

Issuing Authority:	Owner:	Project Editor:
ITSO	Technology at ITSO	Mike Eastham
Document number	Part Number:	Sub-Part Number
ITSO TS 1000	4	
Issue number (stage):	Month:	Year
2.1.3	April	2008
Title:		
<i>ITSO TS1000-4 Interoperable public transport ticketing using contactless smart customer media – Part 4: HOPS</i>		
Replaces Documents:		
<i>ITSO TS1000-4 2007-06 Issue 2.1.2</i>		

Revision history of current edition

Date	ITSO Ref.	Editor ID	Nature of Change to this Document (or Part)
Feb 2003		PQ	Document created
May 2003		PQ	Amended after editorial review
June 2003		PQ	Released for issue as CD.
Aug 2003		JW/CS/PJ	Amended after review by TC & Authors. Issued as 2 nd CD.
Nov 2003		PJ/JW	Amended with comments received
Nov 2003		SLB	Editorial changes only. Issue 1 st consultation draft.
Jan 2004		JC	Implement DRC changes.
Feb 2004		JW	Check/consolidate DRC changes.
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
April 2007		PRJ	Updated to include ISADs following approval by DfT
Jun 2007		MPJE	Final Editing prior to publication
Feb 2008		PRJ	Updated to include ISADs following approval by DfT
Apr 2008		MPJE	Final Editing prior to publication

Document Reference: **ITSO TS 1000-4**

Date: 2008-04-21

Version: 2.1.3

Ownership: ITSO

Secretariat: Technology at ITSO

Project Editor: Mike Eastham

ITSO Technical Specification 1000-4 – Interoperable public transport ticketing using contactless smart customer media – Part 4: HOPS

ISBN: 978-0-9548042-3-7

"Published for the Department for Transport under licence from the Controller of Her Majesty's Stationery Office. The Department for Transport, its officials, Ministers and the Secretary of State for Transport do not guarantee the accuracy, completeness or usefulness of this information; and cannot accept liability for any loss or damages of any kind resulting from reliance on the information or guidance this document contains.

© Queen's Printer and Controller of Her Majesty's Stationery Office, 2008.

Copyright in the typographical arrangement and design rests with the Queen's Printer and Controller of Her Majesty's Stationery Office.

For any other use of this material please apply for a Click-Use Licence at www.opsi.gov.uk/click-use/index.htm, or by writing to the Licensing Enquiries, Information Policy Division, Office of Public Sector Information, St Clements House, 2-16 Colegate, Norwich NR3 1BQ, fax 01603 723000, or e-mail HMSOlicensing@cabinet-office.x.gsi.gov.uk.

This publication, excluding logos, may be reproduced free of charge in any format or medium for research, private study or for circulation within an organisation. This is subject to it being reproduced accurately and not used in a misleading context. The material must be acknowledged as copyright of the Queen's Printer and Controller of Her Majesty's Stationery Office, and the title of the publication specified."

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 7

1.1 Scope of Part 4..... 7

2. Host Operator or Processing System (HOPS) Overview..... 8

2.1 HOPS Components and Functions..... 8

2.2 HOPS configurations..... 10

2.3 HOPS functionality required by the Licensed Member roles..... 10

2.3.1 Shell Ownership 10

2.3.2 Shell Retailer 11

2.3.3 Collection and Forwarding 11

2.3.4 Product Ownership 12

2.3.5 Product Retailer 12

2.3.6 Service Operator..... 13

2.4 HOPS User Functions 13

2.5 HOPS data 14

3. Communications..... 15

3.1 External interfaces..... 15

3.2 Loss Less Communications..... 15

4. HSAM 16

5. The Message Store 17

6. Message Processor 18

6.1 Message Processor overview 18

6.1.1 General 18

6.1.2 Loss Less communication 18

6.1.3 Virtual Private Network (VPN) and Extensive Mark up Language (XML)..... 18

6.2 External entities..... 18

6.2.1 Point Of Service Terminals (POSTs)..... 18

6.2.2 Host Operator or Processing System (HOPS)..... 20

6.2.3 ITSO Security Management Service (ISMS)..... 22

6.3 Internal client components..... 23

6.3.1 Accounts.....23

6.3.2 Services24

6.3.3 AMS24

6.4 Internal resource components25

6.4.1 HSAM25

6.4.2 Message Store26

7. ITSO Shell Accounts (ISA) and ITSO Product Accounts (IPA)27

7.1 Account Types27

7.2 The ITSO Shell Account (ISA).....27

7.2.1 General.....27

7.2.2 Data requirements27

7.2.3 ISA History Data Store28

7.2.4 Managing the ITSO Shell Account (ISA).....29

7.3 ITSO Product Accounts (IPA).....29

7.3.1 Stored Travel Rights (STR) IPA; relating to IPE TYP 229

7.3.2 Charge To Account (CTA) IPA; relating to IPE TYPs 4 and 530

7.3.3 Loyalty IPA, relating to IPE TYPs 3 and 17.....31

7.3.4 ITSO ID IPA32

7.3.5 Entitlement IPA34

7.3.6 Ticket and Similar Product IPAs36

7.4 Account Processing39

7.4.1 User access to accounts39

7.4.2 General Account processing.....39

7.4.4 STR Auto-Top-Up operation39

7.4.5 STR Actionlist top up39

7.4.6 STR scheme exposure40

7.4.7 STR Negative Balance.....40

7.4.8 Handling STR Add-Value Records.....40

7.4.9 CTA IPA processing40

7.4.10 Auto-Renew40

7.5. List Processing40

7.5.1 Creating Lists.....41

7.5.2 Hotlists..... 41

7.5.3 Actionlists 42

7.6. Loyalty schemes..... 43

7.6.1 Loyalty scheme types 43

7.6.2 Loyalty scheme operation 43

7.6.3 Deferred Use Loyalty IPEs 44

7.7 IPE Embodiment Specifications..... 44

8. Asset Management System (AMS)..... 45

8.1 AMS overview 45

8.1.1 General 45

8.1.2 ISMS interface..... 45

8.2 Physical ISAM / HSAM..... 46

8.2.1 General 46

8.2.2 POST allocation 46

8.2.3 HOPS allocation..... 47

8.2.4 ISAM / HSAM state..... 47

8.2.5 ISAM / HSAM memory management..... 48

8.2.6 ISAM grouping 49

8.3 Centrally controlled Acceptance and Capability Criteria tables..... 50

8.4 Locally controlled Acceptance and Capability Criteria tables..... 51

8.4.1 ISAM Configuration 51

8.4.2 ISAM Groups 51

8.4.3 IPEs Accepted..... 52

8.4.4 Criteria 52

8.4.5 Limits List..... 53

8.5 POST stored POST configuration data 53

8.5.1 Products accepted 54

8.5.2 Peak times 54

8.5.3 Public holidays 54

8.5.4 Transfers 54

8.5.5 Rebates..... 54

8.5.6 Loyalty 54

8.5.7 Exchange rates54

8.5.8 Zones54

8.5.9 Sale price54

8.5.10 IIN index54

8.5.11 IPE Embodiment parameters.....55

8.6 AMS interfaces55

8.7 Functionality.....68

8.7.1 Installation / commissioning of ISAMs.....69

8.7.2 Create ISAM grouping69

8.7.3 Change ISAM grouping70

8.7.4 Take an ISAM out of service70

8.7.5 Reinstate an ISAM into service70

8.7.6 Make changes to ISAM Data.....71

8.7.7 Introduction of new product into scheme.....71

8.7.8 Withdrawal of a product.....71

8.7.9 Enabling of a new Customer Media platform72

8.7.10 Update of Directory keys by ITSO Registrar72

8.7.11 Update of Transaction keys by / HSAM Registrar72

8.7.12 Support of regular key rollover73

8.7.13 Removal of an ITSO member73

8.7.14 Change ISAM password parameters73

8.7.15 Change storage of transactions parameters73

9 Services74

9.1 Audit Trail74

9.2 Error Log.....74

9.3 Journal74

9.4 Query Facility74

9.5 ITSO Regulation Compliance Monitoring.....75

9.6 Security Monitoring75

9.7 User Access Control75

9.8 Data Backup and Archiving.....76

9.9 System Clock76

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 ITSO 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 4

This Part of the ITSO Specifications, ITSO TS 1000-4, defines the requirements of the ITSO Host Operator or Processing System (HOPS).

The HOPS modules described in this part are:

- HSAM;
- Message Store;
- Message Processing;
- Asset Management (AMS);
- ITSO Shell Accounts (ISA);
- Product Accounts;
- Services.

Only requirements that are pertinent to Interoperable Smart Customer Media (CM) usage and interfacing to other parts of the ITSO Environment are defined in this document. This document does not define non-ITSO requirements, many of which may be essential to procure a functional ticketing system.

2. Host Operator or Processing System (HOPS) Overview

A HOPS is defined as any entity where the ITSO data is processed, but excluding any entity which simply acts as a 'Store and Forward' node.

All HOPS shall contain the mandatory components defined in subsequent clauses, that is the HSAM, Message Processing function, Message Store and Services functions as shown in figure 1.

All ITSO Compliant Schemes shall provide all the components defined in subsequent clauses, as shown in figure 1, but not necessarily in the same HOPS.

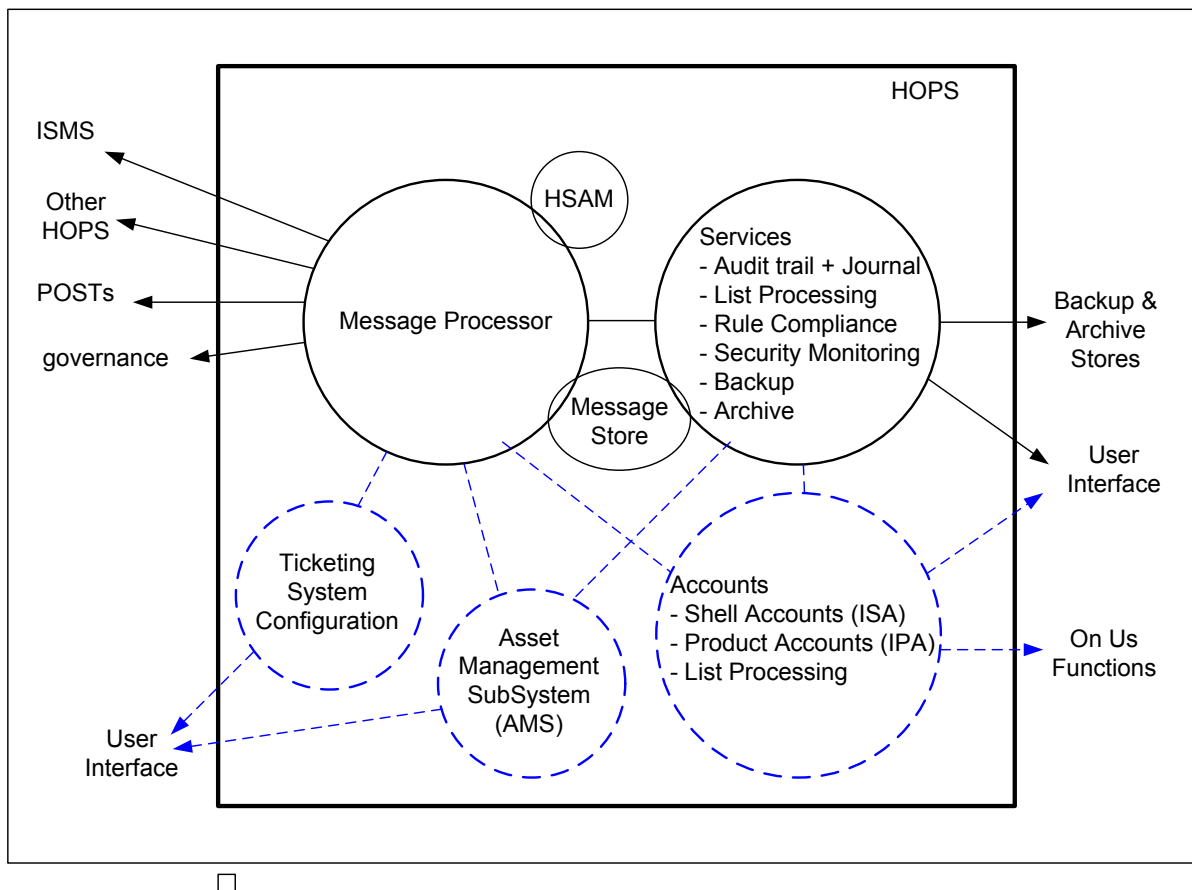


Figure 1 - HOPS overview

2.1 HOPS Components and Functions

The major components and functions of the HOPS are:-

HSAM

Message Store:

- Secure storage of all ITSO data messages transmitted and received;

Message Processing:

- Receiving and processing data and command messages from POSTs, ISMS and other HOPS;
- Sending data and command messages to POSTs, ISMS and other HOPS;

- Forwarding not-on-us transactions to other HOPS;
- HSAM interface;
- Passing received data to the HSAM for integrity checking;
- Passing data for transmission to the HSAM for signing;
- Managing the Loss Less transmission process in conjunction with the HSAM;
- Managing HSAM configuration;
- Handling ISAM configuration files;
- Making on-us data available to other HOPS functions;
- Storing all message data in the Message Store;

Asset Management (AMS):

- Recording status and disposition of all managed POSTs, ISAMs and HSAMs;
- Interface with the ISMS;
- Provision of ISMS generated configuration & key files to POST ISAMs;
- Provision of AMS generated configuration files to POST ISAMs;
- Management of ITSO Compliant Scheme POST configuration files;
- Managing ISAM acknowledgements destined for AMS or ISMS.

Accounts:

- ITSO Shell Accounts;
- ITSO Product Accounts;
- List Processing:
 - Hotlist Management;
 - Actionlist Management;

Services:

- Adding to and managing access to the audit trail and journal;
- Rule compliance monitoring;
- Security monitoring;
- Backup facilities;
- Archival facilities.

Ticketing System Configuration.

2.2 HOPS configurations

All HOPS shall contain the following mandatory components:

- Message Processing;
- Services;
- HSAM; and
- Message Store;

A HOPS may include the following optional components:

- AMS;
- Accounts;
- Ticketing System Configuration.

An individual ITSO Compliant Scheme may use a single HOPS, multiple HOPS or share capacity in a HOPS.

The optional AMS and Accounts components shall be provided in each and every ITSO Compliant Scheme.

2.3 HOPS functionality required by the Licensed Member roles

ITSO defines the following key functions that Licensed Members shall fulfil:

- Application Issuing
 - Shell Ownership
 - Shell Retailing
- Collection and Forwarding
- Product Ownership
- Product Retailing
- Service Operating

Each of the above will require the use¹ of a HOPS, although the configuration and feature set will differ as outlined below.

Note 1: The Shell Ownership and Shell Retailer roles defined in 2.3.1 and 2.3.2 are combined in the ITSO Business Rules into a single Application Issuing role.

Note 2: In some circumstances, a Licensed Member provides a HOPS which, of necessity, contains an HSAM but does not manage ISAMs for any other purpose. For example, this is the case for a Shell Owner who does not perform any other ITSO function. In these circumstances, the services of an AMS is required to manage the HSAM. Where the HOPS does not include this functionality, a commercial relationship is required with another Licensed Member who will provide the AMS functionality necessary to enable the HSAM.

2.3.1 Shell Ownership

The Shell Ownership function is defined as specifying the pricing, usage and commercial rules relating to the loading and use of Instances of a particular ITSO Shell.

¹ Either owner and operated by the Licensed Member, or provided in the form of a contracted service by a 3rd party to that Licensed Member.

In order to carry out the above function the Shell Owner shall be able to define and register the attributes of the Shell with the ITSO Registrar.

The Shell Owner shall maintain an ITSO Shell Account (ISA) for each instance of Shell issued.

The HOPS configuration as used by a Shell Owner shall include:

— HSAM	(Mandatory component);
— Message Store	(Mandatory component);
— Message Processing	(Mandatory component);
— Services	(Mandatory component);
— Asset Management (AMS)	For management of HSAMs only; ²
— ITSO Shell Accounts (ISA)	For management of instances of Shells issued
— ITSO Product Accounts (IPA)	Not required
— List processing	For management of instances of Shells issued

2.3.2 Shell Retailer

The Shell Retailer function is defined as loading Shell Instances onto Customer Media or issuing Customer Media to Customers, where the Media contains a Shell.

In order to carry out the above function the Shell Retailer shall require equipment to encode the Shell onto the media. This encoding equipment must contain an ISAM (i.e. the equipment shall be certified as a POST)

The Shell Retailer will obtain the required Shell embodiment parameters and security keys from the ISMS for which they are authorised by the Shell Owner.

The HOPS configuration as used by a Shell Retailer shall include:

— HSAM	(Mandatory component);
— Message Store	(Mandatory component);
— Message Processing	(Mandatory component);
— Services	(Mandatory component);
— Asset Management (AMS)	For management of HSAMs and ISAMs in encoding equipment only
— ITSO Shell Accounts (ISA)	Not required
— ITSO Product Accounts (IPA)	Not required
— List processing	For list management / targeting

2.3.3 Collection and Forwarding

The Collection and Forwarding function is defined as collecting Transaction Data relating to the loading or use of the Product Instances from Product Retailers and Service Operators, receiving Transaction Data from other Collection and Forwarding Operators including Shell, Product and security data, forwarding On Us Data to the relevant Product Owners and Not On Us Data to the relevant other Collection and Forwarding Operators.

² Shell Ownership, does not involve the more complex function of managing subservient ISAMs

In order to carry out the above function the Collection and Forwarding entity must receive and transmit ITSO messages from POSTs and other Collection and Forwarding entities. The handling of these messages has certain requirements to ensure that the end-to-end transmission is Loss-less.

The core functionality of a HOPS is the handling of ITSO messages. The HOPS configuration as used by a Collection and Forwarding entity shall include:

- HSAM (Mandatory component);
- Message Store (Mandatory component);
- Message Processing (Mandatory component);
- Services (Mandatory component);
- Asset Management (AMS) For management of HSAM(s) only³
- ITSO Shell Accounts (ISA) Not required
- ITSO Product Accounts (IPA) Not required
- List processing Not required

2.3.4 Product Ownership

The Product Ownership function is defined as specifying the pricing, usage and commercial rules relating to the loading and use of Product Instances of a particular ITSO Product.

In order to carry out the above function the Product Owner must be able to define and register the attributes of the product with the ITSO Registrar.

Note: The Product Owner shall define and register the applicable commercial arrangements between himself and Product Retailers / Service Operators in accordance with the ITSO Business Rules. The Product Owner shall maintain an ITSO Product Account (IPA) for each instance of product issued.

The HOPS configuration as used by a Product Owner shall include:

- HSAM (Mandatory component);
- Message Store (Mandatory component);
- Message Processing (Mandatory component);
- Services (Mandatory component);
- Asset Management (AMS) For management of HSAM(s) only⁴
- ITSO Shell Accounts (ISA) Not required
- ITSO Product Accounts (IPA) For management of instances of products issued
- List processing For management of instances of products issued

2.3.5 Product Retailer

The Product Retailer function is defined as loading Product Instances onto Media held by Customers.

³ Collection and Forwarding does not involve the more complex function of managing subservient ISAMs

⁴ Product Ownership does not involve the more complex function of managing subservient ISAMs

In order to carry out the above function the Product Retailer will require equipment to encode the IPE onto the media. This encoding equipment must contain an ISAM (i.e. the equipment shall be certified as a POST)

The Product Retailer will obtain the required IPE embodiment parameters and security keys from the ISMS for which they are authorised by the Product Owner.

The HOPS configuration as used by a Product Retailer shall include:

— HSAM	(Mandatory component);
— Message Store	(Mandatory component);
— Message Processing	(Mandatory component);
— Services	(Mandatory component);
— Asset Management (AMS)	For management of ISAMs in encoding equipment
— ITSO Shell Accounts (ISA)	Not required
— ITSO Product Accounts (IPA)	Not required
— List processing	For list management / targeting

2.3.6 Service Operator

The Service Operator function is defined as providing services to Customers who use the Product Instances loaded onto Media held by them as their entitlement to obtain such services .

In order to carry out the above function the Service Operator will require (POST) equipment to transact with the IPE held on the media. This equipment must contain an ISAM.

The Service Operator will obtain the required security keys from the ISMS.

The HOPS configuration as used by a Service Operator shall include:

— HSAM	(Mandatory component);
— Message Store	(Mandatory component);
— Message Processing	(Mandatory component);
— Services	(Mandatory component);
— Asset Management (AMS)	For management of ISAMs in POSTs
— ITSO Shell Accounts (ISA)	Not required
— ITSO Product Accounts (IPA)	Not required
— List processing	For list management / targeting

2.4 HOPS User Functions

The HOPS shall provide user access to HOPS functions to accomplish the following tasks:

- Enter Hotlist and Actionlist commands, compile and distribute to POSTs, Set up destinations for the lists;
- Amend ITSO Shell, ITSO Product Accounts (IPA) and associated Customer Media data as required to accomplish the functions described below, e.g. Auto-Top-Up levels;
- Create and maintain POST configuration data;

- Create, maintain and distribute local ITSO Compliant Scheme specific ISAM data using AMS secure messaging;
- Create and amend AMS data as subsequently described ;
- Other system configuration functions necessary for the correct operation of the HOPS, e.g. POST polling times, transaction processing run start times, etc;
- Action the AMS to send commands to ISMS, POSTs or other HOPS as required. Provide a facility to create ISAM scripts for the ISMS to send to ISAMs or HSAM;
- Run programs to examine message store records for integrity, validity, consistency, continuity or for unusual usage patterns;
- Search/Report on Message Store, Audit Trail, Journal, as described below:
- Set up and manipulate loyalty schemes;
- Set up and control the Charge to Account(CTA) accounts;
- Requesting allocation of ISAMs from the ISMS;
- Ad-hoc reporting on system health;
- Error reporting, viewing and administrative functions; and
- Ticketing system configuration.

The HOPS shall be able to allow or deny users access to these functions by using the permissions system described in subsequent clauses.

2.5 HOPS data

ITSO does not prescribe how the HOPS should store data, so each supplier may implement data stores appropriate to their needs⁵.

The HOPS shall provide and/or limit access to various data as described in subsequent clauses.

The HOPS shall meet all the requirements herein relating to data retention, data protection, data backup and data archiving.

Note: User functions need only be provided where the associated HOPS component is included in the implementation

⁵ For this reason, henceforth in this document the term 'data store' is used in preference to 'database'.

3. Communications

3.1 External interfaces

The HOPS shall interface to the following external components:

- The ISMS (if AMS functionality provided on this HOPS);
- POSTs;
- Intermediate nodes such as Depot or Station computers with which the HOPS must communicate in order to communicate with a remote POST;
- Other HOPS; and
- Any governance system mandated by the ITSO Operators Licence.

3.2 Loss Less Communications

All HOPS shall support 2-way loss-less communications with:

- POSTs
- Other HOPS
- The ISMS

The HOPS shall comply fully with the communications requirements defined in ITSO TS 1000-9.

4. HSAM ⁶

Every HOPS shall be fitted with an HSAM.

Each and every HSAM type or configuration shall be certified by ITSO as suitable for use in a HOPS.

Each HSAM shall be registered by the ITSO Security Management System (ISMS).

The OID data element within the HSAM ID shall be used to identify the HOPS in ITSO Application Messages generated by the HOPS to other nodes.

The format of the ISAM ID number is defined in ITSO TS 1000-2.

The HOPS shall provide a software interface to the HSAM.

The capability and use of the HSAM is defined in ITSO TS 1000-7 and ITSO TS 1000-8.

HSAMs shall always be installed in a Controlled Environment as defined in TS1000-9 clause 11.2.5.

The management of class 3 messages relating to the HSAM shall be identical to that defined for a POST ISAM, see TS 1000-3 clauses 6.3.7 and 6.3.8

⁶ Refer to ITSO TS 1000-1 for the definition of HSAM.

5. The Message Store

The HOPS shall include a Message Store.

The Message Store shall:

- Record in unaltered form all incoming and outgoing ITSO messages received or transmitted by the HOPS.
- The messages shall be stored in the format in which they are received, and, if received in a non-ITSO format shall also be stored in ITSO transmission format.
- Store all such messages for a minimum period of 2 years and 6 months from the commissioning date for any new HOPS and thereafter store all such messages for a minimum period of 1 year 4 months.
- Include a facility to search and report on the message store. Resultant data extracts shall be presented in XML to facilitate auditing.
- Be protected from any unauthorised addition, modification, renaming, moving or deletion.
- Be protected from unauthorised access of any kind.
- Message data shall be stored in non-volatile memory as immediately as reasonably practical, and in any event prior to handling of the next data message or within 2 seconds of completing transmission or reception of the message, whichever is the sooner.
- The message data store shall comprise two separate non-volatile memory devices, where each device duplicates the other, i.e. each data item shall be stored twice, once in each data storage device.

The Message Store data shall be included in the data set preserved by the HOPS backup and archive facilities.

The HOPS Message Store shall provide a search and reporting facility based on the categories described here individually or in combination:

- Date range;
- Originating device ISAMID or HSAM identity;
- ITSO message class;
- ITSO message code;
- Message direction;
- On-us or not-on-us.

6. Message Processor

The Message Processor is a mandatory component required in every instance of a HOPS.

6.1 Message Processor overview

6.1.1 General

The Message Processor handles all ITSO messaging between the HOPS and the following external entities:

- POSTs;
- HOPS;
- ISMS.

The Message Processor provides a service to the following internal components within a HOPS:

- Accounts;
- Services;
- AMS.

The Message Processor makes use of the services of the following components within the HOPS:

- HSAM;
- Message Store.

Clauses 6.2 to 6.4 define these interfaces and functions in detail.

6.1.2 Loss Less communication

All communications shall conform to the ITSO requirements for lossless data transfer. See ITSO TS 1000-9 for full details of this.

6.1.3 Virtual Private Network (VPN) and Extensive Mark up Language (XML)

All HOPS shall have the capability to communicate over a VPN running on the public Internet. This shall be used for communications to other HOPS and to the ISMS. A VPN may also be utilised for POST to HOPS, and HOPS to POST communications.

Data exchanged on the above link shall be formatted using XML and all HOPS shall support the use of both the full and the minimal tag set as defined in ITSO TS 1000-9.

6.2 External entities

6.2.1 Point Of Service Terminals (POSTs)

Communication with the POSTs under its control is a major role of the HOPS. The Message Processor shall handle these communications as defined in the following clauses.

6.2.1.1 Message format and transmission method

All HOPS shall support the generation and transmission of messages to POSTs in the ITSO transmission format defined in ITSO TS 1000-9.

All HOPS shall support the receiving and processing of messages from POSTs in the ITSO transmission format defined in ITSO TS 1000-9.

HOPS may support other message formats to POSTs in addition to the ITSO defined transmission format, provided said formats:

- Support the loss-less data transmission methodology defined in ITSO TS 1000-9;
- Allow the required data to be transmitted in a robust and secure manner;
- Allow the transmitted data to be fully recovered to its native format.

ITSO does not mandate the transmission method used between HOPS and POSTs / ticketing system. System designers may use any transmission method, provided said methods:

- Support the loss-less data transmission methodology defined in ITSO TS 1000-9;
- Allow the required data to be transmitted in a robust and secure manner;
- Allow the transmitted data to be fully recovered to its native format.

Note: It is the Licensed Member's responsibility to ensure the confidentiality of operational data passed between these nodes. The ITSO Specification does not provide for confidentiality of data messages, i.e. encryption is not specified, with the exception of the ISRN which is encrypted to prevent CM holder movement tracking. Therefore, Licensed Members must decide whether they need to make the messages confidential or not. If confidentiality is required, then the Licensed Member must provide another layer of protection.

6.2.1.2 Message set

The Message Handler shall support the following message set from a POST to a HOPS:

- Transfer of ACK2 positive acknowledgements Class 0;
- Transfer of NAK2 positive acknowledgements Class 0;
- Transfer of Transaction Record Data Messages Class 1;
- Transfer of Queries Class 2;
- Transfer of user defined Data Frames Class 2;
- Transfer of Miscellaneous Messages Class 2;
- Transfer of ISAM Security Acknowledgements Class 3.

The Message Handler shall support the following message set from a HOPS to a POST:

- Transfer of ACK1 positive acknowledgements Class 0;
- Transfer of NAK1 positive acknowledgements Class 0;
- Transfer of ACK2 positive acknowledgements Class 0;
- Transfer of NAK2 positive acknowledgements Class 0;
- Transfer of Query Responses Class 2;
- Transfer of POST Configuration Data Lists Class 2;
- Transfer of Parameter Tables Class 2;
- Transfer of user defined Data Frames Class 2;

- Transfer of Miscellaneous Messages Class 2;
- Transfer of ISAM Security Files Class 3.

See ITSO TS 1000-9 for details of the different message classes.

See ITSO TS 1000-6 for a detailed list of the messages and their message codes.

6.2.1.3 Message security

The Message Processor shall verify the authenticity and integrity of all received messages from a POST in the manner defined in ITSO TS 1000-9.

The Message Processor shall verify the authenticity and integrity of all received Data Frames from a POST in the manner defined in ITSO TS 1000-9. It shall use the services of the HSAM to carry out said verification.

The Message Processor shall seal all Data Frames sent to a POST in the manner defined in ITSO TS 1000-9. It shall use the services of the HSAM to carry out said sealing.

The Message Processor shall store a copy of each and every received message from a POST in the Message Store prior to any processing of said message.

The Message Processor shall store a copy of each and every transmitted message to a POST in the Message Store.

6.2.1.4 Positive acknowledgements and routing

The Message Processor shall generate the required positive acknowledgements to received messages / Data Frames from a POST. See ITSO TS 1000-9 for details of the positive acknowledgement process.

The Message Processor shall re-transmit messages to the POST when a valid ACK is not received within the required period as defined in ITSO TS 1000-9.

The Message Processor shall route (forward on) messages received from a POST that it is not authorised to process. Said routing shall be in the manner defined in ITSO TS 1000-9.

6.2.1.5 Enveloping

The Message Processor shall support the enveloping of received messages / Data Frames from a POST. See ITSO TS 1000-9 for details of the enveloping process.

6.2.1.6 Transaction Session Batch management

The Message Processor shall manage the 'closing' and acknowledging of Transaction Session Batches as defined in ITSO TS 1000-9.

6.2.2 Host Operator or Processing System (HOPS)

To achieve interoperability, ITSO have defined an architecture whereby HOPS shall be able to exchange required data with other HOPS on a peer-to-peer basis. The Message Processor shall handle this communication as defined in the following clauses.

6.2.2.1 HOPS to HOPS Message format and transmission method

All HOPS shall support the generation and transmission of messages to HOPS in the ITSO transmission format defined in ITSO TS 1000-9.

All HOPS shall support the receiving and processing of messages from HOPS in the ITSO transmission format defined in ITSO TS 1000-9.

All HOPS shall support the generation and transmission of XML tagged message files as defined in ITSO TS 1000-9.

All HOPS shall support the receiving and processing of XML tagged message files as defined in ITSO TS 1000-9.

HOPS may support other inter-HOPS message formats in addition to the XML tagged and ITSO defined transmission formats provided said formats:

- Support the loss-less data transmission methodology defined in ITSO TS 1000-9;
- Allow the required data to be transmitted in a robust and secure manner;
- Allow the transmitted data to be fully recovered to its native format.

All HOPS shall provide support for transmission and receipt of message files via a VPN as defined in ITSO TS 1000-9.

HOPS may support other message file transmission methods in addition to the VPN, provided said methods:

- Support the loss-less data transmission methodology defined in ITSO TS 1000-9;
- Allow the required data to be transmitted in a robust and secure manner;
- Allow the transmitted data to be fully recovered to its native format.

6.2.2.2 Message set

The Message Handler shall support the following inter-HOPS message set:

- | | |
|--|----------|
| — Transfer of ACK2 positive acknowledgements | Class 0; |
| — Transfer of NAK2 positive acknowledgements | Class 0; |
| — Transfer of Queries | Class 2; |
| — Transfer of Query Responses | Class 2; |
| — Transfer of POST Configuration Data Lists | Class 2; |
| — Transfer of Parameter Tables | Class 2; |
| — Transfer of Data Correction Records | Class 2; |
| — Transfer of Envelop Frames | Class 2; |
| — Transfer of user defined Data Frames | Class 2; |
| — Transfer of Miscellaneous Messages | Class 2; |
| — Transfer of ISAM Security Files | Class 3; |
| — Transfer of ISAM Security Acknowledgements | Class 3. |

See ITSO TS 1000-9 for details of the different message classes.

See ITSO TS 1000-6 for a detailed list of the messages and their message codes.

6.2.2.3 Message security

The Message Processor shall verify the authenticity and integrity of all received messages from a HOPS in the manner defined in ITSO TS 1000-9.

The Message Processor shall verify the authenticity and integrity of all received Data Frames from a HOPS in the manner defined in ITSO TS 1000-9. It shall use the services of the HSAM to carry out said verification.

The Message Processor shall seal all Data Frames sent to a HOPS in the manner defined in ITSO TS 1000-9. It shall use the services of the HSAM to carry out said sealing.

The Message Processor shall store a copy of each and every received message from a HOPS in the Message Store prior to any processing of said message.

The Message Processor shall store a copy of each and every transmitted message to a HOPS in the Message Store.

6.2.2.4 Positive acknowledgements and routing

The Message Processor shall generate the required positive acknowledgements to received messages / Data Frames from a HOPS. See ITSO TS 1000-9 for details of the positive acknowledgement process.

The Message Processor shall re-transmit messages to the (external) HOPS when a valid ACK is not received within the required period. This re-transmission shall be as defined in ITSO TS 1000-9.

The Message Processor shall route (forward on) messages received from a HOPS that it is not authorised to process. Said routing shall be in the manner defined in ITSO TS 1000-9.

6.2.2.5 Enveloping

The Message Processor shall support the enveloping of received messages / Data Frames from a HOPS. See ITSO TS 1000-9 for details of the enveloping process.

6.2.3 ITSO Security Management Service (ISMS)

The AMS function within a HOPS is required to interface to the central ISMS system via VPN over the public Internet, using XML formatted files. The Message Processor shall handle this communication as defined in the following clauses.

6.2.3.1 Message format and transmission method

All HOPS shall support the generation and transmission of messages to the ISMS in the ITSO transmission format defined in ITSO TS 1000-9.

All HOPS shall support the receiving and processing of messages from the ISMS in the ITSO transmission format defined in ITSO TS 1000-9.

All HOPS shall support the generation and transmission of XML tagged message files as defined in ITSO TS 1000-9.

All HOPS shall support the receiving and processing of XML tagged message files as defined in ITSO TS 1000-9.

All HOPS shall provide support for transmission and receipt of message files via a VPN as defined in ITSO TS 1000-9.

6.2.3.2 Message set

The Message Handler shall support the following message set from ISMS to HOPS:

- Transfer of ISAM Security Files Class 3;
- Transfer of ISMS-AMS Information Packet Class 2.

The Message Handler shall support the following message set from HOPS to ISMS:

- Transfer of ISMS Security Requests Class 3;
- Transfer of ISMS Information Request Class 2;
- Transfer of ISAM Security Acknowledgements Class 3.

See ITSO TS 1000-9 for details of the different message classes.

See ITSO TS 1000-8 for a detailed list of the messages and their message codes.

6.2.3.3 Message security

The Message Processor shall verify the authenticity and integrity of all received messages from the ISMS in the manner defined in ITSO TS 1000-9.

The Message Processor shall verify the authenticity and integrity of all received Secure Data Frames from the ISMS in the manner defined in ITSO TS 1000-9. It shall use the services of the HSAM to carry out said verification.

The Message Processor shall seal all Secure Data Frames sent to the ISMS in the manner defined in ITSO TS 1000-9. It shall use the services of the HSAM to carry out said sealing.

The Message Processor shall store a copy of each and every received message from the ISMS in the Message Store prior to any processing of said message.

The Message Processor shall store a copy of each and every transmitted message to the ISMS in the Message Store.

6.2.3.4 Positive acknowledgements and routing

The Message Processor shall generate the required positive acknowledgements to received messages / Data Frames from the ISMS. See ITSO TS 1000-9 for details of the positive acknowledgement process.

The Message Processor shall re-transmit messages to the ISMS when a valid ACK is not received within the required period as defined in ITSO TS 1000-9.

The Message Processor shall route (forward on) messages received from the ISMS that it is not authorised to process. Said routing shall be in the manner defined in ITSO TS 1000-9.

6.3 Internal client components

6.3.1 Accounts

6.3.1.1 Message Processor to Accounts

The Message Processor shall transfer relevant received and verified 'on-us' data to the following Accounts sub-systems:

- ITSO Shell Accounts;
- Product Accounts.

Verified 'on-us' data will result from reception (by the Message Processor) of the following message types from POSTs and/or HOPS:

- Class 1 Transaction Record Data Messages;
- Class 2 Envelop Frames;
- Class 2 Data Correction Records;
- Class 2 Queries.

Class 1 Transaction Records will usually be the main source of this data, originating from POSTs which are 'directly under' the HOPS in question.

Class 2 Envelop Frames will be the source of data when the data from the POST has had to be routed via another HOPS (i.e. the HOPS in question is not the 'first-line' HOPS for the POST). In effect the intermediate HOPS has treated said data as a 'not-on-us' transaction.

Class 2 Data Correction Records are used to allow corrections to stored entities by external parties.

Class 2 Queries do not provide data that is stored by the Account sub-systems, but acts as a request for already stored data.

6.3.1.2 Accounts to Message Processor

The Message Processor shall accept, seal and transmit out data from the following Accounts sub-systems:

- ITSO Shell Accounts;
- Product Accounts;
- List Processing.

The Message Processor shall generate one or more of the following message types to POSTs and/or HOPS as a result:

- Class 2 Configuration Data Lists;
- Class 2 Query Responses.

Class 2 Configuration Data Lists are sent to POSTs by the HOPS. The current configuration lists are: Hotlist; Actionlist.

Class 2 Query Responses contain the data requested by a Query message previously received.

6.3.2 Services

The Message Processor shall provide the required information to the Services component such that said component can carry out its required tasks.

The Message Processor shall monitor and record relevant Quality of Service metrics relating to its internal tasks, and shall make these available to the Services component as required.

6.3.3 AMS

6.3.3.1 Message Processor to AMS

The Message Processor shall transfer relevant received and verified 'on-us' data to the AMS component. This data will result from reception (by the Message Processor) of the following message types from POSTs, HOPS and the ISMS:

- Class 2 ISMS-AMS Information Packet;
- Class 3 ISAM Security Acknowledgements;
- Class 3 ISAM Security Files from the ISMS.

Class 2 ISMS-AMS Information Packets are originated by the ISMS and are used to provide informative data to the AMS.

Class 3 ISAM Security Acknowledgements are originated by an ISAM (in a managed POST) or an HSAM (in a managed HOPS) in response to a Security File.

Class 3 ISAM Security Files are originated by the ISMS at the request of the AMS for inclusion in an AMS message destined for a target ISAM or HSAM.

Note: ISAM Security Files sent by the ISMS to the local HSAM shall be directly applied to the local HSAM along with any other necessary AMS generated Security Files.

6.3.3.2 AMS to Message Processor

The Message Processor shall accept, seal and transmit out data from the AMS component. The Message Processor shall generate one or more of the following message types to as a result:

- Class 2 Parameter Tables;
- Class 2 ISMS Information Request;
- Class 3 ISMS Security Requests;
- Class 3 ISAM Security Files
- Class 3 ISAM Security Acknowledgements.

Class 2 Parameter Tables are sent from the AMS to managed POSTs. These tables make up the POST configuration data.

Class 2 ISMS Information Requests are sent from the AMS to the ISMS to request data that is not security related.

Class 2 ISMS Security Requests are sent from the AMS to the ISMS to request security related data.

Class 3 ISAM Security files are sent from the AMS to ISAMs in managed POSTs and HOPS to configure locally controlled tables. As part of this process any Security Files originated by the ISMS shall be re-packaged by the AMS into a class 3 message that contains, in the correct order for application to the target ISAM or HSAM, all the Secure Data Frames need to complete a single self contained update to the target. The class 3 message Originator shall be the AMS.

Note: To fulfil the above requirement, Secure Data Frames sourced by AMS are likely to be interleaved with Secure Data Frames sourced by the ISMS. The first Secure Data Frame in the message shall be the first to be applied to the ISAM followed by the next etc....until the Last frame in the message has been applied.

Class 3 ISAM Security Acknowledgements received from a POST or HOPS in a single message may contain acknowledgements destined for the AMS or the ISMS or Both. These shall be filtered by the AMS process and those intended for the AMS processed directly by the AMS. Those intended for ISMS may be inspected as required by an AMS process and shall then be repackaged into a single Class 3 message for forwarding to the ISMS. In this case the class 3 message originator shall be the AMS.

Note: It is recommended that the digital signature of any ISMS Security Acknowledgements inspected by the AMS is verified prior to using any of its contents.

6.3.3.3 AMS - HSAM data transfer

Data transfer between the AMS and the local HSAM shall take place via the Message Processor.

6.4 Internal resource components

6.4.1 HSAM

The Message Processor shall use the services of the local HSAM to:

- Seal Data Frames;
- Seal Secure Data Frames;
- Verify the Seal on Data Frames;
- Generate the IBatch Header delete parameters for Transaction Session Batch management.

6.4.2 Message Store

The Message Processor shall store a copy of each and every incoming message in the Message Store prior to any processing. Each stored message shall be timestamped with its reception time and date.

The Message Processor shall store a copy of each and every transmitted message in the Message Store. Each stored message shall be timestamped with its transmission time and date.

7. ITSO Shell Accounts (ISA) and ITSO Product Accounts (IPA)

This clause defines requirements for the following:

- ITSO Shell Accounts (ISA) which relate to ITSO Shells;
- ITSO Product Accounts (IPA) which relate to ITSO Product Entities (IPE) instances;
- Account processing;
- List processing facilities:
 - Hotlists;
 - Actionlists.

Provision of the facilities defined in this clause is optional in a HOPS instance. It should be noted that only those facilities defined in this clause relevant to a HOPS instance need be provided in that instance.

Each ITSO Compliant Scheme shall include at least one HOPS capable of providing the account management functions defined in this clause.

The account definitions herein are based on the ITSO Transaction Record messages defined in ITSO TS 1000-6. Each data element within an account shall be formatted such that the full value range of any matching parameter in a Transaction Record message may be stored in the account.

7.1 Account Types

The HOPS shall keep each account as a logical copy of the corresponding data in the ITSO Shell or IPE instance as appropriate, together with any other relevant data.

There is no direct link between products (IPE instances) and ITSO Shells. There is however a link between Actors: the Product Owners and ITSO Shell Owners.

7.2 The ITSO Shell Account (ISA)

7.2.1 General

The ITSO Shell Owner shall maintain an ISA for each ITSO Shell issued by them.

The ISA shall store information about the ITSO Shell.

In the instance where a Customer Media is issued containing a single product in a Compact Shell⁷, creation of an ISA is optional.

7.2.2 Data requirements

An ISA shall comprise the following data elements, and may additionally contain additional data elements at the discretion of the HOPS owner:

- The entire data set returned in Transaction Records relating to ITSO Shell creation, message codes 0001 and 0003, and stored as individual data elements;
- The entire data set returned in Transaction Records relating to acceptance of a deposit for the ITSO Shell, message code 0302, and stored as individual data elements;

⁷ Refer to ITSO TS 1000-2 for a definition of Compact Shells.

- Status, which shall be used to record the status of the ITSO Shell, where the following status conditions shall be recorded:
 - ITSO Shell Issued but not activated;
 - ITSO Shell Issued and activated;
 - ITSO Shell dormant;
 - ITSO Shell Hotlisted;
 - ITSO Shell Blocked;
 - ITSO Shell deleted from host Customer Media;
 - Host Customer Media unavailable (i.e. the host Customer Media has been destroyed⁸, Blocked or otherwise disabled);
- HotlistStatus, which shall be used to record the Hotlist status of the ITSO Shell, where the following status conditions shall be recorded:
 - Not Hotlisted;
 - Lost;
 - Stolen;
 - ITSO Shell Holder Rule Breach (the CM holder has breached one of the Shell Owners rules);
 - ITSO Shell Owner Rule Breach (the Shell Owner has withdrawn the Shell for administrative reasons);
 - Security Rule Breach (the Shell Owner has Hotlisted the Shell because a security rule has been breached);
- HotlistAction, which shall be used to record the action to take recorded in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- Customer Media Disposition, which shall be used to record the Customer Media disposition instruction contained in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- Cross Reference to ISA History Data Store.

The Status and HotlistStatus elements shall be updated either upon receipt of the appropriate data message from a POST, or upon operation of a manually operated control indicating a change in status.

7.2.3 ISA History Data Store

Associated with the ITSO Shell ISA shall be an ISA History Data Store. This store shall contain summary details of each IPE written to that ITSO Shell.

An ISA History Data Store shall comprise of the following data elements:

- Cross reference to the ISA;
- The entire data set returned in Transaction Records relating to creation, amendment and deletion of IPE instances, message codes 0005, 0006, 0007, 0008, 0009, and stored as individual data elements;
- Status which shall be used to record the status of the IPE instance, where the following status conditions shall be recorded:

⁸ It is recommended that the destruction process should be an auditable process.

- IPE instance created but not activated;
- IPE instance created and activated;
- IPE instance dormant;
- IPE instance Hotlisted; and
- IPE instance deleted from ITSO Shell.

7.2.4 Managing the ITSO Shell Account (ISA)

The HOPS shall maintain the ISA ensuring that all Transaction Records relating to the ITSO Shell shall be used to promptly update ISA data elements as appropriate.

The HOPS shall maintain the ISA History Data Store by promptly adding to it or updating it as appropriate upon receipt of Transaction Records from POSTs.

7.3 ITSO Product Accounts (IPA)

The HOPS shall create and maintain IPAs for all IPE instances issued under the authority of and controlled by the Product Owner HOPS.

The HOPS shall promptly create, add to or update IPAs upon receipt of Transaction Records from POSTs.

Only relevant Product Account types need be implemented in an ITSO Compliant Scheme, i.e., only Product Account types which will be used by the HOPS Owner need be implemented.

7.3.1 Stored Travel Rights (STR) IPA; relating to IPE TYP 2

The STR IPA shall comprise the following data elements, and may additionally contain additional data elements at the discretion of the HOPS owner:

- The entire data set returned in Transaction Records relating to TYP 2 IPE instance creation, message code 0120, and stored as individual data elements;
- Status, which shall be used to record the status of the IPE instance, where the following status conditions shall be recorded:
 - IPE instance Issued but not activated;
 - IPE instance Issued and activated;
 - IPE instance MaxAmount exceeded;
 - IPE instance Value is zero;
 - IPE instance Value is negative;
 - IPE instance dormant;
 - IPE instance Hotlisted;
 - IPE instance Blocked;
 - IPE instance deleted from the ITSO Shell;
 - Host unavailable (i.e. the host Customer Media has been destroyed, Hotlisted or otherwise disabled).
- HotlistStatus, which shall be used to record the Hotlist status of the IPE Instance, where the following status conditions shall be recorded:

- Not Hotlisted;
- Lost;
- Stolen;
- IPE instance Holder Rule Breach (the CM holder has breached one of the IPE Owners rules);
- IPE instance Owner Rule Breach (the IPE Owner has withdrawn the IPE for administrative reasons);
- Security Rule Breach (the IPE Owner has Hotlisted the IPE because a security rule has been breached);
- HotlistAction, which shall be used to record the action to take recorded in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- Customer Media Disposition, which shall be used to record the Customer Media disposition instruction contained in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- IPE instance Holder information where the STR IPE instance owner is not also the ITSO ID IPE instance owner;
- IPE instance Holders bank or credit card details where appropriate;
- Cross reference to a History Data Store.

The History Data Store shall contain a record of all transactions conducted with the STR IPE instance, and shall be updated promptly upon receipt of transaction records from POSTs. The History Data Store shall comprise of all the data elements defined in the TYP 2 Value Record Group as defined in ITSO TS 1000-5, together with details of any other changes, the location at which the changes were conducted and the operator responsible for the changes.

Upon receipt of a 0103 Load Check transaction record, the HOPS shall check whether a record of this Transaction has already been stored in the IPA. If a record has already been stored then the 0103 message shall be discarded and no further action taken. If a record has not been stored then the HOPS shall make a record in the IPA history store using the information contained in the 0103 message, and the event logged for the attention of the system operator. If subsequently a 0101 or 0102 message relating to the same Transaction is received, this shall be used to update the IPA with those data elements not contained in the 0103 message, and a new IPA record shall not be created. When an 0101 or an 0102 message is received the HOPS shall, before processing it, check whether an 0103 message relating to the same transaction has already been received and processed.

The Status and HotlistStatus elements shall be updated either upon receipt of the appropriate data message from a POST, or upon operation of a manually operated control indicating a change in status.

7.3.2 Charge To Account (CTA) IPA; relating to IPE TYPs 4 and 5

Two forms of CTA IPA shall be provided, reflecting the differences between TYP 4 and TYP 5 IPE's.

The CTA IPA shall comprise the following data elements, and may additionally contain additional data elements at the discretion of the HOPS owner:

- The entire data set returned in Transaction Records relating to TYP 4 IPE instance creation or TYP 5 IPE instance creation, message codes 0122 and 0124, and stored as individual data elements;
- Status, which shall be used to record the status of the IPE instance, where the following status conditions shall be recorded:
 - IPE instance Issued but not activated;
 - IPE instance Issued and activated;
 - IPE instance MaxAmount exceeded;
 - IPE instance dormant;

- IPE instance Hotlisted;
- IPE instance Blocked;
- IPE instance deleted from the ITSO Shell;
- Host unavailable (i.e. the host Customer Media has been destroyed, Hotlisted or otherwise disabled).
- HotlistStatus, which shall be used to record the Hotlist status of the IPE Instance, where the following status conditions shall be recorded:
 - Not Hotlisted;
 - Lost;
 - Stolen;
 - IPE instance Holder Rule Breach (the CM holder has breached one of the IPE Owners rules);
 - IPE instance Owner Rule Breach (the IPE Owner has withdrawn the IPE for administrative reasons);
 - Security Rule Breach (the IPE Owner has Hotlisted the IPE because a security rule has been breached);
- HotlistAction, which shall be used to record the action to take recorded in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- Customer Media Disposition, which shall be used to record the Customer Media disposition instruction contained in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- IPE instance Holder information where the CTA IPE instance owner is not also the ITSO ID IPE instance owner;
- IPE instance Holders bank or credit card details;
- Normal refresh location⁹;
- Cross reference to a History Data Store.

The History Data Store shall contain a record of all transactions conducted with the associated CTA IPE instance, and shall be updated promptly upon receipt of transaction records from POSTs. The History Data Store shall comprise of all the data elements defined in the TYP 4 Value Record Group or the TYP 5 Value Record Group as defined in ITSO TS 1000-5, together with details of any other changes, the location at which the changes were conducted and the operator responsible for the changes.

The Status and HotlistStatus elements shall be updated either upon receipt of the appropriate data message from a POST, or upon operation of a manually operated control indicating a change in status.

7.3.3 Loyalty IPA, relating to IPE TYPs 3 and 17

The loyalty IPA shall comprise the following data elements, and may additionally contain additional data elements at the discretion of the HOPS owner:

- The entire data set returned in Transaction Records relating to IPE instance creation, message codes 020B or 0206, and stored as individual data elements;
- The entire data set returned in Transaction Records relating to IPE instance use, message codes 0203, 0204 or 0205, and stored as individual data elements;

⁹ A location at which the IPE user normally presents the card in order for an Actionlist item to be actioned by means of which the IPE's MaximumAmount data element is reset to reflect a payment made by the IPE user to settle the account.

- Status, which shall be used to record the status of the IPE instance, where the following status conditions shall be recorded:
 - IPE instance Issued but not activated;
 - IPE instance Issued and activated;
 - IPE instance MaxAmount exceeded;
 - IPE instance dormant;
 - IPE instance Hotlisted;
 - IPE instance Blocked;
 - IPE instance deleted from the ITSO Shell;
 - Host unavailable (i.e. the host Customer Media has been destroyed, Hotlisted or otherwise disabled);
- HotlistStatus, which shall be used to record the Hotlist status of the IPE Instance, where the following status conditions shall be recorded:
 - Not Hotlisted;
 - Lost;
 - Stolen;
 - IPE instance Holder Rule Breach (the CM holder has breached one of the IPE Owners rules);
 - IPE instance Owner Rule Breach (the IPE Owner has withdrawn the IPE for administrative reasons);
 - Security Rule Breach (the IPE Owner has Hotlisted the IPE because a security rule has been breached);
- HotlistAction, which shall be used to record the action to take recorded in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- Customer Media Disposition, which shall be used to record the Customer Media disposition instruction contained in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- IPE instance Holder information where the CTA IPE instance owner is not also the ITSO ID IPE instance owner;
- Cross reference to a History Data Store.

The History Data Store shall contain a record of all transactions conducted with the associated Loyalty IPE instance, and shall be updated promptly upon receipt of transaction records from POSTs.

Where the IPA relates to a TYP 3 IPE instance, the History Data Store shall comprise of all the data elements defined in the TYP 3 Value Record Group as defined in ITSO TS 1000-5, together with details of any other changes, the location at which the changes were conducted and the operator responsible for the changes.

Where the IPA relates to a TYP 17 IPE instance, the History Data Store shall comprise the date and time of the transaction; number of loyalty points, and any other information that the IPE instance owner wishes to store, together with details of any other changes, the location at which the changes were conducted and the operator responsible for the changes.

The Status and HotlistStatus elements shall be updated either upon receipt of the appropriate data message from a POST, or upon operation of a manually operated control indicating a change in status.

7.3.4 ITSO ID IPA

The IPA shall comprise the following data elements, and may additionally contain additional data elements at the discretion of the HOPS owner:

- The following data elements returned in Transaction Records relating to IPE instance creation, message code 0200, and stored as individual data elements;
 - StandardData (stored as individual data elements);
 - Amount;
 - AmountCurrencyCode;
 - HolderTitle;
 - HolderSurname;
 - HolderOtherNames;
 - HolderAddress1;
 - HolderAddress2;
 - HolderAddress3;
 - HolderAddress4;
 - HolderPostcode;
 - HolderPhoneDay;
 - HolderPhoneHome;
 - HolderPhoneMobile;
 - HolderEmail;
 - IPELength;
 - IPEBitMap;
 - IPEFormatRevision;
 - RemoveDate;
 - ProductRetailer;
 - IDFlags;
 - PassbackTime;
 - DateOfBirth;
 - Language;
 - HolderID;
 - DepositMethodOfPayment;
 - DepositVATSalesTax;
 - DepositCurrencyCode;
 - DepositAmount;

- Status, which shall be used to record the status of the IPE instance, where the following status conditions shall be recorded:
 - IPE instance Issued but not activated;
 - IPE instance Issued and activated;
 - IPE instance MaxAmount exceeded;
 - IPE instance dormant;
 - IPE instance Hotlisted;
 - IPE instance Blocked;
 - IPE instance deleted from the ITSO Shell;
 - Host unavailable (i.e. the host Customer Media has been destroyed, Hotlisted or otherwise disabled);
- HotlistStatus, which shall be used to record the Hotlist status of the IPE Instance, where the following status conditions shall be recorded:
 - Not Hotlisted;
 - Lost;
 - Stolen;
 - IPE instance Holder Rule Breach (the CM holder has breached one of the IPE Owners rules);
 - IPE instance Owner Rule Breach (the IPE Owner has withdrawn the IPE for administrative reasons);
 - Security Rule Breach (the IPE Owner has Hotlisted the IPE because a security rule has been breached);
- HotlistAction, which shall be used to record the action to take recorded in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- Customer Media Disposition, which shall be used to record the Customer Media disposition instruction contained in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- IPE instance Holder information where the CTA IPE instance owner is not also the ITSO ID IPE instance owner;
- Cross reference to a History Data Store.

The History Data Store shall provide a trail of all changes to the IPE instance and IPA, including the date & time of said changes, the nature of said changes and the location and operator ID responsible for the change.

The History Data Store shall contain a record of all transactions conducted with the associated ITSO ID IPE instance, and shall be updated promptly upon receipt of transaction records from POSTs.

The Status and HotlistStatus elements shall be updated either upon receipt of the appropriate data message from a POST, or upon operation of a manually operated control indicating a change in status.

7.3.5 Entitlement IPA

The IPA shall comprise the following data elements, and may additionally contain additional data elements at the discretion of the HOPS owner:

- The following data elements returned in Transaction Records relating to IPE instance creation, message code 0200, and stored as individual data elements;
 - StandardData – stored as individual data elements;

- Amount;
- AmountCurrencyCode;
- HolderTitle;
- HolderSurname;
- HolderOtherNames;
- HolderAddress1;
- HolderAddress2;
- HolderAddress3;
- HolderAddress4;
- HolderPostcode;
- HolderPhoneDay;
- HolderPhoneHome;
- HolderPhoneMobile;
- HolderEmail;
- IPE-TYP;
- IPELength;
- IPEBitMap;
- IPEFormatRevision;
- RemoveDate;
- ProductRetailer;
- ConcessionaryPassIssuerCostCentre;
- IDFlags;
- PassbackTime;
- DateOfBirth;
- Language;
- HolderID;
- RoundingFlag;
- RoundingValueFlag;
- EntitlementExpiryDate;
- DepositMethodOfPayment;
- DepositVATSalesTax;

- DepositCurrencyCode;
- DepositAmount;
- ConcessionaryClass;
- Status, which shall be used to record the status of the IPE instance, where the following status conditions shall be recorded:
 - IPE instance Issued but not activated;
 - IPE instance Issued and activated;
 - IPE instance MaxAmount exceeded;
 - IPE instance dormant;
 - IPE instance Hotlisted;
 - IPE instance Blocked;
 - IPE instance deleted from the ITSO Shell;
 - Host unavailable (i.e. the host Customer Media has been destroyed, Hotlisted or otherwise disabled);
- HotlistStatus, which shall be used to record the Hotlist status of the IPE Instance, where the following status conditions shall be recorded:
 - Not Hotlisted;
 - Lost;
 - Stolen;
 - IPE instance Holder Rule Breach (the CM holder has breached one of the IPE Owners rules);
 - IPE instance Owner Rule Breach (the IPE Owner has withdrawn the IPE for administrative reasons);
 - Security Rule Breach (the IPE Owner has Hotlisted the IPE because a security rule has been breached);
- HotlistAction, which shall be used to record the action to take recorded in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- Customer Media Disposition, which shall be used to record the Customer Media disposition instruction contained in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- IPE instance Holder information where the CTA IPE instance owner is not also the ITSO ID IPE instance owner;
- Cross reference to a History Data Store.

The History Data Store shall provide a trail of all changes to the IPE instance and IPA, including the date & time of said changes, the nature of said changes and the location and operator ID responsible for the change.

The Status and HotlistStatus elements shall be updated either upon receipt of the appropriate data message from a POST, or upon operation of a manually operated control indicating a change in status.

7.3.6 Ticket and Similar Product IPAs

This IPA shall be used to store details of ticketing and other similar products created using IPE's, where creation of such IPE instances is reported using code 207 messages. It should be noted that the data set returned in the code 0207 messages will vary according to the IPE TYP created

The IPA shall comprise the following data elements, and may additionally contain additional data elements at the discretion of the HOPS owner:

- The entire data set returned in Transaction Records relating to IPE instance creation, message code 0207, and stored as individual data elements.
- Status, which shall be used to record the status of the IPE instance, where the following status conditions shall be recorded:
 - IPE instance Issued but not activated;
 - IPE instance Issued and activated;
 - IPE instance MaxAmount exceeded;
 - IPE instance dormant;
 - IPE instance Hotlisted;
 - IPE instance Blocked;
 - IPE instance deleted from the ITSO Shell;
 - Host unavailable (i.e. the host Customer Media has been destroyed, Hotlisted or otherwise disabled);
- HotlistStatus, which shall be used to record the Hotlist status of the IPE Instance, where the following status conditions shall be recorded:
 - Not Hotlisted;
 - Lost;
 - Stolen;
 - IPE instance Holder Rule Breach (the CM holder has breached one of the IPE Owners rules);
 - IPE instance Owner Rule Breach (the IPE Owner has withdrawn the IPE for administrative reasons);
 - Security Rule Breach (the IPE Owner has Hotlisted the IPE because a security rule has been breached);
- HotlistAction, which shall be used to record the action to take, recorded in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6.
- Customer Media Disposition, which shall be used to record the Customer Media disposition instruction contained in a Hotlist item associated with this ITSO Shell, as defined in ITSO TS 1000-6;
- IPE instance Holder information where the CTA IPE instance owner is not also the ITSO ID IPE instance owner.
- IPE instance Holders bank or credit card details.
- Normal refresh location¹⁰.
- Cross reference to a History Data Store.

The History Data Store shall contain a record of all transactions conducted with the associated IPE instance, and shall be updated promptly upon receipt of transaction records from POSTs. The History Data Store shall comprise of all the data elements defined in the relevant Value Record Group as defined in ITSO TS 1000-5, together with

¹⁰ A location at which the IPE user normally presents the card in order for an Actionlist item to be actioned by means of which the IPE's MaximumAmount data element is reset to reflect a payment made by the IPE user to settle the account.

details of any other changes, the location at which the changes were conducted and the operator responsible for the changes.

The Status and HotlistStatus elements shall be updated either upon receipt of the appropriate data message from a POST, or upon operation of a manually operated control indicating a change in status.

7.4 Account Processing

7.4.1 User access to accounts

The HOPS shall provide user access to accounts and the list processing facility subject to the data access permissions configured for each user.

7.4.2 General Account processing

The HOPS shall receive transaction record messages pertaining to the creation, deletion, Hotlisting, modification, and usage of IPE instances, and shall use the data elements in said messages to promptly update related IPAs, the IPA history store, and the ITSO Shell ISA where required.

The HOPS shall maintain ISAs until after the archive action following either:

- The ITSO Shell ExpiryDate; or
- the CM in which the Shell resides has been destroyed¹¹, and the ISA status has been marked to reflect this; or
- the Shell has been deleted from the CM, and the ISA status has been updated to reflect this.

The HOPS shall maintain IPAs until after the archive action following either:

- a date defined as (IPE ExpiryDate plus IPE RemoveDate); or
- the CM in which the Shell containing the IPE associated with this IPA resides has been destroyed¹², and the ISA and IPA status' has been marked to reflect this; or
- the Shell containing the IPE associated with this IPA has been deleted from the CM, and the ISA and IPA status' has been updated to reflect this.

It is not mandatory that ISAs and IPAs be deleted when the defined triggers occur. A HOPS may maintain the accounts for longer periods if the operator so desires.

7.4.4 STR Auto-Top-Up operation

Stored Travel Rights may be automatically topped up by a predetermined amount when the value of STR falls to a predetermined level.

The HOPS shall include a facility to initiate, modify or cease Auto-Top-Up for STR IPE instances, and shall generate Actionlist messages to do that, as defined in ITSO TS 1000-6.

The HOPS shall, on receipt of an Auto-Top-Up Transaction Record from a POST, update the Stored Travel Rights IPA to reflect the new IPE instance contents¹³.

7.4.5 STR Actionlist top up

Stored Travel Rights may be added through an Actionlist transaction. The HOPS shall include a facility to control, instigate and record use of this feature.

¹¹ It is recommended that the destruction process should be an auditable process.

¹² It is recommended that the destruction process should be an auditable process.

¹³ A payment collection cycle should also be instigated by this event.

7.4.6 STR scheme exposure

In order to limit exposure, the maximum amount of Stored Travel Rights that are allowed to be held within a Stored Travel rights IPE instance is specified within the IPE instance. This is the maximum value that can be held on a Stored Travel Rights IPE instance, and any STR top up request which would cause this value to be exceeded shall fail¹⁴.

The HOPS shall monitor Transaction Records received, and shall highlight error conditions to the STR scheme operator, including but not limited to instances where a STR IPE instance is used for payment, but where no add value Transaction Record is received.

7.4.7 STR Negative Balance

These specifications allow the amount of Stored Travel Rights held within an IPE instance to be negative, subject to IPE element MaximumNegativeAmount. The HOPS shall provide a facility to control and record the use of this feature.

7.4.8 Handling STR Add-Value Records

The HOPS shall from time to time receive duplicate add-value transactions from POSTs. This is a POST function described in ITSO TS 1000-3.

The HOPS shall check whether or not the add-value transaction record has already been received and:

- if the record has been previously received, the record shall be discarded;
- if the record has not been previously received, then it shall be processed in the normal way.

7.4.9 CTA IPA processing

A facility shall be provided for the control and recording of use of CTA IPE instances.

7.4.10 Auto-Renew

Some IPE types have an Auto-Renew facility, whereby the IPE instance validity can be automatically extended, as defined in ITSO TS 1000-5.

The HOPS shall provide facilities to control and record the use of Auto-Renew features, and specifically to:

- enable or disable Auto-Renew within an IPE instance;
- Set Auto-Renew parameters;
- Record instances of Auto-Renew events¹⁵.

7.5. List Processing

This clause describes how the HOPS shall generate and transmit Hotlists and Actionlists.

The HOPS shall provide a facility enabling:

- Generation of Hotlists and Actionlists;

¹⁴ The ISAM also includes aggregate limits. See the AMS section of this document, ITSO TS 1000-3 and ITSO TS 1000-7.

¹⁵ A payment collection cycle should also be instigated by this event.

- Detection that Hotlist and Actionlist items have been fulfilled, by means of processing Transaction Records returned by the POST actioning the list item;
- Transmission of said Hotlists and Actionlists to POSTS, where the AMS shall be used to identify individual POSTs, all POSTs controlled by the AMS, or ranges of POSTs;
- Transmission of said Hotlists and Actionlists to other HOPS for inclusion on their local lists;
- Receiving of Hotlists and Actionlists from other HOPS, and for incorporating items from these lists into local lists for onward distribution to POSTs. Local list content shall be governed by the ITSO Business Rules;
- Forwarding of Transaction Records relating to fulfilment of Hotlist and Actionlist items generated by other HOPS to those HOPS.

7.5.1 Creating Lists

The list format, structure and content are defined in ITSO TS 1000-6. Each list consists of separate items.

The nature of the item structure used shall depend upon whether the target Customer Media contains an ITSO Shell and IPE instance's, or contains just a low memory IPE instance, and also whether the ITSO Shell contains an ISRN.

If the Customer Media contains an ITSO Shell, and the ISRN is known, then:

- a key type 0 header shall be used;
- if an IPE instance is the item's target, the optional IPE identity data group shall be used.

If the Customer Media does not contain an ITSO Shell or ISRN; then:

- a key type 1 header shall be used.

Hotlists and Actionlists may be stored either within POST memory, or within ISAM memory, or both. When creating a list for download to POSTs, the HOPS shall determine from the AMS which type of memory, POST or ISAM, will be used to store the list, and shall create the lists as follows:

- if the list is to be stored in POST memory then the list shall be transmitted as a class 2 message;
- if the list is to be stored in ISAM memory then the list shall be transmitted as a class 3 message.

Where the list is to be stored both within the POST memory and within the ISAM, then two separate messages shall be transmitted.

It should be noted that there is no requirement to store Hotlists and Actionlists in the same place, and the HOPS shall accommodate this. For example, Hotlists could be stored in the ISAM, and Actionlists in the POST memory, or vice versa.

7.5.2 Hotlists

The HOPS shall provide a function to initiate a Hotlist action on either:

- A specific ITSO Shell;
- A Specific IPE instance.

7.5.2.1 Identification of Hotlists

Each Hotlist shall be identified by a HotListIdentifier, generated by the originating HOPS.

All Hotlist items in a list shall contain the same HotListIdentifier value.

A POST shall use a HotListIdentifier when processing a received list as defined in ITSO TS 1000-3.

A HOPS shall use a HotListIdentifier when processing a received list as follows:

- If the HotListIdentifier value is identical to an existing stored Hotlist, then the new items will be appended to the list;
- If the HotListIdentifier value is different from an existing stored Hotlist, then the old list will be deleted and the new list stored.

7.5.2.2 Un-Hot by Actionlist

The HOPS shall provide a facility to unblock ITSO Shells and IPEs by means of an Actionlist item.

Clearly it is possible for an ITSO Shell or IPE instance, previously blocked by Hotlisting, and subsequently unblocked, to be blocked again if the Customer Media is presented to a POST containing the original Hotlist. This is prevented by means of the ITSO Shell and IPE iteration numbers, INS# and INP#. These values are included in the Hotlist search criteria, and only if the values in the list match the values in the ITSO Shell or IPE instance will the Hotlist item be actioned.

When a POST actions an unblock item, it increments the value of INS# or INP# as appropriate, and returns the new value in the event Transaction Record.

The new value received from the POST shall be stored in the ISA or IPA as appropriate, and used in any subsequent Hotlist items generated.

7.5.2.3 Handling Hotlist Action Event Transaction Records.

The HOPS shall process Hotlist action event Transaction Records received, and shall promptly update the appropriate ISA or IPA.

7.5.3 Actionlists

The HOPS shall provide a function to initiate an Actionlist action on either:

- A specific ITSO Shell;
- A Specific IPE instance.

7.5.3.1 Identification of Actionlists

Each Actionlist shall be identified by an ActionListIdentifier, generated by the originating HOPS.

All Actionlist items in a list shall contain the same ActionListIdentifier value.

Note that a POST shall use ActionListIdentifier when processing a received list as defined in ITSO TS 1000-3.

A HOPS shall use ActionListIdentifier when processing a received list as follows:

- If the ActionListIdentifier value is identical to an existing stored Actionlist, then the new items will be appended to the list;
- If the ActionListIdentifier value is different from an existing stored Actionlist, then the old list will be deleted and the new list stored.

7.5.3.2 Prevention of duplicate actioning

In many cases, it is imperative that an Actionlist item does not execute more than once.

To ensure that an Actionlist item is not processed more than once, and that action items are actioned in the correct sequence, the ActionSequenceNumber IPE data element is provided.

Only one Actionlist item shall exist for a given instance of IPE or Shell at any one time. A match event shall have been received and applied to the relevant entity account in the HOPS before the next Actionlist item for the entity

instance is generated. If an Actionlist item is not actioned for any reason then subsequent actions cannot take place.

For an Actionlist item acting on ITSO Shells, or acting on an IPE which does not contain a Value Group,, then ActionSequenceNumber has no meaning because the ITSO Shell or IPE without a Value Group does not contain an ActionSequenceNumber. In these circumstances the HOPS shall set the ActionSequenceNumber in the action item to zero. Actionlist items acting on ITSO Shells and on IPEs which do not contain a Value Group shall only be used where multiple actioning of the item is of no consequence

For Actionlist items acting on IPEs containing a Value Group, the process followed by HOPS and POST is as follows:

- On creating an IPE instance, the value of action ActionSequenceNumber shall be set to 0, the IPA subsequently created shall contain the same value;
- When an Actionlist item is generated in the HOPS, the current value of ActionSequenceNumber shall be obtained from the IPA and stored in the Actionlist item;
- When the POST attempts to action an Actionlist item:
 - If the Actionlist item ActionSequenceNumber value is not equal to the IPE instance ActionSequenceNumber, then the Actionlist item shall not be actioned;
 - Otherwise, If the Actionlist item ActionSequenceNumber value is equal to the IPE instance ActionSequenceNumber, then the POST shall:
 - do the action;
 - Increment the value of ActionSequenceNumber held in the IPE instance;
 - Return the new value of IPE instance action ActionSequenceNumber in the Transaction Record;
- When the HOPS receives the Transaction Record generated as a result of the actioning of the Actionlist item, it shall update the IPA with the new value of ActionSequenceNumber.

Note: ITSO does not provide a mechanism which prevents Actionlist items which create IPEs (where ActionToTake = 1) from being actioned more than once. Prevention of multiple actioning is the responsibility of the Product Owner.

Following use of ActionSequenceNumber = 255, the element shall rollover to zero (0).

7.5.3.3 Actionlist types

Various types of actions may be instigated by the HOPS. These are defined in ITSO TS 1000-6.

7.6. Loyalty schemes

The HOPS shall provide support for the operation of loyalty schemes.

7.6.1 Loyalty scheme types

The HOPS shall support two types of scheme defined as follows:

- Type 1 - A Customer Media based scheme where loyalty points are stored in the IPE instance;
- Type 2 - An Account based scheme where points are held only in the IPA.

7.6.2 Loyalty scheme operation

ITSO does not prescribe how loyalty schemes should operate, apart from the minimum requirements defined in the subsequent clauses.

7.6.3 Deferred Use Loyalty IPEs

ITSO Shells may contain a Loyalty IPE instance, but this may initially not be used. Under these circumstances the associated IPA need not be created until the IPE instance is first used. The POST shall indicate to the HOPS that a first use of Loyalty has occurred, using the appropriate message defined in ITSO TS 1000-6, and at that point the IPA shall be created.

7.7 IPE Embodiment Specifications

Embodiment specifications define the IPE Owner defined parameters necessary for the creation of IPE instances. They are defined in ITSO TS 1000-6, in the form of IPE Embodiment Parameter Lists.

The HOPS shall provide facilities for:

- The creation of embodiment specifications for each IPE embodiment which the IPE Owner requires to be supported by the HOPS;
- The storage of such embodiment specifications;
- The update of such embodiment specifications;
- Marked for deletion;
- The transmission of such embodiment specifications to POSTs and to other HOPS for the purpose of creating IPEs.

The messages for transmitting embodiment specifications to other HOPS are defined in ITSO TS 1000-6.

ISAM or HSAM generated ISAM Security Acknowledgements in response to the ISMS Security Files will be routed to the ISMS via the message handler function of the HOPS.

Clause 8.5.1 details the ISMS interface further.

8.2 Physical ISAM / HSAM

The ISAM is an ITSO-supplied security sub-system, and is one of the main technical security components within the ITSO Environment. Every POST is fitted with an ISAM. Refer to ITSO TS 1000-7 for further details of role and scope of the ISAM security sub-system.

The HSAM is the security sub-system fitted in every HOPS (see clause 4).

8.2.1 General

As the ISAM / HSAM is a critical component of the ITSO Environment, certain attributes of it shall be recorded and maintained in an accurate state by the AMS. These attributes are:

- The ISAM / HSAM serial number;
- The legal entity that owns the ISAM / HSAM;
- The contact details for the person within said legal entity who is responsible for ISAM / HSAM control & management;
- The ITSO OID assigned to said legal entity;
- The date of commissioning of the ISAM / HSAM;
- The date of decommissioning of the ISAM / HSAM;
- The ISAM / HSAM password.

8.2.2 POST allocation

Each instance of a POST within an ITSO Environment shall be fitted with an ISAM. As the ITSO operation of a given POST is defined to a significant extent by the data within its ISAM, the AMS shall provide the capability to assign, maintain and monitor for each ISAM:

- Installation status of the ISAM;
- The operational location of the POST in which said ISAM is fitted;
- The serial number / identification of the POST in which the ISAM is fitted;
- The type of POST;
- The contact details for the person who is responsible for the POST equipment;
- Whether Actionlists and Hotlists are stored in the ISAM or in the POST's memory;
 - Actionlists may be stored in the ISAM or in the POST memory, or both;
 - Hotlists may be stored in the ISAM or in the POST memory, or both;
 - Hotlists and Actionlists may be stored in the same location, or in different locations.

The "Type of POST" element shall be designed such as to enable the following to be recorded:

- generic type, e.g. point of sale, validator, or a personaliser;
- manufacturer identity;

- manufacturer's type number; and
- hardware, firmware, software versions.

The miscellaneous message entitled; Physical ISAM Installation Notification, message Code 0803, shall be supported by the (AMS) HOPS as a means to assist in the maintenance and monitoring of each ISAM. [It is considered informative to the \(AMS\) HOPS and may be used as required to enhance the effective management of the ISAMs / HSAMs under its control.](#)

8.2.3 HOPS allocation

Each instance of a HOPS within an ITSO Environment shall be fitted with an HSAM. The AMS shall provide the capability to assign, maintain and monitor for each HSAM:

- Installation status of the HSAM;
- The operational location of the HOPS in which said HSAM is fitted;
- The serial number / identification of the HOPS in which the HSAM is fitted;
- The type of HOPS;
- The contact details for the person who is responsible for the HOPS.

8.2.4 ISAM / HSAM state

The AMS shall provide the capability to maintain and monitor the state of each ISAM / HSAM for which it is responsible. The state shall be one of:

- Not Deployed;
- Deployed but Not Yet In Service;
- In Service – Operational;
- In Service - Lost / Stolen;
- In Service – Faulty;
- In Service - Not owned;
- In Service – Suspended;
- Deployed but taken Out Of Service;
- Returned and stored;
- Not yet in service – lost/stolen;
- Not yet in service – faulty;
- Not yet in service – not owned;
- Not yet in service – suspended;
- Unknown;
- Hotlisted;
- Destroyed.

8.2.5 ISAM / HSAM memory management

The AMS plays an important role in the allocation and management of the memory within ISAMs / HSAMs under its control. The AMS shall be capable of:

- Generating the required ISAM Security Files to create the locally controlled Acceptance and Capability Criteria tables on the ISAM / HSAM;
- Generating the required ISAM Security Files to create the required centrally controlled Acceptance and Capability Criteria tables on the ISAM / HSAM;
- Setting up and maintaining the required indexes between locally controlled Acceptance and Capability Criteria tables on the ISAM / HSAM;
- Setting up and maintaining the required indexes between locally and centrally controlled Acceptance and Capability Criteria tables on the ISAM / HSAM;
- Setting up and maintaining the required indexes between the Acceptance and Capability Criteria tables and the 'internal counter functions' on the ISAM / HSAM.

The above means that the AMS is required to maintain an image of the memory allocation and table linkages for each ISAM / HSAM under its control. Note for tables populated by the ISMS this image will only reflect the structural aspects and does not include the actual data stored in said tables.

See ITSO TS 1000-7 and ITSO TS 1000-8 for details of the required memory structure and the command scripts used with ISAM Security Files to establish and maintain said structure.

8.2.5.1 ISAM management messaging requirements

The AMS shall create files in the ISAMs and HSAMs it manages sufficient for the storage of the following:

- ISAM Group sequence numbers and ISAM sequence numbers
- A file for the storage of a log of Secure Acknowledgements
- A file indexing the last Secure Acknowledgement stored per message

These files shall be created as defined in TS1000– 8

Only the AMS HOPS shall be able to populate the sequence number file.

In order to manage the application of Secure Data Frames to the ISAM the POST application shall be able to select and read all of the above files whilst also being able to write to the log and index files.

8.2.5.1.1 Normal Message composition rules

The AMS HOPS shall compose class 3 messages and set the values of the Group_Message_Seq# and ISAM_Message_Seq# in accordance with the following rules:

1. All the Secure Data Frames needed to carry out a self contained action on an ISAM or group of ISAMs shall be packed in the correct sequence in a single class 3 message. The first Frame to be applied by the target I/HSAM shall be the first Frame in the message. The final scripts in the last Secure Data Frame in the message shall update the ISAM Group Seq# and the ISAM Seq# as defined in table 1 and are stored in the ISAM LOG1_SEQ# file.
2. Messages that update a Group of ISAMs shall not be dependent on any previously applied update to a single member of the Group unless a single update, with the same dependency but not necessarily the same content, is applied to all members of the Group.
3. Messages intended for application to a single ISAM within a Group unconditional on any previously applied Group updates shall have the Group_Message_Seq# set to 0.

4. Messages intended for application to a single ISAM within a Group that are dependant upon the presence of a previously applied Group update shall have the Group_Message_Seq# set equal to the latest ISAM_Group_Seq#.
5. Messages intended for application to a Group of ISAMs unconditional on any previously applied updates to a single member ISAM shall have the ISAM_Message_Seq# set to 0
6. In order for new Frames to be applied to an ISAM at least one of the sequence numbers in the message shall be set to one greater than the equivalent number stored in the ISAM.
7. The ISAM will not action Secure Data Frames that have a DTS containing a Day count earlier than the Certified DTS held by the ISAM. Thus the AMS HOPS shall ensure that all Secure Data Frames in messages:
 - a. Either: All carry a DTS from the same day in which case they can be positioned in the message in any order consistent with good practice
 - b. Or If not: the Secure Data Frames with a DTS containing a later or earlier day are positioned after or before the others respectively.

Table 1 Updating the ISAM Group Seq# and the ISAM Seq#

Message Seq#(s)	Final script(s) shall be coded to SET the ISAM Seq#(s) as shown below
Group_Message_Seq# = 0	ISAM_Seq# = ISAM_Message_Seq#
ISAM_Message_Seq# = 0	ISAM_Group_Seq# = Group_Message_Seq#
Group_Message_Seq# = ISAM_Group_Seq#	ISAM_Seq# = ISAM_Message_Seq#
Group_Message_Seq# = 1+ ISAM_Group_Seq#	ISAM_Group_Seq# = Group_Message_Seq# AND ISAM_Seq# = ISAM_Message_Seq#
Group_Message_Seq# = ISAM_Group_Seq# AND ISAM_Message_Seq# = ISAM_Seq#	No script(s) needed

Annex B of Part 3 gives an example of a typical progression of sequence numbering.

8.2.5.1.2 DTS Message composition rules

Periodically the AMS HOPS may wish to supply a DTS to update the Certified Date in ISAMs it manages independently from the updates caused by the application of Secure Data Frame updates using normal messages as defined in clause 8.2.5.1.1. In this case a special DTS message composed of a single Secure Data Frame is generated in accordance with the following rules:

1. The TDF Data Element in the Secure Data Frame shall have bit2 set to 1
2. The Secure Data Frame shall be composed of any benign script. (e.g. "Select the ISAM MF") and not contain any scripts designed to update the ISAM Group Seq# and the ISAM Seq# stored in the ISAM.

8.2.6 ISAM grouping

It is recommended that the AMS provides the capability to assign ISAMs to logical groups. ISAMs may belong to one or more logical groups.

The asset administrator will determine the assignment of ISAMs to logical groups. The AMS shall support user defined naming of ISAM groups.

The AMS shall allow actions to be performed on groups of ISAMs, unless said action is specifically prohibited (by the ISMS) for group usage.

Note: Group operations that involve indexing require that all ISAMs in the group use the same index value. This requirement must be accommodated by the ISAM memory management functionality of the AMS.

Note: All ISAMs within a group shall have the same USE (as defined in ITSO TS1000–8).

Note: An ISAM may only be allocated to one physical ISAM Group within the SMS. Logical Groups may be made up of one or more physical groups.

8.3 Centrally controlled Acceptance and Capability Criteria tables

As defined in ITSO TS 1000-7, the ISAM / HSAM functionality is partly defined by a set of tables collectively known as the Acceptance and Capability Criteria. Each table controls a certain aspect of the ISAM / HSAM operation as defined in ITSO TS 1000-8.

Some of these tables are populated by the central ISMS system. These centrally controlled tables enforce the ITSO Environment-wide settings, such as keys, Customer Media platforms, etc.

The centrally controlled tables are:

- ISAM Header Record;
- ISAM Data;
- Customer Media Codes;
- Transaction Keys;
- Access Keys;
- IPE Keysets;
- ISAM Instances;
- RSA Public Keys;
- RSA Private Keys.

As stated in clause 8.2.4, the AMS is required to generate the required ISAM Security Files to create a number of these tables, and to maintain the indexing of records across certain tables as defined in ITSO TS 1000-7 and ITSO TS 1000-8.

Population of these centrally controlled tables will be by data provided by the ISMS in ISAM Security Files. As stated previously, the ISMS only provides ISAM Security Files in response to ISMS Security Requests for data from the AMS that is responsible for the ISAM.

The required ISAM Security Files will be sent from the ISMS to the relevant HOPS. The HOPS does not need to do any processing of the constituent Secure Data Frames, other than enclosing them in Class 3 messages addressed to individual ISAMs and routing said messages to the required POST (or to the required HOPS in the case of HSAM destined files).

ISAM Security Acknowledgements generated in response to the received ISAM Security File will be destined to the ISMS, routed via the HOPS. Again, the HOPS does not need to do any processing of these Secure Data Frames, other than enclosing them in Class 3 messages addressed to the ISMS.

See also ITSO TS 1000-9 for further details on Class 3 messaging.

8.4 Locally controlled Acceptance and Capability Criteria tables

As well as the centrally controlled tables defined in the previous clause, the ISAM's Acceptance and Capability Criteria also contains a number of locally controlled tables. In this context local means directly by the AMS responsible for the ISAM / HSAM.

These locally controlled tables enforce the scheme-specific commercial requirements such as: ISAM grouping, accepted IPEs, POST revalidation capability, etc.

Locally controlled tables are:

- ISAM Configuration;
- ISAM Groups;
- IPEs Accepted;
- Criteria;
- Limits List.

As stated in clause 8.2.4, the AMS is required to generate the required ISAM Security Files to create these tables, and to maintain the indexing of records across certain tables as defined in ITSO TS 1000-7 and ITSO TS 1000-8.

Population of these locally controlled tables will be by data provided by the AMS in ISAM Security Files. These ISAM Security Files will take the form of AMS-generated Class 3 messages directed to the ISAM. The ISMS is not involved in the generation of these ISAM Security Files.

ISAM Security Acknowledgements generated in response to the received ISAM Security Files will be destined to the AMS.

8.4.1 ISAM Configuration

The AMS shall be able to configure and control the following parameters within this table:

- Maximum allowed attempts for presentation of ISAM password;
- ISAM password;
- Transaction Record storage mode (whether records are stored in the ISAM or not).

See ITSO TS 1000-8 for the detailed data formats of these parameters.

8.4.2 ISAM Groups

The AMS shall be able to configure and control records within this table. Each record corresponds to a logical group to which the ISAM belongs. Each record contains the following fields:

- AMS defined logical group number;
- Record revision number;
- Valid from date;
- Valid until date;
- Issuer identifier (IIN);
- ISAM ID / OID;

— Index to the RSA Public Key¹⁶ record that is used for this logical grouping.

See ITSO TS 1000-8 for the detailed data formats of these fields.

8.4.3 IPEs Accepted

The AMS shall be able to configure and control records within this table. Each record corresponds to an IPE embodiment that the ISAM is authorised to accept. Each record contains the following fields:

- AMS defined record number;
- Record revision number;
- Valid from date;
- Valid until date;
- IIN of Product Owner;
- OID of Product Owner;
- TYP;
- PTYP;
- IPE format revision;
- KID;
- Index to the IPE Keysets¹⁷ record that is used for this IPE embodiment;
- Index to the Criteria¹⁸ record that is used for this IPE embodiment.

See ITSO TS 1000-8 for the detailed data formats of these fields.

8.4.4 Criteria

The AMS shall be able to configure and control records within this table. Each record corresponds to a set of ISAM criteria options used against IPE operations. Each record contains the following fields:

- AMS defined record number;
- Record revision number;
- Valid from date;
- Valid until date;
- ISAM schedules to be executed;
- IPE operations allowed;
- Index to the Limits List¹⁹ record that is used for this criteria set.

¹⁶ See clause 8.3

¹⁷ See clause 8.3

¹⁸ See clause 8.4.4

See ITSO TS 1000-8 for the detailed data formats of these fields.

8.4.5 Limits List

The AMS shall be able to configure and control records within this table. Each record corresponds to a set of limits used against IPE operations. Each record contains the following fields:

- AMS defined record number;
- Record revision number;
- Valid from date;
- Valid until date;
- Maximum number of IPE creations allowed in a given Transaction Session Batch;
- IPE creation warning level;
- Maximum value which may be added in a given Transaction Session Batch;
- IPE value addition warning level;
- Index to the internal counter function used.

See ITSO TS 1000-8 for the detailed data formats of these fields.

8.5 POST stored POST configuration data

The AMS is also responsible for maintaining the POST configuration data stored within POSTs under its control. The POST configuration data is the collective term given to a number of parameter tables each of which controls a certain aspect of interoperability. These tables are:

- OID / TYP parameters;
- Peak times;
- Public holidays accept off peak;
- Transfers;
- Rebates;
- Loyalty rules;
- Currency;
- Zone table reference;
- Zone table bitmap;
- Sale price table;
- IIN table;
- IPE parameters table.

ITSO TS 1000-6 defines the required data content for each of the above tables.

¹⁹ See clause 8.4.5

ParameterTableIdentifier shall be managed by the First Line HOPS, such that each list sent to a POST contains the same value for this element. It should be noted that this means that the value of ParameterTableIdentifier contained in Parameter Tables received from other HOPS shall be changed to a value assigned by the First Line HOPS.

8.5.1 Products accepted

The AMS shall maintain the 'OID / TYP' parameter table with the unique reference (IIN, OID, TYP, PTYP) for each product that a POST shall accept and process.

8.5.2 Peak times

The AMS shall maintain the 'Peak Times' parameter table for each product accepted by a POST that requires this information to be available.

8.5.3 Public holidays

The AMS shall maintain the 'Public Holidays Accept Off-Peak' parameter table for each product accepted by a POST that requires this information to be available.

8.5.4 Transfers

The AMS shall maintain the 'Transfers' parameter table for each product accepted by a POST that requires this information to be available.

8.5.5 Rebates

The AMS shall maintain the 'Rebates' parameter table for each product accepted by a POST that requires this information to be available.

8.5.6 Loyalty

The AMS shall maintain the 'Loyalty Rules' parameter table for each product accepted by a POST that requires this information to be available.

8.5.7 Exchange rates

The AMS shall maintain the 'Currency' parameter table that defines exchange rates between currencies accepted by a POST.

8.5.8 Zones

The AMS shall maintain the 'Zone Table Reference' parameter table for each product accepted by a POST that requires this information to be available.

The AMS shall maintain the 'Zone Table Bitmap' parameter table for each relevant product by a POST that requires this information to be available.

8.5.9 Sale price

The AMS shall maintain the 'Sale Price' parameter table for each product accepted by a POST that requires this information to be available.

8.5.10 IIN index

The AMS shall maintain the 'IIN' parameter table for each IIN that is accepted by the POST.

8.5.11 IPE Embodiment parameters

The AMS shall maintain the 'IPE' parameter table for each product type that a POST is authorised to be able to create an instance of.

8.6 AMS interfaces

The AMS component shall interface to:

- The ISMS (via the Message Processing HOPS component);
- The managed ISAMs / HSAMs (via the Message Processing HOPS component);
- The managed POSTs (via the Message Processing HOPS component);
- The asset administrator (via a human interface).

The AMS function makes use of all the mandatory HOPS components (message processor, message store, HSAM and services) in its operation.

In particular the AMS function uses the HOPS message processor to communicate with the ISMS, the HSAM and via the POSTs the installed ISAMs.

8.6.1 ISMS

The ISMS provides security-related data to the AMS only when so requested by the AMS. In this mode, the ISMS acts as a "server" to the AMS "client".

There is also a need for the ISMS to distribute (centrally held) information to AMS systems within the ITSO Environment. Typical examples are when the ITSO Registrar has made changes (via the ISMS) to the list of Licensed Members, Products and supported customer media platforms. In these cases the ISMS will issue the required informative messages to affected AMSs. As a result of the receipt of these informative messages, the AMS may be required to request updated security-related data in the manner described above.

The AMS shall support the following data transfers between itself and the ISMS:

- ISMS Security Requests sent from the AMS to the ISMS;
- ISMS Information Requests sent from the AMS to the ISMS;
- ISAM Security Acknowledgements sent from the AMS to the ISMS;
- AMS Information Acknowledgements sent from the AMS to the ISMS;
- ISAM Security Files sent from the ISMS to the AMS;
- ISMS-AMS Information Packets sent from the ISMS to the AMS.

8.6.1.1 ISMS Security Requests

The AMS shall support the following types of ISMS Security Requests:

- ISMS_SREQ_ISAM_CHANGES
 - ISMS_SREQ_ISAM_DATA;
 - ISMS_SREQ_STATE_CHANGE;

- ISMS_SREQ_KEY_REQUEST
 - ISMS_SREQ_IPE_KEYS;
 - ISMS_SREQ_DIR_KEY;
 - ISMS_SREQ_KEYRING;
 - ISMS_SREQ_CM;
 - ISMS_SREQ_ISMS_PUBLIC_KEY;
 - ISMS_SREQ_HOPS_PUBLIC_KEY;
 - ISMS_SREQ_ISAM_PUBLIC_KEY;
- ISMS_SREQ_ISAM_PROGRAM_UPDATE;
- ISMS_SREQ_ASSYM_KEYS;
- ISMS_SREQ_IMPORT_CM_KEYS;

ISMS Security Requests shall be formatted as XML files. ITSO TS 1000-9 defines the DTD for these files.

ISMS Security Requests shall be secured using a 'hash & MAC' mechanism. The message hash shall be generated by the AMS, which shall then use the services of the HSAM to generate an associated MAC. This mechanism is defined in ITSO TS 1000-8.

8.6.1.1.1 ISMS_SREQ_ISAM_DATA

This requests the ISMS to provide the control data for the specified ISAM / HSAM. Within the request the AMS shall provide:

- ISAM Reference Number (IRN);
- ISAM Usage;
- OID;
- AMS Identity.²⁰

If the request is approved, the ISMS will respond with an ISAM Security File containing the required information. This message will be sent to the HOPS, which shall route it to the required ISAM / HSAM.

The ISMS shall also send an Information Packet message to the AMS containing the assigned ISAM_ID²¹. The AMS shall use this ISAM_ID for all further referencing of the ISAM / HSAM.

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.²²

Notes:

- 1) The ISMS_SREQ_ISAM_DATA message will only be accepted by the ISMS once for a given IRN.
- 2) The IRN is defined at time of ISAM / HSAM manufacture and is printed on the device.

²⁰ For HSAMs only

²¹ See clause 8.6.1.6.12

²² Of type ISMS_INFO_SECURITY_REQUEST_DENIED

3) The allowed values for ISAM Usage are: POST delete Products allowed, POST delete products not allowed, SHELL PERSONALISER, HOPS. These are represented as bit settings in a USE byte defined in ITSO TS 1000-8, ISAM Data table.

- 4) OID shall be the OID to which the ISAM / HSAM is to be assigned to. Once set, this cannot be changed.
- 5) AMS Identity shall identify the AMS to which the HSAM is to be assigned.
- 6) Multiple ISMS_SREQ_ISAM_DATA requests may be sent within an ISMS_SREQ_ISAM_CHANGES message

8.6.1.1.2 ISMS_SREQ_STATE_CHANGE

This requests the ISMS to change the recorded state of the specified ISAM / HSAM. Within the request the AMS shall provide:

- IIN;
- ISAM_ID;
- Required State.

If the request is approved, the ISMS will respond with an ISAM Security File. This message will be sent to the HOPS, which shall route it to the required ISAM / HSAM.

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.

Notes:

- 1) The allowed values for Required State are: LOSTSTOLEN, OPERATIONAL, FAULTY, OUTOFSERVICE (as text).
- 2) Multiple ISMS_SREQ_STATE_CHANGE requests may be sent within an ISMS_SREQ_ISAM_CHANGES message

8.6.1.1.3 ISMS_SREQ_IPE_KEYS

This requests the ISMS to provide the required keys for a given IPE embodiment. Within the request the AMS shall provide:

- Required destination (ISAM or ISAM group);
- IIN of the Product Owner of the IPE in question;
- OID of the Product Owner of the IPE in question;
- TYP code of the IPE in question;
- PTYP code of the IPE in question;
- IPE Format Revision (IFR) of the IPE in question;
- Key ID (KID) of the IPE in question;
- Index for the IPE Keyset table;
- Proxy ISAM reference identifier;^{23 24}
- FN_S reference;
- Request type (Add or Remove IPE keys).

²³ If ISAM is authorised to retail the IPE in question

²⁴ Proxy ISAM reference cannot be used for a group-based command

If the request is approved, the ISMS will respond with an ISAM Security File containing the required information. This message will be sent to the HOPS, which shall route it to the required ISAM(s).

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.

Notes:

1) The IPE Keyset table index is in the form table id + record index. The allowed values for the table id are 00 to 03. (The ISMS will then calculate the actual table id from this value). The allowed values for the record index are 00 to 253. E.g. an allowable value is 0001 where the table id is 00 and the record index is 01.

2) The allowed values for FN_S reference are: 1100 to 14FF (hex values).

3) Multiple ISMS_SREQ_IPE_KEYS requests may be sent within an ISMS_SREQ_KEY_REQUEST message

8.6.1.1.4 ISMS_SREQ_DIR_KEY

This requests the ISMS to provide the required keys for the ITSO Directory. Within the request the AMS shall provide:

- Required destination (ISAM or ISAM group);
- IIN of the ITSO Directory owner;²⁵
- OID of the ITSO Directory owner;²⁶
- Key ID (KID);
- Index for IPE Keyset table;

If the request is approved, the ISMS will respond with an ISAM Security File containing the required information. This message will be sent to the HOPS, which shall route it to the required ISAM(s).

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.

Notes:

1) The allowed values for the IPE Keyset table index are: The IPE Keyset table index is in the form table id + record index. The allowed values for the table id are 00 to 03. (The ISMS will then calculate the actual table id from this value). The allowed values for the record index are 00 to 253. E.g. an allowable value is 0001 where the table id is 00 and the record index is 01.

2) Only one ISMS_SREQ_DIR_KEY request may be sent within an ISMS_SREQ_KEY_REQUEST message

8.6.1.1.5 ISMS_SREQ_KEYRING

This requests the ISMS to provide the environment-wide keys. Within the request the AMS shall provide:

- Required destination (HSAM, ISAM or ISAM group);
- Key ID (KID)

If the request is approved, the ISMS will respond with an ISAM Security File containing the required information. This message will be sent to the HOPS, which shall route it to the required HSAM(s) / ISAM(s).

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.

Notes:

²⁵ This is 633597 (coded as BCD)

²⁶ This is FFF8 (hex)

1) Only one ISMS_SREQ_KEYRING request may be sent within an ISMS_SREQ_KEY_REQUEST message

8.6.1.1.6 ISMS_SREQ_CM

This requests the ISMS to provide the required access keys for a given Customer Media platform. Within the request the AMS shall provide:

- Required destination (ISAM or ISAM group);
- IIN of the Shell Owner of the Customer Media platform in question;
- OID of the Shell Owner of the Customer Media platform in question;
- Format Version Code (FVC) of the Customer Media platform in question;
- Key Strategy Code (KSC) of the Customer Media platform in question;
- Key Version Code (KVC) of the Customer Media platform in question;
- Required keyset (KAS);
- Reference(s) to encrypted key(s);²⁷
- Index for the Access Keys table;
- Index for the Customer Media Codes table;
- Request type (Add or Remove CM keys).

If the request is approved, the ISMS will respond with an ISAM Security File containing the required information. This message will be sent to the HOPS, which shall route it to the required ISAM(s).

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.

Notes:

1) Multiple ISMS_SREQ_CM requests may be sent within an ISMS_SREQ_KEY_REQUEST message

8.6.1.1.7 ISMS_SREQ_ISMS_PUBLIC_KEY

This requests the ISMS to load the ISMS's public key into the specified HSAM / ISAM. Within the request the AMS shall provide:

- Required destination (HSAM or ISAM).

If the request is approved, the ISMS will respond with an ISAM Security File containing the required information. This message will be sent to the HOPS, which shall route it to the required HSAM / ISAM.

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.

Notes:

1) Only one ISMS_SREQ_ISMS_PUBLIC_KEY request may be sent within an ISMS_SREQ_KEY_REQUEST message

²⁷ If the CM platform in question requires such keys

8.6.1.1.10 ISMS_SREQ_HOPS_PUBLIC_KEY

This requests the ISMS to load the public key for the HSAM of the HOPS in question into the specified HSAM / ISAM. Within the request the AMS shall provide:

- Required destination (HSAM or ISAM);
- IIN to which the HSAM whose public key is being requested is registered;
- HSAM ID of the HSAM whose public key is being requested.

If the request is approved, the ISMS will respond with an ISAM Security File containing the required information. This message will be sent to the HOPS, which shall route it to the required HSAM / ISAM.

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.

Notes:

- 1) Only one ISMS_SREQ_HOPS_PUBLIC_KEY request may be sent within an ISMS_SREQ_KEY_REQUEST message

8.6.1.1.11 ISMS_SREQ_ISAM_PUBLIC_KEY

This requests the ISMS to load the public key for the indicated ISAM into the HSAM of the HOPS. Within the request the AMS shall provide:

- Required destination (HSAM).
- IIN to which the ISAM in question is registered;
- ISAM ID of the ISAM in question;
- HSAM's Asymmetric Key File ID.

If the request is approved, the ISMS will respond with an ISAM Security File containing the required information. This message will be sent to the HOPS, which shall route it to the required HSAM.

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.

Notes:

- 1) Although only one ISMS_SREQ_ISAM_PUBLIC_KEY request may be sent within an ISMS_SREQ_KEY_REQUEST message, it is possible to specify multiple ISAM IDs within the request.

8.6.1.1.12 ISMS_SREQ_ISAM_PROGRAM_UPDATE

This requests the ISMS to provide a program update for the given ISAM / HSAM. Within the request the AMS shall provide:

- Required destination (ISAM or HSAM).

If the request is approved, the ISMS will respond with one or more ISAM Security Files containing the required program updates, note more than one upgrade may be required if there are more than one program update versions pending. This message will be sent to the HOPS, which shall route it to the required ISAM / HSAM.

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.

8.6.1.1.13 ISMS_SREQ_ASSYM_KEYS

This requests the ISMS to provide a RSA key pair. Within the request the AMS shall provide:

- IIN;

- Group ID;
- List of ISAM IDs to be added/removed from group (optional);
- and for each ISAM the asymmetric file index into which the key is to be stored. Valid file index values are from C003 to CFFF.

If the request is approved, the ISMS will respond with an ISAM Security File containing the required information. This message will be sent to the HOPS, which shall route it to the required ISAM(s).

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.

8.6.1.1.14 ISMS_SREQ_IMPORT_CM_KEYS

This requests the ISMS to import and store the provided keys for the given Customer Media. Two types of key import are supported: Import of CM Access Keys in the form of the KAS information and the associated keys information and the import of encrypting keys in the form of a Key Block.

For Access Key import the AMS shall provide:

- IIN of the Shell Owner of the Customer Media platform in question;
- OID of the Shell Owner of the Customer Media platform in question;
- Format Version Code (FVC) of the Customer Media platform in question;
- Key Strategy Code (KSC) of the Customer Media platform in question;
- Key Version Code (KVC) of the Customer Media platform in question;
- Valid From Date for key;
- Valid Until Date for key;
- One or more Key Blocks;²⁸
- One or more KAS Blocks.²⁹

For Key Block import the AMS shall provide:

- A single Key Block.³⁰

If the request is approved, the ISMS will import and store the key(s) and respond with an ISMS_INFO_NEW_CM_NOTIFICATION. This message will be sent to the HOPS.

If the request is denied, then the ISMS will provide the AMS with reasons for said denial via an ISMS-AMS Information Packet message.

8.6.1.2 ISMS Information Requests

The AMS shall support the following types of ISMS Information Requests:

²⁸ A Key Block contains a Key Reference and the actual key value (in an encrypted form)

²⁹ A KAS Block consists of one or two pairs of Key Flags and Key References. The Key Reference must be unique.

³⁰ A Key Block contains a Key Reference and the actual key value (in an encrypted form). The ID associated identifies the KAS as stated in spreadsheet produced by CJS.

- ISMS_IREQ_INVENTORY;
- ISMS_IREQ_CHANGE_INVENTORY;
- ISMS_IREQ_MISSING_ACKS.

ISMS Information Requests shall be formatted as XML files. ITSO TS 1000-9 defines the DTD for these files.

ISMS Information Requests shall be secured using a 'hash & MAC' mechanism. The message hash shall be generated by the AMS, which shall then use the services of the HSAM to generate an associated MAC. This mechanism is defined in ITSO TS 1000-8.

8.6.1.2.1 ISMS_IREQ_INVENTORY

This requests the ISMS to provide the AMS with a current inventory of ISAMs / HSAMs assigned to the AMS. No parameter is required for this request.

The ISMS will respond with an ISMS-AMS Information Packet message³¹. See section 8.6.1.6.10 for the content of this Information Packet.

8.6.1.2.2 ISMS_IREQ_CHANGE_INVENTORY

This requests the ISMS to update its ISAM / HSAM listing with the details provided by the AMS. Within the request the AMS shall provide:

- Affected devices (HSAM, ISAM, ISAM group);
- Action Code.

The ISMS will respond with an ISMS-AMS Information Packet message³². See section 8.6.1.6.10 for the content of this Information Packet.

Notes:

- 1) The allowed values for the Action Code are: REQUEST or RELEASE (as text)

8.6.1.2.3 ISMS_IREQ_MISSING_ACKS

This requests the ISMS to provide the AMS with details of ISAMs / HSAMs that have not returned a valid ISAM Security Acknowledgement in response to an ISMS generated ISAM Security File. Within the request the AMS shall provide:

- Number of days;
- Type

The ISMS will respond with an ISMS-AMS Information Packet message³³. See section 8.6.1.6.11 for the content of this Information Packet.

Notes:

- 1) The allowed values for the Type are: MISSING; UNSUCCESSFUL or MISSING_ UNSUCCESSFUL (as text)

³¹ Of type ISMS_INFO_INVENTORY

³² Of type ISMS_INFO_INVENTORY

³³ Of type ISMS_INFO_MISSING_ACKS

8.6.1.3 ISAM Security Acknowledgements

The AMS does not directly generate ISAM Security Acknowledgments.

In the case of an HSAM, the HSAM within the HOPS shall generate security acknowledgements in response to the reception of ISAM Security Files that were destined for the HSAM.

In the case of an ISAM, the ISAM within a POST shall generate security acknowledgements in response to the reception of ISAM Security Files that were destined for the ISAM.

The data within the HSAM / ISAM generated security acknowledgement is encrypted and sealed by the originating node. See ITSO TS 1000-8 for further details.

The HOPS shall accept these security acknowledgements from HSAMs / ISAMs under its control and carry out the required XML framing of these as defined in ITSO TS 1000-9, and then route the resulting ISAM Security Acknowledgments to the ISMS if required.

8.6.1.4 AMS Information Acknowledgements

The AMS shall generate an AMS Information Acknowledgement in response to reception of an ISMS-AMS Information Packet message.

AMS Information Acknowledgements shall be formatted as XML files. ITSO TS 1000-9 defines the DTD for these files.

AMS Information Acknowledgements shall be secured using a 'hash & MAC' mechanism. The message hash shall be generated by the AMS, which shall then use the services of the HSAM to generate an associated MAC. This mechanism is defined in ITSO TS 1000-8.

8.6.1.5 ISAM Security Files

ISAM Security Files are used to transfer sensitive data from the ISMS to the ISAM / HSAM in a secure manner. The data within the Security File is encrypted and sealed by the ISMS. See ITSO TS 1000-8 for details of the Security File.

The ISMS will frame the encrypted Security File within an XML message as defined in ITSO TS 1000-9, prior to sending it as an ISAM Security File to the AMS that generated the associated ISMS Security Request.

8.6.1.6 ISMS-AMS Information Packet

The AMS shall be capable of receiving and processing ISMS Information Packets sent by the ISMS. The AMS shall provide the asset administrator with the received information in a clear and timely manner such that the administrator is able to fulfill their obligations defined by the ITSO Operating License.

Informative data provided by the ISMS will include:

- Notification of the addition of new entities to the ITSO Environment;
- Notification of rolling key updates;
- Notification of security alerts;
- Reasons for denial of ISMS Security Requests.

The AMS shall support the following types of ISMS Information Packets:

- ISMS_INFO_NEW_MEMBER_NOTIFICATION;
- ISMS_INFO_NEW_CM_NOTIFICATION;
- ISMS_INFO_NEW_PRODUCT_NOTIFICATION;
- ISMS_INFO_NEW_KEY_NOTIFICATION;

- ISMS_INFO_SECURITY_ALERT;
- ISMS_INFO_SECURITY_REQUEST_DENIED;
- ISMS_INFO_REQ_IN_PROGRESS;
- ISMS_INFO_SECURITY_SCRIPT_PROCESSING_FAILED;
- ISMS_INFO_SERVICE_NOTIFICATION;
- ISMS_INFO_INVENTORY;
- ISMS_INFO_MISSING_ACKS;
- ISMS_INFO_NEW_ISAM_ID;
- ISMS_INFO_NEW_PROGRAM_UPDATE.

ISMS-AMS Information Packets will be formatted as XML files. ITSO TS 1000-9 defines the DTD for these files.

ISMS-AMS Information Packets will be secured by the ISMS using a 'hash & MAC' mechanism.

The AMS shall generate an AMS Information Acknowledgement in response to reception of an ISMS-AMS Information Packet message.

8.6.1.6.1 ISMS_INFO_NEW_MEMBER_NOTIFICATION

This provides notification of the registration of a new ITSO Licensed Member.

The packet will contain the following pertinent attributes of the new Licensed Member:

- Assigned Licensed Member ID
- Organisation name;
- Assigned IIN;
- Assigned OID(s);
- Role(s);

8.6.1.6.2 ISMS_INFO_NEW_CM_NOTIFICATION

This provides notification of the registration of a new Customer Media platform. ITSO mandates that all POSTs must accept all Customer Media platforms.

The packet will contain the following pertinent attributes of the new platform:

- IIN of the Shell Owner;
- OID of the Shell Owner;
- Valid From Date;
- Valid Until Date;
- FVC;
- KSC;
- KVC;
- Description.

8.6.1.6.3 ISMS_INFO_NEW_PRODUCT_NOTIFICATION

This provides notification of the registration of a new product that must be included in at least one of the ISAMs assigned to a particular AMS.

The packet will contain the following pertinent attributes of the new product:

- IIN of the Product Owner;
- OID of the Product Owner;
- TYP;
- PTYP;
- IFR;
- KID;
- Valid From Date;
- Valid Until Date;
- Proxy ISAM Reference;
- Proxy ISAM ID;
- Description;
- Product key Valid From Date;
- Product key Valid Until Date;
- Product Key crypto index.

8.6.1.6.4 ISMS_INFO_NEW_KEY_NOTIFICATION

This provides notification of a key update. Such updates will usually be due to 'rolling' changes specified by the relevant key owner.

The packet will contain the following pertinent attributes of the new key:

- Description;
- IIN of the owner of the key in question;
- OID of the owner of the key in question;
- Valid From Date;
- Valid Until Date;
- KID.

8.6.1.6.5 ISMS_INFO_SECURITY_ALERT

This is used to issue a security alert. Reasons for this alert may include:

- Revocation of a License Member;
- Revocation of a Customer Media platform;
- Revocation of a product;

— Detection of fraud.

The packet will contain a human readable console message.

8.6.1.6.6 ISMS_INFO_SECURITY_REQUEST_DENIED

This is used to inform the AMS that an ISMS Security Request made to the ISMS has been denied.

The packet will contain the following elements:

- Original ID of the request to which the denial relates;
- Reason;

8.6.1.6.7 ISMS_INFO_REQ_IN_PROGRESS

This is used to inform the AMS that an ISMS Security Request made to the ISMS is in progress.

The packet will contain the following elements:

- Original ID of the request to which this message relates;
- Reason;
- IIN of the HSAM / ISAM device that was provided in the original request;
- IRN of the HSAM / ISAM device that was provided in the original request.

8.6.1.6.8 ISMS_INFO_SECURITY_SCRIPT_PROCESSING_FAILED

This is used to inform the AMS that an ISMS Security Request script failed to be processed correctly.

The packet will contain the following elements:

- Original ID of the request to which this message relates;
- Human readable console message.

8.6.1.6.9 ISMS_INFO_SERVICE_NOTIFICATION

This is used to inform the AMS on the status of the ISMS service.

The packet will contain a human readable console message.

8.6.1.6.10 ISMS_INFO_INVENTORY

This provides a listing of the ISAMs / HSAMs and their groupings (if any) as recorded by the ISMS.

The packet will contain the following elements:

- Original ID of the request to which this message relates;
- Group ID;
- ISAM_ID;
- ISAM State;
- Date of last State change.

8.6.1.6.11 ISMS_INFO_MISSING_ACKS

This provides a listing of the outstanding ISAM Security Acknowledgements for ISAMs / HSAMs under the AMS's control.

The packet will contain the following elements:

- Original ID of the request to which this message relates;
- ISAM_ID;
 - ISAM State;
 - Date of last State change;
 - Number of missing ACKs;
 - Reason
 - Number of unsuccessful ACKs;
 - Reason

8.6.1.6.12 ISMS_INFO_NEW_ISAM_ID

This provides the assigned ISAM ID for a new HSAM / ISAM.³⁴

The packet will contain the following elements:

- Original ID of the request to which this message relates;
- Assigned IIN;
- Assigned ISAM_ID;
- Assigned Usage;
- IRN of device.

8.6.1.6.13 ISMS_NEW_PROGRAM_UPDATE

This is used to inform the AMS that a new program update is available for its ISAMs.

This packet contains the version information of the new ISAM code release.

8.6.2 Managed ISAMs

Control of the ISAM / HSAM asset base is the prime purpose of the AMS. As detailed in clauses 8.3 and 8.4, the AMS either directly or indirectly controls the Acceptance and Capability Criteria within its ISAM population. Data transfer between the AMS and ISAMs / HSAMs under its control is via:

- ISAM Security Files (used to transfer data to an ISAM);
- ISAM Security Acknowledgements (used by ISAM to acknowledge the above).

8.6.2.1 ISAM Security Files

ISAM Security Files originate either from the ISMS when the data within said file relates to centrally controlled tables; or from the AMS when the data relates to a locally controlled table. In the former case the AMS only acts in a routing capacity for the Security Files.

The data within the Security File is encrypted and sealed by the originating node (ISMS or AMS). See ITSO TS 1000-8 for details of the ISAM Security File.

³⁴ Following an ISMS_SREQ_ISAM_DATA Security Request

8.6.2.2 ISAM Security Acknowledgements

ISAM Security Acknowledgements originate from an ISAM / HSAM. They are destined to the node that originated the associated ISAM Security File (i.e. either the ISMS or the AMS).

The data within the HSAM / ISAM generated security acknowledgement is encrypted and sealed by the originating node. See ITSO TS 1000-8 for further details.

8.6.3 Managed POSTs

As detailed in clause 8.5 the AMS shall control the POST configuration data stored within POSTs. Data transfer between the AMS and POST uses the message processor in the HOPS and the following types of messages:

- Class 2 Parameter Table messages (used to transfer data to a POST);
- Class 0 Acknowledgements (used by POST to acknowledge the above).

See ITSO TS 1000-3 and ITSO TS 1000-6 for details of the Parameter Table messages.

8.6.4 Asset administrator

The AMS shall provide an interface that allows the asset administrator (the human operator of the AMS) to carry out all required user functions in an obvious and efficient manner. These functions shall include:

- Setting up and managing of general ISAM / HSAM data (see clause 8.2.1);
- Setting up and managing of POST allocation (see clause 8.2.2);
- Setting up and managing of HOPS allocation (see clause 8.2.3);
- Setting up and managing locally controlled Acceptance and Capability Criteria tables;
- Setting up and managing indexed links between tables;
- Display console for ISMS Information Packets.

Where the AMS supports ISAM grouping, then the interface shall support the setting up and management of logical groupings of ISAMs.

8.7 Functionality

This clause defines the required AMS functionality to support the following:

- Installation / commissioning of ISAMs;
- Create ISAM grouping;
- Change ISAM grouping;
- Take an ISAM out of service;
- Reinstate an ISAM to service;
- Make changes to ISAM Data;
- Introduction of new product into scheme;
- Withdrawal of a product;
- Enabling of a new Customer Media platform;
- Update of Directory keys by ITSO Registrar;

- Update of Transaction keys by ITSO Registrar;
- Support of regular key rollover;
- Removal of an ITSO member;
- Change ISAM password parameters;
- Change storage of transactions parameters.

8.7.1 Installation / commissioning of ISAMs

The AMS shall carry out the following sequence of tasks:

Stage 1: Get and assign a valid ID to the ISAM

- This is likely to be done by a fulfilment bureau.

Stage 2: Create the standard Acceptance and Capability Criteria tables

- Generate the ISAM Security Files required to create the required tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

Stage 3: Populate the centrally controlled Acceptance and Capability Criteria tables

- Generate the ISMS Security Requests required to populate the tables created;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

Stage 4: Populate the locally controlled Acceptance and Capability Criteria tables

- Generate the ISAM Security Files required to populate the required tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

8.7.2 Create ISAM grouping

The AMS shall carry out the following sequence of tasks:

Stage 1: Create logical group and assign ISAMs:

- Create the required group, identify said group and assign one or more ISAMs to the group.

Stage 2: Create any required Acceptance and Capability Criteria table(s):

- Generate the ISAM Security Files required to create the required tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

Stage 3: Update the centrally controlled Acceptance and Capability Criteria tables:

- Generate the ISMS Security Requests required to update the ISMS controlled tables;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

Stage 4: Update the locally controlled Acceptance and Capability Criteria tables:

- Generate the ISAM Security Files required to update the AMS controlled tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

8.7.3 Change ISAM grouping

The AMS shall carry out the following sequence of tasks:

Stage 1: Add / delete ISAM from group:

- Add or remove ISAMs from the group in question.

Stage 2: Inform the ISMS of the inventory change:

- Generate the required ISMS Information Request and send it to the ISMS.

Stage 3: Create any required Acceptance and Capability Criteria table(s):

- Generate the ISAM Security Files required to create the required tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

Stage 4: Update the centrally controlled Acceptance and Capability Criteria tables:

- Generate the ISMS Security Requests required to update the ISMS controlled tables;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

Stage 5: Update the locally controlled Acceptance and Capability Criteria tables:

- Generate the ISAM Security Files required to update the AMS controlled tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

8.7.4 Take an ISAM out of service

Stage 1: Update status of ISAM in local database:

- Change the state of the ISAM as required (see clause 8.2.3).

Stage 2: Inform the ISMS of the inventory change:

- Generate the required ISMS Information Request and send it to the ISMS.

Stage 3: Update ISAM:

- Generate the ISMS Security Requests required to update the ISMS controlled tables;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

8.7.5 Reinstate an ISAM into service

Stage 1: Update status of ISAM in local database:

- Change the state of the ISAM as required (see clause 8.2.3).

Stage 2: Inform the ISMS of the inventory change:

- Generate the required ISMS Information Request and send it to the ISMS.

Stage 3: Update ISAM:

- Generate the ISMS Security Requests required to update the ISMS controlled tables;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

8.7.6 Make changes to ISAM Data

Stage 1: Update the centrally controlled Acceptance and Capability Criteria table:

- Generate the ISMS Security Requests required to update the required ISMS controlled table;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

The ISMS may request that the AMS carry out this operation by use of an ISMS-AMS Information Packet. If this is the case then the AMS shall execute the operation in a timely manner in line with the obligations defined by the ITSO Business Rules.

8.7.7 Introduction of new product into scheme

Stage 1: Create any required Acceptance and Capability Criteria table(s) and the Embodiment parameters:

- Generate the ISAM Security Files required to create the required tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

Stage 2: Update the centrally controlled Acceptance and Capability Criteria tables:

- Generate the ISMS Security Requests required to update the ISMS controlled tables;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

Stage 3: Update the locally controlled Acceptance and Capability Criteria tables:

- Generate the ISAM Security Files required to update the AMS controlled tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

The ISMS may request that the AMS carry out this operation by use of an ISMS-AMS Information Packet. If this is the case then the AMS shall execute the operation in a timely manner in line with the obligations defined by the ITSO Business Rules.

8.7.8 Withdrawal of a product

Stage 1: Update the centrally controlled Acceptance and Capability Criteria tables:

- Generate the ISMS Security Requests required to update the ISMS controlled tables;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

Stage 2: Update the locally controlled Acceptance and Capability Criteria tables:

- Generate the ISAM Security Files required to update the AMS controlled tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

The ISMS may request that the AMS carry out this operation by use of an ISMS-AMS Information Packet. If this is the case then the AMS shall execute the operation in a timely manner in line with the obligations defined by the ITSO Business Rules.

8.7.9 Enabling of a new Customer Media platform

Stage 1: Create any required Acceptance and Capability Criteria table(s):

- Generate the ISAM Security Files required to create the required tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

Stage 2: Update the centrally controlled Acceptance and Capability Criteria tables:

- Generate the ISMS Security Requests required to update the ISMS controlled tables;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

The ISMS may request that the AMS carry out this operation by use of an ISMS-AMS Information Packet. If this is the case then the AMS shall execute the operation in a timely manner in line with the obligations defined by the ITSO Business Rules.

8.7.10 Update of Directory keys by ITSO Registrar

Stage 1: Update the centrally controlled Acceptance and Capability Criteria tables:

- Generate the ISMS Security Requests required to update the ISMS controlled tables;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

The ISMS may request that the AMS carry out this operation by use of an ISMS-AMS Information Packet. If this is the case then the AMS shall execute the operation in a timely manner in line with the obligations defined by the ITSO Business Rules.

8.7.11 Update of Transaction keys by / HSAM Registrar

Stage 1: Update the centrally controlled Acceptance and Capability Criteria tables:

- Generate the ISMS Security Requests required to update the ISMS controlled tables;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

The ISMS may request that the AMS carry out this operation by use of an ISMS-AMS Information Packet. If this is the case then the AMS shall execute the operation in a timely manner in line with the obligations defined by the ITSO Business Rules.

8.7.12 Support of regular key rollover

Stage 1: Update the centrally controlled Acceptance and Capability Criteria tables:

- Generate the ISMS Security Requests required to update the ISMS controlled tables;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

The ISMS may request that the AMS carry out this operation by use of an ISMS-AMS Information Packet. If this is the case then the AMS shall execute the operation in a timely manner in line with the obligations defined by the ITSO Business Rules.

8.7.13 Removal of an ITSO member

Stage 1: Update the centrally controlled Acceptance and Capability Criteria tables:

- Generate the ISMS Security Requests required to update the ISMS controlled tables;
- Forward on to the ISAM in question any ISAM Security Files received from the ISMS as a result of the above request;
- Receive, and send on to the ISMS, the ISAM Security Acknowledgements arising in response to the above.

Stage 2: Update the locally controlled Acceptance and Capability Criteria tables:

- Generate the ISAM Security Files required to update the AMS controlled tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

The ISMS may request that the AMS carry out this operation by use of an ISMS-AMS Information Packet. If this is the case then the AMS shall execute the operation in a timely manner in line with the obligations defined by the ITSO Business Rules.

8.7.14 Change ISAM password parameters

Stage 1: Update the locally controlled Acceptance and Capability Criteria tables:

- Generate the ISAM Security Files required to update the AMS controlled tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

8.7.15 Change storage of transactions parameters

Stage 1: Update the locally controlled Acceptance and Capability Criteria tables:

- Generate the ISAM Security Files required to update the AMS controlled tables;
- Receive and process the ISAM Security Acknowledgements arising in response to the above.

9 Services

9.1 Audit Trail

The HOPS shall provide an audit trail facility with the following capabilities:

- Audit trail of changes to HOPS data;
- Error log;
- Journal.

All data and events recorded shall be stamped with the date and time of the event, together with the identity of the currently logged-on user where appropriate.

The Audit trail of changes to HOPS data shall:

- Record details of any changes to ITSO accounts - ISA & IPA creation, deletion or changes;
- Record details of any changes to HSAM configuration;
- Record details of any changes to AMS data files;
- Be protected from any modification including addition, modification, renaming, moving or deletion;
- Be protected from unauthorised access of any kind.

9.2 Error Log

The HOPS shall record errors in the error log, and mark each entry with an error type.

9.3 Journal

The HOPS shall record all HOPS events in the Journal, including but not limited to:

- All HOPS data modification events;
- Processing summaries;
- Start-up dates and times;
- ISAM installation, removal or changes within the HOPS;
- User sign-on and off;
- AMS activities;
- HOPS software module upgrades/installations if this can be tracked electronically;
- Modifications to the user permissions system data store;
- Modifications to HOPS configuration.

9.4 Query Facility

The HOPS shall provide a search and reporting facility for the Audit Trail, Error Log and Journal based on but not of necessity limited to the following criteria:

- Date range;
- Time range;
- Event type;
- Data store type;
- Error type;
- Logged on user identity;
- Other criteria as required by the scheme;
- A combination of the above.

The search and reporting facility shall provide optional file output of results, and shall use XML format for said output files.

9.5 ITSO Regulation Compliance Monitoring.

The HOPS shall provide a set of services to enable an external governance system mandated by the ITSO Operators Licence to assess compliance with the ITSO Operating Licence.

Said services shall include a facility to transmit compliance information automatically to said external governance function.

9.6 Security Monitoring.

The HOPS shall provide a set of services to enable the HOPS operator and an external governance system mandated by the ITSO Operators Licence to detect security breaches.

Said services shall include the requirements in ITSO TC 1000-7, clause 5, Security Architecture.

Said services shall include a facility to automatically transmit information generated to said external governance function.

9.7 User Access Control

The HOPS shall provide a User Permissions system in order to:

- Provide business entities with access to their own data, and to other data subject to commercial agreements;
- Prevent unauthorised access to data.

For each type of data entity, the HOPS shall provide separate access permissions for:

- Read;
- Update;
- Create;
- Delete functions.

Said access permissions shall be able to be set according to:

- OID;
- TYP;

- PTYP;
- Individual user identity.

The HOPS shall allow each HOPS user to access one or more OID/TYP/PTYP combinations if so required.

Said permissions shall be stored in such a manner that unauthorised access, deletion or modification is not possible. A supervisor permission shall be provided for the purposes of modifying to permissions.

9.8 Data Backup and Archiving

The HOPS shall provide facilities for:

- Data backup;
- Restore from backup;
- Data archive;
- Retrieval of archived data by data query tools;
- Restore from archive.

All HOPS data shall be stored in the backup and archive stores.

Archived data shall be available for immediate retrieval as and when required.

Archived data shall be retained:

- For a minimum period of 2 years and 6 months from the commissioning date for any new HOPS;
- And thereafter for a minimum period of 1 year 4 months.

9.9 System Clock

Where the HOPS provides a system clock function, the clock shall be synchronised to within 1 second of an internationally recognised time source.