



consult hyperion

The Future of UK Transportation Ticketing

A Consult Hyperion white paper

www.chyp.com

June 2003

Version 1

Contents

Abstract	2
Integrated Transport Smartcard Organisation (ITSO)	3
What do the ITSO specifications define?	4
Conclusions	5
Appendix 1: Overview of the ITSO v2.0 Shell	6
Appendix 2: Description of the ITSO SAM	7
Appendix 3: Changes expected in Version 2.1	8
About Consult Hyperion	10
About the Author	10

Public transport organisations have traditionally issued paper tickets, often incorporating a magnetic stripe on which journey information is encoded. These tickets can vary in value from less than a pound for a single short journey to thousands of pounds for an annual season ticket. Some tickets are issued purely as a receipt, while others need to be inserted into automated gates in order to gain entry to, or exit from, stations. Although these tickets cost a fraction of a penny to produce, the cost of operating a system based upon them is significant. They also have limitations, including storage capacity, durability, and the ease with which they can be counterfeited.

In 1997, the Octopus ticketing scheme was launched in Hong Kong using a new reusable ticket medium based upon Radio Frequency Identification Devices (RFID). Although not the first scheme to use the technology, its success demonstrated that it was commercially possible to use much higher cost ticket media in transportation. However the Hong Kong scheme is somewhat unique preventing it being easily replicated by other schemes. Although a number of other organisations have implemented schemes since, most continue to use traditional tickets.

The cost of implementing a scheme based on RFID technology is significant as the majority of a schemes legacy systems and fare collection infrastructure will need to be replaced. However the standardisation of these systems will help reduce this cost by allowing suppliers to develop standard systems for which the development costs can be shared. It is also generally recognised that as organisations update their systems, through standardisation, there exists an opportunity to introduce interoperability.

In 2000 / 2001 the International Standards Organisation (ISO) published a standard covering RFID technology suitable for use as a ticket medium, known as Contactless Proximity Cards. This standard, ISO/IEC 14443, defines the physical, electrical and low level communication properties of the cards, facilitating interoperability between cards and reader devices produced by different manufacturers. The standard however does not address specific application issues such as how Proximity cards can be used as a ticket.

The European Committee for Standardisation (CEN), is however actively preparing some of these higher level standards via two CEN technical committees; namely TC224 for machine readable cards, related device interfaces and operations and TC278 for road transport and traffic telematics. The EN 1545 standard 'Identification Card Systems – Surface Transport Applications' provides the definition of interoperable data elements for machine-readable card data in surface transport applications. This standard originally published in 1998 (ENV 1545) is currently in the process of major revision. The IOPTA standard 'Smart Card Application' defines the data set construction using EN1545 data elements, the security and access environment, and the necessary underlying physical environment for interoperability between surface transport machine-readable cards. This includes the interfaces with other standards concerning machine-readable or smart cards such that an IOPTA application may share a physical smart card environment with other standardised applications to create a multi-application smart card.

“ Although no ITSO compliant schemes have actually been implemented to date, a number are currently in the process of implementation or plan to migrate to compliance as soon as the specifications and core infrastructure are available ”



However standards take a long time to develop. In the meantime a number of organisations have been developing, and in some cases are implementing their own schemes. To date the three most significant have been:

1. The Integrated Transport Smartcard Organisation (ITSO), representing UK transportation operators. To date, no tickets have been issued as the organisation has been concentrating on developing its specifications, business rules and supporting systems.
2. Calypso, developed by a group of European partners from the cities of Brussels, Lisbon, Konstanz, Paris and Venice. These organisations have been concentrating on rolling out local smart card ticketing schemes in each member's city.
3. VDV (Verband Deutscher Verkehrsunternehmen) an association of German transport companies supported by the German Federal Ministry for Education have been developing a technical standard known as 'The Core Application' to allow a universal electronic ticket to be introduced throughout Germany.

All these organisations are actively involved in the CEN standardisation process, providing valuable input while also attempting to influence the final standards.

Integrated Transport Smart card Organisation (ITSO)

ITSO is a non profit distributing organisation owned by its members: UK Passenger Transport Executives (PTEs), bus operators, the operators of Britain's passenger train franchises and suppliers. ITSO is also supported by the UK Department for Transport who has mandated ITSO compliance for any new transport ticketing projects¹ seeking public funding. However, to date ITSO has operated only one level of membership for which fees are charged consisting of an initial joining fee plus annual membership. Although tiered fee scales have existed for local authorities and transport operators, generally a flat fee exists for other organisations regardless of size. As these fees are not insignificant, especially for small organisations, the fee structure effectively limits the current membership. ITSO is currently in the process of revising this fee structure and an announcement is expected imminently.

The organisation is currently developing the specifications and core infrastructure necessary to support schemes compliant with the ITSO specifications being introduced in the UK from early 2004. To achieve this objective, ITSO is concentrating effort on the following:

- **ITSO Specification**, version 2.0 of the 'ITSO Specification for Interoperable Public Transport Ticketing Using Contactless Smartcards' was published under Crown Copyright in November 2001. A revised version, v2.1 (see appendix 3), is currently being developed with publication expected in October 2003.
- **ISAM**, The ITSO Security Access Module (see appendix 2), developed in conjunction with a third party supplier, used to enforce the security policy of ITSO within ticket issuing / acceptance devices and back office systems. Working samples of the first implementation, V1.0, are available and work is about to commence on the first revision.
- **Scheme Rules**, ITSO is currently developing the ITSO brand and a comprehensive set of business rules defining the scheme. Publication is expected in August 2003.
- **Accreditation**, ITSO, in conjunction with a third party supplier, is developing an accreditation process to certify that all equipment carrying the ITSO brand is compliant with the published specifications. A commercial service to undertake testing and certification of equipment is expected to be operational by December 2003.
- **Security Management**, ITSO, in conjunction with a third party supplier, is developing a Security Management Service (SMS) to undertake the generation and distribution of security keys to ISAM's. A commercial operation to provide this service is expected to be operational by December 2003.

Although no schemes compliant with the ITSO specifications have actually been implemented to date, significant progress is being made by suppliers, part of an ITSO working group '12F', testing the interoperability of their ITSO compliant systems. This work is being undertaken using drafts of the revised specification and will facilitate the early introduction of schemes once the final specifications are released. A number of organisations are currently in the process of planning implementation or migration to compliance as soon as this occurs:

- NoW (Cumbria, Lancaster, Blackburn, Blackpool) - Migration of exiting concessionary travel scheme consisting of 20,000 smart cards to ITSO compliance;
- The South Wales Integrated Fast Transit consortium (SWIFT), made up of six local authorities (Caerphilly, Cardiff, Bridgend, Rhondda Cynon

¹e-GIF 5 mandates the use of ITSO for all government sponsored transport ticketing projects

“ The ITSO specifications define a non-confidential data structure, the ITSO Shell, onto which a number of interoperable products entities (IPEs) can be loaded ”



Part 7 is not available from the website and is only available directly from ITSO under Non-disclosure agreement

Taff, Merthyr and Vale of Glamorgan) - Migration of existing concessionary travel scheme consisting of 130,000 smart cards to ITSO compliance;

- The South-West Wales Integrated Transport Consortium (SWITCH) made up of four Unitary Authorities (Carmarthenshire, Neath Port Talbot, Pembrokeshire and Swansea) - Migration of existing concessionary bus travel scheme consisting of 90,000 smart cards to ITSO compliance;
- Greater Manchester PTE (GMPTE) - Introduction of an ITSO compliant concessionary travel scheme now expected to go live in 2004;
- YORCARD- Introduction of a new ITSO compliant full travel card;
- Cornish KeyCard - Migration of exiting tourist and travel card scheme consisting of 50,000 dual interface smart cards to ITSO compliance.

The notable exception to the above list is Transport for London (TfL). Although currently in the process of rolling out its Oyster scheme, which is expected to be the UK's largest transport card scheme, no commitment has currently been given by TfL to migrate this proprietary scheme to ITSO compliance. A technical solution to allow migration or inter-working is however being developed in anticipation of future commitment.

What do the ITSO Specifications Define?

The ITSO specifications define a non-confidential data structure, the ITSO Shell (see appendix 1), onto which a number of

interoperable products entities (IPEs) can be loaded, e.g. tickets, concession passes or an electronic purse. It also defines the functionality and user interface required from the equipment used for ticket issuing / validation (POST), and outlines the requirements on the back-office systems (HOPS). The content of messages between the different entities within a scheme, and a security policy enforced by the ISAM (see appendix 2) are also defined.

ITSO does not define a central clearing and settlement service for transactions. Instead, when an operator accepts a ticket issued by another organisation, the back office system will need to identify the transaction and send it for settlement to the correct organisation. This functionality and the message formats to be used are defined within the specification for the HOPS and are known within ITSO as 'not on us transactions'. ITSO is however building two services to support the operation of schemes; a central service to manage the security keys, the Security Management Service (SMS), and an accreditation service to certify that all equipment and systems carrying the ITSO brand comply with the specifications. Both these services will levy fees to provide an operational income to ITSO.

From these components an organisation can construct an ITSO compliant scheme as shown in figure 1.

The published specification, available under Crown Copyright without charge from www.itsonews.com is currently divided into 7 parts:

- Part 1**, Overview and Business Model
- Part 2**, ITSO Card Data Structure

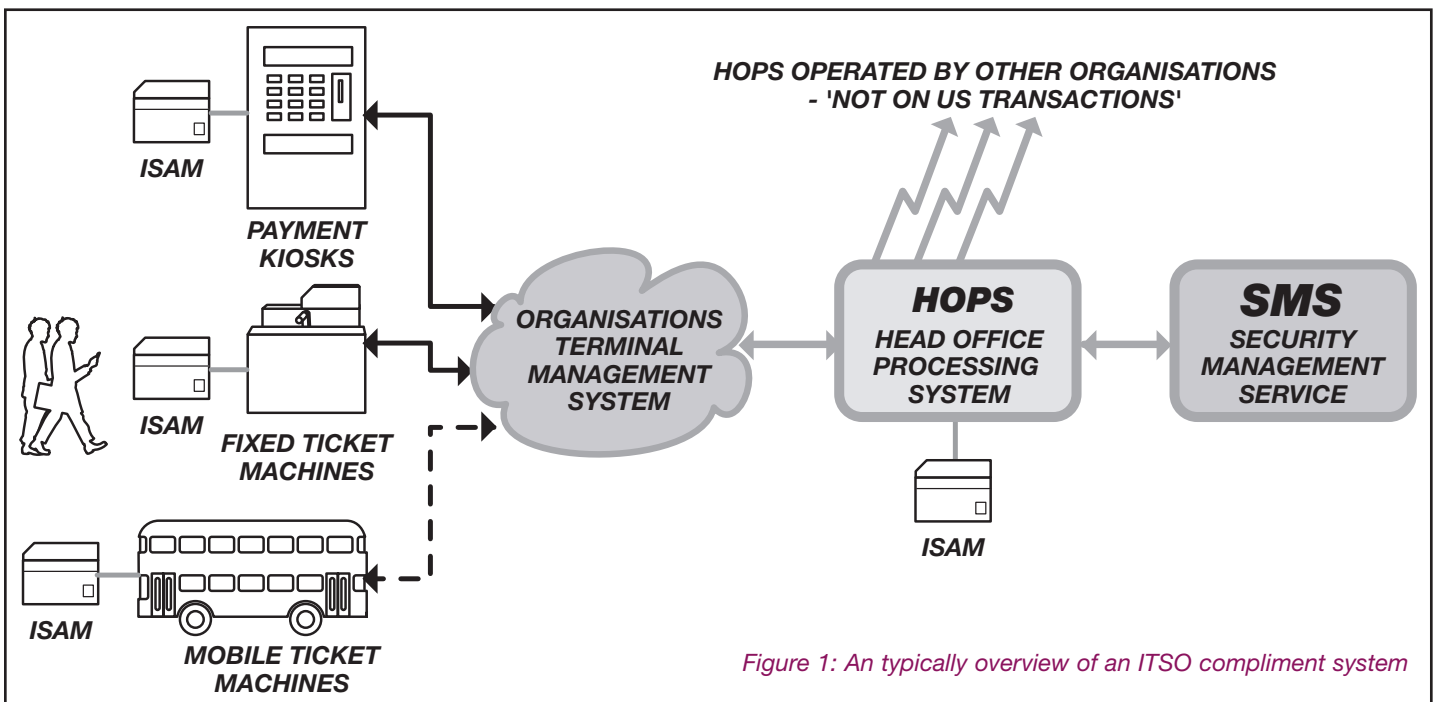


Figure 1: An typically overview of an ITSO compliment system

Part 3, ITSO Terminal Specification

Part 4, Back Office Systems

Part 5, Card format and Data Records

Part 6, ITSO Security Application Module Overview

Part 7², ITSO Security Application Module

The ITSO specification does not attempt to define any electrical or physical properties of the media to be used, selecting instead to mandate ISO/IEC 14443 and ISO/IEC 7816 as appropriate. Data elements within the specification are aligned to the current draft CEN EN1545 standard. However, this standard is currently in the process of major revision so the specification still contains some duplication and discrepancies with the data elements defined in the standard. ITSO is working closely with the CEN committees developing both EN1545 and IOPTA to ensure that future revisions of the ITSO specification are compliant.

By complying with the specification, any ITSO compliant card issued can be read, and the data it contains interpreted, by any other organisation operating an ITSO compliant scheme. However this physical interoperability does not mean that a ticket (IPE) loaded onto a card will be accepted by any transport operator other than the one that issued the original ticket. The situation is therefore exactly the same as with current ticketing systems, except for the fact that smart cards are used in place of traditional tickets. This advance may initially not appear very significant, but it sets the foundations to allow operators to enter into business agreements with other ITSO compliant scheme for the issuance and acceptance of their tickets. It also facilitates the standardisation of ticket media and equipment purchased by transport operators, therefore potentially reducing costs. To ensure that an environment exists to capitalise on this opportunity, ITSO have defined a comprehensive set of business rules to facilitate the formation of these business relationships.

Conclusions

It is generally accepted that the current specification published in November 2001 is not suitable for implementation due to the large number of issues³ identified within it. A revised specification is therefore in development by ITSO which is currently expected to be published (see appendix 3) following formal ratification by ITSO members at an EGM in Mid October 2003. Although the current published specification is publicly available at no charge, other documents like the scheme rules and technical notes are only generally available to members. However these documents and the revised specification are currently being developed with a very limited number of

people having access before publication. In contrast, standards developed by the International Standards Authority (ISO) and the European Committee for Standardisation (CEN) are freely available during the drafting stage to ensure the widest possible consultation. This restrictive practice may be to the detriment of these specifications.

Since its formation, dates published by ITSO for key milestones have frequently been missed. Historically this may have been due to financial issues, as ITSO has struggled to raise sufficient funds for the work it has been undertaking. In late 2001 however, Mersey Travel and GMPTE injected £1.5M to allow the ISAM to be developed and the accreditation process to be set up. More significantly the Department for Transport has recently injected £3.5M funding in order to accelerate the introduction of ITSO compliant schemes. However, delays have continued to occur⁴ this year, with the late publication of version 2.1 of the specifications (originally planned for January this year) and the development and implementation of the SMS centre not currently announced.

The cost of implementing an ITSO compliant scheme is also currently unknown, ITSO have not yet published the fees to be levied for its operational services. However it is believed that an ITSO compliant scheme is likely to be significantly more expensive to implement than a simple proprietary smart card scheme, mainly due to the interoperability and auditability provision. In calculating the additional cost of a compliant scheme, the following should be considered:

- The additional cost of upgrading to ITSO compliant ticket vending and validation equipment
- Initial purchase cost of the ISAM (believed to be in the region of £50.00 per device)
- Cost of implementation and operation of HOPS functionality and communications infrastructure necessary to support communication between SMS and ISAM and receive transaction records from ISAM (even when no further use is made of the collected data).
- Service charge levied by the SMS for management of scheme keys

The revised specification represents only the tip of the iceberg with regard to the effort necessary to implement a country wide interoperable ticketing scheme. Although ITSO have defined business rules, each transport operator or organisation will still need to enter into private agreements with all organisations with which they wish to share tickets. Apart from such co-operation that already exists on

“ ..it is believed that an ITSO compliant scheme is likely to be significantly more expensive to implement than a simple proprietary smart card scheme, mainly due to the interoperability provision

”



³ Separate papers are available from Consult Hyperion detailing some of these issues.

⁴ Original schedule based on dates published in the ITSO newsletter, issue 8, August 2002.

conventional magnetic stripe based tickets, it is questionable if any business case or operational need exists for such interoperability. As systems are deployed, it is possible that demand for such interoperability may increase, it will however take many years before a significant number of schemes have migrated to ITSO compliance. Early adopters will incur the expense of provision of this interoperability, with little prospect of any financial or commercial reward.

If the specifications prove too expensive to implement, or fragmentation occurs within the industry, then ITSO will fail. Fragmentation may occur if ITSO further delays the publication of a stable specification and implementation of the core services. Non ITSO compliant schemes like the London Underground 'Oyster' card are already being implemented. Technical advances in contactless proximity cards may also force significant revision of the specifications leading to expensive upgrades to any implemented schemes in order to maintain interoperability. In order to allay these concerns and to encourage early adoption, ITSO have publicly stated⁵ that once V2.1 is published, any scheme installing a system based on it will not be required to upgrade to subsequent revisions for a period of 10 years. It is not clear however how this statement will be honoured and interoperability maintained over such a long period.

The official ministerial launch of ITSO is expected next year when the first ITSO compliant schemes start operating and have overcome any initial issues. This milestone will be used to pronounce ITSO a success. Ultimately however, ITSO will not be judged by these first operational schemes or the quality of its technical

achievements, but by the number of organisations finally implementing the specifications and the level of interoperability between them.

Appendix 1: Overview of the ITSO V2.0 Shell

The ITSO shell consists of a shell header, a directory frame, and one or more IPEs. Key data elements within the structure are protected from alteration by a certificate or ITSO seal. A simplified diagram of the structure of an ITSO shell is given below in figure 2.

The ITSO shell header contains the 'ITSO shell reference number' (ISRN), a unique reference number used within the ITSO scheme. This number also contains the 'ITSO operator's identification number' (OID) which identifies the owner (or issuer) of the shell application. References to the translation of the data structures defined within the ITSO specification onto the physical memory map of the card platform are also included, together with references to the type of cryptography and key set used by the platform. It is also a requirement that the card platform's unique serial number is available, as this is used within the key diversification algorithms. An ITSO certificate does not protect the shell header as once written to the card it should permanently be protected from being altered (i.e. read only).

The directory frame contains details of the location of IPEs already loaded onto the platform and the availability of memory for the loading of further IPEs. It also contains details of if and when an IPE can be deleted once its validity period has expired. In normal use of the ITSO shell, the entries within the directory will need to be altered as IPEs are loaded, deleted or

⁵ Peter Stoddart, General Manager of ITSO made this statement at the ITSO suppliers meeting, 14th May 2003

⁶ Anti-tear is a feature that allows the integrity of data to be guaranteed even when the card is removed from the reader while data is being written. In such circumstances, the new copy of the data is identified as corrupted or incomplete and the previous copy of the data used instead.

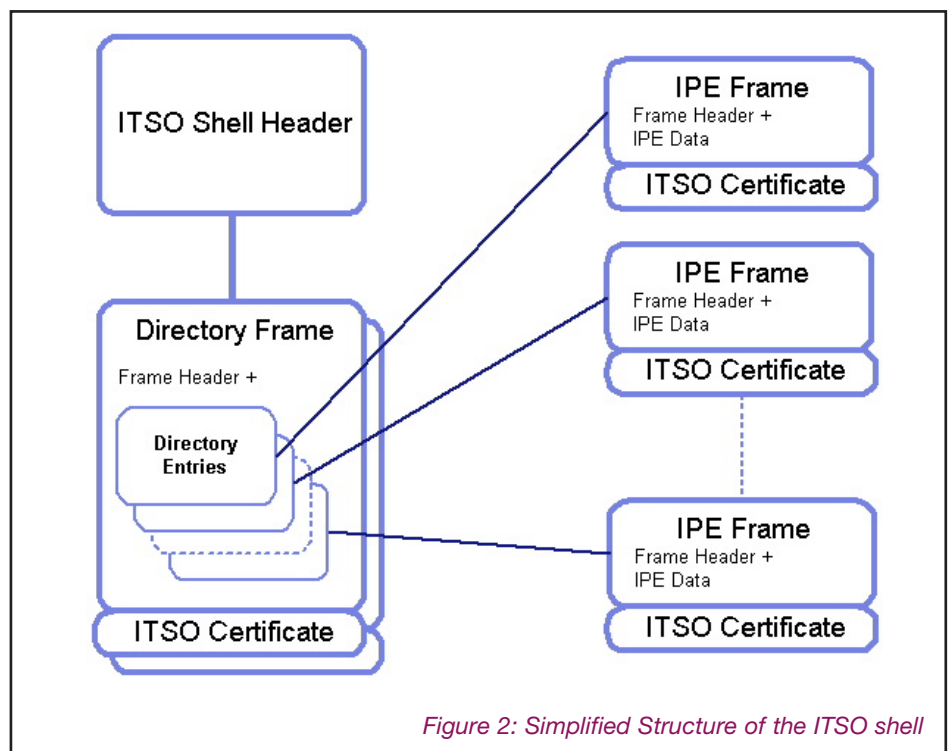


Figure 2: Simplified Structure of the ITSO shell

⁷ *Anti Tear Protected Area (ATPA) is a defined structure within the ITSO specifications for holding value records that may be used within an IPE definition.*

⁸ *ITSO has is currently submitting the ISAM for third party security accreditations, Common Criteria level 4.*

⁹ *ITSO currently somewhat confusingly refer to these signatures as certificates, although other names such as 'Seals' or 'MACs (in the case of symmetric cryptography) are sometimes used.'*

amended. The directory is therefore protected using an ITSO certificate, allowing detection of unauthorised changes. Two copies of the directory frame may also be present on a card to facilitate a terminal based anti-tear⁶ mechanism.

Each directory entry with the directory frame provides limited information about the IPE to which it points with special directory entries defined for Private and Log IPEs. The information stored within the frame header and each directory entry is designed to allow a rapid method of identifying whether the shell contains a valid IPE when presented to a terminal.

IPE frames (typically tickets) contain a structure of data elements as necessary for the purpose for which the IPE is intended. The actual size of each IPE definition varies. Some IPE definitions also include variable length records so are not of a fixed length. Some IPEs essentially are read only, others include anti tear frames (ATPA⁷) to protect the integrity of data when they are updated in normal use. Table 1 lists the 18 IPEs currently defined in the V2.0 of the ITSO specification together with a short description of each:

Appendix 2: Description of the ITSO SAM

The ITSO SAM (ISAM) is a secure⁸ device used to enforce the ITSO security policy and hold scheme keys. The ISAM is required to be installed in all ITSO ticketing / back office systems and is used to perform the following operations:

- **Secure Storage and communication of ITSO scheme Keys.** These include the keys required for the validation and generation of ITSO card signatures⁹ and for secure / protected communication with the HOPS / SMS centre.
- **Enforcement of ITSO security policy.** The ISAM can be configured by the SMS to restrict which operations (using which scheme keys) a device can undertake. When a commercial agreement is made between two parties, details are passed to the SMS so that it may configure each party's ISAMs with the necessary access rights.

Table 1: IPE defined within the specification

IPE	Description
0	Private entity , the definition of which is outside the scope of ITSO
2	Stored travel rights , a basic implementation of an electronic purse.
3	Loyalty type 1 , a loyalty product containing the points balance that the cardholder has accumulated.
4	Charge to Account (CTA) , a structure similar to an electronic purse, however not containing actual funds but recording the value of travel undertaken for post pay applications
6	Pre-Defined Ticket (Area based) , similar to IPE 22 however adding ability to re-use the ticket a specified number times (e.g. 10 single day passes) and allow the ticket to be updated either manually or through an auto-renew capability.
7	Pre-Defined Specific Journey Ticket , similar to IPE 23 however adding ability to re-use the ticket a specified number times (e.g. multi-ride) and allow the ticket to be updated either manually or through an auto-renew capability.
8	Pre-Defined Specific Journey Ticket , similar to IPE 24 however adding ability to re-use the ticket a specified number times (e.g. multi-ride) and allow the ticket to be updated either manually or through an auto-renew capability.
9	Travel Related Voucher , similar to IPE 25 however adding ability to re-use the voucher a specified number times and allow the voucher to be updated either manually or through an auto-renew capability.
10	Open system tolling , similar to IPE 26 however adding ability to re-use the product a specified number times and allow the product to be updated either manually or through an auto-renew capability.
14	Entitlement , a secondary ITSO ID IPE that may be used only in situations where IPE 16 is already present.
15	Combined ITSO Log / ITSO ID IPE , the log contains a record of recent shell events plus an ID element, see below for ID IPE description.
16	ITSO ID IPE , typically this contains the data normally printed on a photo or concession card, it can also optionally contain a digitised image of the cardholder.
17	Loyalty type 2 , this IPE does not contain the loyalty points balance, however can be used to identify the card holder as being a member of a centrally accounted loyalty scheme
22	Pre-Defined Ticket (Area based) , a basic read only travel ticket or period pass
23	Pre-Defined Specific Journey Ticket , a basic read only travel ticket or period pass specifying the journey that may be undertaken.
24	Pre-Defined Specific Journey Ticket , a more complex read only travel ticket similar to IPE 22 but including reservations and special restrictions.
25	Travel Related Voucher , a read only product to identify additional entitlements to the cardholder, e.g. card parking or on-train meals.
26	Open system tolling , a product related to tolling where the fee is not distance related, e.g. for a river crossing either by bridge, tunnel or ferry.

- **Ticket issuing and validation.** Data stored within the ITSO directory frame and IPEs is protected from modification using a certificate. This is generated or verified by submitting the protected data to the ISAM that then undertakes the necessary cryptographic calculations.
- **Storage and secure communication of transaction records.** The ISAM records details of all ITSO transactions undertaken by the POST. These are then assembled into batches protected by a header containing a signature calculated over the batch for transmission to its local HOPS. The HOPS, which also contains an ISAM, validates the batch has been received correctly (using the batch certificates) and replies to the POST with a signed message authorising the deletion of the batch. If this response message is not received within a configured duration, the batch is automatically re-sent by the ISAM within the POST.
- **Security and risk management.** Each ISAM can be configured to only perform a defined number (or value) of transactions before requiring communication to the HOPS. Various safeguards are built into the ISAM to limit its use should the device be stolen

The first implementation, ISAM V1.0, has been developed through a partnership between Ecebs Limited, (lead contractor) Atmel Corporation and Sagem who were awarded a contract to develop the ISAM by ITSO. Key technical features are as follows:

- Multi-chip module containing ATMEL AT90SC3232CS 8/16-bit secure micro-controller and 4M Byte FLASH memory device;
- Physical size as defined in ISO/IEC 7810, ID-000 (SIM format). Typically supplied in ID-001 (bank card) format with ID-000 pop out ;
- Standard smartcard contact plate layout as defined in ISO/IEC 7816 part 2;
- Communication using ISO/IEC 7816 T=1 protocol with communication speeds up to 400k Baud;
- Fast Symmetric and Asymmetric cryptography using hardware accelerators (currently supports DES, Triple DES and RSA);
- Separate parts available for 3v and 5v operation.

The current implementation however does not support all functionality expected to be included within the ITSO V2.1 specifications, most notably the new platform definitions e.g. disposable cards, are not supported. A revised

implementation, ISAM V2.0, is therefore currently being planned which when available will be distributed as a field software update to all ISAM V1.0 users.

Without an ISAM, it is not possible to load or update an ITSO product (IPE) containing an ITSO seal, or validate that a card presented contains a valid ITSO directory / product (IPE). Within the ITSO scheme, it is therefore essential that all ticket vending / acceptance equipment contains an ISAM, which is itself a requirement of ITSO compliance. The only circumstance that an ISAM may not be required is when accessing a private IPE (IPE=0) that is already loaded onto a card (anti-tear must be handled internally within private IPE if required), or in low security applications (as ITSO certificates cannot be validated) where only read access is required.

As the ISAM needs to communicate with its local HOPS on a regular basis (to upload transactions and receive updates), a communication system is required. This will typically be implemented using either network infrastructure or a PSTN modem. In situations where the ISAMs are installed in portable equipment or within vehicles, provision will need to be made to physically bring the devices to a location where communication is possible on a regular basis.

In some circumstances a terminal may require more than one ISAM to support the creation of another operator's IPEs. An option is defined to load a virtual copy of an ISAM, referred to as a 'Proxy ISAM', onto an existing physical ISAM within the POST. This Proxy ISAM will however be registered and treated as a separate entity by the SMS centre.

The ISAM as currently designed and implemented is a powerful device capable of far more than securely holding a limited number of scheme keys. Many of these advanced features are designed to allow the use of legacy equipment, support interoperability requiring large numbers of scheme keys and provide provision for future non transport applications. For many schemes however, these advanced or additional features may not be required.

Appendix 3: Changes expected in Version 2.1

Version 2.1 of the ITSO specifications is currently expected to be published following formal ratification by ITSO members at an EGM in Mid October 2003. This revision represents a major update to resolve issues identified in the original documents, and will be the basis for the implementation of all initial ITSO schemes. The key changes¹⁰ are as follows:

- The Specification will be based on version 2.0 (plus existing technical notes) with a template and definition tidy up.

¹⁰ Based on details as published in the ITSO newsletter, issue 8, August 2002.

¹¹ Technical notes are internal ITSO documents providing clarification / correction to the current specification or advising members of new functionality.

- Technical note 5¹¹, the 'ISAM card edge interface specification', will be included as part 8 of the revised specifications.
- Technical notes 6 and 7, 'Communications Interface Specifications' will be included as part 9 of the revised specifications, these include:
 1. HOPS to POST
 2. Asset manager to ISAM
 3. HOPS to HOPS transfers (inc VPN)
 4. Asset manager to SMS
- The existing 'Card Format definitions', part 2 appendix A, will be moved and expanded into a new section 10. The current card format definition 2 will be revised to form a generic microprocessor card definition and a range of low cost cards (e.g. Mifare Ultra light) will be added.
- Notation and or removal of items that have been included in the ITSO regulations or guides.
- Further changes to ensure convergence to latest draft of GEN EN1545.
- Revision of parts 6 and 7 to align with the new part 8, 'ISAM card edge interface specification'

ITSO have also publicly stated that they are collaborating with the group of European partners representing Calypso¹². This was a rival European electronic ticketing standard that defines the secured dialogue between cards and terminals. The aim is to allow the acceptance of Calypso cards within an ITSO scheme, therefore further improving interoperability. It is not clear if the output of this collaboration will result in changes being introduced into the ITSO specification.

Beyond V2.1, further revision of the specifications is likely. V3.0 is already planned and will introduce any changes required once the EN 1545 and IOPTA standards are published to ensure ITSO remains compliant. Further card format definitions may also be added to part 10, ITSO however will require the card supplier to fund the cost of such updates.

¹² Calypso schemes are currently operating in Brussels (Belgium), Lisbon (Portugal), Konstanz (Germany), Paris (France) and Venice (Italy). For further information on Calypso see <http://www.calypso.tm.fr>

About the Authors



Colin Tanner

colin.tanner@chyp.com

Colin Tanner has extensive knowledge of multi-application smart cards, contactless devices and applications. This includes a detailed working knowledge of the Philips Mifare Classic platform and contactless variants of Multi-application platforms such as MULTOS and Java Card.

Recent assignments have included assisting MasterCard with the PayPass contactless payment trial in Orlando and developing contactless applications for other financial organisations.

Colin currently attends, on behalf of Consult Hyperion, the British Standards Institute (BSI) meetings on contactless cards (ISO 14443 / ISO 15693). These meetings decide the UK position on these standards and how the UK will vote at the International Standards (ISO WG8) meetings. Previously Colin has also regularly attended these ISO meetings as a UK representative in the capacity of 'UK Technical Expert'.

Our Business

Consult Hyperion is an independent information technology consultancy. We have over sixteen years experience of helping organisations to derive maximum benefit from technology. Our success lies in our ability to apply a unique blend of business and systems analysis skills to deliver a strong interface between business and technology.

We specialise in transactions and security, providing professional services from the conceptual stage of a project through to completion. We advise on **business and technical strategy**, performing **requirements analysis** and producing **technical specifications** for internal development or external procurement. We can also help to dramatically shorten project life cycles by building **proof of concept** and **pilot services**.

Our practical experience with key technologies - including cryptography, smart cards, wireless devices, messaging, internet and digital TV - and more than a decade spent working with international blue-chip clients on innovative projects, make us uniquely qualified to advise on turning great business ideas into working systems.

Consult Hyperion

8 Frederick Sanger Road, Surrey Research Park, Guildford, Surrey GU2 7EB, England
T: +44(0)1483 301793 F: +44(0)1483 561657 E: info@chyp.com W: www.chyp.com