ITSO

DOCUMENT DELIVERY NOTE

Issuing Authority:	**Owner:**	**Project Editor:**
ITSO	Technology at ITSO	ITSO Head of Technology
Document number	**Part Number:**	**Sub-Part Number**
ITSO TS 1000	0	
Issue number (stage):	**Month:**	**Year**
2.1.4	February	2010
Title:		
ITSO TS1000-0 *Interoperable public transport ticketing using contactless smart customer media – Part 0: Concept and context*		
Replaces Documents:		
ITSO TS1000-0 2008-04 issue number 2.1.3		

Revision history of current edition

Date	ITSO Ref.	Editor ID	Nature of Change to this Document (or Part)
Nov 2002	DCI 100 / Create	SLB	Create first working document WD ITSO TS 1000-0:2003-11
Mar 2003		SLB	Issue updated (2nd) working document.
Dec 2003		SLB	Assemble Authors' synopses to create 1st Committee Draft.
Jan 2004	N0407 & N0431	SLB	Insert clause on Security Architecture (doc # ITSO TC N0437)
Feb 2004		SLB	Incorporate items arising from updated DRC-P0 20040210. Create 3rd CD.
Feb 2004		SLB	Clean up and format as final draft.
Mar 2004		SLB	Implement final changes and prepare for issue.
Oct 2006		MPJE	Updated to include ISADs following approval by DfT
Jun 2007		MPJE	Updated for V2.1.2 publication – no changes to this part
Mar 2008		CJS	Updated to include ISADs following approval by DfT
Apr 2008		MPJE	Final Editing prior to publication
Feb 2010		MPJE	Final Editing prior to publication of Version 2.1.4
Apr 2015		MPJE	Updated to incorporate Corrigendum 9 to Version 2.1.4

Document Reference: ITSO TS 1000-0

Date: 2010-02-22

Version: 2.1.4

Ownership: ITSO

Secretariat: Technology at ITSO

Project Editor: Mike Eastham

ITSO Technical Specification 1000-0 – Interoperable public transport ticketing using contactless smart customer media – Part 0: Concept and context

ISBN: 978-0-9548042-4-4

COR 9

Foreword

This document is a part of ITSO TS 1000, a Specification published and maintained by ITSO, a membership company limited by guarantee without shareholders. The membership of ITSO comprises transport organisations, equipment and system suppliers, local and national government. For the current list of members see the ITSO web site www.itso.org.uk

ITSO TS 1000 is the result of extensive consultation between transport providers, sponsors, system suppliers and manufacturers. The Department for Transport (DfT) has also contributed funding and expertise to the process.

Its purpose is to provide a platform and tool-box for the implementation of interoperable contactless smart customer media public transport ticketing and related services in the UK in a manner which offers end to end loss-less data transmission and security. It has been kept as open as possible within the constraints of evolving national, European and International standards in order to maximise competition in the supply of systems and components to the commercial benefit of the industry as a whole. In general, it promotes open standards but it does not disallow proprietary solutions where they are offered on reasonable, non-discriminatory, terms and contribute towards the ultimate objective of interoperability.

ITSO has been established to maintain the technical specification and business rules required to facilitate interoperability. It also accredits participants and interoperable equipment. ITSO is a facilitator of interoperability at the minimum level of involvement necessary. It will not involve itself in any commercial decisions or arrangements for particular ticketing schemes; neither will it set them up nor run them. It will however “register” them in order to provide the necessary interoperability services (e.g. issue and control of unique scheme identifiers, certification and accreditation, security oversight).

Consequently, adoption of this Specification for particular ticket schemes will be a matter for the commercial judgement of the sponsors/participants, as will the detailed business rules and precise partnership arrangements.

Contents

1. Scope

ITSO TS 1000 defines the key technical items and interfaces that are required to deliver interoperability. To this end, the end-to-end security system and shell layout are defined in detail; while other elements (e.g. terminals, back-office databases) are described only in terms of their interfaces. The business rules that supplement the technical requirements are defined elsewhere.

1.1 Scope of Part 0

ITSO TS 1000-0 is an informative editorial compilation of synopses provided by the Authors of ITSO TS 1000. It provides a descriptive overview of those normative Parts of the Specification.

2. Customer Media (CM)

The term Customer Media (abbreviated to CM) refers to the electronic platform that is used by passengers to store the ITSO Ticketing Products. Currently most schemes use a smartcard platform as the CM, but this may change in the future - hence the use of the more generic term.

To be compliant with the requirements given in ITSO TS 1000, a CM must support a contactless power and data interface that complies with the relevant parts of ISO/IEC 14443. Other data interfaces may be present on the CM, but are not covered by the scope of ITSO TS 1000.

The CM-to-POST interface is a critical one for interoperability, and ITSO TS 1000 defines the following key attributes of this:

— physical;

— power transfer mechanisms;

— data transfer mechanisms;

— data layout;

— data access and security;

— benchmark transaction times.

These are defined for a number of platforms. Each supported platform type has a Customer Media Definition (CMD) in ITSO TS 1000-10. This CMD covers all defined attributes of the platform, including physical form factor and data layout.

It is highly likely that platforms with differing physical form factors will use the same electronic device and hence have the same data layout. This is catered for by the use of the Format Version Code (FVC), which is stored electronically as part of the ITSO data on the media. POSTs can read this data element and determine the appropriate data processing rules required.

If a platform type is not defined in ITSO TS 1000-10 then it is not supported, cannot be ITSO certified and cannot be used within the ITSO Environment.

One of the most important functions of the CMD is to map the logical ITSO data structures onto the physical electronic storage provided by the media. In some cases this mapping will be to physical bit and byte level (e.g. on a memory card) whereas, in other cases, it will be to logical storage elements provided by the media (e.g. on a processor-based platform with an operating and file storage system).

The CMD will also define or reference the commands required to access the data on the media. ISO/IEC 14443 allows for the use of proprietary commands under certain circumstances and POSTs must be capable of supporting such commands for platforms that make use of them.

Two main classes of media are defined in ITSO TS 1000-10:

— media platforms that carry a Full ITSO Shell;

— media platforms that carry a Compact ITSO Shell.

Platforms that carry a Full ITSO Shell may host a number of ITSO Ticketing Products concurrently, and are required to host a Cyclic Log into which Transient Tickets may be placed.

Platforms with restricted memory use a Compact ITSO Shell, which can only host a single ITSO Ticketing Product at any one time. The Compact ITSO Shell is not capable of hosting a Cyclic Log and has a number of other restrictions, which are fully defined in ITSO TS 1000-10.

Security of data on the CM is critical to successful operation of ITSO Schemes. A number of mechanisms are used to ensure media data security, some of the main ones being:

— use of Anti-tear mechanisms to protect the integrity of the data in situations where the media is removed from the POST's RF field before all the required data is written;

— use of ISAM generated Seals to ensure the authenticity of data;

— use of media access Keys to control write access to the CM and hence protect the integrity of the data;

— use of a fixed number that is unique to the CM to make keys and Seals media instance specific;

In general, all ITSO media can be read without the need for Security Sub-Systems or ISAMs.

The time it takes to carry out a transaction is usually important for a number of reasons. The most obvious is passenger throughput. Long transaction times have been shown in trials to increase the risk of CM being prematurely removed before data update is complete. Because of the impact transaction time has on system operation and reliability ITSO TS 1000-10 defines, for each CMD, a benchmark transaction together with maximum time that is allowed to carry out this transaction.

3. The Customer Media (CM) architecture

The ITSO Customer Media architecture is designed to allow many different ITSO Product Entities to be carried on many different types of Customer Media and be used on all POSTs in an ITSO environment.

3.1 Customer Media and ITSO Shells

The term Customer Media (abbreviated to CM) is used in preference to the term "card" in order to embrace the future use of devices such as mobile phones and PDAs that may be carried by consumers desiring to use an ITSO scheme.

The ITSO architecture supports the logical separation of Products from the media that carries the ITSO Application. Thus in the context of smart cards ITSO adds an additional third layer, namely Products, to the traditional two layer model of card plus Application. This is illustrated in Figure 1.

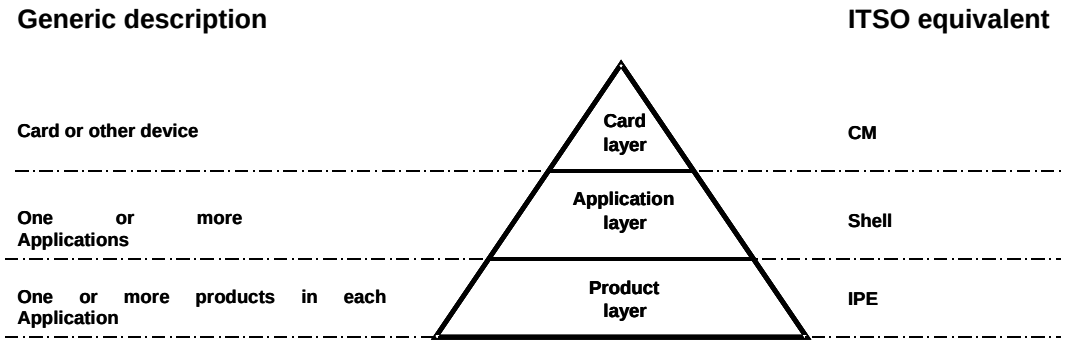

Figure 1 - The ITSO three layer model

This means that an ITSO Application[1] (ITSO Shell) can support multiple Products or an ITSO Product can stand alone in someone else's Application. Furthermore, a CM platform may be dedicated to the ITSO Shell, or the ITSO Shell may be added as the "ITSO Application" alongside others on a multi-application CM platform.

This flexibility maximises the number of ways by which interoperability can be achieved.

ITSO TS 1000-2 specifies the overall architecture of every CM, whilst the different varieties of CM supported are specified per section in ITSO TS 1000-10.

Every ITSO-certified POST supports, at least, the ISO/IEC 14443 proximity card interface plus the ability to interpret the Mifare Classic™ interface. All ITSO CM may be used on any ITSO POST certified to do so by ITSO.

ITSO members have the ability to choose from a wide range of suitable media upon which to deliver their Products. This ranges from types of Customer Media capable of holding only a compact ITSO Shell and a single Product to CM capable of holding a full ITSO Shell and a multiplicity of Products, as illustrated in Figure 2.

[1] Renamed a Shell by ITSO to avoid confusion with the traditional model

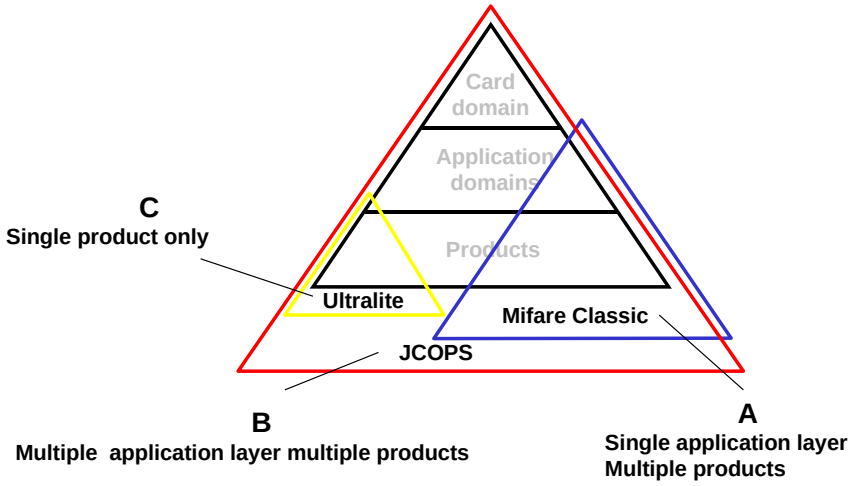

Figure 2 - Multiple CM choices

3.2 Data Groups

All data held in an ITSO Shell is grouped together in Data Groups. The various Data Groups hold:

— data describing the ITSO Shell and the CM upon which the ITSO Shell resides.

— data describing the Directory and its contents.

— the fixed and variable parts of an ITSO Product Entity (IPE).

— the Cyclic Log.

The Directory and IPE Data Groups are sealed such that their authenticity can be verified and related to the type of CM the Product is on. The generic structure of a Data Group is shown in Figure 3.

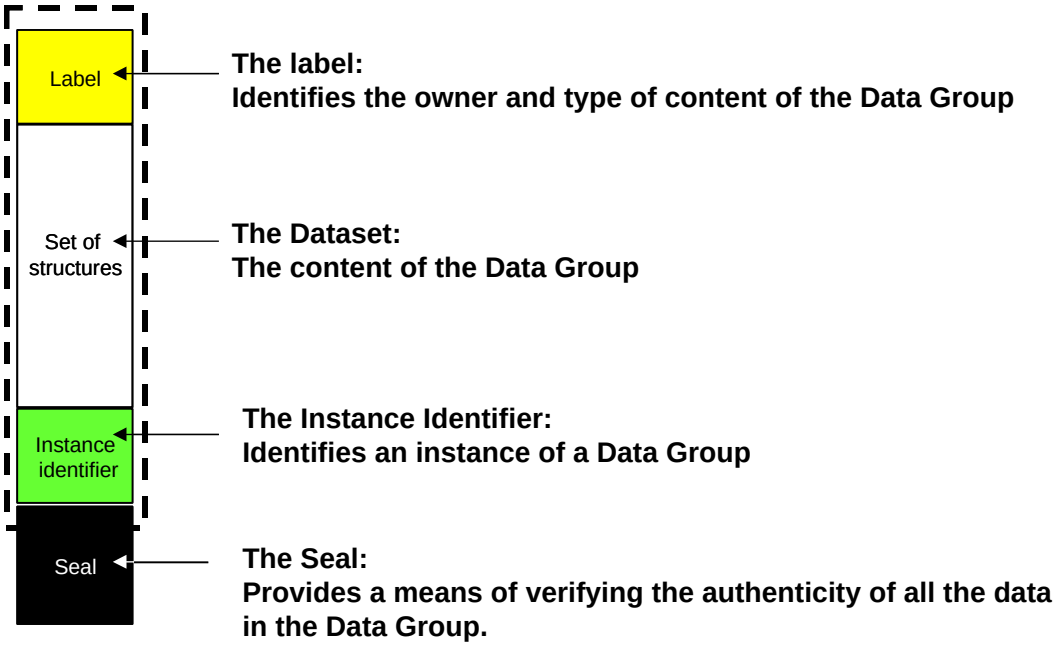

Figure 3 - Data Groups

3.3 Products on Shells

An ITSO Shell can hold a number of Products. Each Product carries a Label that describes the Product Owner, the type and subtype of Product and its expiry date. Labels are listed in a Directory, which also carries an array of Logical Sector information that is interpreted by the POST Application to find out where the Products are actually stored in the CM.

The POST Application uses the Directory to determine which, if any, of the Products in the Shell are accepted at that POST. For some simple Applications using the Directory information alone may be sufficient to perform a transaction, in which case the transaction times can be minimised.

The ITSO Shell, Directory and IPEs are located on the CM in accordance with the definitions found in ITSO TS 1000-10.

All Products and the Directory carry Seals, which provides a means by which the POST Application can verify their authenticity. The Seals are also bound to the CM by cryptographic methods. The relationship between Labels, Products and the Directory is illustrated in Figure 4.

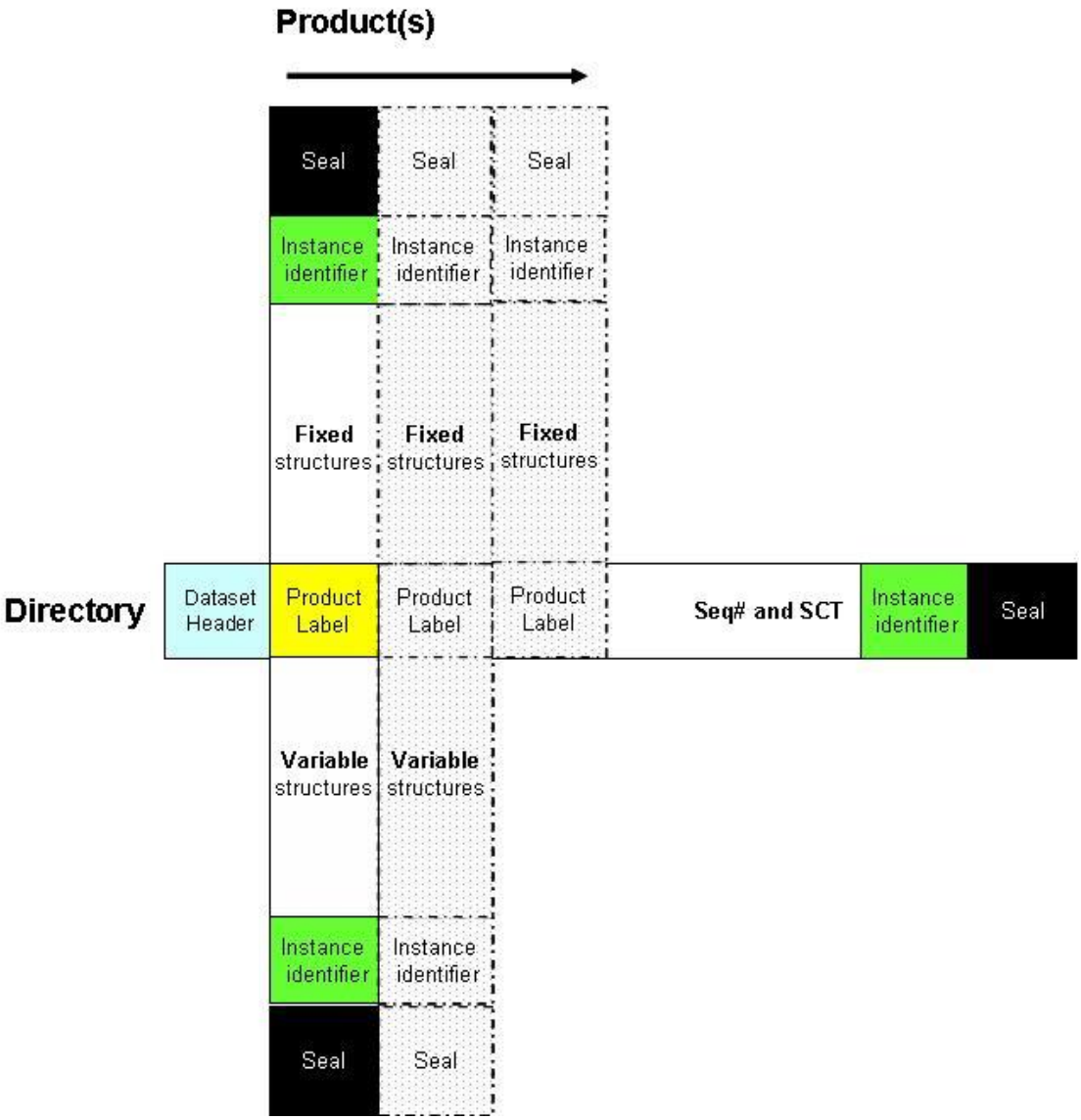

Figure 4 - Make up of the Directory and its relation to Products

3.4 Logs

The Shell supports two forms of log record, the Basic Log and the Normal Log.

The Basic Log is merely an entry in the Directory that can be used to store pass-back times and basic entry / exit details suitable for some Check-in/Check-out systems.

The Normal Log is a Cyclic Log, which can hold much larger records suitable for holding event and or transient ticket information. A special form of entry in the Directory identifies the most current record in the log.

The cyclic nature of the log ensures that if new records are torn they do not affect earlier records.

The content of the Transient Ticket Records intended for storage in the normal log are defined in ITSO TS 1000-5 and each record is encapsulated in Orphan IPE Data Groups as defined in ITSO TS 1000-2. The Orphan IPE Data Groups add a unique identity and a Seal to the records. Records Sealed in this way can be used as tickets and may be authenticated by any ITSO POST.

The Cyclic Log and the use of Orphan IPE Data Groups are illustrated in Figure 5.

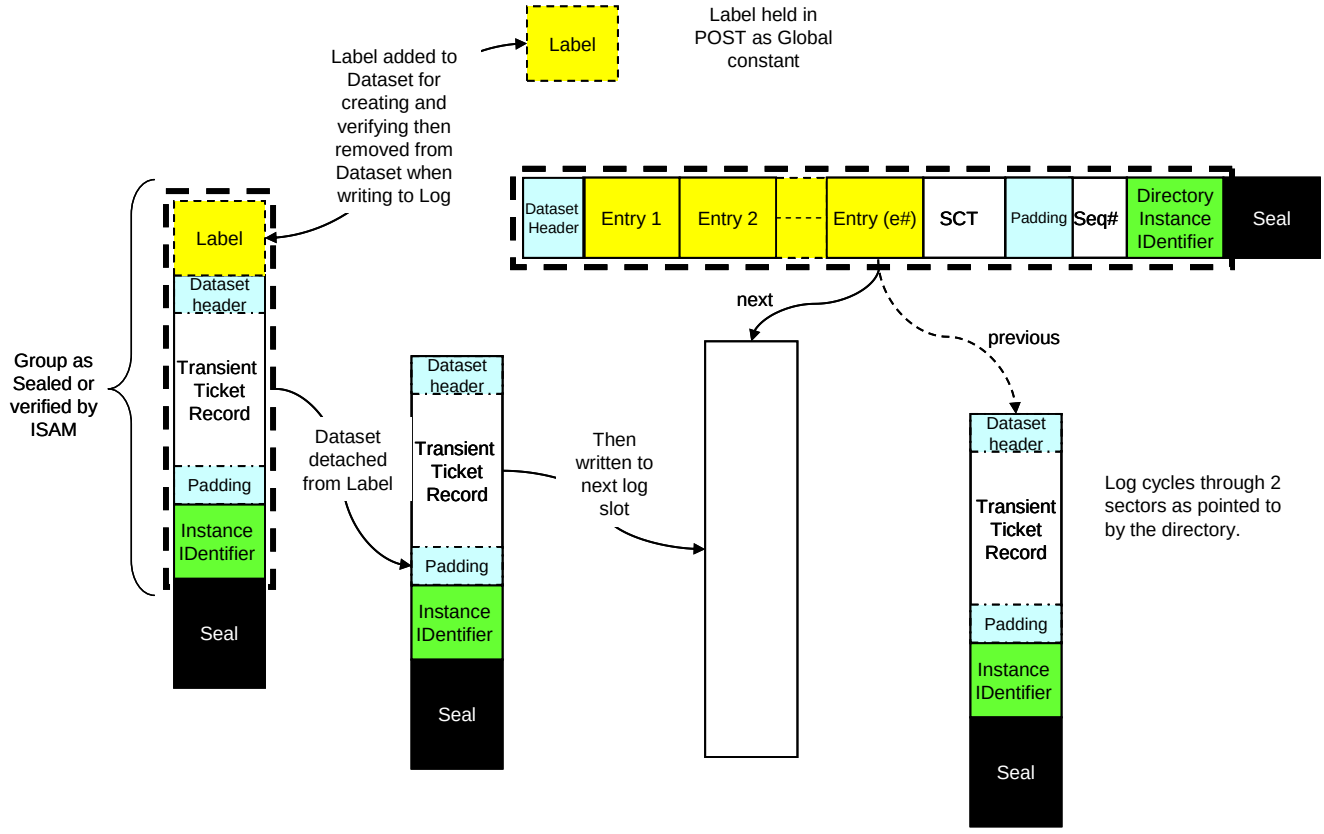

Figure 5 - The Cyclic log and Orphan IPE

3.5 Anti-tear

Where variable information is written to the CM whilst the CM is in motion the process will occasionally fail to write correctly. ITSO specifies that, in this event, it shall be possible to continue using the Media unimpeded. ITSO TS 1000 accommodates various CM-dependent Anti-tear methods that are defined in ITSO TS 1000-10.

CM that support hardware Anti-tear systems that are transparent to the Application are accepted alongside those that require the use of Application software based solutions. Two different methods of software based Anti-tear are specified relating to the capacity of the CM. These are:

— for CM where memory space is limited a method is used that duplicates storage of the current values only.

— for CM with more space available then a method is specified that makes efficient use of a duplicate copy that automatically logs the last few transactions while correct operation is maintained.

In both cases and especially where multiple Value Record Data Groups are altered in the same Customer Media session the Directory Data Group is the last Data Group to be modified.

After updating the Directory the Logical Sector information will point to the latest version of every altered Value Record Data Group. If the Directory update fails then it will point to all the previous versions of the Value Record Groups as if nothing had happened.

4. Product Data Elements stored within the ITSO Shell

Product data elements are defined in ITSO TS 1000-5.

Two classes of data are defined:

— ITSO Product Entities (IPEs);

— Transient Ticket records.

IPEs are used to store Products, such as tickets, concessionary entitlement, Stored Travel Rights (STR), or vouchers for example. An IPE would be used where Products are sold in advance of travel, or where the Product must be maintained for a period of time. Typical examples include rail tickets and season tickets. IPEs are described in more detail below.

Transient Ticket records are used where a ticket is sold at the point of travel, and need not be stored beyond the end of the journey. A typical example of this would be use of concessionary entitlement or Stored Travel Rights to purchase a bus ticket. The use of Transient Tickets is described in more detail below.

4.1 ITSO Product Entities (IPEs).

There are a number of different types of IPEs defined; each type is denoted by a TYP number.

The IPEs currently defined are outlined in Table 1.

Table 1 - IPE types

TYP code	IPE Title	Typical Uses
0	Private entity within the ITSO Directory as defined in ITSO TS 1000-2	Used to store non-interoperable Products[2], and to reserve areas of CM memory for other uses.
1	RFU	Reserved for future use by ITSO.
2	Stored Travel Rights (STR)	A store of travel rights which may be used to procure travel. Action list update and automatic renewal options are provided. Action lists enable the back office to update the Product when the CM is presented to a POST. Automatic renewal enables the POST to automatically update the Product when it is presented to a POST, but the store of travel rights is found to be insufficient for the proposed journey or to have fallen to a threshold value. Following automatic renewal a message is sent to the back office triggering a payment collection event.
3	Loyalty type 1 (Customer media Based)	A loyalty Product where the loyalty points are stored in the Product.
4	Charge to Account (CTA) mode 1 (restriction on value spent)	A post-pay Product which may be used to procure travel. Risk is limited by restricting the total amount which may be spent before payment is collected from the Customer.

[2] ITSO do not encourage the use of private entities. Where a Product has potential for interoperability, then the use of an ITSO defined IPE is preferred, as a basis for future interoperability.

TYP code	IPE Title	Typical Uses
5	Charge to Account (CTA) mode 2 (restriction on quantity of transactions per charge period)	A post-pay Product which may be used to procure travel. Risk is limited by restricting the quantity of transactions which may be conducted in a charge period (typically one week), and by limiting the maximum value of each transaction.
6 – 13	RFU	Reserved for future use by ITSO.
14	Entitlement	A Product which is used to store a Customer's entitlement to a service or privilege, for example, an entitlement to concessionary travel.
15	RFU	Reserved for Future Use by ITSO.
16	ITSO ID & entitlement	A multi purpose Product which may be used to store: Identity information relating to the Customer; A Customer's entitlement to a service or privilege, for example, an entitlement to concessionary travel; Information relating to a deposit paid for the ITSO Shell.
17	Loyalty type 2 (Centrally Accounted)	A Loyalty Product where the points are only stored in a back office, not in the Product.
18 - 21	RFU	Reserved for Future Use by ITSO.
22	Pre-Defined Ticket (Area based) with days selection, Action List amendment and Auto-renew capability options	Area based Period pass or season ticket Products. Features a Stored Ticket capability, with Stored Tickets being activated upon demand. This feature accommodates days selection Products, for example, 7 one-day period passes purchased, with each pass activated upon first use on a given day. The Product may be modified by means of action lists and automatic renewal. Action Lists enable the back office to update the Product when it is presented at a POST. Automatic renewal enables the Product to be updated, for example renewed by extending validity, when it is presented to a POST but the Product is found to be expired. Following Auto-renew a message would be sent to the Back Office triggering a payment collection cycle.
23	Pre-Defined Specific Journey Ticket with Multi-ride, Auto-renew and Action List amendment capability options	Specific journey tickets may be used for single, return or period tickets. Features a Stored journey ticket capability, with stored journeys being activated upon demand. This feature accommodates Multi-ride tickets. The Product may be modified by means of action lists and automatic renewal. Action Lists enable the back office to update the Product when it is presented at a POST. Automatic renewal enables the Product to be updated, for example renewed by extending validity, when it is presented to a POST but the Product is found to be expired. Following Auto-renew, a message would be sent to the back office triggering a payment collection cycle.

TYP code	IPE Title	Typical Uses
24	Pre-Defined Specific Journey Ticket including reservations and special restrictions with action list amendment and auto-renew capability options	Specific Journey Tickets may be used for single, return or period tickets. Provides for reservations and special restriction options. Features a Stored Journey ticket capability, with Stored Journeys being activated upon demand. This feature accommodates Multi-ride tickets. The Product may be modified by means of action lists and automatic renewal. Action Lists enable the Back Office to update the Product when it is presented at a POST. Auto-renew enables the Product to be updated, for example renewed by extending validity, when it is presented to a POST but the Product is found to be expired. Following auto-renew a message would be sent to the back office triggering a payment collection cycle.
25	Travel Related Voucher with multi-use, action list amendment and auto-renew capability options	This Product may be used to store vouchers, which for example may be used to grant access to events or to services such as free refreshments. It is anticipated that the use of such vouchers will be linked in some way to travel. Features a Stored Voucher capability, with Stored Vouchers being activated upon demand. The Product may be modified by means of Action Lists and Auto-renew. Action Lists enable the Back Office to update the Product when it is presented at a POST. Auto-renew enables the Product to be updated, for example renewed by extending the number of uses available, when it is presented to a POST but the Product is found to be expired. Following Auto-renew a message would be sent to the Back Office triggering a payment collection cycle.
26	Open system tolling with multi-use, action list amendment and auto-renew capability options	A season Product suitable for use in road or crossing tolling systems where a flat rate toll charge is paid. Features a Stored use capability, with stored uses being activated upon demand. The Product may be modified by means of Action Lists and Auto-renew. Action Lists enable the Back Office to update the Product when it is presented at a POST. Auto-renew enables the Product to be updated, for example renewed by extending validity, when it is presented to a POST but the Product is found to be expired. Following Auto-renew a message would be sent to the Back Office triggering a payment collection cycle.
27	Period Pass (space saving)	Period pass or season ticket Products. May be used in CM where memory space is limited, for example small memory or disposable Smartcards or for example within multi-function Smartcards where again memory space is limited.
28	Carnet (space saving)	Carnet. May be used in CM where memory space is limited, for example small memory or disposable Smartcards or for example within multi-function Smartcards where again memory space is limited.
29	Multi Journey or Multi leg, Ticket (space saving)	Multi Journey tickets. May be used in CM where memory space is limited, for example small memory or disposable Smartcards or for example within multi-function Smartcards where again memory space is limited.

TYP code	IPE Title	Typical Uses
30 – 31	RFU	Reserved for Future Use by ITSO.
32	ITSO shell environment group	The ITSO Shell data
33	ITSO Directory group	The ITSO Directory
34	ITSO transient ticket group	The ITSO Transient Ticket data
35 and above	RFU	Reserved for Future Use by ITSO.

Note that for IPE groups with TYP numbers greater than 31, the TYP value shall not be used in Directory entries.

4.1.1 IPE definitions, embodiments, instances and identification.

IPEs are identified as shown in Table 2.

Table 2 – IPE identification

Category	Description	Identified by[3]:
IPE Definition	The definition of an IPE type within the ITSO specification	TYP
IPE Embodiment	The instructions necessary to create an IPE Product Instance (a Product Definition)	Product owner IIN +[4] Product owner OID + TYP + PTYP (value is defined by the Product Owner)
IPE Instance	An actual instance of an IPE loaded into an ITSO Shell contained within a Customer Media (a Product Instance)	Product owner IIN + Product owner OID + TYP + PTYP + Creating ISAM ID + Creating ISAM Seq#

4.2 Transient Ticket records.

Transient Ticket records are used to store temporary tickets and records of other specified events:

— tickets sold when an IPE is not created:

for example, when a concessionary ticket is “sold” on the basis of a concessionary entitlement contained within the shell, a record is added to the transient ticket log to record the event;

— Closed System entry records:

a Closed System is one where the user presents their CM both on entry and exit from the system;

— multi-leg journey records:

[3] In all cases the identification string shall be unique to the entity identified.

[4] In this context, the ‘+’ symbol signifies concatenation.

cumulative fare and count of journey legs may be stored, enabling a fare cap to be implemented for a multi-leg journey[5];

— records of STR added.

Two Transient Ticket records may be stored.

[5] Certain Products also incorporate these data elements. Where this is the case, a transient ticket record shall not be created, but the Product based data elements used.

5. Point of Service Terminal (POST)

Within the ITSO environment, a Point of Service Terminal (POST) is defined as one class of instantiations of equipment that allows transactions to be carried out with data entities held on the CM.

Within the ITSO environment, the following actors are typically POST users:

— Product Retailers (Sale & loading of IPE instances into an ITSO Shell);

— Service Operators (Validation and usage of IPE instances);

— Customer (In unattended transactions);

— Shell Retailers (Sale and loading of an ITSO Shell on to the media).

POSTs provide the access mechanism to the media platform to support the ITSO aim of permitting the interoperable use of a variety of ticketing Products, retailed and used on a variety of platforms, from different issuers, on behalf of multiple Product owners.

The range of equipment covered by the term POST is wide and diverse. However, all POSTs have the following key attributes:

— they are able to read and write data to contactless media that comply with the ITSO Specification;

— they periodically exchange data with a HOPS system;

— they contain an ISAM, which is unique to the POST and is not shared by other POSTs.

ITSO TS 1000-3 only defines those requirements that are pertinent to interoperable CM usage and interfacing to other parts of the ITSO environment. These requirements are to be applied as an interoperability layer over the underlying specification of a ticketing terminal. Consequently, the certification of a POST as ITSO Compliant relates only to this overlay and implies nothing in regard to its compliance or otherwise to the underlying ticketing terminal specification.

All compliant POSTs support the entire set of CM platforms defined in ITSO TS 1000-10 and use the appropriate Anti-tear mechanisms for each platform type. It is strongly recommended that POSTs use a software architecture that allows further CM platforms to be added by means of configuration parameters.

All POSTs are capable of parsing and processing all the ITSO data entities defined in ITSO TS 1000-2. Each type of POST supports the set of IPEs that are appropriate to its use within an interoperable environment. Appropriate IPE sets are defined in the ITSO business rules.

Every instance of a POST operating within the ITSO environment has an ISAM fitted. Physical access to the ISAM is restricted to the extent that some form of tool is required but no tamper-proof or warranty seals need be violated.

ITSO specifies certain characteristics of the POST's human interface in order to ensure that there is a consistent and reassuring core of user experience across the range of ITSO-enabled POSTs that a customer may encounter. These ITSO-specific characteristics form only a part of the overall human interface of the equipment and are used as a supplement to the underlying terminal specification.

To provide the required level of interoperability, ITSO TS 1000-3 specifies the functional requirements for the POST that relate to:

— Media handling:

- Detection and validation of the ITSO Shell;
- Validation of the Directory;
- Selection of Products;
- Handling of Anti-tear;

- Media re-presentation;
- Transaction time;

— IPE handling:

- General IPE instance processing;
- IPE instance creation;
- IPE instance deletion;
- Cyclic Log updating;
- Auto-renew;
- Stored Travel Rights (STR) processing;
- Ticket Transaction Reversal;
- Printing of tickets and receipts;

— Message generation and processing;

— Configuration handling:

- Hot lists;
- Action lists;
- POST Configuration Data lists.

6. ITSO Back Office (HOPS) requirements

The conceptual ITSO Back Office entity defined in ITSO TS 1000-4 is the Host Operator or Processing System (HOPS).

ITSO TS 1000-4 covers only those aspects of the Back Office that impact upon interoperability between HOPS, allowing HOPS implementers as much flexibility as possible where interoperability will not be affected.

The HOPS definition does not:

— cover all aspects of a public transport system back office, only those aspects which affect interoperability;

— define in detail how the HOPS will be implemented, but rather defines the functional requirements, excepting where in specific instances functionality must be mandated to provide interoperability.

ITSO has defined the following HOPS functional requirements:

— Lossless communications management (the Message Processor);

— Message data storage;

— ITSO Shell and IPE account management:

- Including Hotlist and Actionlist Processing;

— Asset management;

— Services:

- Audit trail + Journal,
- Rule Compliance,
- Security Monitoring,
- Backup,
- Archive.

These functional requirements are now discussed in more detail.

Lossless communications management (the Message Processor) is the process of managing the lossless communications method prescribed by ITSO TS 1000.

Message data storage is a secure store for all transmitted and received data, retained for data recovery and audit purposes.

ITSO Shell and IPE account management provides for:

— Accounts (data “files”) for each Shell and IPE;

— A method of creating and managing Hot Lists and Action Lists;

The Asset Manager is a facility to manage assets i.e.:

— POST;

— HOPS;

— ISAMs;

— HSAMs.

Not only does the Asset Manager identify assets, their status and location, but is also used to target security and other configuration files onto the correct asset.

All HOPS must include a security management device, the HSAM, which is identical in function to an ISAM. Indeed, in its simplest form, the HSAM comprises a single ISAM, as used in POSTs.

It will be apparent that the HOPS definition does not cover all the functions needed for a fully functioning Back Office, and therefore these functions will be specified by the scheme promoter or supplier. For example, the following are not included in the ITSO HOPS specification:

— Financial Settlement;

— Reimbursement;

— Product Management;

— Customer Media management.

The absence of Customer Media (CM) management from the HOPS specification is intentional. ITSO TS 1000 does not concern itself with actual CM, only with the ITSO Application (the ITSO Shell) held within the media. Therefore it specifies management of ITSO Shells through the Shell Account, but not management of the actual CM.

Each ITSO Compliant Scheme must include at least one HOPS, but the method in which the HOPS functionality is implemented is not mandated. A small scheme could buy in shared capacity on a HOPS owned & run by a third party provider, whilst at the other extreme a large scheme, such as UK national rail for example, would include a number of HOPS.

ITSO TS 1000 does not mandate how a HOPS is implemented. A single computer could be sufficient or the required functionality could be spread over a number of computers, possibly located remotely from each other. All ITSO Compliant Schemes must include all the HOPS functionality, but not necessarily in the same computer. However, all HOPS must include certain basic functions, including:

— Message processing;

— Message store;

— HSAM;

— Services.

7. Security Architecture

ITSO security architecture is designed to give every ITSO Member and Customer Media (CM) holder confidence that only genuine ITSO Products will be accepted by the appropriate Operators. Also the Transactions that are generated, when used as a basis for any revenue claim or apportionment, can be authenticated and if necessary, audited by the Product or Shell owner on behalf of the Customer Media holder.

The security architecture is designed to ensure interoperability can be achieved in an equitable manner by offering members the ability to use several different CM platforms of varying capability/cost, holding the Product(s) that suit their needs. Whilst also ensuring that interoperability with Products from other ITSO members can be accomplished in a controlled manner as and when required.

When Products and Transactions are created they are sealed for their lifetime. They can be Authenticated as unaltered and genuine by any ITSO Scheme member. ITSO has developed a Security Sub-system (SSS) for use by scheme members that ensures security can be managed consistently to the satisfaction of all members regardless of role. ITSO security is an “End-to-End” architecture which embraces the CM platform, the POST and the HOPS as illustrated by the dotted line in Figure 6.

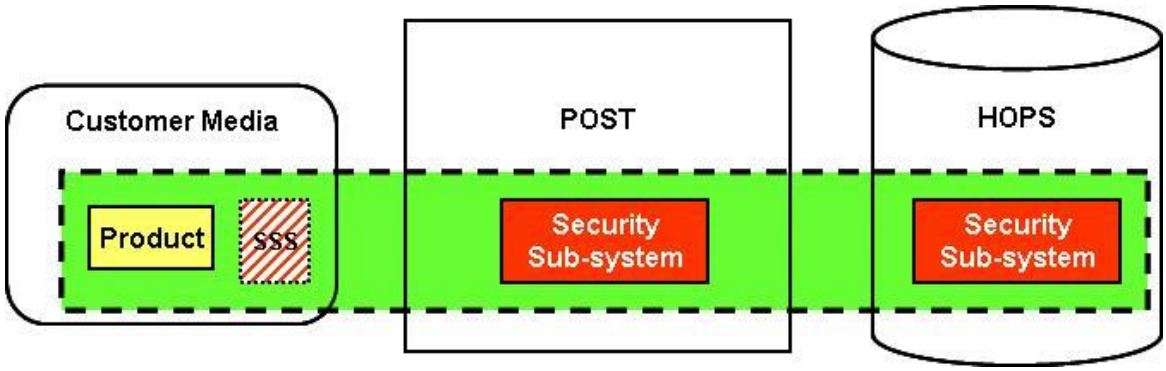

Figure 6 - End to end security

The SSS may be used by any entity within an ITSO Scheme regardless of role. Figure 7 illustrates the roles, primary relationships and locations of Security Sub-Systems in a typical ITSO scheme.

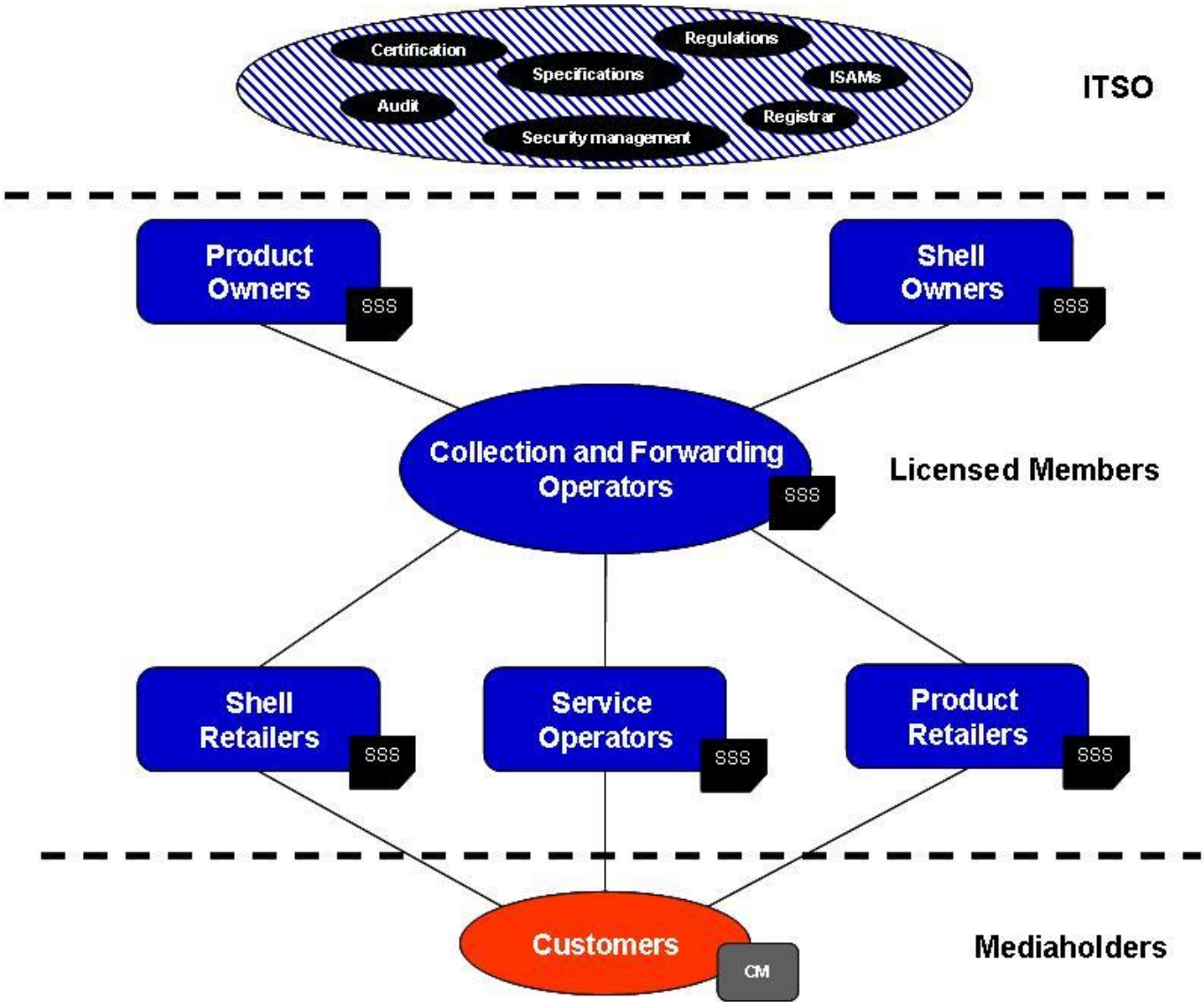

Figure 7 - Security sub-systems in a typical ITSO scheme

7.1 Elements of the security architecture

The security architecture embodies:

— unique numbering of ITSO; Shells, Products and Transactions;

— a numbering scheme and root that is interoperable with other business sectors;

— Product life-time Seals for service operator confidence;

— Key downloads and rollover that can be targeted on a need to know basis;

— Profiles to management of off-line retailer risk;

— Lossless Transaction handling;

— CM holder privacy;

— the facility to add new functions in the future.

The following sub-clauses describe each feature of the architecture in turn

7.1.1 Numbering and root

All ITSO Shells, all Products held therein and all Transaction Records are numbered uniquely throughout the ITSO Scheme. This ensures accountability and a credible audit trail in an interoperable environment. The root of the numbering system used is an International Issuer Number (IIN), registered in accordance with ISO standards, this ensures ITSO worldwide uniqueness should it wish to interoperate with similar schemes (under the IOPTA umbrella) or the many other business sectors that already use this system. The hierarchy of ITSO numbering is illustrated in Figure 8.

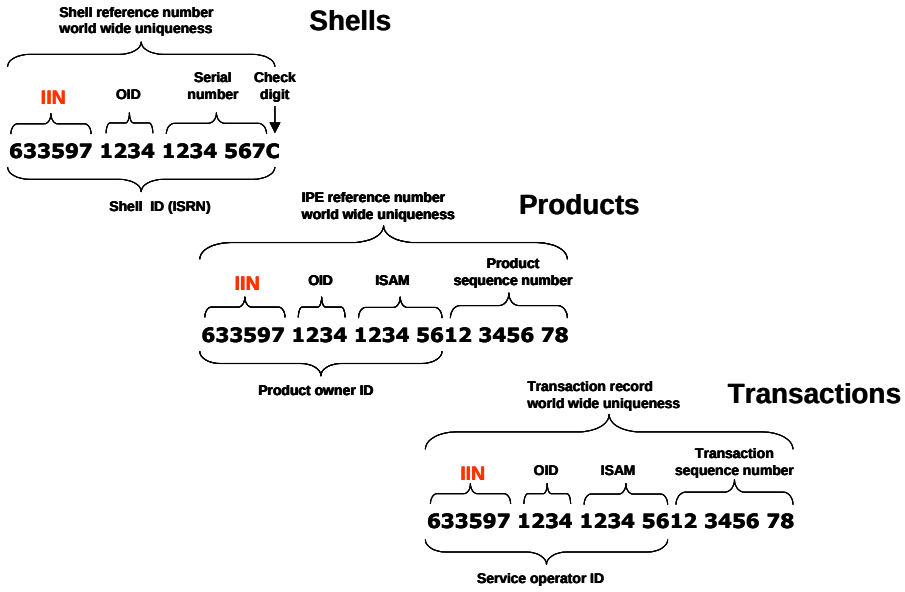

Figure 8 - Hierarchy of ITSO numbering

7.1.2 Seals & Keys

All Products carry at least one Seal. This cryptographic “guarantee of authenticity” is added when the Product is first created and lives with the Product throughout its life. The Product owner controls which members can create and add Seals to Products (retailers) and those that can accept and verify Products (service operators) by instructing the ITSO Security Management Service (ISMS) to download the necessary keys. Authentication of the Seal at the time of use gives the service operator confidence that the Product is genuine and has not been tampered with.

Note: Keys used, throughout the scheme, to access the various CM platforms and for authenticating the Directory are also distributed in a similar manner but at the behest of the ITSO Shell owner.

All ITSO Product and Directory data elements and structures are collected together into Data Groups that are then cryptographically sealed. Seals can only be generated by the SSS. The Data Group structure which includes the seal is illustrated in Figure 9.

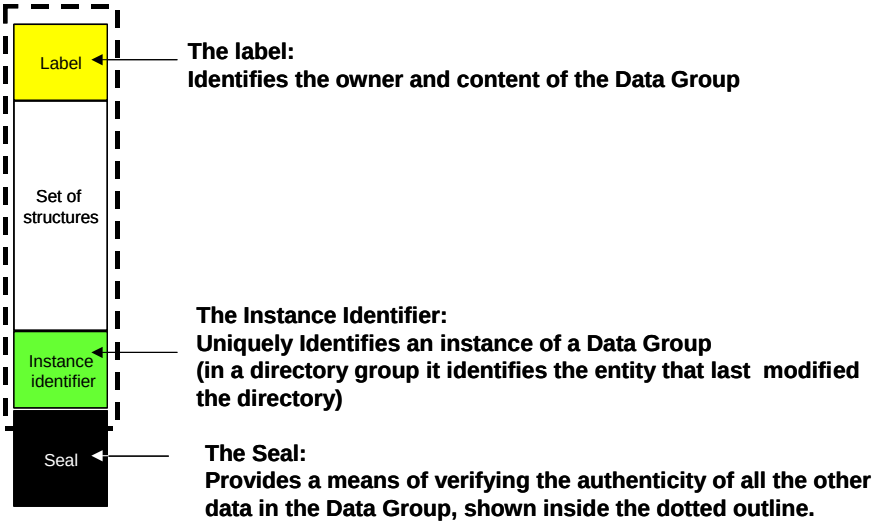

Figure 9 - Data group structure including seal

Where Products include both normally fixed and frequently varying data, the fixed and variable data structures are sealed separately but share a common Label as illustrated in Figure 10.

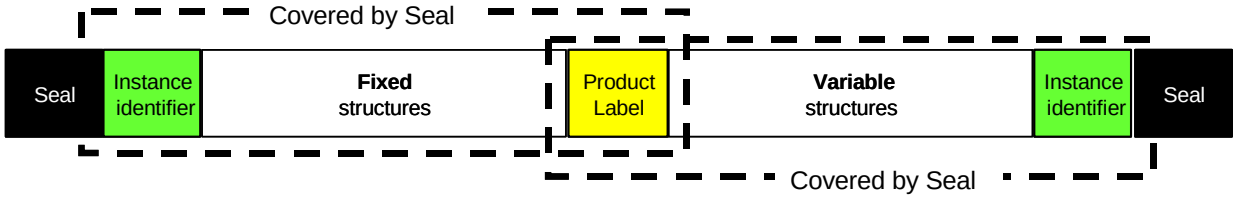

Figure 10 - Product with both fixed and variable data structures

7.1.3 Profiles

Product usage profiles are securely maintained at every POST and can be downloaded from a HOPS. This mechanism gives the Product owners and service operators the ability to ensure that a given POST is not limited to but, for example, able to:

— act as a retailer of some Products but not others;

— create up to a maximum number of season tickets until reset;

— have permission to add value to the STR Product;

— add value to the STR Product up to a maximum aggregated value until reset.

This mechanism ensures the risks involved in off-line operation for retailing high value Products and adding value to the STR Product can be limited.

7.1.4 Lossless Transaction Records

A Transaction Record is wrapped and uniquely numbered in a Data Frame that is then sealed. Each Transaction Record carries the identity of the sealing device and a sequence number that is incremented by one for every Transaction Record sealed. The HOPS receiving the frame may then check the seal as a “guarantee of authenticity” of the message. A Transaction Record batch header is securely maintained for each batch of Transaction Records created and is retained until a “delete batch” cryptogram is received. Undeleted batches

indicate that the relevant Transaction Record should be retransmitted until the receiving entity is in a position to accept the batch. By this mechanism missing, altered, duplicate and out of sequence Transaction Records can be detected. “Not on us” messages are forwarded to other HOPS In this case the integrity of the original Seal is maintained for audit purposes and the forwarded Data Frame is itself Sealed by the source HOPS.

7.1.5 CM holder privacy

Where the ITSO Shell Reference Number (ISRN) forms part of a Transaction Record it is encrypted in such a manner as to ensure only the ITSO Shell owner can link the Transaction Record to a particular individual.

7.1.6 Adding new functions

The ISMS can distribute configuration data and program code that allows the security environment to be updated in the event that:

— new CM access methods are added;

— new IPE designs are introduced.

This mechanism uses secure messaging to ensure that tampering (malicious or accidental) can be detected and that the information cannot be interpreted outside of the secure environment.

7.2 The Security Sub-System (SSS)

In order to implement the desired security architecture the ITSO SSS must be able to be trusted by all scheme members and have the following characteristics:

— Be able to hold keys in secret:

- to create and verify Products;
- to Seal Transactions;
- to access CM platforms;
- to perform secure messaging with other entities.

— Be able to holds sequence counters that cannot be modified by the POST for:

- Transaction Records;
- updates to value records in IPEs;
- security monitoring.

— Be able to hold configuration and limit data to ensure interoperability of:

- Transaction batch processing;
- off-line Product creation and value adding;
- basic POST functionality.

These requirements can only be met by housing the SSS in a tamper resistant device.

7.2.1 The ISAM

The ITSO SSS is supplied in the form of a Secure Application Module constructed from a programmable smart card chip with extended memory.

The ITSO Secure Application Module (ISAM) is supplied as a card of the same size as a conventional bank card but with a removable section having the same form factor as the subscriber identity module (SIM) found in all European digital mobile phones. This can then be fitted into a socket which is mandated for every POST and HOPS in an ITSO scheme.

The ISAM is formally accredited to common criteria level 4+ for a tamper resistant smart card and Application.

The ISAM is controlled by a POST or HOPS Application and implements the secure part of the ITSO Application when handling; CM, Products, ISMS messages and HOPS messages.

7.2.1.1 CM handling

The ISAM interacts with the CM via the POST Application to ensure:

— the various CM platforms specified by ITSO can be opened for access;

— a communications session appropriate to the CM platform can take place;

— the ITSO Shell is an integral part of session management.

7.2.1.2 Product handling

The ISAM interacts with the POST Application to ensure:

— the ITSO Directory can be checked for authenticity;

— any ITSO Products intended to be used can be checked for authenticity;

— any modifications to ITSO Products (such as STR values) are only allowed if permitted and such changes are identified with the ID of the POST service operator and re-sealed;

— any ITSO Products permitted to be created are uniquely identified with the Product owner's OID plus sequence number and Sealed;

— any changes to the Directory as a result of handling a Product can be re-sealed.

7.2.1.3 ISMS message handling

The ISAM interacts with the ISMS via the POST Application using a secure messaging system. These messages, which can only be generated by the ISMS, are passed to the ISAM when it is required to:

— add new or change keys used for CM access or data group authentication / Seal creation;

— change keys used to generate transaction information;

— add new or modify existing SSS functions;

— disable the SSS.

The ISAM acknowledges these changes to its internal configuration with a secure message of its own which is then be passed back to the ISMS.

7.2.1.4 ISAM in POST message handling

The ISAM installed in a POST interacts with a HOPS via the POST Application using a variety of messaging systems.

The ISAM provides the following services:

— it ensures that any Transaction Records resulting from handling an ITSO Product are uniquely identified by the ID of the POST operator plus a sequence number and sealed;

— depending on its configuration, it can also store these Transaction Records;

— it ensures that batch headers are managed correctly;

— under instructions from the HOPS:

- new Products may be added or removed,
- changes may be made to the acceptance and capability criteria used with Products;

— it acknowledges changes to its internal configuration, resulting from instructions from the HOPS, with a secure message;

— it ensures that the hot / action list messages received by the POST can be authenticated;

— it can store the hot / action list;

— it ensures that general housekeeping messages that do not form part of the Transaction Record messaging system can be sealed.

7.1.2.5 ISAM in HOPS message handling

The ISAM installed in a HOPS interacts with a POST or another HOPS via the HOPS Application.

The ISAM ensures that:

— the cryptographic delete strings sent to a POST to acknowledge the receipt of a complete batch of Transaction Records and trigger the delete of the batch can be generated;

— hot / action list messages sent to the POST can be sealed;

— other general messages sent to the POST can be sealed;

— general messages sent from a POST can be authenticated;

— messages sent to other HOPS can be sealed;

— messages received from other HOPS can be authenticated.

In addition, where the HOPS Application supports the asset managing function, the ISAM ensures that:

— secure messages to add or remove Products can be generated;

— secure messages to change acceptance and capability criteria used with Products can be generated;

— secure message acknowledgements received from POSTs can be authenticated.

8. Communications

Data communication between the various entities within the ITSO environment is fundamental to supporting the interoperability that ITSO sets out to provide. ITSO TS 1000-9 defines the data and communications mechanisms at a level that allows delivery of robust, secure and interoperable systems. Mandated requirements are kept to a minimum, allowing as much scope as possible for equipment providers to use existing technology and communications infrastructure.

One of the most important requirements defined is that all ITSO data transmission is lossless at Application level. This requires that the originator of a message retain the data transmitted until a positive acknowledgement is received for the message. If such acknowledgement is not received within a specified time period then the original message is retransmitted.

The data content of ITSO messages is defined in ITSO TS 1000-6. The standard transmission format as defined in ITSO TS 1000-9 is XML, although this is not mandated for communications between POST and HOPS. HOPS are networked in a peer-to-peer manner using a Virtual Private Network (VPN). A separate communications infrastructure is provided between HOPS and the ITSO Security Management Service (ISMS).

ITSO TS 1000-9 defines the structure and layout of the ITSO Application Messages. There are 4 classes of Application Message defined:

— Class 0 Positive acknowledgement message

— Class 1 Batch-orientated POST to HOPS message

— Class 2 General frame-orientated message

— Class 3 ISAM security message

The rules for usage and processing of the various message classes are defined in ITSO TS 1000-9.

The communications mechanisms are designed to handle the secure end-to-end transmission of messages, even when such messages have to pass through scheme-specific communications layers. The mechanisms also protect messages that are routed via intermediate HOPS to their final destination.

The confidentiality of data passed between HOPS is ensured by the use of a VPN. The VPN provides standard data encryption for all data passed over it. Where inter-HOPS communications does not use VPN, then it is the responsibility of the scheme owner / operator to ensure that the confidentiality of data passed between HOPS is secured. For normal operational data exchange between a POST and its associated HOPS, the scheme operator is responsible for ensuring data confidentiality.

The integrity of transmitted data is secured by the use of a Seal on each Data Frame that makes up an Application Message.

The authenticity of transmitted data is secured by the use of a Sequence Number, SealerID and Seal on each Data Frame that makes up an Application Message.

Non-repudiation of transmitted data is secured by the use of a Timestamp, SealerID and Seal on each Data Frame that makes up an Application Message.

The communications architecture allows for the secure transmission of keys and other security-related data between the ISMS, Asset Management Systems (AMS) and ISAMs.

9. ITSO data messages

Data Message definitions are, in general, defined in part 6 of the specification. However, messages relating to the security management are defined in part 8 of the specification.

Table 3 outlines the message types defined in part 6.

Table 3 - ITSO Message Types

Type of message	**Message Group**
Transaction Record data	ITSO shell, IPE Administration, Card issuer messages
Transaction Record data	Stored Travel Rights, CTA
Transaction Record data	ITSO ID, loyalty, create or amend IPE, journey record, action list acknowledge
Transaction Record data	Cancellations and refunds, miscellaneous, list match event records
Other Message Data	Exceptions and CM Transaction error messages (POST to HOPS)
Other Message Data	POST to HOPS queries
Other Message Data	HOPS to HOPS messages
Other Message Data	AMS – ISMS messages, which are defined in ITSO TS 1000-8
HOPS to POST/HOPS messages	Miscellaneous messages
HOPS to POST /HOPS messages	Message control
HOPS to POST /HOPS messages	Parameter tables
HOPS to POST /HOPS messages	Parameter tables
HOPS to POST /HOPS messages	POST Configuration Data, Capability list, Hot List, Action list, Data Correction record
HOPS to POST /HOPS messages	HOPS Response to POST queries
User defined system specific messages	Messages are user defined, and it is the responsibility of the sender to ensure that the addressee can interpret the message. Both data format and content are user defined.