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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.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

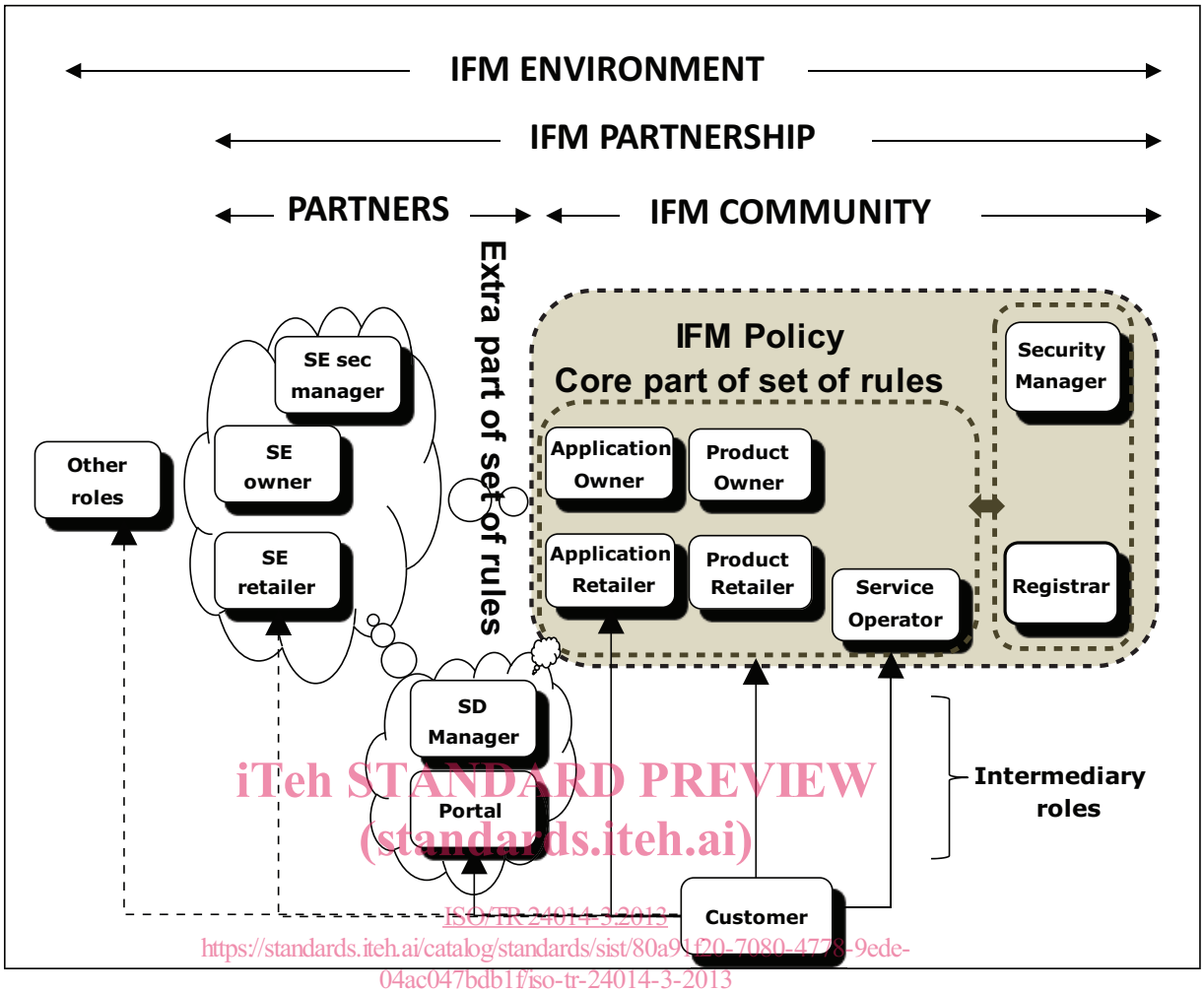

Figure 1 — Main terms and definitions illustrated in the functional model

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.

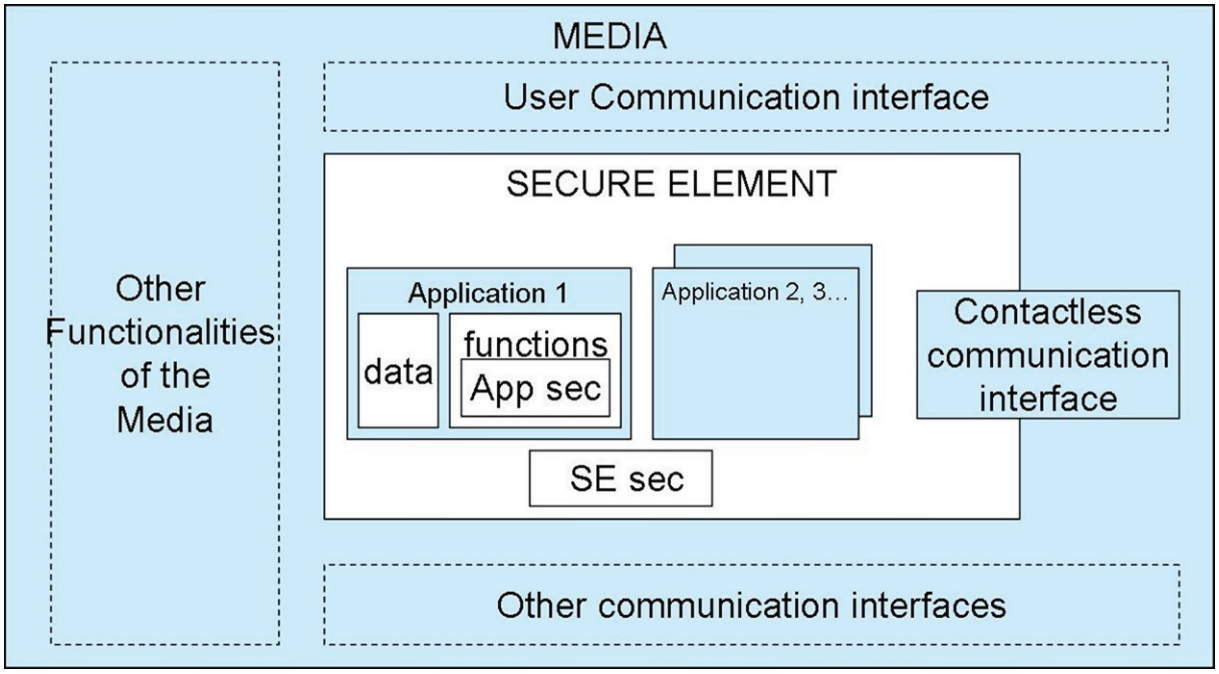

Figure 2 — Media functional model

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.