Reference number of document: **ITSO/COR 2.1.4-9**

Title: Corrigendum to Version 2.1.4 of the ITSO Specification

Specification Part(s) affected by this note: TS 1000-0, 1000-1; 1000-2; 1000-3; 1000-4; 1000-5; 1000-6; 1000-7; 1000-8; 1000-9; 1000-10, 1000-11 (Version 2.1.4)

Source of document: **ITSO**
ITSO – Technical Manager

Document type: ITSO Specification Corrigendum
Document subtype: COR
Document template: ITSO 2

Change History:

Version	Date	Comment
2015_0407	07/04/2015	Initial Publication

ITSO

Corrigendum 9 to Version 2.1.4

This Corrigendum notice identifies the corrections to the Parts as noted below:

Corrected Versions of the Specification may be identified by the indicator COR 9 which can be found on the title page under the ISBN Number. The last modified date in the footer of the front page will be 7th April 2015 (2015-04-07) in Parts 0 to 11 inclusive.

Reasons for the Corrigendum:

Section 1:

A number of Technical Notes have been written since the publication of Version 2.1.4 of the ITSO Specification in 2010 which it has been suggested would be best implemented into the existing version, as they are either corrections or clarification which do not alter the intent of or the implementation of the Specification into devices.

In each of the items in this section the relevant Technical Note (which will have been withdrawn following publication of this notice) is referenced so that readers may understand the source of the item in this notice.

Each item is made up of: a rationale, describing the reason for the change; the originating technical note reference; and the changes that are wrought by the note into the Specification. They are noted in this section of the document in Part number order, so that the changes can be referenced into the Specification Parts themselves. Where more than one Part is amended by a Technical Note then the item number will appear in more than one Part reference.

Item numbers and the original Technical Note numbers are noted in the Table of Items (see next page) together with the Parts that are amended.

Section 2:

The Technical Committee (TC) of ITSO have considered a number of other corrections and clarifications that are also suitable for incorporation into this Corrigendum.

They can be found after the Technical Note section.

Section 3:

Additional Items:

1. *The opportunity is taken to update the [DfT's Crown] Copyright notice in all Parts of the Specification.*
2. *Two typographical errors in Part 0 are corrected.*
3. *The Scope of Part 11 is added into the clause on Scope in Part 1.*

New or changed text is shown in blue. Footnotes where they are shown in black are for information only, as they already exist in the specification text. Text shown in italics is for location and instruction purposes only. Deletions where shown are in red with double strikethrough.

SECTION 1

Table of Items

(Note that hyperlinks to each part are include for ease of reference)

Item No	TN	Part(s) affected
1	0381	1
2	0382	6
3	0386	1
4	0388	3
5	0390	5
6	0391	1
7	0392	6
8	0393	5
9	0396	5
10	0397	4
11	0398	6
12	0399	6
13	0400	1 & 5
14	0401	6
15	0403	6
16	0404	6
17	0405	1
18	0406	1
19	0407	1
20	0408	6
21	0410	7
22	0411	6
23	0412	4 & 6
24	0413	1, 3, 4, 7, 8 & 9
25	0414	6
26	0418	6
27	0419	5
28	0421	5 & 6
29	0422	6
30	0427	8 & 10
31	0430	3
32	0432	8
33	0433	5
34	0434	1
35	0435	5
36	0436	1
37	0437	6
38	0438	8
39	0439	8
40	0440	7 & 8
41	0441	7
42	0442	1, 2 & 10
43	0443	8
44	0444	1, 2, 3 & 8
45	0445	5
46	0446	1
47	0447	2
48	0449	8
49	0450	3

Part 1

Item 1 – TN0381

back

The definition of various types of location is included in the ITSO specification. This definition includes zones, which are normally stored in a bit map.

A previous Technical Note introduced location types with 4 bytes of zone bit map. This should have amended table 42 to define the 4th byte of the bit map, but did not.

The impact is clarification only – it does not change processing, messages or CM data structures.

*Amend Part 1, **Clause 4.2.4.3.11**, Table 42 as follows:*

4.2.4.3.11 Zone Bit Map Definition

Each zone shall be allocated a zone number, a specific zone shall be valid for travel (or an event recorded in that zone) if the relevant bit in the zonal bit map is set. Zone numbers are allocated to bits in the zonal bit map as follows.

Table 42 - Allocation of bits in the zonal bit map

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
1	8	7	6	5	4	3	2	1
2	16	15	14	13	12	11	10	9
3	24	23	22	21	20	19	18	17
4	32	31	30	29	28	27	26	25

Item 3 – TN0386

back

Part 1 contains definitions of:

- *The term ASCII; and*
- *The data type ASCII.*

These define how textual data is stored in products and messages. As currently defined these terms and data types could be misinterpreted leading to interoperability problems. This TN tightens up the specification by referring to various international specifications, and removing an invalid reference.

1/ Printablestring

- *Printablestring is referred to as a base data type, but is not defined in EN1545*
- *Printablestring is defined in ASN.1 - however it's a reduced character set and does not support the '@' character, and is therefore not much use in ITSO (because we do have an email address data element in some messages)*
    - *The references to it should therefore be removed from Part 1 of the specification.*

3/ Part 1 Clause 3 Table 2 definition of the term "ASCII"

- *The definition is a bit weak and could be improved by referring to relevant standards:*

a/ "American National Standard for Information Systems — Coded Character Sets — 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII), ANSI X3.4-1986, American National Standards Institute, Inc., March 26, 1986 "

http://en.wikipedia.org/wiki/ASCII#References

b/ "ISO/IEC 646:1991, Information technology — ISO 7-bit coded character set for information interchange"

Note that a reference to this standard is already included in Part 1.

http://en.wikipedia.org/wiki/ISO/IEC_646

4/ Clause 4.1 Table 3 definition of the data type "ASCII"

- *Elsewhere in the specification we refer to use of the UTF8 character set, and it's proposed that we should formalise this by changing the part 1 definition of the ASCII data type to refer to UTF8*
- *the UTF8 character set does support the '@' symbol, see the following references: http://www.columbia.edu/kermit/utf8-t1.html and http://www.utf8-chartable.de/*
- *UTF8 is defined in ISO/IEC 10646, Information technology — Universal multiple-octet coded character set (UCS) (plus amendments to that standard)*

*Amend **Clause 2** References **table 1**, by adding the following into a new row 2 immediately following the title row:*

ANSI X3.4-1986	American National Standard for Information Systems — Coded Character Sets — 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII)									

And the following row in the appropriate place in the sequence of ISO/IEC standards:

ISO/IEC 10646	Information technology — Universal multiple-octet coded character set (UCS) (plus amendments to that standard)[1]									

*Amend **Clause 3** Definition of terms **Table 2** as follows:*

ASCII	American Standard Code for Information Interchange, as defined in ANSI X3.4-1986 and ISO/IEC 646:1991.

*Amend **Clause 4.1** General Data Types **Table 3** as follows:*

Data Type	Name	Format	Size	EN1545 equivalent (see References)
ASCII	ASCII	Text data coded using those ASCII codes included in the UTF8 character set as defined in ISO/IEC 10646, excluding those codes that require more than one byte of storage.	Variable	~~PrintableString~~

[1] Defines the UTF8 character set

Item 6 – TN0391

back

Part 1 contains definitions of data structures used to store location information. There are a number of types of location definition (identified by LocDefType code) and a number of data structure types (numbered LOC1 to LOC4).

An error has been identified in the calculation of the range of LocDefType codes available for use with LOC3 and LOC4 structures. This TN corrects that error.

*Amend **Part 1 Clauses 4.2.4.2.3 & 4.2.4.2.4** as follows:*

4.2.4.2.3 Fixed length structure, LOC3

Only 0.5 bytes are allocated to Location definition type. To determine the value of LocDefType, 200 (decimal) shall be added to the value contained in the location definition type element. For this reason, only location definition types with LocDefType codes in the range 200..2150~~07~~ shall be stored in a LOC3 structure.

4.2.4.2.4 Fixed length structure, LOC4

Only 0.5 bytes are allocated to Location definition type. To determine the value of LocDefType, 200 (decimal) shall be added to the value contained in the location definition type element. For this reason, only location definition types with LocDefType codes in the range 200 to 2150~~07~~ shall be stored in a ~~LOC3 or~~ LOC4 structure.

Item 13 – TN0400

back

The eURI initiative created a standard for flexible terminal accessibility. This has now been formalised as "ISO/IEC 12905". eURI is referenced in the ITSO specifications and therefore the ISO standard number should be added as a formal reference.

Add the following entry to **Table 1** - References and cross-references used in ITSO TS 1000"*, in the appropriate place*:

ISO/IEC 12905	Enhanced Terminal Accessibility (ETA) using cardholder preference interface.				✓					

Item 17 – TN0405

back

The ITSO specification specifies Data Types which may be used in IPEs and Messages. These include a User Defined data type. This TN clarifies the intent behind the User Defined data type.
Note that this clarification is identical to the content of FAQ Part 1 Answer 3.

Amend ***Part 1, Clause 4.1*** *as follows:*

Amend ***Table 3*** *as follows (noting that unchanged rows are omitted for clarity):*

Data Type	Name	Format	Size	EN1545 equivalent (see References)
UD	User defined	This data field may be formatted as the IPE Owner desires (see note following this table)	Variable	no equivalent

Add the following note immediately after ***Table 3****:*

Note. A User Defined (UD) data element may contain whatever values or encoding that the Product Owner (i.e. the owner of the IPE containing the user defined data element) wishes it to contain. The Product Owner will need to communicate the definition of the use of this data element to all POST developers, via service providers, whose POSTs will have to accept the relevant Product Embodiment.

Item 18 – TN0406

back

Data structures for storing location data in IPEs and data messages are defined in Part 1.

The definition of the variable length location data structure, LOC1, includes a length byte. This is currently defined as data type "integer". However, there is no defined data type (in ITSO) of "integer". This TN therefore changes the data type to HEX, which is defined as a binary integer and is the appropriate data type for this element.

Amend ***Clause 4.2.4.2.2*** *Variable length structure, LOC1,* ***Table 9****, as follows:*

Name	**Offset**	**Size**	**Type**	**Comment**
Location Definition type	0	1	LocDefType	
Length	1	1	~~Integer~~HEX	Length of data and any padding in bytes
Data	2	Variable	LOCE	
Padding	2 + length of (data)	Variable		Trailing zeros (if any)

Item 19 – TN0407

back

Part 1 defines location definition data. This includes LocDefType 206 National Bus stop code (NaptanCode).

The description of the data elements is inconsistent between the various structure types, and this TN corrects this. The correct description is "bus stop code" and this is used in most instances. However in Table 26 the terminology "fare stage" is used, which is incorrect.

Amend ***Clause 4.2.4.3.4, Table 26****, as follows:*

Table 26 - Bus Stop Code, LocDefType = 206, LOC3 format

Name	**Offset**	**Size**	**Type**	**Comment**
Location Definition type	0	0.5	LocDefType	
Origin Bus Stop Code ~~Global Bus Network Fare Stage Number~~	0.5	4		This value shall be a nationally defined NaptanCode bus stop number
Destination Bus Stop Code ~~Global Bus Network Fare Stage Number~~	4.5	4		This value shall be a nationally defined NaptanCode bus stop number

Item 24 – TN0413

back

ISAM Groups and POST Sets are mechanisms by means of which ISAMs and POSTs can be addressed as a group, i.e. a message addressed to the group will be delivered to all the members of that group. This simplifies the activities of profiling and updating ISAMs, and of communicating with POSTs.

The various sets and groups available are not formally defined within the ITSO Specification, and this TN rectifies this.

The clauses in Part 4 which deal with ISAM groups are not entirely clear, and need updating to use the new definitions.

*Amend **Clause 3 ITSO Terminology, Table 2**, by inserting the following definitions in the appropriate places in the table:*

Term	Abbreviation	Definition
Physical ISAM Group		A collection of ISAMs that are identified by a common ISAM Group (ISG)[2] value: - The ISMS is aware of these groups, and some ISMS functions can be targeted at a Physical ISAM Group as well as to individual ISAMs; - ISG is subservient to the Licensed Member's OID; - They are used in class 3 messages; – They are used for bulk ISAM updates; - This is a physical group, in that the ISAMs are aware that they are part of the group, because they store a physical ISAM group file.
POST Set		A collection of POSTs that are identified by a common SETID value: – They are not known to the ISMS; – They are used in class 2 messages; – SETID is subservient to the POST Owner's OID; – They are primarily used for distributing Hotlists, Actionlists and POST configuration data; – This is a physical set, in that the POSTs are aware that they are part of the set; – This is a private set in that it is only known to the HOPS which controls it.
Logical ISAM Group		A collection of individual ISAMs; - Are optional but recommended in part 4; - They provide a method of handling 1 or more ISAMs as a single entity; - This is a logical group, i.e. the group is implemented in the back office only, and the ISAM is unaware of the grouping.
Logical POST Set		A collection of POST Sets; - Are optional; - They provide a method of handling 1 or more POST Sets grouped as a single entity; - This is a logical set, i.e. the set is implemented in the back office only, and the POST is unaware of the grouping; - Logical POST Sets may be private in that they are only known to the HOPS which controls them, or may be published to other HOPS for wider application.

back

[2] The term ISG is defined in ITSO TS1000-8

Item 34 – TN0434

back

One of the methods of recording geographical locations provided by ITSO is a national bus stop code, or NaptanCode. This value is defined in the Naptan specifications and within ITSO is encoded in a LocDefType code 206 data structure.

NaptanCode can be 7 characters or 8 characters long. ITSO provides storage space for 8 characters but does not define how 7 character codes should be stored. This proposed change rectifies this.

*Amend **Clause 4.2.4.3.4** as follows:*

Storing NaptanCode values.

NaptanCode values consist of 8 characters, each of which may be mapped to a numeric value, allowing these 8 characters to be stored in 4 bytes of BCD. The mapping between the allowable characters and the equivalent numeric code is shown in the following table. It is suggested that numeric codes could be used throughout in POSTs, avoiding continuous translation between NaptanCode values and the numeric code values. This means that configuration files should all be converted into numeric code values prior to dispatch to the POST.

In circumstances where the NaptanCode only occupies 7 digits, these shall be encoded in the least significant 7 digits of the location element, and the most significant digit set to zero (0).

Item 36 – TN0436

back

Part 1 contains (amongst other things) definitions of location types. A typographic error has been identified in the definition of LocDefType 210, service numbers. A sentence which should have been removed when editing a previous version of the specification, was not removed. This sentence has no relevance to the current version, and this TN removes it.

*Amend **Part 1**, clause **4.2.4.3.8 Service numbers, LocDefType = 210**, as follows (noting that only the relevant paragraph is shown):*

In this context Service number shall be formatted as follows. Char 1 shall be the most significant character in the service number. ~~Note that only the first service number and part of the second are shown.~~

Item 42 – TN0442

back

This item addresses an inconsistency regarding the Date data type, which has caused some interpretation issues.

The Date data type is based on the EN1545 DateStamp. This is defined as follows:

"Number of days relative to 1 January 1997, where 1 January 1997 is day 0."

ITSO's definition of shell and IPE expiry dates is inconsistent with the EN1545 DateStamp definition, in that it specifies a value of zero as having a meaning other than 1/1/1997. The purpose of this item is to clarify and remove this inconsistency.

The special meaning assigned by ITSO is to indicate that:

- *the shell or IPE never expires; and*
- *the shell expiry is devolved to the CM expiry.*

The same can be achieved by programming an expiry well into the future, in the latter case by programming an expiry which equals or is later than the CM expiry.

It is therefore proposed to remove the inconsistency by deleting the special cases as follows:

It is also sensible to consider date rollover. The value is encoded in 14 bits meaning that dates up to and including 9/11/2041 are allowed. Whilst this is clearly a long way in the future, taking account of rollover now will minimise the risk of problems arising in 2041.

It is therefore proposed to amend the definition of Date in Part 1 of the specification, so that a value of 0 means 10/11/2041.

This approach resolves any interoperability issues with the part 2 change proposed. Older POSTs will interpret a value of 0 as meaning "never expires", whilst newer POSTs will interpret it as 10/11/2041. For the next 10 years this has essentially the same meaning. By the time we approach the 2040's it is quite unlikely that any of today's POSTs or customer media will remain in service, having been replaced by newer devices compliant with the changes proposed in this item.

Note that ITSO are considering the date roll over rules necessary to promote interoperability, and will publish these in due course.

Part 1 changes are shown on the next page.

Part 2 changes

Part 10 changes

*Amend **Part 1**, Clause **4.1**, Table **3**, General Data Types, as follows:*

Data Type	Name	Format	Size	EN1545 equivalent (see References)
		Text omitted for clarity		
DATE	Date	According to EN1545 DateStamp A value of zero shall be interpreted as meaning 10/11/2041[3]	14 bits	DateStamp
		Text omitted for clarity		

back

[3] Note that the interpretation of Date values other than zero remains unchanged.

Item 44 – TN0444

The acronym "ISAM" is expanded to two different definitions throughout the Specification – ITSO Secure Application Module and ITSO Security Application Module - the correct definition is ITSO Secure Application Module. This item corrects the Specification to ensure that all expansions are consistent and correct.

Amend ***Table 2 - Terms, abbreviations and their definitions*** *as follows:*

ISAM	See ITSO ~~Security~~ Secure Application Module
ITSO ~~Security~~ Secure Application Module defined in ITSO 1000-8.	ISAM ITSO ~~Security~~ Secure Application Module, as

back

Item 46 – TN0446

back

In Part 1 definitions, (Table 2):

- *TLV is defined as Tag length variable, when in fact the correct definition for TLV is Tag Length Value;*
- *The definition of Hotlist refers to cards, where it should refer to Customer Media and ITSO Shells;*
- *The term "ITSO Licensed Member" has the same meaning as "ITSO Licensee" which is the term used in the ITSO Operating Licence. This is clarified in Part 1.*

*Amend the definition of TLV in **Table 2** as follows:*

Tag ~~l~~Length ~~variable~~Value	TLV	Also known as Type Length Value; a~~A~~ format for creating/describing data records such that the precise data content does not need to be defined except by the originating and accepting parties.

*Amend the definition of Hotlist in **Table 2** as follows:*

Hotlist	A list of Customer Media, ITSO Shells~~cards~~, products or items of equipment where a transaction requires special attention.

*Amend the definition of ITSO Licensed Member in **Table 2** as follows:*

ITSO Licensed Member	The holder of a current ITSO operating licence. This term has the same meaning as the operating licence term ITSO Licensee.

back

Part 2

Item 42 – TN0442

For the detailed rationale for this item please see the note under Item 41 in the section on Part 1 above.

Amend ***Clause 4.1.8*** *as follows:*

4.1.8 ITSO Shell EXPiry date (EXP)

This is the date, normally the end of a month, after which, the ITSO Shell shall no longer be valid in normal use.

Coded as a Data type DATE. ~~, this Data Element may be set to all zeros indicating:~~

- ~~no expiry if the ITSO Shell is alone on an ITSO CM;~~
- ~~the expiry date is devolved to that of the multi-application CM upon which the ITSO Shell resides.~~

Once set, changes to the ITSO Shell Expiry date Data Element are not permitted during the life of the ITSO Shell.

Note: If the multi-application CM has an expiry date, then it is recommended that a date no later than the multi-application CM expiry date shall be copied across to this Data Element when the ITSO Shell is installed.

Amend ***Clause 6.1.8*** *as follows:*

6.1.8 Expiry (EXP)

A fourteen bit binary integer coded as a DATE data type. ~~A value of 0 shall indicate a permanent IPE.~~

back

Item 44 – TN0444

The acronym "ISAM" is expanded to two different definitions throughout the Specification – ITSO Secure Application Module and ITSO Security Application Module - the correct definition is ITSO Secure Application Module. This item corrects the Specification to ensure that all expansions are consistent and correct.

Amend ***Clause 2.4.7 General requirements,*** *as follows:*

In addition support is provided for CM with limited memory capacity. In this case the ITSO Shell and Directory Data Groups may be reduced to a small number of Data Elements that shall be associated with an Orphan IPE Data Group to form a Single IPE ITSO Shell. For processing by the ITSO ~~Security~~ Secure Application Module (ISAM) the reduced ITSO Shell and Directory Data Groups shall be expanded by the Point of Service Terminal (POST) as defined in the CMD. Figure 5 illustrates a single IPE ITSO Shell.

Amend ***Clause 5.2.3 ITSO Security Application Module Identity (ISAMID),*** *as follows:*

5.2.3 ITSO ~~Security~~ Secure Application Module Identity (ISAMID)

back

Item 47 – TN0447

Part 2 describes the usage of data elements within the Log Directory entry. Table 16 introduces the coding of the Log Directory entry and then the following sub clauses describe the usage of each data element. In most cases the data element description makes it clear how to use the data element in both modes (Basic and Normal). However the Sub-Clause that describes the usage of the Record Offset data element does not explicitly state what to do with this data element in Basic Mode. This item clarifies and resolves this by adding an explicit statement.

Amend Clause 8.1.7 as follows (indenting as shown):

8.1.7 Record Offset (RO)

When writing a Log Directory Entry in Normal Mode:

~~A~~ This two bit Data Element, coded 00 or 01, is used to indicate the next record to be written as follows:

— For CM where each record uses a separate Logical Sector. The offset from the start Sector to the next Sector to be written.

— For CM that support multiple records per Logical Sector. The offset, from the start of a single Logical Sector containing a collection of Log records, to the next record to be written.

The record size for such CM is defined in ITSO TS1000-10.

(Note: examples of the use of Record Offset in Normal Mode can be found in Clause 5.1.5.6.)

When writing a Log Directory Entry in Basic Mode:

This Data Element is not used in Basic Mode, but shall be left in the same state (either 00 or 01) as the last Log Directory entry to preserve the state of Record Offset for the next time Normal Mode is accessed.

back

Part 3

Item 4 – TN0388

Hotlists and Actionlists contain search strings which the POST uses to match list items against Shells and IPEs in presented CMs. This TN clarifies how these search strings are used with Actionlists which act on IPEs.

The change should be considered as a specification correction.

Hotlists and Actionlists targeted at a normal shell[4] are required to use search strings of Key Type 0[5]. This searches for a Shell. If a match occurs, and if the Hotlist or Actionlist item relates to an IPE, then:

- *if the match is against a Hotlist, then Part 3 clause 6.4.1.5 mandates that the POST shall use the "IPE ID Optional Additional Identification Group" included in the Hotlist to identify the relevant IPE;*
- *if the match is against an Actionlist, then there is no similar mandate. However there is no other method for identifying the IPE, and a similar clause should be included for completeness.*

*Amend Part 3, **Clause 6.4.2.5**, by adding the following as a new first bullet point:*

— If the matching Actionlist record relates to an IPE, where an IPE ID Optional Additional Identification Group is included in the Actionlist record, then the POST shall use this information to identify the IPE that is the target of the Actionlist record.

back

Item 24 – TN0413

*Amend **Part 3, Annex B**, title as follows;*

Annex B
Informative
Typical Physical ISAM Group and ISAM sequence number updating

back

[4] i.e. not a compact shell

[5] Part 3 clauses 6.4.1.4 & 6.4.2.4

Item 31 – TN0430

back

The class 3 message application logic as specified in TS1000 is perfectly adequate when Secure Data Frames (SDFs) are applied to the target ISAM(s) in chronological date order. This requirement is enforced by the current ISAM application.

However if SDFs are missed and a later frame applied then the previous frame cannot be applied unless recreated by the ISMS or AMS HOPS with a date later than the date of the last frame applied.

This technical note improves the fault tolerance and robustness of the delivery of SDFs pending the incorporation of all SDF handling logic inside the ISAM at some time in the future.

The following table illustrates the application of SDFs in all combinations of sequence of application of the logic defined in TS1000-3 e.g.Case 1 followed by cases 1 to 4 case 2 followed by cases 1 to 4 etc.....

The flaws identified when using the currently specified logic and Secure Data Frames are applied out of chronological order are shown in red text.

Case (n) in Column followed by Case (n) in row	**Case 1**	**Case 2**	**Case 3**	**Case 4**
Case 1	1.1	1.2	1.3	1.4
Case 2	1.5	1.6	1.7	1.8
Case 3	1.9	1.10	1.11	1.12
Case 4	1.13	1.14	1.15	1.16

The problems identified are:

1. *For 1.2 and 1.5 above:*

   If a case 2 message is created and applied one or more days after a case 1 message and the case 1 message has been missed, the subsequent application of the case 1 message will fail.

   a. *If a case 1 message is created and applied one or more days after a case 2 message and the case 2 message has been missed, the subsequent application of the case 2 message will fail.*

   Issue 1 can be solved by ensuring that (SDFs) are applied in chronological date order and no change is proposed.

2. *For 1.7 above:*

   a. *If a case 3 message is received before the scheduled case 2 message (even on the same day) then the case 3 message will be applied erroneously as it matches the case 4 logic.*

   Issue 2 can be solved by removing the case 4 logic (Case 4 has never reportedly been applied by any current AMS HOPS).

3. *For 1.10 above:*

    a. *If a case 2 message is received before the scheduled case 3 message (even on the same day) then the current case 2 logic will prevent the message being applied*

    Issue 3 can be solve by changing the logic in case 3 to Group_Message_Seq# <= ISAM_Group_Seq#

This corection thus:

1. *Removes the redundant case 4 logic*
2. *Modifies case 3 logic to read ..... Group_Message_Seq# <= ISAM_Group_Seq#*

This correction was put forward as a consensus change from the SSIG WG1.

Amend clause 6.3.8.1.2 as follows:

Case 3 Update depends on previously applied Group update

Where Group_Message_Seq# <= ISAM_Group_Seq#

further text omitted for clarity.....

Delete the contents of Case 4 leaving a placeholder to avoid additional renumbering as follows:

Case 4 ~~Single ISAM Update is part of Group wide update~~ This case is no longer required

~~Where Group_Message_Seq# = 1+ ISAM_Group_Seq#~~

~~IF ISAM_Message_Seq# = 1+ ISAM_Seq# : Execute INDEX_UPDATE function~~

~~FOR each Secure Data Frame in the message: Execute APPLY_FRAME function~~

~~NEXT~~

~~Flag the list of Secure Acknowledgements Logged against this message as a successful ISAM Update.~~

back

Item 44 – TN0444

back

The acronym "ISAM" is expanded to two different definitions throughout the Specification – ITSO Secure Application Module and ITSO Security Application Module - the correct definition is ITSO Secure Application Module. This item corrects the Specification to ensure that all expansions are consistent and correct.

Amend ***Clause 1.2 Context of a POST within the ITSO Environment,*** *as follows:*

— they shall physically contain an ITSO ~~Security~~ Secure Application Module (ISAM), which is unique to the POST and is not shared by other POSTs.

Item 49 – TN0450

back

Annex F to Part 8 of the Specification deals with the use of LOG1 files in an ISAM.

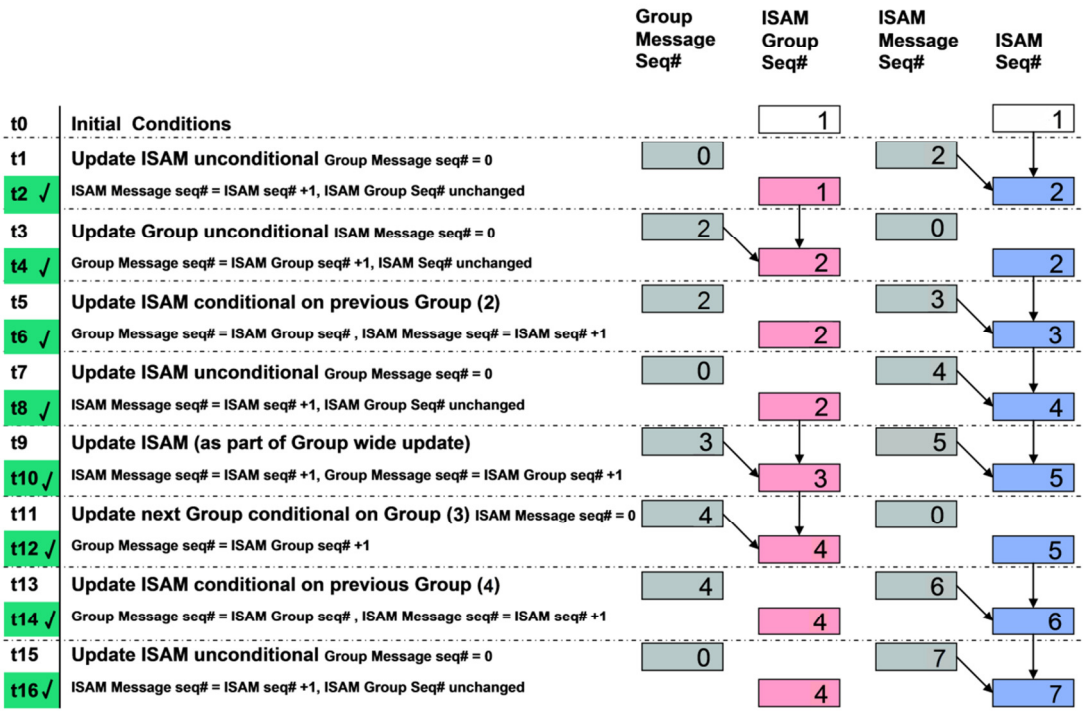
Clause F3 File Content and basic usage, point 3, states that the values in the LOG1_SEQ# file will be initialised at 000001 for both ISAM_Group_Seq# and ISAM _Seq#.

However, the "ISAM Class 3 message sequencing Normal flow" diagram in Annex B to Part 3 of the Specification shows (in step "t0 Initial Conditions") that the starting values of ISAM_Group_Seq# and ISAM_Seq# will be 0.

This diagram therefore needs to be corrected to reflect the initialised and subsequent values as above.

Amend the first diagram "ISAM Class 3 message sequencing Normal flow" in ***Part 3, Annex B*** *as follows:*

ISAM Class 3 message sequencing Normal flow




ITSO

Part 4

Item 10 – TN0397

back

Recording Stored Travel Rights (STR) current values correctly in the HOPS is clearly important. Critical to this is the receipt of add value messages (message codes 0101 & 0102). To maximise the probability that add value messages will be received by the HOPS, the 0103 Load Check message is also generated by POSTs, which sends the same information as the original add value message. This provides a second route by means of which this information can be transmitted to the HOPS.

To clarify use of the 0103 Load Check message a sub-clause was added to part 4, clause 7.3.1 in version 2.1.4 of the specification. The intention of this clause was that the entire STR IPA should be updated upon receipt of an 0103 message in circumstances where the 0101 or 0102 message had not yet been received. As drafted this clause was too restrictive in that it refers only to the IPA History Store, whereas it should have required that the entire IPA be updated. The clause should therefore be amended.

*Amend **Part 4 Clause 7.3.1** as follows:*

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 update the relevant IPA, make a record in the IPA history store using the information contained in the 0103 message, and the event shall be 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 history 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.

Note that FAQ Part 4 item 2 also applies to this issue.

Item 23 – TN0412

back

Parts 4 and 6 contain some incorrect, inconsistent and misleading terminology. The terms "Un-Hot" and "Un-Hotlist" are used whereas the correct term is "Un-Block". This is because the relevant clauses refer to the un-blocking of Shells and IPEs which have previously been blocked. The clauses do not refer to the removal of Hotlist items.

Part 4 clause 7.5.2.2 title includes the term "Un-Hot".

Amend ***Part 4, Clause 7.5.2.2*** *Un-Hot by Actionlist, changing the title as follows:*

7.5.2.2 Un-Block~~Un-Hot~~ by Actionlist

Item 24 – TN0413

back

*Amend the following **Part 4** clauses as shown:*

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:

- Physical 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 Physical 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_Mesage_Seq# set to 0.
4. Messages intended for application to a single ISAM within a Group that are dependent 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

8.2.6.1 Physical ISAM Groups

The AMS shall provide the capability to assign ISAMs to Physical ISAM Groups.

Note: An ISAM may only be allocated to one Physical ISAM Group within the ISMS.

8.2.6.2 Logical ISAM Groups

It is recommended that the AMS provides the capability to assign individual ISAMs ~~Physical ISAM Groups~~ to Logical ISAM Groups. Individual ISAMs ~~Physical ISAM Groups~~ may belong to one or more Logical ISAM Groups.

8.2.6.3 ISAM Group Functions

The provisions of this sub-clause apply to both Physical ISAM Groups and Logical ISAM 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.

Notes: 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 Physical ISAM Group within the ISMS. s may be made up of one or more s.~~

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;

— ISAM Groups (Physical);

— 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: Physical ISAM grouping, accepted IPEs, POST revalidation capability, etc.

Locally controlled tables are:

ISAM Configuration;

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.

8.4.2 Physical ISAM Groups

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

AMS defined Physical~~logical~~ group number;

Record revision number;

Valid from date;

Valid until date;

Issuer identifier (IIN);

ISAM ID / OID;

Index to the RSA Public Key[6] record that is used for this ~~logical~~ grouping.

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

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 Physical ISAM Group);

— IIN of the Product Owner of the IPE in question;

— OID of the Product Owner of the IPE in question;

---

[6] See clause 8.3

— 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;[7] [8]

— FN_S reference;

— Request type (Add or Remove IPE 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) 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 Physical ISAM Group);

— IIN of the ITSO Directory owner;[9]

— OID of the ITSO Directory owner;[10]

— 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:

---

[7] If ISAM is authorised to retail the IPE in question

[8] Proxy ISAM reference cannot be used for a group-based command

[9] This is 633597 (coded as BCD)

[10] This is FFF8 (hex)

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 Physical 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:

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 Physical 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);[11]

— 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:

---

[11] If the CM platform in question requires such keys

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

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, Physical ISAM Group);

Action Code.

The ISMS will respond with an ISMS-AMS Information Packet message[12]. 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)

8.6.4 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 Logical Ggroupsing, then the interface shall support the setting up and management of Llogical Ggroupings ~~of ISAMs~~.

8.7 Functionality

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

— Installation / commissioning of ISAMs;

— Create ISAM Physical Ggroupsing;

— Change ISAM Physical Ggroupsing;

— Take an ISAM out of service;

— Reinstate an ISAM to service;

— Make changes to ISAM Data;

— Introduction of new product into scheme;

[12] Of type ISMS_INFO_INVENTORY

— 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.

8.7.2 Create ISAM Physical Ggroup~~ing~~

The AMS shall carry out the following sequence of tasks:
Stage 1: Create Physical ~~logical~~ Ggroup and assign ISAMs:
— Create the required Physical Ggroup, identify said Physical Ggroup and assign one or more ISAMs to the Physical Ggroup.

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 Physical Ggroup~~ing~~

The AMS shall carry out the following sequence of tasks:

Stage 1: Add / delete ISAM from Physical Ggroup:

— Add or remove ISAMs from the Physical Ggroup 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.

back

Part 5

Item 5 – TN0390

back

All IPEs contain a RemoveDate data element. This element supports a function which retains an expired IPE within the Shell for a defined period of days, so that it can be referred to by either the Product Owner, the CM holder, or any other Licensed Operator. This could be used, for example, as proof of travel, or as evidence for a refund. The IPE may not be removed from the Shell (to free up space for other IPEs to be loaded) until the period of days defined in RemoveDate has elapsed since the IPE expiry date.

The RemoveDate mechanism includes a facility which prevents IPE removal for any reason – to achieve this the RemoveDate element is set to a value of 255. The intention of this was that only the Product Owner (or their authorised representative) could remove an expired IPE. A good example of this is the TYP 16 Identity IPE.

The current specification wording suggests that the IPE may never be deleted from the Shell, whereas the intention was that only the IPE Owner could delete the IPE. This change corrects this.

Amend the following clauses as follows:

- ***Clause 2.2.1.1, table 2, TYP 2***
- ***Clause 2.4.1.1, table 10, TYP 4***
- ***Clause 2.5.1.1, table 15, TYP 5***
- ***Clause 2.7.1.1, table 22, TYP 16***

ITSO Name	Offset	Data Type	Size Bytes	EN1545 Equivalent	Group	Comment
Rows omitted for clarity						
RemoveDate	2	RDATE	1	HangoverPeriod	IPE	For this IPE, the remove date shall always be programmed with 255, indicating that the IPE may not be removed except by the Product Owner or their authorised representative.
Rows omitted for clarity						

Amend the following clauses as follows:

- ***Clause 2.3.1.1, table 7, TYP 3***
- ***Clause 2.6.1.1, table 20, TYP 14***
- ***Clause 2.8.1.1, table 25, TYP 17***
- ***Clause 2.9.1.1, table 27, TYP 22***
- ***Clause 2.9.2.1, table 27a, TYP 22***
- ***Clause 2.10.1.1, table 31, TYP 23***
- ***Clause 2.10.2.1, table 31a, TYP 23***
- ***Clause 2.11.1.1, table 136, TYP 24***
- ***Clause 2.12.1.1, table 36, TYP 25***
- ***Clause 2.13.1.1, table 40, TYP 26***

ITSO Name	Offset	Data Type	Size Bytes	EN1545 Equivalent	Group	Comment
RemoveDate	2	RDATE	1	HangoverPeriod	IPE	A count of days. The IPE can be removed after ExpiryDate + RemoveDate by any POST, except that a~~A~~ value of 255 indicates that the IPE may not be removed except by the Product Owner or their authorised representative.

Item 8 – TN0393

back

The TYP 2 Stored Travel Rights (STR) IPE contains data elements which allow a capped fare system to be implemented. A capped fare system is one in which a user pays for initial Journeys at the normal fare, but once the aggregate of those fares equals a maximum fare for (e.g.) the day (i.e. a cap), then all further journeys that day are free.

One of those elements is CumulativeFare, which is used to store the aggregate fare paid. The instructions relating to this data element are in one small respect incorrect, and this TN amends that.

*Amend **Clause 2.2.1.2**, **Table 4**, as follows:*

ITSO Name	Offset	Data Type	Size Bytes	EN1545 Equivalent	Group	Comment
Rows omitted for clarity						
CumulativeFare	15	VALI	1.625	CumulativeFare	V	Cumulative fare, used for discounting fare in multi-leg journeys, the currency defined by ValueCurrencyCode shall apply. Only positive values shall be stored in this data element. The fare paid for qualifying journey legs shall be added to the value already held in this element. The value held in this element shall be reset ~~to zero (0)~~ upon commencement of a new qualifying journey.
Rows omitted for clarity						

Item 9 – TN0396

back

The TYP 14 and 16 IPEs include an EntitlementExpiryDate data element, which is provided so that the expiry of the entitlement can be defined independently of the expiry of the IPE. This is particularly useful in the case of a TYP 16 IPE which stores combined identity and entitlement data.

The definition of EntitlementExpiryDate in these IPEs is causing confusion. This TN clarifies the definition of this element.

Amend the following clauses:

- ***Clause 2.6.1.1 Table 20*** *TYP 14 IPE Data Group*
- ***Clause 2.7.1.1 Table 22*** *TYP 16 IPE Data Group*

As follows:

ITSO Name	Offset	Data Type	Size bytes	EN1545 Equivalent	Group	Comment
EntitlementExpiryDate	11.25	DATE	1.75	EndDateStamp	IPE	Last date of validity of ~~Date~~ a specific entitlement ~~expires~~*.

*In **Clause 2.6.1.1 Table 20** amend the footnote referenced at the point in the Comment column marked with a [3] as follows:*

For example, the day before the date when a scholar becomes an “adult”.

*In **Clause 2.7.1.1 Table 22** in the row for the data element “EntitlementExpiryDate” add the following footnote referencing it at the point in the Comment column marked with a superscripted footnote number (similar to that described and implemented for the same data element in the Table 20).*

For example, the day before the date when a scholar becomes an “adult”.

*Amend the following typographical error in **Part 5 Clause 2.6.1.1:***

- *The section heading for 2.6.1.1 and the table heading for table 20 have become combined onto a single line. Separate these onto two lines.*

*Amend the following for consistency with other similar tables in **Part 5, Clause 2.7.1.1**:*

- *Move the following text, which is standard in all IPE definition sections of this part, so that it appears after table 22 as the second note.*

Note that the shaded area comprises the Dataset Header as defined in ITSO TS 1000-2.

Item 13 – TN0400

back

The eURI initiative created a standard for flexible terminal accessibility. This has now been formalised as "ISO/IEC 12905". eURI is referenced in the ITSO specifications and therefore the ISO standard number should be added as a formal reference.

*Amend **Clause 2.7** ITSO ID IPE, TYP = 16, footnote 4, as follows:*

The terminal may find URI information in an ITSO Private Application (to be defined) or as defined in ISO/IEC 12905 ~~CWA 13987:2003 Part 1~~ (i.e. in an eURI ISO application selected by the eURI AID).

Item 27 – TN0419

back

A Transaction type code is included in Transient Ticket records, and in various ITSO messages. This code indicates the type of Transaction which has taken place.

The Transaction type code is stored in a data element called TransactionType. The TransactionType code list is derived from EN1545, using the code list entitled EventTypeCode. For the benefit of developers, this code list is reproduced in an informative annex to ITSO TS1000-5.

Code zero is defined as "Not-Specified". As TransactionType is only a 4 bit field, only 16 codes can be stored in TransactionType; code 0 is used for two purposes within ITSO. The following note adds these uses to the informative annex, as a cross reference and for the benefit of developers.

Note that the following is consistent with the guidance in DG0007.

*Amend **Part 5, Annex A, Clause A.20**, by adding the following note at the end of clause A.20.*

Note that code 0 has been used for three purposes within the ITSO environment:

- In a Transient Ticket record created during a mid-journey validation event in a check in – check out environment with Product selection on exit;
- To indicate creation of an IPE which contains no value (e.g. a TYP 2 STR IPE where no value is loaded initially), reference the IPE definitions in this specification; and
- To indicate a Transaction where there is no suitable Transaction Type code defined, for example enabling or amending Auto-Renew.

Item 28 – TN0421

Part 5 contains the definitions of Extended Value Record Groups, which use the abbreviation VGXREF.

VGXREF1 and VGXREF 2 define extended Value Record Groups for Capping.

In both of these VGXREFs one of the accumulators has been assigned a Data Type of HEX when it should be VALI.

*In **Clause 4, Table AD1 and AD2** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

ITSO Name	Offset	Data Type	Size Bytes	EN1545 Equivalent	Group	Comment
Rows omitted for Clarity						
UncappedAccumulator1	5	~~HEX~~ VALI	2	CumulativeFare	VX	
Rows omitted for Clarity						
UncappedAccumulator2	5	~~HEX~~ VALI	2	CumulativeFare	VX	
Rows omitted for Clarity						
UncappedAccumulator3	5	~~HEX~~ VALI	2	CumulativeFare	VX	
Rows omitted for Clarity						
UncappedAccumulator4	5	~~HEX~~ VALI	2	CumulativeFare	VX	
Rows omitted for Clarity						

back

Item 33 – TN0433

There are 4 occurrences of "TYP22Flag" which should be "TYP22Flags".

*In the header for **Clause 2.9.1.3** and the title line for **table 30** amend "TYP22Flag" to "TYP22Flags" as follows:*

2.9.1.3 Typ22Flags definitions

Table 30 - TYP22Flags definitions

*And in the header for **Clause 2.9.2.3** and the title line for **table 30a** amend "TYP22Flag" to "TYP22Flags" as follows:*

2.9.2.3 Typ22Flags definitions

Table 30a - TYP22Flags definitions

back

Item 35 – TN0435

It has generally been accepted that space-saving IPEs (TYP27, 28 & 29) can only be added to Compact ITSO Shells and all other IPEs can only be added to Full ITSO Shells.

However, the definitions for space-saving IPEs in Part 5 of the Specification do not unambiguously preclude the addition of a space-saving IPE to a Full ITSO Shell. Whilst this may or may not be physically possible, this behaviour is not currently supported and is an unintended implication. The ambiguity therefore needs to be removed from the Specification.

*Amend the relevant paragraph in **Part 5, clauses 2.14, 2.15 & 2.16** as follows:*

The IPE is designed to use the minimum amount of memory space possible, and ~~may~~ shall only be implemented in single function small memory customer media types. Details of the mapping of the IPE to a particular CMD are found in the appropriate CMD definition within ITSO TS 1000-10.

back

Item 45 – TN0445

There is a typographical error in the final sentence of the "Flag purpose" description of IPEPriorityOverride.

*Amend **Tables 6, 14 & 19** as follows:*

Data omitted for clarity		
1	IPEPriorityOverride	When set to one (1) this IPE shall be used in preference to any other payment mechanism, stored travel rights or electronic purse, contained within the customer media, whether an IPE, private entity or an entity outside the ITSO shell. This flag shall always take precedence over any other IPE prioritisation method. POSTs setting this flag to one (1) shall ensure that no equivalent flag in any other IPE is set to one (1), and if any such flag is set to one (1), shall only set this flag to one (1) if the other flag has first been cleared.
Data omitted for clarity		

back

Part 6

Item 2 – TN0382

The ITSO specification provides for loyalty products.

This TN defines an editorial change to make the purpose of one of the messages associated with loyalty products clearer.

*The title for the 0205 message, "*Loyalty amendment (transaction reversal)*", is currently causing confusion. A HOPS needs to know precisely what type of transaction took place, and the 0205 message is intended to indicate transaction reversal. The title of the message section is therefore amended to make this clear.*

*Amend Part 6, **Clause 4.4.24** as follows:*

4.4.24 Loyalty add points, Loyalty redemption, Loyalty ~~amendment (~~transaction reversal~~)~~, codes 0203, 0204, 0205.

Table 33 - Loyalty add points, Loyalty redemption, Loyalty ~~amendment (~~transaction reversal~~)~~, codes 0203, 0204, 0205 – RecordFormatRevision = 2.

Note that other text and tables within this clause are omitted for clarity.

back

Item 7 – TN0392

Part 6 uses the term "Licensed Operator" extensively. This term is not defined within the specification (although it is defined in the Operators' Licence). For correctness, this changes the term to "Licensed Member", which is defined in the specification and is used in other parts.

*Amend **Part 6** as follows:*

Change all instances of the term "Licensed Operator" (including plurals and possessives) to "Licensed Member".

back

Item 10 – TN0398

POST Configuration Data (PCD) is a method of sending parameter values to POSTs. This method is defined in Part 6 of the specification. This change formally clarifies an ambiguity in the specification – the ambiguity had already been dealt with in the form of an answer in the FAQ register.

Part 6 Table 98 defines the general structure of POST Configuration Data (PCD) messages. It is not clear how the ParameterTableIdentifier element is used, and this was clarified in a FAQ answer on Part 6, number 21. This amendment adds that answer to Part 6.

*Amend **Part 6 Clause 6.2** by adding the following below Table 98:*

Note that ParameterTableIdentifier shall be prefixed to every row in the table.

back

Item 12 – TN0399

Embodiment parameter lists are used to send the parameter values necessary for IPE creation to POSTs. These are defined in Part 6.

A data element common to all IPE types and therefore common to all embodiment parameter list types is IPEBitMap. The data length currently specified in embodiment lists for this element is "0 or value".

There are two rule codes defined for this data element:

- *if rule code 1 is used, then the element length in the embodiment specification is 0;*
- *if rule code 2 is used, then IPEBitMap is included in the embodiment specification.*

In the latter case where rule code 2 is used, then the element length should be set to an appropriate value. This value is clearly one byte. This TN amends the specification to mandate that length is one byte. This is an editorial change only with no impact on product design or configuration.

It should be noted that Part 6 FAQ item 49 also applies to this issue.

*Amend **Part 6, Clause 8**, **Tables 131 - 139, 141 - 145, 2.138 – 2.140, 2.145, 3.131, 3.133, 3.134**, as follows (noting that unaffected table rows are omitted for clarity:*

LD	Information only					LD	LD	LD
Element Number	**Target IPE Group**	**Target IPE ITSO Name**	**Target IPE Data Type**	**Included in target IPE?**	**Content generation rule**	**Rule Code**	**List Data Size**	**List Data**
*	H	IPEBitMap	BMP	Always	Set to value in embodiment spec or set to value determined upon IPE creation	1 or 2	0 or 1~~value~~	null or value

back

Item 14 – TN0401

TN0351 made various amendments to the instructions for handling first use of an ITSO Stored Travel Rights (STR) IPE, and the associated 0106 message. These changes included removing the word "load", which was incorrect, from the title of the Part 6 clause which defined the 0106 message.

Unfortunately, whilst the word "load" was removed from the clause title, it was not removed from the table title.

*Amend **Clause 4.4.9, Table 17** title as follows:*

Table 17 - First Use of Stored Travel Rights ~~(Load)~~, code 0106 – RecordFormatRevision = 2.

back

Item 15 – TN0403

Auto-Renew is a feature provided by ITSO which allows a product to be automatically renewed upon expiry. The 0304 message is used to report to the HOPS when Auto-Renew events take place.

There is a minor error in the definition of this message. The Auto-RenewValue data element is used to indicate the monetary value of the Auto-Renew transaction, and is defined as being extracted from the IPE. This latter point is incorrect because the value is not stored within the IPE, and the value should be deduced by the POST. The opportunity is also taken to add explanation.

*Amend **Part 6, Clause 4.4.32, Table 64**, as follows:*

Auto-RenewValue	~~IPE~~POST	VALI	2	The Monetary value of the Auto-Renew Transaction, where known~~Revised value~~.

back

Item 16 – TN0404

0207 & 0208 Messages are used to send data relating to the creation and amendment of IPEs.

These messages contain a complex structure, allowing different data to be sent depending upon the TYP of the IPE to which the message refers.

In specification version v2.1.4, the definition of a 0207/0208 message for TYP 24 IPEs was removed at Record Format Revision (RFR) 2, 3 and 4. This change was authorised by TN0234.

The way this was done has caused some confusion, and this amendment is proposed to avoid such confusion.

Modify Part 6 as follows:

4.4.26.6 ~~Not Used~~IPE TYP 24

In this version of the specification, transmission of 0207 and 0208 messages relating to TYP 24 IPEs is not permitted at Record Format Revision 2.

4.5.26.6 ~~Not Used~~IPE TYP 24

~~set to 0.set to 0.set to 0.~~

In this version of the specification, transmission of 0207 and 0208 messages relating to TYP 24 IPEs is not permitted at Record Format Revision 3.

4.6.26.6 ~~Not Used~~IPE TYP 24

~~set to 0.set to 0.set to 0.~~

In this version of the specification, transmission of 0207 and 0208 messages relating to TYP 24 IPEs is not permitted at Record Format Revision 4.

4.7.26 Create or Amend Ticket IPE, code 0207, 0208 – RecordFormatRevision = 5

This records the creation or amendment of a ticket IPE. If a simultaneous journey is made a journey record shall also be transmitted.

The actual Data is depend~~a~~ent upon the type of IPE being created or amended. For efficiency, the record is split into common data (common to all IPEs), IPE TYP specific data and a footer.

Note that for this version of the Specification, only data relating to a TYP 24 IPE may be transmitted using RecordFormatRevision 5 of these messages.

Data from the most recently written IPE Value Group only shall be recorded in the appropriate elements of this transaction record. Only one set of elements shall be recorded in the record, even where more than one Value Group exists.

It is not mandatory to send a 0208 message in parallel with a specific change message (e.g. a 0303 deposit refund message), if the 0208 message does not convey any additional information (i.e. the contents of the additional data items sent in the 0208 message are unchanged), and if both messages would have been sent to the same destination(s).

However, optionally 0208 messages can be sent under these conditions.

back

Item 20 – TN0408

Part 6 tables 27 and 3.27 define the 0120 and 0121 "Create or Amend Stored Travel Rights" message. Table 27 defines RecordFormatRevision 2, and Table 3.27 defines RecordFormatRevision 3. This message is created by POSTs and sent to HOPS when a TYP 2 IPE is created or amended.

RecordFormatRevision 3 (Table 3.27) was introduced in version 2.1.4 of the specification. Two data elements were incorrectly named in Table 3.27, TYP2Flags was misnamed IPE2Flags, and TYP2ValueFlags was misnamed IPE2ValueFlags. These message data elements are intended to match IPE data elements (which are TYP2Flags and TYP2ValueFlags), and for the avoidance of doubt should be renamed to match the names used in the IPE and in RecordFormatRevision 2.

Another element name mismatch between the definition of the TYP 2 IPE in Part 5 and the associated message definitions in Part 6 has been detected. The IPE element StartDateAutoTopUp has been misnamed in the following messages, where the element is misnamed StartDateSTR:

- *0106 RecordFormatRevision 2 Table 17;*
- *0120/0121 RecordFormatRevision 2 Table 27;*
- *0120/0121 RecordFormatRevision 3 Table 3.27;*
- *0D01 Table 122.*

All these instances should be corrected for proper matching between the IPE definition and the message definition.

*Amend **Clause 4.4.9** First Use of Stored Travel Rights code 0106 as follows:*

Table 17 - First Use of Stored Travel Rights (Load), code 0106 – RecordFormatRevision = 2.

Name	Source	Format	Size	Comment
Rows omitted for clarity				
StartDateAutoTopUp~~StartDateSTR~~	IPE	DATE	2	A 1.75 byte value, occupying bits 0-7 of the least significant byte, and bits 0-5 of the most significant byte. Bits 6-7 of the most significant byte shall be set to 0.
Rows omitted for clarity				

back

*Amend **Clause 4.4.19** Create or Amend Stored Travel Rights, Codes 0120, 0121, RecordFormatRevision = 2 as follows:*

Table 27 - Create or Amend Stored Travel Rights, codes 0120, 0121 – RecordFormatRevision = 2.

Name	Source	Format	Size	Comment
Rows omitted for clarity				
StartDateAutoTopUp~~StartDateSTR~~	IPE	DATE	2	A 1.75 byte value, occupying bits 0-7 of the least significant byte, and bits 0-5 of the most significant byte. Bits 6-7 of the most significant byte shall be set to 0.
Rows omitted for clarity				

*Amend **Clause 4.5.19** Create or Amend Stored Travel Rights, Codes 0120, 0121, RecordFormatRevision = 3 as follows:*

Table 3.27 - Create or Amend Stored Travel Rights, codes 0120, 0121 – RecordFormatRevision = 3.

Name	Source	Format	Size	Comment
Rows omitted for clarity				
TYP2Flags~~IPE2Flags~~	IPE	BMP	1	
Rows omitted for clarity				
StartDateAutoTopUp~~StartDateSTR~~	IPE	DATE	2	A 1.75 byte value, occupying bits 0-7 of the least significant byte, and bits 0-5 of the most significant byte. Bits 6-7 of the most significant byte shall be set to 0.
Rows omitted for clarity				
TYP2ValueFlags~~IPE2ValueFlags~~	IPE VG	BMP	1	A 0.375 byte value, occupying bits 0 to 2, bits 3 to 7 shall be set to 0
Rows omitted for clarity				

*Amend **Clause 7.3.2** Stored Travel Rights details, Code 0D01 as follows:*

Table 122 - Stored Travel Rights details, Code 0D01, Transaction details record

ITSO Name	Format	Size bytes
Rows omitted for clarity		
StartDateAutoTopUp~~StartDateSTR~~	DATE	2

back

Item 22 – TN0411

This amendment corrects references to "directory header" as this became obsolete in version 2.1 but was overlooked at the time, and also removes spurious restriction on the content of the Data Element FormatVersionCode.

*Amend **Clause 4.2.1 item 2** as follows:*

2. Records of transactions which create or delete an ITSO shell, or which change the directory contents shall be sent to the owner of the ITSO shell, identified by the OID in the ~~directory header~~ Shell Environment Data Group, except that in the case of Compact Shells messages with message codes 0001 to 0007 (inclusive) shall not be created or sent. In the case of Compact Shells all other messages which would normally be sent to the Shell Owner shall be sent to the Product Owner.

*Amend **Footnote 6 on Page 15 under Table 7** as follows:*

Data records returned to the card or shell owner, identified by OID found in the ~~directory header~~ Shell Environment Data Group.

*Amend **Tables 8 rows 6-8, Table 3.8 rows 6-8, Table 4.8 rows 6-8, and Table 5.8 rows 6-8** as follows:*

Name	***Source***	***Format***	***size***	***Comment***
Rows omitted for clarity	----	----	--	----------
FormatVersionCode	Shell	FVC	*1*	Format version information from the ~~directory header~~ Shell Environment Data Group ~~A 4-bit number occupying bits 0-3, bits 4-7 shall be set to 0.~~
KeyStrategyVersion	Shell	KSC	*1*	Format version information from the ~~directory header~~ Shell Environment Data Group
KeyVersion	Shell	KVC	*1*	Format version information from the ~~directory header~~ Shell Environment Data Group
Rows omitted for clarity	----	----	--	----------

back

Item 23 – TN0412

back

Parts 4 and 6 contain some incorrect, inconsistent and misleading terminology. The terms "Un-Hot" and "Un-Hotlist" are used whereas the correct term is "Un-Block". This is because the relevant clauses refer to the un-blocking of Shells and IPEs which have previously been blocked. The clauses do not refer to the removal of Hotlist items.

Part 6 tables 95 & 96 defines the actions which may be conducted by Actionlist. - Action codes 6 and 7 use the terms "Un-Hotlist" and "Un-Hot".

*Amend **Part 6, Clause 5.3.3.3, Table 95** - Actionlist, Code 0C03, ActionToTake Definition, as follows:*

Code	Meaning
	Rows omitted for clarity
6	Un-Block~~Un-Hotlist~~ Shell
7	Un-Block~~Un-Hotlist~~ IPE
	Rows omitted for clarity

*Amend **Clause 5.3.3.3, Table 96** - Actionlist, Code 0C03, Actions Which May Be Taken, as follows:*

Code	Action to Take	Specific Action	Shell or IPE data elements acted upon	Optional Actionlist data elements used	Contents of optional Actionlist data elements
					Rows omitted for clarity
6	Un-Block~~Un-Hot~~ Shell		Shell blocked flag in DirBitMap	None	Clear shell blocked flag in DirBitMap, increment shell iteration number INS#
7	Un-Block~~Un-Hot~~ IPE		Data group blocked by SCT setting	None	Clear data group blocked SCT setting, increment IPE iteration number INP#.
					Rows omitted for clarity

Item 25 – TN0414

back

The 0C04 Data Correction message allows a Licensed Operator to amend a transaction record message created by a POST, where this is known to contain an error. This message would be sent by the Licensed Operator (for example a service provider whose POST created the original message in question) to another Licensed Operator (such as a Product Owner whose product was used in the Transaction the record of which is being changed).

Note that if the change was "internal" and did not need communicating to another Licensed Operator, then this message would not be used, and the Licensed Operator concerned would simply change their own database.

This change provides additional information on the use of this message.

Note that this change encompasses guidance already provided in Developer Guide DG0034.

*Amend **Part 6, Clause 5.4** as follows:*

5.4 Data Correction Record, Code 0C04.

Note that this record type is only used between HOPS, not for transmission to POSTs. It is used when a correction to a transaction data record is required. This message would be sent by a Licensed Operator (for example a service provider whose POST created the original message in question) to another Licensed Operator (such as a Product Owner whose product was used in the Transaction the record of which is being changed).

Table 97 - Data Correction Record, Code 0C04

Name	Format	Size	Comment
StandardData		21	Standard data returned with all transaction records
InitialRecordLength	HEX	2	Length of the InitialRecord structure in bytes (where the count excludes the comma between the InitialRecordLength and InitialRecord data elements, includes commas within the InitialRecord Structure, and excludes the comma between the InitialRecord and AmendedRecordLength data elements. The length shall be calculated of the message in transmission format.)
InitialRecord		Variable	A structure containing a copy or clone of the initial data record before correction, (comprising the whole ITSO transaction data frame including Sequence number, timestamp, data including message code and destinations, and the Seal) as originally transmitted.
AmendedRecordLength	HEX	2	Length of the AmendedRecord structure in bytes (where the count excludes the comma between the AmendedRecordLength and AmendedRecord data elements, and includes commas within the AmendedRecord Structure. The length shall be calculated of the message in transmission format.)
AmendedRecord		Variable	A structure containing the amended record after correction comprising the whole ITSO transaction data frame (including Sequence number, timestamp, data including message code and destinations, and with the original sealer ID (ISAM ID and ISAM sequence number) and Seal.

In this context the standard data shall be written as follows:
— Transaction date and time shall record the date and time of creating the correction message;

— IPE-ID shall be taken from the transaction record being amended;

— StaffID shall identify the member of staff responsible for creating the correction message.

The InitialRecord and AmendedRecord shall contain an entire ITSO message data frame. When transmitted the individual data elements within these data frames shall be separated by commas. These structures shall not be converted to transmission format twice.

The InitialRecord shall contain the complete original message Data Frame including:
— Header;
— Standard data;

- Data;
- Footer & original Seal.

It is sent so that the receiving HOPS can identify the original data.

The AmendedRecord shall contain the complete amended message Data Frame including:
- Original Header;
- Original or Amended Standard data;
- Original or Amended Data;
- Original Footer & original Seal.

For the AmendedRecord the same structure as a class 1 message shall be used, which may simplify the processing required in the receiving HOPS. The Seal will of course be invalid for this data set, and the outcome of the seal check should be ignored

back

Item 26 – TN0418

Clause 9.5, of Part 6 defines POST Information Notification messages. These are transmitted by POSTs when certain defined information changes, so that the HOPS becomes automatically aware of the change. For example, the message is sent when an ISAM is installed or replaced.

The clause contains two format versions of the message, 1 and 2. However the clause title indicates that it refers to version 1 only.

*Amend **Part 6, Clause 9.5**, title as follows:*

9.5 POST Information Notification, code 0803~~ - RecordFormatRevision = 1~~

back

Item 28 – TN0421

back

Part 5 contains the definitions of Extended Value Record Groups, which use the abbreviation VGXREF.

VGXREF1 and VGXREF 2 define extended Value Record Groups for Capping.

In both of these VGXREFs one of the accumulators has been assigned a Data Type of HEX when it should be VALI.

The following corrections apply this to the Part 6 messages which use these data elements.

*In **Clause 4.5.6.1, Table 3.14** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

Name	Source	Format	Size	Comment
Rows omitted for Clarity				
UncappedAccumulator1	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator2	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator3	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator4	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				

*In **Clause 4.5.6.2, Table 3.14A** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

Name	Source	Format	Size	Comment
Rows omitted for Clarity				
UncappedAccumulator1	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator2	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the

Name	Source	Format	Size	Comment
				message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator3	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator4	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				

*In **Clause 4.5.10, Table 3.18** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

Name	Source	Format	Size	Comment
Rows omitted for Clarity				
UncappedAccumulator1	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator2	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator3	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator4	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				

*In **Clause 4.5.11, Table 3.19** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

Name	Source	Format	Size	Comment
Rows omitted for Clarity				
UncappedAccumulator1	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator2	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the

Name	Source	Format	Size	Comment
				message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator3	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator4	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				

*In **Clause 4.5.13, Table 3.21** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

Name	Source	Format	Size	Comment
Rows omitted for Clarity				
UncappedAccumulator1	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator2	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator3	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator4	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				

*In **Clause 4.5.16, Table 3.24** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

Name	Source	Format	Size	Comment
Rows omitted for Clarity				
UncappedAccumulator1	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator2	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the

				message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator3	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator4	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				

*In **Clause 4.5.17, Table 3.25** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

Name	Source	Format	Size	Comment
Rows omitted for Clarity				
UncappedAccumulator1	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator2	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator3	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator4	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				

*In **Clause 4.5.19, Table 3.27** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

Name	Source	Format	Size	Comment
Rows omitted for Clarity				
UncappedAccumulator1	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator2	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				

UncappedAccumulator3	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator4	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				

*In **Clause 4.5.20, Table 3.28** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

Name	Source	Format	Size	Comment
Rows omitted for Clarity				
UncappedAccumulator1	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator2	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator3	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator4	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				

*In **Clause 4.5.21, Table 3.29** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

Name	Source	Format	Size	Comment
Rows omitted for Clarity				
UncappedAccumulator1	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator2	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				
UncappedAccumulator3	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.

Rows omitted for Clarity				
UncappedAccumulator4	IPE-VGX	~~HEX~~ VALI	2	This element shall be included in the message only if MessageBitMap/0 = 1.
Rows omitted for Clarity				

*In **Clause 8.5, Table 3.131** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

LD	**Information only**					**LD**	**LD**	**LD**
Element Number	**Target IPE Group**	**Target IPE ITSO Name**	**Target IPE Data Type**	**Included in target IPE?**	**Content generation rule**	**Rule Code**	**List Data Size**	**List Data**
					Rows Omitted for Clarity			
59	VX	UncappedAccumulator1	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			
66	VX	UncappedAccumulator2	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			
73	VX	UncappedAccumulator3	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			
80	VX	UncappedAccumulator4	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			

*In **Clause 8.5, Table 3.133** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

LD	**Information only**					**LD**	**LD**	**LD**
Element Number	**Target IPE Group**	**Target IPE ITSO Name**	**Target IPE Data Type**	**Included in target IPE?**	**Content generation rule**	**Rule Code**	**List Data Size**	**List Data**
					Rows Omitted for Clarity			
57	VX	UncappedAccumulator1	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			

LD	Information only					LD	LD	LD
Element Number	**Target IPE Group**	**Target IPE ITSO Name**	**Target IPE Data Type**	**Included in target IPE?**	**Content generation rule**	**Rule Code**	**List Data Size**	**List Data**
64	VX	UncappedAccumulator2	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			
71	VX	UncappedAccumulator3	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			
78	VX	UncappedAccumulator4	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			

*In **Clause 8.5, Table 3.134** amend the data type from HEX to VALI for all references of UncappedAccumulator1, 2, 3 and 4 as follows:*

LD	Information only					LD	LD	LD
Element Number	**Target IPE Group**	**Target IPE ITSO Name**	**Target IPE Data Type**	**Included in target IPE?**	**Content generation rule**	**Rule Code**	**List Data Size**	**List Data**
					Rows Omitted for Clarity			
61	VX	UncappedAccumulator1	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			
68	VX	UncappedAccumulator2	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			
75	VX	UncappedAccumulator3	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			
82	VX	UncappedAccumulator4	~~HEX~~ VALI	Always	set to zero (0)	4	0	-------
					Rows Omitted for Clarity			

back

Item 29 – TN0422

back

0209 messages are used by POSTs to record all "ITSO" Journeys.

The specification of the 0209 message includes a sub-clause which defines when the message should be used. In clause 4.4.27 this sub-clause contains a typographical error which makes the meaning unclear. In addition the sub-clause text is generally drafted in such a way that it is difficult to understand. This TN proposes reformatted text which resolves these issues, without changing the meaning of the text.

*Amend the following clauses in **Part 6**:*

4.4.27 Journey Record, code 0209.

4.5.27 Journey Record, code 0209 – RecordFormatRevision = 3.

4.6.27 Journey Record, code 0209 – RecordFormatRevision = 4.

By replacing the following text:

~~This record shall be used to record all Journeys made using an ITSO Customer Media, including those made when a Ticket IPE is used; to record Journeys where a Transient Ticket record is created (in addition to a 0210 record); to record Closed System entry and exit transactions; to record use of a voucher or open system toll IPE; and to record a free concessionary journey authorised solely by the ITSO ID/Entitlement IPEs; TYPs 14 and 16. This record may also be used to record other types of Transaction, at the discretion of the relevant Licensed Operator.~~

With this text:

This record shall be used to record all Journeys made using an ITSO Customer Media. For the avoidance of doubt this includes (but is not necessarily limited to):

- Journeys when a Ticket IPE is used;
- Journeys when a Transient Ticket record is created (in addition to a 0210 record);
    - Where more than one Transient Ticket is created in the course of a Journey it is only mandatory to create one 0209 message for that Journey;
- Closed System entry and exit transactions;
    - The 0209 message shall be sent for either the entry or the exit transaction so as to record the Journey, and optionally may be sent for both transactions.
- Usage of STR or CTA to purchase a ticket;
- Usage of a voucher or open system toll IPE; and
- Free concessionary Journeys authorised solely by the ITSO ID/Entitlement IPEs, TYPs 14 and 16.

This record may also be used to record other types of Transaction, at the discretion of the relevant Licensed Operator.

back

Item 37 – TN0437

The data messages used to transmit Hotlists and Actionlists from HOPS to POSTs are defined in part 6.

Originally, these lists could be transmitted using class 2 messages, if the lists were to be stored in the POST, or using class 3 messages, if the lists were to be stored in an ISAM. Part 3 of the specification has been amended (in a previous version) to prohibit the use of class 3 messages and ISAM storage. However, a sentence in part 6 had not been amended to reflect this.

Amend ***Part 6****,* ***Clause 5.3.3 Hotlist and Actionlist item records****, by modifying the initial paragraph as follows:*

This data set shall~~may~~ be transmitted as a class 2 message, using the message codes defined in table 78, when the data will be stored in and processed by a POST. ~~Alternatively, this data set may be transmitted as a class 3 message, in accordance with ITSO 1000-8, when the data is to be stored in and processed by an ISAM.~~

back

Part 7

Item 21 – TN0410

*There is a spelling mistake in **Annex A, Clause A.2**, The command set. Amend as follows:*

READ~~K~~PK **90 7E**		**Return the ISAM's public keys.**			
				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

back

Item 24 – TN0413

back

*Amend **Clause 6.7 – ISAM Groups**, by inserting the following immediately following the header:*

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

*Amend **Clause 7.3.1 bullet 2** as follows:*

Identify the destination of the Secure Data Frame as an ISAMID or Physical ISAM Group~~group of ISAMs~~;

*Amend **Clause 7.3.1.2** as follows:*

The concatenation of Physical ISAM G~~g~~roup 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.

*Amend **Clause 7.3.1.5** (note following the clause) as follows:*

Note: Where the ISAM is referenced as part of a Physical ISAM G~~g~~roup 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.

*Amend **Clause 7.3.2** (Paragraph 2) as follows:*

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 ~~to a group sharing a common password~~.

back

Item 40 – TN0440

back

*In **Table 2 (Clause 6.3.1)** add "I" in front of "Batch" in the row for IMAC, Poll, LBatch, VBatch_MAC. Also change "batch" to "Batch" where appropriate.*

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

*In **Clause 7.1.5**, fourth bullet, replace "batch" with "IBatch", and also change the 3 other occurrences in this clause in the same way, including the footnote. (Note that the section break is not required in the actual document but is here in order to get the correct footnote number to display.) Also correct typo in bullet Number 2.*

- Sourcing Transaction ~~batch~~ IBatch headers

****Text omitted****

As part of the same process the ISAM updates the header data that covers all transactions of the current ~~batch~~ IBatch[13].

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 ~~batch~~ IBatch header and associated Seal.

[13] A new ~~batch~~ IBatch is only created as a result of a POLL command

*In **Table 3, Row 7 (Clause 7.1.7)**, amend Batch to IBatch, and batches to IBatches.*

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 ~~Batch~~ IBatch Header cryptogram. The IMAC command shall only seal messages if the number of open ~~batches~~ IBatches is less than a limit held in the ACC stored within the ISAM.

*In **Clause 7.2.3** penultimate paragraph, amend batch to IBatch*

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

*In **Clause 7.2.4,** amend the 2 occurrences of batch to IBatch.*

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

*Amend the Heading of **Clause 7.2.5** by inserting "I" in front of Batch.*

7.2.5 IBatch Headers

*Amend **Clause 7.2.5** inserting "I" in front of Batch where relevant; and correct the spelling of "resettable":*

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-resettable grand total data[14] 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.

*Amend the Heading of **Clause 7.3.4.2** by inserting "I" in front of Batch.*

7.3.4.2 Verification of IBatch Headers

*Amend **Clause 7.3.4.2** inserting "I" in front of Batch where relevant:*

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.

In Clause A.2 (The command set) insert "I" in front of Batch or change "batch" to "IBatch" where relevant:

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

IMAC 90 5A	Store a transaction in the ISAM.				
			POST	HOPS	
Command	90 5A 00 00 00				
Response	<New ~~batch~~ 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 90 5E	Return a list of ~~batch~~ IBatch headers.			
		POST	HOPS	
Command	90 5E 00 00 00			
Response	<List of ~~batch~~ 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 90 74	Create and delete ~~batch~~ IBatch headers.				
			POST	HOPS	
Command	90 74 00 <P2 = number of delete parameters> <Lc = 12 + (P2*11)> <12xCreate ~~batch~~ 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

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

back

Item 41 – TN0441

back

Part 7 includes an [informative] Annex containing a summary of the ISAM Command set. There is an error in the command code for the External Authenticate command. The value of the command code [00] is correctly shown in the [normative] Part 8. This TN corrects this error. The opportunity is also taken to correct a typographical error in the command name.

*In **Annex A, Clause A.2,** amend the table for the External Authenticate command as shown following:*

EXTERNAL_ AUTHENTICATE ~~9~~00 82			**Mutually authenticates ITSO Shell and ISAM**		
				POST	**HOPS**
Command	~~9~~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

back

Part 8

Part 8 is available by request only, so the changes are in a separate document that can be requested through ITSO's support system Serena.

The document name is ITSO_COR_2_1_4_-9_20150407_Part_8_content.pdf

Item 24 – TN0413

Changes can be found detailed in the above mentioned document.

back

Item 30 – TN0427

Changes can be found detailed in the above mentioned document.

back

Item 32 – TN0432

Changes can be found detailed in the above mentioned document.

back

Item 38 – TN0438

Changes can be found detailed in the above mentioned document.

back

Item 39 – TN0439

Changes can be found detailed in the above mentioned document.

back

Item 40 – TN0440

back

Changes can be found detailed in the above mentioned document.

Item 43 – TN0443

Changes can be found detailed in the above mentioned document.

back

Item 44 – TN0444

Changes can be found detailed in the above mentioned document.

back

Item 48 – TN0449

Changes can be found detailed in the above mentioned document.

back

Part 9

Item 24 – TN0413

back

Amend the following paragraphs in ***Clause 11.2.4.2 Protocol*** *as follows:*

The Physical ISAM Group or Set parameter shall be used by the requesting POST (or depot system) to indicate to the HOPS the ISAMs, Physical ISAM Groups and /or POST Sets, using the ISAMID, ITSO group identifier (IIN + OID + ISG) or ITSO set identifier (IIN + OID + SetId), whose messages are being requested. The parameter name "ISAM" takes the form of the ITSO IIN + ISAMID.

A request for “ISAM” shall result in any messages addressed to that individual ISAM being sent from the server to the client. A request for “Group” shall result in any messages addressed to that ITSO Physical ISAM ~~physical group~~ Group being sent from the server to the client. A request for “Set” shall result in any messages addressed to that POST Set being sent from the server to the client. The above example request may result in a single message being returned for ISAM 6335970058004C, ISAM 6335970058004D, Physical ISAM Group 633597000B1234 or POST Set 633597000B1234.

Amend the following paragraph in ***Clause 11.2.5 Controlled environment*** *as follows:*

Table 11 defines the relationship between the environment and the type of processes. It also shows whether the process can be applied to Physical ISAM Groups or not.

back

Part 10

Item 30 – TN0427

*In **Clause 1.1 Scope of Part 10** remove the line relating to:*

~~London Oyster CMD6 clause 7;~~

***Delete** the whole of **Clause 7**; then add the following text (so that Clause numbering in the rest of the document remains unchanged):*

7. CMD6 - RFU

back

Item 42 – TN0442

For the detailed rationale for this item please see the note under Item 41 in the section on Part 1 above.

There are also 3 instances where EXP is defined as zero in Part 10. Two of these will be removed by technical notes in the next version of the specification, when FVC 5 and FVC 6 are removed. The remaining instance which affects FVC 4 Mifare Ultralite needs to be amended.

It should be noted that in this instance EXP is an assumed value which is not actually stored in the CM. When the POST wishes to validate a shell, it uses the limited data which is stored in the CM, plus assumed values for the other data elements needed to create the string sent to the ISAM. Table 42 in part 10 defines these assumed values. Changing the assumed values will have no material effect.

back

*Amend **Part 10, clause 5.4.1** as follows:*

Table 42 - Fixed platform parameter values

Data Element	Value	Comment
ShellLength	6	As defined in TS 1000-2, this defines (in units of BL bytes), the length of the re-constructed Shell.
ShellBitMap	msb-000000-lsb	Compact Shell
ShellFormatRevision	1	For this version of the Specification
IIN	633597	
OID	8189	Reserved OID used for Compact Shells
ISSN	0	
CHD	<computed>	As computed by the POST according to ITSO TS 1000-2
FVC	4	
KSC	0	For this version of the Specification
KVC	1	For this version of the Specification
EXP	0x3FFF~~0~~	ITSO Shell does not expire for the foreseeable future
B	32	1-off 32-byte Sector for IPE storage
S	1	
E	1	1 Directory Entry supported
SCTL	0	No SCT used
SECRC	<computed>	As computed by the POST according to ITSO TS 1000-2

back

~ End of Section 1 ~

SECTION 2

The following changes were agreed by the TC at its meeting in February 2015. The changes in this section are arranged by subject matter and then Part number. There is a hyperlink to each change in the Table of Items below.

Table of Items

Part 6 – 0300 RFR3 Title Correction

TN0270 to Part 6 of v2.1.2 ITSO Specification introduced a new RFR (3) of the 0300 message RFR3, copying Clause 4.4.29 and Table 61 to Clause 4.5.29 and Table 3.61. At the time of writing, this message was entitled "Transaction cancellation".

Subsequently, TN0286 was written to redefine "Transaction cancellation" as "TransactionReversal", but this did not take into account the new RFR introduced in TN0270 and the 0300 RFR3 titles have remained as referring to "Transaction cancellation".

This typographical change corrects this accordingly.

Part 6

*Amend Clause **4.5.29** and **Table 3.61** as follows:*

4.5.29 TransactionReversal ~~cancellation~~, code 0300 – RecordFormatRevision = 3

Table 3.61 - TransactionReversal ~~cancellation~~, code 0300 – RecordFormatRevision = 3

Back to Top of Section

Part 6 – Table 7 - 0205 Message Name

In TN0382 the name of the 0205 message was changed to make it more clear what the message does. The headings were all changed but the Table 7 entry was missed. This change makes it consistent.

In Table 7 amend the row for the 0205 message as follows:

	Loyalty ~~amendment (~~transaction reversal~~)~~,	0205	2	POST IPE

Back to Top of Section

Part 1 – KID Definition Correction

The definition of KID in Part 1 of the Specification includes a reference to the KSD. This is a historical reference that has been left in the Specification since v2.1 but has no current relevance. It is therefore removed by this item.

Part 1

*Amend **Table 2** as follows:*

Key Identity Definition	KID	A single byte coded to indicate the identity of the key used ~~as defined in the KSD~~.

Back to Top of Section

Parts 8 & 10 – Remove CMD5

The requirement for POSTs to support CMD5 has already been removed from the Test requirement following a Board resolution.

This is formalised by removing the relevant Clauses from the Specification

Part 8

Part 8 is available by request only, so the changes are in a separate document that can be requested through ITSO's support system Serena.

The document name is ITSO_COR_2_1_4_-8_20150402_Part_8_content.pdf

Part 10

*In **Clause 1.1 Scope of Part 10** remove the line relating to CMD5 as follows:*

~~– Innovision Jewel 0301/70 CMD5 clause 6;~~

*Delete the **whole** of Clause 6; then add the following text (so that Clause numbering in the rest of the document remains unchanged):*

6. CMD5 - RFU

Back to Top of Section

Back to Top of Corrigendum

Parts 0, 1, 4, 6 & 8 – ISMS Definition Correction

The acronym "ISMS" is expanded to two different definitions throughout the Specification – ITSO Security Management Service and ITSO Security Management System - the correct definition is ITSO Security Management Service.

This change corrects the Specification to ensure that all expansions are consistent and correct.

Part 0

*Amend **Clause 8 Communications** as follows:*

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

Part 1

*Amend **Clause 1.6 Scope of Part 6** as follows:*

ITSO TS 1000-6 defines the ITSO message data elements and structures except for messages between the ITSO Security Management ~~System~~ Service (ISMS) and ISAMs / HSAMs, which are defined in ITSO TS 1000-8.

Part 4

*Amend **Clause 4 HSAM** as follows:*

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

Part 6

*Amend **Clause 1.1 Scope of Part 6** as follows:*

This Part of ITSO TS 1000 defines the ITSO message data elements and structures, excepting that messages between the ITSO Security Management ~~System~~ Service (ISMS) and ISAMs / HSAMs are not detailed in this document[1]

Part 8

Part 8 is available by request only, so the changes are in a separate document that can be requested through ITSO's support system Serena.

The document name is ITSO_COR_2_1_4_-8_20150402_Part_8_content.pdf

Parts 3 & 7 – Remove v1 ISAM

ITSO support for v1 ISAMs was withdrawn with effect from 1st April 2014 (see https://www.itso.org.uk/members-home/member-news/#phasing-out-version-1-isams).

This change removes the references to the v1 electrical characteristics from the Specification.

Part 3

*Delete the whole of **Clause 4.3.2 5-volt device**.*

Part 7

*Amend **Clause 6.2 Electrical characteristics overview** as follows:*

~~Note: A 5V version of the ISAM having a restricted voltage tolerance can be used as an alternative by special arrangement with ITSO.~~

back to Top of Section

Back to Top of Corrigendum

~ End of Section 2 ~

SECTION 3

All Parts - Copyright Notice

The following new copyright notice replaces the copyright notice on the Document Reference page of each Part of the Specification:

Although this information was commissioned by the Department for Transport (DfT), the specifications are those of the authors and do not necessarily represent the views of the DfT. The information or guidance in this document (including third party information, products and services) is provided by DfT on an 'as is' basis, without any representation or endorsement made and without warranty of any kind whether express or implied.

OGL

© Queen's Printer and Controller of Her Majesty's Stationery Office, 2015, except where otherwise stated

Copyright in the typographical arrangement rests with the Crown.

You may re-use this information (not including logos or third-party material) free of charge in any format or medium, under the terms of the Open Government Licence v3.0. To view this licence visit http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or e-mail: psi@nationalarchives.gsi.gov.uk.

Part 0 – Typographical Errors

In Clause 7.2.1.3 – 3rd line point amend as follows:

— ~~and~~add new or modify existing SSS functions;

In Clause 7.1.5 – amend the text as follows:

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

Part 1 – Scope of Part 11

Copy "Scope of Part 11" from Part 11 and add as Part 1 Clause 1.11

This part of ITSO TS 1000 defines the requirements on Remote Point of Service Terminals (POSTs) in order that such terminals are able to support the Interoperable Smart Customer Media environment defined by ITSO. These Remote POST requirements are grouped as follows.

- Remote POST Overview

- Remote POST Interfaces

- Remote POST Functional Requirements

Only requirements that are pertinent to Interoperable Smart Customer Media usage and interfacing to other parts of the ITSO Environment are defined herein. These requirements shall be applied as an Interoperability layer over the basic specification of a web or LAN based ticketing solution. The overall specification of such a solution is outside the scope of this document.

For the avoidance of doubt, the fact that a Remote POST may be certified as ITSO compliant does not mean that it is fit for purpose in any area other than its support for Interoperable Smart Customer Media usage. The design of any Remote POST shall mitigate all appropriate risks identified within the risk assessments for the environment within which it operates.

The opportunity is taken to amend the capitalisation of the headings for the other Parts' scopes so they are consistent.

Back to Top of Corrigendum

~ End of Section 3 ~

~ End of Corrigendum ~