ITSO

DOCUMENT DELIVERY NOTE

Issuing Authority:	**Owner:**	**Project Editor:**
ITSO	Technology at ITSO	ITSO Head of Technology
Document number	**Part Number:**	**Sub-Part Number**
ITSO TS 1000	7	
Issue number (stage):	**Month:**	**Year**
2.1.4	January	2010
Title:		
ITSO TS1000- 7 *Interoperable public transport ticketing using contactless smart customer media – Part 7: ITSO Security Subsystem*		
Replaces Documents:		
ITSO TS1000-7 2008-04 issue number 2.1.3		

Revision history of current edition

Date	ITSO Ref.	Editor ID	Nature of Change to this Document (or Part)
July 2003	DCI 100 /create 2.1	CJS	Create working document
Aug 2003		JC / SLB	Edit / issue working document
Aug 2003		CJS	Further edits and additions of state diagram flow charts table and move Annex A to Annex B add new Annex A.
Oct 2003		CJS	General editorial changes re Disposition of comments
Nov 2003		SLB	Format update, implement global changes and issue at 2nd CD
Nov 2003		SLB	Editorial changes only. Issue 1st consultation draft.
Jan 2004		JC	Implement DRC changes.
Feb 2004		CS	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
June 2007		MPJE	Updated to Version 2.1.2 – no change in text
Feb 2008		CJS	Updated to include ISADs following approval by DfT
Apr 2008		MPJE	Final Editing prior to publication
Feb 2010		MPJE	Updated to Version 2.1.4 – no change in text
Apr 2015		MPJE	Updated to incorporate Corrigendum 9 to Version 2.1.4

Document Reference: ITSO TS 1000-7

Date: 2010-01-29

Version: 2.1.4

Ownership: ITSO

Secretariat: Technology at ITSO

Project Editor: Mike Eastham

ITSO Technical Specification 1000-7 – Interoperable public transport ticketing using contactless smart customer media – Part 7: ITSO Security Subsystem

ISBN: 978-0-9548042-4-4

COR 9

Foreword

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

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

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

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

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

Contents

1. Scope

ITSO TS 1000 defines the key technical items and interfaces that are required to deliver interoperability. To this end, the end-to-end security system and 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 7

This Part of ITSO TS 1000 defines the requirements for a Security Subsystem used in ITSO Point of Service Terminals (POSTs) and Head Office Processors (HOPS). It does not cover the specification of any other security related functions outside the management of data flowing between Customer Media (CM), POSTS and HOPS, nor does it cover the management of keys and secure devices. The Security Subsystem specified here is designed to be flexible enough to allow for the use of CM that differ in capability and security strategies. The overall efficacy of the architecture will depend on the CM type and security strategy chosen as well as the monitoring and policing of the scheme by the ITSO Licensed Members involved.

This Specification uses, as its base, the Data Structures and architecture defined in the emerging European Standards IOPTA and Interoperable public transport fare management system architecture, referenced in the Bibliography in ITSO TS 1000-1.

2. Normative references

Normative references for all Parts of ITSO TS 1000 are given in ITSO TS 1000-1.

3 Terms and definitions

Terms and definitions for all Parts of ITSO TS 1000 are given in ITSO TS 1000-1.

4 Data types

Data type definitions for all Parts of ITSO TS 1000 are given in ITSO TS 1000-1.

5 Security architecture

The ITSO security architecture embraces the principles of the emerging CEN standards in combination with the structure and use of ITSO Data Groups and messages in such a way that, confidentiality, integrity, authenticity and non-repudiation of data can be managed as required, whilst also accommodating the placing of ITSO Data Groups on CM ranging in functionality from memory only CM to high performance microprocessor CM.

5.1 Security architecture objectives

An ITSO Environment shall consist of Licensed Members who provide Products to the Mediaholders who use them. It shall be the responsibility of the Licensed Members to ensure that Mediaholders can, with confidence, use the Products provided by the Licensed Members throughout the ITSO Environment and as agreed by the Licensed Members subject to the relevant licence with ITSO.

Correct use of the ITSO security architecture defined herein and in ITSO TS 1000-8 is one of the tools that shall be used by the Licensed Members in meeting their responsibilities.

IPE Data Groups contain the ITSO Product Entities (IPEs) which when carried on an ITSO Shell offer the cardholder access to services. Any Licensed Members of an ITSO Compliant Scheme shall be able to create IPEs of their own or on behalf of others on any Licensed Members ITSO Shell. Any Licensed Members in an ITSO Compliant Scheme shall be able to accept any IPEs as required. A Licensed Member may be a single entity or belong to a group of Licensed Members having a separate logical identity. In summary, all Licensed Members or registered groups of Licensed Members shall be able to create and / or modify IPEs as required by commercial arrangement;

— For their own use;

— For their own use and use by others;

— For exclusive use by others;

— On behalf of others for own use;

— On behalf of others for own use and use by others;

— On behalf of others for exclusive use by others.

In addition IPEs accepted by Licensed Members may be;

— Their own (On Us IPEs);

— Belonging to other Licensed Members (Not On Us IPEs).

Also IPEs may be resident on ITSO Shells that vary in security capability and are:

— Their own;

— Belonging to other Licensed Members.

Licensed Members of an ITSO Compliant Scheme may carry out one or more of the roles as defined in the ITSO Business Rules. These roles are illustrated in Figure 1.

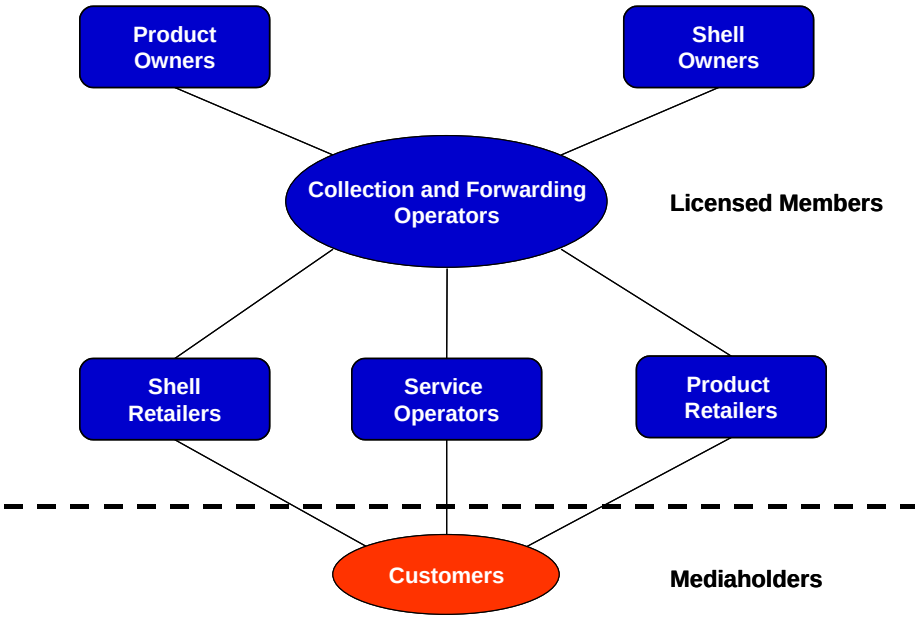

Figure 1 - ITSO Compliant Scheme Licensed Members' roles

Note: The roles of Shell Owner and Shell Retailer are interchangeable with Application Issuer and Application Retailer respectively as used in the ITSO Business Rules.

5.2 Security architecture requirements

To achieve the security objectives all Licensed Members, all IPEs, all ITSO Shell environments and all Transactions in an ITSO Compliant Scheme shall be uniquely identifiable and provided with a guarantee of authenticity. The security architecture developed by ITSO provides a mechanism capable of embodying these requirements.

It is expected that the capability of CMs and CM operating systems will change over time and the full implementation of this security architecture as defined in ITSO TS 1000-8 is programmable to allow for reasonable advances in CM capability.

It must be understood that overall security cannot be achieved by the use of the ITSO Security Subsystem (SSS) alone and business procedures outside the scope of this technical specification must be taken to minimise the risks from, deliberate or accidental misuse of the ITSO Compliant Scheme.

The security architecture separates the logical security requirements for ITSO IPEs from the requirements of physical access to the CM and incorporates the application of basic rules and limits when handling IPE Data Groups.

This shall be accomplished by the mandatory incorporation of an ITSO Security Subsystem in every accredited ITSO POST and HOPS. The Security Subsystem provides secure storage of keys and scheme parameters and shall be controlled by a POST or HOPS application in order to;

— Provide the unique identification, sealing and verification of all instances of any IPE Data Group;

— Provide the unique identification and sealing of all transaction messages;

— Determine and supply the access and authentication methods for the particular CM in use;

— Apply basic rules and limits covering the acceptance, creation and modification of Data Groups;

— Ensure cardholder privacy is maintained.

Figure 2 shows the distribution of ITSO Security Subsystems overlaid on the Licensed Members' roles.

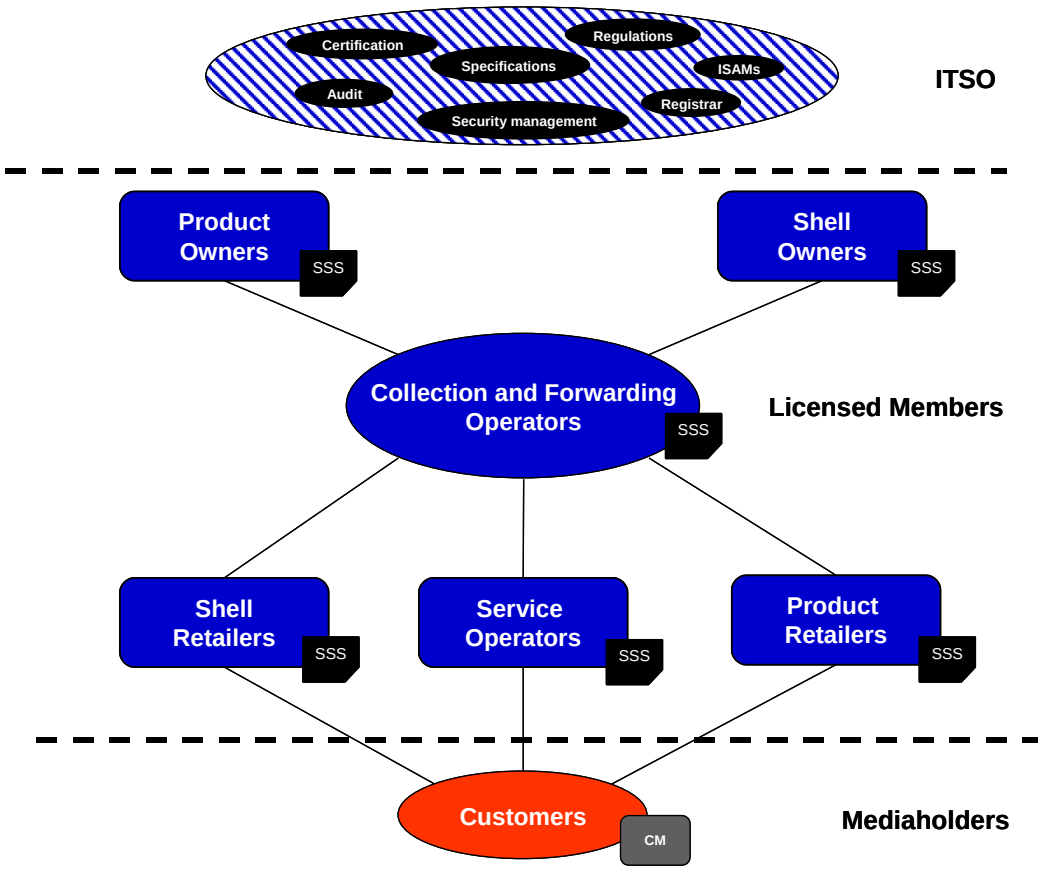

Figure 2 - The distribution of Security Subsystems

The Mediaholders' CM shall provide part of the overall security architecture to a varying degree dependent upon the Customer Media Definition (CMD) as defined in ITSO TS 1000-10 for said media.

ITSO shall offer various services to its Licensed Members by providing:

- Specification maintenance,
- ITSO Shell and IPE registration,
- Security and key management,
- Equipment accreditation,
- Business regulations.

5.2.1 Security layers

The security architecture is designed to protect ITSO IPEs in multiple ways. Each can be considered as a layer within the overall security architecture.

Note: Not every layer need be present on a particular CM.

A brief description of the rationale for the various layers of security is shown in Table 1.

Table 1 — Security Layers

Layer Ref	Layer description	Purpose	Description
1	All IPEs are uniquely Sealed	To provide an audit trail of IPEs and the ability to detect unauthorised changes to IPEs	Uses a unique IPE instance number and Seal to provide an audit trail and a guarantee of authenticity. Prevents undetectable IPE creation and alteration. However this alone does not prevent IPEs being copied from CM to CM (cloning). Locking the IPE to an individual CM significantly reduces this risk. However 'after the event' clone detection shall also be provided by the HOPS system.
2	IPE locked to an individual CM	To prevent simple cloning of IPEs from CM to CM	Diversifies the IPE Seal by a combination of the MID / ISRN to significantly increase the difficulty of cloning IPEs between ITSO Shells
3	IPE access restricted	To limit access to authorised entities only	Access may be read only or read and conditional write. POSTs may be restricted to certain functions only (i.e. balance viewers can only read, whereas an IPE Retailer can create IPEs etc)
4	IPE creation or value modification restrictions	To limit exposure of the Service Operators from prolonged misuse of lost or stolen POSTs	For a given IPE or group of IPEs each POST contains a programmable limit on the total number of IPE Instances that can be created and total value that may be added to value records. Once either of these limits is reached the Security Subsystem shall no longer execute IPE creation or value modification. A cryptographically protected delete parameter shall be returned from a HOPS to the Security Subsystem and shall be verified before the limits are reset.
5	CM / POST authentication	To reduce the risk of simulated CM use	Prevents the use of simple CM simulation and is particularly relevant if the basic transaction is both unattended and read only. However 'after the event' fraud detection shall also be provided by the HOPS system.
6	CM to POST Secure messaging	To prevent the malicious alteration of intercepted data	All data flows between the CM and POST in any one session shall be unique and as a consequence protected from the substitution of earlier messages. This is particularly important when value records are used. However 'after the event' value record transaction sequence number monitoring shall also be provided by the HOPS system.
7	Transaction message Seals	To ensure the detection of records that have been altered, duplicated or deleted.	Every Transaction Record in the ITSO Compliant Scheme is uniquely identified back to its source and the ITSO Shell used. The ITSO transaction collection system minimises the occurrence or effect of "lost" transactions. Additional audit trail storage and fraud detection shall also be provided by the HOPS system.
8	ITSO Shell Reference Number (ISRN) encryption	To protect the CM user against unauthorised usage tracking.	Each POST encrypts the ISRN uniquely so that only those authorised (i.e. the original ITSO Shell Owner) can trace a complete usage history of the ITSO Shell. This protects both the cardholder and the operator from malevolent or commercial eavesdropping.

5.2.2 The Security Subsystem

The role the Security Subsystem plays in implementing the security layers in any ITSO Compliant Scheme is summarised in the series of Figures 3 to 5

The Security Subsystem shall be configurable to ensure unique numbering of the Data Groups created, the generation and verification of Seals as required, the management of Transaction Records and the basic criteria for IPE usage on behalf of ITSO Licensed Members.

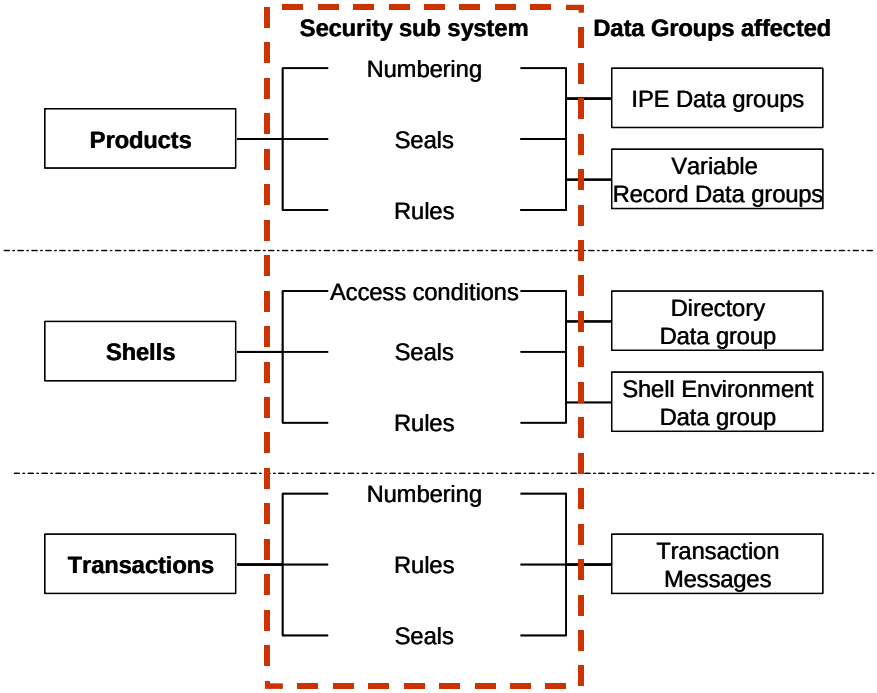

Figure 3 - The role of the Security Subsystem

The Security Subsystem also provides a means to authenticate the accuracy of data transferred between CM, POST and HOPS on behalf of the Licensed Members. It provides the “first Line” defence against fraud and maintains audit trail integrity as part of an end-to-end security architecture illustrated by the dotted line in Figure 4.

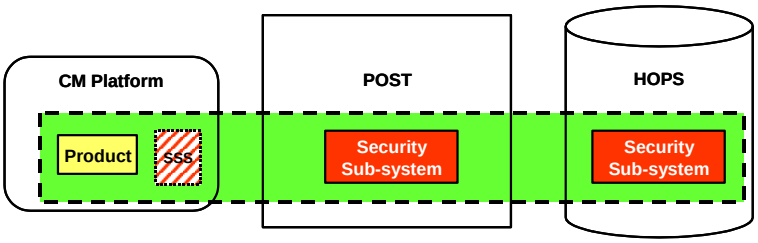

Figure 4 - End to end security architecture

The type of CM dictates how the Security Subsystem interacts with the CM and what form of CM access mechanism shall be used. This sets the level of the CM's contribution to end-to-end security shown in Figure 5.

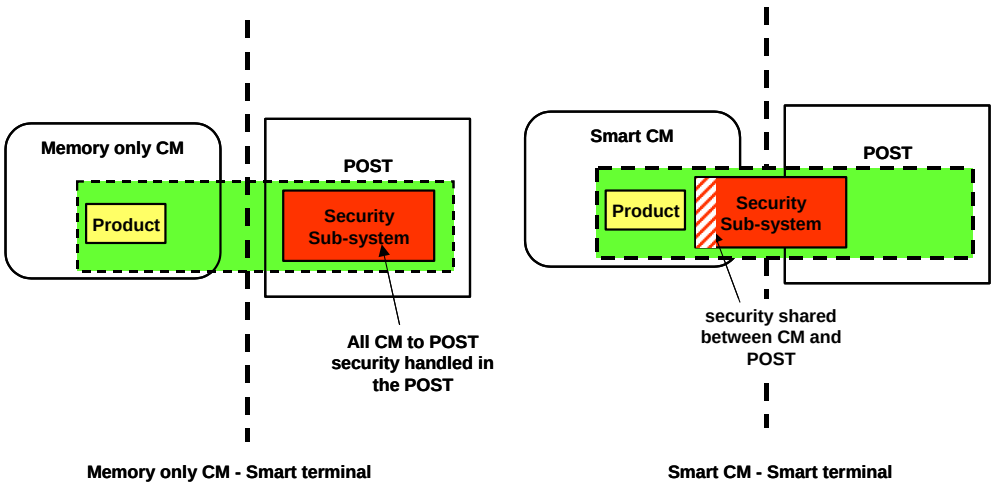

Figure 5 - The varying role of different CM types in end to end security

5.2.3 Secure messaging

The Security Subsystem shall be programmable and shall embody a secure messaging protocol. It shall be able to be configured for commercially related data, from the Asset Management System (AMS) part of a collection and forwarding operator or, for keys and other security related data, from the ITSO Security Management Service (ISMS), both using Data Structures as defined in ITSO TS 1000-8 that are embedded in class 3 messages as defined in ITSO TS1000-9. The following Figure 6 illustrates the typical message flows for distribution of a new Product key.

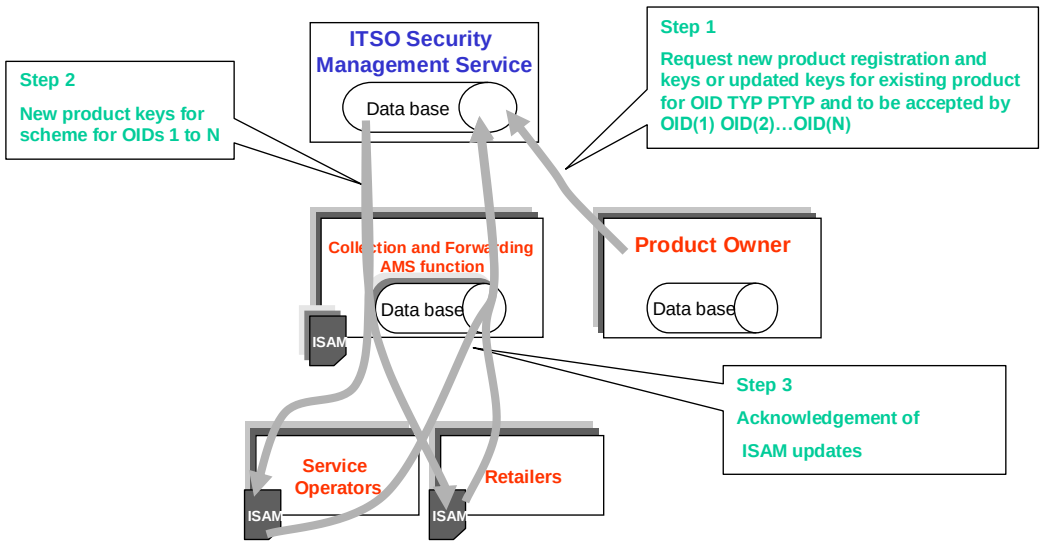

Figure 6 - Typical key distribution messages flow

5.3 Data Group security

ITSO Data Groups are collections of Data Structures and Elements that occupy ITSO Shells in an ITSO Compliant Scheme. Embedded in these groups are the Labels, Instance Identifiers and Seals that are fundamental to the security architecture.

5.3.1 Generic Data Group security principles

Data Groups are made up of four parts:

— The Label;

— A set of Data Structures;

— An Instance Identifier;

— The Seal.

This is illustrated in the following Figure 7.

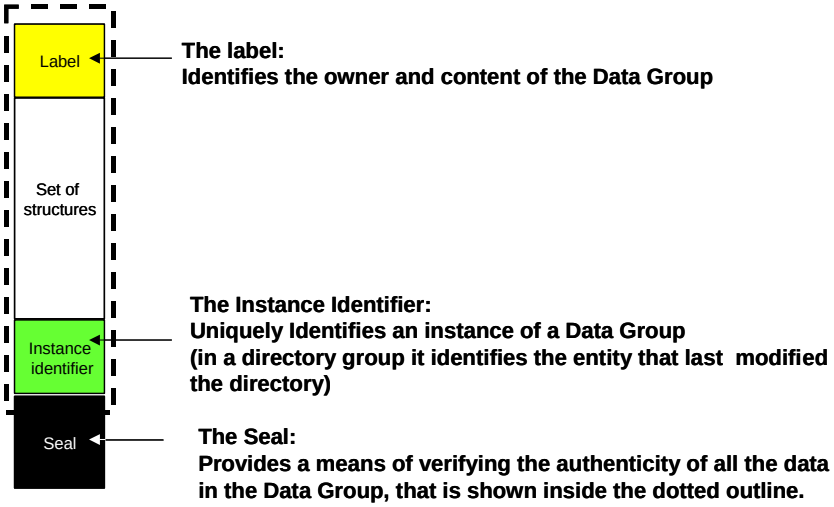

Figure 7 - Data Group security principles

Note: In certain cases Data Groups, when assembled in an ITSO Shell share a common Label. For example, where an IPE has one fixed and one or more variable sets of structures associated with it. The Label shall also be shared as a Directory Entry in any one of the positions available in a Directory Data Group where said group is present.

5.3.2 ITSO Shell Environment and Directory Data Groups

An ITSO Shell Environment and Directory shall comprise two[1] Data Groups linked together by a common Label[2]. One of these Data Groups, known as the ITSO Shell Environment Data Group, shall hold Data Structures fixed for the life of the ITSO Shell. The other group, known as the Directory Data Group, shall hold Data Structures that frequently change throughout the life of the ITSO Shell. Figure 8 illustrates this.

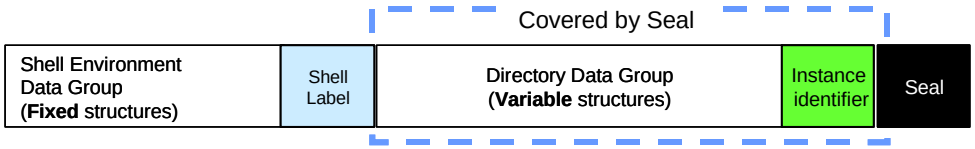

Figure 8 - ITSO Shell Environment and Directory Data Groups

Note: A special, compact, version of the ITSO Shell Environment and Directory Data Groups are used on CM that has a very limited memory capacity. In this case the POST shall expand these into full Data Groups as defined in the CMD before processing by the Security Subsystem.

1 Where software Anti-tear is mandated by the CMD an additional copy of the Directory Data Group shall be accommodated.

2 In this case the Label is derived from the Issuer Identification Number (IIN) Operator Identification Number (OID) Format Version Code (FVC) and Key Strategy Code (KSC) held in the environment group and linked to the directory by reference to the CMD for each CM platform as defined in ITSO TS 1000-10

5.3.3 IPE Data Groups

IPEs in an ITSO Shell shall comprise one or more[3] Data Groups linked together by a common Label. One of the groups, known as the Fixed IPE Data Group, shall always be present in an IPE and shall hold Data Structures that are normally fixed for the life of the IPE. Another group, known as the Variable Record Data Group, may also be present and shall hold Data Structures that are frequently changed throughout the life of the IPE. Figure 9 illustrates the case of an IPE with Fixed and Variable Data Structures.

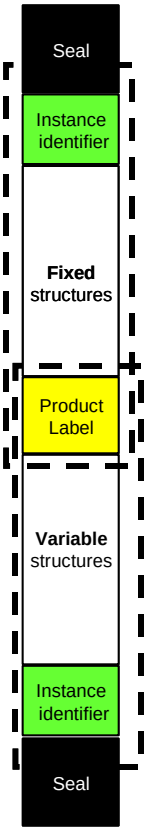

Figure 9 - IPE Data Groups

[3] Where software Anti-tear is mandated by the CMD an additional copy of the Variable Record Data Group shall be accommodated as defined by the CMD.

5.3.4 Relationship between IPEs and the ITSO Shell

Multiple IPEs may be held on an ITSO Shell. In this case the IPE Label also acts as the Directory Entry. The Seals of the IPE and the Directory are bound together via the Label. Figure 10 illustrates the relationship of a single IPE to an ITSO Shell that only supports software Anti-tear using two Variable Record Data Groups.

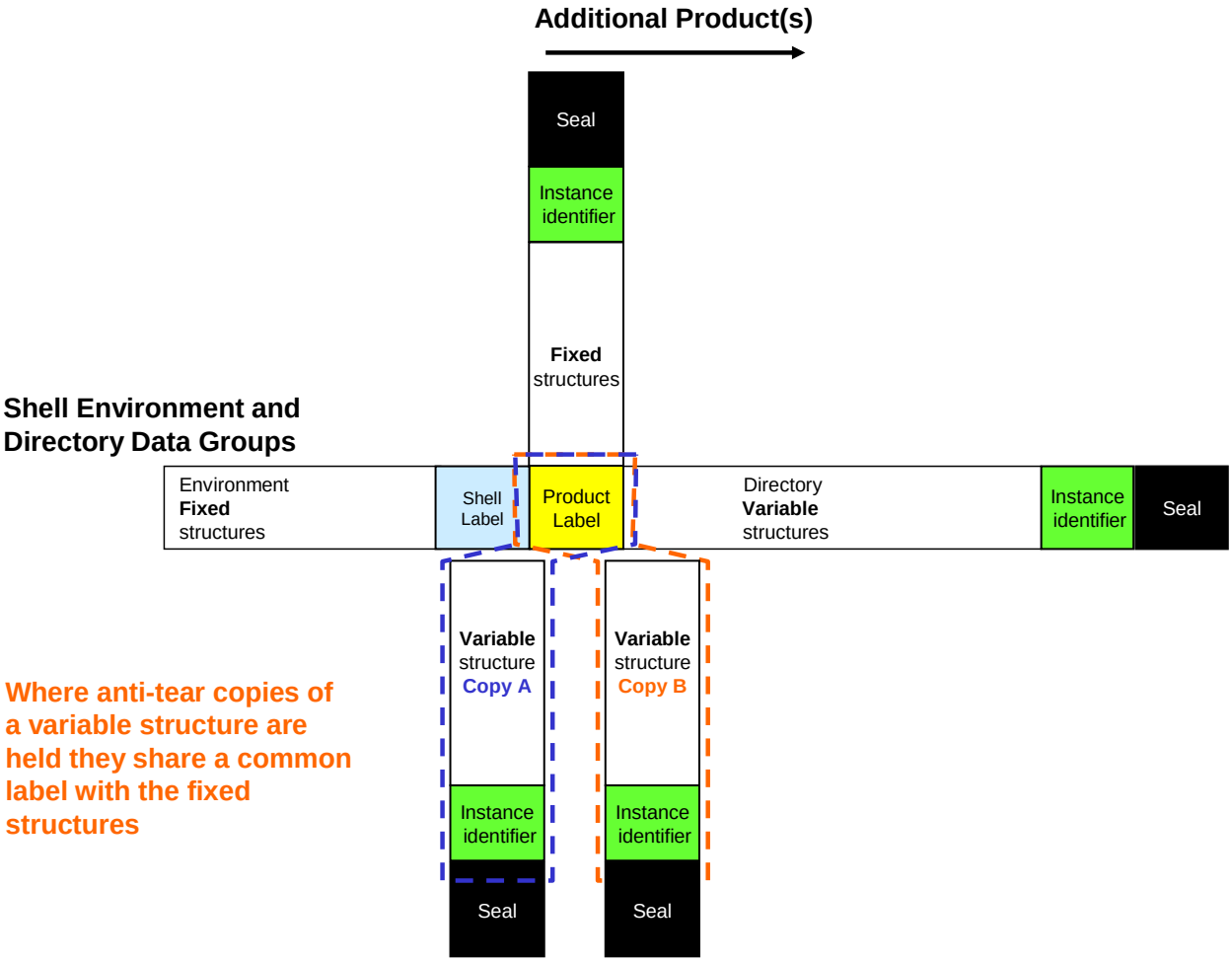

Figure 10 - Relationship between an IPE and the ITSO Shell

Figure 11 illustrates the case where multiple IPEs are present on an ITSO Shell that supports hardware Anti-tear. It also shows which Data Groups are typically the responsibility of retailers and Service Operators respectively.

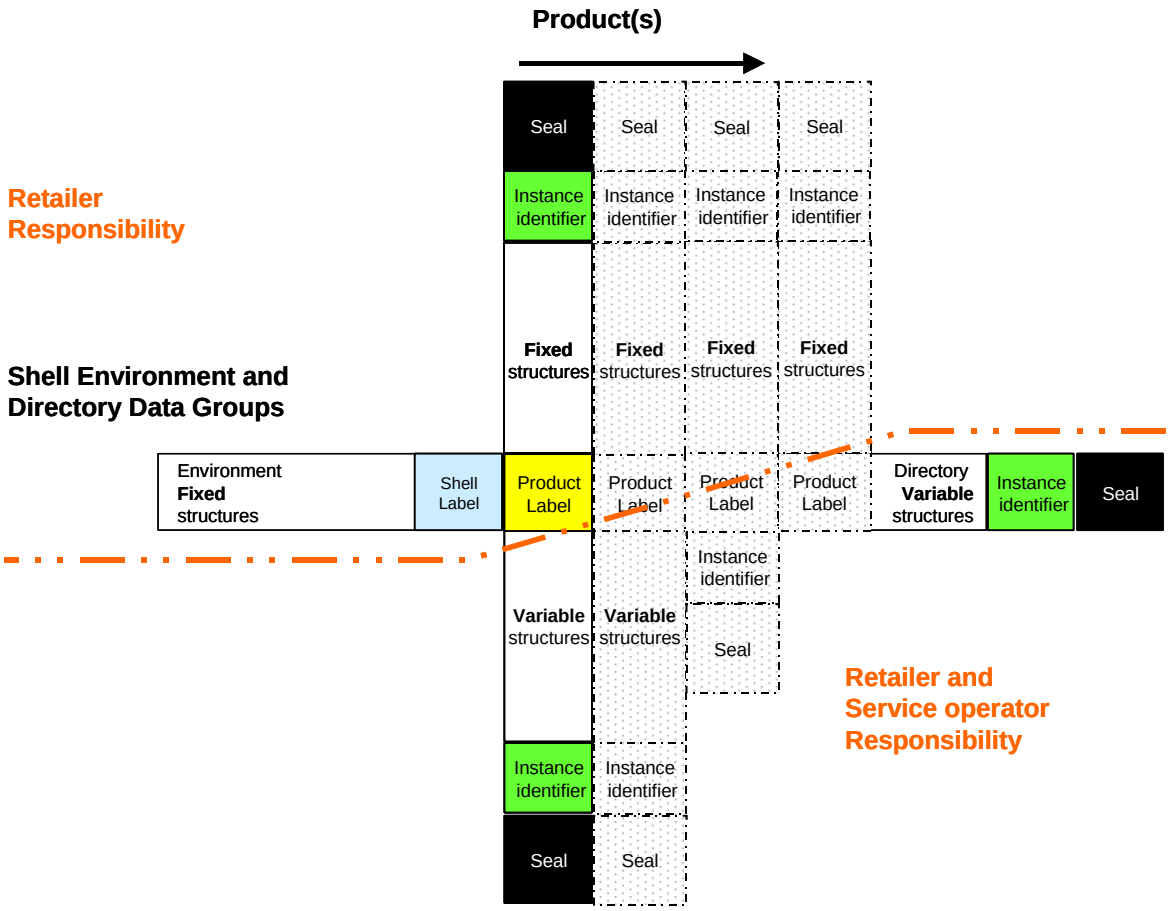

Figure 11 - Multiple IPEs on an ITSO Shell

5.4 Security Subsystem Processes

During a Transaction between the CM and POST the functions that involve using the Security Subsystem shall be split into five sequential concatenated processes numbered and defined as follows:

— 1 Authenticating the CM and opening the Directory;

— 2 IPE processing;

— 3 Updating the Directory and committing the Transaction to the CM;

— 4 Terminating the CM session;

— 5 Transaction Record processing.

The last process shall take place concurrently or contiguously with the penultimate process. Other Security Subsystem related processes shall not be accepted during the above sequence.

Additional processes generically described as process 0 are used for Security Subsystem messaging and additional functionality when the Security Subsystem is used in a POST or HOPS application.

5.4.1 Security Subsystem transaction processes

The five main processes relating to a CM transaction require data flows between three entities, namely, the CM, the POST and the Security Subsystem. These processes, numbered as in this clause, are illustrated in Figure 12.

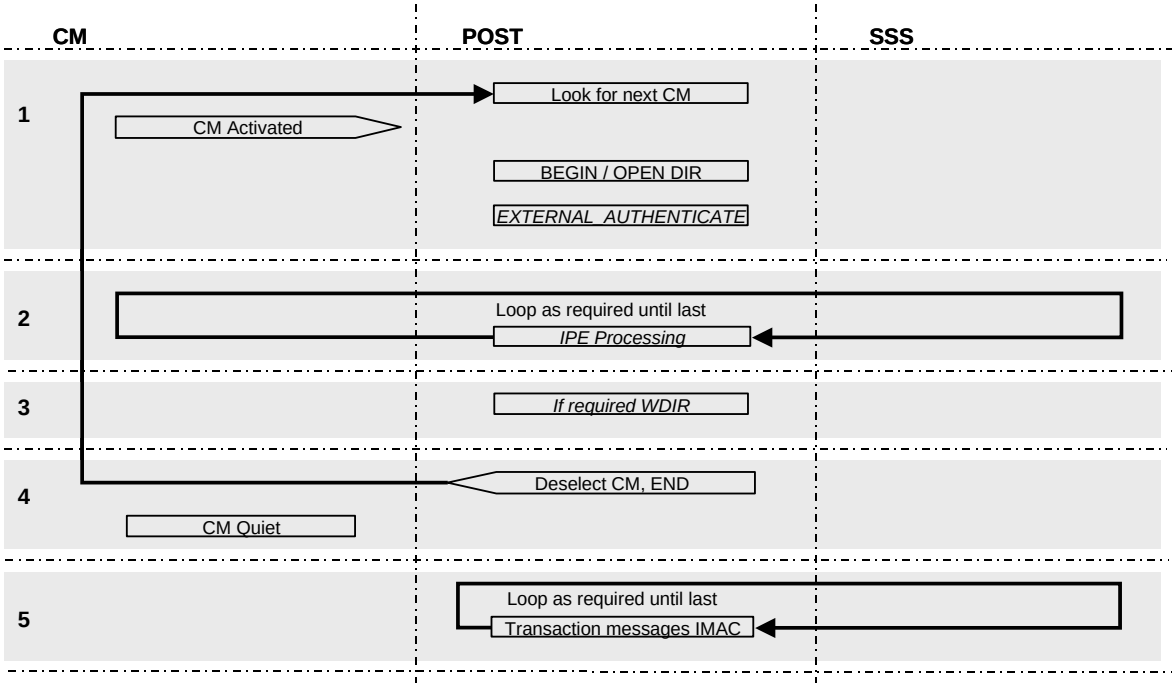

Figure 12 - Security Subsystem transaction processes

Note: In all the process diagrams items in italics are optional.

5.4.1.1 Security Subsystem transaction process rules

Not all processes shall be used in every CM transaction:

Processes 1 and 4	Shall always occur once a CM is detected.
Process 2	Shall always occur during a transaction where an IPE is verified, created or modified. This process may be repeated dependent on the nature of transaction.
Process 3	Shall always occur during a transaction where an IPE is created or modified.
Process 5	Shall always occur if a Transaction Record is required.

5.4.1.2 Security Subsystem transaction Schedules

Different sequences of processes shall be used when handling IPEs. The Acceptance and Capability Criteria (ACC) for any given IPE mandates a Schedule of processes that shall be used. Schedules are defined as follows:

Schedule 1	Transactions that only read the Directory need only processes 1, 4 and 5.
Schedule 2	Transactions that read the Directory and read an IPE require only processes 1, 2, 4 and 5.
Schedule 3	Transactions that alter the contents of the ITSO Shell require all 5 processes.

6 Security Sub System Mechanisation

The Security Subsystem shall be mechanised as a removable secure application module known as the ITSO Secure Application Module (ISAM). This approach is chosen in order to simplify the provision of the Security Subsystem.

6.1 ISAM physical attributes overview

The ISAM contains a tamper resistant microprocessor and external memory mounted in an industry standard package. All data held in the external memory shall be encrypted.

The ISAM shall be accredited to Common Criteria EAL 4.

The ISAM shall be housed in an ID 000 package suitable for mounting in a socket in every POST / HOPS.

ITSO TS 1000-8 defines in detail the form and function of the ISAM.

6.2 Electrical characteristics overview

The ISAM requires a 3 volt DC supply and shall be operated when clocked in the frequency range 1 – 5 MHz.

ITSO TS 1000-8 defines in detail the electrical characteristics of the ISAM.

6.3 ISAM overall Logic

The ISAM shall be considered as subordinate to the POST and activated by commands sent from the POST. However the ISAM also has some basic rule checking functions (ACC) built in to it and ensures that functions that modify Data Groups and messages are controlled, in so far as any seals shall not be issued to the POST for modified or created Data Groups that conflict with ACC held in the ISAM.

The commands recognised by the ISAM shall be mechanised using the T= 1 protocol as defined ISO /IEC 7816-3 and are specified in detail in ITSO TS 1000-8.

The ISAM has an ITSO command buffer of 1024 data bytes length that is used to store command and response data.

6.3.1 Command set

The commands used by the ISAM to mechanise the processes described in this Specification are shown in Table 2.

Shown in the table against each command are:

— the processes that make use of the commands listed;

— the application (POST or HOPS) in which the commands are normally used;

— marked * the WDIR command may be configured to allow the creation of an ITSO Shell by an ITSO Shell Retailer;

— marked ** the IMAC command may be configured to turn on or off the storage of Transaction Records in the ISAM.

Note: Additional commands as defined by ISO and in ITSO TS 1000-8 are used in scripts which when embedded in class 3 messages load data / program code into the ISAM if permitted.

Table 2 - Command set

Command	INS	Process	POST	HOPS	Function
WSAM	0x40	A/R	•	•	Writes data to the ITSO command buffer
RSAM	0x42	A/R	•	•	Reads data from the ITSO command buffer
BEGIN	0x48	1	•		Initiates the authentication and session between the ITSO Shell and the ISAM
EXTERNAL_ AUTHENTICATE	0x82	1	•		Verifies the encryption of a previously issued challenge and concludes mutual authentication between the ISAM and the ITSO Shell.
VERIFY_ITSO (DIR)	Ox4 E	1	•		Authenticates the contents of a Directory Data Group
OPEN_IPE	0x4C	2	•		Provides “passkeys” for read only access to the LAS of the selected IPE Data Group
VERIFY_ITSO (IPE)	0x4E	2	•		Authenticates an IPE Data Group
MODIFY_IPE	0x50	2	•		Creates a Seal for a modified IPE Fixed Data Group (this function is also linked to the WDIR function and is dependent upon the ACC set in the ISAM). Also provides “passkeys” for read/write access to the location of the Data Group selected
CREATE_IPE	0x52	2	•		Creates a Seal for a new IPE (this function is linked to the WDIR function and is dependent upon the ACC set in the ISAM). Also provides “passkeys” for read/write access to the location requested
MODIFY_VALUE_IP E	0x2E	2	•		Creates a Seal for a modified Value Record Data Group (this function is also linked to the WDIR function and is dependent upon the ACC set in the ISAM). Also provides the “passkeys” for read/write access to the location of the Data Group selected
DELETE_IPE	0x54	2	•		Removes an IPE Data Group from an ITSO Shell
WDIR *	0x56	3	•		Creates a Seal for the contents of a modified Directory Data Group if permitted. Also provides the “passkeys” for read/write access to the location of the Data Group selected
END	0x58	4	•		Resets security attributes and concludes the session with the ITSO Shell
IMAC **	0x5A	5	•	•	Adds a sequence number and Seal to Transaction Record passed to the ISAM, encrypts the ISRN and updates the IBatch Header. If enabled this command also stores the Transaction Record in the ISAM
POLL	0x74	0	•	•	Creates a transaction IBatch “header” and deletes earlier headers as indicated by parameters in this command. Transactions held in deleted batches are then free to be overwritten
VERIFY_ISAM_ID	0x18	0	•	•	Sends a password to log the POST / HOPS on to the ISAM after power up
LBATCH	0x5E	0	•	•	Returns a list of all open IBatch Headers currently held in the ISAM
VTRANS_MAC	0x76	0		•	Verifies the Seal of Transaction Records passed to the ISAM
VBATCH_MAC	0x78	0		•	Verifies the Seal of the IBatch Header and generates the delete parameter for that IBatch

Command	INS	Process	POST	HOPS	Function
CREATE_FRAME	0x7A	0		•	Creates a signature for a class 3 ITSO message and optionally encrypts the data.
UPDATE_FRAME	0x7C	0	•	•	Authenticates and decrypts, if necessary, the attached data file embedded in a class 3 message. If purpose and content are suitable accepts the contents into the ISAM and acknowledges the file. This function is intended for updates to the configuration of an ISAM after installation in a POST. For example changes to the ACC.
READPK	0x7E	0	•	•	Returns public keys stored in the ISAM
SELFTEST	0x30	0	•	•	Instructs the ISAM to carry out a self test routine
SEARCH_ITSO	0x8A	0	•	•	Searches an ISAM held file for a match to a supplied string and if successful returns an instruction string
UPDATE_ITSO_ RECORD	0xDE	0	•	•	An ITSO specific instruction used during script processing that automatically ensures that a record shall only be updated with a record of greater version number

6.4 Data I/O speed

Speed of response / operation of the ISAM is critical in the transport environment where fast transactions are often imperative. The ISAM shall be able to handle data I/O at a speed of 447K bits per second when driven at 3.579MHz clock rate. ITSO TS 1000-8 defines the data transmission options in detail.

6.5 ISAM allocation to Licensed Members

ISAMs shall be visibly numbered with an ISAM reference number (IRN) that shall also be embedded in the ISAM header table.

Each Licensed Member shall be allocated at least one unique Operator ID number (OID). Licensed Members may also be grouped together, in this case they may share a different but common (OID). The OID is concatenated with a serial number and embedded in the ISAM as a unique ISAMID record. ISAMs issued to Licensed Members for their own use shall carry their own OID.

An ITSO Licensee's OID shall be used in ISAMs for the execution of the Function, or Functions, for which the Licensee is licensed by ITSO to perform.

The ISAMID, as defined in ITSO TS 1000-2, shall be inserted by the ISAM into every transaction message or IPE Data Group created on behalf of the owner of the ISAM. It provides the trusted identification required in mechanising all revenue apportionment between Licensed Members. Every ISAM shall be registered as part of an ITSO Compliant Scheme. To facilitate auditing, Licensed Members shall maintain a list of their allocated ISAMs, against the equipment it is installed in and the normal location where it can be found.

If ISAMs are known to be lost or stolen then they shall be Hotlisted by the AMS and any subsequent actions attributed to that ISAMID will raise an exception report and may be investigated.

6.6 Creating other Licensed Members IPEs

Where one Licensed Member has the right to create (retail) another Licensed Members IPEs then their own ISAMID shall not be used. In this case the following options are available:

— A logical instance, of the other Licensed Members ISAM, may be installed in the retailers physical ISAM. In this case the instance of the other Licensed Members ISAM shall be known as a Proxy ISAM and shall be registered as such with ITSO;

— An additional ISAM registered to the other Licensed Member may be added to the retailers POST;

— A schedule 3 transaction may be carried out (using some form of ITSO certified secure messaging) on-line to the other Licensed Members Host and ISAM.

6.7 ISAM Groups

All references to ISAM groups or to groups of ISAMs in this clause 6.7 are references to Physical ISAM Groups.

In order to facilitate the distribution of identical messages to a collection of ISAMs, the destination address for the message may be targeted at a single or a group of ISAMs. ISAM grouping utilises the coding of the OID, the ISAMID and a group number to define to which group of ISAMs the file shall be addressed. An ISAM may belong to more than one group. Further details may be found in ITSO TS 1000-8.

ISAMs shall be addressable in hierarchical groups. These are:

— A global group addresses all ISAMs with the same group number;

— A Licensed Member supra group addresses all ISAMs having the same group number and IIN but different OIDs;

— A Licensed Member group addresses all ISAMs having the same group number and the same IIN and OID;

— An individual ISAM.

7 ISAM general operation

This clause describes the interaction between the ISAM, the CM, the IPEs and the POST. The sequence of operations between CM and ISAM will vary depending on the IPE chosen and the CMD.

7.1 CM to POST to ISAM general processes

CM activity takes place within a CM session. Once the POST has determined the values of ISRN, FVC, KSC and Key-set Version Code (KVC) as defined in ITSO TS 1000-2 a CM session can commence. A CM session may be terminated once processing of IPEs is complete and any required Directory Data Group updates made.

The ISAM shall be activated for a CM session once the BEGIN command is received from the POST and finish a CM session once the END command is received. Whilst a CM session is in progress cryptographic processes shall relate to the CM present at the commencement of the CM session. Processes within the CM session are illustrated by the heavy dotted line in Figure 13.

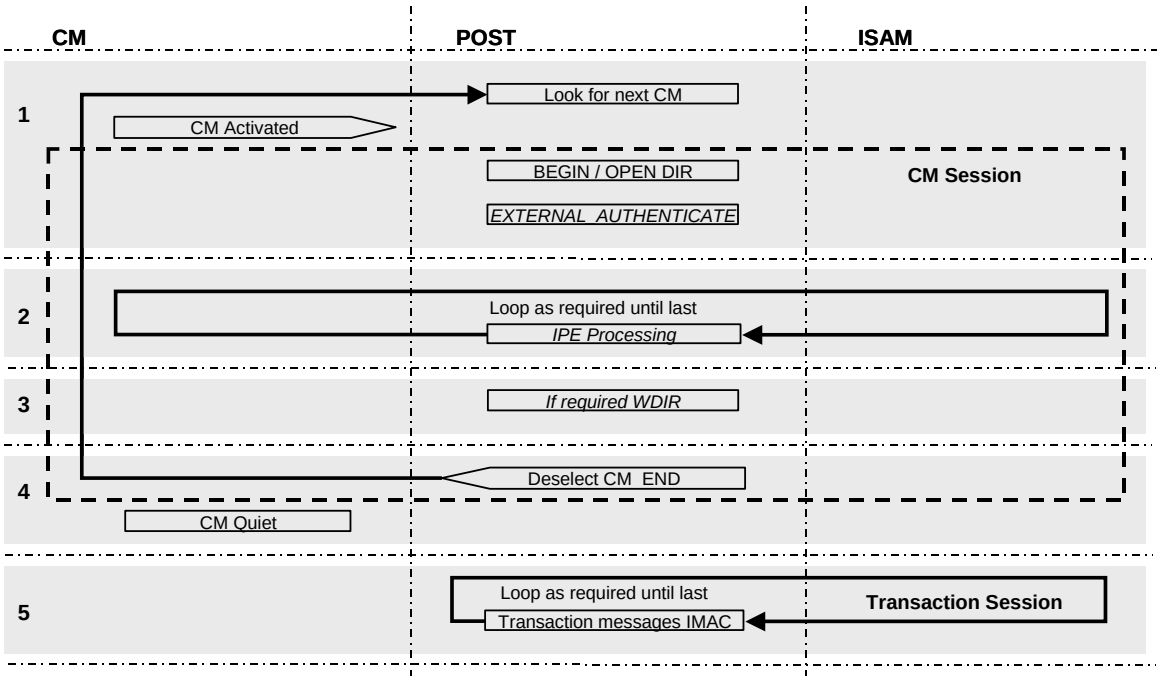

Figure 13 - General Transaction process

Note: Items in italics may be optional.

After ending process 4 the CM may, if required, be removed. In the transaction session, process 5, the ISAM provides the necessary message inserts and Seals for Transaction Records presented by the POST.

During the CM or transaction sessions information shall be passed between POST and ISAM using the commands and protocol specified in TS 1000-8.

Two general commands, Write SAM (WSAM) and Read SAM (RSAM) allow data of up to 255 Bytes in length to be written to and read from any position in the 1024 byte ITSO buffer in the ISAM. These Functions are available for use by the POST as required to facilitate handling long messages and transferring serial data to and from the ISAM as concurrently as possible with the POST's own transfer of data to and from a contactless CM reading subsystem.

The major processes between CM, ISAM and the POST application defined in clause 5.4 may be expanded as follows:

— Process 1: the CM shall be authenticated as defined in the CMD and the Directory Data Group shall be opened. The ISAM shall return the means of opening the Directory where "free read" is not permitted;

— Process 2: each IPE or Value Record, Data Group (as they are selected) shall be verified as required by the ISAM and any modified IPE or Value Record, Data Groups shall be re-sealed and the new seal returned by the ISAM;

— Process 3: where the Directory has been changed the group shall be re-sealed and the new seal returned by the ISAM;

— Process 4: the session with the CM shall then be ended;

— Process 5: any required Transaction Records are uniquely numbered, included in a batch record and the Seal returned by the ISAM. Where an ISRN is included in the Transaction it shall be encrypted in such manner that only a HOPS authorised by the ITSO Shell Owner may decrypt it. The ISAM may also be configured to keep a copy of each Transaction Record.

Taking and expanding each process in turn:

7.1.1 Transaction process 1 - Authenticating the CM and opening the Directory

Authentication of the CM and POST is dependent on the CM. For example, a memory card may not support mutual authentication. However this clause describes a generic process that supports both. An expansion of Process 1 of the 5 is illustrated in Figure 14.

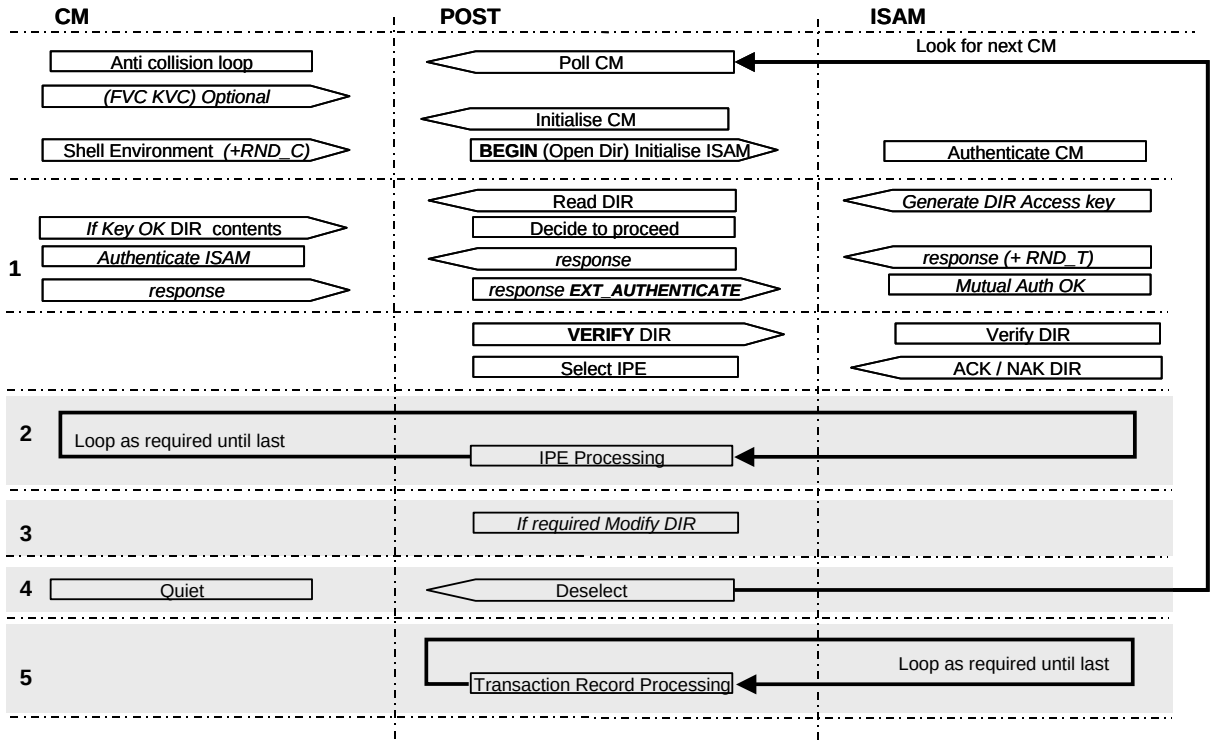

Figure 14 - Process 1

This process initiates the session between all types of CM and the ISAM and consists of a number of steps.

1. The POST detects the presence of CM and recovers the ITSO Shell Environment Data Group.

2. The BEGIN command shall be executed to initiate authentication of the CM and return any access keys if required to read the Directory. The Directory Data Group may then be read, the current copy determined and checked for appropriate content.

3. Where mutual authentication is supported then the EXTERNAL_AUTHENTICATE command shall be executed.

4. The Directory Data Group shall then be checked for authenticity using the VERIFY (DIR) Command.

7.1.2 Transaction process 2 – IPE processing

IPE processing is, generally, independent of the CM. However certain compact platforms require special IPEs and handling as defined by the CMD.

An expansion of Process 2 of the 5 is illustrated in Figure 15.

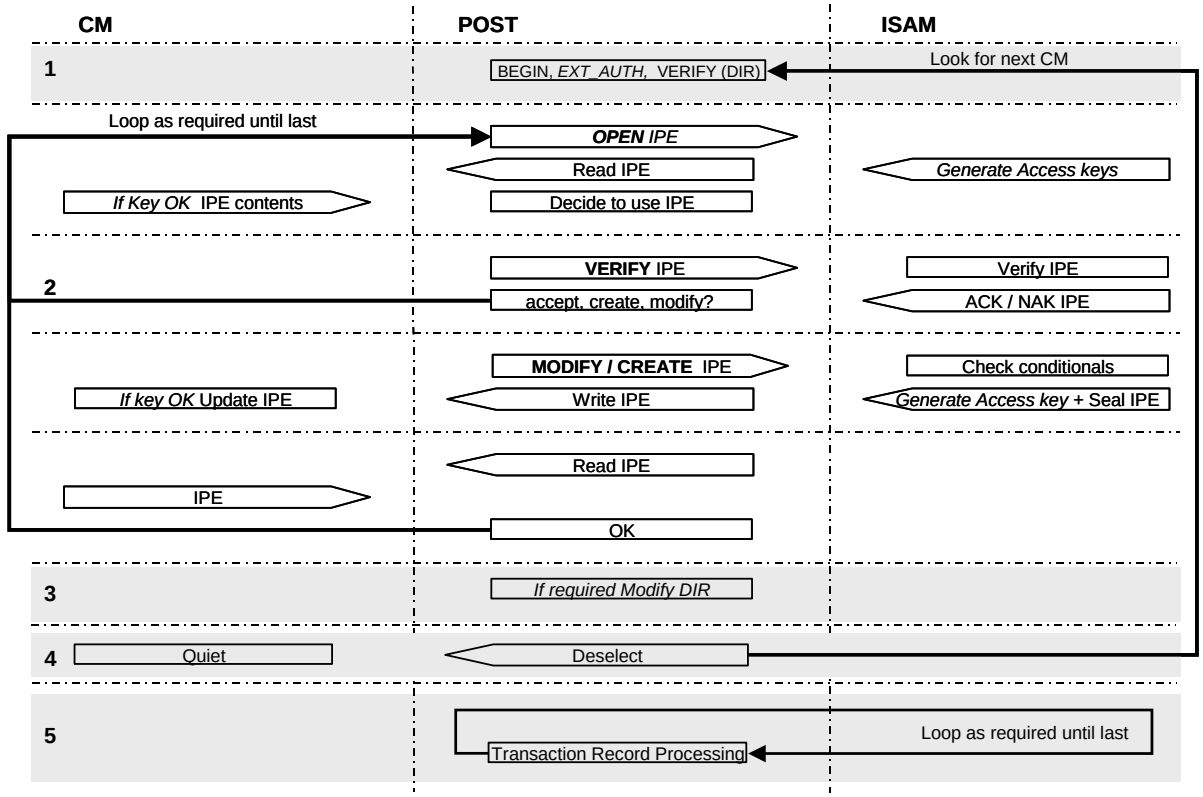

Figure 15 - Process 2

If needed, providing the necessary keys / permissions are present in the ISAM, this process occurs as often as required during the secure session between all types of IPE and the ISAM and consists of a number of steps:

1. If an IPE Data Group is to be created then steps 2 and 3 shall normally be omitted.

2. The OPEN (IPE) command returns any access keys, if required, for reading the selected IPE Data Group.

3. The selected IPE Data Group shall then be checked for authenticity using the VERIFY (IPE) command.

4. If an IPE or its associated Value Record Data Group is to be modified, then the MODIFY command shall be executed. If an IPE is to be created then the CREATE command shall be executed. Both commands return a new Seal for the Data Group.

5. This process may be repeated from step 1 for up to a maximum of 4 different IPEs in one CM session.

7.1.3 Transaction Process 3 – Directory update and commit

DIR processing is, in general, independent of the CM. However certain compact platforms require special handling as defined by the CMD. New Directory entries are only permitted for those IPEs that have been verified, modified, created or deleted during the current session. An expansion of Process 3 of the 5 is illustrated in Figure 16.

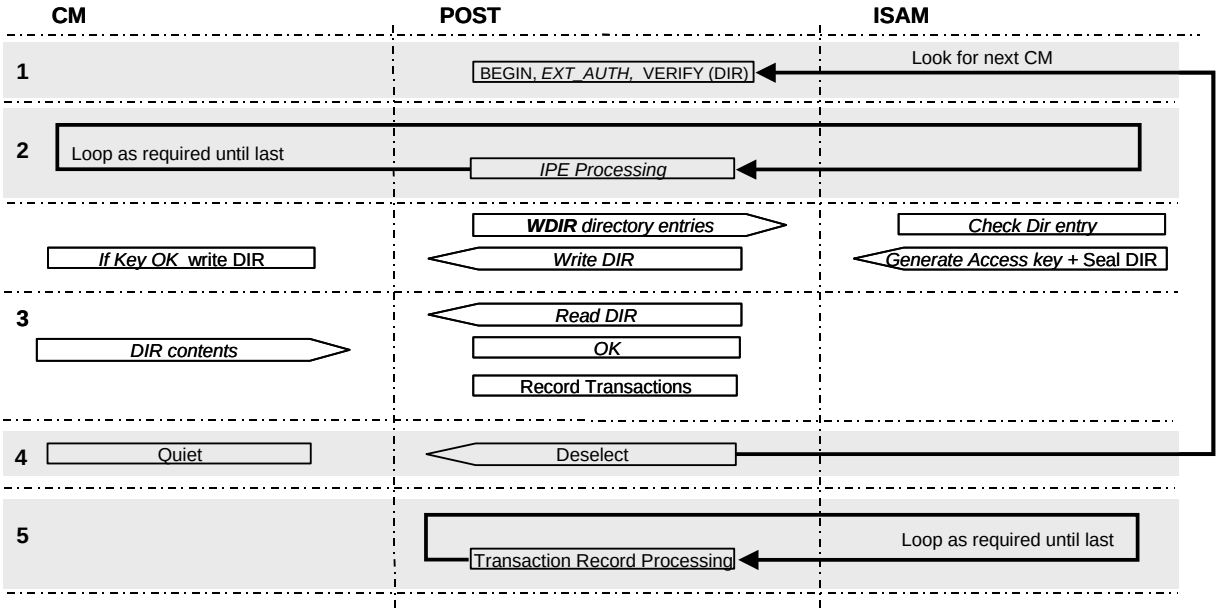

Figure 16 - Process 3

If the Directory requires modification then it must be Sealed by the ISAM:

1. The WDIR command shall be the last command executed after all other CM modifications have taken place.

2. Execution of the WDIR command incorporates a consistency check of the proposed new Directory Data Group against the previously verified Directory Data Group prior to the return of a new Seal.

3. The POST then writes the Directory to the CM and re-reads it. If the contents are correct the POST has determined that the CM has been successfully committed to its new state.

4. The CM session may now be terminated and Transaction Records made.

7.1.4 Transaction process 4- Terminate CM session

This simple process terminates the session handling the CM. An expansion of Process 4 of the 5 is illustrated in Figure 17.

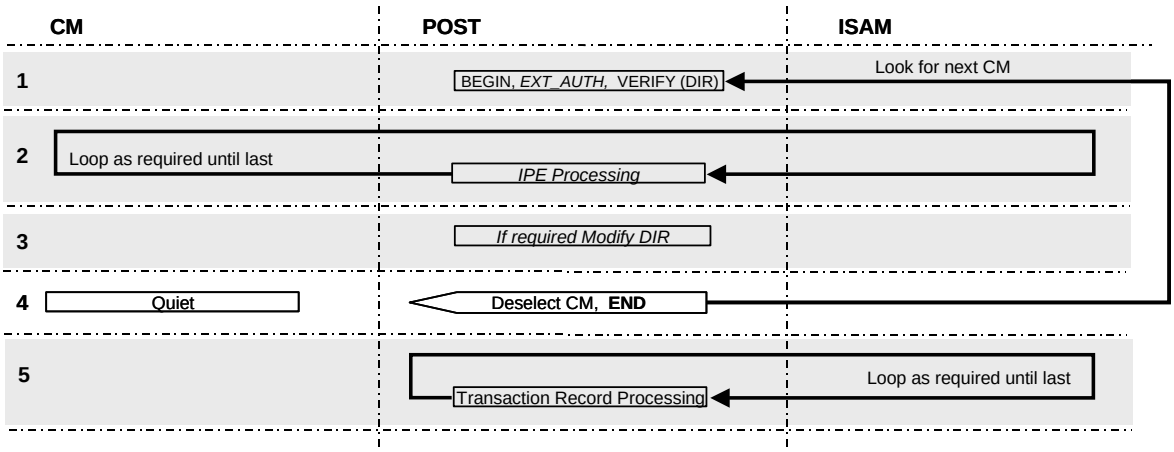

Figure 17 - Process 4

The CM is shall be deselected and END command shall be executed. At which time the ISAM resets all internal temporary key stores and data buffers ready to accept a BEGIN, IMAC or SEARCH ITSO Command.

7.1.5 Transaction process 5- Transaction message authentication

All transactions are recorded in the POST and if so configured the ISAM. The ISAM adds logical security to individual Transaction Records by:

— Adding its own identity (ISAMID) and a Seal to every Transaction Record;

— Encrypting the ISRN part of the Transaction Record;

— Sourcing Transaction Record sequence numbers;

— Sourcing Transaction IBatch headers.

An expansion of Process 5 of the 5 is illustrated in Figure 18.

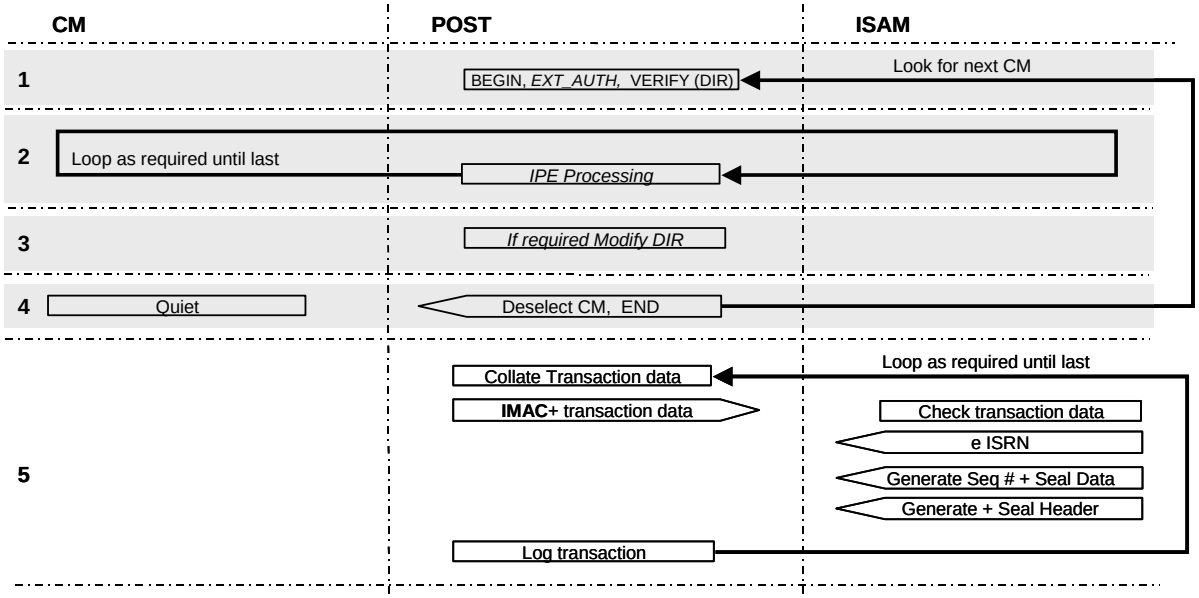

Figure 18 - Process 5

All transaction messages generated by the POST require a Seal that shall be generated by the ISAM.

As part of the same process the ISAM updates the header data that covers all transactions of the current IBatch[4].

1. The IMAC command shall be executed using, as parameters, the transaction Datasets as defined in ITSO TS 1000-6 and a Date Time Stamp (DTS).

2. The ISAM encrypts the ISRN, adds its own ISAMID and the next Transaction sequence number to the Dataset. It then Seals and returns the modified transaction Dataset.

3. The ISAM also returns the updated IBatch header and associated Seal.

[4] A new IBatch is only created as a result of a POLL command

7.1.6 (Clause contents deleted numbering retained)

7.1.7 ITSO Shell and IPE enforced command flows

The ISAM is a slave to the POST or HOPS application and apart from the Answer to Reset shall only respond when it receives one of the commands as defined in ITSO TS 1000-8. Correct operation of the POST to ISAM application program interface shall also be tested as part of the formal ITSO test and certification process.

The ISAM does however enforce certain command sequence flows in order to resist manipulation of IPEs by an incorrectly programmed application. Taking as reference the security layers highlighted in Table 1 of this Specification the commands and sequences associated with the mechanisation of each security layer are listed in Table 3.

Note: The ACC in the following table and are as defined in clause 7.2 of this Specification and ITSO TS 1000-8.

Table 3 - Relationship between ISAM commands and security layers

Ref	Security Layer	Associated ISAM commands
1	All IPEs are uniquely Sealed	The ISAM shall have been set to state 3 by the BEGIN command. The CREATE_IPE command shall only seal a newly created Product if permitted by reference to the ACC stored within the ISAM. This command shall internally generate the IPE instance identifier, which is included in the IPE Data Group(s) and is unique to any given Product Owner and instance of Product.
2	IPE locked to an individual CM	The ISAM shall have been set to state 3 by the BEGIN command. The IPE Seal produced as a result of the CREATE_IPE, MODIFY_IPE, MODIFY_VALUE_IPE and DELETE_IPE commands shall be diversified by a combination of the MID / ISRN to significantly increase the difficulty of cloning IPEs onto other ITSO Shells. The said commands shall only seal an IPE if permitted by reference to the ACC stored within the ISAM.
3	IPE access restricted	The ISAM shall have been set to state 3 by the BEGIN command. **Read only access** The OPEN_IPE command returns the keys needed for read only access to ITSO Shell memory locations. Permissions to gain read only access to locations in the ITSO Shell may be restricted by the presentation of diversified passkeys or left unrestricted and freely readable by any terminal equipment whether certified by ITSO or not. For CMDs where the unrestricted option is specified then the passkey shall be publicly known and not diversified. In this case no ISAM shall be required to gain read only access to the ITSO Shell contents. **Read / write access** With the exception of the CREATE_IPE command the IPE to be changed shall have been correctly authenticated by the VERIFY_ITSO command before read write access shall be granted. The CREATE_IPE, MODIFY_IPE, MODIFY_VALUE_IPE and DELETE_IPE commands return the passkey(s) needed to gain read/write access to the location(s) where the IPE is stored in the ITSO Shell, if permitted by reference to the ACC stored within the ISAM. A WDIR command shall normally be executed following use of the commands granting read write access
4	IPE creation or value modification restrictions	The ISAM shall have been set to state 3 by the BEGIN command. The CREATE_IPE command refers to the ACC to ensure that the limit for the number of IPEs that can be created has not been reached. The MODIFY_VALUE_IPE command refers to the ACC to ensure that the limit for the maximum value that can be created has not been reached. Once a limit has been reached the ISAM shall no longer Seal the Data Group associated with the particular command. The limits shall be reset once the ISAM receives and has verified a delete parameter from a HOPS

Ref	Security Layer	Associated ISAM commands
5	CM / POST authentication	The ISAM shall have been set to state 3 by the BEGIN command. The EXTERNAL_AUTHENTICATE command provides the necessary responses to random challenges between the POST and CM such that the CM can be deemed authentic and linked to the ISRN presented. Use of the EXTERNAL_AUTHENTICATE command shall be mandatory for all CM that do not carry an accessible embedded MID.
6	CM to POST Secure messaging	The ISAM shall have been set to state 3 by the BEGIN command. In this case the EXTERNAL_AUTHENTICATE command provides the necessary responses to random challenges between the POST and CM as before but in addition protects communications between the CM and POST by MACs or message encryption unique to the current session. This protects data flows between the CM and POST from the substitution of earlier messages.
7	Transaction message Seals	The IMAC command may be executed if the ISAM is in state 2 or 3 and internally generates a unique source identity and sequence number for transaction messages, appends them to the message and Seals the result. The IMAC command also returns the current IBatch Header cryptogram. The IMAC command shall only seal messages if the number of open IBatches is less than a limit held in the ACC stored within the ISAM.
8	ITSO Shell reference number encryption	The IMAC command also encrypts and replaces the ISRN presented to it in every CM transaction message. The encryption shall be diversified by the OID contained in the ITSO Shell and may only be successfully decrypted by an ISAM containing the same OID

7.2 Acceptance and capability criteria (ACC)

The CMs that may be accessed, IPEs that may be accepted and the functions that can be used with them, shall be defined by a configurable set of linked tables held in the ISAM and known collectively as the Acceptance and Capability Criteria. The ACC ensure that:

— CMs are only accessed as intended;

— IPEs are only accepted as intended;

— Only authorised IPE Seals are generated;

— An upper limit shall be assigned to number of IPEs created;

— An upper limit shall be assigned to aggregate value creation;

— The correct keys are used;

— ISAM configuration data and messaging cryptography are managed securely.

The tables and indexed links are illustrated in Figure 22.

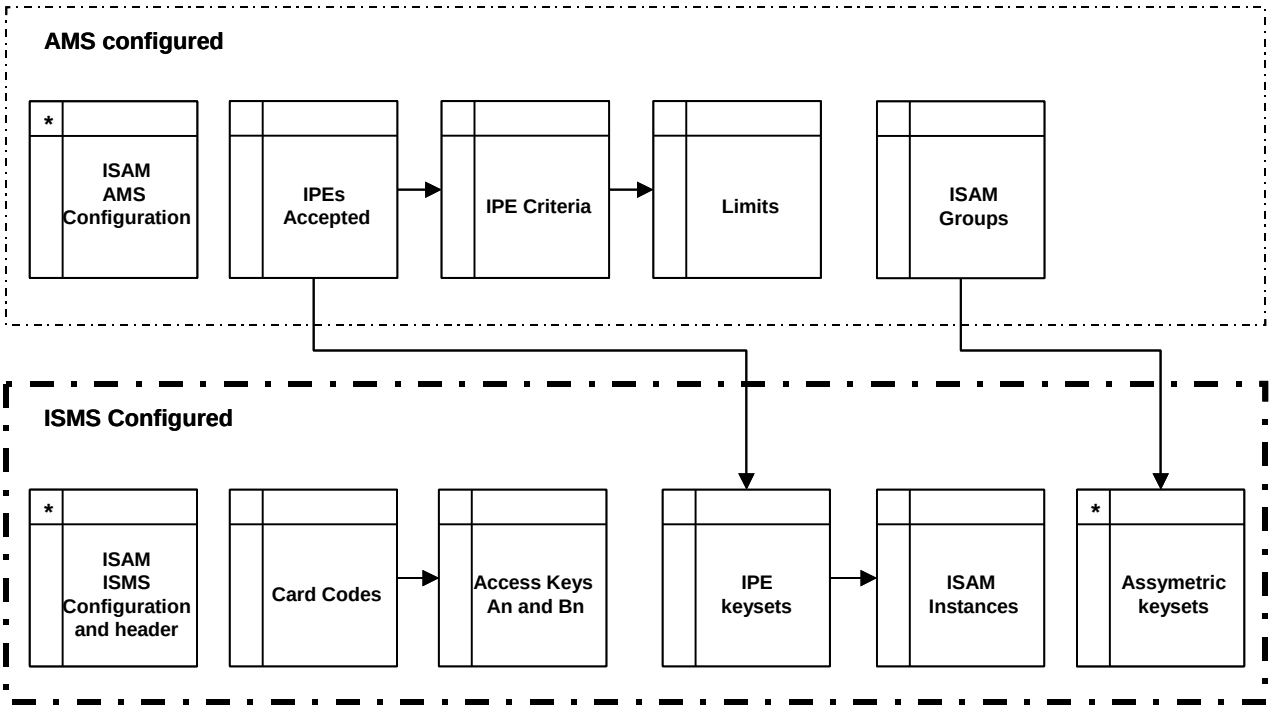

Figure 22 - ISAM Acceptance and Capability tables

The thin dotted line indicates the tables that shall be loaded in the ISAM, using class 3 messages from an AMS.

The thick dotted line indicates the tables that shall only be loaded into the ISAM using encrypted class 3 messages from the ISMS.

In either case data transfer may take place on or off line and the mechanisation of Class 3 messages is defined in ITSO TS 1000-8 and 1000-9.

The ACC shall consist of as many tables that are required at any one time to be loaded into the ISAM subject to its capacity limit. Records in tables may be updated or appended as required. The ISAM configuration, header table and asymmetric keyset shall exist before loading of any other tables shall be possible.

All records (except those in tables marked with a star in Figure 22) shall become valid on the date coded in the VFR Data Element and shall expire after the date coded in the VUT. The VFR Data Element uses the same coding as the VUT Data Element defined in ITSO TS 1000-2. A value 0x0000 in the VFR Data Element indicates the record shall be valid now whilst a value 0x0000 in the VUT Data Element means the record shall remain valid until replaced.

7.2.1 Selection of CM access keys and associated security algorithms

The selection of the security algorithms required and the keyset needed to gain access to specific areas of a CM shall be determined by the contents of the IIN, OID, FVC, KSC and KVC Data Elements found in the ITSO Shell Environment Data Group and the KAS Data Element provided by the POST. The aforementioned Data Elements are defined in ITSO TS 1000-2 and 1000-3 and must be matched to records in the card codes table for CM access to be granted.

Keysets shall be divided into to A keys and B keys. A keys shall be used to gain read only access to Data Group memory locations and are associated with the opening of ITSO Shells, IPEs and the Directory for reading. The B keys shall grant read / write access to the same locations and are associated with the creation and modification of said Data Groups.

The ISAM shall store a table of access keysets indexed to records in the card codes table. Records shall only be appended or updated in the card access keys tables upon receipt of secure messages from the ISMS.

7.2.2 Selection of IPE keys and associated security algorithms

ITSO Data Groups will be found on any of the CMs as defined in ITSO TS 1000-10.

ITSO IPEs shall be verified and certified using Keysets that are determined separately from those used for access to the CM. In this case the Keys to use, shall be selected by the concatenation of: IIN as determined by reference to: the ITSO Shell Environment, or the IPE Data Group where the IIN is not that of the ITSO Shell and TYP, PTYP, IFRN, KID and OID as determined from the IPE Data Group. The aforementioned Data Elements are defined in ITSO TS 1000-2 and must be matched to a record in the IPEs accepted table in order to process IPEs.

Where the creation of IPEs is allowed and the owner of the IPE is the owner of the physical ISAM then its identity shall be used to generate the instance identifier of the IPE. If the owner of the IPE is not the owner of the ISAM then a proxy ISAM registered to the owner of the IPE and stored in the physical ISAM instances table shall normally be used to generate the instance identifier of the IPE.

The ISAM shall store IPE records in the IPEs accepted table. Records shall only be appended or updated in the IPEs accepted table upon receipt of secure messages from a verified AMS.

The ISAM shall store tables of IPE keysets indexed to records in the IPEs accepted table and ISAM instances table. Records shall only be appended or updated in these tables upon receipt of secure messages from the ISMS.

7.2.2.1 Selection of IPE keys using wild cards

The records in the IPEs accepted tables are searched for a match in sequence, starting from the first record of the first table and ending with the last record in the last table. In order to give IPE Owners the flexibility to minimise the proliferation of keys the TYP or PTYP entries in the IPEs accepted table if set to 0xFF shall be considered as “wild card” characters and have the following significance:

— For a given IPE Owner if the TYP and PTYP first match a record in the table, then the key and ACC indexed to that record are selected;

— For a given IPE Owner when the TYP first matches a record in the table where the PTYP Data Element is set to 0xFF, then the value of PTYP is ignored and the key and ACC indexed to that record covers all remaining PTYPs for that IPE TYP, that have not been previously matched;

— For a given IPE Owner when a record in the table with the TYP Data Element set to 0xFF is first encountered in the search, then the value of TYP and PTYP are ignored and the key and ACC indexed to that record covers all remaining TYP and PTYP combinations for that IPE Owner, that have not been previously matched.

Note: By the method described in this clause it is possible for an IPE Owner to specify specific keys and ACC for some IPEs and a common key and ACC for the remaining IPEs.

7.2.3 IPE criteria and limits

Independent from the CM access and IPE keys and part of the ACC are criteria and limits tables. These shall be indexed from the IPEs accepted table and define the actions that may be performed thereon.

The actions permitted are defined in ITSO TS 1000-8.

For an IPE of a given TYP or range of TYPs belonging to a particular IPE Owner, records in the criteria tables shall be set to allow or disallow any combination of:

— Verification;

— Creation;

— Modification;

— Deletion.

In addition if the IPE contains a Value Record Data Group, the record in the criteria table may be set to allow or disallow any combination of:

— Adding value;

— Deducting value.

The schedule to be observed when processing the associated IPE shall also be stored in this table.

Indexed to a criteria table is a limits table that contains records with programmable counters that shall be used to determine the maximum aggregate value that can be added to any associated Value Record Data Groups and the maximum number of instances of the indexed IPE TYP that, where allowed, may be created. Warning codes will be returned by the ISAM as these counts accumulate towards the maximum preset values and reach configurable trigger levels.

These inbuilt limits are automatically reset upon receipt by the ISAM of a valid IBatch delete cryptogram generated by a HOPS. This limits the exposure to certain frauds in the event that a POST is stolen.

The ISAM shall store tables of criteria and limits indexed to records in the IPEs accepted table. Records shall only be appended or updated in these tables upon receipt of secure messages from the AMS.

7.2.4 Security limits

The ISAM monitors certain thresholds which if exceeded prevent execution of any CM, IPE or transaction processes until it receives a new configuration file. These conditions are:

— Undeleted IBatch Headers reach the maximum number of concurrent IBatch Headers allowed.

The ISAM shall store this information in a data table. Information in this table shall only be updated upon receipt of a secure message from the AMS.

— The security error counter reaches the maximum value allowed.

The ISAM shall store this information in a data table. Information in this table shall only be updated upon receipt of a secure message from the ISMS.

7.2.5 IBatch Headers

During the processing of Transaction Records the ISAM provides a means to add logical security to batches of said records.

For batches of Transaction Records the ISAM shall:

— Create and store IBatch Headers;

— Manage a Loss Less Transaction Record handling scheme;

— Delete IBatch Headers upon receipt of a verified acknowledgement;

— Block further use of ISAM processes when the number of unacknowledged IBatch Headers exceeds a limit;

— Reset, to predefined values, any limits in the ACC if a valid IBatch Header delete cryptogram is received.

Continuously the ISAM shall:

— Aggregate various Stored Travel Rights (STR) usage totals.

Transaction Records are grouped into batches. The header for a IBatch shall be re-computed and returned to the POST application every time a transaction message is sealed. Upon receipt of a Poll command a new IBatch Header shall be generated and the final value of the previous IBatch Header stored in the ISAM until deleted by the receipt of a delete batch cryptogram generated by a HOPS.

The IBatch Header mechanism allows either a POST or HOPS to create IBatches. It is assumed that transactions may be sent to the HOPS as complete or part batches. Once complete batches have been received and are verified as complete and correct, the HOPS shall output as many delete batch cryptograms as required, allowing the ISAM that created the IBatch to delete the related IBatch Header and reset any internal limits in the ACC to their configured values.

The ISAM requires the match of a delete batch cryptogram with an individual ISAM and batch before the matching IBatch Header may be deleted.

Non-resetable grand total data[5] shall be stored in the ISAM and returned with every IBatch Header. This ensures that certain information about the use of the STR IPE shall be accumulated and may be used for audit purposes.

The grand total data includes:

— The total amount added to an STR IPE by this ISAM;

— The total amount deducted from an STR IPE by this ISAM;

— The total number of additive STR transactions;

— The total number of subtractive STR transactions.

7.3 ISAM Housekeeping functions

Housekeeping functions are implemented in process 0. The ISAM interacts with the POST application in order to:

— Facilitate the transfer of secure messages in Secure Data Frames between POST and AMS / ISMS;

— Test and Link the ISAM to a given POST or group of POSTs;

— Enable the ISAM to store data in a file and subsequently search that file for matching parameters;

— Enable the ISAM to facilitate the management of Transaction Records in a HOPS application.

The remainder of this clause describes these functions in more detail.

[5] These totals are intended for use where there is a single STR Product or all STR Product owners use the same unit value.

7.3.1 Secure messaging function

The ISAM may be configured from either an AMS (for commercial data) or ISMS (for keys and other security related data). This function uses secure class 3 messages and the ISAM commands as defined in detail ITSO TS 1000-8 and ITSO TS 1000-9.

For secure message implementation the ISAM Command UPDATE_FRAME shall be used in the POST application whereas the HOPS application shall also use the READ_PK and CREATE_FRAME commands.

In order to transfer data securely between the ISAM and another entity an ISAM Secure Data Frame shall be used.

Upon completion of the UPDATE_FRAME command on a Secure Data Frame the target ISAM shall generate a signed Secure Data Frame that acknowledges the execution of the UPDATE_FRAME command. This shall be included in a message containing one or more acknowledging Secure Data Frames and forwarded to the AMS that delivered sourced the original Secure Data Frames applied by the UPDATE_FRAME command to the ISAM. These acknowledgements are not themselves acknowledged.

The ISAM Secure Data Frame encloses data destined for ISAMs within a secured packet. It ensures integrity of data and an audit trail for ISAM data updates. The Secure Data Frame links the ISAM data source and destination together.

Each ISAM Secure Data Frame shall:

— Identify the ISAMID of the Secure Data Frame source;

— Identify the destination of the Secure Data Frame as an ISAMID or Physical ISAM Group;

— Identify the type of ISAM Secure Data Frame;

— Contain the ISAM data file;

— Protect the contents using encryption and / or a digital signature.

7.3.1.1 Source of ISAM Secure Data Frame

The concatenation of IIN and ISAM ID as specified in ITSO TS 1000-2 defines the source of the ISAM Secure Data Frame. In normal use a POST will only process Secure Data Frames from a single AMS and the ISMS.

7.3.1.2 Destination of ISAM Secure Data Frame

The concatenation of Physical ISAM Group number (ISG), IIN and ISAM ID defines the destination of the ISAM data file. The coding of ISG for implementing the group hierarchy as defined in clause 6.7 is specified in ITSO TS 1000-8.

7.3.1.3 Type of ISAM Secure Data Frame (TDF)

This Data Element, defined in ITSO TS 1000-8, is updated during a CREATE_FRAME command and indicates the Secure Data Frame format and purpose as follows:

— The data file in this Secure Data Frame shall either be encrypted or shall not;

— The Secure Data Frame is signed by an AMS or the ISMS;

— The Secure Data Frame is an acknowledgement of receipt of a data file;

— The data file in this Secure Data Frame contains ISAM program data.

7.3.1.4 ISAM data file

Once an ISAM is operational in a POST data files that alter its contents may be sent from an AMS. Such files contain sequences of commands known as a script, which are executed by the recipient ISAM.

An ISAM shall not execute any received scripts unless the Secure Data Frame containing them has been authenticated, decrypted if required and is intended for that ISAM.

After the running of a script the ISAM shall return an Acknowledgement Secure Data Frame relating to the Secure Data Frame just processed. Any script failure shall be listed in the Secure (ACK) Data Frame. In the event that a command within a script fails any subsequent commands in that script will not be executed by the ISAM. The status code (indicating error) of the failed command will follow the last status code (indicating success) recorded by any previously executed command.

7.3.1.5 Secure Data Frame cryptography

Secure Data Frames shall all be sealed using a digital signature and data files therein may be encrypted. The following general rules shall apply:

— The public key of the AMS or ISMS shall be used by the recipient ISAM to verify the signature of the Secure Data Frame;

— Then the ISAMs individual secret key or group secret key shall be used to decrypt any data files as required;

— The individual secret key of the ISAM generating the acknowledgement shall be used to sign the acknowledgement Secure Data Frame;

— The public key of the individual ISAM shall be used by the AMS or ISMS to verify any acknowledgement Secure Data Frames received.

Note: Where the ISAM is referenced as part of a Physical ISAM Group then all ISAMs in that group will share the secret key of the group key pair if the decryption of data files is required. Although unconventional, by this means the same ISAM messaging application code can be used to accept group messages as for individually addressed messages. Whether part of a group or not, the ISAM shall sign acknowledgements using only its individual secret key.

7.3.2 ISAM Test and Linking

In order to facilitate the detection of ISAMs that have been moved between POSTs all ISAMs carry a programmable password. In order to initialise an ISAM for operation, every time an ISAM is powered up its associated POST shall log on to the ISAM with a password.

The AMS in whatever manner the Licensed Members require shall set this password. For example, the AMS may code an ISAM with an individual password or allocate a common password to a number of ISAMs.

Each time an ISAM is powered up the POST shall send a VERIFY_ISAM_ID command with a “log on” password to the ISAM. Upon receipt of the correct password the ISAM shall, prior to permitting the ISAM to execute any CM transaction processes, carry out a basic self-test program that non-destructively tests the validity of ROM and EEPROM contents. If further testing of RAM and XMEM is deemed necessary then the POST may issue a SELFTEST command (see ITSO TS 1000-8).

If an incorrect password is presented for more than a configurable number of re-tries then the ISAM shall not be able to execute any CM transaction processes until reconfigured by a secure message from an AMS.

7.3.3 ISAM Hot / Action list file

The AMS shall be able, by creating a data file with appropriate scripts, to update and append records to a file that may be searched by the POST application using the SEARCH_ITSO command having an 8 Byte search string as a parameter. This command returns a variable length data string from within the record in the file where the first 8 bytes matches the search string.

This file is intended to facilitate the storage of lists of records, such as Hot or Action lists, where the capability of the POST is limited. In this case the data string returned, when a match is found, is interpreted and acted upon by the POST.

The SEARCH_ITSO command is not intended to be a replacement for implementation of Hot / Action list functions by a suitably capable POST without the use of an ISAM.

Details of the search string coding, file and record formats can be found in ITSO TS 1000-6 and ITSO TS 1000-8.

7.3.4 ISAM HOPS transaction processing

The ISAM when installed in a HOPS shall be defined as an HSAM and may be configured to support the VTRANS_MAC, VBATCH_MAC and CREATE_FRAME commands. These commands allow the post application to use the HSAM to:

— Verify incoming Transaction Records;

— Verify incoming IBatch Headers and generate delete parameters;

— Implement class 3 message generation.

7.3.4.1 Verification of received Transaction Records

Transaction Records originate from a POST and are sealed using the physical ISAM installed in it. This ISAM ID identifies the source of the Transaction Records for subsequent settlement purposes. The seal of the Transaction Record may be verified by any HOPS using the VTRANS_MAC command on an HSAM allocated to the same source. Subsequent to this the Transaction Records may be split into On Us and Not On Us transaction messages or passed in entirety to other HOPS as required.

7.3.4.2 Verification of IBatch Headers

IBatch Headers originate from a POST ISAM and shall be passed to a nominated HOPS along with a batch of Transaction Records. The IBatch Header may be verified at any time. However, once the nominated HOPS has received all the Transaction Records relating to the batch indicated in the header then the delete parameter returned by the HSAM as a result of a successful IBatch Header verification process shall be sent to the originating POST.

7.3.4.3 Class 3 message implementation

The AMS function requires the generation of secure messages for the creating of ISAM resident tables and the subsequent loading of records into those tables (shown as “AMS configured” in Figure 22).

Class 3 messages as defined in ITSO TS 1000-9 are used to transport the data files containing the necessary scripts, as defined in ITSO TS 1000-8, that are required to alter the ISAMs AMS configurable tables.

The CREATE_FRAME command gives the HOPS application the ability to use asymmetric cryptography to encrypt and or Seal a Secure Data Frame, as used in class 3 messaging. In this case the Seal shall be an RSA digital signature.

Annex A
(informative)
Summary of the ISAM command set

A.1 Introduction

The following tables show a summary of all commands accepted by the ISAM. Each command has its own table that shows the command name, its CLA INS numbers, a brief description, an indication of whether the command is active in a POST and/or HOPS ISAM and the formats of the command sent to & response received by the ISAM.

In addition, details of the command's use of the ISAM I/O buffer are shown in the WSAM and RSAM commands sections.

The required section shows the commands, selected from five commands (shown greyed out when not required) that shall be performed either before (shown bold) or after (shown normal) the command tabulated.

The convention used in the *Command* and *Response* rows is to show the command and response data in hexadecimal bytes. Where parameters are to be inserted, the parameter's name is placed between single angle brackets <>. In this case, the number of bytes contained within the parameter is indicated according to the table below:

Indication	**Example**	**Comment**
<Param>	<SW1>	The parameter is a single byte in size.
<AxParam>	<5xDir entry>	The parameter is A bytes in size.
<A?xParam>	<8?Access key>	The parameter may be of variable length but is most likely to be A bytes in size in most current situations.
<??xParam>	<??xNewly created Data Group>	The parameter's length is unknown and will depend on the context of the command's use.
<XXxParam>	<LcxData group>	The parameter may be of any size but it will be defined by a function of some other parameter XX.

A.2 The command set

VERIFY_ISAM_ID **90 18**			**Authenticate ISAM/POST relationship.**		
				POST	**HOPS**
Command	90 18 00 00 <Lc> <Lc bytes of ISAM ID Password>				
Response	<SW1> <SW2>				
WSAM					
RSAM					
Required	V_ISAM_ID	BEGIN	VERIFY_ITSO	WDIR	END

WSAM	**Write data to ISAM I/O buffer.**			
90 40			**POST**	**HOPS**
Command	90 40 <Offset Hi> <Offset Lo> <Lc> <Lc bytes of data>			
Response	<SW1> <SW2>			
WSAM	N/A			
RSAM	N/A			
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

RSAM	**Read data from ISAM I/O buffer.**			
90 42			**POST**	**HOPS**
Command	90 42 <Offset Hi> <Offset Lo> <Le>			
Response	<Le bytes of ITSO data read from Offset> <SW1> <SW2>			
WSAM	N/A			
RSAM	N/A			
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

BEGIN	**Begin session between ITSO Shell and ISAM**			
90 48			**POST**	**HOPS**
Command	90 48 00 <KAS> <Lc> <2xDate> <??xShell Header> <8xMID> <8xRND_C> 00			
Response	<8?xAccess Key> <SW1> <SW2>			
WSAM				
RSAM				
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

OPEN_IPE	**Returns keys required to read an IPE**			
90 4C			**POST**	**HOPS**
Command	90 4C 00 00 01 <KAS> 00			
Response	<8?xAccess Key> <SW1> <SW2>			
WSAM				
RSAM				
Required	**V_ISAM_ID**	**BEGIN**	VERIFY_ITSO	WDIR	END

EXTERNAL_ AUTHENTICATE	**Mutually authenticates ITSO Shell and ISAM**				
00 82				**POST**	**HOPS**
Command	00 82 00 <KAS> <Lc> <Lc bytes of Encrypted RND_T>				
Response	<SW1> <SW2>				
WSAM					
RSAM					
Require	**V_ISAM_ID**	**BEGIN**	VERIFY_ITSO	WDIR	END

VERIFY_ITSO	**Verify Directory or IPE in ISAM I/O buffer.**				
90 4E				**POST**	**HOPS**
Command	90 4E 00 <Mode> 00				
Response	<SW1> <SW2>				
WSAM	Load ISAM I/O buffer with Directory, Fixed or Value Data Group to be verified.				
RSAM					
Required	**V_ISAM_ID**	**BEGIN**	VERIFY_ITSO	WDIR	END

MODIFY_IPE	**Create a certificate for a modified IPE.**				
90 50				**POST**	**HOPS**
Command	90 50 00 00 01 <KAS> 00				
Response	<8?xAccess key> <SW1> <SW2>				
WSAM	Load ISAM I/O buffer with the modified Data Group to be certified.				
RSAM	Read same Data Group (plus certificate) from ISAM I/O buffer.				
Required	**V_ISAM_ID**	**BEGIN**	**VERIFY_ITSO**	WDIR	END

MODIFY_VALUE_IPE	**Create a certificate for a modified value IPE.**				
90 2E				**POST**	**HOPS**
Command	90 2E 00 00 01 <KAS> 00				
Response	<8?xAccess key> <SW1> <SW2>				
WSAM	Load ISAM I/O buffer with <5xDir entry> <48?xData Group containing oldest record> <15?xNew value record>.				
RSAM	Read <5xDir entry> <48xNew Data Group> from ISAM I/O buffer.				
Required	**V_ISAM_ID**	**BEGIN**	**VERIFY_ITSO**	WDIR	END

CREATE_IPE	**Create a certificate for a newly created IPE.**				
90 52				**POST**	**HOPS**
Command	90 52 00 <Type> 01 <KAS> 00				
Response	<8?xAccess key> <SW1> <SW2>				
WSAM	Load ISAM I/O buffer with <5xDir entry> <??xNewly created Data Group>.				
RSAM	Read <5xDir entry> <??+8xCertified Data Group> from ISAM I/O buffer.				
Required	**V_ISAM_ID**	**BEGIN**	VERIFY_ITSO	WDIR	END

DELETE_IPE	**Delete an IPE from an ITSO Shell.**			
90 54		**POST**	**HOPS**	
Command	90 54 00 00 01 <KAS> 00			
Response	<8?xAccess key> <SW1> <SW2>			
WSAM	Load ISAM I/O buffer with an empty IPE Data Group.			
RSAM	Read <5xDir entry> <??+8xCertified Data Group> from ISAM I/O buffer.			
Required	**V_ISAM_ID**	**BEGIN**	**VERIFY_ITSO**	WDIR	END

WDIR	**Create a certificate for a modified Directory.**				
90 56				**POST**	**HOPS**
Command	90 56 00 00 01 <KAS> 00				
Response	<8?xAccess key> <SW1> <SW2>				
WSAM	Load ISAM I/O buffer with modified Directory Data Group.				
RSAM	Read modified Directory Data Group from ISAM I/O buffer.				
Required	**V_ISAM_ID**	**BEGIN**	VERIFY_ITSO	WDIR	END

END	**End session between ITSO Shell & ISAM.**				
90 58				**POST**	**HOPS**
Command	90 58 00 00 00				
Response	<SW1> <SW2>				
WSAM					
RSAM					
Required	**V_ISAM_ID**	**BEGIN**	VERIFY_ITSO	WDIR	END

IMAC	**Store a transaction in the ISAM.**				
90 5A			**POST**	**HOPS**	
Command	90 5A 00 00 00				
Response	<New IBatch header record > <SW1> <SW2>				
WSAM	Load ISAM I/O buffer with transaction data.				
RSAM	Read transaction & MAC from ISAM I/O buffer				
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

LBATCH	**Return a list of IBatch headers.**			
90 5E			**POST**	**HOPS**
Command	90 5E 00 00 00			
Response	<List of IBatch headers> <SW1> <SW2>			
WSAM				
RSAM	Read the transList from the ISAM I/O buffer.			
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

POLL	**Create and delete IBatch headers.**			
90 74			**POST**	**HOPS**
Command	90 74 00 <P2 = number of delete parameters> <Lc = 12 + (P2*11)> <12xCreate IBatch params> <P2*11xDelete params>			
Response	<SW1> <SW2>			
WSAM				
RSAM	Read failed delete parameters from the ISAM I/O buffer.			
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

VTRANS_MAC	**Verify transaction data MAC.**			
90 76				**HOPS**
Command	90 76 00 00 00			
Response	<SW1> <SW2>			
WSAM	Load ISAM I/O buffer with the transaction to be verified.			
RSAM				
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

VBATCH_MAC	**Verify IBatch header MAC.**				
90 78					**HOPS**
Command	90 78 00 00 2C <44xIBatch header to be verified> 00				
Response	<11xDelete IBatch parameters> <SW1> <SW2>				
WSAM					
RSAM					
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

CREATE_FRAME	**Create a signature over a Data Group.**				
90 7A					**HOPS**
Command	90 7A 00 <Sign/Ensign> 00				
Response	<SW1> <SW2>				
WSAM	Load ISAM I/O buffer with the Data Group to signed and (optionally) encrypted.				
RSAM	Read the signed Data Group from the ISAM I/O buffer				
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

UPDATE_FRAME	**Update internal ISAM data.**			
90 7C		**POST**	**HOPS**	
Command	90 7C 00 00 00			
Response	<SW1> <SW2>			
WSAM	Load the ISAM I/O buffer with the Data Group to be processed.			
RSAM	Read the Data Group acknowledgement from the ISAM I/O buffer.			
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

READPK	**Return the ISAM's public keys.**			
90 7E		**POST**	**HOPS**	
Command	90 7E <2xISAM group number> 04			
Response	<2xLength of PK template XX> <2xLength of Certificate YY> <SW1> <SW2>			
WSAM				
RSAM	Read <4xISAM ID> <XxxPublic key template> <YyxCertificate> from the ISAM I/O buffer.			
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

SELFTEST	**Cause the ISAM to test its memory.**				
90 30				**POST**	**HOPS**
Command	90 30 00 <Test> 00				
Response	<SW1> <SW2>				
WSAM					
RSAM					
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

SEARCH_ITSO	**Search the Hot/Action lists**				
90 8A				**POST**	**HOPS**
Command	90 8A 00 <Begin/Cont> 08 <8xISRN>				
Response	<SW1> <SW2>				
WSAM					
RSAM	Read the Hot/Action instructions from the ISAM I/O buffer (if <SW1> <SW2> indicates instructions found).				
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

UPDATE_ITSO_ RECORD	**ITSO specific Update Record command.**				
90 DE				**POST**	**HOPS**
Command	90 DE <Rec Index> <File> <Lc> <Lc bytes of record data>				
Response	<SW1> <SW2>				
WSAM					
RSAM					
Required	**V_ISAM_ID**	BEGIN	VERIFY_ITSO	WDIR	END

Annex B removed