European handbook on rules and regulations for privacy protection in fare devices and back-offices

Deliverable 2.3

Version 1.4

March 2010

For further information please contact:

Work package 2 leader
Michel Arnaud
michel.arnaud@u-paris10.fr

Université Paris Ouest Nanterre La Défense
Labo CRIS InfoCom UFR LLPhi bât L 200 avenue de la République
92001 Nanterre Cedex
France

Main authors
Michel Arnaud
Michel.arnaud@u-paris10.fr

Cord Bartels, NXP
Harald Kelter, BSI
Rainer Oberweis, BSI
Birger Rosenberg, NXP
TG 03126 - Technical Guidelines for the Secure Use of RFID
TG 03126-1 Application area "eTicketing in public transport"

Gilles de Chantérac
gdc@interappli.fr
Jean-Louis Graindorge
jl.graindorge@wanadoo.fr
Jean-Philippe Amiel
jean-philippe.amiel@nextendis.com

For further information on the IFM Project please contact:

Coordination
ITSO Ltd.

Phone +44 121 634 3700
Fax   +44 121 634 3737
E-mail: compliance@itso.org.uk

Visit the webpage **www.ifm-project.eu**

Secretariat
TÜV Rheinland Consulting GmbH

Phone +49 221 806 4165
Fax   +49 221 806 3496
E-mail: oliver.althoff@de.tuv.com

Table of content

1. Scope of the document

The objective of WP2 of IFM project is to propose a privacy model to address traveller's personal data protection issues. This proposed model is compliant with the working paper "e-ticketing in public transport" that was adopted by the international working group on data protection in telecommuniacation. The objective of this deliverable 2.3 is to provide a code of conduct and a European Handbook on rules and regulations for privacy protection in fare-devices and back-office of IFM transport systems. This process has to be performed under stakeholders control in order to increase confidence among them, to remain customer oriented and technologically flexible. It could be proposed that UITP takes over managing these documents with all interested persons, including non-members, before the specific organisation proposed by the IFM project to manage specifications of the future European application is established.

Source of theses documents are German Federal Office for Information Security 53 TG 03126-1: Application area "eTicketing in public transport" and Gilles de Chanterac focus paper on "privacy in transport IFM applications" version 3.2

2. Executive summary

The objective of this document is to propose a common basis to build a "Privacy by Design" system and organisation for IFM systems. This leads to define architecture and monitoring principles to apply rules and regulations for information security and privacy for travellers. Common definitions of data typology: privacy, confidentiality, integrity, availability, unlinkability, unobservability, anonymity, authenticity, non-repudiation, accountability are presented. They are completed by operational concepts such as personal identifiers, object identifiers, anonymous objects, subscriber identity, transaction fare data, bank transaction data, indirectly personalised fare transaction data, authorised user identity and statutes, with links established between object identification and subscriber's identity.

Specific information security and privacy targets include protection of personal data, protection of entitlements, protection of logistical data (anonymised usage data), reliable invoicing, protection of applications and entitlements, protection against the creation of movement profiles, for data minimization. Protection demand categories formed on the basis of security targets described above are leading to a code of conduct which guarantees anonymous accessibility, protection against risks of abusive use of personal data from applications in the media, by staff, of abnormal events, of direct marketing tools, of hacking and criminal use of personal data in back-offices, of uncontrolled dissemination of identity data through multi-application management. Generic safeguard measures are finally presented in agreement with the common IFM System Architecture.

3. Handbook on rules and regulations

3.1 Definitions related to privacy protection

Privacy: The purpose of privacy is to protect against infringements of the personal rights of the individual through the handling of his personal data. Privacy refers to the protection of personal data against possible misuse by third parties (not to be confused with data security) [EU_REF].

Confidentiality: confidentiality means protection against the unauthorised disclo-sure of information. Confidential data and information may only be accessible to authorised people in an authorised manner. Formulated as a protection target this means: stored information and information that is to be communicated is to be pro-tected against access by unauthorised persons.

Integrity: integrity means ensuring that data is correct (intact) and that systems function properly. Formulated as a protection target this means: stored information and information that is to be communicated is to be protected against unauthorised modification.

Availability: the availability of services, of the functions of an IT system, IT applica-tions and IT networks – and also of information – exists if these things are always available to their users when required. Formulated as a protection target this means: information and operating systems are to be protected against being with-held improperly.

Unlinkability: if two communication elements within a system are unlinkable, it means they are not any more or less related to one another than is already known and established. Within the system, no further information about the relationship between these communication elements can be obtained. In practical terms this means that a single user can make use of services and resources more than one time, without third parties being able to see that these access events (in the com-munication model: messages) are related through the user.

Unobservability: an event is unobservable if it cannot be determined whether it has happened or not. Sender-unobservability means it cannot be seen that anything has been sent; recipient-unobservability is the same: it is not possible to ascertain that something has been received. Relationship-unobservability means that it can-not be seen that anything is sent from the group of possible senders to the group of possible recipients.

Anonymity: anonymity is the condition of being unidentifiable within one's anonym-ity group. Using the term unlinkability, anonymity can be more precisely defined as the unlinkability of the identity of a user and an event initiated by that user. Sender-anonymity is therefore unlinkability of sender and message, and recipient-anonymity is the unlinkability of message and recipient.

Authenticity: the term authenticity designates a situation in which the partner in a communication process is actually the person he claims to be. Authentic informa-tion is information that genuinely comes from the stated source. The term is not only used when people's identity is being checked, but also for IT components and applications.

Non-repudiation: protection should exist against the possibility of denying that messages have been sent and received by persons whose authenticity has been determined.

Accountability: binding validity joins together the IT security targets of authenticity and non-repudiation. When transmitting information this means that the source of the information has proven its identity and that the receipt of the message cannot be disputed.

3.2 Definition of entities in identification data bases

The following concepts are used in the document.

Personal Identifiers

Is considered as a personal identifier (PID) any set of data describing enough individual characteristic of a person to allow his direct identification, i.e. to find him (official identity, addresses, bank references) or to prove he is himself (biometrics of any sort).

PIDs	Personal IDentity	Official identity : Name, nationality, birth place & date
		Addresses : postal or tel. or web address
		Physical description : photograph, biometrics
		Bank accounts (BID)

Objects

Is considered as an object any hardware or software component in hand of the customer that can be individually managed by integrated fare management systems.

The main objects are defined by ISO 24014-1 standard:

- Transport products are encoded for use in a piece of software called application where IFM data can be secured, processed and stored.
Originally, applications were installed in the media when this one was issued. (e.g. cards).
- One only identifier can be used for both objects.

With downloadable media, it is necessary to consider two different identifiers.

In the most complex use cases, some media use removable secure elements which have their own identifiers.*e.g. mobile set number MID in which SIM Card Number SEID is inserted was downloaded with application number AID where product number TID was made available to access public transport*

Unique identification of objects is most often necessary to address technical basic processing needs (i.e. medium ID is necessary to manage contactless transactions), commercial needs (operating and maintenance of applications) or security issues (blacklisting of fraudulent components).
Transport products not always have a unique ID.

<u>Objects identifiers</u>

Objects exist by themselves and their identifier exists without any link to any individual.
They can be become indirect Personal identifiers only if a link is created as described further.

OIDs	Object IDentifiers that can become Indirect Personal IDentifiers	
MID	**Medium ID**	Unique number individually identifying each portable objet independently of its form factor (e.g. card, USB Key, telephone set) where one or more applications or Secure elements can be implemented
SEID	**Secure Element ID**	Unique number individually identifying each secure element (e.g. SIM card or SD card) where one or more applications can be implemented
AID	**Application IDentity**	Unique number individually identifying each instantiation of each application (piece of software in a MID.
TID	**Product ID** (optional)	Unique number individually identifying each instantiation of each product

<u>Anonymous objects</u>

Most systems have anonymous use-cases where media (cards), applications and products are issued to customers completely anonymously.
The AID is used as the reference in the processes.
No subscriber applied an therefore was inscribed in any Commercial management list (CML)
Therefore, seen from the system anyone can travel (no authorised user) and no automatic invoicing or charging is possible.

<u>Subscriber</u>

But many use cases need a subscriber to be registered to <u>at least one</u> of the stakeholders of the Integrated Fare Management system for functional reasons:
▪ Contractual responsibility
▪ Billing processes

These functionalities are processed by the back-office, and therefore encoding the subscriber's ID in the media is not necessary.
Objects then become personal and their object-identifier however becomes an indirect personal identity.

The subscriber is the person who subscribed to be registered as a customer in the IFM. As such, the subscriber is the legal person who will be responsible for the use of the resources provided by the IFM such as the media and the applications.
Subscribers are also responsible for paying the products when the product includes a billing facility such as post-payment, automatic renewal of products, automatic reloading of stored value.

SID	Suscriber's IDentity	PID of the subscriber

<u>Example of imbrications</u>

In multi-application contexts as envisaged in the IFM project, these different IDS can co-exist.
In most complex use cases, it could happen for example that mobile set number MID belonging to Mr Smartphonein which SD Card Number SEID is inserted belonging to Mr EssDee was downloaded with application number AID1 subscribed by Mr Subscriber1 and with application number AID2 anonymous.

Mr EssDee has borrowed his son's NFC phone and inserted his Transport SD card where he downloaded his concessionary application for his domestic IFM and an anonymous application to travel elsewhere.

Transactions

Transactions are events in the life cycle of the process that imply an action by the customer.
They can relate to the fare system itself or to the related bank orders.

In this document, the word *payment* is avoided, because it relates to a complex process that includes purchasing, pricing, billing and collecting the money, all actions that don't imply the same participants.
Purchasing, billing and pricing are processes belong to the fare management processes.
Collecting the money doesn't.

Fare transactions

Fare Transaction exist by themselves, referring to the event itself, without mention of any personal or objet identifier, e.g. "entrance in station x at such moment with such product"

This definition is compliant with the recommendation from the Berlin Group: *System design should be such as to separate the personal information from travel information (two component model).*

By themselves, they are sufficient for global marketing or operational monitoring purposes:

FTD	Fare Transaction Data	Data set describing a fare management event (Purchase, Validation, Inspection …) Without association with an OID

Bank transaction data

Bank transaction data always need to refer to a bank identity and therefore they are always indirectly personalised.

BTD	Bank Transaction Data	Any bank transaction data (always associated with a BID)

Indirectly personalised fare transaction data

Fare transactions are associated to an Object Identity for some of the fare management processes as described further.

Conceptually, fare management systems combine functions of access control and billing management.
Their life cycle must therefore be permanently kept under control to manage the commercial processes as well as to prevent all imaginable types of fraud.

Object identity/identities are therefore always attached to the Transactions data issued by the front-office when they are forwarded to back-offices.
Automatic routines will then split transaction data between the different data bases that are necessary for all the processes.

A special attention is kept to validation data:
False products would give fraudulent access rights IFM security managers therefore rely on back-office verifications to detect attempts of attacks.

The objective is not so much to detect past fraudulent events than to avoid risks of future ones by black-listing the suspected objects.

The authorised user

Unipersonal fares give special access rights or special prices to individuals that can justify some statutes (concessionary fares) or that applied to special commercial offers sold for use by one unique person (i.e. carte orange tariff in Paris, or loyalty schemes).
The authorised user is designated by the subscriber, but can be different from himself.
E.g. parents can subscribe personal cards for their children, or employers for their staff.

Control of unipersonal fares

IFMs need to control that the special rights are not unduly claimed or used.
Therefore, the identity of the authorised user is inscribed in a data base and eventually associated with the corresponding statute
This allows revoking expired rights and controlling the authenticity of the corresponding fare transactions with back office routines.

AUID	Authorised User's IDentity	PID of the authorised user (for personalised contracts)
AUS	Authorised User's Statutes	CEN1545 statutes, language, birth date, special rights, etc…associated to the authorised user

Statutes data are encoded in the card, so that vending machines can only load the concessionary products on the appropriate application or media.

It must also be possible for inspection staff on board to control that the effective user is the authorised person.
For that reason, PID data may be

- Printed on the medium (only possible for dedicated media)   <u>visual</u> personalisation of media.
- And/or encoded in the medium (e.g. a digital photograph)   <u>electronic</u> personalisation of media

Free visual personalisation of the media

For unipersonal products that are accessible without any statute, some IFMs permit customers to personalise themselves their media for visual inspection by sticking their photograph and/or writing their name.
Physical dispositions are taken to make fraud visible from inspection staff.

That method however doesn't seem applicable to downloadable media as they are envisaged in the EU-IFM project.

Links from an Object Identification to a Private Identity (from OID to PID)

The above description and typology of data shows that direct identification of the individuals is only a functional necessity in IFM fare transaction processes (i.e. outside bank transactions) for:
- Subscription / modification / resignation of applications or products when they include
- Billing facilities such as post-payment, automatic renewal of products or reloading of stored value
- Designation of an authorised user.
These transactions require the customer to register to one or more of the actors of the IFM.

All other fare transactions can be processed with object identifiers, whatever their nature: purchasing, validation, inspection, security checks.
Most Privacy issues therefore depend upon how the links from the objet identifiers to the personal identities of the subscriber and the authorised user are secured to be only accessible for legitimate needs.

Two different technical architectures are possible:

Direct database

Object Identities (OID) are directly linked to the Subscriber's personal identity (SID) or authorised user's personal identity (AUID) somewhere in a data base where correspondence from one to the other is directly given.

OID	**Object Identity**	Defined as above
SID	**Subscriber's IDentity**	PID of the subscriber
AUID	**Authorised User's Identity**	PID of the authorised user

Indirect database

No common data bases exist where an OID is encoded next to the Subscriber's Personal identity (SID) or The Authorised User's Personal Identity (AUID).

All transaction processes can be done with the pseudos.
Access to each individual pseudo is necessary to reach the PIDs.

Only the corresponding owner (medium / secure element / application or product) can do it.

LIDs	Links (or pseudos) from objects IDs to Personal IDs		
LMID	Medium Identity	←→	Medium Holder's PID
LSEID	Secure Element Identity	←→	Secure Element Holder's PID
LAID	Application Identity	←→	Subscriber's PID
LUID	Application Identity	←→	Authorised user's IDentity

3.3 Information security and privacy targets

Protection of the customer's privacy is a general requirement representing the protection targets of privacy, confidentiality, unlinkability, unobservability and anonymity.

Specific information security and privacy targets for the customer

Traveller's personal data protection known as privacy protection is dependent on information security which offers protection against intentional attacks.

Information security

Security target code and name		Description of security target
SCI1	Protection of personal data	The customer data stored in the system and/or customer me-dium is used to identify the customer, make payments, deliver entitlements, and so on. Misuse, manipulation or passing-on to unauthorised persons could incur commercial damage to the customer along with the loss of safety, and should be prevented.
SCI2	Protection of entitlements	Entitlements may be exposed to DoS attacks and manipulation by third parties. This would cause inconvenience and possibe damage to the customer. The damage would normally be limited, since usually the service can still be used provided the cus-tomer can prove that he purchased a valid entitlement. Manipu-lation of the entitlement by unauthorised persons should be pre-vented.
SCI3	Protection of usage data	Usage data is used to invoice the use of the "automatic fare calculation" product. This data must therefore be reliable.

SCI4	Reliable invoicing	When a service has been used, the customer must be able to see the time of activation and, in the case of check-in / check-out, the time, place and service provider.
		Calculation data (pricing) must be traceable and reliable.
SCI5	Protection of applications and entitlements	Customer media can accommodate more than one application, and these applications may belong to different application issuers. Furthermore, one application can hold multiple entitlements supplied by different product owners. It must be ensured that applications and entitlements are reliably separated from a technical point of view, or that agreements exist between the entities that regulate multiple usage and conflict resolution.

Protection of privacy

Security target code and name		Description of security target
SCP1	Protection of personal data	Personal data given to the product provider (CCP) must be treated confidentially, and only used for the agreed purposes.
SCP2	Protection of usage data	Non-anonymised, personal data about the use of a service may only be employed for the purposes of the product provider or service provider with the agreement of the customer.
SCP3	Protection against the creation of movement profiles	Third parties must be prevented from utilising RFID technology to generate personal movement profiles.

Specific information security and privacy targets for the product provider

The product provider's specific information security and privacy targets are listed in the following sections.

Information security

Security target code and name		Description of security target
SPI1	Protection of personal data	The customer data stored in the system and in the customer medium is used to identify the customer, make payments, deliver entitlements, and so on.
		Misuse, manipulation or passing-on to unauthorised persons could incur commercial damage to the product provider and a loss of customer acceptance, and could be punished as a viola-tion of the law. This must be avoided.
SPI2	Protection of entitlements	The manipulation of, damage to and in particular the counterfeiting of entitlements could incur considerable commercial damage to the product provider, product owner and service provider.
		Securing entitlements against counterfeiting is an important ob-jective for the product owner.
SPI3	Protection of usage data	The availability and integrity of usage data is of great value to the product provider, the product owner and the service pro-vider. This data is used for invoicing, planning products and ca-pacities, and increasing customer loyalty.
SPI4	Reliable invoicing	It must be ensured that earnings from the sale of entitlements by the product provider can be allocated correctly to the transport services provided by the service provider.
SPI5	Protection of applications and entitlements	Customer media can accommodate more than one application, and these applications may belong to different application issu-ers. Furthermore, one application can hold multiple entitlements supplied by different product owners. It must be ensured that applications and entitlements are reliably separated from a tech-nical point of view, or that agreements exist between the entities that regulate multiple usage and conflict resolution.

Protection of privacy

Security target code and name		Description of security target
SPP1	Protection of personal data	Misuse, manipulation or passing-on to unauthorised persons could incur commercial risks for the customer contract partner and result in a loss of customer acceptance, and could also be punished as a violation of the law.
SPP2	Protection of usage data	Non-anonymised, personal data about the use of a service may only be employed for the purposes of the product provider with the agreement of the customer. The aim for certain products (automatic fare calculation, CICO, etc) is to obtain this consent, so as, for example, to enable invoicing.
SPP4	Data minimiza-tion	Only the data required for the specified purpose should be gath-ered and stored, no more.

Specific information security and privacy targets for the service provider

The service provider's specific information security and privacy targets are listed in the following sections.

Information security

Security target code and name		Description of security target
SSI1	Protection of personal data	The customer data stored in the system and in the customer medium is used to identify the customer, make payments, de-liver entitlements, and so on.
		Misuse, manipulation or passing-on to unauthorised persons could incur commercial damage to the service provider and a loss of customer acceptance, and could be punished as a viola-tion of the law.
SSI2	Protection of entitlements	The manipulation of, damage to and in particular the counterfeit-ing of entitlements could incur considerable commercial damage to the product provider, product owner and service provider.
		Securing entitlements against counterfeiting is an important ob-jective for the service provider. Entitlements are also used in the service provider's system infrastructure, and they must be safe-guarded there as well.

SSI3	Protection of usage data	Usage data is of great value to the service provider. It is used for invoicing and for planning capacities.
		From the point of view of the customer and for legal reasons, customer-specific usage data must be treated confidentially by the service provider. Contravention of this would cause a loss of customer acceptance and could be punished as a violation of the law.
SSI4	Reliable invoicing	It must be ensured that earnings from the sale of entitlements by the product provider can be allocated correctly to the transport services provided by the service provider.
SSI5	Protection of applications and entitlements	Customer media can accommodate more than one application, and these applications may belong to different application issuers. Furthermore, one application can hold multiple entitlements supplied by different product owners. It must be ensured that applications and entitlements are reliably separated from a tech-nical point of view, or that agreements exist between the entities that regulate multiple usage and conflict resolution.

Protection of privacy

Security target code and name		Description of security target
SSP1	Protection of personal data	Misuse, manipulation or passing-on to unauthorised persons could incur commercial risks for the service provider and result in a loss of customer acceptance, and could also be punished as a violation of the law.
SSP2	Protection of usage data	Non-anonymised, personal data about the use of a service may only be employed for the purposes of the service provider with the agreement of the customer. The aim for certain products (automatic fare calculation, CICO, etc) is to obtain this consent, so as, for example, to enable invoicing.
SSP4	Data minimization	Only the data required for the specified purpose should be gath-ered and stored, no more.

Summary of the entities' information security and privacy targets

The following table sums up the aforementioned information security and privacy targets of the various entities involved. Role-specific security targets have been summarised to specific security targets associated to the generic security targets safety, information security and privacy. Used abbre-viations are:

- SS := specific security target regarding to the generic security target safety
- SI := specific security target regarding to the generic security target information security
- SP := specific security target regarding to the generic security target privacy

Security target		Customer targets	Product provider targets	Service provider targets
SI1	Protection of personal data	SCI1, SCP1	SPI1, SPP1	SSI1, SSP1
SI2	Protection of entitlements	SCI2	SPI2	SSI2
SI3	Protection of logistical data (ano-nymised usage data)	SPI3	SSI3	
SI4	Reliable invoicing	SCI3, SCI4, SCP2	SPI3, SPI4, SPP2	SSI3, SSI4, SSP2
SI5	Protection of applications and entitlements	SCI5	SPI5	SSI5
SP3	Protection against the creation of movement profiles	SCP3		
SP4	Data minimization	SPP4	SSP4	

Protection demand categories

Three protection demand categories are formed on the basis of the security targets described above. Category 1 represents the lowest protection demand, category 3 the highest.

The following table lists the criteria for allocating protection requirements to protection demand categories, these criteria being based on the assumption that no protective measures have been put in place.

Security target		Protection demand category	Criteria for allocating to protection demand category
SS1	Technical com-patibility	1	All of the system components come from the same supplier. The supplier ensures that they are compatible.
		2	The system has to function with components from a small number of defined suppliers. The system manager or a system integrator ensures compati-bility.
		3	Open system that has to function with components from any company in the market.
SS2	Fallback solution in the event of malfunction	1	Malfunction affects only a few customers.
		2	Malfunction affects many customers.
		3	Malfunction affects a large proportion of custom-ers.
SS3	Intuitive, fault-tolerant operation	1	A few customers cannot operate it intuitively.
		2	Many customers cannot operate it intuitively.
		3	A large proportion of customers cannot operate it intuitively.
SI1	Protection of personal data (including per-sonal usage data) – data become known to third parties	1	Customer's reputation is damaged.
		2	Customer's social existence is damaged.
		3	Customer's physical existence is damaged.
SI2	Protection of entitlements	1	Predicted product-related loss of sales through counterfeiting,

			damage or manipulation <0.5%.
		2	Predicted product-related loss of sales through counterfeiting, damage or manipulation <3%.
		3	Predicted product-related loss of sales through counterfeiting, damage or manipulation >3%.
SI3	Protection of logistical data (anonymised usage data) internal invoicing	1	Data becomes known to third parties.
		2	Data is lost.
		3	Data is falsified.
SI4	Reliable invoicing	1	Data is not available.
		2	Data is lost.
		3	Data is falsified, misused, etc.
SI5	Protection of applications and entitlements	1	Applications are issued by the same application issuer and entitlements by the same product owner.
		2	Applications are issued by a single application issuer but different application providers, and entitlements come from different product owners, product providers and service providers. Several companies collaborate and "trust" each other in the process.
		3	Applications are issued by different application providers, and entitlements by different product owners, product providers and service providers. Several companies collaborate but do not "trust" each other in the process.

SP3	Protection against the creation of movement profiles	1	Customer's reputation is damaged.
		2	Customer's social existence is damaged.
		3	Customer's physical existence is damaged.
SP4	Data minimization	1	Personal data, and data that can be linked to particular people, is not used.
		2	Personal data is used, but no usage data is collected.
		3	Personal data is used, as is usage and calculation data that can be related to particular people.

3.4 Code of conduct for e-ticketing privacy protection

Privacy respectful parties will apply the following charter and accept to be audited about them while applying for interoperability of fare management systems between European countries. Stakeholders and third parties will themselves be privavy respectful parties.

Anonymous accessibility

Under the responsibility of each entity (authority or operator) in charge of fare policies, travellers keep a possibility to access public transport anonymously and to benefit from all non-unipersonal concessionary or commercial fares anonymously (i.e. without any inscription in a data base)

Protection against risks of abusive use of personal data from applications in the media

Under the responsibility of the controller:
- Name and address are not be encoded in application in the media to prevent electronic indiscretion
- Name and photo can be printed on the media to make inspection possible.
- Number of historical records in the application are limited to the necessary number for operational needs of access management functions and inspection to limit private indiscretion.
- Authorised user's statutes and other useful data (such as birth date or preferred language) are only encoded in a common application to unlock access to special fares or services on the explicit demand of the subscriber.

Protection against risks of abusive use of personal data by staff

Under the responsibility of each processor:

- Each staff person is individually authorised to access data bases containing personal identification or object identification
- Personal identification or object identification modifications in data bases are traceable (date, responsible staff or process reference)
- Requests to personal identification data base are traceable.

Protection against risks of abusive usage of abnormal events

- Data about abnormal individual events (such as technical incidents or abnormal sequence of transactions) recorded on the media are protected so they are not readable by non-concerned stakeholders.
- Black listing will be restricted to the concerned product or application.

Protection against risk of abuse of direct marketing tools

Under the responsibility of the controller:
- Independent processes are organised to answer different business needs:

<u>Anti-fraud processes</u>
They are dedicated to analyse transactions in linkage with objecti identification to detect any possible fraud of the system.
They will be processed within a limited period of time.
After this period is expired, only suspicious transactions are kept

<u>Personal commercial processes</u>
Personalised transport transactions (where & when) are only stored the necessary time to fully complete the contractual commercial process (e.g. until post-payment, expiry of the re-imbursement delay or guaranteed period of prepaid product re-issuance as defined by the applicable fare).
After this period is expired, transport transactions (where and when) are simplified to make any tracing of traveller's mobility impossible.
Timing of transactions in commercial database are never be inferior to one week.

<u>Global Marketing processes and network monitoring:</u>
Databases are anonymous and include no personal identification or object identification
If needed for global anonymous marketing surveys, object identifications in transaction data are therefore replaced by a non reversible hashed identification.
Personal identifications are replaced by statutes for the need of segmented surveys.

Protection against risks of hacking and criminal use of personal data in back-offices

Under the responsibility of each processor:
- Appropriate technical means protect personal data against any attempt of intrusion.

Protection against risks of uncontrolled dissemination of identity data

Under the responsibility of the controller:
- Personal identity,bank identifier as well as all individual data are only transmitted [and/or made accessible] from one stakeholder to another one to fulfil

interoperable processes such as replacement of guaranteed products or in case of shared responsibility such as common products.

- Any other transmission [or access] is submitted to an explicit approval of the customer.
- If different stakeholders share common commercial data bases, they do not contain :
    - Identifiers (personal identities) or bank identifiers unless the customer has been informed of the stakeholders who can access his/her data.
    - Authorised user's statutes and object identifiers.
    - Direct use of personal data.
- Links or pseudos are used to protect easy access to personal identifications.

Multi-application management

Under the responsibility of the privacy manager:
- Loading agents must be privacy respectful
- Complete independence of applications is maintained with partners who don't apply a compatible privacy charter.

3.5 Safeguards

These safeguards are defined in such a way that, when built successively upon each other, they afford increasing levels of security – in cases where different levels are possible. Level 1 represents the lowest security category, level 3 the highest.

The following safeguards are generally not defined as isolated measures, but rather are to be understood as "safeguard packages". As a rule, the security of components and interfaces, and of the system as a whole, can only be increased in a meaningful way if safeguards are employed across the board as packages. Furthermore, alternative possibilities are defined within the security levels; for instance, a secure environment (which generally does not exist) can replace the encrypted storage of data.

Safeguards for the protection of the system as a whole

The following safeguards relate to the system as a whole, the focus being on the sales, inspection and management systems, including the associated interfaces.

Separate sections will deal with the RF interface; readers installed in terminals, vending machines and so on; carrier media; and the key management system.

Protection of the system as a whole through separation of applications

	Code and name of safeguard	
	Identifying the customer when selling and handing over products	
General	The identity of the customer must be established when setting up a customer account, ordering and collecting personalised products, and blocking.	
1	Declaration by customer: • The customer submits the details of his or her identity verbally or on the Internet.	

2	Application form, customer cards:
	
	        • The customer declares himself in writing and signs to confirm his identity. The product provider checks the information using conventional means:
	        • Address check.
	        • Sending the customer medium to the address given.
	        • Identity data is passed into the system (Internet, vending machine) from an existing secure customer medium.	

3	Identity document check when setting up a customer account and handing over entitlements
	
	        • Secure identification with photograph is presented.
	        • The identity data is taken into the system from a secure electronic identity card (eID)	

Protection of the system as a whole through identifying the customer

	Code and name of safeguard	
	Satisfying the data minimization obligation	
General	Data minimization must be satisfied in accordance with the applicable legal regulations on privacy.	
1	Satisfying legal requirements: • When the processes and system as a whole are being defined, the principle of data minimization is applied in accordance with the legal foundations. This requires in particular the definition of deadlines for deletion of data that isn't needed any more.	
2	Special safeguards In addition, the following measures will be deployed: • Precise, purpose-related definition of data content; data and access/usage rights are acquired and stored using the role model of the system as a whole. • The customer is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people.	

Protection of personal data on the transponder

	Code and name of safeguard	
	Protection of settlement data against retrieval and overwriting/manipulation	
General	Settlement data is generated using personal usage data, and is used to invoice the services of the service provider. In the case of products with automatic fare calculation, the settlement data is also used to invoice the customer. In the case of simpler products, the validation information about the entitlement stored in the carrier medium can also be treated as the invoicing date. Settlement data is stored in the carrier medium and the terminal when beginning a journey or when checking in or out. If interoperability is required, then settlement data must also be protected against internal attacks.	

1	Protection of settlement data: • Write protection or access protection • Data is transmitted in encrypted form and stored in the chip • Settlement data and entitlements are protected using various keys • Diversification of keys.
2	Specific access and manipulation protection: • Access protection • Data is transmitted in secured form and stored in the chip specifically for the application. • Settlement data and entitlements are protected using various keys. • The data may need to be protected against manipulation on the system side (e.g. using MAC) • Diversification of keys.
3	Access and manipulation protection in the case of interoperability: • Access protection. • Data is transmitted in secured form and stored in the chip specifically for the application. The various types of settlement data are protected in accordance with a defined role model using defined access rights and specific, varying keys. • If interoperability is required in the system, then settlement data must be protected against manipulation on the system side (e.g. using MAC, signa-tures). • Diversification of keys.

3.6 Links with the EU-IFM scheme

In agreement with the 7 migration steps of EU-IFM developed to get a full interoperable fare management in Europe and in agreement with the common IFM System Architecture described in the standard ISO EN 24014-1 (Fig 1) which is also the basis for the EU-IFM Organisation Model, cooperative Organisational Models (OMs) for the European IFM area are proposed in deliverable 4.3. Essential for the establishment of interoperability is to use the same customer medium in all EFM systems and guarantee the security, which is required for the connected systems. Necessary organisational units and related rules and procedures of the cooperative OMs are also identified. Privacy regulations are part of this global approach.
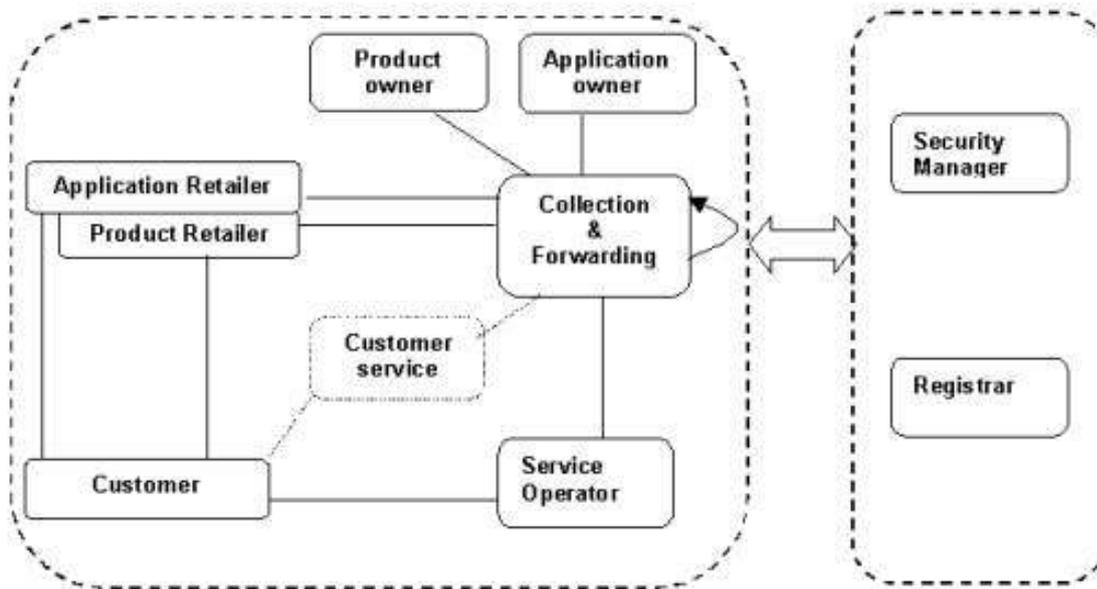
Figure 1 — The two IFM organisational domains (operational and management Entities)[1]

Among IFM roles model of the ISO/EN Standard, EU-Security Manager:
- Specifies security requirements that apply to accepted media for all PT applications and the Secure Elements used for the download process
- Certifies the SE and provides means of authentication as well as enforces legal requirements related to privacy.

Moreover functional requirements on the media are also enforcing privacy rules as expressed in D3.2"Common requirements and recommendations on interoperable media and multi-application management":
- Customer media ensures an absolute data isolation between applications to guarantee application code & data privacy,
- GlobalPlatform secure messaging provide confidential loading for application code and confidential application personalisation ensuring data privacy for the Application Owner and Application retailer with the actors involved in the operational process (Media/SE Owner, Media/SE loader, Controlling Authority…).

In this perspective, the SE Loader may play a key role to enforce privacy rules. Being considered as a Trusted 3rd party by Application Retailers, SE loader can receive and encrypt the customer personal data that need to be stored onto the ticketing application during the installation and personalisation process. Once encrypted, the data can be routed securely through a 3G/GSM network (OTA) or internet connections (OTI) till the Customer Media.
Such a SE Loader role can be played by a 3rd party offering such web privacy service and providing a unique entry point for personal data handling operations to all the Application

---

[1]   Source: ISO/EN 24014-1:2005

Retailers. Such a role can be part of TSM (Trusted Services Manager) role as described in the next scheme.
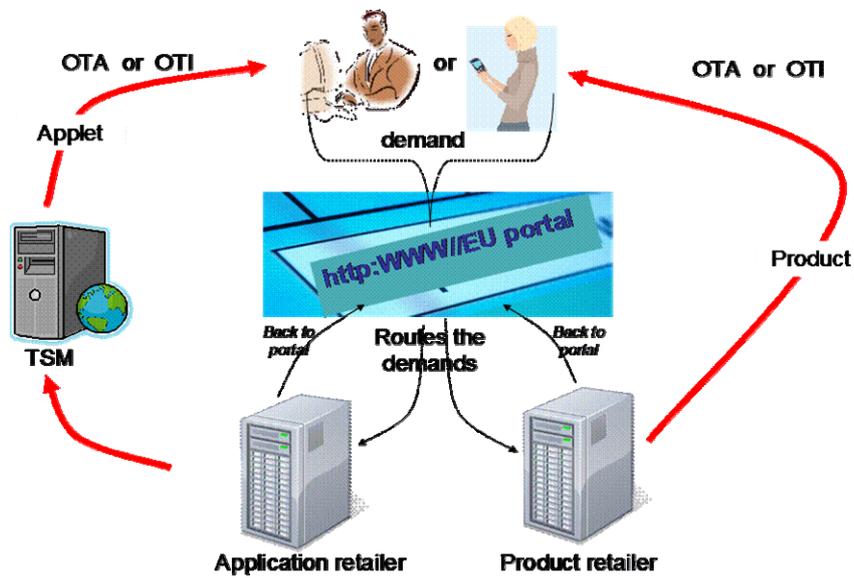
As part of the legal framework designed for EU-IFM partners, legal requirements concerning privacy are to be included.

Annex I

TG 03126 - Technical Guidelines for the Secure Use of RFID

TG 03126-1 Application area "eTicketing in public transport"

TG 03126-1: Application area "eTicketing in public transport"
Authors:

Cord Bartels, NXP
Harald Kelter, BSI
Rainer Oberweis, BSI
Birger Rosenberg, NXP

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn, Germany
Tel.: +49 (0) 228 99 9582 0
E-mail: rfid@bsi.bund.de
Website: https://www.bsi.bund.de

Contents

List of Tables

List of Illustrations