TECHNICAL REPORT

ISO/TR 24014-3

First edition
2013-04-15

Public transport — Interoperable fare management system —

Part 3: Complementary concepts to Part 1 for multi-application media

Transport public — Système de gestion tarifaire interopérable —

Partie 3: Concepts complémentaires à la Partie 1 pour medias multiapplications

Reference number
ISO/TR 24014-3:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 24014-3 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

ISO/TR 24014-3 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems* in collaboration with Technical Committee CEN/TC 278, *Road transport and traffic telematics*.

This first edition is a partial revision of ISO 24014-1:2007.

ISO 24014 consists of the following parts, under the general title *Public transport — Interoperable fare management system*:

— Part 1: *Architecture*[1)]

— Part 2: *Business practices* [Technical Report][2)]

— Part 3: *Complementary concepts to Part 1 for multi-application media* [Technical Report]

1) International Standard under development.

2) Technical Report under development.

Introduction

This Technical Report explains the functions to be identified by Public Transport stakeholders to set up Interoperable Fare Management. From that functional view, there was no need to distinguish the implementation as a stand-alone application from the implementation in a multi-application environment.

Since the publication of ISO 24014-1, multi-application contactless devices have become available such as multi-application smart cards, USB-keys and mobile phones. They are able to host Public Transport Applications in embedded or additional Secure Elements.

This Technical Report addresses the introduction of multi-application media into the transit ecosystem from the organizational and functional perspectives with the objective to provide a basis for transit to leverage its large customer base.

Only the use of standardized processes can put Public Transport in a position to benefit from such a multi-application environment

— to diminish investment and operational costs with the use of Media issued by a third party,

— to increase the convenience and interoperability for the customer and therefore the ridership, and

— to make the same service available with multiple solution providers without developing specific middleware.

This Technical Report therefore acknowledges technical requirements that refer to existing ISO and non-ISO open standards to favour the convergence of transit Fare Management Systems.

Document outline

The technical points to be harmonized for regional implementations that need to find possibilities of commercial interoperability are described:

— Common model of the multi functional architecture of the media (Clause 6).

— Requirements for a common management process of the Application Templates in multi-application media and in the IFM Systems themselves (Clause 7).

The complements to the functional model of Part 1 and to Part 2 when independent Fare Management Systems decide together to use multi-application media to develop interoperability are described:

— Insertion of the IFM functional model in a multi-application environment, and new roles that are not included in Part 1 but are necessary for the management of the Media and of the Applications (see Clause 8).

— Use cases and processes (see Clause 9).

These conclusions may be used to make different IFM Systems interoperable

— When each of them independently issues its Application Template for use in multi-application media.

— When they use a common complementary Application Template for a progressive integration.

Public transport — Interoperable fare management system —

Part 3: Complementary concepts to Part 1 for multi-application media

1 Scope

This Technical Report describes how to implement Interoperable Fare Management (IFM) Applications in a multi-application environment, and the additional roles and use cases that appear.

Multi-application media open new possibilities for separate secure IFM Applications to be loaded and operated separately on the same Media.

This enables a customer oriented commercial interoperability with the possibility for the customer to use the same Media in different Fare Management Systems independently of the fare policies and specific local systems and without the need for any common commercial policies.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7816 (all parts), *Identification cards — Integrated circuit cards*

ISO/IEC 14443-1, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 1: Physical characteristics*

ISO/IEC 14443-2, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 2: Radio frequency power and signal interface*

ISO/IEC 14443-3, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 3: Initialization and anticollision*

ISO/IEC 14443-4, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 4: Transmission protocol*

ISO/IEC 18092, *Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)*

ISO 24014-1:2007, *Public transport — Interoperable fare management system — Part 1: Architecture*

ISO/TR 24014-2, *Public transport — Interoperable fare management system — Part 2: Business practices*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 24014-1, ISO/TR 24014-2 and the following apply.

3.1
media
device that can hold at least one Secure Element

3.2
Customer Media
device that holds a Secure Element initialised with one or more Applications

3.3
Secure Element
SE
physical component, whatever its form factor (embedded, removable or not) that can be installed in a media to host Applications in a secure environment for their execution

3.4
SE Specification
set of specifications designed to Install, select, process and delete Applications in the SE

3.5
Secure Channel
communication mechanism from any source to a Secure Element that provides the required level of assurance

3.6
Security Domain
SD
software unit providing support for the control, security, and communication requirements of a Role, e.g. the Application Retailer

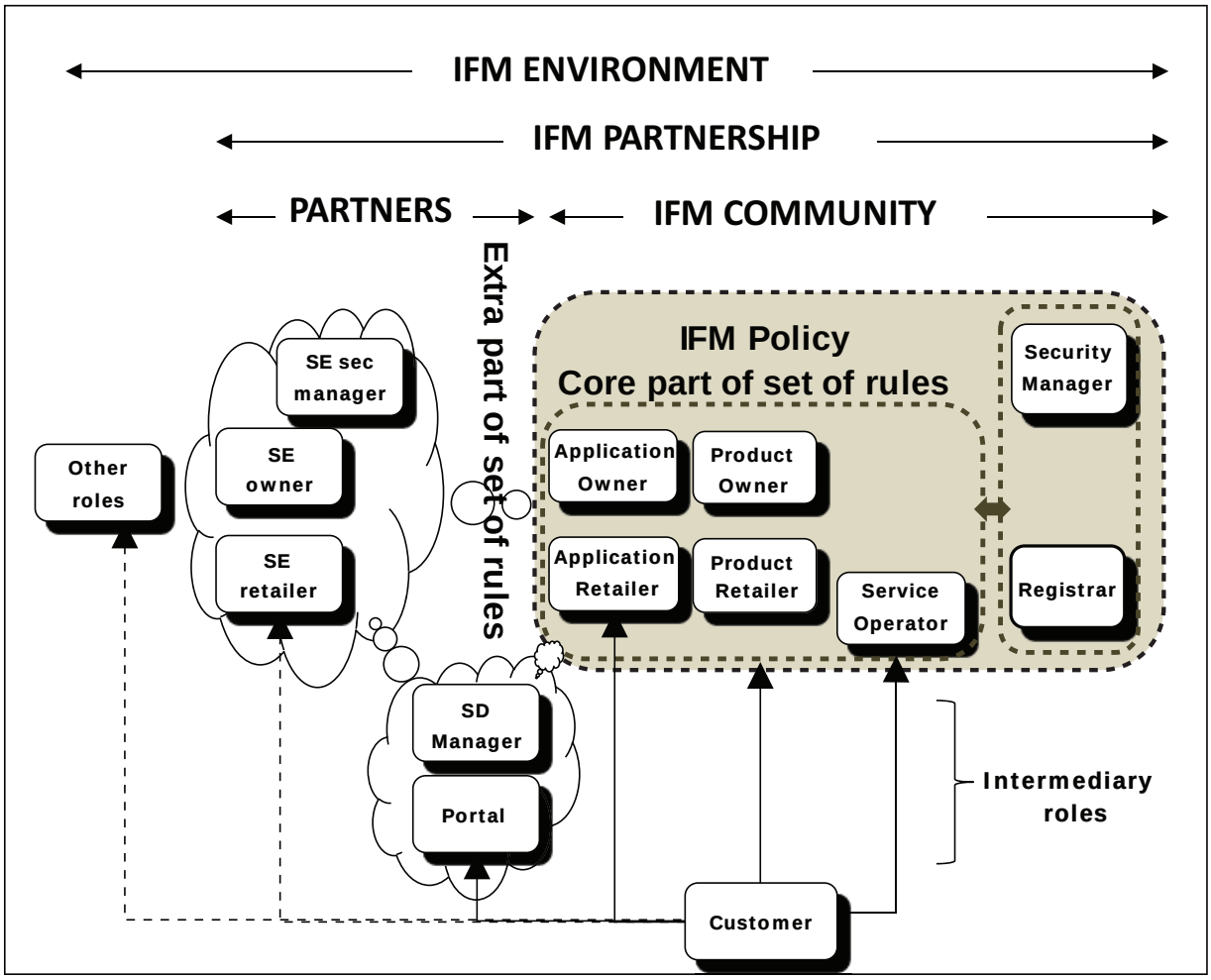

Figure 1 — Main terms and definitions illustrated in the functional model

NOTE Figure 1 illustrates the above definitions in the functional model described in this Technical Report.

4 Symbols and abbreviated terms

GP	GlobalPlatform
IFM	Interoperable Fare Management
IFMS	Interoperable Fare Management System
NFC	Near Field Communication (refer to ISO/IEC 18092)
PT	Public Transport
PTA	Public Transport Authority
PTO	Public Transport Operator
SCP	Secure Channel Protocol
SE	Secure Element
SD	Security Domain

NOTE The usual term of 'SD-Card' may also be used in this Technical Specification in which case it refers to the particular type of component.

UICC	Universal Integrated Circuit Card

5 General context and limitations

This Technical Report first describes objectives and requirements for multi-application management that are compatible with the type of Applications as described in the use cases of ISO 24014-1, which require a high security level and must, in the multi-application context, be securely protected against the other Applications (see Clauses 6 and 7).

A standardized technical architecture and standardised processes are needed to manage a multi-application environment.

GlobalPlatform is acknowledged to be the only known currently available open standard to meet the objectives and requirements defined herein. It is therefore proposed as today's solution for the standards process.

The internal security process of the Applications remains only dependant on each security policy.

Proprietary materials and methods do exist and may be chosen to address local needs for backward compatibility, as a business alternative or as an answer to specific customers' demands with limited interoperability, despite the risk of unpredictable updates.

Other types of architectures mainly based on direct payment or on back-office centric systems using the Media as an ID management have different needs and are not considered here.

The Technical Report then describes an extension of the ISO 24014-1 functional model to address additional roles necessary to operate Applications in the new context independently of the Media form factor or of its Secure Element (see Clause 8).

The details of applying multi-application to mobile ticketing form factors through the establishment of associated partnerships agreements that may be needed between mobile network operators and transit systems operators are not described herein.

The Technical Report does not address the financial processes that are attached to the Fare Management System.

The ways the Fare Management System can address the variety of payment means, e.g. credit or debit cards, debit accounts, loyalty programs, bank-to-bank transfers or any access control accounts that may provide payment, are not described.

The ways they can serve different service operators via a clearing house is also not described.

The use cases provided at the end of this Technical Report are limited to the cases when the set of Applications installed within the multi-application media accordingly to the customer's demand is installed and updated under the responsibility of an organization that is not the customer itself.

Use cases that permit self-managed media are not discussed (see Clause 9).

6 Media functional architecture

6.1 Multi-application

Multi-application in the context of this Technical Report is an environment for the Secure Element (SE) with the following characteristics as defined in ISO/IEC 7816-13 standard for cards.

(In the following list (a) to (i), the term SE replaces the terms 'card' or 'media' originally used in ISO/IEC 7816-13

a) An application is a uniquely addressable set of functionalities on a multi-application media that provides data storage and computational services.

b) An application may be added to the SE before or after the SE is issued.

c) This Technical Report focuses on Applications that can be added or deleted after the issuance, independently from the fact that some of them can be installed during the issuance of the SE.

d) More than one application may be added to the SE.

e) The SE platform provides mechanisms for managing SE resources, e.g. memory.

f) The SE platform provides a security boundary mechanism for each application to prevent unauthorized interaction and security violation from any other application on the SE.

g) The life cycle of an application is independent from the life cycle of any other application in the same SE.

h) The life cycle of an application is independent from the life cycle of the SE except when the SE is in the termination state, as defined in ISO/IEC 7816-9.

This rule (i) is to be understood technically, independently from any business rules and responsibilities that can be agreed between the Application Owners and Media Owner.

6.2 Functional model of the Media

The functional architecture of the Media considered in this Technical Report is described by Figure 2.

NOTE Functional blocks drawn with dotted lines are optional.

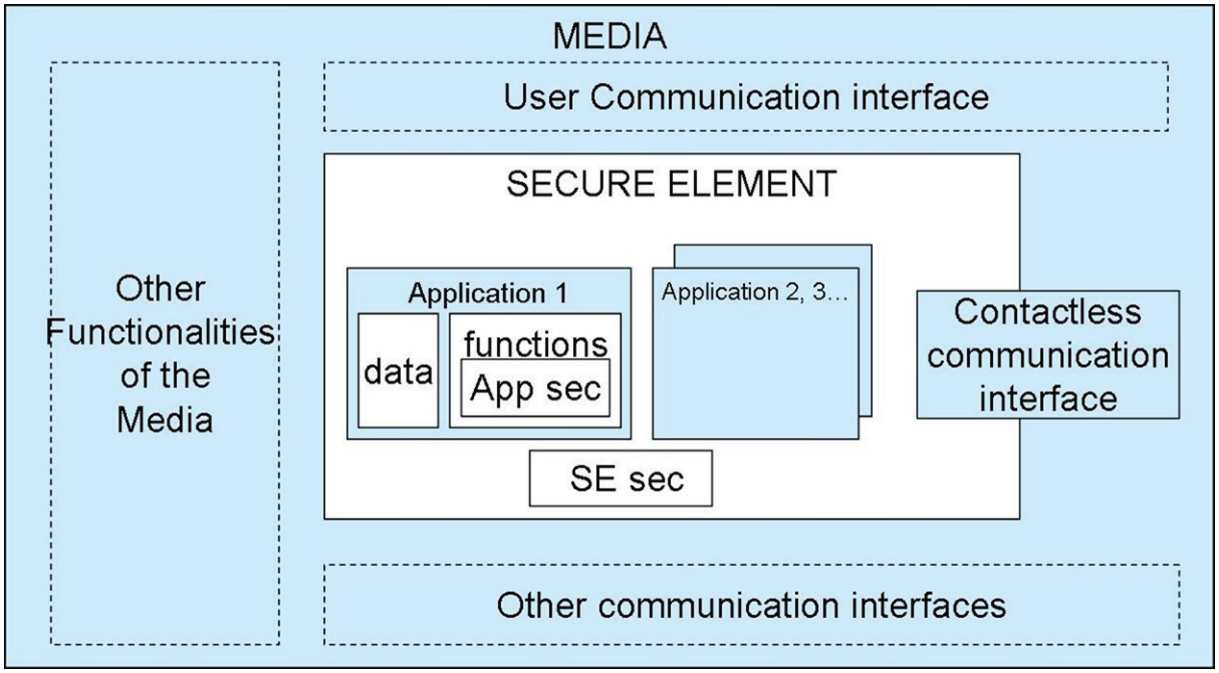

Figure 2 — Media functional model

The Media is equipped with communication interfaces which may vary and use different protocols and communication networks or links: USB, 3G/GSM mobile networks, Bluetooth, eSata, Firewire, etc and may work over the air (OTA)or over the Internet (OTI).

It may also include a direct user interface (display outputs and/or command inputs) and be equipped for other functionalities.

The Media contains a Secure Element that can host and execute the Applications.

Its operating system includes a security function (drawn as SE sec on Figure 2) that manages multi-application environment and thus controls the downloading/upgrading/deletion operation of the Applications.

This SE security function ensures application insulation with firewall and secures that the messages coming from any communication interface are routed to the appropriate Application.

The routing process is performed without changing the content of the message itself.

A contactless proximity communication compliant with ISO/IEC 14443 or ISO/IEC 18092 standards is compulsorily implemented.

It can be implemented in the Media itself or in the 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).

Each Application contains a set of data and functions.

Among these functions that are internal to the Application is the internal security management of the Application (shown as App Sec on Figure 2) that remains fully independent from the SE itself.

The credentials required by the applicative security function may depend upon the communication interface that is used.

As described, this functional architecture is

— Independent from the form factor of the Media itself that may be a contactless or dual (contact and contactless) interface card, an NFC mobile phone with SE stored in the UICC, a contactless USB key or take any other form.

  It can be used to describe conventional contactless cards as they were considered when ISO 24014-1 was approved:

  — The concepts of SE and of Media are merged.

  — A contact interface could exist besides the contactless one in dual interface cards.

  — Other functions also could exist in dual chip cards.

  — No interface to the user existed.

— Independent from the type of implementation of the Secure Element itself inside the Media.

  — The SE can be embedded in the Media. In that case, the technical implementation of the security functions can be shared between the Media and the SE.

    It is the case with Java Cards, USB contactless devices, Suica Mobile Handsets:

  — The SE can be inserted in the Media.

    — In the case of SIM cards, the Media security functions are also used to monitor the GSM link as well as other functions inside the Media itself.

    — In the case of mobiles or other devices equipped with slots for SDcards, the SE is completely independent from the Media.

— Independent from the location of the necessary facilities (hardware and software) with which the Application will communicate via the interface. These facilities can be local and accessed via a local communication interface, e.g. in the contactless reader, or distant and implemented in remote servers.

In relation with this model, the functions of the Medium Access Device [MAD] are split into parts.

— Some communications will address the Media, some will address the Secure Element and some will address the Application.

— Some communications will be established with local hardware or software facilities, some will address distant servers.

— Furthermore, each local communication interface may link to a different device.

Similarly, the management and the life cycle of these three elements (Media, SE, Application) can be different.

Hence, new functions are necessary. They are described in Clause 8.

6.3 Security Domain management

Security domains are created in the Secure Element to achieve application insulation and provide the security context of a specific Application Owner. An Application Template can only be installed in the SE after a Security Domain has been assigned in the Secure Element to the Application Owner.

The creation of Security Domains and the loading/deletion of the Application templates in the SE have to be secured and will only be possible using a Secure Channel Protocol (SCP) connection to the SE.

A SCP ensures the confidentiality and the integrity of the application code and of the application data during application loading and personalisation.

It ensures the mutual authentication between the Secure Element and the system serving a role (Application Owner, SE Owner, ...) and protects the APDUs exchanged between them (over a logical channel) by encrypting and/or signing each APDU.

In this Technical Report it is considered that this Secure Channel is under control of a role, called SD Manager which is in charge of handling the commands to create the Security Domains and to let the Application Retailer move the Application Templates inside them: loading, installation and deletion.

Figures 3, 4 and 5 describe the management process.

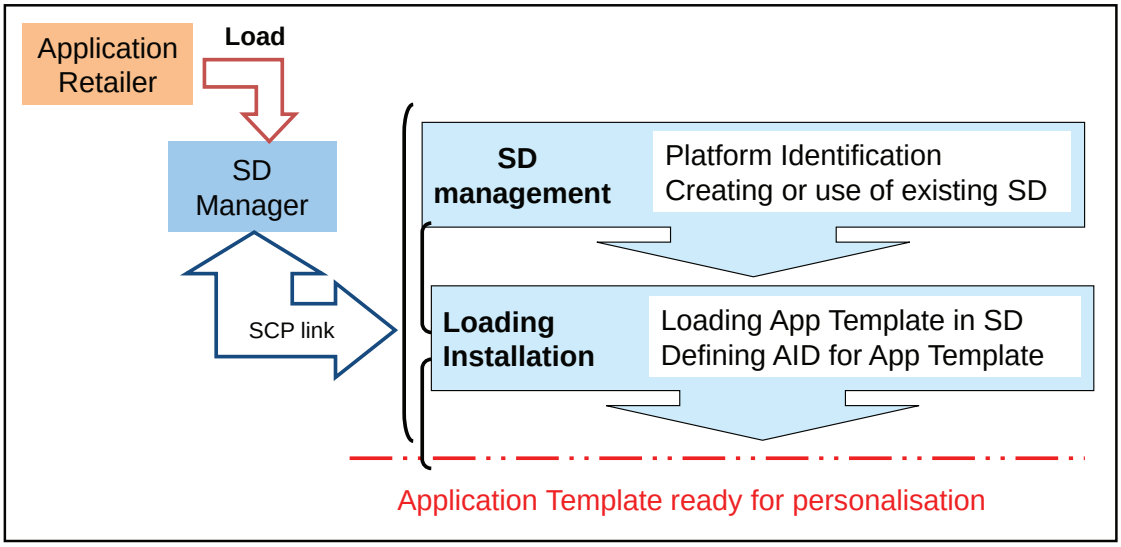

Figure 3 — Loading and installation of an Application Template

The personalisation phase of the application can then be performed by the Application Retailer either using the application specific commands or requiring the SD Manager to use the SCP link to do it

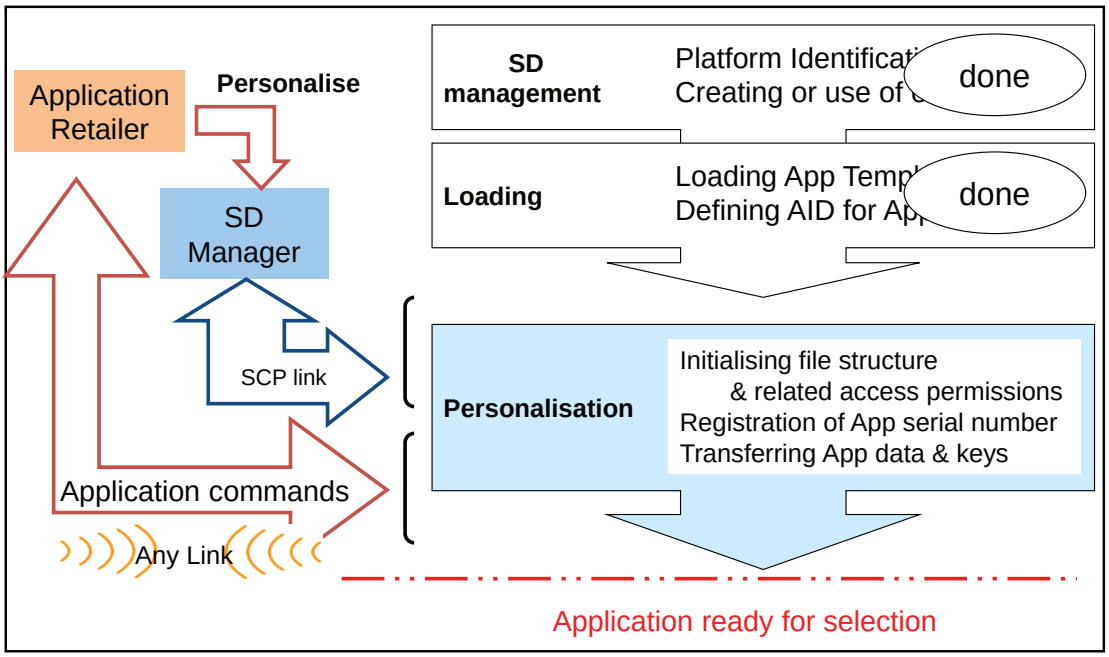

Figure 4 — Personalising an Application

Once the Application Template has been personalised, the Application can be selected and then can be run with any application specific commands without any need to involve the SD Manager

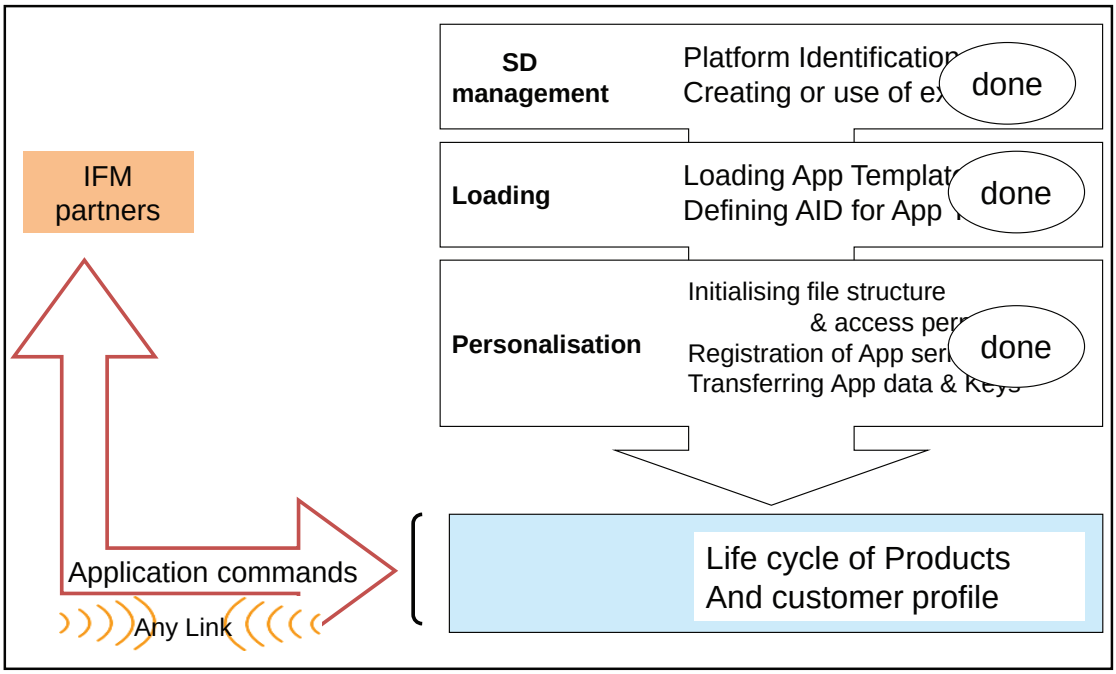

Figure 5 — Running an Application

6.4 Composite Customer Media certification and validation

In the current clause, the term 'Application' is used for 'Application Template'.

For mono application Media, the certification process is generally used to be a monolithic process including the test of the chip, of the operating system and of the Application Template.

In a dynamic multi-application environment where Applications can be pre loaded at the issuance of the Media or loaded after it, such a certification is not adapted anymore as each introduction of a new Application cannot imply the full retesting of the complete Media.

The approach named "Composite evaluation" aims at targeting UICC certification in the NFC ecosystem.

This evolutionary certification process aims to be more cost and time effective in Application certification.

It allows the coexistence of standard and secure Applications.

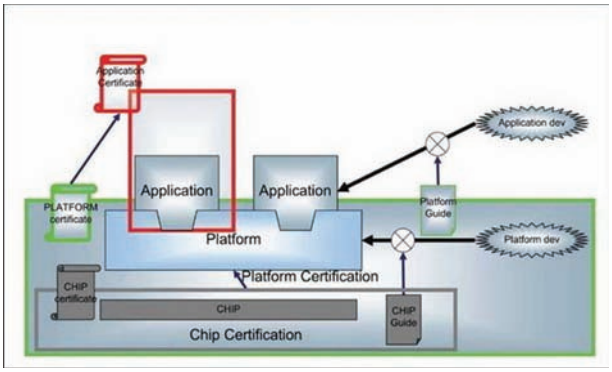

Figure 6 — Composite Certification of a Media (source GlobalPlatfom)

— Chip certification:

Chip certification is achieved nearly as usual via standard Common Criteria certification.

It is managed by chip manufacturers.

— OS certification:

  OS certification is specified for a defined perimeter excluding Applications.

  It is managed with the Media manufacturer and requires cross industry players to agree on a Protection Profile per type of Media.

  — Initiatives are on going in the 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.

  Some Protection Profiles have already been published [R20].

— Application certification:

  Each certification is managed independently from the certification of other Applications.

  It is managed by the Application Owner and certification tests are application dependent.

  The respect by all the Applications of the OS security guidelines and the certification of the underlying OS warranty to each Application Owner that its Application is executed in a trusted environment.

Basic Applications 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 Applications go through the same validation test as standard Applications and in addition need to go through a certification process to ensure that the Application is appropriately protecting its own assets (keys, sensitive application data, …) according to the security policy defined by the Application Owner.

7 Public Transport requirements for multi-application Customer Media

7.1 Business requirements

7.1.1 Emulation of existing Applications

This Technical Report aims to propose solutions that do not require major changes in the existing IFM Systems.

It considers the type of Applications as described in ISO 24014-1.

The multi-application media must therefore, whatever its form factor, allow the Application to communicate as a regular smartcard

— at least when presented to a transport contactless reader such as a validation gate,

— optionally when using other communication channels.

The Media must support proximity exchanges in contactless mode regardless of the other interfaces that depend on its form factor.

7.1.2 Security

The considered IFM Applications require a high security level and must, in a Multi-Application context, be securely managed.

Other types of architectures, e.g. using vouchers, coupons or limited to an ID management, are out of the scope of this Technical Report.

The multi-application media and the associated management processes must ensure that the Applications and Products inside the Applications are secured both by themselves and against each other.

No level of certification of the chip or OS is specified as a minimum requirement. Each Application Owner will specify it according to its security policy.

The transit industry requirement (January 2012) currently varies from EAL1+ to EAL 5+ for the chip certification.

Cross industry Media will need to match the payment industry requirements for IC Chips.

7.1.3 Uniqueness

7.1.3.1 Universality of the communication layers

As a guarantee for universality, all types of Media able to host contactless IFM Applications, including mobile phones, should be able to host any contactless application that could be used to pay fare products, such as credit or debit or other payment Applications, loyalty programs, access controls.

7.1.3.2 Management of Applications

The proposed multi-application model must also be open to any type of Media and any communication link to download/upgrade/delete the Applications.

The objective is therefore to provide a unique and universal management process of the Applications as illustrated in Figure 7.

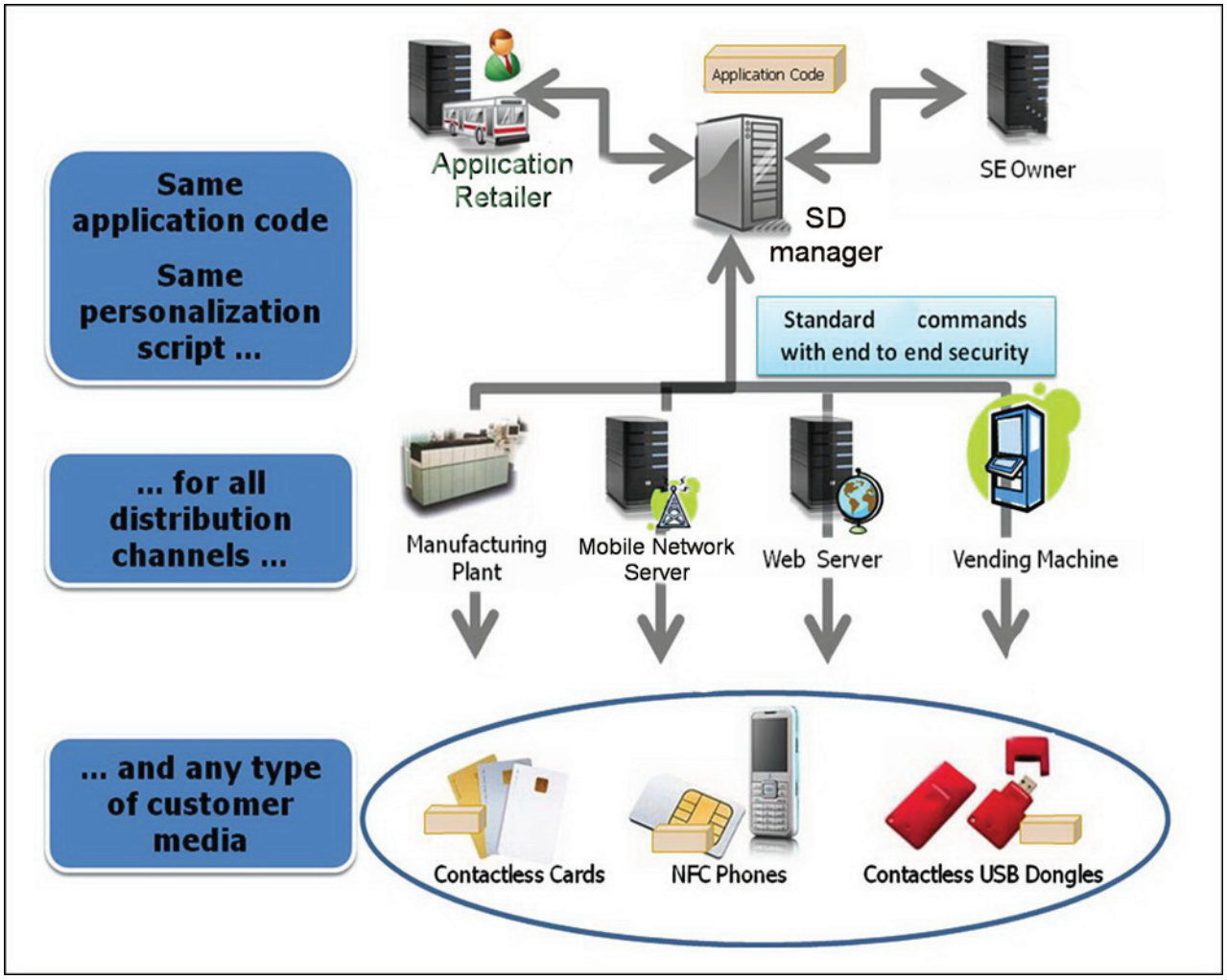

Figure 7 — Universality and uniqueness for application management

Figure 7 illustrates the fact that the same process is used to handle the Applications whatever the communication channel:

— Industrial channel represented as the manufacturing plant for installing Applications in the Secure Element when it is issued,

— Telephone link for use of NFC phones,

— Internet for accessing the Media via a personal computer,

— Local communication channels for vending machines.

7.1.3.3 Selection of Applications

PT terminals will be in a situation to meet not only PT Applications but also Applications from other businesses.

The standard activation and anti-collision process is already defined by ISO/IEC 14443.

Application selection according to ISO/IEC 7816-4 has to be mandatorily supported.

For ISO/IEC 7816-4 selectable Applications, standardized AIDs shall be used.

Implicit or default selection processes may be used in dedicated terminals for local Applications.

Depending on the Media capabilities, implicit selection by a recognition algorithm on a first command shall be possible.

7.2 General functional requirements

In this subclause, the term Media is used for requirements that apply to the Media and the Secure Element considered together as a whole device, regardless of the implementation of the required features inside the Secure Element or not.

[Req 1]. The customer can load and manage several (transport) Applications in the same device.

[Req 2]. The Media enables customers to select, buy and load a fare Product through the existing product retailing channels.

[Req 3]. The Media enables customers to select, buy and load a fare Product remotely, at the user's chosen place and time (notably using a mobile phone or a Media connected to the Internet)

[Req 4]. The customer can access the transport network and benefit from the service directly with the Media.

[Req 5]. When the Media provides a user interface, the customer can use that interface to select the fare Product or the transport Application he wants to use.

7.3 Secure Element's profile

[Req 6]. Each Secure Element is assigned an "SE profile" by the SE Owner.

The characteristics of the Secure Element in terms of supported features, available memory size and execution performance are known by the SE Owner and are important for the Application Owner to determine if a third party Secure Element can be eligible for hosting its Application.

There is a need for exchanging such information in a standardized way.

[Req 7]. The SE profile includes a set of information including:

— List of supported RF protocols;

— List of supported algorithms;

— Available memory size;

— Performance class.

[Req 8]. The way a performance class is assigned to an SE is 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.

[Req 9]. The SE profile is held on the Media. The SE profile shall be freely accessible in read mode through all interfaces of the SE.

7.4 Security

The following requirements meet the security objectives previously listed.

[Req 10]. The Media holds a Secure Element which is a microprocessor based Component.

[Req 11]. The Application (and the Products inside the Application) is stored and executed in the Secure Element.

[Req 12]. The Secure Element ensures an absolute separation between Applications to ensure integrity and confidentiality of the Application code and data.

[Req 13]. If a common security policy defines a certification process for PT Application, each Application Template is certified according to this process.

[Req 14]. The Secure Element supports a set of standard algorithms to offer the cryptographic capabilities required by the security policies of the current existing transport Application Templates: DES, 3DES, RSA, AES.

This list may evolve in the future. The ISO TC 204 group should agree collectively those protocols suitable for Public Transport among the ones enabled by the approved version of GP to remain compliant with [Req 25]

[Req 15]. Disposable Secure Elements that can be moved from one Media to another one support the security algorithms independently from the OS of the Media.

[Req 16]. The management of transport Application Templates on the Secure Element is secured by SCPs.

7.5 Uniqueness

7.5.1 General

Uniqueness requires standard processes and protocols for:

— Contact and contactless interfaces;

— Application management;

— Application selection;

— Application operation.

PT organisations that use proprietary technologies must be aware that it may be a barrier to interoperability with other IFMs or with other businesses.

7.5.2 Contact and contactless interfaces

[Req 17]. The Media relies on the open industry standards widely used for contactless devices.

Table 1 summarizes the available standardized interfaces per type of Customer Media.

Table 1 — Types of Media and their interfaces

Type of Media	SE	SE contact interface	SE contactless interface
Contactless smart card	IC Chip	None	ISO/IEC 14443
Dual (contact & contactless) smart card	IC chip	ISO/IEC 7816	ISO/IEC 14443
NFC mobile phone with application stored in the UICC	UICC	ISO/IEC 7816	None[a]
NFC mobile phone with application stored in an embedded SE	Emb. SE	ISO/IEC 7816	None[a]
NFC mobile phone with application stored in a removable SE	SD card/ micro SD	ISO/IEC 7816	ISO/IEC 14443 or None[a]
Contactless USB key	IC chip	ISO/IEC 7816 over USB protocol	ISO/IEC 14443

[a] For SE into mobile phone, contactless capabilities can be provided by the NFC chip + antenna inside the mobile phone. The connection between SE and the NFC chip can be either ETSI HCI data protocol or SWP protocol for the UICC or dependent on mobile phone implementations in other cases.

[Req 18]. The Media supports an ISO/IEC 14443 RF communication protocol.

To improve interoperability between contactless cards and readers, EMVCo has defined additional requirements for implementing ISO/IEC 14443 communication protocol.

It is premature to evaluate if such recommendations are applicable to IFMSs, 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.

[Req 19]. Other interfaces to access to the SE may be optional.

[Req 20]. The Media behaves like a regular contactless card from a transport network contactless reader point of view for transactions (validation, ticket top up, inspection …).

[Req 21]. The remote communication channels only support standard protocols:

— For Internet communications (OTI): HTTP and SSL to communicate with the user's browser or a proxy application in a PC,

— For mobile networks communications (OTA): wireless data connection to communicate with a proxy application in the mobile or directly with the UICC.

7.5.3 Application management

7.5.3.1 GP acceptance

GlobalPlatform has been a field proven application management standard in the banking industry since the end of the 1990s, and provides specifications for Secure Elements and system to support application issuance and management into a multi-application environment.

GP Secure Communication Protocols ensure the confidentiality and the integrity of the application code and of the application data during application loading and personalisation as required.

GlobalPlatform SCPs can also provide authentication and/or mutual authentication between the Secure Element and the component serving a Role (Application Owner, SE Owner, …).

GP security scheme does not overlap with the possibility for each Application Owner to apply its own security scheme (Ap sec on Figure 2) when exchanging commands directly with its Application.

Some security schemes have already endorsed the GP composition model.

GP technologies at this date therefore appear to be the most appropriate available open solution for universal interoperability as required, to manage SDs, load and personalise Applications.

Different application selection processes are proposed using the SELECT standard command or implicit selection algorithms [R12]

[Req 22]. The Secure Element complies with GlobalPlatform Card Specification for content management

[Req 23]. The management of Applications in the Secure Element is secured by a GlobalPlatform SCP, independently of the transport layer.

[Req 24]. The information exchanged between any component serving a Role and the corresponding Security Domain in the Secure Element is secured by a GlobalPlatform SCP, independently of the transport layer.

[Req 25]. The OS certification checks compliance in particular with Java Card and GlobalPlatform mechanisms.

7.5.3.2 GP versions

GlobalPlatform 2.2 specifications support the following list of cryptographic standards: DES, 3DES, RSA, AES, HMAC-SHA1, ISO 9797, MAC. All the standards used by PT Application Templates are in that list.

Different SCPs have been specified by GlobalPlatform 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.

All SCP can be used independently of the transport layer and the communication technologies.

SCP02 provides integrity, origin authentication and confidentiality of the data, independently of each other.

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

— Integrity and data origin authentication, confidentiality;

— Its asynchronous mode allows a script of commands to be sent that can cope with low bandwidth and high latency of wireless networks.

SCP02 is currently supported by a large range of Secure Elements that connect to the Internet via a proxy application in a PC as illustrated in Figure 8 as well as by non SIM centric mobiles.

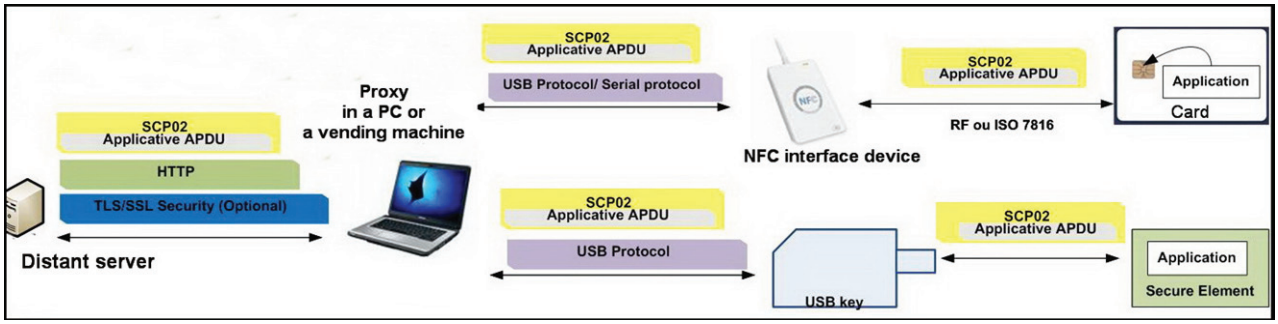

Figure 8 — SCP02 connecting a USB key plugged to a PC or a smart card connected to a PC or vending machine via contact or contactless reader

SIM based mobiles combine both SCP02 and SCP80 as illustrated in Figure 9:

— SCP02 is used to encrypt the message destined to the APSD.

— SCP80 is used to protect the OTA communication as shown in Figure 9.

It provides end to end secure communication between a server and the UICC and can be used over SMS or BIP transport protocols.

It allows managing transparently SE contents without the need for the end user to interact. No proxy application is required in the phone.

GP commands can be sent directly to a UICC as defined in ETSI TS102.225. The lists of available commands are defined by GP and ETSI TS 102.226.

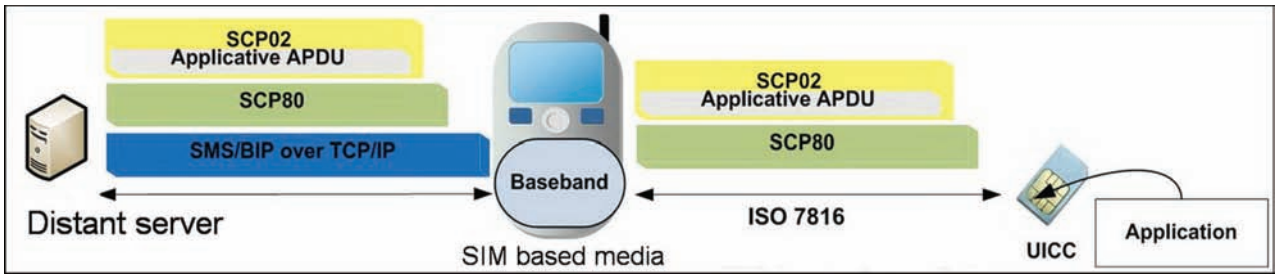

Figure 9 — SCP80 and SCP02 connecting the Secure Element in a SIM based architecture

[Req 26]. The Secure Element is compliant with GP specification 2.2 (and amendments A, B, C, D) or higher.

Should extensions or a new version of GP standards be referenced as the market develops, ISO/TC 204 may complement the present requirements.

[Req 26]. The Secure Element at least supports GlobalPlatform SCP02.

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

[Req 28]. It is recommended from a universality perspective that the two protocol options of SCP02 are available for use at the convenience of each Application Owner for its application download.

[Req 29]. SIM cards used as Secure Elements for PT support GlobalPlatform SCP80.

[Req 30]. Other GP SCPs may be optional.

7.5.4 Application selection

[Req 31]. Application selection according to ISO/IEC 7816-4 is mandatorily supported.

[Req 32]. APDU communication according to ISO/IEC 7816-4 possible over the contact and contactless interfaces of the Secure Element.

7.5.5 Application operation

In addition to the security mechanism provided by GP for the application loading and personalisation, Java Card environment also provides a security framework that offers application firewalling. It is used extensively in the smart card industry and provides an easy extension to USB Keys and mobile phone form factors that will be beneficial for future multi-application environments. These benefits make JAVA technologies a convenient choice that provides an available open architecture environment from which to execute and operate Applications defined herein.

JAVA technologies at this date therefore appear to be the most appropriate available open solution for universal interoperability as required, to execute and operate the Applications.

However, should further extensions or a new version of JAVA standards be referenced as the market develops, or should standards meeting the same criteria be available in the future and widely accepted by the transport and related industry, ISO/TC 204 may revise and complement the present requirements.

[Req 33]. The Secure Element OS is compliant to Java Card 2.1 or higher;

[Req 34]. Each Application Owner certifies that its Application Template can be executed by the Java Card OS.

8 Insertion of the IFM functional model in the multi-application context

8.1 General

The basic Functional model inside an IFM Community described in the ISO 24014-1 can be presented as in Figure 10.

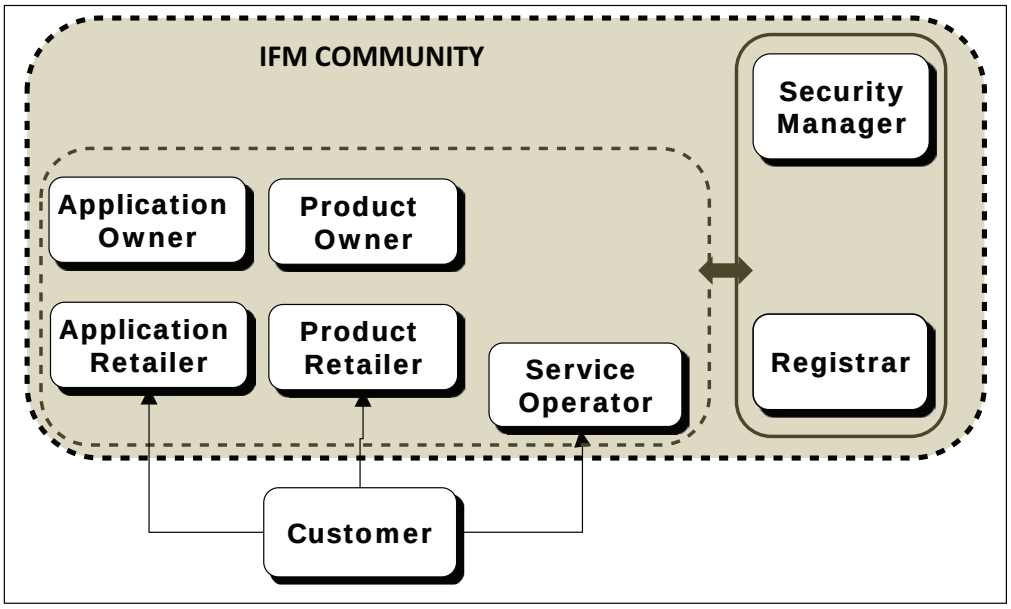

Figure 10 — Basic functional model in an IFM Community

Considering how the functional model can be implemented, ISO/TR 24014-2 introduces the concepts of IFM Partners as Roles that are not subject to the IFM Policy but are however directly related to the IFM Community and therefore share with the IFM Community an extra set of rules.

The operation of multi-application devices as described in the previous clauses leads to the functional model described in this Clause.

Figure 11 illustrates that environment.

The Roles to manage the life cycle of the Media have no direct interaction with the IFM Community, they are not IFM partners. They are described in 8.2.

The Roles to manage the life cycle of the SE have direct interaction, they are IFM Partners. They are described in 8.3.

The roles to handle the Applications inside the SE are 'Intermediary Roles', between the IFM Community and the SE Community. They are described in 8.4.

— Different IFM Communities are shown. They illustrate the multi-applicative context for PT itself. Other businesses than Transport can have similar links to the IFM partners and are not represented.

— Similarly, several dotted lines around the SE Community [SE Security Manager, SE-Owner, SE-Retailer] illustrate the fact that not only one SE but many of them can be used.

— Transversal Roles may be separate for each couple of [IFM and SE].

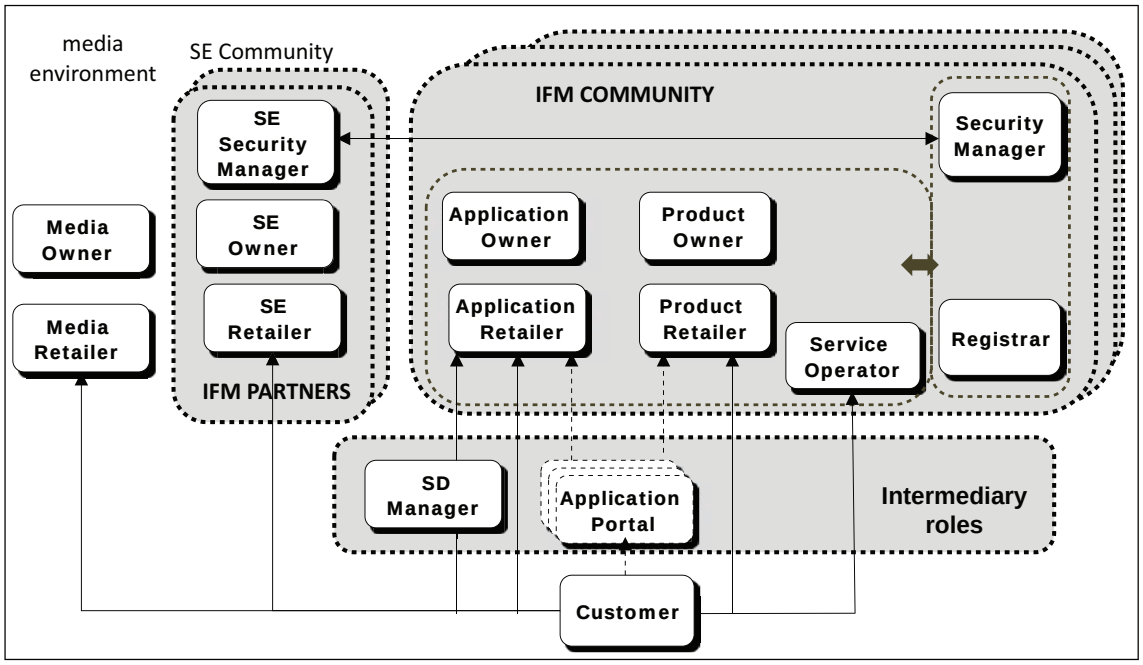

Figure 11 — Insertion of the IFM - Functional model in a multi-application context

8.2 Media environment

The Media Owner and Media Retailer, as Roles, are not IFM Partners as they have no direct interaction with the IFM Community but only indirect via the SE Community.

They are represented in Figure 11 and defined in the next paragraph to explicitly differentiate them from the SE Owner and SE Retailer although some of the use cases may not clearly distinguish the Media Owner from SE Owner or the Media Retailer from SE Retailer when the SE is embedded in the Media or is paired with it to operate functions inside it, for example when the SE is the SIM card of a mobile telephone handset.

The Role of Media Owner is to:

— release the Media for the use with different Applications;

— release the Media for the use of one or more Secure Elements by Secure Element Owners.

The Role of Media Retailer is to:

— provide the multi-application media to a customer;

— hold the customer contract and related customer service in relation to the.

8.3 SE Community

Roles in the SE Community are IFM Partners.

The Role of Secure Element (SE) Owner is to:

— define the SE Specifications;

— define the business rules for the use of the SE;

— authorize SE Retailers to distribute SE to customers;

— authorize the Application Retailer to have the Application loaded/updated/deleted on the SE;

— authorize the SD Manager to manage the loading/updating/deletion of Applications inside the SE;

— be responsible for the SE to comply with the requirements of the SE Security Manager.

The Role of the Secure Element (SE) Retailer is to:

— provide the SE to customers and the related Customer Service;

— guarantee to customer the compliance of the SE to the requirements set by the SE Security Manager.

All interfaces with the customer relative to the SE are part of that role.

The Role of Secure Element (SE) Security Manager is to:

— specify security requirements that apply to the Secure Element and to its operation process;

— determine the corresponding validation process of the Secure Element.

8.4 Intermediary Roles

8.4.1 General

Intermediary Roles comply to the Core part of Set of Rules and to the set of rules of the SE Community.

The SD Manager securely operates the download operation. It has two entry points, as it must comply with both security policies from the IFM Community and from the SE Community.

The Application Portal helps the customer find the appropriate application that can fit into a given SE.

8.4.2 Security Domain (SD) Manager

The Role of Security Domain Manager is to:

— handle the commands of the Secure Protocol Channel as described in 6.3;

— operate loading/updating/personalisation/deletion of Application Templates or Applications, Product Templates or Products in the SE;

— create Security Domains and securely load/update/delete Application Templates or Applications in the SE on request from the Application Retailer as authorized by the SE Owner;

— manage customer's directives as authorized by SE Owner and Application Owner if conflicts appear when loading/updating an Application (e.g. overflow of SE's capacity, conflicting Applications, …).

The role of the SD manager may also be to use the Secure Protocol Channel for loading/deletion/updating of Products in the Application if required by the Product Retailer, (e.g. when the SIM card of a mobile phone is used as SE and the OTA communication link is used for remote management of Products such as sales, renewal, profile update…).

The internal security of the Application (see App sec in Figure 2) remains a role of the Product Retailer.

The role of SD manager is under control of both the SE Security Manager and the IFM Security Manager.

8.4.3 Application Portal

The Application Portal [Portal] is an optional Role addressing the issue to help customers find the appropriate Applications when they move or prepare their journey and check whether these Application(s) can or can't be downloaded on his own Secure Element.

— The Application Portal is an entry point indicating to the customer which Applications he can download to his Media and the appropriate Application Retailers.

— Once the Application is loaded, the Application Portal may also help the customer by routing his demand for Products to the appropriate Product Retailer.

— When the Application Portal and the Application Retailer functions are merged, the term "Application Store" [Store] is used.

The Application Portal function is separate from the Application Retailer function.

The Application and Product Retailers remain responsible for providing the download in a secure manner.

The customer's download request will be routed from the Application Portal to one of the Application Retailer's website for the requested Application, or to one of the Product Retailers for the Product he needs once the Application has been loaded.

An extra set of rules is needed between the Application Portal and the IFM Community and with the SE Community

8.5 Impact on the roles in the IFM Community

8.5.1 General

The multi-application environment creates new concrete functions to be performed by some of the Roles of the IFM Community as they are defined in ISO 24014-1.

8.5.2 IFM Security manager

The role of IFM Security manager includes the following new functions:

— to specify the security policy for SEs that is compatible with the IFM security requirements;

— to specify the security policy for SD Managers;

— to contract with SE Security manager to validate compliance of each SE device to that security policy.

8.5.3 Registrar

The role of Registrar includes the following new functions:

— to register and authorize Secure Elements;

— to register SD Managers to allow Application Owners to contract with them;

— to register the SE Owners, the authorized Secure Elements and the participating Application Owners with their Application Templates as well as the participating Application Retailers.

8.5.4 Application owner

The role of Application owner includes the following new functions:

— to contract with SE Owner to use registered SE for his Application;

— to authorize Application Retailers to contract with registered SD Manager.

8.5.5 Application retailer

The role of Application retailer includes the following new function:

— to contract with registered SD Manager as authorized by Application Owner.

Multi-application media can also host non-transport Applications with their own non-PT application community. Their existence may lead to new business rules:

— between the IFM Community [or some of its members] with these other communities;

— between the IFM Community and the SE Owner to limit their field.

These business aspects are not considered in this Technical Report.

8.5.6 Customer

The customer still:

— subscribes Applications from Application Retailers appointed by Application Owners;

— buys Products from Product Retailers [that may propose remote distribution channels] appointed by Product Owners;

— consumes Products for services by Service Operators.

The relations between the customer and his Internet service provider or mobile phone network operator are not in the scope of the Technical Report.

Each Role in relation to the customer shall organize the corresponding customer service. A set of rules is necessary to organize the cross-cutting of these services.

Each Role in direct relation with the customer provides the Customer service that relates to his role.

8.6 Certification of SE and Application Templates

Table 2 summarizes the certification modules and the responsibility of SE and Applications owners in the certification process.

Table 2 — Responsibilities for certification

Certification module		Responsible	Objectives
Platform Certification		SE Owner	Ensure that the platform environment can provide 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.

A cross recognition of application validation between SE Owners may avoid an Application Owner to have to re-validate its Application Template for every SE Owner proposing the same type of SE.

9 Use cases

9.1 General

This section only describes the new use cases that result from the downloading processes of the Applications and from the new possibilities given to access the Application via other communication channels than the contactless proximity channel.

The conditions of use of the Application Portals or Application Stores or the possibilities for the customer to force the selection of a particular Application are not depicted, as they depend on each implementation or device.

9.2 Main sequence diagram

All use cases could not be represented in a single diagram. Details are given in the description of the different use cases in the next subclauses.

The sequence diagram in Figure 12 shows the main principles that drive the description of the use case.

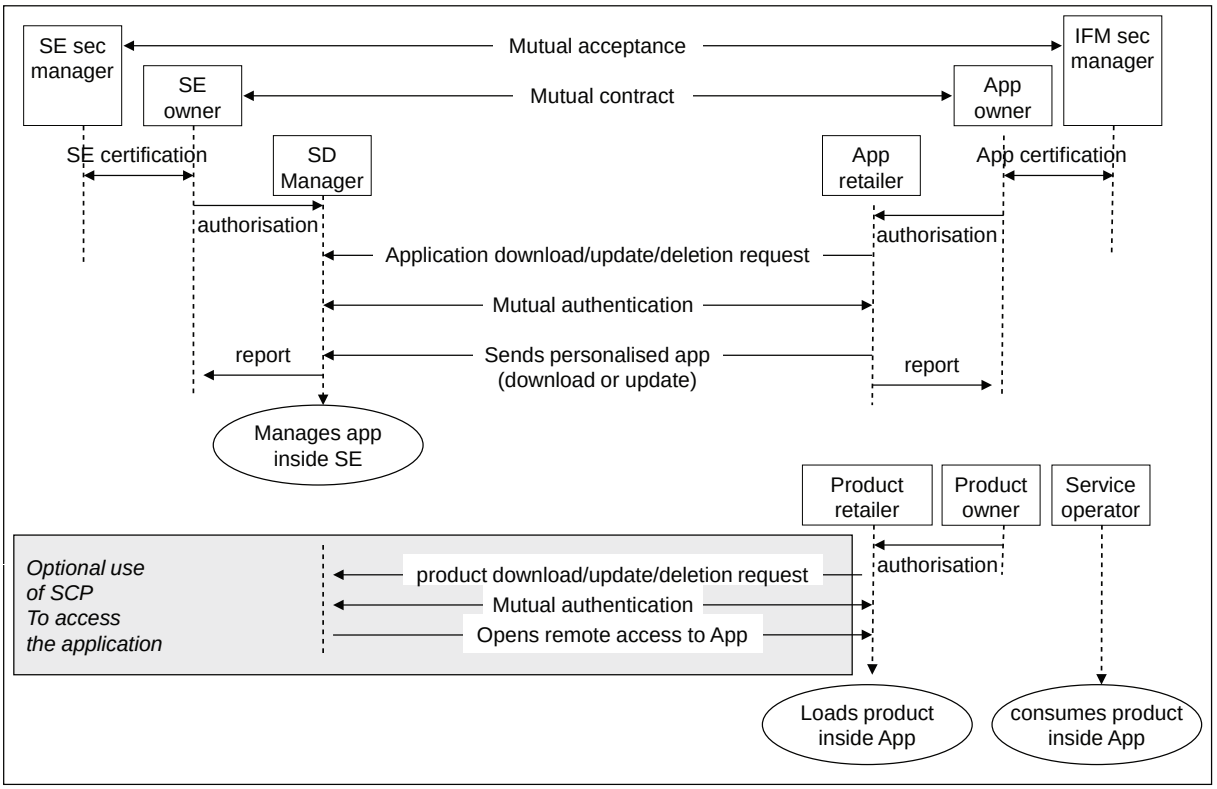

Figure 12 — Main sequence diagram

— The security management is based upon a mutual acceptance of the security policies between the SE- and IFM-security managers. Each of them then is responsible to certify the Components and processes of his side.

  This mutual acceptance guarantees that the Media fulfills the extra set of rules (e.g. security and technical requirements) from the IFMS and that the IFM Application Templates fulfil the specific set of rules of the Media Owner.

— The management of the Applications inside the SE is made by the SD Manager on request from the Application Retailer.

— The management of the Products inside the Application remains under the responsibility of the Product Retailer.

  In some implementations and for some communication channels the Product Retailer may require the SD Manager to use the Secure Communication Protocol to access the Application.

  This condition applies when the SIM card is used as SE in mobile phones.

— The SE Owner is kept informed about the Application Templates downloaded into his SE, and the Application Owner is kept informed about the SEs into which his Application has been downloaded.

9.3 Table of the use cases

Table 3 indicates how the use cases described in ISO 24014-1:2007 are modified by the multi-application context.

Table 3 — Table of use cases

Use case name	Ref ISO 24014-1	Status of use case in a multi-application context
Certification		
Certification	6.1	SE must be added to the list of components
Certification of Organization	6.1.1	Unchanged
Certification of Components	6.1.2	Unchanged for components other than SE
Certification of SE	NEW	See 9.4
Certification of Application Specification and Template	6.1.3	Unchanged
Certification of Product Specification and Template	6.1.4	Unchanged
Registration		
Registration of Organization	6.2.1	SE owners to be added to the list of organisations
Registration of Component	6.2.2	SEs are not registered
Registration of Application Template	6.2.3	Unchanged. Applets are just new templates.
Registration of Application	6.2.4	Unchanged
Registration of Product Template	6.2.5	Unchanged
Registration of Product	6.2.6	Unchanged
Management of Application	6.3	New context
Dissemination of Application Template	6.3.1	Unchanged
Installation of Application Template	NEW	See 9.5
Acquisition of Application	6.3.2	See 9.6
Termination of Application Template Regular termination Forced termination	6.3.3	Unchanged
Update of application	NEW	See 9.7
Termination of Application Regular termination Forced termination	6.3.4	See 9.8
Management of Product		

Table 3 *(continued)*

Use case name	Ref ISO 24014-1	Status of use case in a multi-application context
Dissemination of a Product Template	6.4.1	Unchanged. SE owner and SD Manager do not have to be informed about internal operations of the Applications (e.g.. Personalisation or product data) In SIM centric organizations, the SD Manager is in control of the OTA channel.
Termination of Product Template	6.4.2	
Management of Action List	6.4.3	
Acquisition of Product	6.4.4	
Modification of Product parameter	6.4.5	
Termination of Product	6.4.6	
Use and Inspection of Product	6.4.7	
Collection of data	6.4.8	
Forwarding data	6.4.9	
Generation and distribution of clearing reports	6.4.10	
Security management		
Monitoring of IFM processes and IFM data life cycle	6.5.1	Unchanged
Management of IFM security keys	6.5.2	
Management of security lists	6.5.3	
Termination of SE		
Regular termination	NEW	See 9.9
Forced termination	NEW	
Termination on customer's demand	NEW	
Customer Service Management	6.6	See 9.10

9.4 Certification of SE

The IFM Security Manager and SE Security manager mutually agree their security policy and sign a security agreement

This security agreement includes the acceptance by the IFM Security Manager of the certification process of the SE managed by the SE Owner.

This agreement can be built directly by the parties or via a trusted third party.

The role of such a third party is called a Controlling Authority in GP specifications

9.5 Installation of Application template

9.5.1 Pre-installation of the Application Template in the SE

Trigger: Application owner and SE owner agree on a systematic pre-installation.

Authorized Application Retailer sends the Application Template to authorized SD manager.

SD manager creates Security Domain and installs Application Template.

SD Manager reports to the Application Retailer.

9.5.2 Installation of the Application Template on request

9.5.2.1 Trigger: application retailer

Application retailer requests authorization from SD Manager indicating the size needed for the SD.

SD Manager and Application retailer mutually authenticate themselves.

SD Manager checks that the Application Template capacity is available in the SE.

SD Manager asks customer to agree to the downloading of the Application Template.

SD Manager creates the Security Domain inside the SE (if not existing yet).

SD Manager circulates the Application ID and the size of the SD to the SE owner for customer service.

9.5.2.2 Installation without personalisation

Application Retailer sends the Application template to SD Manager.

SD Manager downloads the Application template inside the Security Domain.

SD Manager reports to the Application retailer that the operation is complete.

9.5.2.3 Installation and personalisation

SD Manager and Application retailer mutually authenticate themselves.

SD manager informs Application retailer if the SE has a time limit of validity.

Application Retailer sends the Application template and the personalisation data to SD Manager.

SD Manager downloads the personalised Application inside the Security Domain.

SD Manager reports to the Application retailer that the operation is complete.

Application Retailer informs Application owner.

9.6 Personalisation of pre-installed Application template

Trigger: Customer subscribes for the application to the application retailer and provides him with his SE-ID.

Application Retailer personalises the Application Template.

Application Retailer circulates the SE ID to the Application Owner for customer service.

9.7 Update of Application Template

Trigger: Application Owner updates the software or personalisation data of the application without changing the size of the Security Domain. If the size of the Security Domain needs to change, the Application Template should be considered as a new one.

Application Retailer calls attention to the customer for him to request the update.

Customer requests the update from the Application Retailer.

Application Retailer requests authorization from SD Manager.

SD Manager and Application Retailer mutually authenticate.

SD Manager checks the current status and content of the Application and forwards it to Application Retailer.

Application Retailer reconstitutes the new Application Template with the current Products and forwards it to SD Manager.

SD Manager updates the Application in the SD

SD Manager reports to the Application Retailer that the operation is complete.

Application Retailer informs customer about the update of the Application.

9.8 Termination of application

Trigger: Customer or Application Owner.

Customer or Application Owner requires Application Retailer to terminate the Application.

If the Application contract requires it, Application Retailer asks the other party to approve the termination of the Application.

Application Retailer requests SD Manager to delete the Application and eventually the SD.

SD Manager and Application Retailer mutually authenticate.

If also required by Application Retailer, SD Manager checks the current status and content of the Application and forwards it to Application Retailer.

SD Manager deletes the Application in the SD and if required the SD.

SD Manager reports to the Application Retailer that the operation is complete.

Application Retailer informs customer about the deletion of the Application.

9.9 Termination of SE

9.9.1 Regular termination of SE

When Application Owner was informed about the installation and personalization of its Application on an SE (9.5.2.2), he was also informed of the time limit of validity of the SE.

When the time limit comes, Application Owner proceeds to the Application according to the Application contract.

9.9.2 Forced termination by SE owner

SE Owner was informed of the Applications downloaded in his SE (9.5.2).

SE Owner informs Application Owner that he is going to terminate the SE.

Application Owner proceeds to the Application according to the Application contract.

9.9.3 Forced termination by Customer

Application Owner proceeds about the Application accordingly to the Application contract.

9.10 Customer service management

As indicated in 8.2, the Media Retailer, the SE Retailer and the Application Retailer in direct relation with the customer provide the Customer service that relates to their role.

The use cases depend on the corresponding set of rules agreed by the Media Owner, SE Owner and Application Owner to organize the cross-cutting of these services.

10 Practices for implementing the use of multi-application

10.1 General

The following subclauses provide some examples or recommendation of practices for using multi-application environment.

Using multi-application devices may not only be considered as an economic opportunity to avoid managing specific transport Media and to propose interoperable Media for customers to address different fare systems.

It can also be an opportunity to enhance interoperability between existing IFMs in a given area following migration paths as described in ISO/TR 24014-2.

10.2 Implementation of Roles into Organisations

The attribution of the functions to Organisations is implementation dependant and will differ from case to case without any consequence towards interoperability.

Roles can be split between different Organisations to meet industrial and economical objectives.

Organisations may fulfil Roles that are in the IFM Community and therefore comply with the Core part of Set of Rules and other Roles that do not and are modellised as IFM Partners or just as an IFM Environment, e.g. an Application Owner may decide to act as a SE Owner to issue proprietary SD-cards as SE.

However, that possibility may be limited by business rules for commercial or trust reasons.

10.3 Legal ownership of the Media and SE

The legal ownership does not refer to the concepts of Roles described in this Technical Report.

It belongs to an Organization whatever Roles that Organization may fulfil.

The legal ownership of the Media doesn't refer to the Role described as Media Owner.

Similarly, the legal ownership of the SE doesn't refer to the Role described as SE Owner.

They can be a legal responsibility of different types of Organisations.

— PT Organization, e.g. if a PTA or PTO decides to issue a PT based Media or SE such as a Java contactless card, SD-Card or USB device, and allows it to be downloaded with other transport –or non-transport- Applications.

— Other types of business, e.g. payment, business or telephone if an IFM Community agrees to use their SE to host its Application.

— The Customer himself.

10.4 Implementation of the Role of SD manager

Trust into the organisations that participate in the security functions gathered in the role of SD Manager is an absolute requirement.

These organisations must therefore be agreed as Trusted Service Managers both by the SE and the IFM Security Manager as shown in Figure 13.

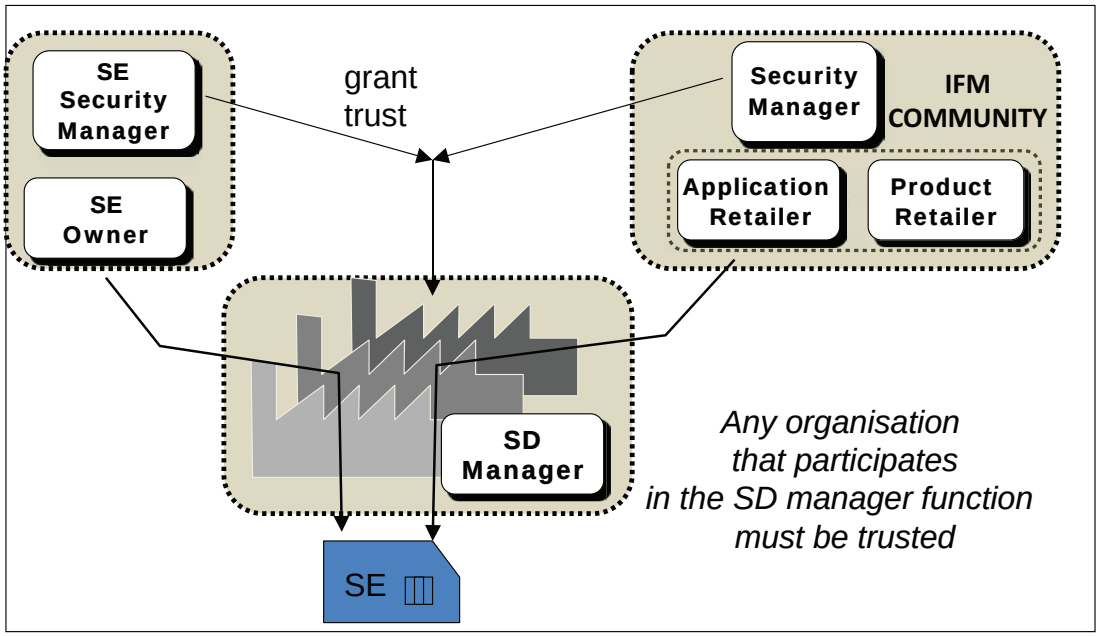

Figure 13 — Trusted Service Managers acting as SD manager

They can be third parties or can also fulfil Roles in the IFM Community or in the SE Community.

This trust regime is independent from the fact that the organization fulfils or does not fulfil any of the roles defined in the Functional model.

Whatever the implementation into one or more organisations depending or not from the PT Community or from the parallel SE Community, it requires a specific set of rules about the secure management of the SCP and of the data sources.

In some implementations, the same Organization that is SE owner will create the Secure Domains and the same organization that is Application Retailer will load the Application Templates.

In some other implementations, the IFM Community and its partners will agree to call for other organisations to act as trusted third parties.

This may be particularly suited when an IFM-Community agrees that its Application may be downloaded into different SEs that belong to different SE owners.

Such an IFM Community is likely to have to interface with different SD Managers.

It may then be convenient to use a common technical interface for the benefit of the Application Retailer and Product Retailer and to attribute the management of that interface to one Organization.

Similarly, different SE Owners may agree to use a common trusted third party to manage the SCPs.

10.5 Implementation of the Portal function

The Application Portal should be neutral to any competition inside the IFM Community and let the Customer choose among the different possible Application Retailers.

Application Portals may be driven by TP related or non-TP related Organisations.

In an area where there is a need and a political will to enhance interoperability based on Multi-Application between different IFMs, PT can propose an Application Portal on a common website.

Similarly, SE Owner or Retailers can propose an Application Portal on a website listing all the PT or non PT Applications that are available for download on their SE.

10.6 The EU-IFM Project proposal

10.6.1 Context

France, Germany and UK drove (2008-2010) a project funded by the European Commission with the objective of making their respective IFMs interoperable.

The project recommends the use of multi-application media to overcome the differences without the need for any IFM Community to throw away their previous investments.

In a first phase, drawn as "parallel IFMs" in Figure 14, the existing IFMs continue their life, and the Customer chooses the set of Applications as he needs.

In a second phase, a complementary European application is issued that can be progressively used as a complement to the existing ones, and may in a longer term replace them as well.

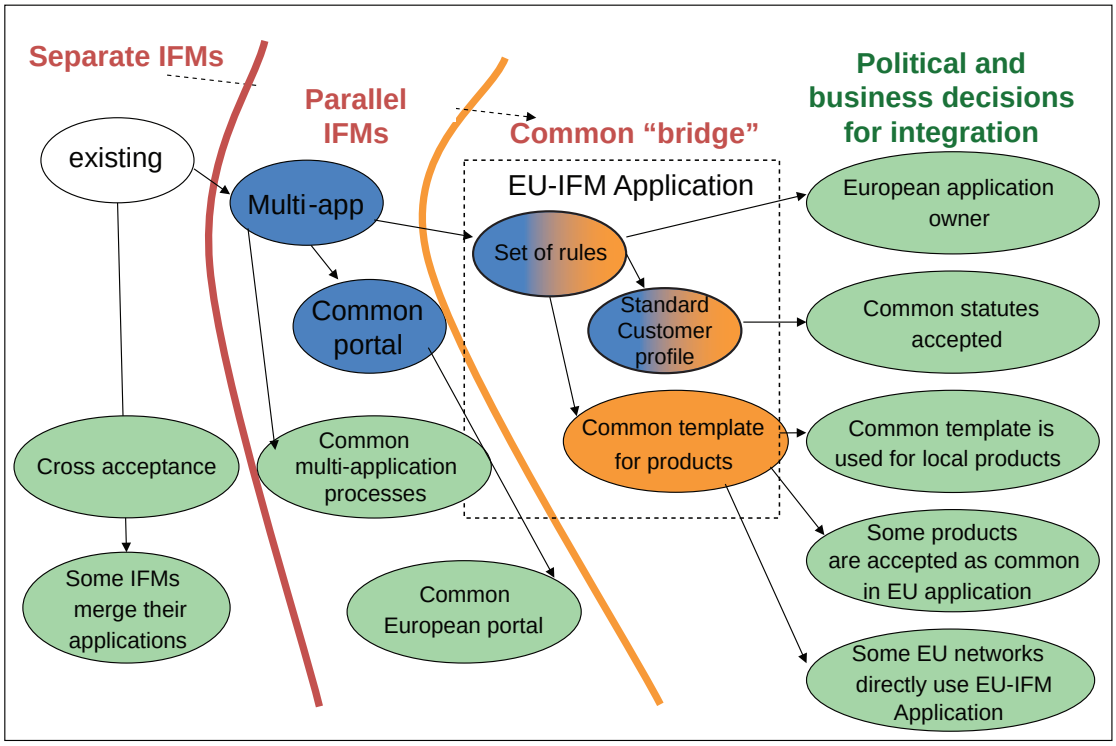

Figure 14 — European EU-IFM migration path

10.6.2 Technical conclusions

The above perspective was limited in the project to PT Applications only, although it does not exclude other businesses.

The envisaged Media were transport issued multi-application media, e.g. Java cards or Java USB keys, which are considered as embedded Secure Elements.

The use of mobile phones was not excluded, but NFC perspective was not mature enough for any description.

The conclusions of the projects completely endorse the list of requirements of Clause 7.

A laboratory demonstration has been realized with a Java Card loaded with three Applications from the three participating countries.

This card, presented to vending machines and validators from the three Applications proved to work without these devices having been modified.

10.6.3 Functional model

An alliance would be created to fulfil the following roles:

— Specify the necessary common specifications for the Media;

— Build and administrate the extra set of rules between IFMs;

— Be the common SE security manager.

Table 4 summarizes how the roles and functions are envisaged in the project.

Table 4 — Implementation of the IFM Project

Role	Organisations
First step: parallel IFMs	
SE Owner	Participating PT card issuers who join the Alliance
SE Retailer	All organisations currently acting as Application retailers and therefore distributing cards to the customers would not compulsorily retail multi-application media
SD Manager	On decision of each SE owner
Application Owners	PTAs / PTOs currently acting as Application owners who join the Alliance
Application Retailer	The current organisations acting as Application retailers and therefore distributing cards to the customers would not compulsorily retail the application on multi-application media. An Internet vending service would be created by each Application owner to retail the application on multi-application media.
Second step: common EU IFM application	
Application Owner	The alliance
Application Retailer	To be determined. A common organization may be agreed to retail the common application via Internet, but it is also likely that each member of the alliance will have the possibility to do so.
Application Portal	A European PT Application Portal is intended
Application Store	The possibility for above PT EU Application Portal to act as an application remains an open point. Whatever the answer, no monopoly on application retail can be accepted.

10.6.4 Conclusion

Technically, the Media does not seem to be the hard point, but rather the insufficient standardization of the proximity contactless communication RF protocols.

Besides the business case and the related political decision for investment, the main difficulty for a real implementation appears to be the necessity for business rules at a wide scale. The current Technical Report can help as a tool for the envisaged Alliance to define this extra set of rules.

10.7 Mobile SUICA

10.7.1 Context

“mobile Suica” is an implementation of Suica application (an IFM Application) on mobile handsets. East Japan Railway Company (JR East) plays Application Owner. It has been in practical use since January 2006.

"mobile Suica" is provided by Suica application and the supporting functions outside SE in a handset (communicating with the back office, providing user interfaces and so on).

SE is used not only for Suica application but for other non-IFM Applications such as electronic money, loyalty programs and so on. Currently all the SEs are provided as embedded in mobile handsets.

In addition to Suica application products for smart cards*, Suica application for mobile handsets is capable of other products such as IC tickets for Shinkansen, Japanese high speed train system.

Suica application products for smart cards:

— Type 1: Pre-loaded products: season pass and green car (first class) ticket.

— Type 2: Automatic fare calculation product: Single trip with Entry/Exit validation rule using prepaid "stored fare (SF) value." (SF value can be used for shopping.)

10.7.2 Technical conclusions

— Media (mobile handsets) have communication functions using ISO/IEC 18092 (NFC) and OTA.

— SEs confirm SCPs of which implementation is independent from ISO/IEC 7816.

— The SCPs are used (1) between Suica application and the NFC interface device when using NFC, (2) between Suica application and the distant server when using OTA executed by the supporting functions and (3) between Suica application and the supporting functions.

— Load/update/delete of Suica application and the products is basically executed via OTA, using the SCPs.

— Suica application is preinstalled in SEs in some mobile handsets.

— The implementation of the application selection mechanism for Suica application in the SEs is independent from ISO/IEC 7816. However Applications can be identified by application ID prepared by JIS X 6319-4, and customers also are able to select an application.

— SEs are required to be certified as ISO/IEC 15408 (CC) EAL4+ or above.

10.7.3 Functional model

Despite that "mobile Suica" has some different technical requirements from those described in Clauses 7 and 8, the same functional model described in Clause 9 is led by the technical requirements of "mobile Suica".

Table 5 summarizes which organizations play the roles of IFM-Roles, IFM-partners, and Intermediary roles.

Table 5 — Implementation of Mobile SUICA

Role	Organisations
SE Owner	FeliCa Networks
SE Retailer	mobile handset retailers
SD Manager	FeliCa Networks / JR East
	FeliCa Networks executes the functions complied with the set of rules of the SE Community.
	JR East executes the functions complied with the Core part of Set of Rules.
SD Security Manager	FeliCa Networks
Application Owner	JR East
Application Retailer	JR East
Application Portal	Application Portal: JR East (excluding smart phones)
Application Store	Application Store: application market operator for smart phones

10.8 France interoperability project

10.8.1 Context

The major mobile networks operators and transport operators operating in France have agreed common technical specifications and organisations for the deployment of mobile ticketing, mobile payment and tag reading in SIM based NFC phones.

The objective is to build an open mobile ticketing organization.

CITYZI is the trade mark for implementation, under free licensing by AFSCM (non-profit organization).

In parallel, the Public Transport authorities issued a functional list of requirements, know as "NFC DOFOCO standing [in French] for "COmmon FOnctionnal DOcument".

Nice started as the first pilot for mobile ticketing. A set of local services, including Public Transport Fare management, city services, and a PayByPhone application is proposed on SIM based mobile phones. Simultaneously, contactless EMV bank cards are issued by a few banks.

Fifteen other cities in France are initiating similar sets of services.

The customer can purchase tickets from the phone, and either be billed on his telephone monthly bill or pay with the PaybyPhone application (preregistration of the customer's bank card).

Tag reading is used to assist mobility including PT real time customer information.

Not all NFC services in the pilot rely on secured Applications complying to the restricted definition in this Technical Report.

Some of them rely on vouchers and may be managed differently.

A Transport application for occasional trips will be issued and shared to host local occasional fare products as well as trans-regional products, providing customers with a large customer friendly interoperability.

This application will be proposed either on multi-application cards or on mobiles.

10.8.2 Technical conclusions

The pre-existing ticketing infrastructure complies with ISO/IEC 7816-4.

The program confirms the need for a complete coherence between contactless standards ISO/IEC 14443 and ISO/IEC 18092 (NFC) and for a complete implementation in the infrastructure.

The technical specifications for the implementation of the Applications in the phones or other sorts of multi-application media comply with GP standards and with the requirements listed in Clause 7.

A new national standard to attribute AIDs has been approved.

10.8.3 Functional model

Table 6 summarizes how the roles and functions are envisaged.

Table 6 — Implementation of the French interoperability project

Role	Organisations
Media Owner	CITYZI mobiles are certified by AFSCM
SE owner	Mobile network operators
SE retailer	Mobile phone shops
SD manager	Mobile network operators
	The 3 MNOS in the trial have agreed a standardized interface for SD management (AFSCM Specifications 1.2).
	Each MNO subcontracts individually with TSM organisations to handling the SD manager role.
Application owners	PT Authority for the local Applications.
	Not yet determined for the common application (December 2012).
Application retailer	PT Operator
Product retailer	PT Operator.
	The Mobile Network Operator of the customer may act as a billing and settlement organization.
Application Portal	
Application store	

10.9 Case of Korea

10.9.1 Context

IC Card business which started in 1995, is now reaching seven trillion won as of December, 2011. It has been used by more than 80 % of cities and provinces. It started mobile service in 2002, especially NFC based traffic card services started in 2011 and it will be spread nation-wide by 2012.

In Korea, the smart card has been servicing the transportation payment for the bus, subway, taxi etc. It is also used at the convenience store, theatre, coffee shop, fast food, mart, amusement park, public parking lot fee, public document issuing fee, national park entrance fee etc.

Card issuing and infrastructure operation companies in Korea are financial companies (T-money, Cashbee, etc.), Transport organisations (UPASS, Toppass), Telecommunications organisations (K-cash), Roadtolling organisations (Hi-pass, X-cash, GLORY CARD), and many credit card companies.

Especially, the Hi-pass card is using at ETCS.

10.9.2 Mobile device

Through mobile phones, there are various ways to use a pre-paid card including on/off-line, transportation/distribution. Mobile pre-paid card is USIM based. In case of a smart phone (NFC based), to download the application from an App store, the customer can charge the cash through a mobile phone integrated payment system. It also has auto top-up function. A mobile pre-paid card can be used for most public transportation and also can be used in the distribution and public service industry as a payment method. Service transaction log can be easily checked by application. This kind of mobile service is available with all mobile network operators in Korea.

10.9.3 Technique

— Technique of Card issuing and infrastructure operation companies (cashbee, T-money, etc.)

  RF card: It complies with ISO/IEC 14443, Type A/B. To keep stable function, RF tuning is executed according to each company guideline;

  Applet/application: Card issuing and infrastructure operation companies in Korea perform functional test to guarantee a high level performance.

— Technique of Hi-pass

  Hi-pass card is designed to comply with International Standards and Technology (ISO/IEC 7816, ISO/IEC 14443, etc.) related to the IFMS to ensure compatibility and interoperability.

  In addition, a nationally recognized testing laboratory with expertise in testing ensures the quality of the card.

— Contact Card: It is used to communicate with On Board Equipment (OBE) in Vehicles. Basically it complies with ISO/IEC 7816 (including USB-ICC)

— Contactless Card (RF Card): It is used to communicate with Payment Terminals on Toll booths. It complies with ISO/IEC 14443, Type A/B.

10.9.4 Role Model

Table 7 summarizes how the roles and functions are envisaged in the Mobile payment device context.

Table 7 — Implementation of Mobile Payment

Entity	Organisations (Business Entities)
Media Owner	Customer Specifications are managed by Mobile network operators
SE Owner	Mobile Network Operators
SE Retailer	Mobile Phone Shops
SD Manager	Mobile Network Operators & Payment Operators
Application Owner	Payment Operators
Application Retailer	Mobile Network Operators & Payment Operators
Application Portal	All kinds of operators

10.10 Comparison with EPC-GSMA white paper

The European Payments Council (EPC) and the GSM Association (GSMA) published a whitepaper to describe the Service Management functions for Mobile Payment and how they should be distributed between the MNO community and the bank community.

The categorization of the service management functions over the two communities as done in this EPC-GSMA whitepaper matches with the emerging concepts of an ‘MNO TSM’ grouping all the service

management functions of the SE Community, and a 'Service Provider TSM' grouping all the service management functions of the bank community.

This description can be compared to the one described in this Technical Report, considering the MNO as one particular instance of the SE Community and the bank instead of the IFM Community.

Table 8 summarizes the implementation of the service management functions and compare it to the different roles introduced in the report.

Table 8 — Implementation of functions in GSMA white paper

	EPC-GSMA function	ISO/TR 24014-3 **role**
SE Issuer Community		
1.	SE Security Policy	SE Security Manager
2.	SE certification	SE Security Manager
3.	Manage list of Apps stored on the SE	SE Owner
4.	Creation of APSD	SD Manager
5.	Management of Secure Keysets (for pre-created SSD keysets)	SD Manager
6.	Assignment of SSD	SD Manager
7.	Management of the SE Memory	SD Manager
8.	Contractual and technical pre-controls (eligibility check)	SD Manager
9.	Management of OTA NFC application on behalf of the Application Provider (Simple Mode)	SD Manager
10.	Customer service	SE Retailer
11.	Management of Customer lifecycle events (change of phone number (MSISDN), SE Change	SE Retailer
Application Provider Community		
12.	Development of Application	Application Owner
13.	Development of Application UI	Function not considered in ISO/TR 24014-3
14.	Application Approval	IFM Security Manager
15.	Data Preparation (personalisation data)	Application Retailer
16.	Application Provider SD key management (logical and physical secure storage and delivery)	SD Manager
17.	Download and Installation of Application	SD Manager
18.	Download of Application UI	Function not considered in ISO/TR 24014-3
19.	Personalisation of Application	Application Retailer
20.	Activation of Application	Function not identified in ISO/TR 24014-3
21.	OTA Functional management of Application (application update: holder profile change, auto-reload management, product sale, product renew)	Application Retailer / Product Retailer
22.	OTA Applicative management of Application (lock / unlock)	Application Owner
23.	Customer Service	Application Retailer
24.	Management of Customer lifecycle events	Application Retailer

In terms of ISO/TR 24014-3 the SD Manager Intermediary Role is implemented in two parts:

The MNO TSM is responsible for the SE issuer part of the SD manager function and takes care of the Security Domain Lifecycle Management:

— Manage list of Applications stored on the SE

— Creation of APSD

— Management of Secure Keysets for pre-created APSD keysets and ISD keysets

— Assignment of APSD to the Application Provider SD Manager

— Management of SE Memory

— Eligibility check

— Download of the SE User Interface

The Application provider TSM is responsible for the Service Provider (bank or transit) art of the SD manager function and takes care of the Application Lifecycle Management:

— Application Provider Security Domain key management

— OTA Download and installation of the application

— OTA Download of Application User Interface

— OTA Personalisation of Application

— OTA Functional and applicative management of the application.

The comparison with an IFM environment clearly shows that these latter functions are very close to the heart of the roles of Application Owner, Application Retailer, Product Owner and Product Retailer in the IFM Community.

As a conclusion, a similar implementation of the SD manager Role into two organisations is one of the possible implementations of the Multi-Application role model specified in the report to develop mobile ticketing.

It can make sense to establish a Transit TSM organization rather than depending on an MNO TSM or on a single 'everything for everyone' TSM.

This set up has a number of advantages for transit:

— Reduced operational costs for applicative management, compared to the situation where the MNO TSM is needed for every OTA change in the transit application.

— Sharing the OTA services between multiple transit organisations will also share the costs between the participating transit organisations.

— Having direct OTA access to the transit application in the Secure Element allows the transit organisations to value added services next to the core fare management service. Real time travel information and location based information/warnings are two examples of these value added services.

Bibliography[3)]

[1] GlobalPlatform Card Specification 2.2.1 January 2011

[2] GlobalPlatform Card Specifications 2.2 – Amendment A: Confidential Card Content Management v1.0.1 – January 2011

[3] GlobalPlatform Card Specifications 2.2 – Amendment B: Remote Application Management over HTTP

[4] GlobalPlatform Card Specifications 2.2_Amendment_C_Contactless-services_v1.0.1

[5] GlobalPlatform UICC Configuration 1.0.1 – January 2011

[6] GlobalPlatform Messaging Specification 1.0 – October 2003

[7] GlobalPlatform Messaging Specification for Management of Mobile NFC Services V1.0 – February 2011

[8] GlobalPlatform System Web Services profile for GlobalPlatform Messaging

[9] GlobalPlatform Composition Model

[10] JCP — Java Card Platform Specification 3.0.1 Classic Edition

[11] (U)SIM Java Card Platform Protection Profile – Basic and SCWS Configurations, ref. PU-2009-RT-79, version 2.0.2

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

[13] EU IFM Project — Common requirements and recommendations on interoperable media and multi-application management — Deliverable 3.2 – September 2009

[14] EU IFM Project — Migration paths — Deliverable 3.3 – February 2010

[15] IFM Project — Development of Cooperative Organisational Models — Deliverable 4.3

[16] EMVCo — EMV Contactless Specifications for Payment Systems, EMV Contactless Communication Protocol Specification 2.1

[17] ETSI TS 102 225, Smart Cards; Secured packet structure for UICC based applications (Release 7) (2006-04)

[18] ETSI TS 102 226, Smart Cards; Remote APDU structure for UICC based applications (Release 7) (2007-07)

[19] ETSI TS 102 613, UICC CLF interface — Part 1 Physical and data link layer characteristics (Release 7 2007-11)

[20] ETSI TS 102 622, Smart Cards, UICC — Contactless Front-end (CLF) interface; Host Controller Interface (HCI) (Release 7 2008-02)

3) References 1 to 11 available at http://www.globalplatform.org. References 12 to 16 available at http://www.ifm-project.eu/

ICS 03.220.01;35.240.60

Price based on 39 pages