Operators, Certification Authorities and SIM vendors.

- **Application certification:**
  Each certification shall be managed independently from other application' certification. Application certification is managed by the Application Provider and certification tests are application dependent.
  The composite approach shall allow to the coexistence of standard and secure applications.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Standard application shall require some validation test to ensure that the application is using the OS platform in compliance with the security rules defined for OS certification.

Secure application shall go through the same validation test than standard applications and in addition shall need to go through a Certification process to ensure that the application is protecting appropriately its own assets (keys, sensitive application data, …) according the Security policy defined by the application provider.

It's very likely that most of the Transport application owners will consider their application as needing to be secured and will ask for application certification.

The respect by all the applications of the OS security guidelines and the certification of the underlying OS shall warranty to each application owner that its application is executed in a trusted environment.

The certification by composite approach is leading then to the following requirements:

[Req25]: Platform Certification: The Secure Element chip shall be certified with CC EAL1+ or higher.
Platform certification shall be under the responsibility of the SE owner.

[Req26]: Application's SE validation: Each public transport application shall be tested to check that it uses the (Java Card) OS platform in compliance with the security rules defined for OS certification.
SE validation shall be under the responsibility of the SE owner.

[Req27]: Application's Application Owner certification: If a certification process exists for public transport application, each application shall be certified according to the defined process.
AO certification shall be under the responsibility of the Application Owner.

The following table summarizes the certification modules and the responsibility of SE and Applications owners in the certification process.

Certification module		Responsible	Objectives
Platform Certification		SE Owner	Ensure that the platform environment can provided a trusted and isolated environment for application execution.
Application	SE Validation	SE Owner	Check the innocuousness of application towards SE environment and other applications on the SE.
	AO Certification	Application Owner	Validate application implementation versus application specifications and eventually check the way application protects its secret data.

[Req28]: There shall be some cross recognition of application validation between SE Owners to avoid an Application Provider to have to re-validate its application for every SE Owner proposing the same type of SE.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

6 Links between IFM and non IFM roles

Technical Committee ISO/TC 204, *Intelligent Transport Systems*, Subcommittee WG8 , and Technical Committee CEN/TC 278 WG3 SG5, *Road Transport and Traffic Telematics* are currently working on ISO/CEN 24014-2 standard ([R2]).

This new standard document aims to give a tool which gives a clear and unambiguous picture of Part 1 and its relationship with related systems, such as, other IFMS, mobile and financial systems, from a broader multi-application view.

At the time of the writing of the present document, standardisation work is still on going within the TC204 and TC278.

The present chapter is aiming at depicting an extended IFM model in multi application context taking into account the latest 24014-2 standardisation work and to highlight the impact on existing IFM scheme for accepting multi application CM not fully owned by the IFM actors.

Some initial business elements are included in the present document, but further organisation considerations will be addressed in the Work Package 4 document "**Development of cooperative organisational models**" As a consequence, only media related requirements will be expressed in this chapter, all the organisation related requirements will be defined in WP4 document.

6.1 Cross References from IFM standard ISO 24014 -1

The way IFM systems are represented and addressed in the ISO standard are extracted below:

Interoperable fare management (IFM) encompasses all systems and processes designed to manage the distribution and use of fare products in an interoperable Public Transport environment.
Such systems are called interoperable when they enable the customer to use a portable electronic medium (e.g. a contact/contactless smart card) with compatible equipment (e.g. at stops, with retail systems, at platform entry points or on board vehicles). IFM concepts can also be applied to fare management systems not using electronic media.
Potential benefits for the customer includes reductions in queuing, special and combined fares, one Medium for multiple applications, loyalty programs and seamless journeys.
Interoperability of fare management systems also provides benefits to operators and the other parties involved. However, it requires an overall system architecture that defines the system functionalities, the Actors involved and their roles, the relationships and the interfaces between them.
Interoperability requires also the definition of a security scheme to protect privacy, integrity and confidentiality between the Actors to ensure fair and secure data flow within the IFMS.
The overall architecture is the subject of this document. The standard recognises the need for legal and commercial agreements between members of an IFM, but does not specify their form. The technical specifications of the Component parts, and particularly the standards for customer media (e.g. smart cards), are not included.
Note that there is not one single IFM. Individual operators, consortia of operators, public authorities and private companies can manage and/or participate in IFMs. An IFM can span country boundaries, and can be combined with other IFMs. Implementations of IFMSs

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

require security and registration functionalities. This standard allows for the distribution of these functions to enable the coordination/convergence of existing IFMSs to work together.

.....
;;;;;
This standard covers the definition of a conceptual framework, which is independent of organisational and physical implementation. Any reference within this standard to organisational or physical implementation is purely informative.

Obviously and as addressed in the next chapter, multi application customer media handling introduces some changes in the system functionalities with new roles, and new relationship and interfaces between them.

In line with the IFM 24014-1 standard, the same rules apply to the IFM project and by consequence to this document :

- **The IFM project will define the new roles and the related new relationship and interfaces between new and existing roles.**
- **The IFM project recognises the need for new business agreements but does not specify their form,**
- **The IFM project defines role but does make any assumption on how Actors may organize themselves to cover one or several roles, can span over several IFMSs or can establish joint agreement for performing one role through several Actors, …,**
- **Any reference within this standard to organisational or physical implementation is purely informative**

6.2 Extended IFM mode in multi application context

The usage of multi application media not only dedicated to the hosting of transport applications is introducing new links and new roles in relation with the existing IFM conceptual model.

New actors, external to the IFM model are going to play a role in the life cycle of the IFM customer media, and by consequence on the life cycle of IFM applications and products.

The Customer Medium contains a Secure Element that hosts and executes the applications. Because the Secure Element, can be embedded or removable, the management of the Secure Element can therefore be different from the management of the Customer Medium itself. Hence, the new roles an d functions are focused on the life cycle management of the Secure Element rather than the Customer media itself.

The following scheme represents a global view about how the IFM conceptual model should be extended to include the new actors outside transport domain that will manage the SE life cycle and must interact with the roles of the IFM model.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

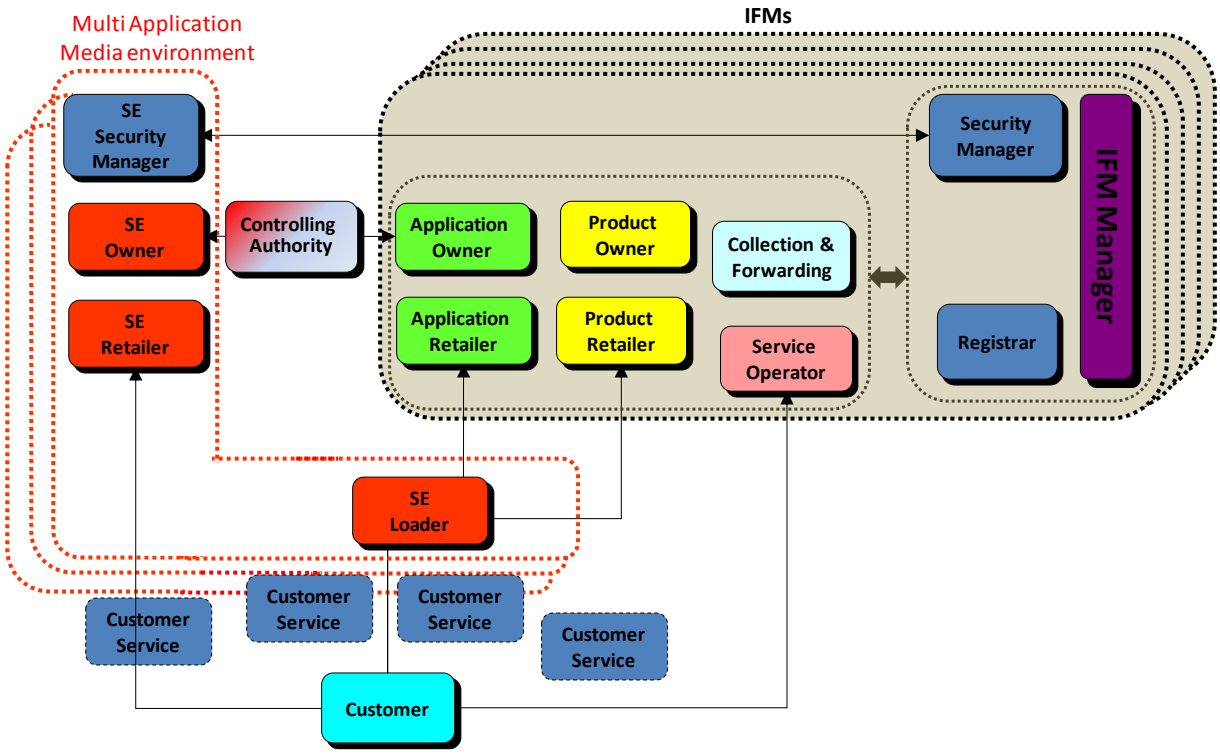


Fig. 6-1: Extended IFM model in multi application context

The new actors involved in this extended IFM conceptual model are:

SE Owner:

- Defines the specifications and design of the SE, complying with the requirements of the SE Security Manager
- Authorises the Application Retailer to access, load and update applications on the SE.

SE Retailer

- Provides Secure Element to customers and the related customer service
- Guarantees to customer the compliance of the SE to the requirements set by SE security manager

SE Loader:

- Is required by the Application Retailer to operate loading / deletion / updating of applications in the SE as authorised by SE owner and by Application Owner
- Manages customer's directives as authorised by SE owner and Application owner if conflicts appear when loading/updating an application (e.g. overflow of SE's capacity, conflicting applications, …)

SE Security Manager

- Specifies security requirements that apply to Secure Elements and to their operation process
- Determines the corresponding validation process of Secure Elements (Validation Authority as defined in GP).

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Controlling Authority

- Is a trusted third party both for the SE Owner and for the Application Owner
- Enables application code and personalization data confidentiality for Application Owner/Provider towards SE Owner during post issuance loading and personalization of application (see GP specifications [R10] for a complete description of Controlling Authority role)

These new roles have also impacts on the existing IFM roles that must be extended to integrate the following functions:

IFM Security manager

- Acknowledges the proper security of the secure element as compatible with the IFM security requirements and relies on SE Security manager to validate compliance of each SE device
- Specifies security requirements for SE Loaders

Registrar

- Registers authorised Secure Elements
- Registers SE Loaders to allow Application Owners to contract with them

Application owner

- Contracts with SE Owner to use registered SE for his Application
- Authorises Application Retailers to contract with registered SE Loaders

Application retailer

- Contracts with registered SE Loader as authorised by Application Owner

6.3 Secure Element Registration

For several distinct IFMs scheme, the same Secure Element can be used to host the different IFM applications.
Hence, a SE Security Manager will have a “one to many” relationship with IFM Security Manager and Registrar pairs. Reciprocally, because each IFM may accept different types of multi application CM, each IFM Security Manager and Registrar pair will have a” one to many” relationship with SE Security Managers.

To offer a seamless acceptance of multi application media into IFM schemes, it is essential to have **a single certification and validation process** of Secure Element handled by the SE Security Manager and not replicated by each IFM scheme.

[Req29]: Secure Element should be certified only once by the SE Security Manager entity.

[Req30]: The validation or certification process for multi application media shall check the compliance to the requirements listed in the present document.

One of the point raised by the IFM project members is that the public transport industry is lacking of a global EU representation for monitoring that public transport requirements are properly taken into account by SE owners.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

The payment industry is organized through EMVCo and international payment schemes organizations. The mobile telecom industry is organized through ETSI and GSMA organizations.
An equivalent organization at EU level should be set up for the public transport industry to define public transport requirements for the specification, testing and certification of cross industry customer media.
The need for such an EU representation and the role it shall have is further developed into Work Package 4 document "**Development of cooperative organisational models**".
.

It is very important that the present list of requirements is considered as adequate and exhaustive for multi application CM acceptance by all EU IFM schemes. The success for reaching downloading interoperability is relying on the acceptance of the same common requirements by all IFM.

As a next step, this list of requirement should get disseminated within the transport industry via the IFM Forum and also shared for cross adoption with the other sectors of the industry (banking, retailer, access control, hotel …) which are looking for interoperable and multi application customer media.

It would a major drawback to make a mandatory prerequisite the pre-registration of the SEs by IFM scheme. One of the main objectives of using multi application media is for IFM scheme the ability to be able to accept third party CM which are distributed according to distribution channels not necessarily managed by the IFM actors and relying on business model where transport application hosting is representing only a part of the revenues.

The main points to be checked for accepting and registering a multi application CM by an IFM scheme are:

1. To retrieve SE ID, SE Owner and SE Security Manager information directly from the CM
2. To check if the Application Owner can be authorized by the SE Owner to load its application into the SE (a business agreement shall be already in place between SE Owner and Application Owner).
3. To send SE Security Manager identification to the IFM Security Manager
4. To ensure via the SE Security Manager that the SE is compliant to the present multi application Customer Media requirements and to eventual additional local IFM scheme requirements.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

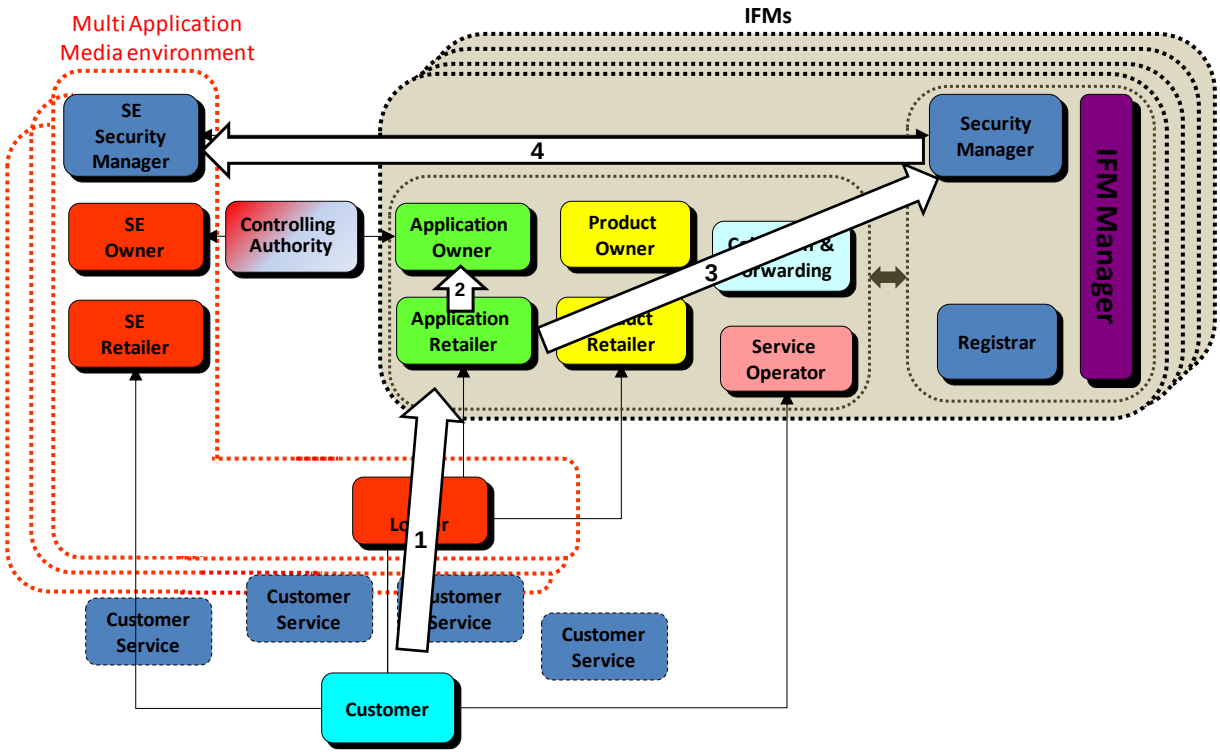


Fig. 6-2: Main steps for SE registration

[Req31]: The registration process for SE shall be handled dynamically and shall start at the time when a customer requests to download a transport application on its CM.

Step 1:

[Req32]: The Secure Element shall provide a unique identifier that can later allow the Registrar to uniquely identify the SE within the IFM scheme.

[Req33]: The Secure Element shall provide a mean for identifying the SE Security Manager via a SE Security Manager URI and the SE Owner via a SE Owner URI.

[Req34]: Any Application retailer shall be able to read from a Secure Element the SE Security Manager URI and the SE Owner URI data, either via the contactless interface, via the contact interface (when any) or remotely.

For example, URI data could be retrieved via a GP Get_Status or Get_Data command sent to the Controlling Authority SD (CASD) or to the ISD which could return the 2 URIs.

Step 2:

[Req35]: Upon retrieval of SE Owner URI, the Application Retailer shall check whether the Application Owner has a business agreement in place with the SE Owner.

Step 3:

[Req36]: Upon retrieval of SE Security Manager URI, the Application Retailer shall send this information to the IFM security Manager for processing.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Step 4:

[Req37]: Upon retrieval of SE Security Manager URI, the IFM Security Manager shall be able to connect via the URI to receive evidence of the SE certification.

[Req38]: The IFM Registrar shall register the SE as authorized SE upon successful verification of the evidence of the SE certification.

After all this process is complete, the SE should be registered in the IFM and ready for application and product loading.

6.4 Business Agreements between IFM and SE roles

As indicated in the §6.2 role definitions, some business agreements must be set up by each IFM scheme:

A. Between Application Owner and SE Loader to define the term and conditions under which the SE loader is able to operate the loading, personalisation and delete of the application into SEs for any Application Retailers.

B. Between SE owner and Application Owner to define the term and conditions under which the SE owner is ready to host the Application Owner's applications into its SEs.

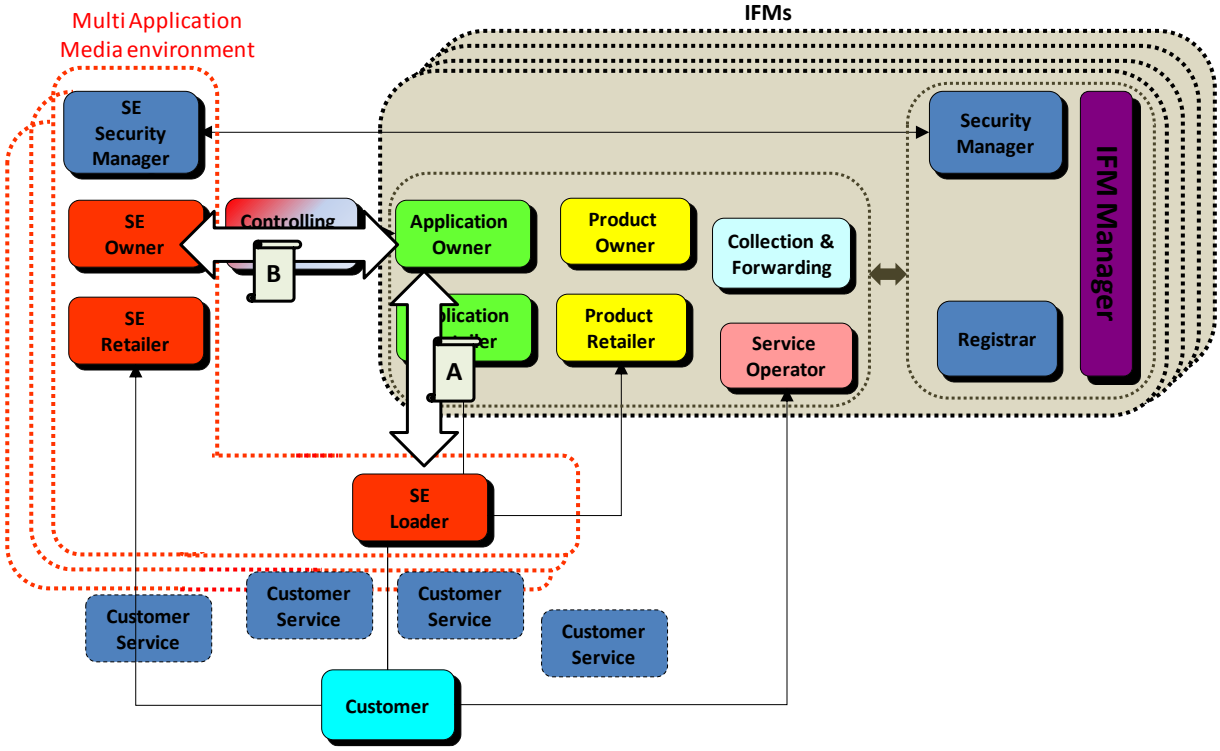


Fig. 6-3: Business agreements with non IFM entities

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Application Owner / SE Loader agreement:

The SE Loader will have to provide connection to the CM via a WEB connection (USB key, smart card connected to the user's PC) or via a mobile network (NFC phones) and to enable secure communication over those networks.

For Web connection, a Web Access Provider can provide a service that may allow addressing any SE connected via the WEB. So a single business agreement should be sufficient per Application Retailer.

For NFC ecosystem, the problem is different and a central issue for large scale roll-out is: "How to create an interoperable mobile NFC ecosystem that makes it easy for Service Providers (SP) and Mobile Network Operators (MNO) to work together?"
The GSM-A answer was the creation of the role of Trusted Service Manager (TSM) who is in charge to make the link between the SP world and the MNO one from a technical and business point of view.

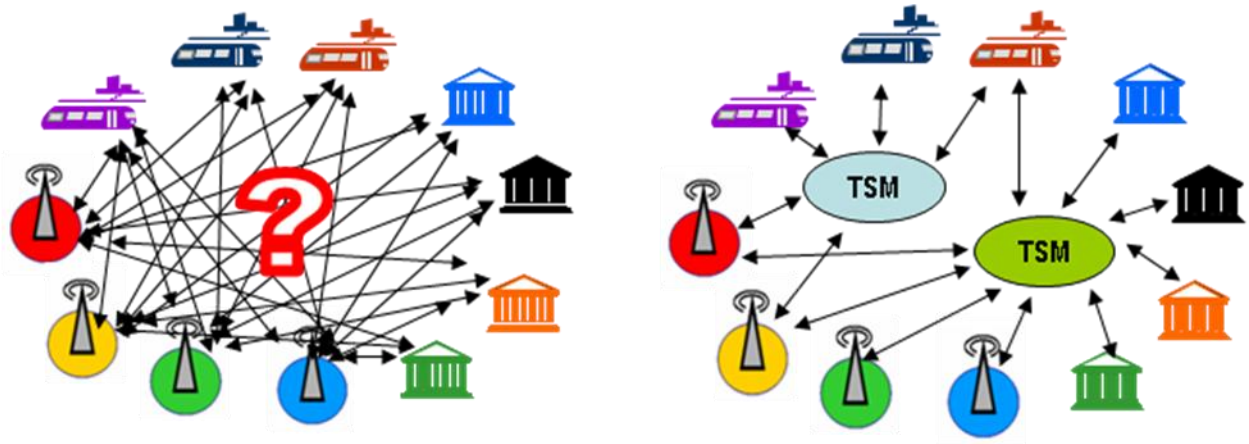


Fig. 6-4: Trusted Service Manager Role

A TSM will provide technical bricks such as OTA platform and Card Management System that will allow SP to perform SE content management over a given set of mobile networks.

A TSM may also have a business role with business agreements already in place with several SE owners (MNO, SE chip manufacturers, mobile handset manufacturers, …). Such agreement may allow a TSM to retail SE space to Application Owners and remove the need for a business agreement between SE owner and Application Provider.

Moreover, even if the TSM concept comes from the NFC ecosystem, some TSM are also proposing to manage SEs over the Web as it represents only few additional investment for them.

By relying on TSM actors that can act as business facilitators, Application Providers can drastically reduce the number of business agreements to set up per IFM Scheme.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Application Owner / SE Owner agreement:

The core concept of multi application media is the ability for an Application Owner to find a business agreement with a SE owner in order to be able to distribute its application into the SE of a third party Customer media.
The SE Owner role can be assumed by entities like an IFM scheme offering to others IFM schemes to host their transport applications into its media, or a Mobile Network Operator offering to load application in the UICC of customer's NFC phones.

In all cases, the SE Owner must be perceived by the Application Owner as both a trusted and an accountable entity for SE content management.

Definition of the trust criteria that can make possible such agreement are investigated in the WP1 of this project.

6.5 Data links between IFM and SE roles

When looking at the data that need to be exchanged between IFM and SE roles, the following new links must be established:

SE Owner / Application retailer:
The Application retailer must get from the SE owner an **authorization** and the necessary **keyset** to access to the SE media in order to perform the necessary operations to install and manage its application.

Application retailer / Controlling Authority:
The Application Retailer may wish to update the keyset received from the SE owner and allowing him to access to the media. The keyset can be updated according to the confidential key renewal process described in Global Platform specification ([R10]) involving some exchanges between the Application retailer and the Controlling Authority. Once this key process is performed, the Application Retailer and its on card representative (its APSD) are the only ones to know the keyset values.

.
Application retailer / SE Loader :
The Application Retailer must rely on a SE Loader to establish the secure communication between its Off Card / server environment and the Secure Element.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

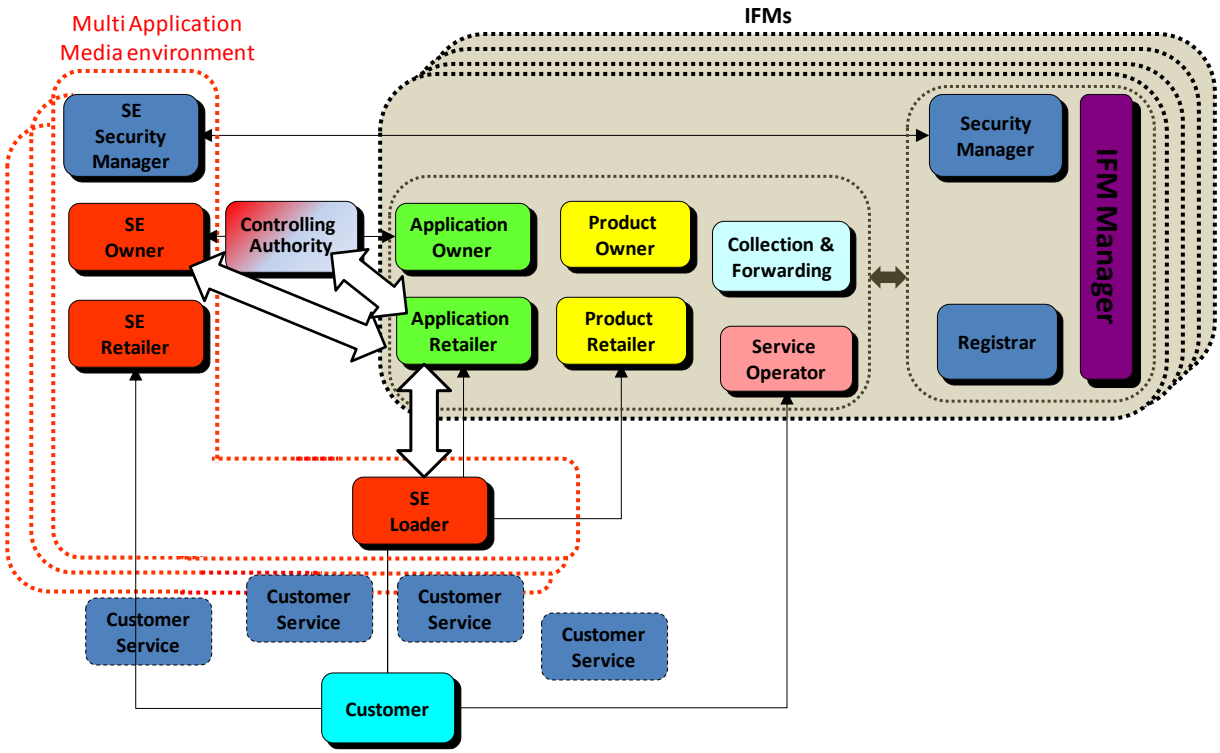


Fig. 6-5: Operational links with non IFM entities

As described in §5.4.2, the secure communication is built on a 2 layers:

- A GP Secure Channel Protocol is used to secure the data exchanged between the Application Retailer (or Application Provider according to GP terminology) and its Security Domain into the SE.
- A secure transport protocol is used to secure the data transportation over the network (Http(s) for web connection and mobile data connection, SCP80 for OTA connection when the UICC is the SE).

The security of each layer is managed totally independently.

For the same reason as explained in the previous chapter, the TSM can be a facilitator for simplifying the number of data link that an Application retailer must set up with SE Loader. A TSM can offer to be the unique entry point for routing the message and ensuring the transportation security for several mobile networks.

A first keyset is needed by the Application Provider from the SE owner to be able to establish a GP secure session with the SE. The first operation of the Application Provider will be to replace the initial keyset according to standard GP mechanisms ensuring that the new keyset can only be known by the Application Provider (this will need exchanges with the Controlling Authority).

As a consequence, in some cases TSM can also be delegated by the SE Owner the ability of creating and forwarding the initial keyset to the Application Provider in an autonomous way.

By relying on TSM actors that can act as technical facilitators, Application Providers can drastically reduce the number of data links to set up per IFM Scheme.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

7 Common requirements for multi application management

The requirements for multi application management shall address the whole life cycle of applications:

- Application loading when not pre loaded at customer media issuance
- Application personalization and activation
- Application deactivation
- Application removal

7.1 Main phases of application installation

This chapter describes the different stages in the installation of the transport application adapted to a Customer Media context.

These phases assumes that the SE has already been registered into the IFM scheme as described in the previous chapter (§6.3).

Application installation is made up of 4 phases:

- Application Loading:
  - The Application Provider Security Domain is created if not already existing.
  - The application code is loaded under the Application Provider Security Domain.
  - If the application code is already preloaded in the SE, the code may be just “extradited” to the Application Provider Security Domain.
- Application Instantiation:
  - The application is created and memory space is assigned for application data.
- Application Personalisation:
  - A set of commands is sent to configure the application.
  - This phase can be performed after or before Application activation
- Application Activation;
  - Before this phase, it is not possible to send commands to the application.
  - The application is able to be selected and commands can be send directly to the application.

The following scheme represents the different steps for loading, instantiating, personalizing and activating a transport application.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

One of the critical phase of application installation is the secure provisioning of the transport application key :

- For some application, proprietary mechanism already exists to allow the secure provisioning of the application keys without requiring any transport protection for the exchanged commands. This is the case for VDV KA application for example.
- For others applications, GlobalPlatform can provide standard mechanism to securely provision the transport application key by transporting the commands via a Secure Channel. This is the case for Calypso application for example.

These 2 options are detailed hereafter.

7.2 Installation with key provisioning secured by GP

When a security mechanism is required for protecting the provisioning of application keys, the communication between the Application Provider and the Application Provider SD (APSD) in the SE can be secured via a GP Secure Channel Protocol.

A personalisation script must be defined by each Application Provider to personalize the transport application data according to its specific requirements based on GP STORE DATA commands which allow to personalize an application through its Security Domain.The personalisation script is sent to the APSD via SCP02.

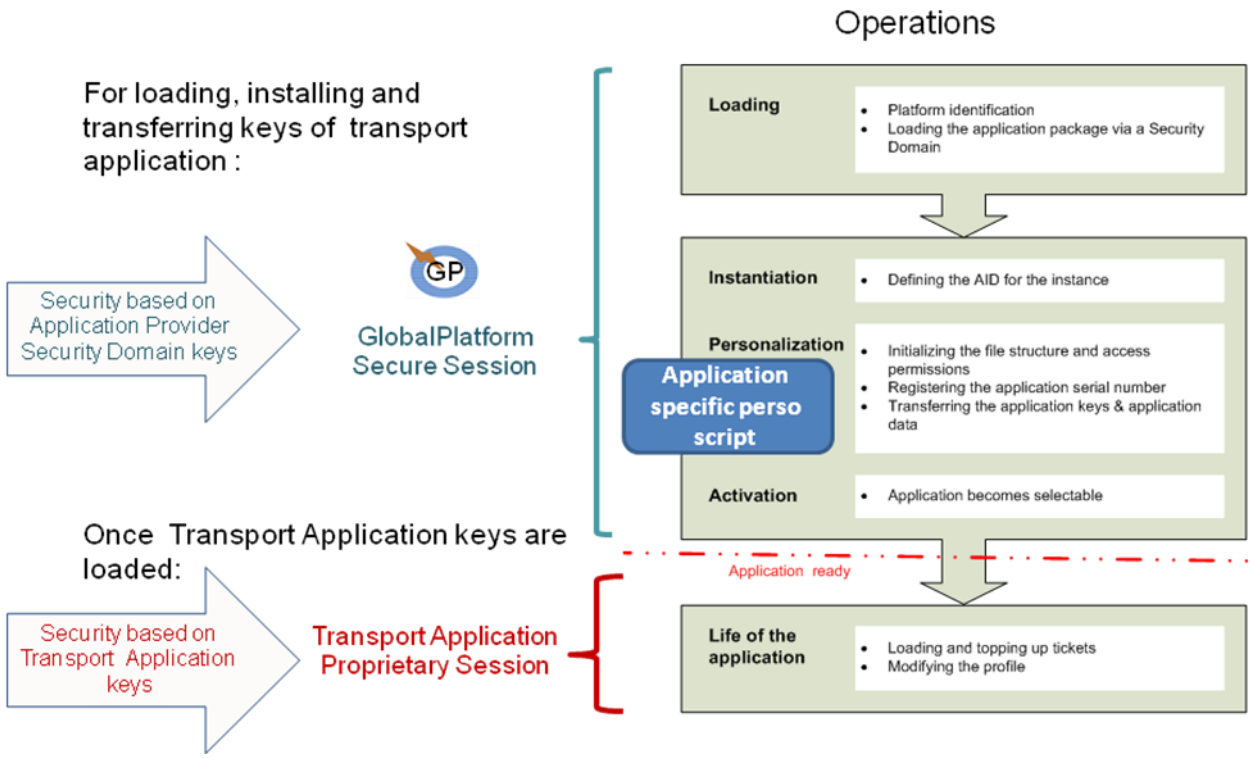


Fig. 7-1: Installation phases of a transport application with perso secured by GP

The following diagram gives an outlook of the command flows used for application installation when the personalisaion is secured via GP Secure Channel.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

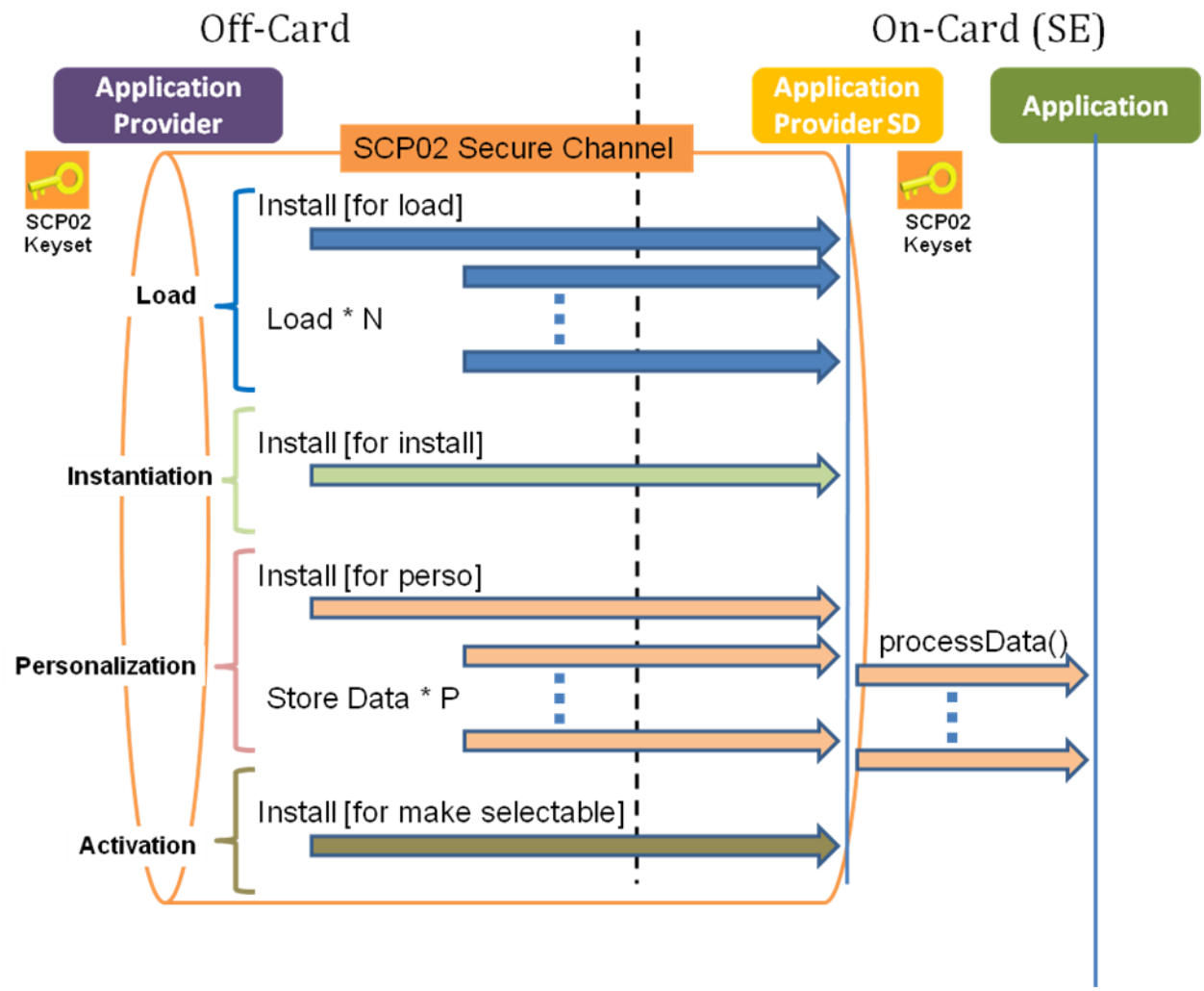


Fig. 7-2: Flow of commands for application installation with perso secured by GP

7.3 Installation with proprietary key provisioning

When the set of application commands exchanged for personalizing is already including the necessary security mechanisms to protect the exchanged data, the installation can be performed as described in the scheme hereafter.

Once the application is activated, the personalisation is performed by sending directly the usual personalisation command to the application.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

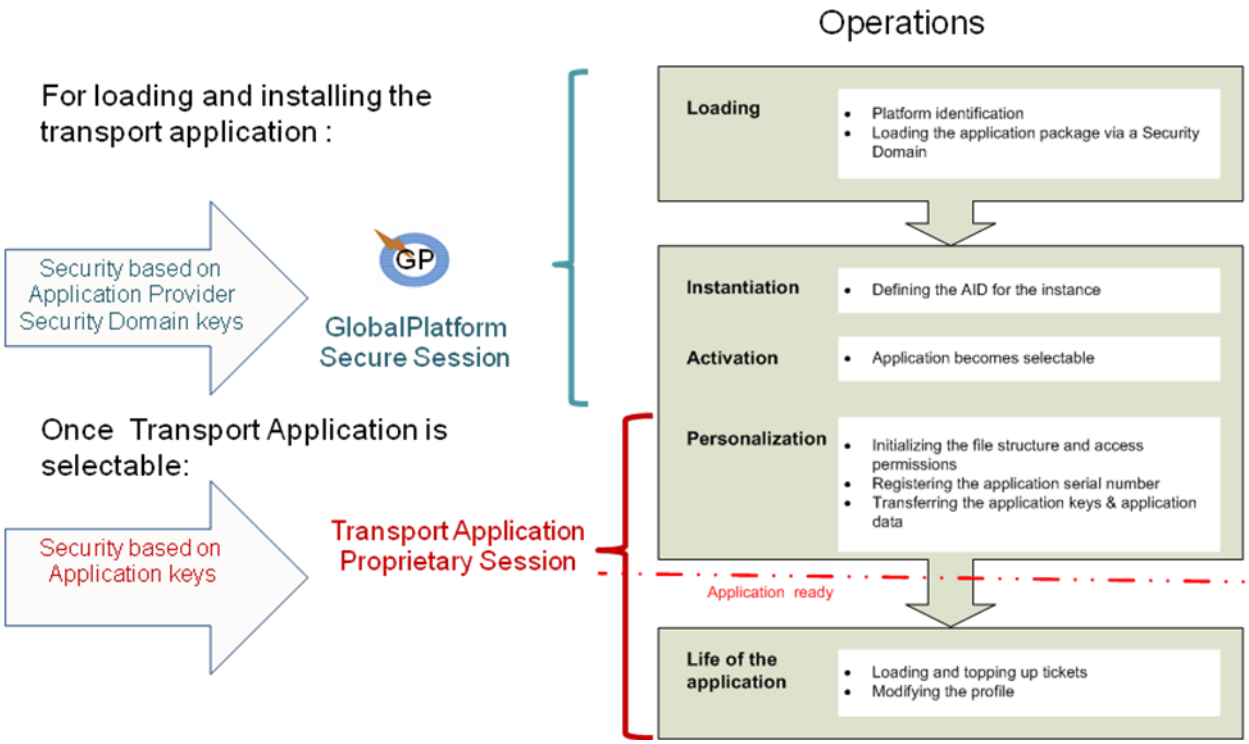


Fig. 7-3: Installation phases of a transport application with proprietary perso

The following diagram gives an outlook of the command flows used for application installation with a proprietary personalisation script.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

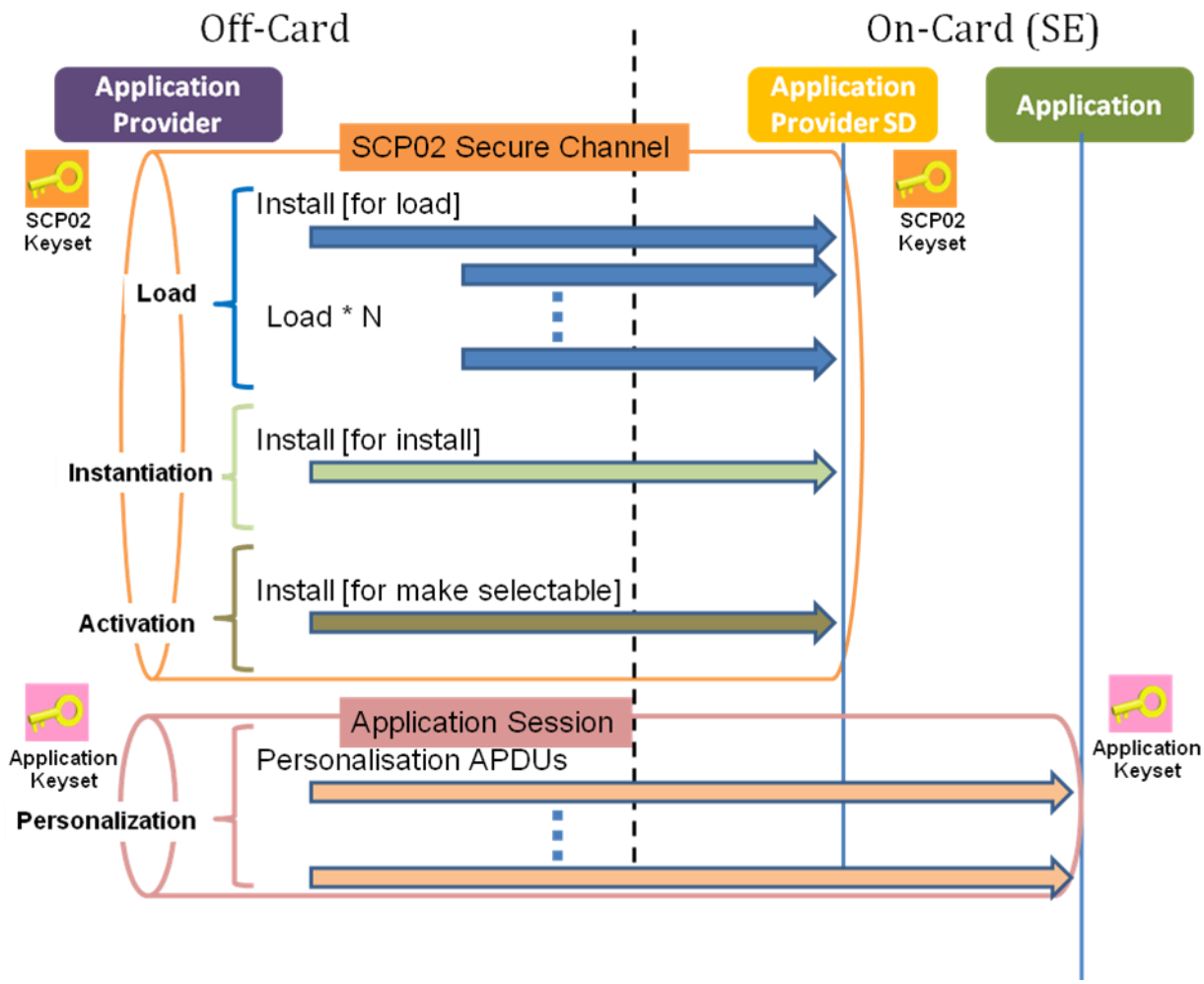


Fig. 7-4: Flow of commands for application installation with proprietary perso

7.4 Application Package

[Req39]: In order to be downloaded in a multi application CM, the transport application must be available as a Java Card Application package.

[Req40]: The application shall first be subject to certification and/or validation according to the IFM management rules defined by the Validation Manager and the Security Manager.

[Req41]: The Customer Media/Secure Element must be subject to certification and/or validation according to the rules defined by the SE Manager (see §6.3 for more details on relationship between SE roles and IFM roles).

[Req42]: The SE must be registered by the IFM Registrar (see §6.3 for more details on relationship between SE roles and IFM roles).

[Req43]: The application loading, installation and personalization phases until the stage when application is ready to receive and treat applicative commands shall be managed via GlobalPlatform process as described in GP2.2 card specifications ([R9])

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

for all type of SE and according to GP UICC Configuration Guide ([R11]) for NFC phone where the SE is the UICC.

[Req44]: Once the application is ready to receive and treat applicative commands, the application shall be able to exchanges data via its contactless and contact interfaces without any impact on the application session handling.

7.5 Loading phase

Every application in a GlobalPlatform SE is assigned to a Security Domain (SD).

An Application Provider Security Domain (APSD) must be then created and assigned to the Application Provider in order to host the transport application.

The SE Owner owns the Issuer Security Domain (ISD) keyset and is able to open a secure communication with the ISD in order to request an APSD creation.

The SE Owner creates an Application Provider Security Domain (APSD) and forwards the APSD keyset to the Application Provider. At this stage, the APSD keyset is both known by the SE Owner and the Application Provider, hence no confidential application loading and personalisation can occur.

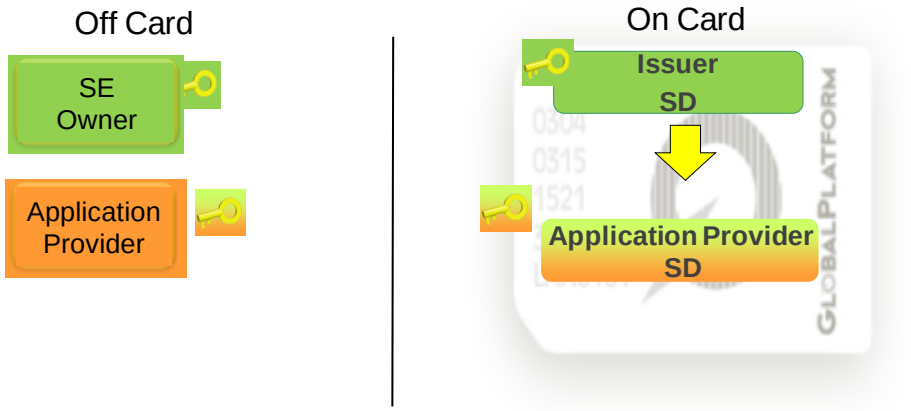


Fig. 7-5: Initialisation of APSD keyset

[Req45]: To establish confidentiality, the Application Provider shall push its own keyset into the APSD (Application Provider Security Domain) or retrieve an onboard generated keyset from the APSD in a confidential way.

This APSD keyset update shall be performed according to the scenarios specified in GlobalPlatform Card Specifications 2.2 – Amendment A ([R10]).

This requires the involvement of a third party which is named the **Controlling Authority**. The controlling authority is a neutral entity that can enforce the security policy on all application code loaded in the SE and enables an Application Provider to manage the keys of its APSD

in a confidential manner, i.e. keys remain unknown from all actors except from the Application Provider itself.

Several scenarios are proposed in GlobalPlatform to generate a keyset for the Application Provider in a confidential way. The following example is only one of the proposed scenarios which may be the simplest to implement as it requires **no interaction of the Application Provider with a third party**.

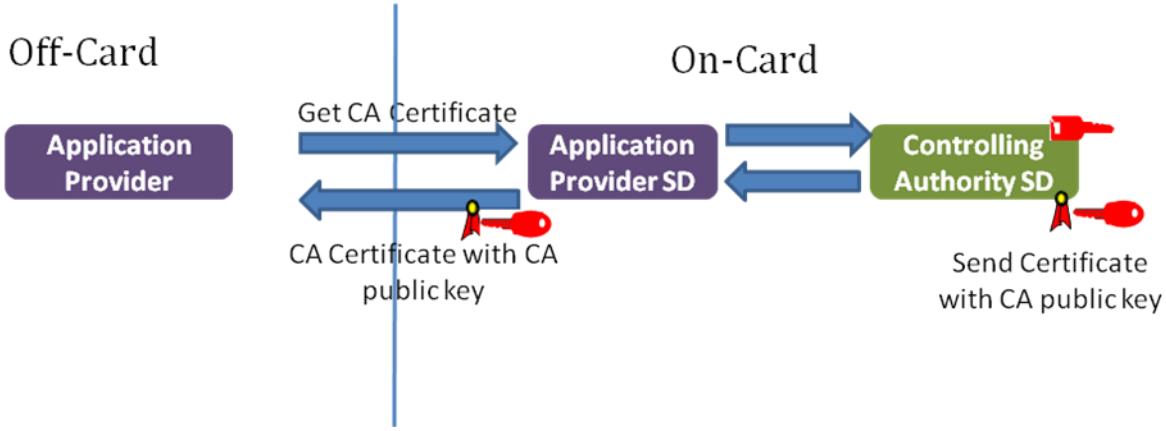


Fig. 7-6: Application Provider retrieves the CA Certificate

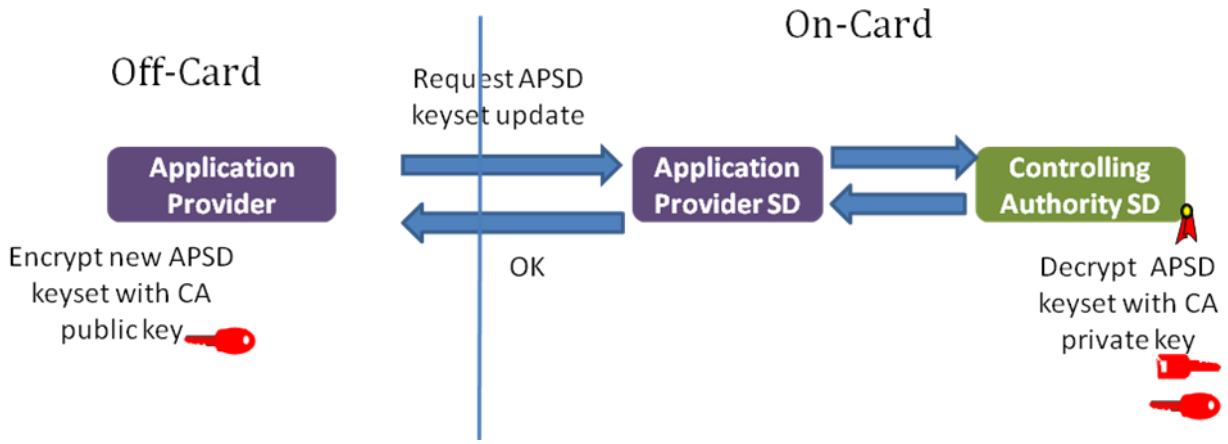


Fig. 7-7: Application Provider updates of the APSD keyset

From this stage, the Application Provider is the only one to know the APSD keyset.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

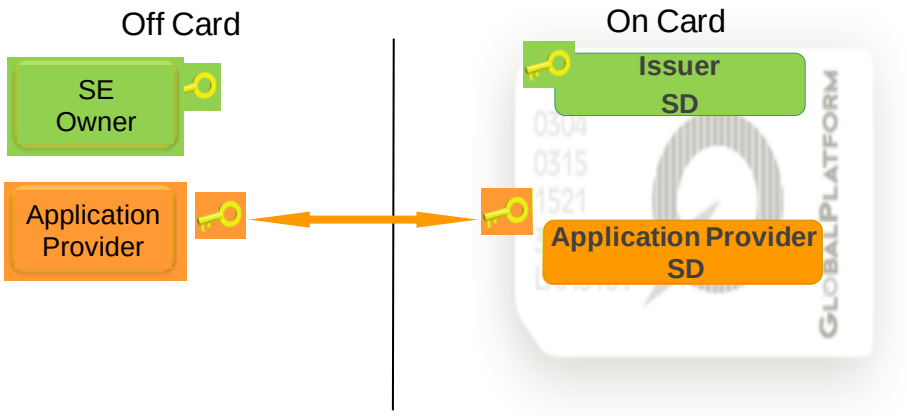


Fig. 7-8: Update of APSD keyset

Application Provider can then download and configure its application via the APSD Secure Channel in a confidential way via a SCP session. Application code and application keys can be then transferred in a confidential way from the Application Owner to the Customer Media.

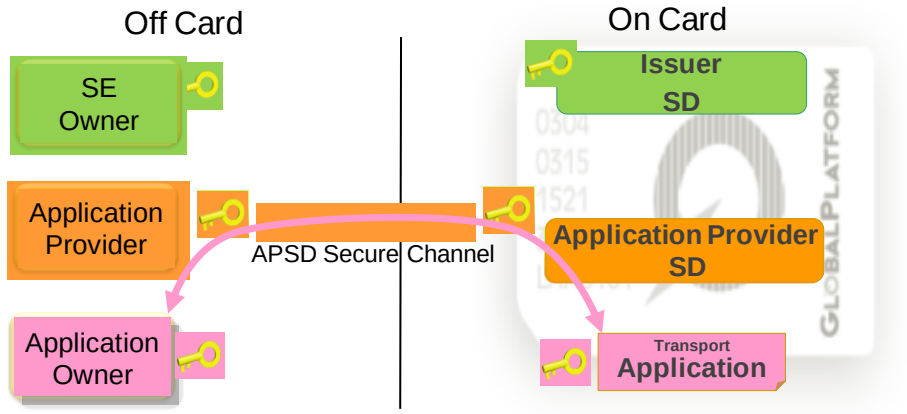


Fig. 7-9: Application Loading

7.6 Personalisation phase

Application personalisation may include application installation, personalisation and activation commands.

The application personalisation data is protected by the secure channel between the Application Provider and the APSD that can provide data confidentiality, integrity check and sender/receiver authentication.

The process of application activation can be separated from the personalization phase if necessary.

When the personalisation phase is complete, the application is ready to be used in IFM transport network.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

Later personalisation may occur to load a customer profile, contract and initialize some products.

[Req46]: Optionally, GP session can be used for further personalization of the application.

7.7 Deletion phase

It may be necessary at some time to delete a transport application hosted on the customer Media.
The deletion phase can include the deletion of the transport application, the EU status application and the GUI MIDlet (if the Customer Media is a mobile). The deletion depends on the customer acceptation of this action.

[Req47]: The transport application can be removed and this removing is possible only if it is requested by the Customer.

7.8 Application proprietary life cycle phases

The application proprietary life cycle depend of the specificity of each application provided in different transport network, the main common functions are described below:

- The function of writing and reading the profile of the customer
- The function of writing and reading the IFM products.
- The function of invalidating an IFM application.
- The function of backing up tickets. The ticket back-up function is designed to be used when transferring tickets to another platform, whether it be another phone or a contactless card

These functions must be present in the customer media (no-regression). No change is required for the application proprietary life cycle phases.

[Req48]: There is no impact on the application proprietary life cycle phase and no change is required by the integration of multi-application Customer Media.

The specificity of the transport environment with its existing interoperability, allow to the customer to load different products provided by transport operator present in a multimodal area.
This possibility involve that an application can be installed by an unique transport operator and each transport operator present in this multimodal area can download its product in the application.

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program

8 Common Requirements for EU status application

As presented in the IFM project vision described in WP3.1 deliverable ([R14]), the EU status application aims at making customers benefit from their status all over Europe. In order to respect customer privacy, such application will only be offered if customers explicitly ask for it to their home transport network as some person may not like to convey personal information in their Customer Media.

[Req49]: In order to respect customer privacy, the EU application shall only be downloaded following an explicit request from the customer.

[Req50]: Like transport application, the EU application is downloaded in the Secure Element of the Customer Media.

[Req51]: The downloading of the EU Application can only be requested to an Application Retailer who already download a transport application and for which personal information of the customer has been registered.

As proposed in the IFM project vision, the personal data contents in the EU status application should be standardized to allow reading and interpretation from any EU IFM. This standardisation work is not part of the current IFM project. Standardisation will focus both on data format and on the type of information required for the EU Status Application.

A **privacy model** is needed to allow the different stakeholders to consider themselves as privacy respectful parties. As a consequence, personal data reading shall only be possible for IFM schemes which have committed to respect those EU IFM privacy requirements as expressed in WP2.

[Req52]: All EU IFM actor able to read the data from the EU Application shall respect the corresponding privacy charter defined in the WP2 of this project.

An authentication process shall then take place prior to be able to read the EU Status data. It specification will be part of the standardisation work.

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

This report is a result from the IFM Project -
a project funded through the 7th EU Framework Program