ITSO

DOCUMENT DELIVERY NOTE

Issuing Authority:	**Owner:**	**Project Editor:**
ITSO	Technology at ITSO	ITSO Head of Technology
Document number	**Part Number:**	**Sub-Part Number**
ITSO TS 1000	10	
Issue number (stage):	**Month:**	**Year**
2.1.4	February	2010
Title:		
ITSO TS1000-10 *Interoperable public transport ticketing using contactless smart customer media – Part 10: Customer Media Definitions*		
Replaces Documents:		
ITSO TS1000-10 2008-04 issue number 2.1.3		

Revision history of current edition

Date	ITSO Ref.	Editor ID	Nature of Change to this Document (or Part)
Feb 2002	DCI 100 / create 2.1	CJS / SLB	Delete body (retain Annex A only)
April 2002		CJS / SLB	Add clause 9 moved from part 2. Filed as WD.
Feb 2003		JW	New document created
May 2003		JW / SLB	Amended after editorial review. Issued as CD.
July 2003		SLB	Pictures repaired. Issued as 2nd CD.
Sept 2003	ISAD6, ISAD7	JW	Incorporate changes agreed by ISAD6 and ISAD7 Incorporate changes suggested in DOC
Oct 2003	ISAD1, ISAD5	JW / SLB	Incorporate changes agreed by ISAD1 and ISAD5 Incorporate changes suggested in DOC Format and issue as 4th CD.
Nov 2003		JW / SLB	Incorporate changes for small rail IPE Incorporate revised Directory layout to improve speed Incorporate changes suggested in DOC Added placeholders for DESFire and Calypso
Nov 2003		SLB	Editorial changes only. Issue 1st consultation draft.
Jan 2004		JC	Implement DRC changes
Feb 2004		JW	Check/approve DRC changes
Feb 2004		SLB	Clean up and format as final draft (FD)
Mar 2004		SLB	Implement final changes and prepare for issue.
Oct 2006		MPJE	Updated to include ISADs following approval by DfT
Jun 2007		MPJE	Updated to include ISADs following approval by DfT
Feb 2008		CJS	Updated to include ISADs following approval by DfT
Apr 2008		MPJE	Final editing prior to publication
Dec 2009		CJS	Updated to include ISADs TN0294and 0342 following approval by DfT
Feb 2010		MPJE	Final Edit prior to publication
Apr 2015		MPJE	Updated to incorporate Corrigendum 9 to Version 2.1.4

Document Reference: ITSO TS 1000-10

Date: 2010-02-22

Version: 2.1.4

Ownership: ITSO

Secretariat: Technology at ITSO

Project Editor: Mike Eastham

ITSO Technical Specification 1000-10 – Interoperable public transport ticketing using contactless smart customer media – Part 10: Customer media definitions

ISBN: 978-0-9548042-4-4

COR 9

Foreword

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

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

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

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

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

Contents

1. Scope

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

1.1 Scope of Part 10

This Part of ITSO TS 1000 defines the Customer Media Definitions (CMDs). The CMD describes the mapping of the logical Data Elements onto a (defined) physical CM platform.

This document defines CMDs for the following platforms:

— Mifare® standard 1K	CMD1	clause 2;
— Generic micro-processor	CMD2	clause 3;
— Mifare® standard 4K	CMD3	clause 4;
— Mifare® ultra light	CMD4	clause 5;
— Mifare® DESFire	CMD7	clause 8;
— Calypso	CMD8	clause 9.

1.2 Physical form factor

All CMDs defined herein conform to ISO/IEC 14443-1.

2. Mifare® standard 1K

2.1 Scope

This clause defines the CMD for platforms on which the ITSO Application is the only or parent application and that use:

— The Philips Mifare® Standard MF1 S50 IC.

— Second-sourced ICs that are equivalent to the Philips MF1 S50 IC.

— A micro-processor which emulates the MF1 S50 IC.

2.1.1 Terminology

Throughout this clause reference will be made to terms defined within the Philips Mifare® Standard Card IC MF1 IC S50 Functional Specification (May 2001). These terms include, but are not limited to: Sector; Block; key; access condition flag.

2.2 Platform capability

2.2.1 General

This platform is capable of supporting a full set of Data Groups, as defined below:

— ITSO Shell Environment	With all optional elements present.
— Directory	Two instances (Anti-tear support); 5 Directory Entries supported.
— IPE	Up to 5 IPE instances may be present.
— Value Record	May be associated with IPEs subject to overall memory limits.
— Cyclic Log	Support for Basic and Normal mode logging.

2.2.2 Memory architecture

The memory architecture of this platform is summarised below:

— 1024 bytes of EEPROM, divided into 16 Sectors of 64 bytes each

  — 16 bytes are reserved for manufacturer data

  — 256 bytes are reserved for keys and access control settings

  — 752 bytes are available for the general storage of user data

— Storage capacity of 752 bytes is available for the ITSO Application.

  — 128 bytes are used for the ITSO Shell Environment and Directory Data Groups

  — 624 bytes are available for IPE instance, Value Record and Cyclic Log storage.

2.2.3 Security provisions

The platform provides the following security-related features:

— A unique 4-byte manufacturer’s serial number (MID).

— A pair of 6-byte keys controlling access to each Sector of memory.

— Within each Sector, access control flags controlling the allowed operations on each 16-byte Block.

— Mutual 3-pass authentication between media and reader (to ISO/IEC DIS9798-2).

— CRYPTO1 stream-cipher for the air interface (proprietary to Philips).

2.2.4 ISO/IEC 14443 compliance

All platforms covered by this CMD shall comply with the following parts of ISO/IEC 14443:

— part 2: RF power & signal interface Compliance with ISO/IEC 14443 Type A requirements;

— part 3: Initialisation & anticollision Compliance with ISO/IEC 14443 Type A requirements.

2.3 Format Version Code

Platforms that conform to this CMD shall use the Format Version Code (FVC) of 01.

2.4 ITSO Shell Environment Data Group

The ITSO Shell Environment Data Group shall be located in Sector 0, Blocks 1 and 2. The elements and layout of this data structure are fully defined in ITSO TS 1000-2.

2.4.1 Platform parameters with fixed values

The following platform parameter Data Elements within the ITSO Shell Environment Data Group shall have the fixed values specified herein for all implementations of this CMD.

Table 1 - Fixed platform parameter values

Data Element	Value	Comment
ShellLength	6 8	If the optional MCRN[1] is not present If the optional MCRN is present
ShellBitMap	msb-000001-lsb msb-000011-lsb	If the optional MCRN is not present If the optional MCRN is present
ShellFormatRevision	1	For this version of the Specification
FVC	1	See section 2.3
KSC	1	For this version of the Specification
B	48 (30 hex)	Size of memory Sector.
S	16 (10 hex)	This gives a Ψ of 4
E	5	Number of Directory Entries
SCTL	7	Length of SCT

2.4.2 Platform parameters with default values which may be overridden

This CMD does not support the overriding of platform parameter values.

[1] MCRN = Multi-application Card Reference Number.

2.4.3 ITSO Shell Environment detailed layout

Table 2 details the location of the Data Elements in Block 1. Table 3 details the location of the Data Elements in Block 2. Shading indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Byte and bit numbers are as defined in the S50 Functional Specification.

Table 2 - Sector 0, Block 1 data content

Data Element Label	# of bits	Start location	End location
ShellLength	6	Byte 0, bit 7	Byte 0, bit 2
ShellBitMap	6	Byte 0, bit 1	Byte 1, bit 4
ShellFormatRevision	4	Byte 1, bit 3	Byte 1, bit 0
IIN	24	Byte 2, bit 7	Byte 4, bit 0
OID	16	Byte 5, bit 7	Byte 6, bit 0
ISSN	28	Byte 7, bit 7	Byte 10, bit 4
CHD	4	Byte 10, bit 3	Byte 10, bit 0
FVC	8	Byte 11, bit 7	Byte 11, bit 0
KSC	8	Byte 12, bit 7	Byte 12, bit 0
KVC	8	Byte 13, bit 7	Byte 13, bit 0
RFU	2	Byte 14, bit 7	Byte 14, bit 6
EXP	14	Byte 14, bit 5	Byte 15, bit 0

Table 3 - Sector 0, Block 2 data content - No MCRN present

Data Element Label	# of bits	Start location	End location
B	8	Byte 0, bit 7	Byte 0, bit 0
S	8	Byte 1, bit 7	Byte 1, bit 0
E	8	Byte 2, bit 7	Byte 2, bit 0
SCTL	8	Byte 3, bit 7	Byte 3, bit 0
PAD	16	Byte 4, bit 7	Byte 5, bit 0
SECRC	16	Byte 6, bit 7	Byte 7, bit 0

Table 3a - Sector 0, Block 2 data content - MCRN present

Data Element Label	# of bits	Start location	End location
B	8	Byte 0, bit 7	Byte 0, bit 0
S	8	Byte 1, bit 7	Byte 1, bit 0
E	8	Byte 2, bit 7	Byte 2, bit 0
SCTL	8	Byte 3, bit 7	Byte 3, bit 0
MCRN	80	Byte 4, bit 7	Byte 13, bit 0
SECRC	16	Byte 14, bit 7	Byte 15, bit 0

2.5 Directory Data Group

The Directory Data Group shall be located in Sector 14 (copy A) and Sector 15 (copy B). Table 4 details the location of the Data Elements for each copy. Shading indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Table 4 - Directory Data Group

Data Element Label	# of bits	Start location	End location
DIRLength	6	Block 0, byte 0, bit 7	Block 0, byte 0, bit 2
DIRBitMap	6	Block 0, byte 0, bit 1	Block 0, byte 1, bit 4
DIRFormatRevision	4	Block 0, byte 1, bit 3	Block 0, byte 1, bit 0
E1	40	Block 0, byte 2, bit 7	Block 0, byte 6, bit 0
E2	40	Block 0, byte 7, bit 7	Block 0, byte 11, bit 0
E3	40	Block 0, byte 12, bit 7	Block 1, byte 0, bit 0
E4	40	Block 1, byte 1, bit 7	Block 1, byte 5, bit 0
E5	40	Block 1, byte 6, bit 7	Block 1, byte 10, bit 0
SCT1	4[2]	Block 1, byte 11, bit 7	Block 1, byte 11, bit 4
SCT2	4	Block 1, byte 11, bit 3	Block 1, byte 11, bit 0
SCT3	4	Block 1, byte 12, bit 7	Block 1, byte 12, bit 4
SCT4	4	Block 1, byte 12, bit 3	Block 1, byte 12, bit 0
SCT5	4	Block 1, byte 13, bit 7	Block 1, byte 13, bit 4
SCT6	4	Block 1, byte 13, bit 3	Block 1, byte 13, bit 0
SCT7	4	Block 1, byte 14, bit 7	Block 1, byte 14, bit 4
SCT8	4	Block 1, byte 14, bit 3	Block 1, byte 14, bit 0
SCT9	4	Block 1, byte 15, bit 7	Block 1, byte 15, bit 4
SCT10	4	Block 1, byte 15, bit 3	Block 1, byte 15, bit 0
SCT11	4	Block 2, byte 0, bit 7	Block 2, byte 0, bit 4
SCT12	4	Block 2, byte 0, bit 3	Block 2, byte 0, bit 0
SCT13	4	Block 2, byte 1, bit 7	Block 2, byte 1, bit 4
PAD	4	Block 2, byte 1, bit 3	Block 2, byte 1, bit 0
DIRS#	8	Block 2, byte 2, bit 7	Block 2, byte 2, bit 0
KID	4	Block 2, byte 3, bit 7	Block 2, byte 3, bit 4
INS#	4	Block 2, byte 3, bit 3	Block 2, byte 3, bit 0
ISAMID	32	Block 2, byte 4, bit 7	Block 2, byte 7, bit 0
Seal	64	Block 2, byte 8, bit 7	Block 2, byte 15, bit 0

2.5.1 DIRLength

This is RFU and shall contain a value of 0.

2.5.2 DIRFormatRevision

This shall contain a value of 1 (1 hex).

---

[2] The number of bits for the SCTx fields is equal to Ψ

2.5.3 Sector Chain Table (SCT) usage

The relationship between the SCT entries and the physical storage on the media is done on a Sector-by-Sector basis. Each SCT Label corresponds to a Mifare® Sector on the media. As noted before, each Sector contains 48 bytes of user-data storage.

Each SCT entry shall contain a number in the range 0 to 15 (decimal). The following values shall have special significance as defined in ITSO TS 1000-2.

Note: As stated in section 2.4.1, S is 16 for this CMD.

Table 5 - Special SCT values

SCT entry value (decimal)	Significance
0	Corresponding Sector (see Table 6) is un-allocated and may be used to store product data.
'Self'[3]	Terminating Sector for product in question. Product is Virgin
14	Terminating Sector for product in question. Product is Blocked
15	Terminating Sector for product in question. Product is not Blocked

Table 6 defines the mapping between SCT Label and media Sectors. Sector numbers are as defined in the S50 Functional Specification.

Table 6 - SCT Label vs. media Sector

SCT Label	Media Sector
SCT1	Sector 1
SCT2	Sector 2
SCT3	Sector 3
SCT4	Sector 4
SCT5	Sector 5
SCT6	Sector 6
SCT7	Sector 7
SCT8	Sector 8
SCT9	Sector 9
SCT10	Sector 10
SCT11	Sector 11
SCT12	Sector 12
SCT13	Sector 13

Note that the 13 Sectors listed above shall be used to store Data Elements associated with the following Data Groups:

— IPE;

[3] Where 'Self' means that the value in the entry corresponds to the entry's own number / Label. For example if SCT11 contains the value 11 (decimal) then this is a 'self' reference.

— Value Record;

— Cyclic Log.

As defined in ITSO TS 1000-2, SCT1 to SCT5 (shown shaded) have special significance, and are reserved as Starting Sectors.

Any Private Applications stored on the media shall also be located exclusively in the above 13 Sectors.

2.5.4 PTYP usage for Private Applications

Where the data associated with a Directory Entry is a Private Application, the PTYP field within the Directory Entry may be proprietary to the (private) application.

2.6 Key usage

All Sectors shall use keys derived from the same master key pair.[4]

Read-only access to all Sectors shall be allowed by use of the A key. Key diversification shall not be employed for such access.

Note: This means that all Sectors of all platforms that conform to this CMD (FVC = 01) can be read by use of a single, non-diversified key.

Read-write access to all Sectors shall be allowed by use of the B key. Key diversification shall be employed for such access. The diversification mechanisms are defined in ITSO TS 1000-8.

For key diversification purposes, the following logical Sector numbers shall be used:

— ITSO Shell Logical Sector 0;

— Directory (copy A) Logical Sector S-2; (i.e. 14)

— Directory (copy B) Logical Sector S-1; (i.e. 15)

Where the access key returned by the ISAM is longer than the 6 byte key required by this platform the key to be used shall consist of the last 6 bytes only. Thus for a key of value 0x123456789ABCDEF0 returned by the ISAM 0x56789ABCDEF0 shall be used as the access key for the CM.

2.7 Key strategy

This CMD shall use the Key Strategy Code (KSC) value as defined in clause 2.4.1. The ISAM shall use this to determine the appropriate cryptographic processes to be applied to such media platforms.

2.8 Access conditions

2.8.1 Sector 0, Block 0

This Block is always read-only and the access condition flag settings are ignored.

2.8.2 User-data Blocks

The access condition flags for all 47 user-data Blocks on the media shall be set as follows, unless said Block is within a Sector that contains a Private Application: [5]

---

[4] Sectors containing ‘Private Applications’ which are marked as such in the ITSO Directory may use alternate key arrangements.

C1 = 1; C2 = 0; C3 = 0.

This setting has the effect of:

— Allowing read access with key A or key B.

— Allowing write access with key B.

— Not allowing the use of the increment command.

— Not allowing the use of the decrement command.

— Not allowing the use of the transfer command.

— Not allowing the use of the restore command.

2.8.3 Sector trailer Blocks

The access condition flags for all 16 Sector-trailer Blocks (i.e. Block 3) on the media shall be set as follows, unless said Block is within a Sector that contains a Private Application: [6]

C1 = 0; C2 = 1; C3 = 1.

This setting has the effect of:

— Allowing key A to be written to if the Sector was opened with key B.

— Allowing key B to be written to if the Sector was opened with key B.

— Both the A and B keys on the Sector cannot be read.

— Allowing the access condition flags to be read if the Sector was opened with key A or key B.

— Allowing the access condition flags to be written to if the Sector was opened with key B.

2.9 Anti-tear

Software Anti-tear protection mechanisms as defined in Annex A shall be employed on the following Data Groups:

— Directory;

— Value Record;

— Cyclic Log.

2.10 Manufacturer's ID

All media conforming to this CMD contain a unique 4-byte manufacturer's serial number in bytes 0 to 3 of Block 0 of Sector 0. This shall be used wherever an ITSO MID is required (e.g. for security algorithms).

The usage of this serial number when generating the 8-byte ITSO MID shall be as follows:

---

[5] Blocks within sectors containing 'Private Applications' which are marked as such in the ITSO Directory may use alternate access condition arrangements

[6] Trailer Blocks within sectors containing 'Private Applications' which are marked as such in the ITSO Directory may use alternate access condition arrangements

Table 7 - ITSO MID computation

ITSO MID byte	Contents
Byte 0 (MSB)	00 (hex)
Byte 1	00 (hex)
Byte 2	00 (hex)
Byte 3	00 (hex)
Byte 4	Block 0, byte 3
Byte 5	Block 0, byte 2
Byte 6	Block 0, byte 1
Byte 7 (LSB)	Block 0, byte 0

2.10.1 Verification of the serial number

Point of Service Terminals (POSTs) shall verify that the serial number data in bytes 0 to 3 of Block 0 of Sector 0 corresponds to the UID that the media provided during the anti-collision loop process. This check shall always be carried out unless it can be proven that the POST does not have access to said UID data.

2.11 Detection of the ITSO Shell

The ITSO Shell detection sequence for this CMD shall be as follows:

— If a Mifare® standard 1k platform is detected[7], then the POST shall attempt to read Sector 0 with the non-diversified ITSO FVC = 01 A key[8].

— If Sector 0 can be opened for reading, then its contents shall be read and parsed as per section 2.4.

— A CRC shall be computed for the data read and checked against the SECRC field of the parsed data.

— If this check passes, then the POST shall assume that the platform carries a valid ITSO Shell.

— The POST shall read and confirm that all the Data Elements listed in Table 1 have the specified values. If this check passes then an ITSO Shell of FVC = 01 shall be deemed to be present.

2.12 Benchmark transaction

2.12.1 IPE with Transient Ticket Record creation

The benchmark transaction for this CMD shall comprise:

— Detection of a platform carrying a valid ITSO Shell with FVC = 01.

— Verification of the Directory, where there is no corruption on either Anti-tear copy.

— Verification of an IPE Data Group where there is only a single candidate product and the IPE Data Group resides in a single Sector.

---

[7] Refer to the Philips application note ‘Type Identification Procedure’ (m018411) for details of how to differentiate between the various Mifare® variants. Note that Philips makes proprietary use of certain bits in the SAK byte.

[8] Note that this key cannot be requested from the ISAM in the normal manner using the IIN, OID, FVC, KSC selection method, as these parameters are unknown at this stage. In effect the POST must hold this ‘global’ read key as a constant in its own memory.

— Creation of a sealed 48-byte Transient Ticket Record.

— Read after write verification of the updated Directory.

The target execution time for the above, subsequent to detection of the platform, shall be 300ms or less.

Note: The target execution time includes all necessary POST application functions. (i.e. normal operation, Hotlist processing etc…)

2.12.1 IPE with Value Record Data Group modification

The benchmark transaction for this CMD shall comprise:

— Detection of a platform carrying a valid ITSO Shell with FVC = 01.

— Verification of the Directory, where there is no corruption on either Anti-tear copy.

— Verification of an IPE Data Group where there is only a single candidate product and the IPE Data Group resides in a single Sector.

— Verification and modification of an associated Value Record Data Group where there is no corruption on either Anti-tear copy, and the Value Record Data Group resides in a single Sector.

— Modification of the Directory to reflect the changes made to data group and product above.

— Read after write verification of the updated Directory.

The target execution time for the above, subsequent to detection of the platform, shall be 300ms or less.

Note: The target execution time includes all necessary POST application functions. (i.e. normal

operation, Hotlist processing etc…)

2.13 List search method

This CMD supports a full ITSO Shell as defined in ITSO TS 1000-2. When a POST carries out a Hotlist or Actionlist search against a platform where FVC = 01, then it shall use ITSO Shell Referencing as defined in ITSO TS 1000-3.

3. Generic micro-processor

3.1 Scope

This clause defines the CMD for microprocessor-based platforms supporting a minimal and generic set of ISO/IEC 7816-4:1995 commands.

The design of this CMD allows for the hosting of the ITSO Application on a single or multi-application microprocessor-based CM platform that:

— Supports the standard ISO/IEC 7816-4:1995 commands and filing system functions required by this CMD;

— Supports application selection via AID; and

— Has sufficient data storage capacity.

Use of this CMD allows an ITSO Compliant Shell (Application) to be provided with minimum development effort on such platforms.

3.1.1 Terminology

Throughout this clause reference will be made to terms defined within ISO/IEC 7816-4:1995.

3.2 Platform capability

3.2.1 General

This platform is capable of supporting a full set of ITSO Data Groups as defined below:

— ITSO Shell Environment With all optional elements present.

— Directory Two instances (Anti-tear support).

— IPE

— Value Record May be associated with IPEs subject to overall memory limits.

— Cyclic Log Support for Basic and Normal mode logging.

This Specification defines a set of default parameters for this CMD that control the size of storage and the number of products stored. ITSO Shell Owners may use alternate parameter values to those specified herein. POSTs shall be able to process media with alternate parameter values. See section 3.7.4.4.2 for further details.

The default parameters define a memory structure that will support:

— 8 Directory Entries;

— 29 Sectors for IPE instance, Value Record and Cyclic Log storage;

The standard ISO/IEC 7816-4:1995 command set used by this platform supports:

— Selection of the ITSO Directory and files.

— Reading of data from these files (without the need for media/POST authentication).

— Establishing of mutual authentication between the media and the POST.

— Provision of media access control key(s).

— Update of the ITSO files (after required security exchanges).

3.2.2 Memory architecture

The memory architecture of this platform is summarised below:

— Based around a filing system complying with ISO/IEC 7816-4:1995.

— The ITSO Application consists of a Dedicated File (DF) containing an Elementary File (EF) and a number of DFs. These DFs hold the Storage Sector EFs for the ITSO Shell, the IPEs and the Directory copies. Optional DFs may also be present to store any Private Applications.

— Each Storage Sector DF contains an EF that holds a single 48-byte[9] 'Sector'. Each Storage Sector EF will have an associated set of access keys (sometimes termed the Card Holder Verification or PIN keyfile).

— Each Directory DF contains an EF that holds a copy of the Directory. Each Directory Sector EF will have an associated set of access keys (sometimes termed the Card Holder Verification or PIN keyfile).

— Default storage capacity of 1392 bytes is available for IPE instances, Value Records and the Cyclic Log. This is roughly twice that available on media with FVC = 01.

3.2.3 Security provisions

The platform shall provide the following security-related features:

— Support for mutual authentication between POST and media via DES or triple-DES.

— Support for use of access keys (PIN / cardholder verification).

The platform may optionally provide the following security-related features:

— Support for the use of secure messaging between POST and media using a triple-DES session key derived during mutual authentication.

3.2.3.1 Security of data records

As outlined above, this CMD uses EFs with a 48-byte[10] transparent binary format for most data storage. The platform shall guarantee that any changes made to any EF shall not, under any circumstances, modify in any way, data stored in any other files on the media.

The above requirement is mandatory and shall apply under all operating conditions including, but not limited to, where the media is prematurely removed from the field of the reader.

Failure to atomically update an individual EF is acceptable so long as said failure is detectable and further writes are not attempted.

3.2.4 Application Family Identifier usage

ISO/IEC 14443-3 provides for support of an Application Family Identifier (AFI) pre-selection mechanism.

ITSO does not mandate the use of AFI coding, although where the platform supports such coding and only the ITSO Application is present, then use of the Transport Family code (10 hex) is recommended.

POSTs shall not assume that media uses AFI coding, and shall default to using the Select All code of 00 (hex).

3.2.5 ISO/IEC 14443 compliance

All platforms covered by this CMD shall comply with the following parts of ISO/IEC 14443:

---

[9] Default size

[10] Default size

— Part 2: RF power & signal interface Compliance with ISO/IEC 14443 Type A or Type B requirements;

— Part 3: Initialisation & anticollision Compliance with ISO/IEC 14443 Type A or Type B requirements;

— Part 4: Transmission protocol Compliance with ISO/IEC 14443 Type A or Type B requirements.

Note: If a media reports (to the POST) that it supports ISO/IEC 14443-4, then ISO/IEC 14443 requires that this protocol shall be selected. The implications of this are that if any applications (including an ITSO one) reside either in a 'classic Mifare®' area on the media, or are accessed by use of other proprietary protocols, then these will not be able to be accessed. This is a known limitation of ISO/IEC 14443.

3.3 Format Version Code

Platforms that conform to this CMD shall use the Format Version Code (FVC) of 02.

3.4 Command set

The platform shall support the following ISO/IEC 7816-4:1995 commands[11]. The instruction (INS) codes are shown in hex.

— SELECT FILE (INS code = A4);

— READ BINARY (INS code = B0);

— UPDATE BINARY (INS code = D6);

— GET CHALLENGE (INS code = 84);

— EXTERNAL AUTHENTICATE (INS code = 82);

— INTERNAL AUTHENTICATE (INS code = 88);

— VERIFY (INS code = 20).

The detailed usage of these commands will be defined in subsequent sections of this document.

3.5 Authentication algorithms

Platforms shall, as a minimum, support the Data Encryption Standard (DES) algorithm for use by the INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE commands.

The manner in which the platform notifies the POST of the algorithm(s) supported is defined in section 3.7.2.3.1.

3.5.1 Authentication keys

The platform shall be able to store a pair of secret keys, specific to the ITSO Application, for use with the following commands:

— EXTERNAL AUTHENTICATE;

— INTERNAL AUTHENTICATE.

Where DES is used, these keys shall be 8 bytes in length.

Where triple DES is used these keys shall be 16 bytes in length.

[11] These commands are the ones required during normal usage of the platform. They do not include the commands required for the creation of the ITSO Application on the platform.

These internal (secret) keys shall be diversified by use of the ITSO Shell Reference Number (ISRN). The diversification mechanisms are defined in ITSO TS 1000-8.

Note: It is strongly recommended that the operating system used within the platform provides support for a session count for failed mutual authentication. Where such a counter is available, then the COS should apply an ‘exponential hold-off’, where the delay applied relates to the failed authentication attempt count.

3.6 Secure messaging

Secure messaging is supported as an option on this CMD.

The use of secure messaging adds protection from “replay attacks”, where the POST has additional confidence that the data presented was read from the media in the current session. The use of secure messaging for updates to the media provides protection from updating the media with a previous copy of data.

Message transfer between the media and the POST shall be secured by use of a MAC that is generated using a triple-DES session key derived during mutual authentication.

Where the media indicates that secure messaging is supported (see section 3.7.2.3.1), it is mandatory that POSTs shall support this feature for all media updates. However the use of this feature, when applied to Directory and Cyclic Log updates only, may be optional as determined by the application.

3.7 File system structure

Figure 1 illustrates the structure of the default ITSO file system. All FIDs and SIDs are in hex.

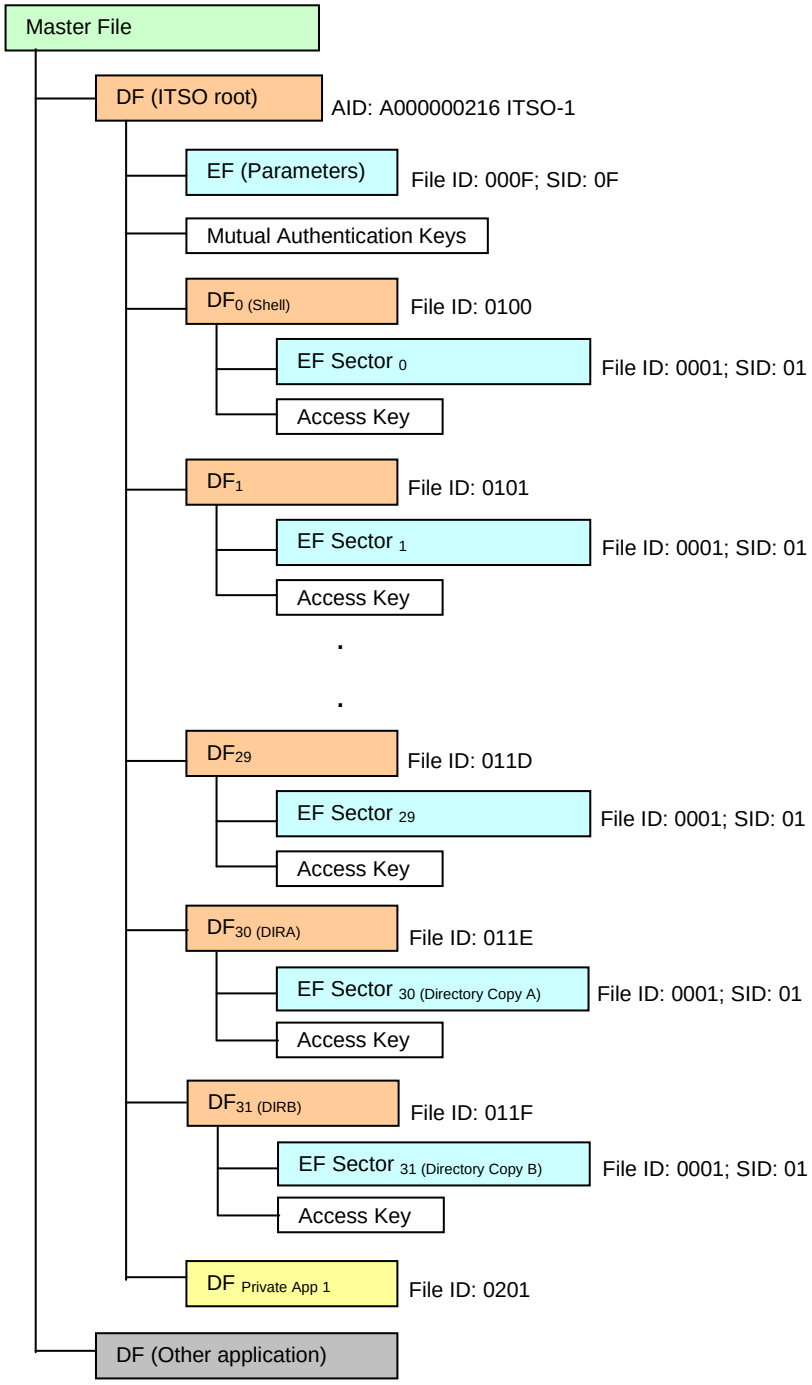

Figure 1 - ITSO file structure

The file system structure shall consist of the following mandatory files:

— A Dedicated File (DF) that acts as the root for the ITSO Application.

— An Elementary File (EF) containing parameter information.

— 1 DF containing the EF used for storage of the ITSO Shell Environment.

— 1 EF used for storage of the ITSO Shell Environment.

— 29[12] DFs containing the EFs used for storage of the ITSO IPE instances.

— 29[13] EFs used for storage of the ITSO IPE instances.

— 2 DFs containing the EFs used for storage of the ITSO Directory copies.

— 2 EFs used for storage of the ITSO Directory copies.

If Private Applications are hosted within the ITSO Shell, then they shall reside in separate DFs.

3.7.1 ITSO Application DF

This file shall have the following attributes:

3.7.1.1 Name

The DF Name for this file shall be the ITSO Application Identifier (AID), in line with recommended practice for DF naming and selection. See section 3.8 for details of the AID.

3.7.1.2 File ID

To ensure compatibility on different card platforms, ITSO does not define a File ID for this file. At the time of DF creation, an appropriate FID shall be generated. The value of this FID shall be stored in the Parameter EF (see section 3.7.2.3.6).

3.7.1.3 Access conditions

Creation	- At personalisation only;
Update	- Not allowed;
Read	- Unconditional;
Delete	- Not allowed.

3.7.2 Parameter EF

This read-only EF file contains parameters relating to the platform.

This file shall have the following attributes.

3.7.2.1 File ID

This file shall be assigned the FID of 000F (hex).

This file shall be assigned the short EF identifier of 0F (hex).

---

[12] Default value - See clause 3.7.4.4.2

[13] Default value - See clause 3.7.4.4.2

3.7.2.2 Access conditions

Creation	- At personalisation only;
Update	- Not allowed;
Read	- Unconditional;
Delete	- Not allowed.

3.7.2.3 File structure

This file shall use a transparent binary structure. The contents of the file shall consist of the following BER-TLV coded data objects:

— Mutual authentication algorithm support	Tag value = C1 (hex);
— Verify command parameter	Tag value = C2 (hex);
— Storage EF short file ID	Tag value = C3 (hex);
— Directory size	Tag value = C4 (hex);
— Anti-tear mechanism	Tag value = C5 (hex);
— ITSO DF file ID	Tag value = C6 (hex);
— ITSO DF path	Tag value = C7 (hex).

3.7.2.3.1 Mutual authentication algorithm support object

The Parameter EF shall contain one or more instance(s) of this object.

This object shall contain the following Data Elements:

Table 8 – Data Elements of the mutual authentication algorithm support object

Item		Size	Value	Comment
Tag		1 byte	C1 (hex)	
Length		1 byte	04	
Data	Algorithm type	1 byte	01, 02 or 03	'Algorithm type' defines the form of mutual authentication that the platform supports. Allowed values (in hex) are listed below. Other values are RFU. 01 - DES with 8 byte key and 8 byte cryptogram 02 - Triple DES with 16 byte key and 8 byte cryptogram 03 - Platform supports secure messaging by use of a MAC. Triple DES with 16 byte key and 8 byte cryptogram. Session key derived and used for secure messaging.
Data	P1 code	1 byte	As required	'P1 code' defines the P1 code that must be sent to the platform as part of the EXTERNAL AUTHENTICATE and the INTERNAL AUTHENTICATE to enable the associated algorithm.
Data	P2 code (EXT)	1 byte	As required	'P2 code (EXT)' defines the P1 code that must be sent to the platform as part of the EXTERNAL AUTHENTICATE. The default value for this is 81 (hex) indicating DF-specific key number 1 to be used. However, if the platform requires another P2 value, then it shall be stored here.
Data	P2 code (INT)	1 byte	As required	'P2 code (INT)' defines the P1 code that must be sent to the platform as part of the INTERNAL AUTHENTICATE. The default value for this is 82 (hex) indicating DF-specific key number 2 to be used. However, if the platform requires another P2 value, then it shall be stored here.

It is mandatory that all platforms support at least one of the algorithm types shown in Table 8.

If the platform supports more than a single algorithm type this may be indicated by the presence of multiple instances of the mutual authentication algorithm support object within the Parameter EF. In this case the algorithm type of the highest value supported shall be the first instance of the object in the Parameter EF, further instances may be present, appended in descending order of algorithm Type value.

3.7.2.3.2 VERIFY command parameter object

The Parameter EF shall contain one instance of this object.

This object shall contain the following Data Elements:

Table 9 - Data Elements of the VERIFY command parameter object

Item		Size	Value	Comment
Tag		1 byte	C2 (hex)	
Length		1 byte	02	
Data	P1 code	1 byte	As required	'P1 code' defines the P1 code that must be sent to the platform as part of the VERIFY command.
Data	P2 code	1 byte	As required	'P2 code' defines the P1 code that must be sent to the platform as part of the VERIFY command. The code shall select a DF-specific password.

3.7.2.3.3 Storage EF short file ID object

The Parameter EF shall contain one instance of this object.

This object shall contain the following Data Elements:

Table 10 - Data Elements of the storage EF short file ID object

Item		Size	Value	Comment
Tag		1 byte	C3 (hex)	
Length		1 byte	01	
Data	Short file ID for storage EFs	1 byte	01 or as required	The recommended short file ID for the storage EFs is 01. If the platform reserves this value (01) for other use, then the short ID actually used for the EFs shall be indicated by this field.

3.7.2.3.4 Directory size object

The Parameter EF shall contain one instance of this object.

This object shall contain the following Data Elements:

Table 11 - Data Elements of the Directory size object

Item		Size	Value	Comment
Tag		1 byte	C4 (hex)	
Length		1 byte	01	
Data	Directory size	1 byte	96 or as required	The recommended Directory size for this CMD is 96 bytes. If the platform uses a different size of Directory then the size (in bytes) shall be indicated by this field. The following are recommended alternative Directory sizes: 32, 48, 64, 80, 112, 128, 144, 160, 176 and 192 bytes

3.7.2.3.5 Anti-tear mechanism object

The Parameter EF shall contain one instance of this object.

This object shall contain the following Data Elements:

Table 12 - Data Elements of the Anti-tear mechanism object

Item		Size	Value	Comment
Tag		1 byte	C5 (hex)	
Length		1 byte	01	
Data	Software Anti-tear mechanism	1 byte	00 (none) 01 (type A)	This defines which form of software Anti-tear shall be used. A value of 00 indicates that the card does not require any form of software Anti-tear to be provided. The default value is 01 (type A).

3.7.2.3.6 ITSO DF file ID object

The Parameter EF shall contain one instance of this object if the platform supports selection by FID, and does not support selection by path (see section 3.7.2.3.7).

The Parameter EF shall not contain both this object and the ITSO DF path object.

On platforms supporting this form of selection, the ITSO DF shall be a child of the MF.

This object shall contain the following data elements:

Table 13 - Data elements of the ITSO DF file ID object

Item		Size	Value	Comment
Tag		1 byte	C6 (hex)	
Length		1 byte	02	
Data	File ID for the ITSO DF	2 bytes	As required	This shall store the FID for the ITSO application DF (see section 3.7.1)

If this object is present, then POSTs shall use selection by FID.

3.7.2.3.7 ITSO DF path object

If the media supports selection by path[14], then the Parameter EF shall contain one instance of this object.

This object shall contain the following data elements:

Table 14 Data elements of the ITSO DF path object

Item		Size	Value	Comment
Tag		1 byte	C7 (hex)	
Length		1 byte	As required	
Data	Full path to the ITSO DF	As required	As required	This shall store the full path to the ITSO application DF

If this object is present, then POSTs shall use selection by path.

3.7.3 Storage Sector DFs

By default the platform shall contain 32 of these files. Their default usage is:

— The first shall be used to store the ITSO Shell Environment EF.

— The next 29 shall be used to store the IPE EFs.

— The penultimate shall be used to store the EF containing Directory copy A.

— The last one shall be used to store the EF containing Directory copy B.

Each file shall have the following attributes:

3.7.3.1 File ID

Each file shall have a unique FID. Files shall be numbered sequentially, starting at 0100 (hex). A platform that supports the default 29 IPE Sectors (S = 29) shall have files 0100 to 011F inclusive.

3.7.3.2 Access conditions

Creation - At personalisation only;

Update - Not allowed;

[14] As defined in ISO / IEC 7816-4:1995

Read - Unconditional;

Delete - Not allowed.

3.7.4 ITSO Shell Environment EF

This EF (the first of the storage EFs) contains the ITSO Shell Environment Data Group. This file shall have the following attributes.

3.7.4.1 File ID

As per the other storage EFs this file shall have a standard FID with a value of 0001.

By default this file shall have the short EF identifier of 01. Where a platform does not allow the use of this short ID for user files, then the alternative value shall be specified in the Parameter EF (see section 3.7.2.3.3)

3.7.4.2 Access conditions

Creation - At personalisation only;

Update - Allowed, subject to valid mutual authentication and presentation of correct access key;

Read - Unconditional;

Delete - Not allowed.

3.7.4.3 File structure

This file shall use a transparent binary structure. The size of the file shall be 'B' bytes[15], where 'B' is defined as in ITSO TS 1000-2.

3.7.4.4 ITSO Shell Environment Data Group

The ITSO Shell Environment Data Group shall be stored in this EF. The elements and layout of this data structure are fully defined in ITSO TS 1000-2.

3.7.4.4.1 Platform parameters with fixed values

The following platform parameter Data Elements within the ITSO Shell Environment Data Group shall have the fixed values specified herein for all implementations of this CMD.

Table 15 - Fixed platform parameter values

Data Element	Default value	Comment
ShellLength	6 8	If the optional MCRN is not present If the optional MCRN is present
ShellBitMap	msb-000001-lsb msb-000011-lsb	If the optional MCRN is not present If the optional MCRN is present
ShellFormatRevision	1	For this version of the Specification
FVC	2	See section 3.3

[15] The default value of 'B' is 48

3.7.4.4.2 Platform parameters with default values which may be overridden

The following platform parameter Data Elements within the ITSO Shell Environment Data Group shall have (explicit) default values as listed below. However, ITSO Shell Owners may override these defaults by specifying an alternative value within the associated data field of the ITSO Shell Environment Data Group at the time of ITSO Shell creation.

POSTs shall correctly parse and use the parameter values provided by the platform.

Table 16 - Default Data Element values

Data Element	Default value	Comment
KSC	2 or 3	For Micro processor with mutual authentication using one key KSC = 2 For Micro processor with mutual authentication using two keys KSC = 3
B	48 (30 hex)	Size of storage Sector.
S	32 (20 hex)	This gives a Ψ of 5
E	8	Number of Directory Entries
SCTL	19 (13 hex)	Length of SCT

As well as the above parameters held within the ITSO Shell Environment Data Group, this CMD allows ITSO Shell Owners to specify non-default Directory sizes (see section 3.7.2.3.4) at the time of ITSO Shell creation.

3.7.4.4.3 ITSO Shell Environment detailed layout

Table 17 details the location of the Data Elements when the default platform parameter values are used. Shading indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Table 17 - Default ITSO Shell Environment data content - No MCRN present

Data Element Label	# of bits	Start location	End location
ShellLength	6	Byte 0, bit 7	Byte 0, bit 2
ShellBitMap	6	Byte 0, bit 1	Byte 1, bit 4
ShellFormatRevision	4	Byte 1, bit 3	Byte 1, bit 0
IIN	24	Byte 2, bit 7	Byte 4, bit 0
OID	16	Byte 5, bit 7	Byte 6, bit 0
ISSN	28	Byte 7, bit 7	Byte 10, bit 4
CHD	4	Byte 10, bit 3	Byte 10, bit 0
FVC	8	Byte 11, bit 7	Byte 11, bit 0
KSC	8	Byte 12, bit 7	Byte 12, bit 0
KVC	8	Byte 13, bit 7	Byte 13, bit 0
RFU	2	Byte 14, bit 7	Byte 14, bit 6
EXP	14	Byte 14, bit 5	Byte 15, bit 0
B	8	Byte 16, bit 7	Byte 16, bit 0
S	8	Byte 17, bit 7	Byte 17, bit 0
E	8	Byte 18, bit 7	Byte 18, bit 0
SCTL	8	Byte 19, bit 7	Byte 19, bit 0
PAD	16	Byte 20, bit 7	Byte 21, bit 0
SECRC	16	Byte 22, bit 7	Byte 23, bit 0

Table 17a - Default ITSO Shell Environment data content - MCRN present

Data Element Label	# of bits	Start location	End location
ShellLength	6	Byte 0, bit 7	Byte 0, bit 2
ShellBitMap	6	Byte 0, bit 1	Byte 1, bit 4
ShellFormatRevision	4	Byte 1, bit 3	Byte 1, bit 0
IIN	24	Byte 2, bit 7	Byte 4, bit 0
OID	16	Byte 5, bit 7	Byte 6, bit 0
ISSN	28	Byte 7, bit 7	Byte 10, bit 4
CHD	4	Byte 10, bit 3	Byte 10, bit 0
FVC	8	Byte 11, bit 7	Byte 11, bit 0
KSC	8	Byte 12, bit 7	Byte 12, bit 0
KVC	8	Byte 13, bit 7	Byte 13, bit 0
RFU	2	Byte 14, bit 7	Byte 14, bit 6
EXP	14	Byte 14, bit 5	Byte 15, bit 0
B	8	Byte 16, bit 7	Byte 16, bit 0
S	8	Byte 17, bit 7	Byte 17, bit 0
E	8	Byte 18, bit 7	Byte 18, bit 0
SCTL	8	Byte 19, bit 7	Byte 19, bit 0
MCRN	80	Byte 20, bit 7	Byte 29, bit 0
SECRC	16	Byte 30, bit 7	Byte 31, bit 0

3.7.5 IPE storage EFs

By default the platform shall contain 29 of these files. These EFs are used to store the following Data Groups:

— IPE;

— Value Record;

— Cyclic Log.

Each of these files shall have the following attributes.

3.7.5.1 File ID

Each file shall have a standard FID with a value of 0001.

By default each file shall have the short EF identifier of 01. Where a platform does not allow the use of this short ID for user files, then the alternative value shall be specified in the Parameter EF (see section 3.7.2.3.3)

3.7.5.2 Access conditions

Creation	- At personalisation only;
Update	- Allowed, subject to valid mutual authentication and presentation of correct access key;
Read	- Unconditional;
Delete	- Not allowed.

3.7.5.3 File structure

Each file shall use a transparent binary structure. The file size shall be 'B' bytes[16].

3.7.6 Directory EFs

These two EFs (the last 2 of the storage EFs) shall be used to store the following Data Groups:

— Directory (copy A);

— Directory (copy B).

These files shall have the following attributes.

3.7.6.1 File ID

As per the other storage EFs these files shall have a standard FID with a value of 0001.

By default each file shall have the short EF identifier of 01. Where a platform does not allow the use of this short ID for user files, then the alternative value shall be specified in the Parameter EF (see section 3.7.2.3.3)

3.7.6.2 Access conditions

Creation	- At personalisation only;
Update	- Allowed, subject to valid mutual authentication and presentation of correct access key;
Read	- Unconditional;
Delete	- Not allowed.

[16] The default value of 'B' is 48

3.7.6.3 File structure

These files shall use a transparent binary structure.

The default file size shall be 96 bytes. Where a platform does not use this default Directory size, then the actual value shall be specified in the Parameter EF (see section 3.7.2.3.4). POSTs shall check for and correctly process Directories of non-default size.

3.7.6.4 Directory Data Group location

Table 18 details the location of the Data Elements for each copy when the default platform parameter values are used. Shading indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Table 18 - Default Directory Data Group

Data Element Label	# of bits	Start location	End location
DIRLength	6	Byte 0, bit 7	Byte 0, bit 2
DIRBitMap	6	Byte 0, bit 1	Byte 1, bit 4
DIRFormatRevision	4	Byte 1, bit 3	Byte 1, bit 0
E1	40	Byte 2, bit 7	Byte 6, bit 0
E2	40	Byte 7, bit 7	Byte 11, bit 0
E3	40	Byte 12, bit 7	Byte 16, bit 0
E4	40	Byte 17, bit 7	Byte 21, bit 0
E5	40	Byte 22, bit 7	Byte 26, bit 0
E6	40	Byte 27, bit 7	Byte 31, bit 0
E7	40	Byte 32, bit 7	Byte 36, bit 0
E8	40	Byte 37, bit 7	Byte 41, bit 0
SCT1	5 [17]	Byte 42, bit 7	Byte 42, bit 3
SCT2	5	Byte 42, bit 2	Byte 43, bit 6
SCT3	5	Byte 43, bit 5	Byte 43, bit 1
SCT4	5	Byte 43, bit 0	Byte 44, bit 4
SCT5	5	Byte 44, bit 3	Byte 45, bit 7
SCT6	5	Byte 45, bit 6	Byte 45, bit 2
SCT7	5	Byte 45, bit 1	Byte 46, bit 5
SCT8	5	Byte 46, bit 4	Byte 46, bit 0
SCT9	5	Byte 47, bit 7	Byte 47, bit 3
SCT10	5	Byte 47, bit 2	Byte 48, bit 6
SCT11	5	Byte 48, bit 5	Byte 48, bit 1
SCT12	5	Byte 48, bit 0	Byte 49, bit 4
SCT13	5	Byte 49, bit 3	Byte 50, bit 7
SCT14	5	Byte 50, bit 6	Byte 50, bit 2
SCT15	5	Byte 50, bit 1	Byte 51, bit 5
SCT16	5	Byte 51, bit 4	Byte 51, bit 0
SCT17	5	Byte 52, bit 7	Byte 52, bit 3
SCT18	5	Byte 52, bit 2	Byte 53, bit 6
SCT19	5	Byte 53, bit 5	Byte 53, bit 1
SCT20	5	Byte 53, bit 0	Byte 54, bit 4
SCT21	5	Byte 54, bit 3	Byte 55, bit 7
SCT22	5	Byte 55, bit 6	Byte 55, bit 2
SCT23	5	Byte 55, bit 1	Byte 56, bit 5
SCT24	5	Byte 56, bit 4	Byte 56, bit 0
SCT25	5	Byte 57, bit 7	Byte 57, bit 3
SCT26	5	Byte 57, bit 2	Byte 58, bit 6
SCT27	5	Byte 58, bit 5	Byte 58, bit 1

[17] The number of bits for the SCTx fields is equal to Ψ

SCT28	5	Byte 58, bit 0	Byte 59, bit 4
SCT29	5	Byte 59, bit 3	Byte 60, bit 7
PAD	7	Byte 60, bit 6	Byte 60, bit 0
DIRS#	8	Byte 61, bit 7	Byte 61, bit 0
KID	4	Byte 62, bit 7	Byte 62, bit 4
INS#	4	Byte 62, bit 3	Byte 62, bit 0
ISAMID	32	Byte 63, bit 7	Byte 66, bit 0
Seal	64	Byte 67, bit 7	Byte 74, bit 0

3.7.6.4.1 DIRLength

This is RFU and shall contain a value of 0.

3.7.6.4.2 DIRFormatRevision

This shall contain a value of 1 (1 hex).

3.7.6.4.3 Sector Chain Table (SCT) usage

The relationship between the SCT entries and the physical storage on the platform is done on a Sector-to-EF basis. Each SCT Label corresponds to an EF (contained within a DF) on the platform.

When the default platform parameters are used then each SCT entry shall contain a number in the range 0 to 31 (decimal). The following values shall have special significance as defined in ITSO TS 1000-2.

Note: As stated in section 3.7.4.4.2, the default value of S is 32 for this CMD. If an alternate S is used, then the above value ranges and the latter two special SCT values in the table below shall be adjusted accordingly (as defined in ITSO TS 1000-2).

Table 19 - Special SCT values

SCT entry value (decimal)	Significance
0	Corresponding EF (see Table 20) is un-allocated and may be used to store product data.
'Self'[18]	Terminating Sector / EF for product in question. Product is Virgin
30	Terminating Sector / EF for product in question. Product is Blocked
31	Terminating Sector / EF for product in question. Product is not Blocked

Table 20 defines the mapping between SCT Label and the IPE DFs / EFs.

[18] Where 'Self' means that the value in the entry corresponds to the entry's own number / Label. For example if SCT11 contains the value 11 (decimal) then this is a 'self' reference.

Table 20 - SCT Label vs. IPE DF and EF

SCT Label	IPE DF / IPE EF
SCT1	0101 / 0001
SCT2	0102 / 0001
SCT3	0103 / 0001
SCT4	0104 / 0001
SCT5	0105 / 0001
SCT6	0106 / 0001
SCT7	0107 / 0001
SCT8	0108 / 0001
SCT9	0109 / 0001
SCT10	010A / 0001
SCT11	010B / 0001
SCT12	010C / 0001
SCT13	010D / 0001
SCT14	010E / 0001
SCT15	010F / 0001
SCT16	0110 / 0001
SCT17	0111 / 0001
SCT18	0112 / 0001
SCT19	0113 / 0001
SCT20	0114 / 0001
SCT21	0115 / 0001
SCT22	0116 / 0001
SCT23	0117 / 0001
SCT24	0118 / 0001
SCT25	0119 / 0001
SCT26	011A / 0001
SCT27	011B / 0001
SCT28	011C / 0001
SCT29	011D / 0001

Note that the 29 EFs listed above shall be used to store Data Elements associated with the following Data Groups:

— IPE;

— Value Record;

— Cyclic Log.

As defined in ITSO TS 1000-2, Sectors SCT1 to SCT'E'[19] (shown shaded) have special significance, and are reserved as Starting Sectors.

[19] Default value of E is 8

3.7.6.4.4 PTYP usage for Private Applications

Where the data associated with a Directory Entry is a Private Application, the PTYP field within the Directory Entry shall be used to generate the DF identifier (see section 3.7.7). In such cases the value within the PTYP field shall be in the range 01 (hex) to 0F (hex).

3.7.7 Private Application DFs

Private Applications are permitted under the ITSO DF. They shall be in the form of a child DF within the ITSO DF.

DF status enables the Private Application to either inherit ITSO's security policy, or replace it with its own. It also removes any constraints for EF naming between ITSO and the Private Application(s).

Up to 8 Private Applications may be concurrently hosted on a platform with default parameters. Note however that this would not leave any available Directory Entries for ITSO products.

3.7.7.1 Identification and naming of Private Applications

As defined in ITSO TS 1000-2, a Private Application is indicated by a TYP value of 0 within the ITSO Directory Entry.

The name of the DF containing the Private Application shall be generated by adding the value contained in the PTYP field of the ITSO Directory Entry to 0200 (hex). This will result in a DF name in the range 0201 to 020F.

3.7.7.2 Access conditions

Creation	- As required by application owner;
Update	- As required by application owner;
Read	- As required by application owner;
Delete	- As required by application owner.

3.8 ITSO Application selection

The ITSO Application shall be selected by use of the SELECT FILE command in a direct application selection manner. The data field of this command shall be the ITSO Application Identifier (AID), defined and used in accordance to ISO/IEC 7816-5:1994. Application selection shall only be done by use of the AID.

In accordance with ISO/IEC 7816-5:1994, the AID shall be made up of:

— Registered Application Provider Identifier (RID) for ITSO 5 bytes;

— Proprietary Application Identifier Extension (PIX) 6 bytes.

3.8.1 ITSO RID

The international RID assigned to ITSO is (in hex): A0, 00, 00, 02, 16

As defined in ISO/IEC 7816-5:1994, the registration category for this RID is International and as such is represented by A (hex) in the 4 most significant bits.

3.8.2 ITSO PIX

The PIX field shall be 6 bytes in length and shall contain the ASCII string "ITSO-1".[20]

[20] Which is hex is: 49, 54, 53, 4F, 2D, 31

This format provides for explicit identification of the ITSO Application, and allows for the support of multiple ITSO Applications in the future.

3.8.3 SELECT FILE

3.8.3.1 Command pre-conditions

None. The POST may issue this command at any time. This command must be used to select the ITSO Application on the media. It would not normally be required to be issued again during a session.

3.8.3.2 Command parameters

The table below defines the parameters required for the SELECT FILE command for the ITSO Application.

Table. 21 - SELECT FILE parameters

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with ISO/IEC 7816-4:1995 Secure messaging not used
1	INS	A4	SELECT FILE command
2	P1	04	Selection by DF name
3	P2	00	Select first or only occurrence of ITSO Application and return FCI
4	Lc	0B	Length of data field
5	Data	A0	Category code and ms digit of RID
6	Data	00	RID
7	Data	00	RID
8	Data	02	RID
9	Data	16	RID
10	Data	49	PIX ”I”
11	Data	54	PIX “T”
12	Data	53	PIX “S”
13	Data	4F	PIX “O”
14	Data	2D	PIX “-“
15	Data	31	PIX “1”
16	Le	00[21]	Maximum response length

3.8.3.3 Response status codes

The SW1 and SW2 status bytes shall contain the appropriate response code in accordance with ISO/IEC 7816-4:1995.

Response codes other than those signifying normal processing (9000 or 61xx) shall cause the POST to abort the session and indicate an error to the user.

[21] The response length will vary dependant on the platform’s FCI Proprietary Template support.

3.8.3.4 Response data

The response data to the SELECT FILE command shall comprise of the following BER-TLV data objects within the File Control Information (FCI) template.

— DF Name

— FCI Proprietary Template[22]

In accordance with ISO/IEC 7816-4:1995, the above data objects shall be ASN.1 tagged. The following tags shall be used:

— 6F (hex) FCI Template [23]

— 84 (hex) DF Name [24]

— A5 (hex) FCI Proprietary Template[25]

3.8.3.4.1 DF Name object

The DF Name object shall consist of the following Data Elements:

— ITSO Application Identifier

The table below details the data structure of this object.

Table 22 - DF Name object

Byte offset	Label	Value (hex)	Description
0	TAG	84	Tag denoting DF Name
1	LEN	0B	Length of Data Element
2	Data	A0	Category code and ms digit of ITSO RID
3	Data	00	ITSO RID
4	Data	00	ITSO RID
5	Data	02	ITSO RID
6	Data	16	ITSO RID
7	Data	49	PIX “I”
8	Data	54	PIX “T”
9	Data	53	PIX “S”
10	Data	4F	PIX “O”
11	Data	2D	PIX “-“
12	Data	31	PIX “1”

[22] Where the platform supports the use of an FCI Proprietary Template

[23] ISO/IEC 7816-4:1995, table 1;

[24] ISO/IEC 7816-4:1995, table 2;

[25] ISO/IEC 7816-4, table 2; ISO/IEC 7816-6, 4.2.1.

3.8.3.4.2 FCI Proprietary Template object

Where the card platform supports the return of a FCI Proprietary Template, then this shall form part of the response data to the SELECT FILE command. The FCI Proprietary Template constructed object shall consist of the following data objects:

— ITSO Shell Environment EF (see section 3.7.4)

— Parameter EF (see section 3.7.2)

The above data objects shall be ASN.1 tagged. The following tags shall be used:

— C0 (hex) ITSO Shell Environment EF;

— E0 (hex) Parameter EF.

3.9 Mutual authentication and session communications

If a transaction requires an update to any of the contents of files within the ITSO Application area[26], then a secured session shall be established between the media and the POST. This shall be done by the use of mutual authentication.

Note: Where a media platform does not support EF access to be controlled by both mutual authentication and CHV/PIN presentation, then CHV/PIN access control shall be used. However, the mutual authentication sequence defined in the following sections shall still be carried out, and all platforms shall support the commands as defined herein.

The mutual authentication shall be carried out by use of the following commands:

— GET CHALLENGE;

— EXTERNAL AUTHENTICATE;

— INTERNAL AUTHENTICATE.

In addition to the above commands, the following data is used by the POST to establish the secured session.

— ITSO Shell Reference Number[27] (contained in ITSO Shell Environment EF)

Note that on platforms that support secure messaging, this feature is not available until a successful mutual authentication exchange has been carried out and a secure session established.

3.9.1 Command sequence

Mutual authentication between media and POST shall take place by the following exchange of commands.

[26] ITSO does not mandate the use of mutual authentication for Private Application updates.

[27] As defined in ITSO TS 1000-1

Table 23 - Mutual authentication command sequence

POST to Media	Media to POST
GET CHALLENGE	
	GET CHALLENGE Response
EXTERNAL AUTHENTICATE	
	EXTERNAL AUTHENTICATE Response
INTERNAL AUTHENTICATE	
	INTERNAL AUTHENTICATE Response

The POST to media mutual authentication sequence (including the command sequences to/from the ISAM) is fully detailed in ITSO TS 1000-7.

3.9.2 GET CHALLENGE

3.9.2.1 Command pre-conditions

The ITSO Application must have been previously selected by use of the SELECT FILE command (see section 3.8.3).

3.9.2.2 Command parameters

The table below defines the parameters required for the GET CHALLENGE command.

Table 24 - GET CHALLENGE parameters

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with ISO/IEC 7816-4:1995 Secure messaging not used
1	INS	84	GET CHALLENGE command
2	P1	00	As ISO/IEC 7816-4:1995
3	P2	00	As ISO/IEC 7816-4:1995
4	Le	08	Reply length

3.9.2.3 Response status codes

The SW1 and SW2 status bytes shall contain the appropriate response code in accordance with ISO/IEC 7816-4:1995.

Response codes other than those signifying normal processing (9000 or 61xx) shall cause the POST to abort the session and indicate an error to the user.

3.9.2.4 Response data

The response data to the GET CHALLENGE command shall be an 8-byte random number generated by the media.

3.9.3 EXTERNAL AUTHENTICATE

3.9.3.1 Command pre-conditions

The ITSO Application must have been previously selected by use of the SELECT FILE command (see section 3.8.3).

The POST must have issued a GET CHALLENGE command and received an 8-byte random number from the media (see section 3.9.2).

3.9.3.2 Command parameters

The table below defines the parameters required for the EXTERNAL AUTHENTICATE command.

Table 25 - EXTERNAL AUTHENTICATE parameters

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with ISO/IEC 7816-4:1995 Secure messaging not used
1	INS	82	EXTERNAL AUTHENTICATE command
2	P1	??	Algorithm P1 code (see section 3.7.2.3.1)
3	P2	??	P2 code - EXT (see section 3.7.2.3.1)
4	Lc	08	Length of data field
5	Data	??	Encrypted random number
6	Data	??	Encrypted random number
7	Data	??	Encrypted random number
8	Data	??	Encrypted random number
9	Data	??	Encrypted random number
10	Data	??	Encrypted random number
11	Data	??	Encrypted random number
12	Data	??	Encrypted random number

3.9.3.3 Response status codes

The SW1 and SW2 status bytes shall contain the appropriate response code in accordance with ISO/IEC 7816-4:1995.

Response codes other than those signifying normal processing (9000 or 61xx) shall cause the POST to abort the session and indicate an error to the user.

3.9.3.4 Response data

There is no response data for the EXTERNAL AUTHENTICATE command.

3.9.4 INTERNAL AUTHENTICATE

3.9.4.1 Command pre-conditions

The ITSO Application must have been previously selected by use of the SELECT FILE command (see section 3.8.3).

The POST must have issued a GET CHALLENGE command and got a valid response from the media (see section 3.9.2).

The POST must have issued an EXTERNAL AUTHENTICATE command and got a valid response from the media (see section 3.9.3).

3.9.4.2 Command parameters

The table below defines the parameters required for the INTERNAL AUTHENTICATE command.

Table 26 - INTERNAL AUTHENTICATE parameters

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with ISO/IEC 7816-4:1995 Secure messaging not used
1	INS	88	INTERNAL AUTHENTICATE command
2	P1	??	Algorithm P1 code (see section 3.7.2.3.1)
3	P2	??	P2 code - INT (see section 3.7.2.3.1)
4	Lc	08	Length of data field
5	Data	??	Random number
6	Data	??	Random number
7	Data	??	Random number
8	Data	??	Random number
9	Data	??	Random number
10	Data	??	Random number
11	Data	??	Random number
12	Data	??	Random number
13	Le	08	Response length

3.9.4.3 Response status codes

The SW1 and SW2 status bytes shall contain the appropriate response code in accordance with ISO/IEC 7816-4:1995.

Response codes other than those signifying normal processing (9000 or 61xx) shall cause the POST to abort the session and indicate an error to the user.

3.9.4.4 Response data

The response data to the INTERNAL AUTHENTICATE command shall be an 8-byte cryptogram computed by the media using:

— The 8-byte random number sent with the command.

— The (media-specific) ITSO Application internal secret key associated with the INTERNAL AUTHENTICATE command.

— The selected authentication algorithm.

3.10 Parameter EF access

The Parameter EF shall be accessed by use of the READ BINARY command, with implicit selection using the short EF identifier.

Read access to this EF shall be unconditional, and can be done at any time after the ITSO Application has been selected (see section 3.8.3).

Update access to this EF is not allowed.

3.10.1 READ BINARY

3.10.1.1 Command pre-conditions

The ITSO Application must have been previously selected by use of the SELECT FILE command (see section 3.8.3).

3.10.1.2 Command parameters

The table below defines the READ BINARY command parameters required.

Table 27 - READ BINARY parameters

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with ISO/IEC 7816-4 Secure messaging not used
1	INS	B0	READ BINARY command
2	P1	8F	Implicit selection of EF 0F
3	P2	00	Offset to the first byte to be read
4	Le	00[28]	Response length

Note: Where secure messaging is supported then an alternative CLA byte shall be used to activate its use in accordance with ISO/IEC 7816-4

The table below defines the READ BINARY command parameters required when secure messaging is used.

Table 27a - READ BINARY parameters (secure messaging)

Byte offset	Label	Value (hex)	Description
0	CLA	04	Command compliant with ISO/IEC 7816-4:1995 Secure messaging used
1	INS	B0	READ BINARY command
2	P1	81	Implicit selection of EF 01
3	P2	00	Offset to first byte to be read
4	Le	00[29]	Response length

3.10.1.3 Response status codes

The SW1 and SW2 status bytes shall contain the appropriate response code in accordance with ISO/IEC 7816-4:1995.

Response codes other than those signifying normal processing (9000 or 61xx) shall cause the POST to abort the session and indicate an error to the user.

[28] No response length specified.

[29] No response length specified.

3.10.1.4 Response data

The response to the READ BINARY command is a variable length data Block, consisting of a number of BER-TLV data objects. The data structure shall be as defined in section 3.7.2.

If secure messaging is activated an additional MAC Data Element will be appended to the data in the block. This MAC should be verified by the ISAM to ensure the data was read from the media in the current secured session.

3.11 Storage EF access

The storage EFs shall be accessed by use of the READ BINARY and UPDATE BINARY commands, with implicit selection using the short EF identifier.

Read access to these EFs shall be unconditional, and can be done at any time, subject to selection of the required DF (by use of the SELECT FILE command).

Update access to these EFs shall require a valid mutual authentication session to have taken place, followed by the presentation of the correct access key.

3.11.1 SELECT FILE

3.11.1.1 Command pre-conditions

The ITSO Application must have been previously selected by use of the SELECT FILE command (see section 3.8.3).

3.11.1.2 Command parameters

The table below defines the parameters required for the SELECT FILE command for the storage DF, where the media does not support selection by path (see section 3.7.2.3.7).

Table 28 - SELECT FILE parameters (storage DF)

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with ISO/IEC 7816-4:1995 Secure messaging not used
1	INS	A4	SELECT FILE command
2	P1	00	Selection by FID
3	P2	00	Select first or only occurrence and return FCI
4	Lc	02	Length of data field
5	Data	01	MS byte of FID
6	Data	??	LS byte of FID Range 00 to 1F[30] (hex)
7	Le	00[31]	Maximum response length

On media without selection by path support, it is necessary to select the ITSO DF before selecting another storage DF. This SELECT FILE command will take the form shown in the table below:

[30] Based on default parameter values

[31] No response length specified.

Table 29 - SELECT FILE parameters (ITSO DF)

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with ISO/IEC 7816-4:1995 Secure messaging not used
1	INS	A4	SELECT FILE command
2	P1	00	Selection by FID
3	P2	00	Select first or only occurrence and return FCI
4	Lc	02	Length of data field
5	Data	??	MS byte of ITSO DF FID. FID value obtained from parameter EF (see section 3.7.2.3.6)
6	Data	??	LS byte of ITSO DF FID
7	Le	00[32]	Maximum response length

The following is an example of the command sequence required to read 3 storage EFs. It assumes the ITSO application has already been selected.

— SELECT FILE (0101)

— READ BINARY (01)

— SELECT FILE (0101)

— SELECT FILE (ITSO DF)

— SELECT FILE (0102)

— READ BINARY (01)

— SELECT FILE (0102)

— SELECT FILE (ITSO DF)

— SELECT FILE (0103)

— READ BINARY (01)

Where the media supports selection by path (see section 3.7.2.3.7), then an alternative selection mechanism shall be used by the POST. This reduces the number of SELECT FILE commands required.

This alternate SELECT FILE command will take the form shown in the table below:

[32] No response length specified.

Table 30 - SELECT FILE parameters (by path)

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with ISO/IEC 7816-4:1995 Secure messaging not used
1	INS	A4	SELECT FILE command
2	P1	08	Selection by path
3	P2	00	Select first or only occurrence and return FCI
4	Lc	??	Length of data field
5	Data	??	First byte of path to ITSO DF. Path value obtained from parameter EF (see section 3.7.2.3.7)
6	Data	??	Second byte of path to ITSO DF
n-2	Data	01	MS byte of FID
n-1	Data	??	LS byte of FID Range 00 to 1F[33] (hex)
n	Le	00[34]	Maximum response length

Using the same example as above, the required command sequence for reading 3 storage EFs with this mechanism is:

— SELECT FILE (PATH 0101)

— READ BINARY (01)

— SELECT FILE (PATH 0102)

— READ BINARY (01)

— SELECT FILE (PATH 0103)

— READ BINARY (01)

3.11.1.3 Response status codes

The SW1 and SW2 status bytes shall contain the appropriate response code in accordance with ISO/IEC 7816-4:1995.

Response codes other than those signifying normal processing (9000 or 61xx) shall cause the POST to abort the session and indicate an error to the user.

3.11.1.4 Response data

The response data to the SELECT FILE command will be the File Control Information (FCI) for the selected DF.

3.11.2 READ BINARY

3.11.2.1 Command pre-conditions

The relevant DF must have been previously selected by use of the SELECT FILE command (see section 3.11.1).

---

[33] Based on default parameter values

[34] No response length specified.

If the platform supports secure messaging and the read is being carried out within a secured session, then the ITSO Application must have previously been selected and mutually authenticated (see sections 3.9.2 to 3.9.4).

3.11.2.2 Command parameters

The table below defines the READ BINARY command parameters required when secure messaging is not used.

Table 31 - READ BINARY parameters (normal)

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with ISO/IEC 7816-4:1995 Secure messaging not used
1	INS	B0	READ BINARY command
2	P1	81	Implicit selection of EF 01
3	P2	00	Offset to first byte to be read
4	Le	00[35]	Response length

The table below defines the READ BINARY command parameters required when secure messaging is used.

Table 31a - READ BINARY parameters (secure messaging)

Byte offset	Label	Value (hex)	Description
0	CLA	04	Command compliant with ISO/IEC 7816-4:1995 Secure messaging used
1	INS	B0	READ BINARY command
2	P1	81	Implicit selection of EF 01
3	P2	00	Offset to first byte to be read
4	Le	00[36]	Response length

3.11.2.3 Response status codes

The SW1 and SW2 status bytes shall contain the appropriate response code in accordance with ISO/IEC 7816-4:1995.

Response codes other than those signifying normal processing (9000 or 61xx) shall cause the POST to abort the session and indicate an error to the user.

3.11.2.4 Response data

The response to the READ BINARY command is a data block of up to ‘B’ bytes in length if an IPE storage Sector was selected. If a Directory Sector was selected, then the default data block length is 96 bytes.

If secure messaging is activated an additional MAC Data Element will be appended to the data in the block. This MAC should be verified by the ISAM to ensure the data was read from the media in the current secured session.

[35] No response length specified.

[36] No response length specified.

3.11.3 VERIFY

3.11.3.1 Command pre-conditions

The ITSO Application must have previously been selected and mutually authenticated (sections 3.9.2 to 3.9.4)

The relevant DF must have been previously selected by use of the SELECT FILE command (see section 3.11.1).

3.11.3.2 Command parameters

The table below defines the parameters required for the VERIFY command.

Table 32 - VERIFY parameters

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with ISO/IEC 7816-4:1995 Secure messaging not used
1	INS	20	VERIFY command
2	P1	??	VERIFY P1 code (see section 3.7.2.3.2)
3	P2	??	VERIFY P1 code (see section 3.7.2.3.2)
4	Lc	08	Length of data field
5	Data	??	Access key
6	Data	??	Access key
7	Data	??	Access key
8	Data	??	Access key
9	Data	??	Access key
10	Data	??	Access key
11	Data	??	Access key
12	Data	??	Access key

3.11.3.3 Response status codes

The SW1 and SW2 status bytes shall contain the appropriate response code in accordance with ISO/IEC 7816-4:1995.

Response codes other than those signifying normal processing (9000 or 61xx) shall cause the POST to abort the session and indicate an error to the user.

3.11.3.4 Response data

There is no response data for the VERIFY command.

3.11.4 UPDATE BINARY

3.11.4.1 Command pre-conditions

The ITSO Application must have previously been selected and mutually authenticated (see sections 3.9.2 to 3.9.4)

The relevant DF must have been previously selected by use of the SELECT FILE command (see section 3.11.1).

The correct access key must have been presented (see section 3.11.3)

If secure messaging is activated, a MAC must have been generated over the command data and appended to the end of the data.

3.11.4.2 Command parameters

The table below defines the UPDATE BINARY command parameters required when default 48-byte storage EFs are used, and the platform does not support secure messaging.

Table 33 - UPDATE BINARY parameters (normal)

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with ISO/IEC 7816-4 Secure messaging not used
1	INS	D6	UPDATE BINARY command
2	P1	81	Implicit selection of EF 01
3	P2	00	Offset to first byte to be written
4	Lc	30[37]	Data length
5	Data	??	Data to be written
6	Data	??	Data to be written
.	Data	??	Data to be written
.	Data	??	Data to be written
52	Data	??	Data to be written

The table below defines the UPDATE BINARY command parameters required when default 48-byte storage EFs are used, and the platform does support secure messaging.

[37] Based on re-writing an entire EF of default size

Table 33a - UPDATE BINARY parameters (secure messaging)

Byte offset	Label	Value (hex)	Description
0	CLA	04	Command compliant with ISO/IEC 7816-4 Secure messaging used
1	INS	D6	UPDATE BINARY command
2	P1	81	Implicit selection of EF 01
3	P2	00	Offset to first byte to be written
4	Lc	38[38]	48 bytes of data and 8 byte MAC
5	Data	??	Data to be written
6	Data	??	Data to be written
.	Data	??	Data to be written
.	Data	??	Data to be written
52	Data	??	Data to be written
53	Data	??	MAC byte 0
54	Data	??	MAC byte 1
.	Data	??	MAC bytes 2-5 .
59	Data	??	MAC byte 6
60	Data	??	MAC byte 7

3.11.4.3 Response status codes

The SW1 and SW2 status bytes shall contain the appropriate response code in accordance with ISO/IEC 7816-4:1995.

Response codes other than those signifying normal processing (9000 or 61xx) shall cause the POST to abort the session and indicate an error to the user.

3.11.4.4 Response data

There is no response data for the UPDATE BINARY command.

3.12 Private Application DF access

Access to the Private Application DF(s) shall be via the command set defined in section 3.4.

File access conditions shall be determined by the application owner.

Application owners shall define the data content and format for the above commands.

3.13 Key usage

Selection of the ITSO Application (the DF) shall be unconditional, and shall not require the use of any keys.

Read-only access of all EFs shall be unconditional, and shall not require the use of any keys:

After media personalisation[39], the parameter EF (FID = 000F hex) shall be locked as read-only.

---

[38] Based on re-writing an entire EF of default size

Update of storage EFs (FID = 0001 hex) shall only be allowed after a successful mutual authentication session, followed by the presentation of the correct access key for the relevant DF.

Mutual authentication shall employ the use of a pair of diversified secret keys held in the media. Each of these keys shall be either 8 bytes (DES) or 16 bytes (Triple DES) in length.

— Secret key '1' shall be associated with the EXTERNAL AUTHENTICATE command.

— Secret key '2' shall be associated with the INTERNAL AUTHENTICATE command.

This key pair shall be generated at the time of CM personalisation. They shall not be changed for the life of the media. They shall be media-specific, key diversification being provided by use of the ISRN. The diversification mechanisms are defined in ITSO TS 1000-8.

If the platform supports secure messaging, then the session key shall be derived during the mutual authentication process. This key shall be used to generate and verify the secure messaging MAC.

DF access keys (CHV or PIN numbers) shall be 8 bytes in size. Again, these shall be generated at the time of media personalisation. They shall not be changed for the life of the media. They shall be media-specific, diversification being provided by use of the ISRN. The diversification mechanisms are defined in ITSO TS 1000-8.

Where the DF access key returned by the ISAM is longer than the 8 byte key required by this platform the key to be used shall consist of the first 8 bytes only. Thus for a key of value 0x12123434565678789A9ABCBCDEDEF0F0 returned by the ISAM 0x1212343456567878 shall be used as the access key for the CM.

For key diversification purposes, the following logical Sector numbers shall be used:

— ITSO Shell	Logical Sector 0	
— Directory (copy A)	Logical Sector S-2	(i.e. 30 using default parameters)
— Directory (copy B)	Logical Sector S-1	(i.e. 31 using default parameters)

3.13.1 Private Applications

The access conditions and key usage for Private Applications shall be defined by the application owner.

3.14 Key strategy

This CMD shall use the Key Strategy Code (KSC) value as defined in clause 3.7.4.4.2. The ISAM shall use this to determine the appropriate cryptographic processes to be applied to such media.

3.15 Anti-tear

Where the platform indicates that software Anti-tear is required (see section 3.7.2.3.5), then the appropriate Anti-tear mechanism shall be employed for data contained within the following files:

— IPE EFs

— Directory EF

3.16 Manufacturer's ID

ISO/IEC 7816 does not provide for access to the MID in a standardised manner. Thus this CMD cannot provide for the use of the MID.

---

[39] Where this is taken to mean the creation of the ITSO Shell on the CM.

The following values shall be used when an ITSO MID is required by the POST:

Table 34 - ITSO MID values

ITSO MID byte	Contents
Byte 0 (MSB)	00 (hex)
Byte 1	A5 (hex)
Byte 2	5A (hex)
Byte 3	A5 (hex)
Byte 4	5A (hex)
Byte 5	A5 (hex)
Byte 6	5A (hex)
Byte 7 (LSB)	A5 (hex)

3.17 Detection of the ITSO Shell

The ITSO Shell detection sequence for this CMD shall be as follows:

— If a platform supporting ISO/IEC 14443-4 is detected, then the POST shall issue a SELECT FILE command with the ITSO AID as the target.

— If a valid response is received then the presence of the ITSO Application has been established.

— The POST shall select DF 0100 (hex), and read EF 0001.

— The POST shall parse the data as per section 3.7.4.4.

— A CRC shall be computed for the data read and checked against the SECRC field of the parsed data.

— If this check passes, then the platform carries a valid ITSO Shell.

— The POST shall read and confirm that all the Data Elements listed in Table 15 have the specified values. If this check passes then an ITSO Shell of FVC = 02 shall be deemed to be present.

3.18 Benchmark transaction

3.18.1 IPE with Transient Ticket Record creation

The benchmark transaction for this CMD shall comprise:

— Detection of a platform carrying a valid ITSO Shell with FVC = 02 and default data element values.

— Verification of the Directory, where there is no corruption on either Anti-tear copy

— Verification of an IPE Data Group where there is only a single candidate product, and the IPE Data Group resides in a single Sector (i.e. one EF)

— Creation of a sealed 48-byte Transient Ticket Record

— Update of the log entry and modification of the directory.

— Read after write verification of the updated Directory.

The target execution time for the above, subsequent to detection of the platform, shall be 300ms or less.

Note: The target execution time includes all necessary POST application functions. (i.e. normal operation, Hotlist processing etc…)

3.18.2 IPE with Value Record Data Group modification

The benchmark transaction for this CMD shall comprise:

— Detection of a platform carrying a valid ITSO Shell with FVC = 02 and default data element values.

— Verification of the Directory, where there is no corruption on either Anti-tear copy.

— Verification of an IPE Data Group where there is only a single candidate product and the IPE Data Group resides in a single Sector.

— Verification and modification of an associated Value Record Data Group where there is no corruption on either Anti-tear copy, and the Value Record Data Group resides in a single Sector.

— Modification of the Directory to reflect the changes made to data group and product above.

— Read after write verification of the updated Directory.

The target execution time for the above, subsequent to detection of the platform, shall be 300ms or less.

Note: The target execution time includes all necessary POST application functions. (i.e. normal operation, Hotlist processing etc…)

3.19 List search method

This CMD supports a full ITSO Shell as defined in ITSO TS 1000-2. When a POST carries out a Hotlist or Actionlist search against a platform where FVC = 02, then it shall use ITSO Shell Referencing as defined in ITSO TS 1000-3.

4. Mifare® standard 4K

4.1 Scope

This clause defines the CMD for platforms that use:

— The Philips Mifare® Standard MF1 S70 IC.

— Second-sourced ICs that are equivalent to the Philips MF1 S70 IC.

— A micro-processor which emulates the MF1 S70 IC.

4.1.1 Terminology

Throughout this clause reference will be made to terms defined within the Philips Mifare® Standard Card IC MF1 IC S70 Functional Specification (October 2002). These terms include, but are not limited to: Sector; Block; key; access condition flag.

4.2 Platform capability

4.2.1 General

This platform is capable of supporting a full set of Data Groups, as defined below:

— ITSO Shell Environment	With all optional elements present.
— Directory	Two instances (Anti-tear support); 13 Directory Entries supported.
— IPE	Up to 13 IPE instances may be present.
— Value Record	May be associated with IPEs subject to overall memory limits.
— Cyclic Log	Support for Basic and Normal mode logging.

4.2.2 Memory architecture

The memory architecture of this platform is summarised below:

— 4096 bytes of EEPROM, divided into 2 main areas:

  — An area of 32 Sectors of 64 bytes each (herein termed zone A)

  — An area of 8 Sectors of 256 bytes each (herein termed zone B)

— Within zone A:

  — 16 bytes are reserved for manufacturer data

  — 512 bytes are reserved for keys and access control settings

  — 1520 bytes are available for the general storage of user data

— Within zone B:

  — 128 bytes are reserved for keys and access control settings

  — 1920 bytes are available for the general storage of user data

— Storage capacity of 3408 bytes is available for the ITSO Application.

- Blocks 1 and 2 of Sector 0 are not used
- 288 bytes are used for the ITSO Shell Environment and Directory Data Groups
- 3120 bytes are available for IPE instance, Value Record and Cyclic Log storage.

4.2.3 Security provisions

The platform provides the following security-related features:

- A unique 4-byte manufacture's serial number (MID).
- A pair of 6-byte keys controlling access to each Sector of memory.
- Within each Sector of zone A, access control flags controlling the allowed operations on each 16-byte Block.
- Within each Sector of zone B, access control flags controlling the allowed operations on each set of five 16-byte Blocks.
- Mutual 3-pass authentication between media and reader (to ISO/IEC 9798-2).
- CRYPTO1 stream-cipher for the air interface (proprietary to Philips).

4.2.4 ISO/IEC 14443 compliance

All platforms covered by this CMD shall comply with the following parts of ISO/IEC 14443:

- part 2: RF power & signal interface Compliance with ISO/IEC 14443 Type A requirements;
- part 3: Initialisation & anticollision Compliance with ISO/IEC 14443 Type A requirements;

4.3 Format Version Code

Platforms that conform to this CMD shall use the Format Version Code (FVC) of 03.

4.3.1 Implicit parameters

The following implicit parameter values shall be used for all FVC = 03 platforms.

4.3.1.1 Sector size (B)

The value of B shall be 48 (30 hex) for Sectors 1 to 31 (i.e. Sectors within zone A).

The value of B shall be 240 (F0 hex) for Sectors 32 to 39 (i.e. Sectors within zone B).

4.4 ITSO Shell Environment Data Group

The ITSO Shell Environment Data Group shall be located in Sector 16, Blocks 1 and 2. The elements and layout of this data structure are fully defined in ITSO TS 1000-2.

Block 0 of Sector 16 shall be reserved for future use by ITSO and shall be initialised to all zeros when the ITSO Shell is created.

4.4.1 Platform parameters with fixed values

The following platform parameter Data Elements within the ITSO Shell Environment Data Group shall have the fixed values specified herein for all implementations of this CMD.

Table 35 - Fixed platform parameter values

Data Element	Value	Comment
ShellLength	6 8	If the optional MCRN is not present If the optional MCRN is present
ShellBitMap	msb-000001-lsb msb-000011-lsb	If the optional MCRN is not present If the optional MCRN is present
ShellFormatRevision	1	For this version of the Specification
FVC	3	See section 4.3
KSC	1	For this version of the Specification
B	0	Size of memory Sector. B shall be implicit for this CMD (see section 4.3.1.1)
S	40 (28 hex)	This gives a Ψ of 6
E	13 (0D hex)	Number of Directory Entries
SCTL	28 (1C hex)	Length of SCT

4.4.2 Platform parameters with default values which may be overridden

This CMD does not support the overriding of platform parameter values.

4.4.3 ITSO Shell Environment detailed layout

Table 36 details the location of the Data Elements in Block 1. Table 37 details the location of the Data Elements in Block 2. Shading indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Byte and bit numbers are as defined in the S70 Functional Specification.

Table 36 - Sector 16, Block 1 data content

Data Element Label	# of bits	Start location	End location
ShellLength	6	Byte 0, bit 7	Byte 0, bit 2
ShellBitMap	6	Byte 0, bit 1	Byte 1, bit 4
ShellFormatRevision	4	Byte 1, bit 3	Byte 1, bit 0
IIN	24	Byte 2, bit 7	Byte 4, bit 0
OID	16	Byte 5, bit 7	Byte 6, bit 0
ISSN	28	Byte 7, bit 7	Byte 10, bit 4
CHD	4	Byte 10, bit 3	Byte 10, bit 0
FVC	8	Byte 11, bit 7	Byte 11, bit 0
KSC	8	Byte 12, bit 7	Byte 12, bit 0
KVC	8	Byte 13, bit 7	Byte 13, bit 0
RFU	2	Byte 14, bit 7	Byte 14, bit 6
EXP	14	Byte 14, bit 5	Byte 15, bit 0

Table 37 - Sector 16, Block 2 data content - No MCRN present

Data Element Label	# of bits	Start location	End location
B	8	Byte 0, bit 7	Byte 0, bit 0
S	8	Byte 1, bit 7	Byte 1, bit 0
E	8	Byte 2, bit 7	Byte 2, bit 0
SCTL	8	Byte 3, bit 7	Byte 3, bit 0
PAD	16	Byte 4, bit 7	Byte 5, bit 0
SECRC	16	Byte 6, bit 7	Byte 7, bit 0

Table 37a - Sector 16, Block 2 data content - MCRN present

Data Element Label	# of bits	Start location	End location
B	8	Byte 0, bit 7	Byte 0, bit 0
S	8	Byte 1, bit 7	Byte 1, bit 0
E	8	Byte 2, bit 7	Byte 2, bit 0
SCTL	8	Byte 3, bit 7	Byte 3, bit 0
MCRN	80	Byte 4, bit 7	Byte 13, bit 0
SECRC	16	Byte 14, bit 7	Byte 15, bit 0

4.5 Directory Data Group

The Directory Data Group shall be located in physical Sector 39. Copy A shall reside in Blocks 0 to 6, and copy B in Blocks 8 to 14. Table 38 details the location of the Data Elements for copy A. Copy B shall be in the same order but starting in Block 8, byte 0, bit 7. Shading indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Table 38 - Directory Data Group - copy A

Data Element Label	# of bits	Start location	End location
DIRLength	6	Block 0, byte 0, bit 7	Block 0, byte 0, bit 2
DIRBitMap	6	Block 0, byte 0, bit 1	Block 0, byte 1, bit 4
DIRFormatRevision	4	Block 0, byte 1, bit 3	Block 0, byte 1, bit 0
E1	40	Block 0, byte 2, bit 7	Block 0, byte 6, bit 0
E2	40	Block 0, byte 7, bit 7	Block 0, byte 11, bit 0
E3	40	Block 0, byte 12, bit 7	Block 1, byte 0, bit 0
E4	40	Block 1, byte 1, bit 7	Block 1, byte 5, bit 0
E5	40	Block 1, byte 6, bit 7	Block 1, byte 10, bit 0
E6	40	Block 1, byte 11, bit 7	Block 1, byte 15, bit 0
E7	40	Block 2, byte 0, bit 7	Block 2, byte 4, bit 0
E8	40	Block 2, byte 5, bit 7	Block 2, byte 9, bit 0
E9	40	Block 2, byte 10, bit 7	Block 2, byte 14, bit 0
E10	40	Block 2, byte 15, bit 7	Block 3, byte 3, bit 0
E11	40	Block 3, byte 4, bit 7	Block 3, byte 8, bit 0
E12	40	Block 3, byte 9, bit 7	Block 3, byte 13, bit 0
E13	40	Block 4, byte 14, bit 7	Block 4, byte 2, bit 0
SCT1	6[40]	Block 4, byte 3, bit 7	Block 4, byte 3, bit 2
SCT2	6	Block 4, byte 3, bit 1	Block 4, byte 4, bit 4
SCT3	6	Block 4, byte 4, bit 3	Block 4, byte 5, bit 6
SCT4	6	Block 4, byte 5, bit 5	Block 4, byte 5, bit 0
SCT5	6	Block 4, byte 6, bit 7	Block 4, byte 6, bit 2
SCT6	6	Block 4, byte 6, bit 1	Block 4, byte 7, bit 4
SCT7	6	Block 4, byte 7, bit 3	Block 4, byte 8, bit 6
SCT8	6	Block 4, byte 8, bit 5	Block 4, byte 8, bit 0
SCT9	6	Block 4, byte 9, bit 7	Block 4, byte 9, bit 2
SCT10	6	Block 4, byte 9, bit 1	Block 4, byte 10, bit 4
SCT11	6	Block 4, byte 10, bit 3	Block 4, byte 11, bit 6
SCT12	6	Block 4, byte 11, bit 5	Block 4, byte 11, bit 0
SCT13	6	Block 4, byte 12, bit 7	Block 4, byte 12, bit 2
SCT14	6	Block 4, byte 12, bit 1	Block 4, byte 13, bit 4
SCT15	6	Block 4, byte 13, bit 3	Block 4, byte 14, bit 6
SCT16	6	Block 4, byte 14, bit 5	Block 4, byte 14, bit 0
SCT17	6	Block 4, byte 15, bit 7	Block 4, byte 15, bit 2
SCT18	6	Block 4, byte 15, bit 1	Block 5, byte 0, bit 4
SCT19	6	Block 5, byte 0, bit 3	Block 5, byte 1, bit 6
SCT20	6	Block 5, byte 1, bit 5	Block 5, byte 1, bit 0
SCT21	6	Block 5, byte 2, bit 7	Block 5, byte 2, bit 2
SCT22	6	Block 5, byte 2, bit 1	Block 5, byte 3, bit 4

[40] The number of bits for the SCTx fields is equal to s#

SCT23	6	Block 5, byte 3, bit 3	Block 5, byte 4, bit 6
SCT24	6	Block 5, byte 4, bit 5	Block 5, byte 4, bit 0
SCT25	6	Block 5, byte 5, bit 7	Block 5, byte 5, bit 2
SCT26	6	Block 5, byte 5, bit 1	Block 5, byte 6, bit 4
SCT27	6	Block 5, byte 6, bit 3	Block 5, byte 7, bit 6
SCT28	6	Block 5, byte 7, bit 5	Block 5, byte 7, bit 0
SCT29	6	Block 5, byte 8, bit 7	Block 5, byte 8, bit 2
SCT30	6	Block 5, byte 8, bit 1	Block 5, byte 9, bit 4
SCT31	6	Block 5, byte 9, bit 3	Block 5, byte 10, bit 6
SCT32	6	Block 5, byte 10, bit 5	Block 5, byte 10, bit 0
SCT33	6	Block 5, byte 11, bit 7	Block 5, byte 11, bit 2
SCT34	6	Block 5, byte 11, bit 1	Block 5, byte 12, bit 4
SCT35	6	Block 5, byte 12, bit 3	Block 5, byte 13, bit 6
SCT36	6	Block 5, byte 13, bit 5	Block 5, byte 13, bit 0
SCT37	6	Block 5, byte 14, bit 7	Block 5, byte 14, bit 2
PAD	2	Block 5, byte 14, bit 1	Block 5, byte 14, bit 0
DIRS#	8	Block 5, byte 15, bit 7	Block 5, byte 15, bit 0
KID	4	Block 6, byte 0, bit 7	Block 6, byte 0, bit 4
INS#	4	Block 6, byte 0, bit 3	Block 6, byte 0, bit 0
ISAMID	32	Block 6, byte 1, bit 7	Block 6, byte 4, bit 0
Seal	64	Block 6, byte 5, bit 7	Block 6, byte 12, bit 0

4.5.1 DIRLength

This is RFU and shall contain a value of 0.

4.5.2 DIRFormatRevision

This shall contain a value of 1 (1 hex).

4.5.3 Sector Chain Table (SCT) usage

The relationship between the SCT entries and the physical storage on the media is done on a Sector-by-Sector basis. Each SCT Label corresponds to a Mifare® Sector on the media.

Each Sector in zone A contains 48 bytes of user-data storage. Each Sector in zone B contains 240 bytes of user-data storage

Each SCT entry shall contain a number in the range 0 to 39 (decimal). The following values shall have special significance as defined in ITSO TS 1000-2.

Note: As stated in section 4.4.1, S is 40 for this CMD.

Table 39 - Special SCT values

SCT entry value (decimal)	Significance
0	Corresponding Sector (see Table 40) is un-allocated and may be used to store product data.
'Self'[41]	Terminating Sector for product in question. Product is Virgin
38	Terminating Sector for product in question. Product is Blocked
39	Terminating Sector for product in question. Product is not Blocked

Table 40 defines the mapping between SCT Label and media Sectors. Sector numbers are as defined in the S70 Functional Specification.

[41] Where 'Self' means that the value in the entry corresponds to the entry's own number / Label. For example if SCT11 contains the value 11 (decimal) then this is a 'self' reference.

Table 40 - SCT Label vs. media Sector

SCT Label	Media Sector
SCT1	Sector 1
SCT2	Sector 17
SCT3	Sector 18
SCT4	Sector 19
SCT5	Sector 20
SCT6	Sector 21
SCT7	Sector 22
SCT8	Sector 23
SCT9	Sector 24
SCT10	Sector 32
SCT11	Sector 33
SCT12	Sector 34
SCT13	Sector 35
SCT14	Sector 2
SCT15	Sector 3
SCT16	Sector 4
SCT17	Sector 5
SCT18	Sector 6
SCT19	Sector 7
SCT20	Sector 8
SCT21	Sector 9
SCT22	Sector 10
SCT23	Sector 11
SCT24	Sector 12
SCT25	Sector 13
SCT26	Sector 14
SCT27	Sector 15
SCT28	Sector 25
SCT29	Sector 26
SCT30	Sector 27
SCT31	Sector 28
SCT32	Sector 29
SCT33	Sector 30
SCT34	Sector 31
SCT35	Sector 36
SCT36	Sector 37
SCT37	Sector 38

Note that the 37 Sectors listed above shall be used to store Data Elements associated with the following Data Groups:

— IPE

— Value Record

— Cyclic Log

As defined in ITSO TS 1000-2, SCT1 to SCT13 (shown shaded) have special significance, and are reserved as Starting Sectors.

Any Private Applications stored on the media shall also be located exclusively in the above 37 Sectors and/or in Sector 0.

4.5.4 PTYP usage for Private Applications

Where the data associated with a Directory Entry is a Private Application, the PTYP field within the Directory Entry may be proprietary to the (private) application.

4.6 Key usage

All Sectors shall use keys derived from the same master key pair.[42]

Read-only access to all Sectors shall be allowed by use of the A key. Key diversification shall not be employed for such access.

Note: This means that all Sectors of all platforms that conform to this CMD (FVC = 03) can be read by use of a single, non-diversified key.

Read-write access to all Sectors shall be allowed by use of the B key. Key diversification shall be employed for such access. The diversification mechanisms are defined in ITSO TS 1000-8.

For key diversification purposes, the following logical Sector numbers shall be used:

— ITSO Shell Logical Sector 0;

— Directory (copy A) Logical Sector S-2; (i.e. 38)

— Directory (copy B) Logical Sector S-1. (i.e. 39)

Note: On this CMD, both copies of the Directory reside in the same physical Sector. The keys used for this Sector shall be those provided for copy A (i.e. logical Sector 38).

Where the access key returned by the ISAM is longer than the 6 byte key required by this platform the key to be used shall consist of the last 6 bytes only. Thus for a key of value 0x123456789ABCDEF0 returned by the ISAM 0x56789ABCDEF0 shall be used as the access key for the CM.

4.7 Key strategy

This CMD shall use the Key Strategy Code (KSC) value as defined in clause 4.4.1. The ISAM shall use this to determine the appropriate cryptographic processes to be applied to such media platforms.

4.8 Access conditions

4.8.1 Sector 0, Block 0

This Block is always read-only and the access condition flag settings are ignored.

[42] Sectors containing ‘Private Applications’ which are marked as such in the ITSO Directory may use alternate key arrangements.

4.8.2 User-data Blocks

The access condition flags for all user-data Blocks on the media shall be set as follows, unless said Block is within a Sector that contains a Private Application: [43]

C1 = 1; C2 = 0; C3 = 0.

This setting has the effect of:

— Allowing read access with key A or key B.

— Allowing write access with key B.

— Not allowing the use of the increment command.

— Not allowing the use of the decrement command.

— Not allowing the use of the transfer command.

— Not allowing the use of the restore command.

4.8.3 Sector trailer Blocks

The access condition flags for all Sector-trailer Blocks (i.e. Block 3) on the media shall be set as follows, unless said Block is within a Sector that contains a Private Application: [44]

C1 = 0; C2 = 1; C3 = 1.

This setting has the effect of:

— Allowing key A to be written to if the Sector was opened with key B.

— Allowing key B to be written to if the Sector was opened with key B.

— Both the A and B keys on the Sector cannot be read.

— Allowing the access condition flags to be read if the Sector was opened with key A or key B.

— Allowing the access condition flags to be written to if the Sector was opened with key B.

4.9 Anti-tear

Software Anti-tear protection mechanisms as defined in Annex A shall be employed on the following Data Groups:

— Directory;

— Value Record;

— Cyclic Log;

[43] Blocks within sectors containing ‘Private Applications’ which are marked as such in the ITSO Directory may use alternate access condition arrangements

[44] Trailer Blocks within sectors containing ‘Private Applications’ which are marked as such in the ITSO Directory may use alternate access condition arrangements

4.10 Manufacturer's ID

All media conforming to this CMD contain a unique 4-byte manufacturer's serial number (UID) which is returned as part of the anti collision process and is also stored in bytes 0 to 3 of Block 0 of Sector 0. Either of these identical numbers shall be used wherever an ITSO MID is required (e.g. for security algorithms) and shall be mapped to the 8-byte ITSO MID as shown in Table 41.

The usage of this serial number when generating the 8-byte ITSO MID shall be as follows:

Table 41 - ITSO MID computation

ITSO MID byte	Contents
Byte 0 (MSB)	00 (hex)
Byte 1	00 (hex)
Byte 2	00 (hex)
Byte 3	00 (hex)
Byte 4	Block 0, byte 3
Byte 5	Block 0, byte 2
Byte 6	Block 0, byte 1
Byte 7 (LSB)	Block 0, byte 0

4.10.1 Verification of the serial number

POSTs shall verify that the serial number data in bytes 0 to 3 of Block 0 of Sector 0 corresponds to the UID that the media provided during the anti-collision process. This check shall always be carried out unless it can be proven that the POST only has access to either Block 0 of Sector 0 or the UID.

4.11 Detection of the ITSO Shell

The ITSO Shell detection sequence for this CMD shall be as follows:

— If a Mifare® standard 4K platform is detected[45], then the POST shall attempt to read Sector 16 with the non-diversified ITSO FVC = 03 A key[46].

— If Sector 16 can be opened for reading, then its contents shall be read and parsed as per section 4.4.

— A CRC shall be computed for the data read and checked against the SECRC field of the parsed data.

— If this check passes, then the POST shall assume that the platform carries a valid ITSO Shell.

— The POST shall read and confirm that all the Data Elements listed in Table 35 have the specified values. If this check passes then an ITSO Shell of FVC = 03 shall be deemed to be present.

[45] Refer to the Philips application note 'Type Identification Procedure' (m018411) for details of how to differentiate between the various Mifare® variants. Note that Philips makes proprietary use of certain bits in the SAK byte.

[46] Note that this key cannot be requested from the ISAM in the normal manner using the IIN, OID, FVC, KSC selection method, as these parameters are unknown at this stage. In effect the POST must hold this 'global' read key as a constant in its own memory.

4.12 Benchmark transaction

4.12.1 IPE with Transient Ticket Record creation

The benchmark transaction for this CMD shall comprise:

— Detection of a platform carrying a valid ITSO Shell with FVC = 03.

— Verification of the Directory, where there is no corruption on either Anti-tear copy.

— Verification of an IPE Data Group where there is only a single candidate product and the IPE Data Group resides in a single zone A Sector.

— Creation of a sealed 48-byte Transient Ticket Record.

— Update of the log entry and modification of the directory.

— Read after write verification of the updated Directory.

The target execution time for the above, subsequent to detection of the platform shall be, 300ms or less.

> Note: The target execution time includes all necessary POST application functions. (i.e. normal operation, Hotlist processing etc…).

4.12.2 IPE with Value Record Data Group modification

The benchmark transaction for this CMD shall comprise:

— Detection of a platform carrying a valid ITSO Shell with FVC = 03.

— Verification of the Directory, where there is no corruption on either Anti-tear copy.

— Verification of an IPE Data Group where there is only a single candidate product and the IPE Data Group resides in a single zone A Sector.

— Verification and modification of an associated Value Record Data Group where there is no corruption on either Anti-tear copy, and the Value Record Data Group resides in a single zone A Sector.

— Modification of the Directory to reflect the changes made to data group and product above.

— Read after write verification of the updated Directory.

The target execution time for the above, subsequent to detection of the platform, shall be 300ms or less.

Note: The target execution time includes all necessary POST application functions. (i.e. normal operation, Hotlist processing etc…)

4.13 List search method

This CMD supports a full ITSO Shell as defined in ITSO TS 1000-2. When a POST carries out a Hotlist or Actionlist search against a platform where FVC = 03, then it shall use ITSO Shell Referencing as defined in ITSO TS 1000-3.

5. Mifare ultra light

5.1 Scope

This clause defines the CMD for platforms based on the Philips Mifare® ultra light chip. Because of the very limited memory space available, this platform shall be limited to the hosting of a single Space Saving IPE (TYP 27, 28 or 29).

5.1.1 Terminology

Throughout this clause reference will be made to terms defined within the Philips Mifare® ultra light Contactless Single-trip Ticket IC MF0 IC U1 Functional Specification (January 2003).

5.2 Platform capability

5.2.1 General

This platform is capable of supporting a minimal set of Data Groups, as defined below:

— ITSO Shell Environment Compact Shell with implied IIN;

— Directory Single static IPE entry;

— IPE 1 instance only of a Space Saving IPE.

5.2.2 Memory architecture

The memory architecture of this platform is summarised below:

— 64 bytes of EEPROM, divided into 16 pages of 4 bytes each

  — 10 bytes are reserved for manufacturer data;

  — 2 bytes are reserved for access control settings;

  — 48 bytes are available for the general storage of user data;

  — 4 bytes are dedicated to one-time programmable usage with bit-level granularity.

5.2.3 Security provisions

The platform provides the following security-related features:

— A unique 7-byte manufacture’s serial number (MID);

— Ability to lock each 4-byte page of memory to a read-only state;

— Provision of 32 bits of One Time Programmable (OTP) memory, which can be atomically and irreversible changed from a 0 to a 1.

5.2.4 ISO/IEC 14443 compliance

All platforms covered by this CMD shall comply with the following parts of ISO/IEC 14443:

— part 2: RF power & signal interface Compliance with ISO/IEC 14443 Type A requirements;

— part 3: Initialisation & anticollision Compliance with ISO/IEC 14443 Type A requirements.

5.3 Format Version Code

Platforms that conform to this CMD shall use the Format Version Code (FVC) of 04.

5.4 ITSO Shell Environment Data Group location

This CMD uses a Compact ITSO Shell as defined in ITSO TS 1000-2.

The ITSO Shell Environment Data Group shall be located in page 6. The elements and layout of this data structure are fully defined in ITSO TS 1000-2.

5.4.1 Platform parameters with fixed values

The following platform parameter Data Elements within the ITSO Shell Environment Data Group shall have the fixed values specified herein for all implementations of this CMD.

Note that for the Compact Shell, only Data Elements shown shaded are actually stored on the media. The other Data Elements are implicit for the CMD and shall be generated by the POST where the data is required by the ISAM as defined in ITSO TS 1000-8.

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	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

5.4.1.1 Use of the ISRN Data Element

For this CMD the ISRN used as input to the ISAM in transaction messages, for computation of eISRN, and the ISRN used to populate uISRN, shall:

1. Be set to the concatenation of IIN, OID, ISSN and CHD as defined in clause 5.4.1above.

Or

2. Be set to all zeros

Case 1 above is recommended for use in new POST application developments.

5.4.2 Platform parameter with default values which may be overridden

This CMD does not support the overriding of platform parameter Data Element values.

5.4.3 ITSO Shell Environment detailed layout

Table 43 details the location of the Data Elements of the Data Group. Byte and bit numbers are as defined in the U1 Functional Specification.

Table 43 - ITSO Shell Environment Data Group

Data Element Label	# of bits	Start location	End location
ShellLength	6	Data8, bit 7	Data8, bit 2
ShellBitMap	6	Data8, bit 1	Data9, bit 4
ShellFormatRevision	4	Data9, bit 3	Data9, bit 0
FVC	8	Data10, bit 7	Data10, bit 0

5.5 Directory Data Group

This CMD does not support a full ITSO Directory Data Group. The only part of the Directory Data Group that is present is a single Directory Entry.

This Directory Entry shall be located in pages 6 to 7. Table 44 details the location of the Data Elements of the Data Group. Shading indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Table 44 - Directory Data Group

Data Element Label	# of bits	Start location	End location
E1	40	Data11, bit 7	Data15, bit 0

5.6 IPE data

This clause defines the mapping of the data content of Space Saving IPEs to this media. The data content consists of:

InstanceID

IPE static data

IPE dynamic data

Seal

5.6.1 InstanceID

A single instance of the Instance Identifier Data Structure as defined in ITSO TS 1000-2 shall be located in pages 8 and 9. Table 45 details the location of the Data Elements.

Table 45 – InstanceID

Data Structure Label	# of bits	Start location	End location
IPE Instance Identifier	64	Data16, bit 7	Data23, bit 0

5.6.2 IPE static data

This Structure shall contain the static Data Elements of the IPE as defined in ITSO TS 1000-5. It is limited to a single instance of 16 bytes in total and shall be located in pages 10-13 inclusive as detailed in Table 45a.

Table 45a –IPE static data

Data Structure Label	# of bits	Start location	End location
IPE Static Data	128	Data24, bit 7	Data39, bit 0

5.6.3 IPE dynamic data

A single instance of IPE dynamic data is present on this media which includes an area of one time programmable bits. It shall contain the dynamic Data Elements of the IPE as defined in ITSO TS 1000-5 and is limited to 12 bytes in total and shall be located in pages 3 – 5 inclusive as detailed in Table 45b.

Table 45b –IPE dynamic data

Data Structure Label	# of bits	Start location	End location
IPE Dynamic Data	64	Data0, bit 7	Data7, bit 0
IPE Dynamic Data	32	OTP0, bit 7	OTP3, bit 0

Note: Each bit in Page 3 of this CMD is one time programmable (OTP) and shall be used to store data that is:

either

- normally fixed upon product creation for the life of the IPE

or

- be set from logic 0 to logic 1 in turn by the application

See annex C for an example of use of the OTP area

5.6.4 Seal

A single instance of the Seal is present on this media as defined in ITSO TS 1000-2 and is limited to 8 bytes in total. It shall be defined as the IPE Static & Dynamic Data Seal and shall be located in pages 14 and 15 as detailed in Table 45c.

Table 45c – Seal

Data Element Label	# of bits	Start location	End location
Static and Dynamic Data Seal	64	Data40, bit 7	Data47, bit 0

5.6.4.1 Seal computation

The value of the Seal is calculated in accordance with ITSO TS1000-8 and covers data elements and structures concatenated together in the order shown in Table 45d.

Table 45d Data covered by the Seal

Element or structure	# of bytes	As defined in
Directory Data Group	5	Clause 5.5
IPE static Data	16	Clause 5.6.2
IPE dynamic Data	12	Clause 5.6.3
InstanceID	8	Clause 5.6.1

5.7 Overall mapping

The mapping of the Data Structures, defined in clauses 5.4 – 5.6 above, to the CMD 4 platform is illustrated in Table 46.

The mifare® Ultralite pages available for Space Saving IPEs when installed on a CMD 4 platform are shown in column 1. Column 2 shows which pages are to be locked against further changes after being populated for the first time.

Table 46 – Overall Map

Page/Byte	Status after creation	0	1	2	3
Page 3		OTP area			
Page 4		IPE Dynamic Data			
Page 5					
Page 6	**Locked**	Shell			
Page 7	**Locked**	Directory			
Page 8	**Locked**	InstanceID			
Page 9	**Locked**				
Page 10	**Locked**	IPE Static Data			
Page 11	**Locked**				
Page 12	**Locked**				
Page 13	**Locked**				
Page 14		Static & Dynamic Data Seal			
Page 15					

5.8 Key usage

The platform defined by this CMD does not provide for key-based access control. As such, all pages of the media shall have unconditional read access.

All pages that have not been locked shall have unconditional write access (see section 5.10).

5.9 Key strategy

This CMD shall use the Key Strategy Code (KSC) value as defined in clause 5.4.1. The ISAM shall use this to determine the appropriate cryptographic processes to be applied to such media.

5.10 Access conditions

The platform allows each page to be configured as read-only. This configuration is via the lock bits and is a one-way process (i.e. once a page is made read-only, it cannot be re-configured back to read-write).

5.10.1 Delivered conditions

By default, the following pages are read-only when the media is delivered from the manufacturer:

— Page 0 UID and BCC0

— Page 1 UID;

— Page 2 (bytes 0 and 1) BCC1 and reserved.

5.10.2 Post-issue conditions

After the ITSO Shell Environment, Directory and IPE Data Groups have been loaded onto the media, the following pages shall be configured as read-only:

— Pages 6 and 7 ITSO Shell Environment and Directory;

— Pages 8 and 9 IPE Instance Identifier;

— Pages 10 to 13 inclusive IPE static Data Elements;

5.11 Anti-tear

Anti-tear protection is not provided on the following data areas, which shall all be static and read-only after the Space Saving IPE has been created:

— the ITSO Shell Environment Data Group;

— the Directory Data Group;

— the static portion of the IPE.

Note:

Certain Data Elements in the IPE Dynamic Data shall make use of the native hardware Anti-tear protection, provided by the one time programmable area as defined for the space saving IPEs in ITSO TS1000 part 5. A write to one of these bits is guaranteed to either be successful (i.e. convert a 0 to a 1) or to have no effect (i.e. leave the bit as it was).

No form of Anti-tear protection is used on the remaining Dynamic Data. The Seal allows corruption to be detected.

For this Customer Media the one time programmable bit map of n bits shall have n = 32.

In use bits shall be set from 0 to 1 in the following order:

The first bit to be set shall be OTP3, bit 0 followed by OTP3, bit 1 then in order through OTP2, bit0; OTP2, bit 1 … until the 32nd bit to be set which shall be OTP0, bit7Note:

Because of the limitations of the anti-tear mechanisation the following constraints apply to the use of this customer media:

1. Data Elements that change during use and are not within the OTP area may contain data that can be detected as unreliable but is not recoverable to its previous value.

2. Incremental Data Elements mechanised within the OTP area can be considered as recoverable.

3. Data Elements not in the OTP area that have a backup copy stored in the OTP area may be recovered but only to a limited accuracy for scaling factors > 1.

5.12 Manufacturer’s ID

All media conforming to this CMD contain a 7-byte manufacturer’s serial number in pages 0 and 1. This shall be used wherever a MID is required (e.g. for security algorithms).

The usage of this serial number when generating the 8-byte ITSO MID shall be as follows:

Table 47 - MID computation

MID byte	Contents
Byte 0 (MSB)	00 (hex)
Byte 1	SN0
Byte 2	SN1
Byte 3	SN2
Byte 4	SN3
Byte 5	SN4
Byte 6	SN5
Byte 7 (LSB)	SN6

5.12.1 Verification of the serial number

POSTs shall verify that the serial number data in pages 0 and 1 corresponds to the UID (or part thereof) that the media provided during the anti-collision loop process. This check shall always be carried out unless it can be proven that the POST does not have access to said UID data.

5.13 Detection of the ITSO Shell

The ITSO Shell detection sequence for this CMD shall be as follows:

— If a Mifare® ultra light platform is detected[47], then the POST shall read page 6.

— The POST shall read and confirm that all the highlighted Data Elements listed in Table 42 have the specified values. If this check passes then an ITSO Shell of FVC = 04 shall be deemed to be present.

5.14 Benchmark transaction

The benchmark transaction for this CMD shall comprise:

— Detection of a platform carrying a valid ITSO Shell with FVC = 04

— Verification of a Space Saving IPE Data Group

— Modification of IPE Dynamic Data.

— Read after write verification of the updated dynamic data

The target execution time for the above subsequent to detection of the platform shall be 200ms or less.

> Note: The target execution time includes all necessary POST application functions. (i.e. normal operation, Hotlist processing etc…).

5.15 List search method

This CMD only supports a Compact ITSO Shell as defined in ITSO TS 1000-2. When a POST carries out a Hotlist or Actionlist search against a platform where FVC = 04, then it shall use IPE Referencing as defined in ITSO TS 1000-3.

---

[47] Refer to the Philips application note ‘Type Identification Procedure’ (m018411) for details of how to differentiate between the various Mifare® variants. Note that Philips makes proprietary use of certain bits in the SAK byte.

5.16 IPE blocking

Typically products on this CMD are limited to a short life only and as such hot listing and marking the product as blocked is unlikely to be required.

However in the event that it is required to mark a product as blocked, where possible the SEAL shall be set to all zeros.

6. CMD5 - RFU

7. CMD6 - RFU

8. mifare® DESFire

8.1 Scope

This clause defines the CMD for platforms based on media platforms that comply with revision 3.1 of the Philips mifare® DESFire specification.

8.1.1 Terminology

Throughout this clause reference will be made to terms defined within revision 3.1 of the mifare® DES*Fire* specification for the MF3 IC D40 IC.

8.2 Platform capability

8.2.1 General

This platform is capable of supporting a full set of ITSO Data Groups as defined below:

— Shell Environment With all optional elements present

— Directory

— IPE

— Value Record May be associated with IPEs subject to overall memory limits

— Cyclic Log Support for Basic and Normal mode logging

For this CMD the ITSO cyclic log shall always be present and sited in logical sector 14. Directory Entry number 8 shall be reserved exclusively for a normal log entry and point implicitly to logical sector 14.

Note: this implicit selection replaces the normal rule for most CMD's whereby Directory Entry 8 would point to a logical start sector number = 8.

This specification defines a set of default parameters for this CMD that control the size of storage and the number of products stored. Shell Owners may use alternate parameter values to those specified herein. POSTs shall be able to process media with alternate parameter values. See sections 8.7.3.4, 8.7.4.4 and 8.7.5.4 for further details.

The default parameters define a memory structure that will support:

— 8 Directory entries

— 14 sectors (files) for IPE instance, Value Record and Cyclic Log storage

8.2.2 Memory architecture

The memory architecture of this platform is summarised below:

— Total platform capacity is 4096 bytes of non-volatile data storage.

— Up to 28 applications may be hosted

— Data storage is file-based

— Each application can have up to 16 files

— By default, the ITSO application will use 1760 bytes of non-volatile data storage

  — 160 bytes are used for the ITSO Shell Environment and Directory Data Group storage

- 1216 bytes are available for IPE instance and Value Record storage
- 384 bytes are available for Cyclic Log storage

— 5 types of file are supported by the platform. The types used by ITSO are indicated.

- Standard Data Files (Used by ITSO for static data storage)
- Backup Data Files (Used by ITSO for dynamic data storage)
- Value Files with Backup
- Linear Record Files with Backup
- Cyclic Record Files with Backup

8.2.3 Security provisions

The platform provides the following security-related features:

— A unique 7-byte manufacture's serial number (MID)

— Support for mutual 3-pass authentication

— Support for plain, MACed and enciphered air communication between POST and media (using DES/3DES).

— Support for up to 14 keys to control access to storage files

— Support for native Anti-tear protection.

8.2.4 Application Family Identifier usage

ISO/IEC 14443-3 provides for support of an Application Family Identifier (AFI) pre-selection mechanism.

ITSO does not mandate the use of AFI coding, although where the platform supports such coding and only the ITSO application is present, then use of the Transport Family code (10 hex) is recommended.

POSTs shall not assume that media uses AFI coding, and shall default to using the Select All code of 00 (hex).

8.2.5 ISO/IEC 14443 compliance

All platforms covered by this CMD shall comply with the following parts of ISO/IEC 14443:

— Part 2: RF power & signal interface Compliance with ISO/IEC 14443 Type A requirements

— Part 3: Initialisation & anticollision Compliance with ISO/IEC 14443 Type A requirements

— Part 4: Transmission protocol Compliance with ISO/IEC 14443 Type A requirements

8.3 Format Version Code

Platforms that conform to this CMD shall use the Format Version Code (FVC) of 07.

8.4 Command set

The following commands shall be supported.[48]. The command codes are shown in hex.

— SelectApplication (command code = 5A)

— GetFileSettings (command code = F5)

— Authenticate (command code = 0A)

— ReadData (command code = BD)

— WriteData (command code = 3D)

— CommitTransaction (command code = C7)

The detailed usage of these commands will be defined in subsequent sections of this document.

8.5 Authentication

Mutual authentication shall be used before any updates are carried out to data stored on the media. This shall be done by use of the Authenticate command. See section 8.9.1, ITSO TS 1000-7 and ITSO TS 1000-8 for further details.

8.5.1 Authentication keys

Authentication shall be carried out using the key number appropriate to the file that is to be accessed. This will be the Key number as defined in Table 60.

8.5.2 Command sequence

The POST to media mutual authentication sequence (including the command sequences to/from the ISAM) is fully detailed in ITSO TS 1000-7 and ITSO TS 1000-8.

8.6 Secure messaging

The default data transmission between the POST and the media shall be plain data transfer.

If a mutual authentication session has been successfully completed, then a DES/3DES MAC will secure the plain data transfer. This MAC shall be generated / validated by the ISAM (see ITSO TS 1000-7 and ITSO TS 1000-8).

Encrypted messaging between POST and media is not used for this CMD.

8.7 File system structure

Table 60 details the structure of the default ITSO file system. Unless otherwise stated, all numbers are in decimal.

[48] These commands are the ones required during normal usage of the platform. They do not include the commands required for the creation of the ITSO application on the platform.

Table 60 - Default file system

Logical Sector	FID	File type	Size (bytes)	Key number (Read; Write)	Usage	Comms mode (see note below)	Access rights (MSB; LSB)
15	0	Backup data file	64	14; 1	Directory	Plain; MACed	E1; 1F (hex)
14	1	Backup data file	4*48	14; 1	Cyclic Log storage	Plain; MACed	E1; 1F (hex)
13	2	Backup data file	64	14; 1	IPE Fixed or Value DG	Plain; MACed	E1; 1F (hex)
12	3	Backup data file	64	14; 1	IPE Fixed or Value DG	Plain; MACed	E1; 1F (hex)
11	4	Backup data file	64	14; 1	IPE Fixed or Value DG	Plain; MACed	E1; 1F (hex)
10	5	Backup data file	64	14; 1	IPE Fixed or Value DG	Plain; MACed	E1; 1F (hex)
9	6	Backup data file	64	14; 1	IPE Fixed or Value DG	Plain; MACed	E1; 1F (hex)
8	7	Backup data file	64	14; 1	IPE Fixed or Value DG	Plain; MACed	E1; 1F (hex)
7	8	Standard data file	64	14; 1	IPE Fixed DG	Plain; MACed	E1; 1F (hex)
6	9	Standard data file	64	14; 1	IPE Fixed DG	Plain; MACed	E1; 1F (hex)
5	10	Standard data file	64	14; 1	IPE Fixed DG	Plain; MACed	E1; 1F (hex)
4	11	Standard data file	64	14; 1	IPE Fixed DG	Plain; MACed	E1; 1F (hex)
3	12	Standard data file	64	14; 1	IPE Fixed DG	Plain; MACed	E1; 1F (hex)
2	13	Standard data file	64	14; 1	IPE Fixed DG	Plain; MACed	E1; 1F (hex)
1	14	Standard data file	64	14; 1	IPE Fixed DG	Plain; MACed	E1; 1F (hex)
0	15	Standard data file	32	14; 0	Shell	Plain	E0; 0F (hex)

Note on communications mode:

The DESFire specification states that if one of the access keys for a file is 14, then communication is covered by a Message Authentication Code (MAC) and or enciphered in the case of a valid authentication or in the case of no valid authentication communication takes place in the clear without a MAC.

8.7.1 ITSO Shell Environment file

This file contains the ITSO Shell Environment Data Group. This file shall have the following attributes.

8.7.1.1 File number

This file shall have a file number (FID) of 15 (0F hex).

8.7.1.2 Access conditions

Creation - At personalisation only

Update - Not allowed

Read - Unconditional

Delete - Not allowed

8.7.1.3 File structure

This file shall be a Standard Data type. The size of the file shall be 32 bytes.

8.7.1.4 Shell Environment Data Group

The Shell Environment Data Group shall be stored in this file. The elements and layout of this data structure are fully defined in ITSO TS 1000-2.

8.7.1.4.1 Platform parameters with fixed values

The following platform parameter data elements within the Shell Environment Data Group shall have the fixed values specified herein for all implementations of this CMD.

Table 61 - Fixed platform parameter values

Data element	Default value	Comment
ShellLength	6 8	If the optional MCRN is not present If the optional MCRN is present
ShellBitMap	msb-000001-lsb msb-000011-lsb	If the optional MCRN is not present If the optional MCRN is present
ShellFormatRevision	1	For this version of the specification
FVC	7	See section 8.3

8.7.1.4.2 Platform parameters with default values which may be overridden

The following platform parameter data elements within the Shell Environment Data Group shall have (explicit) default values as listed below. However, Shell Owners may override these defaults by specifying an alternative value within the associated data field of the Shell Environment Data Group at the time of Shell creation.

POSTs shall correctly parse and use the parameter values provided by the platform.

Table 62 - Default data element values

Data element	Default value	Comment
KSC	4	For this version of the specification
B	64 (40 hex)	Size of logical storage sector.
S	16 (10 hex)	This gives a Ψ of 4
E	8	Number of Directory Entries
SCTL	7	Length of Sector Chain Table

8.7.1.4.3 Shell Environment detailed layout

Table details the location of the data elements when the default platform parameter values are used. Shading indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Table 63 - Default Shell Environment data content - No MCRN present

Data element label	# of bits	Start location	End location
ShellLength	6	Byte 0, bit 7	Byte 0, bit 2
ShellBitMap	6	Byte 0, bit 1	Byte 1, bit 4
ShellFormatRevision	4	Byte 1, bit 3	Byte 1, bit 0
IIN	24	Byte 2, bit 7	Byte 4, bit 0
OID	16	Byte 5, bit 7	Byte 6, bit 0
ISSN	28	Byte 7, bit 7	Byte 10, bit 4
CHD	4	Byte 10, bit 3	Byte 10, bit 0
FVC	8	Byte 11, bit 7	Byte 11, bit 0
KSC	8	Byte 12, bit 7	Byte 12, bit 0
KVC	8	Byte 13, bit 7	Byte 13, bit 0
RFU	2	Byte 14, bit 7	Byte 14, bit 6
EXP	14	Byte 14, bit 5	Byte 15, bit 0
B	8	Byte 16, bit 7	Byte 16, bit 0
S	8	Byte 17, bit 7	Byte 17, bit 0
E	8	Byte 18, bit 7	Byte 18, bit 0
SCTL	8	Byte 19, bit 7	Byte 19, bit 0
PAD	16	Byte 20, bit 7	Byte 21, bit 0
SECRC	16	Byte 22, bit 7	Byte 23, bit 0

Table 63a - Default Shell Environment data content - MCRN present

Data element label	# of bits	Start location	End location
ShellLength	6	Byte 0, bit 7	Byte 0, bit 2
ShellBitMap	6	Byte 0, bit 1	Byte 1, bit 4
ShellFormatRevision	4	Byte 1, bit 3	Byte 1, bit 0
IIN	24	Byte 2, bit 7	Byte 4, bit 0
OID	16	Byte 5, bit 7	Byte 6, bit 0
ISSN	28	Byte 7, bit 7	Byte 10, bit 4
CHD	4	Byte 10, bit 3	Byte 10, bit 0
FVC	8	Byte 11, bit 7	Byte 11, bit 0
KSC	8	Byte 12, bit 7	Byte 12, bit 0
KVC	8	Byte 13, bit 7	Byte 13, bit 0
RFU	2	Byte 14, bit 7	Byte 14, bit 6
EXP	14	Byte 14, bit 5	Byte 15, bit 0
B	8	Byte 16, bit 7	Byte 16, bit 0
S	8	Byte 17, bit 7	Byte 17, bit 0
E	8	Byte 18, bit 7	Byte 18, bit 0
SCTL	8	Byte 19, bit 7	Byte 19, bit 0
MCRN	80	Byte 20, bit 7	Byte 29, bit 0
SECRC	16	Byte 30, bit 7	Byte 31, bit 0

8.7.2 Directory file

This file contains the ITSO Directory Data Group. This file shall have the following attributes.

8.7.2.1 File number

This file shall have a file number (FID) of 0.

8.7.2.2 Access conditions

Creation	- At personalisation only
Update	- Allowed, subject to valid mutual authentication with correct access key
Read	- Unconditional
Delete	- Not allowed

8.7.2.3 File structure

This file shall be a Backup Data type. The size of the file shall be 64 bytes.

8.7.2.4 Directory Data Group location

Table 64 details the location of the data elements for each copy when the default platform parameter values are used. Shading indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Table 64 - Directory Data Group

Data element label	# of bits	Start location	End location
DIRLength	6	Byte 0, bit 7	Byte 0, bit 2
DIRBitMap	6	Byte 0, bit 1	Byte 1, bit 4
DIRFormatRevision	4	Byte 1, bit 3	Byte 1, bit 0
E1	40	Byte 2, bit 7	Byte 6, bit 0
E2	40	Byte 7, bit 7	Byte 11, bit 0
E3	40	Byte 12, bit 7	Byte 16, bit 0
E4	40	Byte 17, bit 7	Byte 21, bit 0
E5	40	Byte 22, bit 7	Byte 26, bit 0
E6	40	Byte 27, bit 7	Byte 31, bit 0
E7	40	Byte 32, bit 7	Byte 36, bit 0
E8	40	Byte 37, bit 7	Byte 41, bit 0
SCT1	4 [49]	Byte 42, bit 7	Byte 42, bit 4
SCT2	4	Byte 42, bit 3	Byte 42, bit 0
SCT3	4	Byte 43, bit 7	Byte 43, bit 4
SCT4	4	Byte 43, bit 3	Byte 43, bit 0
SCT5	4	Byte 44, bit 7	Byte 44, bit 4
SCT6	4	Byte 44, bit 3	Byte 44, bit 0
SCT7	4	Byte 45, bit 7	Byte 45, bit 4
SCT8	4	Byte 45, bit 3	Byte 45, bit 0
SCT9	4	Byte 46, bit 7	Byte 46, bit 4
SCT10	4	Byte 46, bit 3	Byte 46, bit 0
SCT11	4	Byte 47, bit 7	Byte 47, bit 4
SCT12	4	Byte 47, bit 3	Byte 47, bit 0
SCT13	4	Byte 48, bit 7	Byte 48, bit 4
PAD	4	Byte 48, bit 3	Byte 48, bit 0
DIRS#	8	Byte 49, bit 7	Byte 49, bit 0
KID	4	Byte 50, bit 7	Byte 50, bit 4
INS#	4	Byte 50, bit 3	Byte 50, bit 0
ISAMID	32	Byte 51, bit 7	Byte 54, bit 0
Seal	64	Byte 55, bit 7	Byte 62, bit 0

8.7.2.4.1 DIRLength

This is RFU and shall contain a value of 0.

8.7.2.4.2 DIRFormatRevision

This shall contain a value of 1 (1 hex).

[49] The number of bits for the SCTx fields is equal to Ψ

8.7.2.4.3 Sector Chain Table (SCT) usage

The relationship between the Sector Chain Table entries and the physical storage on the platform is done on a sector-to-EF basis. Each SCT label corresponds to a file on the platform.

When the default platform parameters are used then each SCT entry shall contain a number in the range 0 to 15 (decimal). The following values shall have special significance as defined in ITSO TS 1000-2.

Note: As stated in section 8.7.1.4.2, the default value of Ψ is 4 for this CMD. If an alternate Ψ is used, then the above value ranges and the latter two special SCT values in the table below shall be adjusted accordingly (as defined in ITSO TS 1000-2).

Table 65 - Special SCT values

SCT entry value (decimal)	Significance
0	Corresponding sector / file is un-allocated and may be used to store product data.
'Self'[50]	Terminating sector / file for product in question. Product is Virgin
14	Terminating sector / file for product in question. Product is Blocked
15	Terminating sector / file for product in question. Product is not Blocked

Table 66 defines the mapping between SCT label and the file number.

Table 66 - SCT label vs. file number

SCT label	File number
SCT1	14
SCT2	13
SCT3	12
SCT4	11
SCT5	10
SCT6	9
SCT7	8
SCT8	7
SCT9	6
SCT10	5
SCT11	4
SCT12	3
SCT13	2

Note that the 13 files listed above shall be used to store data elements associated with the following Data Groups:

— IPE

[50] Where 'Self' means that the value in the entry corresponds to the entry's own number / label. For example if SCT11 contains the value 11 (decimal) then this is a 'self' reference.

— Value Record

— Cyclic Log

As defined in ITSO TS 1000-2, sectors SCT1 to SCT(E[51]-1) (shown shaded) have special significance, and are reserved as Starting Sectors.

Any Private Applications stored within the ITSO application shall be located exclusively in the above 13 files.

8.7.2.4.4 PTYP usage for Private Applications

Where the data associated with a Directory Entry is a Private Application, the PTYP field within the Directory Entry may be proprietary to the (private) application.

8.7.3 IPE storage files

By default the platform shall contain 7 files that can only be used to store static IPE Data Groups. These files are used to store static IPE Data Group data.

These files shall have the following attributes.

8.7.3.1 File number

These files shall each have a unique file number (FID). The FID range shall be 8 to 14.

8.7.3.2 Access conditions

Creation	- At personalisation only
Update	- Allowed, subject to valid mutual authentication with correct access key
Read	- Unconditional
Delete	- Not allowed

8.7.3.3 File structure

These files shall be of type Standard Data File. The default size of each file shall be 64 bytes.

8.7.3.4 Options

The Shell Issuer may elect to use a non-default file size for IPE and Value Record files. The selected value shall be stored in the ‘B’ field within the Shell Data Group.

The file size for IPE and Value Record files shall always be equal.

Note: The MF3 IC D40 internally allocates non-volatile memory in multiples of 32 bytes. It is recommended that the value of ‘B’ is a multiple of 32.

8.7.4 Value Record storage files

By default the platform shall contain 6 files that can be used to store static IPE Data Groups or Value Record Data Groups. These files are used to store Value Record Data Groups.

These files shall have the following attributes.

8.7.4.1 File number

These files shall each have a unique file number (FID).The FID range shall be 2 to 7.

---

[51] Default value of E is 8

8.7.4.2 Access conditions

Creation	- At personalisation only
Update	- Allowed, subject to valid mutual authentication with correct access key
Read	- Unconditional
Delete	- Not allowed

8.7.4.3 File structure

These files shall be of type Backup Data File. The default size of each file shall be 64 bytes.

8.7.4.4 Options

The Shell Issuer may elect to use a non-default file size for IPE and Value Record files. The selected value shall be stored in the 'B' field within the Shell Data Group.

The file size for IPE and Value Record files shall always be equal.

Note: The MF3 IC D40 internally allocates non-volatile memory in multiples of 32 bytes. It is recommended that the value of 'B' is a multiple of 32.

8.7.5 Cyclic Log storage files

By default the platform shall contain 1 instance of this file, which shall be used to store the Cyclic Log.

The file shall have the following attributes.

8.7.5.1 File number

This file shall have a file number (FID) of 1.

8.7.5.2 Access conditions

Creation	- At personalisation only
Update	- Allowed, subject to valid mutual authentication with correct access key
Read	- Unconditional
Delete	- Not allowed

8.7.5.3 File structure

This file shall be of type Backup Data File. The default size of the file shall be 192 bytes, equating to 4 Transient Ticket records of 48 bytes each.

8.7.5.4 Options

The Shell Issuer may elect to use a Cyclic Log with non-default number of records.

To support the above, all POSTs shall issue the GetFileSettings command against file number 1 prior to attempting to use the Cyclic Log (see section 8.14.1).

8.8 ITSO application selection

The ITSO application shall be selected by use of the SelectApplication command. The data field of this command shall be the ITSO Application Identifier (AID).

8.8.1 ITSO AID

The DESFire platform does not support an AID that is formatted in accordance with ISO/IEC 7816-5:1994. Only 3 bytes are available for coding of the AID, as opposed to the 6 to 16 bytes required by ISO/IEC 7816-5:1994 for a registration category 'A' AID[52].

The ITSO AID in accordance with ISO/IEC 7816-5:1994 is made up of:

— Registered Application Provider Identifier (RID) for ITSO 5 bytes

— Proprietary Application Identifier Extension (PIX) 6 bytes

The international RID assigned to ITSO is (in hex): A0, 00, 00, 02, 16

A sub-set of the international RID shall be used to generate the 3-byte AID for this platform.

8.8.2 SelectApplication

8.8.2.1 Command pre-conditions

None. The POST may issue this command at any time. This command must be used to select the ITSO application on the media. It would not normally be required to be issued again during a session.

8.8.2.2 Command parameters

The table below defines the parameters required for the SelectApplication command for the ITSO application.

Note: The byte order in which the AID is presented to the card is reversed from the normal conventions used in this specification but is the order specified in the DESfire specification.

Table 67 - SelectApplication command

Byte offset	Label	Value (hex)	Description
0	Cmd	5A	
1	Data	16	AID
2	Data	02	AID
3	Data	A0	AID

8.8.2.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.8.2.4 Response data

There is no response data for the SelectApplication command.

[52] Which ITSO is

8.9 Mutual authentication and session communications

If a transaction requires an update to any of the contents of files within the ITSO application area, then a secured session shall be established between the media and the POST. This shall be done by the use of mutual authentication.

8.9.1 Authenticate

8.9.1.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

8.9.1.2 Command parameters

The table below defines the parameters required for the Authenticate command. The key number shall be the appropriate key for the file that is to be modified.

Note: It is not possible to have more than one secured session active at any given time. If a transaction requires the update of files that use different keys, then after the first file update has been carried out, a second secured session must be started with a new Authenticate command using the other key.

Table 68 - Authenticate command

Byte offset	Label	Value (hex)	Description
0	Cmd	0A	
1	Data	??	Key number

8.9.1.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.9.1.4 Response data

The response to the Authenticate command is an Additional Frame containing an 8-byte field. This field shall contain an encrypted 8-byte random number, using the key number passed in the command.

8.9.1.5 Additional frame

In response to the Additional Frame response from the media, the POST shall generate a further Additional Frame as defined in the mifare® DESFire specification and send this to the media. The media will reply to this Additional Frame with a final response and data. See ITSO TS 1000-7 and ITSO TS 1000-8 for further details.

8.10 Shell access

The file containing the ITSO Shell shall be accessed by use of the ReadData command.

Read access to this file is unconditional, and can be done at any time, subject to the ITSO application being selected.

Update access to this file is not allowed.

8.10.1 ReadData

8.10.1.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

8.10.1.2 Command parameters

The table below defines the parameters required for the ReadData command.[53]

Table 69 - ReadData command

Byte offset	Label	Value (hex)	Description
0	Cmd	BD	
1	Data	0F	File number
2	Data	00	Offset (LSB)
3	Data	00	Offset .
4	Data	00	Offset (MSB)
5	Data	00	Length (LSB) - No length specified, read entire file
6	Data	00	Length .
7	Data	00	Length (MSB)

8.10.1.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.10.1.4 Response data

The response to the ReadData command for the entire Shell file will be a:

— 32-byte frame of data; if a valid mutual authentication session has not taken place; OR

— 32-byte frame of data followed by a 4-byte MAC; if a valid mutual authentication session has taken place.

8.11 Directory access

The Directory shall be accessed by use of the ReadData and WriteData commands.

Read access to this file is unconditional, and can be done at any time, subject to the ITSO application being selected.

Update access to this file shall require a valid mutual authentication session to have taken place.

Updates to this file shall require the use of the CommitTransaction command.

[53] Showing the read of the entire Shell

8.11.1 ReadData

8.11.1.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

Whilst not essential, it is strongly recommended that a valid mutual authentication has taken place and a secure session is in progress. This will result in a MAC been applied to the data read, thus increasing the security of the transfer.

8.11.1.2 Command parameters

The table below defines the parameters required for the ReadData command.[54]

Table 70 - ReadData command

Byte offset	Label	Value (hex)	Description
0	Cmd	BD	
1	Data	00	File number
2	Data	00	Offset (LSB)
3	Data	00	Offset .
4	Data	00	Offset (MSB)
5	Data	00	Length (LSB) - No length specified, read entire file
6	Data	00	Length .
7	Data	00	Length (MSB)

8.11.1.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.11.1.4 Response data

The response to the ReadData command for the entire Directory file will consist of 2 data frames[55], which when concatenated will result in a:

— 64-byte block of data; if a valid mutual authentication session has not taken place; OR

— 64-byte block of data followed by a 4-byte MAC; if a valid mutual authentication session has taken place.

[54] Showing the read of the entire Directory

[55] A data frame can hold up to 59 bytes. See the mifare® DESFire specification for further details

8.11.2 WriteData

8.11.2.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

A valid mutual authentication must have taken place and a secure session must be in progress.

8.11.2.2 Command parameters

The table below defines the parameters required for the WriteData command and its associated Additional Frame which is required if full update of the Directory is required.

Note: The Directory is structured to allow partial updates to be used for most transactions. It is recommended that POSTs make use of this capability to improve transaction speed.

Table 71 - WriteData command

Byte offset	Label	Value (hex)	Description
0	Cmd	3D	
1	Data	00	File number
2	Data	00	Offset (LSB)
3	Data	00	Offset .
4	Data	00	Offset (MSB)
5	Data	40	Length (LSB)
6	Data	00	Length .
7	Data	00	Length (MSB)
8	Data	??	Data to be written
.	Data	??	Data to be written
59	Data	??	Data to be written

Table 71a - WriteData Additional Frame

Byte offset	Label	Value (hex)	Description
0		AF	Additional Frame tag
1	Data	??	Data to be written
.	Data	??	Data to be written
12	Data	??	Data to be written
13	MAC	??	MAC of data to be written
14	MAC	??	MAC of data to be written
15	MAC	??	MAC of data to be written
16	MAC	??	MAC of data to be written
17	Padding	00	Padding to make entire data string a multiple of 8 bytes
18	Padding	00	Padding to make entire data string a multiple of 8 bytes
19	Padding	00	Padding to make entire data string a multiple of 8 bytes
20	Padding	00	Padding to make entire data string a multiple of 8 bytes

8.11.2.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.11.2.4 Response data

There is no response data for the WriteData command.

8.11.3 CommitTransaction

This command validates and commits all write operations that have been made to Backup files within the selected application. Failure to issue this command after an update to a Backup file will result in the loss of the update (i.e. the file will remain unchanged).

8.11.3.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

A valid mutual authentication must have taken place and a secure session must be in progress.

8.11.3.2 Command parameters

The table below defines the parameters required for the CommitTransaction command.

Table 72 - CommitTransaction command

Byte offset	Label	Value (hex)	Description
0	Cmd	C7	

8.11.3.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.11.3.4 Response data

There is no response data for the CommitTransaction command.

8.12 IPE access

The IPE Data Groups shall be accessed by use of the ReadData and WriteData commands.

Read access to these files is unconditional, and can be done at any time, subject to the ITSO application being selected.

Update access to these files shall require a valid mutual authentication session to have taken place.

8.12.1 ReadData

8.12.1.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

Whilst not essential, it is strongly recommended that a valid mutual authentication has taken place and a secure session is in progress. This will result in a MAC been applied to the data read, thus increasing the security of the transfer.

8.12.1.2 Command parameters

The table below defines the parameters required for the ReadData command.[56]

Table 73 - ReadData command

Byte offset	Label	Value (hex)	Description
0	Cmd	BD	
1	Data	08 to 0E	File number required
2	Data	00	Offset (LSB)
3	Data	00	Offset .
4	Data	00	Offset (MSB)
5	Data	00	Length (LSB) - No length specified, read entire file
6	Data	00	Length .
7	Data	00	Length (MSB)

8.12.1.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.12.1.4 Response data

The response to the ReadData command for the entire IPE file will consist of 2 data frames[57], which when concatenated will result in a:

— 64-byte block of data; if a valid mutual authentication session has not taken place; OR

— 64-byte block of data followed by a 4-byte MAC; if a valid mutual authentication session has taken place.

[56] Showing the read of the entire IPE file

[57] A data frame can hold up to 59 bytes. See the mifare® DESFire specification for further details

8.12.2 WriteData

8.12.2.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

A valid mutual authentication must have taken place and a secure session must be in progress.

8.12.2.2 Command parameters

The table below defines the parameters required for the WriteData command and its associated Additional Frame which is required if full update of the IPE file is required.

Table 74 - WriteData command

Byte offset	Label	Value (hex)	Description
0	Cmd	3D	
1	Data	08 to 0E	File number required
2	Data	00	Offset (LSB)
3	Data	00	Offset .
4	Data	00	Offset (MSB)
5	Data	40	Length (LSB)
6	Data	00	Length .
7	Data	00	Length (MSB)
8	Data	??	Data to be written
.	Data	??	Data to be written
59	Data	??	Data to be written

Table 74a - WriteData Additional Frame

Byte offset	Label	Value (hex)	Description
0		AF	Additional Frame tag
1	Data	??	Data to be written
.	Data	??	Data to be written
12	Data	??	Data to be written
13	MAC	??	MAC of data to be written
14	MAC	??	MAC of data to be written
15	MAC	??	MAC of data to be written
16	MAC	??	MAC of data to be written
17	Padding	00	Padding to make entire data string a multiple of 8 bytes
18	Padding	00	Padding to make entire data string a multiple of 8 bytes
19	Padding	00	Padding to make entire data string a multiple of 8 bytes
20	Padding	00	Padding to make entire data string a multiple of 8 bytes

8.12.2.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.12.2.4 Response data

There is no response data for the WriteData command.

8.13 Value Record access

The Value Record files shall be accessed by use of the ReadData and WriteData commands.

Read access to these files is unconditional, and can be done at any time, subject to the ITSO application being selected.

Update access to these files shall require a valid mutual authentication session to have taken place.

Updates to these files shall require the use of the CommitTransaction command.

8.13.1 ReadData

8.13.1.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

Whilst not essential, it is strongly recommended that a valid mutual authentication has taken place and a secure session is in progress. This will result in a MAC been applied to the data read, thus increasing the security of the transfer.

8.13.1.2 Command parameters

The table below defines the parameters required for the ReadData command.[58]

Table 75 - ReadData command

Byte offset	Label	Value (hex)	Description
0	Cmd	BD	
1	Data	02 to 07	File number required
2	Data	00	Offset (LSB)
3	Data	00	Offset .
4	Data	00	Offset (MSB)
5	Data	00	Length (LSB) - No length specified, read entire file
6	Data	00	Length .
7	Data	00	Length (MSB)

8.13.1.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

[58] Showing the read of an entire Value Record file

8.13.1.4 Response data

The response to the ReadData command for the entire Value Record file will consist of 2 data frames[59], which when concatenated will result in a:

— 64-byte block of data; if a valid mutual authentication session has not taken place; OR

— 64-byte block of data followed by a 4-byte MAC; if a valid mutual authentication session has taken place.

8.13.2 WriteData

8.13.2.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

A valid mutual authentication must have taken place and a secure session must be in progress.

8.13.2.2 Command parameters

The table below defines the parameters required for the WriteData command and its associated Additional Frame which is required if full update of the Value Record is required.

Note: The Value Record is structured to allow partial updates to be used for most transactions. It is recommended that POSTs make use of this capability to improve transaction speed.

Table 76 - WriteData command

Byte offset	Label	Value (hex)	Description
0	Cmd	3D	
1	Data	01 to 05	File number required
2	Data	00	Offset (LSB)
3	Data	00	Offset .
4	Data	00	Offset (MSB)
5	Data	40	Length (LSB)
6	Data	00	Length .
7	Data	00	Length (MSB)
8	Data	??	Data to be written
.	Data	??	Data to be written
59	Data	??	Data to be written

[59] A data frame can hold up to 59 bytes. See the mifare® DESFire specification for further details

Table 76a - WriteData Additional Frame

Byte offset	Label	Value (hex)	Description
0		AF	Additional Frame tag
1	Data	??	Data to be written
.	Data	??	Data to be written
12	Data	??	Data to be written
13	MAC	??	MAC of data to be written
14	MAC	??	MAC of data to be written
15	MAC	??	MAC of data to be written
16	MAC	??	MAC of data to be written
17	Padding	00	Padding to make entire data string a multiple of 8 bytes
18	Padding	00	Padding to make entire data string a multiple of 8 bytes
19	Padding	00	Padding to make entire data string a multiple of 8 bytes
20	Padding	00	Padding to make entire data string a multiple of 8 bytes

8.13.2.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.13.2.4 Response data

There is no response data for the WriteData command.

8.13.3 CommitTransaction

This command validates and commits all write operations that have been made to Backup files within the selected application. Failure to issue this command after an update to a Backup file will result in the loss of the update (i.e. the file will remain unchanged).

8.13.3.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

A valid mutual authentication must have taken place and a secure session must be in progress.

8.13.3.2 Command parameters

The table below defines the parameters required for the CommitTransaction command.

Table 77 - CommitTransaction command

Byte offset	Label	Value (hex)	Description
0	Cmd	C7	

8.13.3.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.13.3.4 Response data

There is no response data for the CommitTransaction command.

8.14 Cyclic Log access

The Cyclic Log shall be accessed by use of the ReadData and WriteData commands.

Read access to this file is unconditional, and can be done at any time, subject to the ITSO application being selected.

Update access to this file shall require a valid mutual authentication session to have taken place.

Updates to this file shall require the use of the CommitTransaction command.

The presence and size of the Cyclic Log shall be established by use of the GetFileSettings command.

8.14.1 GetFileSettings

8.14.1.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

8.14.1.2 Command parameters

The table below defines the parameters required for the GetFileSettings command.

Table 78 - GetFileSettings command

Byte offset	Label	Value (hex)	Description
0	Cmd	F5	
1	Data	01	File number

8.14.1.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

The Cyclic Log shall only be used if the response code indicates the presence of the file.

8.14.1.4 Response data

If the Cyclic Log file is present, the response to the GetFileSettings command will be an 8-byte frame of data that includes the size of the file.

8.14.2 ReadData

8.14.2.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

Whilst not essential, it is strongly recommended that a valid mutual authentication has taken place and a secure session is in progress. This will result in a MAC been applied to the data read, thus increasing the security of the transfer.

8.14.2.2 Command parameters

The table below defines the parameters required for the ReadData command.[60]

Table 79 - ReadData command

Byte offset	Label	Value (hex)	Description
0	Cmd	BD	
1	Data	07	File number
2	Data	??	Offset (LSB)
3	Data	00	Offset .
4	Data	00	Offset (MSB)
5	Data	30	Length (LSB)
6	Data	00	Length .
7	Data	00	Length (MSB)

The offset parameter shall be used to select the require Transient Ticket Record as shown below:

Table 80 - Offset

TT Record	Offset (hex) lsb, . ,msb
1	00, 00, 00
2	30, 00, 00
3	60, 00, 00
4	90, 00, 00

8.14.2.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.14.2.4 Response data

The response to the ReadData command will be a:

— 48-byte frame of data; if a valid mutual authentication session has not taken place; OR

— 48-byte frame of data followed by a 4-byte MAC; if a valid mutual authentication session has taken place.

8.14.3 WriteData

8.14.3.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

A valid mutual authentication must have taken place and a secure session must be in progress.

[60] Showing the read of an entire TT record of 48 bytes

8.14.3.2 Command parameters

The table below defines the parameters required for the WriteData command.

Table 81 - WriteData command

Byte offset	Label	Value (hex)	Description
0	Cmd	3D	
1	Data	00	File number
2	Data	??	Offset (LSB)
3	Data	00	Offset .
4	Data	00	Offset (MSB)
5	Data	30	Length (LSB)
6	Data	00	Length .
7	Data	00	Length (MSB)
8	Data	??	Data to be written
.	Data	??	Data to be written
55	Data	??	Data to be written
56	MAC	??	MAC of data to be written
57	MAC	??	MAC of data to be written
58	MAC	??	MAC of data to be written
59	MAC	??	MAC of data to be written

Table 81a - WriteData Additional Frame

Byte offset	Label	Value (hex)	Description
0		AF	Additional Frame tag
1	Padding	00	Padding to make entire data string a multiple of 8 bytes
2	Padding	00	Padding to make entire data string a multiple of 8 bytes
3	Padding	00	Padding to make entire data string a multiple of 8 bytes
4	Padding	00	Padding to make entire data string a multiple of 8 bytes

8.14.3.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.14.3.4 Response data

There is no response data for the WriteData command.

8.14.4 CommitTransaction

This command validates and commits all write operations that have been made to Backup files within the selected application. Failure to issue this command after an update to a Backup file will result in the loss of the update (i.e. the file will remain unchanged).

8.14.4.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SelectApplication command (see section 8.8).

A valid mutual authentication must have taken place and a secure session must be in progress.

8.14.4.2 Command parameters

The table below defines the parameters required for the CommitTransaction command.

Table 82 - CommitTransaction command

Byte offset	Label	Value (hex)	Description
0	Cmd	C7	

8.14.4.3 Response status codes

The status byte shall contain the appropriate response code in accordance with the mifare® DESFire specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

8.14.4.4 Response data

There is no response data for the CommitTransaction command.

8.15 Key usage

Selection of the ITSO application (the DF) shall be unconditional, and shall not require the use of any keys.

Read-only access all EFs shall be unconditional, and shall not require the use of any keys:

After media personalisation[61], the Shell Environment file (file number = 0F hex) shall be read-only during normal usage.

Update of other files shall only be allowed after a successful mutual authentication and establishment of a secure session with the appropriate key. The Directory and the Cyclic Log files share the same key (key number 14).

The access key set shall be generated at the time of customer media personalisation. They shall not be changed for the life of the media. They shall be media-specific, key diversification being provided by use of the MID. The diversification mechanisms are defined in ITSO TS 1000-8.

8.15.1 Application master key setting

The application master key (key number 0) settings shall be configured to:

— Require application master key authentication to change any key

— Allow master key settings to be changed if authenticated with the application master key

— Require application master key authentication to create / delete files

— Allow file attribute access without application master key authentication

[61] Where this is taken to mean the creation of the ITSO Shell on the customer media.

— Allow the application master key to be changed

The above corresponds to an application master key setting value of 0B (hex).

8.16 Key strategy

This CMD shall use the Key Strategy Code (KSC) value as defined in clause 8.7.1.4.2. The ISAM shall use this to determine the appropriate cryptographic processes to be applied to such media platforms.

8.17 Anti-tear

Platforms that conform to this CMD shall provide native hardware Anti-tear protection. The use of the CommitTransaction command will commit updates made to Backup files in an atomic manner. Thus either all updates are executed, or none are.

8.18 Manufacturer's ID

All media conforming to this CMD contain a unique 7-byte manufacturer's serial number. This shall be used wherever an ITSO MID is required (e.g. for security algorithms).

The usage of this serial number when generating the 8-byte ITSO MID shall be as follows:

Table 83 - ITSO MID computation

ITSO MID byte	Contents
Byte 0 (MSB)	00 (hex)
Byte 1	SN0
Byte 2	SN1
Byte 3	SN2
Byte 4	SN3
Byte 5	SN4
Byte 6	SN5
Byte 7 (LSB)	SN6

8.19 Detection of the ITSO Shell

The Shell detection sequence for this CMD shall be as follows:

— If a platform supporting ISO/IEC 14443-4 is detected, then the POST shall issue a SelectApplication command with the ITSO AID as the target.

— If a valid response is received then the presence of the ITSO application has been established.

— The POST shall read the Shell Environment file (file number 15).

— The POST shall parse the data and a CRC shall be computed for the data read. This shall be checked against the SECRC field of the parsed data.

— If this check passes, then the platform carries a valid ITSO Shell.

— The POST shall read and confirm that all the data elements listed in Table 61 have the specified values. If this check passes then an ITSO Shell of FVC = 07 shall be deemed to be present.

8.20 Benchmark transaction

8.20.1 IPE with Transient Ticket Record creation

The benchmark transaction for this CMD shall comprise:

— Detection of a platform carrying a valid Shell with FVC = 07 and default data element values

— Verification of the Directory

— Verification of an IPE Data Group where there is only a single candidate product, and the IPE Data Group resides in a single sector (file)

— Creation of a sealed 48-byte Transient Ticket Record.

— Update of the log entry and modification of the directory.

— Read after write verification of the updated Directory

The target execution time for the above, subsequent to detection of the platform, shall be 300ms or less.

> Note: The target execution time includes all necessary POST application functions. (i.e. normal operation, Hotlist processing etc…)

8.20.2 IPE with Value Record Data Group modification

The benchmark transaction for this CMD shall comprise:

— Detection of a platform carrying a valid ITSO Shell with FVC = 07 and default data element values.

— Verification of the Directory.

— Verification of an IPE Data Group where there is only a single candidate product and the IPE Data Group resides in a single Sector.

— Verification and modification of an associated Value Record Data Group where the Value Record Data Group resides in a single Sector.

— Modification of the Directory to reflect the changes made to data group and product above.

— Read after write verification of the updated Directory.

The target execution time for the above, subsequent to detection of the platform, shall be 300ms or less.

> Note: The target execution time includes all necessary POST application functions. (i.e. normal operation, Hotlist processing etc…)

8.21 List search method

This CMD supports a full ITSO Shell as defined in ITSO TS 1000-2. When a POST carries out a Hotlist or Action List search against a platform where FVC = 07, then it shall use Shell Referencing as defined in ITSO TS 1000-3.

9. Calypso Format Revision 2

9.1 Scope

This clause defines the CMD for Calypso-based platforms.

The design of this CMD allows for the hosting of the ITSO Application on a Calypso based platform that:

— Supports application selection via AID; and

— Is compatible with revision 2 and Version 3 of the Calypso specification.

— Has sufficient data storage capacity.

Use of this CMD allows an ITSO Compliant Shell (Application) to be provided with minimum development effort on such platforms.

9.1.1 Terminology

Throughout this clause reference will be made to terms defined within ISO/IEC 7816-4:1995 and the Calypso Specification for Ticketing V3.

9.2 Platform capability

9.2.1 General

This CMD is capable of supporting a full set of ITSO Data Groups as defined below

- Shell Environment	Full Shell environment
- Directory	One copy
- IPE	Multiple IPE instances may be present
- Value Record	May be associated with relevant IPEs subject to overall memory limits
- Cyclic Log	Support for Basic and Normal mode logging

This Specification defines a set of default parameters for this CMD that control the size of storage and the number of products stored. ITSO Shell Owners may use alternate parameter values to those specified herein. POSTs shall be able to process media with alternate parameter values.

The default parameters define a memory structure that will support:

— 5 Directory Entries;

— 13 Sectors for IPE instance, Value Record and Cyclic Log storage

The Calypso command set used by this platform supports:

— Selection of the ITSO Directory and files.

— Reading of data from these files (without the need for media/POST authentication).

— Establishing of mutual authentication between the media and the ISAM.

— Update of the ITSO files (after required security exchanges).

9.2.2 Memory architecture

The memory architecture of this platform is summarised below:

— Based around a filing system complying with ISO/IEC 7816-4:1995.

— The ITSO application consists of a Dedicated File (DF) containing the following Elementary Files (EF), structured and sized as shown below.

— Parameter File, SFI=0F, Single Record, Size

— Shell, SFI=0x01, Single Record, Linear File, Size

— Directory, SFI=02, Single Record, Linear File, Size=B Bytes

— IPE Storage, SFI=03[62], S-3 Records, Record Size=B Bytes, Linear File.

9.2.3 Security provisions

The platform shall provide the following security-related features:

— Support for mutual authentication between POST and media via Calypso Secure Messaging Standard.

— Support for use of access keys to EFs (3 levels supported).

— Support for native Anti-tear protection.

9.2.4 ISO/IEC 14443 compliance

All platforms covered by this CMD shall comply with the following parts of ISO/IEC 14443:

— Part 2: RF power & signal interface Compliance with ISO/IEC 14443 Type B requirements;

— Part 3: Initialisation & anti-collision Compliance with ISO/IEC 14443 Type B requirements;

— Part 4: Transmission protocol Compliance with ISO/IEC 14443 Type B requirements.

Note: If a media reports (to the POST) that it supports ISO/IEC 14443-4, then ISO/IEC 14443 requires that this protocol shall be selected. The implications of this are that if any applications (including an ITSO one) reside either in a 'classic Mifare®' area on the media, or are accessed by use of other proprietary protocols, then these will not be able to be accessed. This is a known limitation of ISO/IEC 14443.

9.3 Format Version Code

Platforms that conform to this CMD shall use the Format Version Code (FVC) of 08.

9.4 Command set

The platform shall support the following Calypso commands[63]. The instruction (INS) codes are shown in hex.

— SELECT FILE (INS code = A4);

---

[62] Unless modified by the contents of the parameter file see clause 9.7.2.3.2.

[63] These commands are the ones required during normal usage of the platform. They do not include the commands required for the creation of the ITSO Application on the platform.

— READ RECORD (INS code = B2);

— UPDATE RECORD (INS code = DC);

— OPEN SECURE SESSION (INS code = 8A);

— CLOSE SECURE SESSION (INS code = 8E);

The detailed usage of these commands will be defined in subsequent sections of this document.

9.5 Authentication algorithms

Platforms use the Calypso authentication algorithms (implemented in the ISAM).

9.5.1 Authentication keys

The platform shall be able to store a secret key, specific to the ITSO Application, for use with the following commands:

— OPEN SECURE SESSION;

— UPDATE RECORD.

9.6 Secure Session

Secure Session support is mandatory on this CMD.

The use of secure sessions allows the mutual authentication of the card and the ISAM, the authentication of the data exchanged and the proof that the CM actually recorded the data

9.7 File system structure

Figure 2 illustrates the structure of the default ITSO file system. All SFIs are in hex.

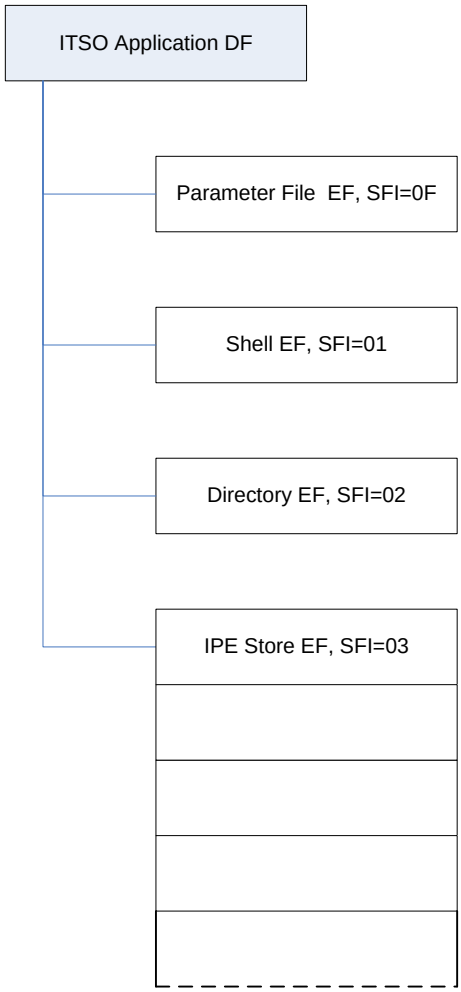

Figure 2 - ITSO file structure

The file system structure shall consist of the following mandatory files:

— A Dedicated File (DF) that acts as the root for the ITSO Application.

— An Elementary File (EF) containing parameter information.

— 1 EF used for storage of the ITSO Shell Environment.

— 1 EF with 13[64] records used for storage of the ITSO IPE instances.

— 1 EF used for storage of the ITSO Directory copies.

If Private Applications are hosted within the ITSO Shell, then they shall optionally reside in separate DFs.

[64] Default value - See clause 3.7.4.4.2

9.7.1 ITSO Application DF

This file shall have the following attributes:

9.7.1.1 Name

The DF Name for this file shall be the ITSO Application Identifier (AID), in line with recommended practice for DF naming and selection. See section 9.8 for details of the AID.

9.7.1.2 Access conditions

Creation - At personalisation only;

Update - Not allowed;

Read - Unconditional;

Delete - Not allowed.

9.7.2 Parameter EF

This read-only EF file contains parameters relating to the platform.

This file shall have the following attributes.

9.7.2.1 File ID

This file shall be assigned the Short File Identifier of 0F (hex).

9.7.2.2 Access conditions

Creation - At personalisation only;

Update - Not allowed;

Read - Unconditional;

Delete - Not allowed.

9.7.2.3 File structure

This file shall use a transparent binary structure. The contents of the file shall consist of the following BER-TLV coded data objects:

— Mutual authentication algorithm support Tag value = C1 (hex);

— Storage EF short file ID Tag value = C3 (hex);

— Directory size Tag value = C4 (hex);

— Anti-tear mechanism Tag value = C5 (hex);

9.7.2.3.1 Mutual authentication algorithm support object

The Parameter EF shall contain one or more instance(s) of this object.

This object shall contain the following Data Elements:

Table 84 – Data Elements of the mutual authentication algorithm support object

Item		Size	Value	Comment
Tag		1 byte	C1 (hex)	
Length		1 byte	01	
Data	Algorithm type	1 byte		'Algorithm type' defines the form of mutual authentication that the platform supports. Allowed values (in hex) are listed below. Other values are RFU. 04 – Calypso type mutual authentication.

9.7.2.3.2 Storage EF short file ID object

The Parameter EF shall contain one instance of this object.

This object shall contain the following Data Elements:

Table 85 - Data Elements of the storage EF short file ID object

Item		**Size**	**Value**	**Comment**
Tag		1 byte	C3 (hex)	
Length		1 byte	01	
Data	Short file ID for storage EF	1 byte	03 or as required	The short file ID for the storage EF. If the platform reserves the above value for other use, then the short ID actually used for the EF shall be indicated by this field.

9.7.2.3.3 Directory size object

The Parameter EF shall contain one instance of this object.

This object shall contain the following Data Elements:

Table 86 - Data Elements of the Directory size object

Item		Size	Value	Comment
Tag		1 byte	C4 (hex)	
Length		1 byte	01	
Data	Directory size	1 byte	30 (hex) or as required	The default Directory size for this CMD is 48 bytes. If the platform uses a different size of Directory then the size (in bytes) shall be indicated by this field. The following are recommended alternative Directory sizes: 32, 48, 64, 80, 96, 112, 128, 144, 160, 176 and 192 bytes

9.7.2.3.4 Anti-tear mechanism object

The Parameter EF shall contain one instance of this object.

This object shall contain the following Data Elements:

Table 87 - Data Elements of the Anti-tear mechanism object

Item		Size	Value	Comment
Tag		1 byte	C5 (hex)	
Length		1 byte	01	
Data	Software Anti-tear mechanism	1 byte	00 (none) 01 (type A)	This defines which form of software Anti-tear shall be used. A value of 00 indicates that the card does not require any form of software Anti-tear to be provided. The default value is 00.

9.7.3 Storage EFs

By default the platform shall contain 3 of these files. Their default usage is:

— One shall be used to store the ITSO Shell Environment.

— One shall be used to store Directory.

— One shall be used to store the IPEs.

9.7.4 ITSO Shell Environment EF

This EF (the first of the storage EFs) contains the ITSO Shell Environment Data Group. This file shall have the following attributes.

9.7.4.1 File ID

This file shall have the short EF identifier of 01.

9.7.4.2 Access conditions

Creation - At personalisation only;

Update - Allowed, subject to valid mutual authentication and presentation of correct access key;

NOTE: Update of the Shell EF should be one time only during ITSO perso.

Read - Unconditional;

Delete - Not allowed.

9.7.4.3 File structure

This file shall use a binary structure. The size of the file shall be ‘B’ bytes, where ‘B’ is defined as in ITSO TS 1000-2.

9.7.4.4 ITSO Shell Environment Data Group

The ITSO Shell Environment Data Group shall be stored in this EF. The elements and layout of this data structure are fully defined in ITSO TS 1000-2.

9.7.4.4.1 Platform parameters with fixed values

The following platform parameter Data Elements within the ITSO Shell Environment Data Group shall have the fixed values specified herein for all implementations of this CMD.

Table 88 - Fixed platform parameter values

Data Element	Default value	Comment
ShellLength	6 8	If the optional MCRN is not present If the optional MCRN is present
ShellBitMap	msb-000001-lsb msb-000011-lsb	If the optional MCRN is not present If the optional MCRN is present
ShellFormatRevision	1	For this version of the Specification
FVC	8	See section 9.3

9.7.4.4.2 Platform parameters with default values which may be overridden

The following platform parameter Data Elements within the ITSO Shell Environment Data Group shall have (explicit) default values as listed below. However, ITSO Shell Owners may override these defaults by specifying an alternative value within the associated data field of the ITSO Shell Environment Data Group at the time of ITSO Shell creation.

POSTs shall correctly parse and use the parameter values provided by the platform.

Table 89 - Default Data Element values

Data Element	Default value	Comment
KSC	4	As defined in ITSO TS1000-8.
B	48 (30 hex)	Size of storage Sector.
S	16 (10 hex)	This gives a Ψ of 4
E	5	Number of Directory Entries
SCTL	7	Length of SCT

As well as the above parameters held within the ITSO Shell Environment Data Group, this CMD allows ITSO Shell Owners to specify non-default Directory sizes (see section 9.7.2.3.3) at the time of ITSO Shell creation.

9.7.4.4.3 ITSO Shell Environment detailed layout

Table 90 details the location of the Data Elements when the default platform parameter values are used. Shading indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Table 90 - Default ITSO Shell Environment data content - No MCRN present

Data Element Label	# of bits	Start location	End location
ShellLength	6	Byte 0, bit 7	Byte 0, bit 2
ShellBitMap	6	Byte 0, bit 1	Byte 1, bit 4
ShellFormatRevision	4	Byte 1, bit 3	Byte 1, bit 0
IIN	24	Byte 2, bit 7	Byte 4, bit 0
OID	16	Byte 5, bit 7	Byte 6, bit 0
ISSN	28	Byte 7, bit 7	Byte 10, bit 4
CHD	4	Byte 10, bit 3	Byte 10, bit 0
FVC	8	Byte 11, bit 7	Byte 11, bit 0
KSC	8	Byte 12, bit 7	Byte 12, bit 0
KVC	8	Byte 13, bit 7	Byte 13, bit 0
RFU	2	Byte 14, bit 7	Byte 14, bit 6
EXP	14	Byte 14, bit 5	Byte 15, bit 0
B	8	Byte 16, bit 7	Byte 16, bit 0
S	8	Byte 17, bit 7	Byte 17, bit 0
E	8	Byte 18, bit 7	Byte 18, bit 0
SCTL	8	Byte 19, bit 7	Byte 19, bit 0
PAD	16	Byte 20, bit 7	Byte 21, bit 0
SECRC	16	Byte 22, bit 7	Byte 23, bit 0

Table 90a - Default ITSO Shell Environment data content - MCRN present

Data Element Label	# of bits	Start location	End location
ShellLength	6	Byte 0, bit 7	Byte 0, bit 2
ShellBitMap	6	Byte 0, bit 1	Byte 1, bit 4
ShellFormatRevision	4	Byte 1, bit 3	Byte 1, bit 0
IIN	24	Byte 2, bit 7	Byte 4, bit 0
OID	16	Byte 5, bit 7	Byte 6, bit 0
ISSN	28	Byte 7, bit 7	Byte 10, bit 4
CHD	4	Byte 10, bit 3	Byte 10, bit 0
FVC	8	Byte 11, bit 7	Byte 11, bit 0
KSC	8	Byte 12, bit 7	Byte 12, bit 0
KVC	8	Byte 13, bit 7	Byte 13, bit 0
RFU	2	Byte 14, bit 7	Byte 14, bit 6
EXP	14	Byte 14, bit 5	Byte 15, bit 0
B	8	Byte 16, bit 7	Byte 16, bit 0
S	8	Byte 17, bit 7	Byte 17, bit 0
E	8	Byte 18, bit 7	Byte 18, bit 0
SCTL	8	Byte 19, bit 7	Byte 19, bit 0
MCRN	80	Byte 20, bit 7	Byte 29, bit 0
SECRC	16	Byte 30, bit 7	Byte 31, bit 0

9.7.5 IPE storage EF

By default the platform shall contain 1 IPE Storage file. Each with S-3 records of B bytes each. These are used to store the following Data Groups:

— IPE;

— Value Record;

— Cyclic Log.

Each of these files shall have the following attributes.

9.7.5.1 File ID

By default the file shall have the short EF identifier of 03 unless the platform does not allow the use of this short ID for user files, then the alternative value shall be specified in the Parameter EF (see section 9.7.2.3.2)

9.7.5.2 Access conditions

Creation - At personalisation only;

Update - Allowed, subject to valid mutual authentication and presentation of correct access key;

Read - Unconditional;

Delete - Not allowed.

9.7.5.3 File structure

Each file shall use a binary structure. The file size shall be 'B' bytes[65] multiplied by (S-3).

9.7.6 Directory EF

This EF shall be used to store the following Data Groups:

— Directory (one copy only)

This file shall have the following attributes.

9.7.6.1 File ID

By default the file shall have the short EF identifier of 02.

9.7.6.2 Access conditions

Creation	- At personalisation only;
Update	- Allowed, subject to valid mutual authentication and presentation of correct access key;
Read	- Unconditional;
Delete	- Not allowed.

9.7.6.3 File structure

These files shall use a binary structure.

The default file size shall be 48 bytes. Where a platform does not use this default Directory size, then the actual value shall be specified in the Parameter EF (see section 9.7.2.3.3). POSTs shall check for and correctly process Directories of non-default size.

9.7.6.4 Directory Data Group location

Table 91 details the location of the Data Elements for the directory when the default platform parameter values are used. Shading indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

[65] The default value of 'B' is 48

Table 91 - Default Directory Data Group

Data Element Label	# of bits	Start location	End location
DIRLength	6	Block 0, byte 0, bit 7	Block 0, byte 0, bit 2
DIRBitMap	6	Block 0, byte 0, bit 1	Block 0, byte 1, bit 4
DIRFormatRevision	4	Block 0, byte 1, bit 3	Block 0, byte 1, bit 0
E1	40	Block 0, byte 2, bit 7	Block 0, byte 6, bit 0
E2	40	Block 0, byte 7, bit 7	Block 0, byte 11, bit 0
E3	40	Block 0, byte 12, bit 7	Block 1, byte 0, bit 0
E4	40	Block 1, byte 1, bit 7	Block 1, byte 5, bit 0
E5	40	Block 1, byte 6, bit 7	Block 1, byte 10, bit 0
SCT1	4^{66}	Block 1, byte 11, bit 7	Block 1, byte 11, bit 4
SCT2	4	Block 1, byte 11, bit 3	Block 1, byte 11, bit 0
SCT3	4	Block 1, byte 12, bit 7	Block 1, byte 12, bit 4
SCT4	4	Block 1, byte 12, bit 3	Block 1, byte 12, bit 0
SCT5	4	Block 1, byte 13, bit 7	Block 1, byte 13, bit 4
SCT6	4	Block 1, byte 13, bit 3	Block 1, byte 13, bit 0
SCT7	4	Block 1, byte 14, bit 7	Block 1, byte 14, bit 4
SCT8	4	Block 1, byte 14, bit 3	Block 1, byte 14, bit 0
SCT9	4	Block 1, byte 15, bit 7	Block 1, byte 15, bit 4
SCT10	4	Block 1, byte 15, bit 3	Block 1, byte 15, bit 0
SCT11	4	Block 2, byte 0, bit 7	Block 2, byte 0, bit 4
SCT12	4	Block 2, byte 0, bit 3	Block 2, byte 0, bit 0
SCT13	4	Block 2, byte 1, bit 7	Block 2, byte 1, bit 4
PAD	4	Block 2, byte 1, bit 3	Block 2, byte 1, bit 0
DIRS#	8	Block 2, byte 2, bit 7	Block 2, byte 2, bit 0
KID	4	Block 2, byte 3, bit 7	Block 2, byte 3, bit 4
INS#	4	Block 2, byte 3, bit 3	Block 2, byte 3, bit 0
ISAMID	32	Block 2, byte 4, bit 7	Block 2, byte 7, bit 0
Seal	64	Block 2, byte 8, bit 7	Block 2, byte 15, bit 0

9.7.6.4.1 DIRLength

This is RFU and shall contain a value of 0.

9.7.6.4.2 DIRFormatRevision

This shall contain a value of 1 (1 hex).

9.7.6.4.3 Sector Chain Table (SCT) usage

The relationship between the SCT entries and the physical storage on the platform is done on a Sector-to-EF record basis. Each SCT Label corresponds to a record (contained within the IPE storage EF) on the platform.

When the default platform parameters are used then each SCT entry shall contain a number in the range 0 to 15 (decimal). The following values shall have special significance as defined in ITSO TS 1000-2.

---

[66] The number of bits for the SCTx fields is equal to Ψ

Note: As stated in section 9.7.4.4.2, the default value of S is 16 for this CMD. If an alternate S is used, then the above value ranges and the latter two special SCT values in the table below shall be adjusted accordingly (as defined in ITSO TS 1000-2).

Table 92 - Special SCT values

SCT entry value (decimal)	Significance
0	Corresponding EF (see Table 93) is un-allocated and may be used to store product data.
'Self'[67]	Terminating Sector / EF for product in question. Product is Virgin
14	Terminating Sector / EF for product in question. Product is Blocked
15	Terminating Sector / EF for product in question. Product is not Blocked

Table 93 defines the mapping between SCT Label and the IPE DFs / EFs.

Table 93 - SCT Label vs. IPE DF and EF

SCT Label	IPE EF SFI/ Record
SCT1	03 / 0001
SCT2	03 / 0002
SCT3	03 / 0003
SCT4	03 / 0004
SCT5	03 / 0005
SCT6	03 / 0006
SCT7	03 / 0007
SCT8	03 / 0008
SCT9	03 / 0009
SCT10	03 / 0010
SCT11	03 / 0011
SCT12	03 / 0012
SCT13	03 / 0013

Note that the 13 Records listed above shall be used to store Data Elements associated with the following Data Groups:

— IPE;

— Value Record;

— Cyclic Log.

As defined in ITSO TS 1000-2, Sectors SCT1 to SCT'E'[68] (shown shaded) have special significance, and are reserved as Starting Sectors.

[67] Where 'Self' means that the value in the entry corresponds to the entry's own number / Label. For example if SCT11 contains the value 11 (decimal) then this is a 'self' reference.

9.7.6.4.4 PTYP usage for Private Applications

Where the data associated with a Directory Entry is a Private Application, the PTYP field within the Directory Entry shall be used to generate the record identifier (see section 9.7.7). In such cases the value within the PTYP field shall be in the range 01 (hex) to 0F (hex).

9.7.7 Private Applications

Private Applications are either constructed outside of the scope of the ITSO application on the CM or are stored (as TYPE 0 IPE) within the IPE storage EF. This requires use of the secure session keys and the ISAM.

9.8 ITSO Application selection

The ITSO application shall be selected by use of the SELECT FILE command in a direct application selection manner. The data field of this command shall be the Application Identifier (AID).

POSTs shall attempt to select using the ITSO AID first. If this fails, then selection using the Calypso AID shall be attempted.

9.8.1 ITSO AID

In accordance with ISO/IEC 7816-5:1994, the ITSO AID shall be made up of:

— Registered Application Provider Identifier (RID) for ITSO 5 bytes

— Proprietary Application Identifier Extension (PIX) 6 bytes

The international RID assigned to ITSO is (in hex): A0, 00, 00, 02, 16

As defined in ISO/IEC 7816-5:1994, the registration category for this RID is International and as such is represented by A (hex) in the 4 most significant bits.

The PIX field shall be 6 bytes in length and shall contain the ASCII string “ITSO-1”.

This format provides for explicit identification of the ITSO Application, and allows for the support of multiple ITSO Applications in the future.

9.8.2 SELECT FILE

9.8.2.1 Command pre-conditions

None. The POST may issue this command at any time. This command must be used to select the ITSO Application on the media. It would not normally be required to be issued again during a session.

9.8.2.2 Command parameters

The table below defines the parameters required for the SELECT FILE command for the ITSO Application.

---

[68] Default value of E is 8

Table 94 - SELECT FILE parameters

Byte offset	Label	Value (hex)	Description
0	CLA	94	As per Calypso specification
1	INS	A4	SELECT command
2	P1	04	Selection by DF name
3	P2	00	Select first or only occurrence of ITSO application and return FCI
4	Lc	0B	Length of data field
5	Data	A0	AID
6	Data	00	AID
7	Data	00	AID
8	Data	02	AID
9	Data	16	AID
10	Data	49	AID
11	Data	54	AID
12	Data	53	AID
13	Data	4F	AID
14	Data	2D	AID
15	Data	31	AID
16	Le	00[69]	Maximum response length

9.8.2.3 Response status codes

The SW1 and SW2 status bytes will contain the appropriate response code in accordance with the Calypso specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

9.8.2.4 Response data

The response data to the SELECT command shall comprise of the following BER-TLV data objects within the File Control Information (FCI) template. The Tag values (in hex) are also shown.

— DF Name 84

— FCI Proprietary Template A5

— FCI Issuer Discretionary Data BF0C

— Application Serial Number (contains the MID) C7

— Discretionary Data 53

Refer to the Calypso specification for further details.

[69] The response length will vary dependant on the platform's FCI Proprietary Template support.

9.9 Mutual authentication and session communications

If a transaction requires an update to any of the contents of files within the ITSO application area, then a secured session shall be established between the media and the POST. This shall be done by the use of the following commands:

— OPEN SECURE SESSION

— CLOSE SECURE SESSION

9.9.1 Command sequence

The POST to media mutual authentication sequence (including the command sequences to/from the ISAM) is fully detailed in Document SS00010 “Calypso Technical Use Guide”.

9.9.2 OPEN SECURE SESSION

9.9.2.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SELECT FILE command (see section 9.7.3).

9.9.2.2 Command parameters

The table below defines the parameters required for the OPEN SECURE SESSION command.

Table 95 - OPEN SECURE SESSION parameters

Byte offset	Label	Value (hex)	Description
0	CLA	94	As per Calypso specification
1	INS	8A	OPEN SECURE SESSION command
2	P1	01	Use key number 1
3	P2	00	No file to select
4	Lc	4	Length of data field
5	Data	??	Random number
6	Data	??	Random number
7	Data	??	Random number
8	Data	??	Random number

9.9.2.3 Response status codes

The SW1 and SW2 status bytes will contain the appropriate response code in accordance with the Calypso specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

9.9.2.4 Response data

The response data to the OPEN SECURE SESSION command shall comprise:

— A 1-byte field containing the KVC of the selected key.

— A 4-byte field containing a random number challenge generated by the media.

— An optional 2-byte field. This field is only present if ratification of the previous session was not carried out by the media.

9.9.3 CLOSE SECURE SESSION

9.9.3.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SELECT FILE command (see section 9.7.3).

A secure session must be open (see section 9.8.2)

9.9.3.2 Command parameters

The table below defines the parameters required for the CLOSE SECURE SESSION command, when it is used to for normal termination of a secure session.

Table 96 - CLOSE SECURE SESSION parameters

Byte offset	Label	Value (hex)	Description
0	CLA	94	As per Calypso specification
1	INS	8E	CLOSE SECURE SESSION command
2	P1	80	Immediately ratify session
3	P2	00	
4	Lc	04	Set Lc to 0 to cancel the session
5	Data	??	SignatureHi
6	Data	??	SignatureHi
7	Data	??	SignatureHi
8	Data	??	SignatureHi

9.9.3.3 Response status codes

The SW1 and SW2 status bytes will contain the appropriate response code in accordance with the Calypso specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

9.9.3.4 Response data

The response data to the CLOSE SECURE SESSION command shall comprise of a 4-byte data block containing the low-order bytes of the session signature.

9.10 Shell access

The Environment EF that contains the Shell shall be accessed by use of the READ RECORD command, with implicit selection using the short EF identifier.

Read access to this EF shall be unconditional, and can be done at any time, subject to selection of the ITSO application (by use of the SELECT FILE command).

Update access to this EF is not allowed.

9.10.1 READ RECORD

9.10.1.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SELECT FILE command (see section 9.7.3).

9.10.1.2 Command parameters

The table below defines the READ RECORD command parameters required.

Table 97 - READ RECORD parameters (Shell)

Byte offset	Label	Value (hex)	Description
0	CLA	94	As per Calypso specification
1	INS	B2	READ RECORD command
2	P1	01	Record number 1
3	P2	0C	SFI = 01 (hex) ; Record as in P1
4	Le	18[70]	Response length

9.10.1.3 Response status codes

The SW1 and SW2 status bytes will contain the appropriate response code in accordance with the Calypso specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

9.10.1.4 Response data

The response to the READ RECORD command is a data block of ‘the record size of the EF’ bytes in length.

9.11 Directory access

The EF that contains the Directory shall be accessed by use of the READ RECORD and UPDATE RECORD commands, with implicit selection using the short EF identifier.

Read access to this EF shall be unconditional, and can be done at any time, subject to selection of the ITSO application (by use of the SELECT FILE command).

Update access to this EF is only allowed after a secure session has been opened with key number 2.

9.11.1 READ RECORD

9.11.1.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SELECT FILE command (see section 9.7.3).

9.11.1.2 Command parameters

The table below defines the READ RECORD command parameters required.

[70] Shell size is 24 bytes

Table 98 - READ RECORD parameters (Directory)

Byte offset	Label	Value (hex)	Description
0	CLA	94	As per Calypso specification
1	INS	B2	READ RECORD command
2	P1	01	Record number 1
3	P2	14	SFI = 02 (hex) ; Record as in P1
4	Le	30[71]	Response length

9.11.1.3 Response status codes

The SW1 and SW2 status bytes will contain the appropriate response code in accordance with the Calypso specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

9.11.1.4 Response data

The response to the READ RECORD command is a data block of ‘record size’ bytes in length.

9.11.2 UPDATE RECORD

9.11.2.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SELECT FILE command (see section 9.7.3).

A secure session must be open (see section 9.8.2)

Note that only 3 record updates (in total) can be made in any one secure session.

9.11.2.2 Command parameters

The table below defines the UPDATE RECORD command parameters required.

[71] Read the entire record

Table 99 - UPDATE RECORD parameters (Directory)

Byte offset	Label	Value (hex)	Description
0	CLA	94	As per Calypso specification
1	INS	DC	UPDATE RECORD command
2	P1	01	Record number 1
3	P2	14	SFI = 02 (hex) ; Record as in P1
4	Lc	30[72]	Data length
5	Data	??	Data to be written
.	Data	??	Data to be written
.	Data	??	Data to be written
..	Data	??	Data to be written

9.11.2.3 Response status codes

The SW1 and SW2 status bytes will contain the appropriate response code in accordance with the Calypso specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

9.11.2.4 Response data

There is no response data for the UPDATE RECORD command.

9.12 IPE access

The EF that contains the IPE data shall be accessed by use of the READ RECORD and UPDATE RECORD commands, with implicit selection using the relevant short EF identifier.

Read access to this EF shall be unconditional, and can be done at any time, subject to selection of the ITSO application (by use of the SELECT FILE command).

Update access to this EF is only allowed after a secure session has been opened.

9.12.1 READ RECORD

9.12.1.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SELECT FILE command (see section 9.8.2).

9.12.1.2 Command parameters

The table below defines the READ RECORD command parameters required.

[72] Write the entire record

Table 100 - READ RECORD parameters (IPE)

Byte offset	Label	Value (hex)	Description
0	CLA	94	As per Calypso specification
1	INS	B2	READ RECORD command
2	P1	01 to 0D	Record number 1 to 13
3	P2	1C	SFI =03 (hex) ; Record as in P1
4	Le	30[73]	Response length

9.12.1.3 Response status codes

The SW1 and SW2 status bytes will contain the appropriate response code in accordance with the Calypso specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

9.12.1.4Response data

The response to the READ RECORD command is a data block of 29 bytes in length.

9.12.2 UPDATE RECORD

9.12.2.1 Command pre-conditions

The ITSO application must have been previously selected by use of the SELECT FILE command (see section 9.7.3).

A secure session must be open (see section 9.8.2)

Note that only 3 record updates (in total) may be made in any one secure session.

9.12.2.2 Command parameters

The table below defines the UPDATE RECORD command parameters required.

[73] Read the entire record

Table 101 - UPDATE RECORD parameters (Directory)

Byte offset	Label	Value (hex)	Description
0	CLA	94	As per Calypso specification
1	INS	DC	UPDATE RECORD command
2	P1	01 to 04	Record number 1 to 4
3	P2	1C	SFI = 03 (hex) ; Record as in P1
4	Lc	30[74]	Data length
5	Data	??	Data to be written
.	Data	??	Data to be written
.	Data	??	Data to be written
..	Data	??	Data to be written…

9.12.2.3 Response status codes

The SW1 and SW2 status bytes will contain the appropriate response code in accordance with the Calypso specification.

Response codes other than those signifying normal processing shall cause the POST to abort the session and indicate an error to the user.

9.12.2.4 Response data

There is no response data for the UPDATE RECORD command.

9.13 Key usage

Selection of the ITSO application (the DF) shall be unconditional, and shall not require the use of any keys.

Read-only access all EFs shall be unconditional, and shall not require the use of any keys:

After media personalisation[75], the Shell Environment EF (SFI = 01 hex) shall not be changeable in normal use. Writing data to the Shell Environment EF shall only be allowed after a successful secure session command sequence using key number 1.

Update of other EFs shall only be allowed after a successful secure session command sequence, using key number 2. The Directory and all logical sectors for IPE storage share the same key (key number 2).

The access key set shall be generated at the time of customer media personalisation. They shall not be changed for the life of the media. They shall be media-specific, key diversification being provided by use of the MID. The diversification mechanisms are defined in ITSO TS 1000-8.

9.14 Key strategy

This CMD shall use the Key Strategy Code (KSC) value as defined in clause 9.4.1. The ISAM shall use this to determine the appropriate cryptographic processes to be applied to such media platforms.

---

[74] Write the entire record

[75] Where this is taken to mean the creation of the ITSO Shell on the customer media.

9.15 Anti-tear

Platforms that conform to this CMD provide native hardware Anti-tear protection. The closing of a secure session will commit up to 3 record updates to the media in an atomic manner. Thus either all updates are executed, or none are.

9.16 Manufacturer's ID

All media conforming to this CMD return an 8-byte serial number in the SELECT application response (see section 9.8.2.4) This shall be used wherever an ITSO MID is required (e.g. for ISAM PIMO commands).

The usage of this serial number when generating the 8-byte ITSO MID shall be as follows:

Table 102 - ITSO MID computation

ITSO MID byte	Contents
Byte 0 (MSB)	Byte offset 0
Byte 1	Byte offset 1
Byte 2	Byte offset 2
Byte 3	Byte offset 3
Byte 4	Byte offset 4
Byte 5	Byte offset 5
Byte 6	Byte offset 6
Byte 7 (LSB)	Byte offset 7

9.17 Detection of the ITSO Shell

The Shell detection sequence for this CMD shall be as follows:

— If a platform supporting ISO/IEC 14443-4 (type B) is detected, then the POST shall issue a SELECT FILE command with the ITSO AID as the target.

— If a valid response is received then it is possible that an ITSO application is present.

— The POST shall read the Shell from the Shell EF

— The POST shall parse the data and a CRC shall be computed for the data read. This shall be checked against the SECRC field of the parsed data.

— If this check passes, then the platform carries a valid ITSO Shell.

9.18 Benchmark transaction

9.18.1 IPE with Transient Ticket Record creation

The benchmark transaction for this CMD shall comprise:

— Detection of a platform carrying a valid Shell with FVC = 08 and default data element values

— Verification of the Directory

— Verification of an IPE Data Group where there is only a single candidate product, and the IPE Data Group resides in a single sector

— Creation of a sealed 48-byte Transient Ticket Record.

— Update of the log entry and modification of the directory

The target execution time for the above, subsequent to detection of the platform, shall be 300ms or less.

Note: The target execution time includes all necessary POST application functions. (i.e. normal operation, Hotlist processing etc…).

9.18.2 IPE with Value Record Data Group modification

The benchmark transaction for this CMD shall comprise:

— Detection of a platform carrying a valid ITSO Shell with FVC = 08 and default data element values

— Verification of the Directory

— Verification of an IPE Data Group where there is only a single candidate product and the IPE Data Group resides in a single sector.

— Verification and modification of an associated Value Record Data Group where the Value Record Data Group resides in a single sector.

— Modification of the Directory to reflect the changes made to data group and product above.

The target execution time for the above, subsequent to detection of the platform, shall be 300ms or less.

Note: The target execution time includes all necessary POST application functions. (i.e. normal operation, Hotlist processing etc…)

9.19 List search method

This CMD supports a full ITSO Shell as defined in ITSO TS 1000-2. When a POST carries out a Hotlist or Actionlist search against a platform where FVC = 08, then it shall use Shell Referencing as defined in ITSO TS 1000-3.

Annex A
(normative)
Anti-tear - type A

A.1 Introduction

This Annex defines the type A form of Anti-tear. This form of Anti-tear is what was originally defined in earlier versions of the Specification.

A.2 Overview

The general concept behind this type of Anti-tear is to hold 2 complete copies of the data to be protected, with a form of pointer indicating the most recently written to copy. If this copy is found to be damaged in any way, then the earlier copy will be used.

Although two copies of the Directory and Value Record Data Groups are held, a different mechanism is used for the Cyclic Log.

A.3 Operation

The following sections define the rules and sequences to be used when implementing type A Anti-tear.

The illustrations used are based on a FVC = 01 platform.

A.3.1 Directory Data Group

A.3.1.1 General

There shall be two copies of the Directory Data Group. These two copies shall be labelled Copy A and Copy B respectively.

The Directory Dataset contains the DIRS# Data Element which is incremented every time the Directory is updated. This number will rollover many times during the life of the ITSO Shell and said rollover shall be taken into account by the software implementing Anti-tear mechanisms.

There is no pointer available to point directly to the current version of the Directory. Therefore in order to establish the current version, both copies of the Directory shall be read.

A.3.1.2 Directory initial conditions

When two copies of the Directory Data Group are first created in an ITSO Shell , both copies of the Directory Data Group shall be set to contain the same information with the exception that the DIRS# Data Element shall be set to 00 (hex) in Copy A and 01 (hex) in Copy B.

A.3.1.3 Operational rules

1 Read the ITSO Shell Environment Data Group to establish the required parameters for the platform and data structures.

2 Read both copies of the Directory Data Group.

3 Determine the Directory with the latest DIRS# value (with consideration given to rollover). Confirm the Seal of this copy. If this is OK then said copy shall be referred to as the ***Current*** Directory. The other shall be referred to as the ***Oldest*** Directory. Go to step 6.

4 If the above test fails then verify the Seal of the other copy. If this is OK then said copy shall be referred to as the ***Current*** Directory. The other shall be referred to as the ***Oldest*** Directory. Go to step 6.

5 If both copies are found to have incorrect Seals then the media shall be deemed to be non-functional and no further processing shall take place.

6 When manipulating Directories the POST shall always make updates to a local[76] copy of the ***Current*** Directory and shall terminate a transaction by writing this ***Revised*** Directory over the ***Oldest*** Directory on the media.

7 A read after write operation shall be carried out by the POST to verify that the ***Revised*** Directory was correctly written to the media.

[76] i.e. a copy held within the POST's memory

A.3.2 Value Record Data Group

The mechanism described herein also allows for the accumulation of a Value Record history automatically as Value Records are updated. This auto-logging attribute should, where possible, be used in preference to creating a separate Transient Ticket Record in the Cyclic Log.

A.3.2.1 Relationship of Value Record Data Groups to IPE Data Groups

Where an IPE Data Group is associated with a Value Record Data Group, there shall be two copies of the Value Record Data Group. These two Value Record Data Groups shall be labelled Copy A and Copy B respectively.

The relationship of the Value Record Data Group to the IPE Data Group is given by the sequence of Sectors linked by the SCT. The sequence shall always start with the first Sector of the IPE Data Group. On initial creation, Data groups shall be linked in the following order:

— IPE Data Group

— Value Record Data Group - Copy A

— Value Record Data Group - Copy B

This is illustrated in Figure A.1 for a Virgin, non-Blocked IPE of TYP 2. The example shows the storage arrangements when the IPE's Directory Entry is the first entry in the Directory group and where the Value Record Data Groups are in Sectors 6 and 9.

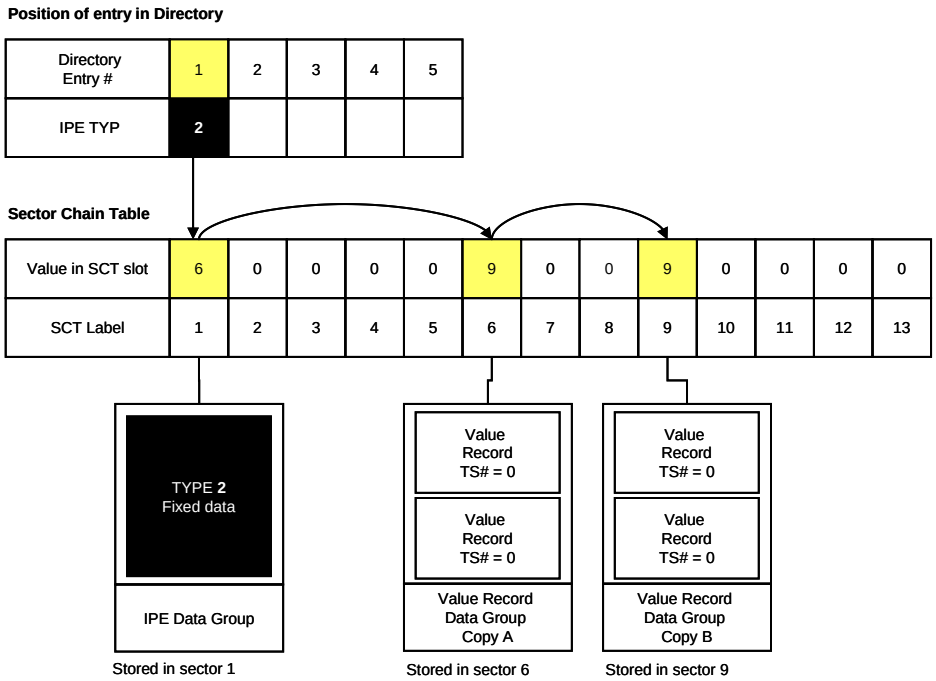

Figure A.1 - Physical relationships of IPE and Value Record Data Groups to an IPE Directory Entry

A.3.2.2 Relationship of Value Records to Value Record Data Groups

Value Records contain a Transaction Sequence Number (TS#) Data Element. They are numbered in increasing order as they are created or overwritten. A number of Value Records are held in a Value Record Dataset that is cryptographically bound to the Seal of the Value Record Data Group.

When a Value Record Data Group is created, sufficient memory space shall be allocated for the number of Value Records supported. The VGBitMap Data Element indicates how many Records a Value Record Dataset supports and the A and B copies of the Data Group shall support the same number. The minimum number of records per Value Record Dataset shall be 2.

The Product Owner shall define the initial conditions for the Value Record. However the TS# for all Value Records shall remain set to zero until the first transaction that uses the Value Record occurs.

The Value Record copy that follows the IPE Data Group in the SCT linked list shall be termed the *Current* copy. In Figure A.1 this is Copy A. The other copy shall be termed the *Previous* copy.

When a transaction is carried out, the POST shall read the *Current* copy to determine the pre-transaction data. If the TS# of the candidate Value Record is duplicated within the *Current* copy the most significant Value Record in the Data Group shall be used to determine the pre-transaction data. It shall then write the revised (post-transaction) data to the *Previous* copy. The *Previous* copy is then made current by changing the link order in the SCT.

Figure A.2 illustrates this, based on a transaction (with TS# of 1) occurring on the IPE example of Figure A.1.

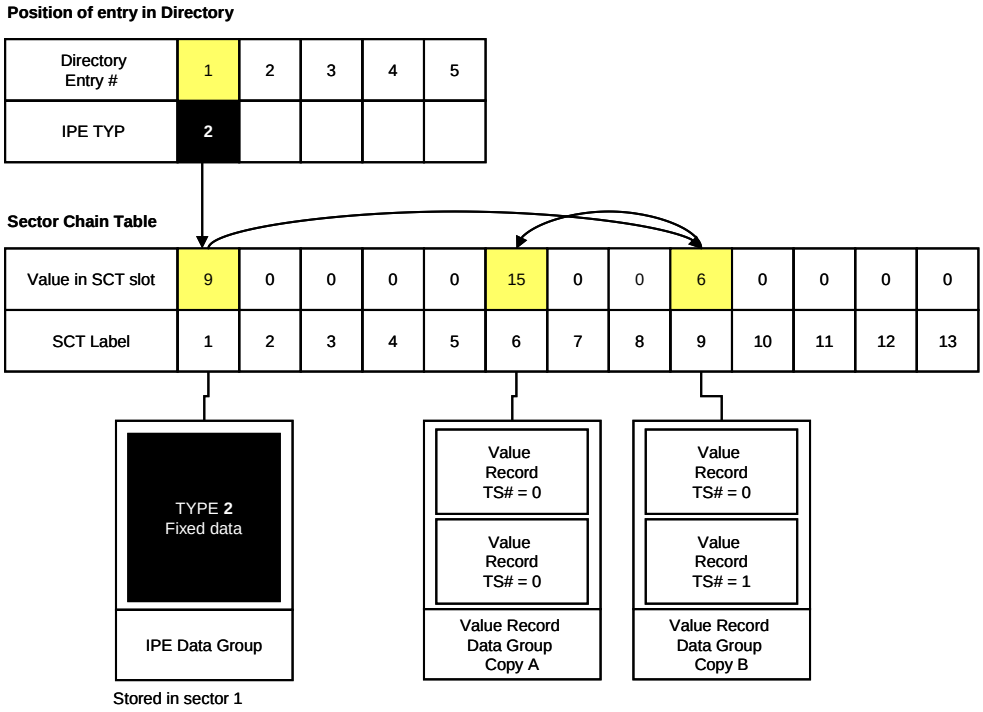

Figure A.2 - Current VR copy indicated by SCT linkage change

A.3.2.3 Value Record updating sequence diagrams

Value Records are written in order of sequence number first into Copy B then to Copy A then back to Copy B…etc. As detailed in the previous section, the SCT linkage order for the Value Record Datasets defines the *Current* and *Previous* Data Group Copies.

In the example illustrated in Figure A.3, the Value Record Dataset supports two Value Records each. The figure shows the state of the Value Records in a sequence of views marked 'A' to 'C'.

View 'A' illustrates the situation prior to transaction with TS#=4 taking place. Copy B is indicated as *Current* by the SCT link order (i.e. the pre-transaction data to be read in held in said copy).

View 'B' illustrates the situation immediately after the TS#=4 Record has been written, but prior to Directory update. Copy B is still indicated as *Current* by the SCT link order.

View 'C' illustrates the situation after the (TS#=4) Record has been verified as correctly written and the SCT link order in the Directory has been updated to point to Copy A as *Current*.

Value Records shall be populated in the order shown in view 'C' of Figure A.3, where the first Record is the least significant Record of the Value Record Dataset in Data Group Copy B and the TS# shall be set to 1 on first use. The second Record shall then be the least significant Record of the Value Record Dataset in Data Group Copy A where the TS# shall be set to 2 on first use. On next use the next least significant Value Record in Data Group Copy B is used…etc.

Throughout the life of the Value Record Dataset even numbered Value Records should remain in Copy A with odd numbered ones in Copy B.

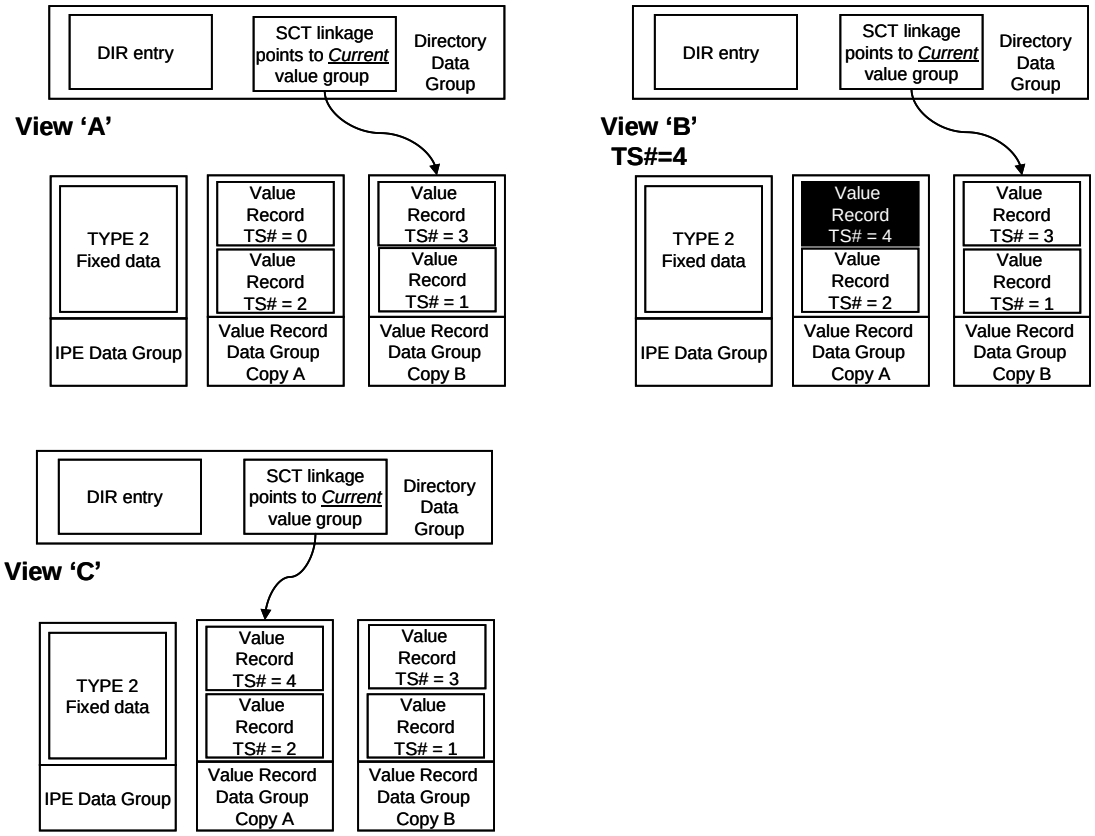

Figure A.3 - Value Record updating

Figure A.4 shows a sequence of 4 transactions (TS#=4 to TS#=7). Each view is taken at the point immediately after the Record has been written, but prior to Directory update (i.e. equivalent to view 'B' in Figure A.3). As can be seen the Record with TS#=5 shall overwrite the record with TS#=1 as shown in view 'B'; TS#=6 shall overwrite the record with TS#=2 as shown in view 'C', etc.

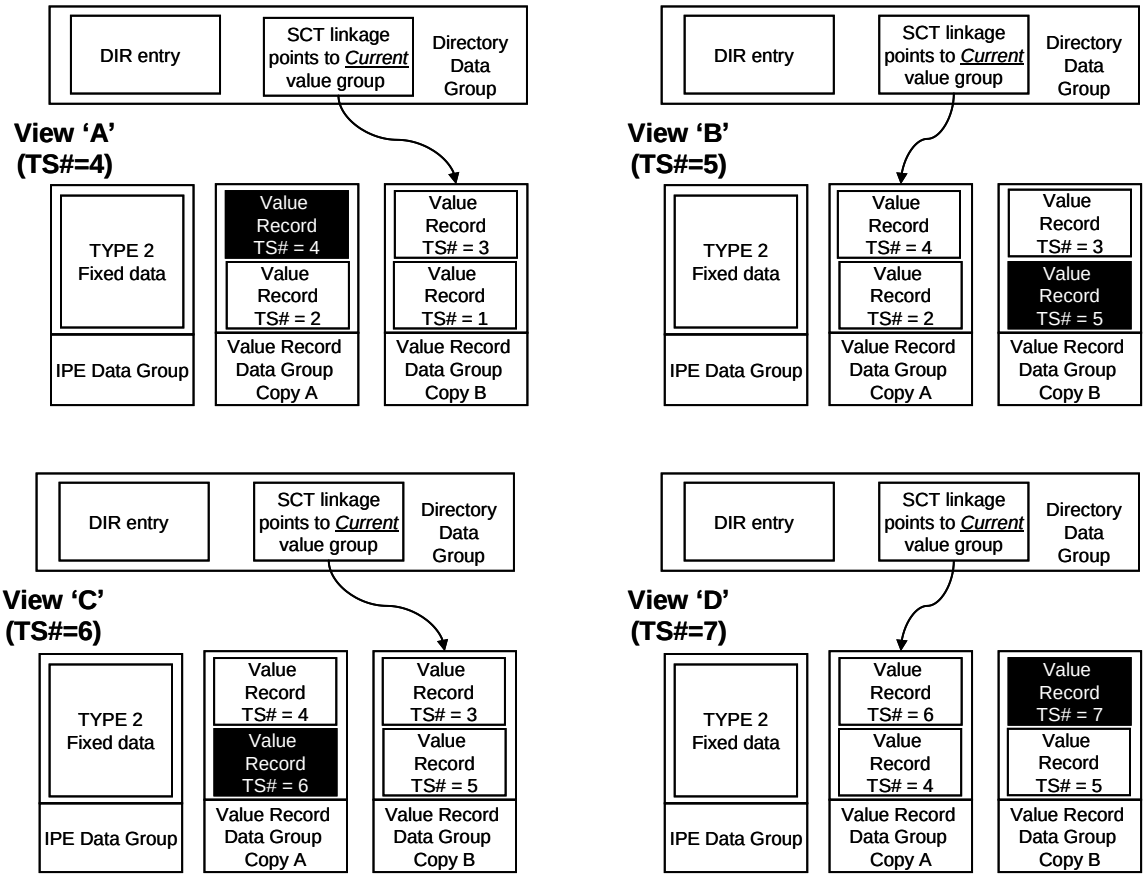

Figure A.4 - Value Record updating

A.3.2.3.1 Transaction Sequence Numbers

The POST shall determine the Transaction Sequence Number to be used by reading and verifying both Value Record Datasets (Copy A and Copy B).

If both copies have a valid Seal, then the highest Transaction Sequence Number in the *Current* copy shall be incremented by 1 and used.

If only the *Current* copy has a valid Seal, then the highest Transaction Sequence Number in this shall be incremented by 1 and used.

If only the *Previous* copy has a valid Seal, then the highest Transaction Sequence Number in this shall be incremented by 1 and used. During normal operation the situation should not arise where only the *Previous* copy has a valid Seal. See section A.3.2.4.3 for operation under these conditions.

Note: All increments shall take account of roll-over as defined in ITSO TS 1000-2.

A.3.2.4 Tear handling

A.3.2.4.1 Directory tear

Figure A.5 illustrates the case when the update to the Directory Data Group is torn after the Value Record Data Group has been successfully updated. In this event the Directory pointer will point to the 'wrong' copy of the Value Record Dataset.

View 'A' illustrates the situation prior to transaction with TS#=7 taking place. Copy A is indicated as *Current* by the SCT link order.

View 'B' illustrates the situation immediately after the TS#=7 Record has been written, but prior to Directory update. Copy A is still indicated as Current by the SCT link order.

View 'C' illustrates the situation after the CM has been 'torn' during the Directory write[77]. The SCT link order in the Directory has not been correctly updated to point to Copy B as Current.

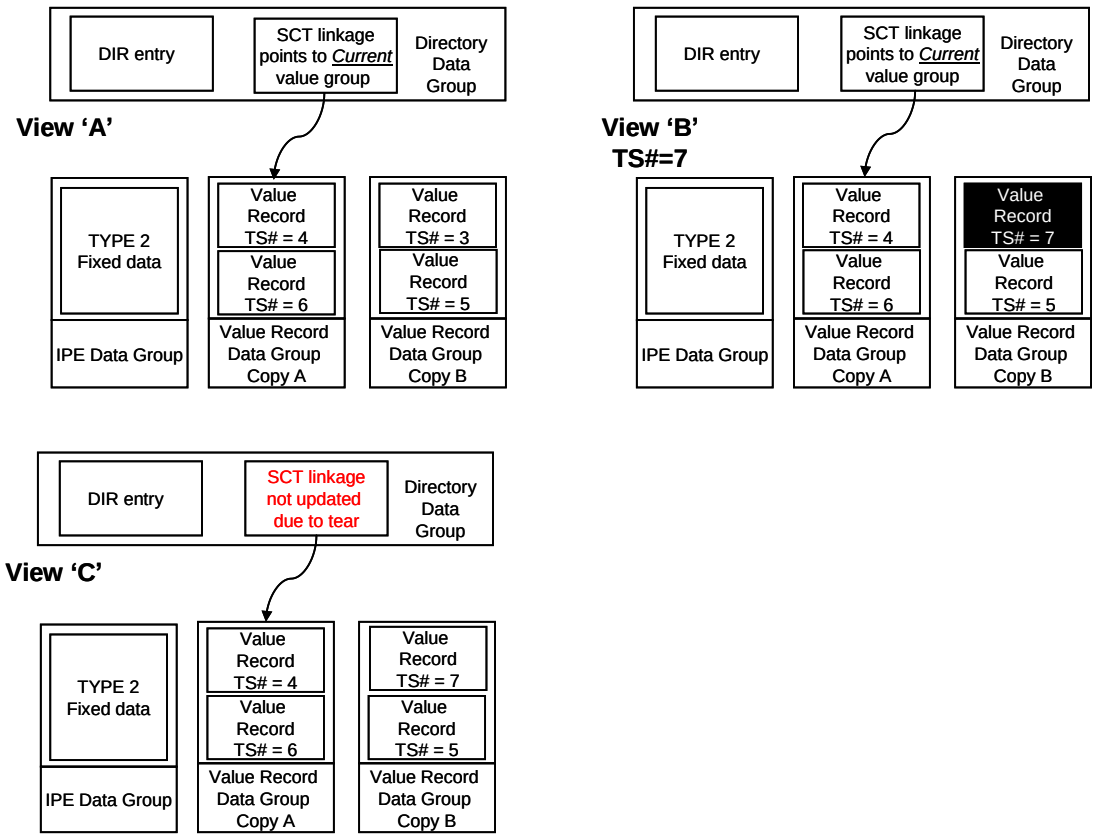

Figure A.2 - Torn transaction (Directory write)

[77] Note: As defined in ITSO TS 1000-3, the POST must check for such tearing and must take appropriate actions and generate specific messages if detected.

Figure A.6 illustrates what will happen the next time the CM is presented to a POST. View 'A' illustrates the 'torn' media (i.e. View 'C' from Figure A.5). Although Copy B has the highest Transaction Sequence Number, Copy A is still denoted by the SCT linkage as *Current*. Using the rules in section A.3.2.3.1 the Transaction Sequence Number to be used is established as "7".

As shown in view 'B', the POST uses the SCT linkage as its reference for determining where to write the post-transaction data. Thus it will select Copy B (the *Previous* copy), writing a Record with TS#=7.

Note that as detailed in section A.3.2.5, where a Record already exists with the same Transaction Sequence Number as that about to be written (i.e. TS#=7 in this example), then this indicates an 'orphan' record - which shall be overwritten.

View 'C' illustrates the situation after the (TS#=7) Record has been verified as correctly written and the SCT link order in the Directory has been updated to point to Copy B as *Current*.

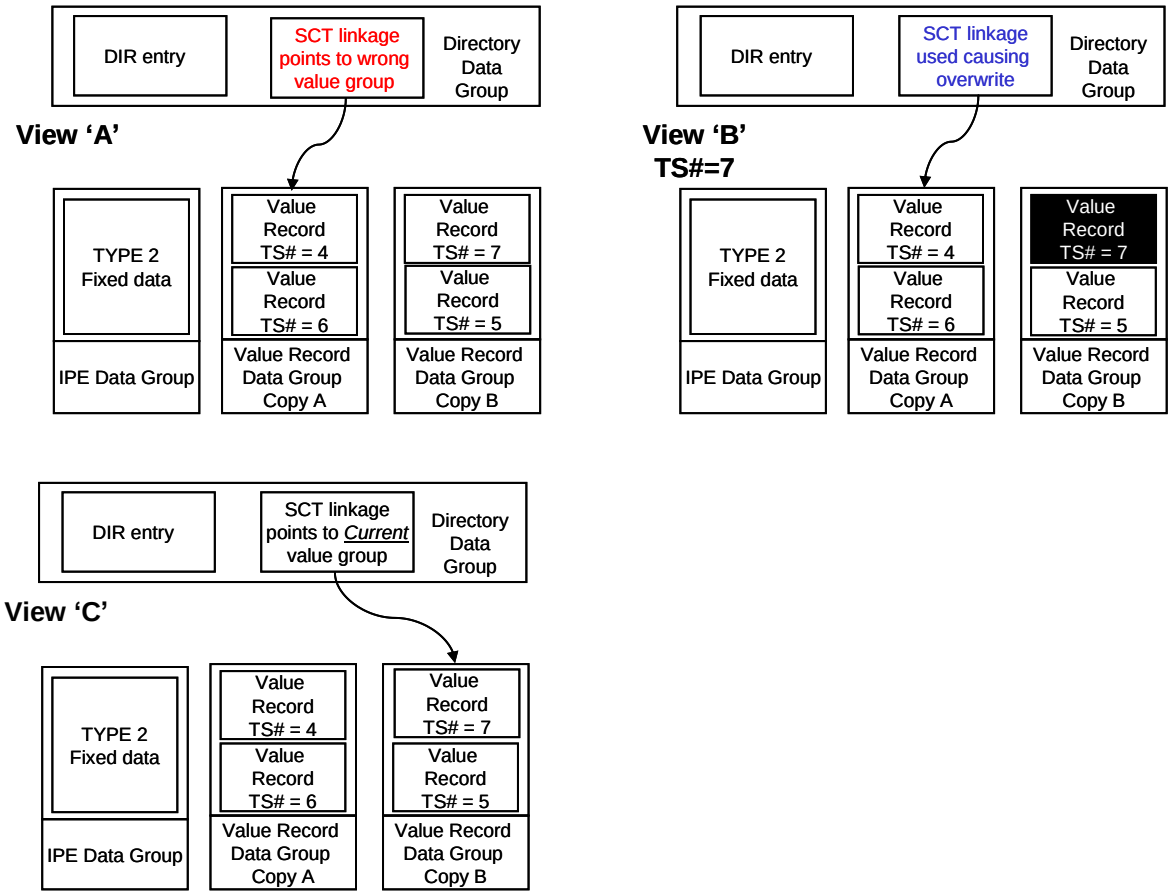

Figure A.3 - Processing after torn Directory write

A.3.2.4.2 Value Record Data Group tear

Figure A.7 illustrates the case when the update to the Value Record Data Group is torn.

View 'A' illustrates the situation prior to transaction with TS#=7 taking place. Copy A is indicated as *Current* by the SCT link order.

View 'B' illustrates the situation as the 'tear' occurs. The TS#=7 Record has not been fully written when the media is removed. Depending on the exact instant that the tear occurred, the data in this copy will either be unchanged, corrupt or fully updated. The first case is a 'non-event'. The third case has been covered in A.3.2.4.1. The following describes the second case when the Value Record Dataset copy is now corrupt (i.e. does not carry a valid Seal).

View 'C' illustrates the final result, with Copy A still indicated as *Current* by the SCT link order. Note that no Directory changes will have occurred as the media was removed prior to this point.

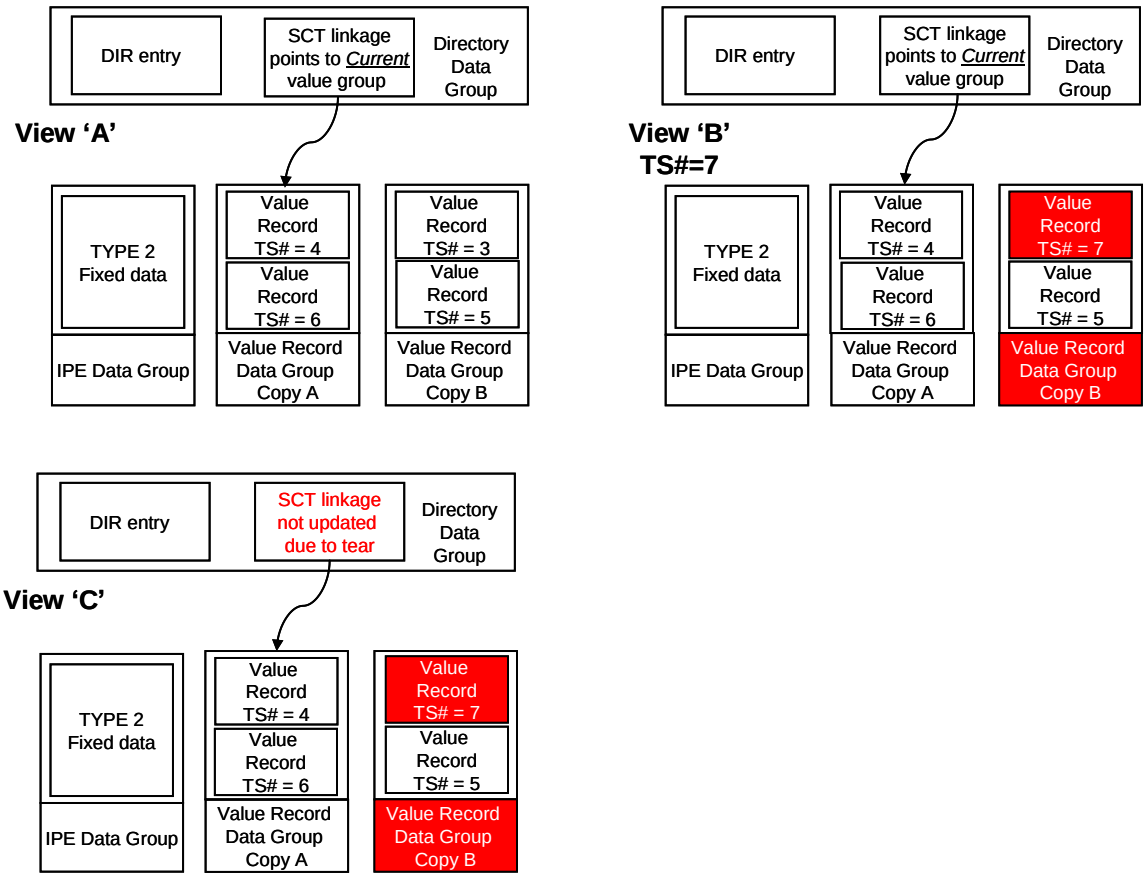

Figure A.7 - Torn transaction (Value Record write)

Figure A.8 illustrates what will happen the next time the CM is presented to a POST.

View ‘A’ illustrates the ‘torn’ media (i.e. View ‘C’ from Figure A.7). Copy A is denoted by the SCT linkage as *Current*, with Copy B being *Previous*. Using the rules in section A.3.2.3.1 the Transaction Sequence Number to be used is established as”7”.

As shown in view ‘B’, the POST uses the SCT linkage as its reference for determining where to write the post-transaction data. Thus it will select Copy B (the corrupt *Previous* copy), writing a Record with TS#=7.

Note that as detailed in section A.3.2.5, when a corrupt Value Record copy is written to, the POST shall fill the entire value record with copies of the new record. Thus in this example 2 copies of TS#=7 are written.

View ‘C’ illustrates the situation after the (TS#=7) Record has been verified as correctly written and the SCT link order in the Directory has been updated to point to Copy B as *Current*.

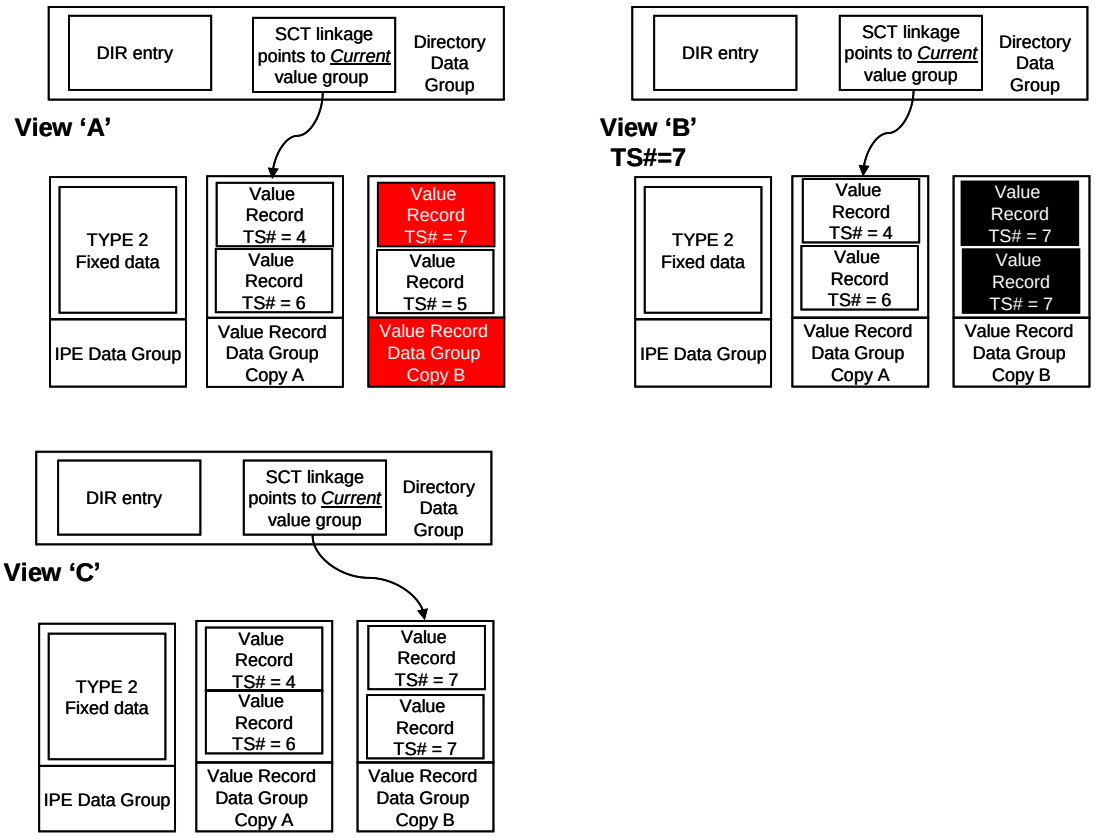

Figure A.8 - Processing after torn Value Record write

Figure A.9 shows a sequence of 4 transactions (TS#=8 to TS#=11). Each view is taken at the point immediately after the Record has been written, but prior to Directory update (i.e. equivalent to view 'B' in Figure A.3). As can be seen in view B, the Record with TS#=9 shall overwrite the 'least significant' of the two records with TS#=7 (see section A.3.2.5)

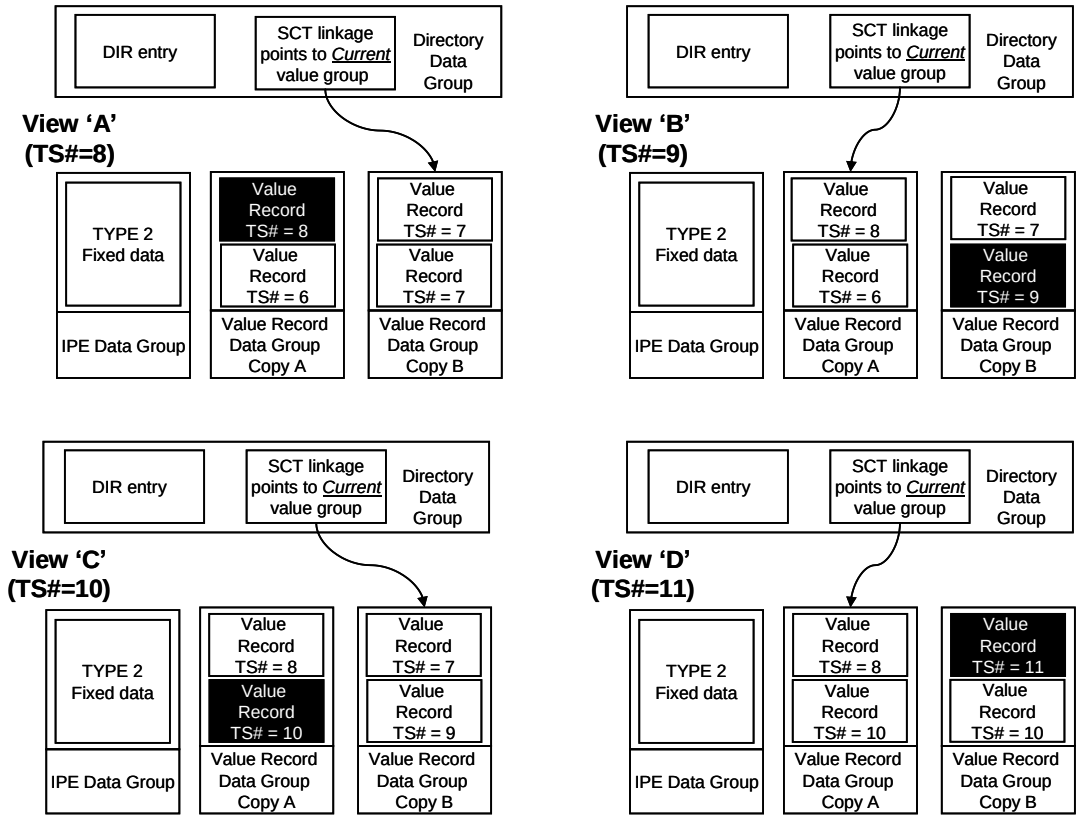

Figure A.9 - Overwriting where there are multiple records with same TS#

A.3.2.4.3 Corrupt Current copy

Under normal operation the *Current* copy of the Value Record Dataset should not become corrupted[78] as a result of tearing. However, POSTs shall be able to handle the case where the media has a corrupt *Current* copy of the Value Record Dataset, but the Seal on the *Previous* copy is correct.

In these cases the POST shall use the data in the *Previous* copy to establish the sequence number.

Figure A.10 illustrates the sequence of operations to be carried out when the Seal on the *Current* copy of the Value Record Dataset is invalid.

View 'A' illustrates the situation prior to the transaction. Copy A is indicated as *Current* by the SCT link order but has an invalid Seal. As defined in section A.3.2.3.1, the sequence number is established to be 11.

[78] Where corrupt is taken to mean that the Seal is not correct.

As shown in view ‘B’, the POST shall override normal usage of the SCT linkage for determining where to write the post-transaction data. Instead, it will select the corrupt copy, writing a Record with TS#=11.

Note that as detailed in section A.3.2.5, when a corrupt Value Record copy is written to, the POST shall fill the entire value record with copies of the new record. Thus in this example 2 copies of TS#=11 are written.

View ‘C’ illustrates the final result. Note that the SCT linkage shall not be updated in this case, resulting in Copy B still being indicated as *Current*.

Note: The approach taken for corrupt *Current* copy handling allows media operation to continue at the cost of ‘losing’ the last record that was written to the (now corrupt) copy. It is recognised that this poses a potential security risk in terms of a ‘play-back’ attack. The Security Monitoring within the Host Operator or Processing System (HOPS) (see ITSO TS 1000-4) shall be cognisant to this operation, and shall take appropriate action if deliberate abuse is suspected.

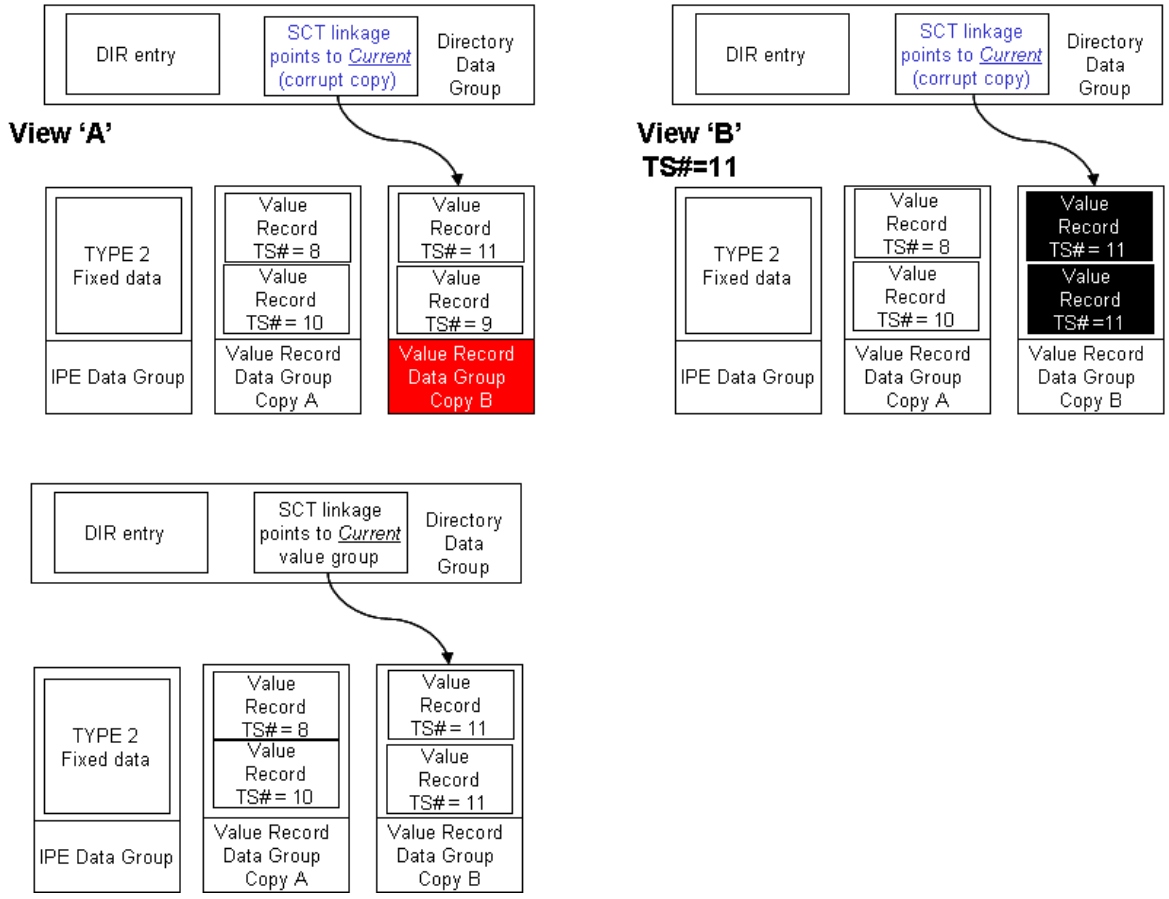

Figure A.10 - Processing when *Current* copy is corrupt

A.3.2.5 General operational rules for Value Records

1 Using the SCT linkage contained in the *Current* Directory (see section A.3.1.3), read and verify both the *Current* and *Previous* copies of the Value Record Dataset.

2 If both copies of the Value Record Dataset have incorrect Seals then the product shall be deemed to be non-functional and no further processing shall take place.

3 If both copies of the Value Record Dataset have valid Seals, then establish the Transaction Sequence Number in the manner defined in A.3.2.3.1. Go to step 6.

4 If the Seal on the *Previous* copy of the Value Record Dataset is incorrect, then establish the Transaction Sequence Number in the manner defined in A.3.2.3.1. Go to step 7.

5 If the Seal on the *Current* copy of the Value Record Dataset is incorrect but the Seal on the *Previous* copy is correct then establish the Transaction Sequence Number in the manner defined in A.3.2.3.1. Go to step 12.

6 If the Transaction Sequence Number determined above matches that of a Record in the *Previous* copy of the Value Record Dataset, then overwrite said Record with the new transaction data. If there is no match of Transaction Sequence Number then overwrite the Record in the *Previous* copy that has the lowest sequence number. In the case where more that one record has this lowest sequence number then overwrite the least significant record. Go to step 8.

7 Generate the required record and write said record to **all** slots in the *Previous* copy of the Value Record Dataset.

8 Generate the Seal for the updated *Previous* copy of the Value Record Dataset. Write all data to the media.

9 Verify that the data has been written correctly to the *Previous* copy of the Value Record Dataset.

10 Update the SCT table in the Directory and write this *Revised* Directory over the *Oldest* Directory on the media. This has the effect of making the old *Previous* Value Record copy *Current*.

11 Verify that the *Revised* Directory was correctly written to the media. **This terminates normal and torn media processing (skip following steps).**

12 Generate the required record and write said record to **all** slots in the *Current* copy of the Value Record Dataset.

13 Generate the Seal for the updated *Current* copy of the Value Record Dataset. Write all data to the media.

14 Verify that the data has been written correctly to the *Current* copy of the Value Record Dataset.

15 Do not update the SCT table in the Directory. If the *Revised* Directory has changed for any other reason then write this *Revised* Directory over the *Oldest* Directory on the media.

A.3.3 Cyclic Log

The Cyclic Log uses a different Anti-tear mechanism to that used for the Value Record Data Group. There is no concept of an ‘A’ and ‘B’ copy. and the Sector linkage remains static.

A.3.3.1 Relationship of the Cyclic Log to the Directory Data Group

If a Cyclic Log is present, then a Log entry shall be present in the Directory. As defined in ITSO TS 1000-2, this entry shall be in the last Directory slot.

The Starting Sector associated with this Directory slot shall store the first Transient Ticket Record (termed record T0). Subsequent record usage is as defined in ITSO TS1000-2 clause 5.1.5.5.

A.3.3.2 Operational rules

1. Establish the *Current* Directory as detailed in section A.3.1.3.
2. Use the SCT and the relevant Directory Entry to establish which record was last written.
3. Establish which is the next available record.
4. Create the Orphan IPE Data Group containing the required Transient Ticket Record Data.
5. Write the Orphan IPE Data Group to the next available record.
6. Write the *Revised* Directory entry to point to the record next used.
7. Generate a new Seal for the *Revised* Directory.
8. Write the *Revised* Directory over the *Oldest* Directory on the media.
9. A read after write operation shall be carried out by the POST to verify that the *Revised* Directory was correctly written to the media.

Annex B
(normative)
Anti-tear - type C

B.1 Introduction

This Annex defines the type C form of Anti-tear. This form of Anti-tear is only used on platforms with a Compact Shell.

B.2 Overview

This type of Anti-tear is similar to type A, but is simpler in operation, due to the limited storage capacity of the platforms on which it is used. Like type A, it is based on the storage of 2 complete copies of the data to be protected, with a form of pointer indicating the most recently written to copy. If this copy is found to be damaged in any way, then the earlier copy will be used.

B.3 Operation

The following sections define the rules and sequences to be used when implementing type C Anti-tear.

Anti-tear protection shall be used on the dynamic IPE data (both class 1 and class 2). Two complete copies of this data is stored, each copy been protected by a Seal.

A sequence number Data Element is present in each copy. This Data Element shall be incremented prior to the data being re-written to the card. Thus, on a correctly written card, one copy shall have a sequence number that is 1 greater than the other (with rollover taken into account); the copy with the highest sequence number being the most recently written.

B.3.1 Operational rules

1 Read both copies of the dynamic IPE data.

2 Determine which copy has the highest sequence number (with consideration given to rollover). Confirm the Seal of this copy. If this is OK then said copy shall be referred to as the *Current* copy. The other shall be referred to as the *Oldest* copy. Go to step 5.

3 If the above test fails then verify the Seal of the other copy. If this is OK then said copy shall be referred to as the *Current* copy. The other shall be referred to as the *Oldest* copy. Go to step 5.

4 If both copies are found to have incorrect Seals then the media shall be deemed to be non-functional and no further processing shall take place.

5 When manipulating dynamic IPE data the POST shall always make updates to a local[79] copy of the *Current* copy and shall terminate a transaction by writing this *Revised* copy over the *Oldest* copy on the media.

6 A read after write operation shall be carried out by the POST to verify that the *Revised* copy was correctly written to the media.

[79] i.e. a copy held within the POST's memory

Annex C
(Normative)
Handling of the ScaledQtyBackup in a one time programmable area

C.1 Introduction

This annex is applicable to customer media that do not support Software or hardware anti-tear systems, but do contain an area of one time programmable memory in the form of n bits that may be set at will but, once set, not changed.

This Annex defines the method whereby the one time programmable area shall be used to determine the value of the QtyRemaining data element if it is corrupted during writing.

As defined in ITSO TS 1000 -5;

- The Data Element ScaledQtyBackup takes the form of a BitMap array of n bits that are set as required in accordance with the formula given for the appropriate space saving IPE's.
- The ScaledQtyBackup maintains a prescribed relationship to the value of the QtyRemaining data element as it's value is altered.

The formula used to determine the number of bits to be left unset in the OTP area shall be defined as follows.

The number of Coupons or Rides remaining divided by the ScalingFactor all rounded to the nearest integer.

Where:

For the TYP 29 having IPEFormatRevision = 1 the Coupons remaining = 8191 – QtyRemaining

For the TYP 29 having IPEFormatRevision = 2 the Rides remaining = 255 - QtyRemaining

The number of bits and the order in which the bits are progressively set is defined in ITSO TS 1000-10 for a particular customer media.

C.2 Examples for use with CMD4

The following examples show the relationship between the settings of the OTP bits and the QtyRemaining Data Element for a variety of values of Coupons or rides remaining. The Calculated refund is obtained by multiplying the ScalingFactor by the number of OTP bits left unset.

Use of the Scaling Factor and actual refund given are determined by the business rules of the IPE owner.

Note: there is no requirement to recode the CM using a value of QtyRemaining determined from the Calculated refund.

Coupons or rides remaining	64
Scaling factor	2
Max # of OTP bits	32
QtyRemaining for Coupons (TYP 29 FR1)	8127
QtyRemaining for Rides (TYP 29 FR2)	191
OTP setting in hex	0x00000000
# of OTP bits left unset	32
Calculated refund	64

Coupons or rides remaining	17
Scaling factor	2
Max # of OTP bits	32
QtyRemaining for Coupons (TYP 29 FR1)	8174
QtyRemaining for Rides (TYP 29 FR2)	238
OTP setting in hex	0x007FFFFF
# of OTP bits left unset	9
Calculated refund	18

Coupons or rides remaining	16
Scaling factor	2
Max # of OTP bits	32
QtyRemaining for Coupons (TYP 29 FR1)	8175
QtyRemaining for Rides (TYP 29 FR2)	239
OTP setting in hex	0x00FFFFFF
# of OTP bits left unset	8
Calculated refund	16

Coupons or rides remaining	500
Scaling factor	20
Max # of OTP bits	32
QtyRemaining for Coupons (TYP 29 FR1)	7691
QtyRemaining for Rides (TYP 29 FR2)	NOT VALID
OTP setting in hex	0x0000007F
# of OTP bits left unset	25

Calculated refund	500
Coupons or rides remaining	480
Scaling factor	20
Max # of OTP bits	32
QtyRemaining for Coupons (TYP 29 FR1)	7711
QtyRemaining for Rides (TYP 29 FR2)	NOT VALID
OTP setting in hex	0x000000FF
# of OTP bits left unset	24
Calculated refund	480