Issuing Authority:	**Owner:**	**Project:**
ITSO	Technology at ITSO	Technical
Document number	**Part Number:**	**Sub-Part Number**
ITSO TS 1000	10	
Issue number (stage):	**Month:**	**Year**
2.1.5	March	2025
Title:		
ITSO TS 1000-10 Interoperable public transport ticketing using contactless smart customer media – Part 10: Customer Media Definitions		
Replaces Documents:		
ITSO TS 1000-10 2010-02 issue number 2.1.4		

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
May 2024		AM	Draft publication of Version 2.1.5
Mar 2025		AM	Updated to include ISADs following approval by DfT.
Mar 2025		AM	Final Editing prior to publication of Version 2.1.5

Document Reference: ITSO TS 1000-10

Date: 2025-03-31

Version: 2.1.5

Ownership: ITSO

Secretariat: Technology at ITSO

ITSO Technical Specification 1000-10 – Interoperable Public Transport Ticketing using contactless smart customer media – Part 10: Customer Media definitions

ISBN: 978-1-3999-8707-3

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

Foreword

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

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

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

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

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

Contents

1. Scope

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

1.1 Scope of Part 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:

• Generic micro-processor	CMD2	clause 3
• Mifare® ultra light	CMD4	clause 5
• Mifare® DESFire	CMD7	clause 8
• Mifare® NTAG215/216	CMD9	clause 10
• Mifare®Ultralight EV1	CMD10	clause 11
• Intelligent Programmable Media	CMD11	clause 12
• Mifare®DESFire	CMD12	clause 13

1.2 Physical form factor

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

2. Mifare® standard 1K-Obselete

Clause retained for numbering.

3. Generic micro-processor

3.1 Scope

This clause defines the CMD for microprocessor-based platforms supporting a minimal and generic set of [ISO 7816-4] 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 7816-4] 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 7816-4].

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 7816-4] 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 7816-4]
- 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[1] '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.

3.2.3 Security provisions

The platform shall provide the following security-related features:

- Support for mutual authentication between POST and media via triple-DES
- Support for use of access keys (PIN / cardholder verification)
- 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[2] 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 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 14443]:

[1] Default size.

[2] Default size.

• Part 2: RF power & signal interface	Compliance with [ISO 14443] Type A or Type B requirements
• Part 3: Initialisation & anticollision	Compliance with [ISO 14443] Type A or Type B requirements
• Part 4: Transmission protocol	Compliance with [ISO 14443] Type A or Type B requirements

Note: If a media reports (to the POST) that it supports [ISO 14443-4], then [ISO 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 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 7816-4] commands[3]. 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 (DES3) algorithm for use by the INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE commands.

The manner in which the platform notifies the POST of the supported algorithm type (03) 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.

[3] 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.

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

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 the only available option for media compliant with the CMD2 definition in this version of the Specification.

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. The use of this feature shall also be applied to Directory and Cyclic Log updates.

3.7 File system structure

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

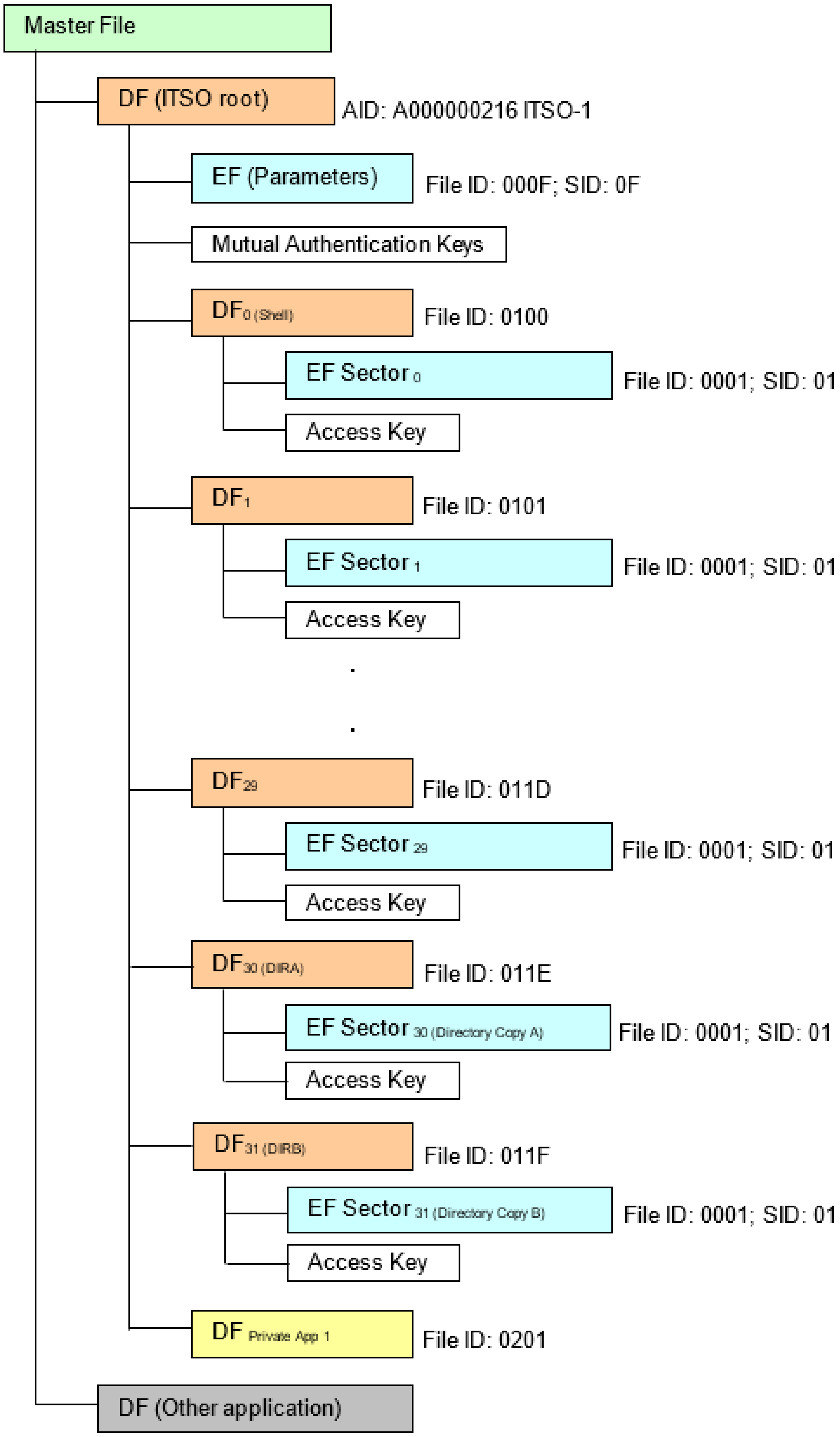


Figure 1 - ITSO file structure

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 DFs[4] containing the EFs used for storage of the ITSO IPE instances
- 29 EFs[5] 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.

[4] Default value - See clause 3.7.4.4.2

[5] Default value - See clause 3.7.4.4.2

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).

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	03	'Algorithm type' defines the form of mutual authentication that the platform supports. Note that this Specification only supports Algorithm type (03). Allowed value (in hex) is listed below. Other values are RFU. 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 Algorithm type (03) as shown in Table 8. Note that no other Algorithm types are supported for CMD2 media compliant to this version of the Specification. For backwards compatibility reasons, POSTs compliant to this version of the Specification may still accept CMD2 media compliant to previous versions of the Specification that utilise Algorithm types 01 or 02 - however, this is deprecated and will be removed from the next version of the Specification.

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[6], 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.

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

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
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[7], 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

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 Microprocessor with mutual authentication using one key KSC = 2 For Microprocessor 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

[7] The default value of B is 48

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[8].

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
Write	- Not allowed

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.

[8] The default value of B is 48

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[9]	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

[9] The number of bits for the SCTx fields is equal to psi

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
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'[10]	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.

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

[10] 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.

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'[11] (shown shaded) have special significance, and are reserved as Starting Sectors.

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

[11] Default value of E is 8

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 7816-5]. Application selection shall only be done by use of the AID.

In accordance with [ISO 7816-5] 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 7816-5] 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”[12].

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 7816-4] 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

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

			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[13]	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 7816-4].

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.

3.8.3.4 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[14]

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[15]
• 84 (hex)	DF Name[16]

[13] The response length will vary dependent on the platforms FCI Proprietary Template support.

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

[15] ISO-IEC 7816-4:1995, table 1

[16] ISO-IEC 7816-4:1995, table 2

• A5 (hex)	FCI Proprietary Template[17]

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”

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

[17] ISO-IEC 7816-4:1995, table 2; ISO-IEC 7816-6, 4.2.1

• 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[18], then a secured session shall be established between the media and the POST. This shall be done by the use of mutual authentication.

Note that CHV/PIN access control without mutual authentication is now deprecated and shall not be used for reasons of backwards compatibility. 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 (deprecated) 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 [19] (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.

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.

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

[19] As defined in ITSO TS 1000-1

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 7816-4] Secure messaging not used
1	INS	84	GET CHALLENGE command
2	P1	00	As [ISO 7816-4]
3	P2	00	As [ISO 7816-4]
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 7816-4].

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 7816-4] 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 7816-4].

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 7816-4] 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 7816-4].

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 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[20]	Response length

Note: Where secure messaging is supported then an alternative CLA byte shall be used to activate its use in accordance with [ISO 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 7816-4] Secure messaging used
1	INS	B0	READ BINARY command
2	P1	81	Implicit selection of EF 01

[20] No response length specified

3	P2	00	Offset to first byte to be read
4	Le	00[21]	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 7816-4].

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.

3.10.1.4 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 7816-4] Secure messaging not used

[21] No response length specified

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 (hex)[22]
7	Le	00[23]	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:

Table 29 - SELECT FILE parameters (ITSO DF)

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with [ISO 7816-4] 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[24]	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)

[22] Based on default parameter values

[23] No response length required

[24] No response length specified

- 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:

Table 30 - SELECT FILE parameters (by path)

Byte offset	Label	Value (hex)	Description
0	CLA	00	Command compliant with [ISO 7816-4] 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[25] (hex)
n	Le	00[26]	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)

[25] Based on default parameter values

[26] No response length specified

3.11.1.3 Response status codes

The SW1 and SW2 status bytes shall contain the appropriate response code in accordance with [ISO 7816-4].

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).

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 7816-4] 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[27]	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 7816-4] Secure messaging used
1	INS	B0	READ BINARY command

[27] No response length specified

2	P1	81	Implicit selection of EF 01
3	P2	00	Offset to first byte to be read
4	Le	00[28]	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 7816-4].

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.

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 7816-4] 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

[28] No response length specified

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 7816-4].

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 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[29]	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.

Table 33a - UPDATE BINARY parameters (secure messaging)

Byte offset	Label	Value (hex)	Description
0	CLA	04	Command compliant with [ISO 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[30]	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

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

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

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

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:

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

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

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 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-Obselete

Clause retained for numbering.

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, bit7
>
> Note: 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[32], 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.).

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

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.

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

Clause intentionally left blank.

7. CMD6 - RFU

Clause intentionally left blank.

8. Mifare® DESFire

8.1 Scope

This clause defines how this CMD can be implemented for platforms that are backwards compatible with the original DESFire specification.

8.1.1 Terminology

Throughout this clause the media definition shall mean a DESFire or compatible device that complies with features defined within revision 3.1 of the mifare® DESFire specification.

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 however only the following type is used by ITSO.
  - Backup Data Files

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[33]. The command codes are shown in hex.

• SelectApplication	(command code = 5A)
• GetFileSettings	(command code = F5)
• Authenticate	(command code = 0A)

[33] 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

- 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 with mutual authentication.

If a mutual authentication session has been successfully completed, then a 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.

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 Data Group or Value Record Data Group	Plain; MACed	E1; 1F (hex)
12	3	Backup data file	64	14; 1	IPE Data Group or Value Record Data Group	Plain; MACed	E1; 1F (hex)
11	4	Backup data file	64	14; 1	IPE Data Group or Value Record Data Group	Plain; MACed	E1; 1F (hex)

10	5	Backup data file	64	14; 1	IPE Data Group or Value Record Data Group	Plain; MACed	E1; 1F (hex)
9	6	Backup data file	64	14; 1	IPE Data Group or Value Record Data Group	Plain; MACed	E1; 1F (hex)
8	7	Backup data file	64	14; 1	IPE Data Group or Value Record Data Group	Plain; MACed	E1; 1F (hex)
7	8	Standard data file	64	14; 1	IPE Data Group	Plain; MACed	E1; 1F (hex)
6	9	Standard data file	64	14; 1	IPE Data Group	Plain; MACed	E1; 1F (hex)
5	10	Standard data file	64	14; 1	IPE Data Group	Plain; MACed	E1; 1F (hex)
4	11	Standard data file	64	14; 1	IPE Data Group	Plain; MACed	E1; 1F (hex)
3	12	Standard data file	64	14; 1	IPE Data Group	Plain; MACed	E1; 1F (hex)
2	13	Standard data file	64	14; 1	IPE Data Group	Plain; MACed	E1; 1F (hex)
1	14	Standard data file	64	14; 1	IPE Data Group	Plain; MACed	E1; 1F (hex)
0	15	Backup 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.

Note:

ShellFormatRevision = 1 is retained for backwards compatibility and is deprecated in this version of the Specification. All devices certified to this version of the Specification shall support ShellFormatRevision = 2.

Once all POST & HOPS devices within a supported scheme are certified to this version of the Specification, the associated Perso-POST device(s) shall only create CMD7 Shells with ShellFormatRevision = 2.

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	See note
FVC	7	See section 8.3

Table 61a - Fixed platform parameter values, SFR=2

Data element	Default value	Comment
ShellLength	68	If the optional MCRN is not presentIf the optional MCRN is present
ShellBitMap	msb-000001-lsbmsb-000011-lsb	If the optional MCRN is not presentIf the optional MCRN is present
ShellFormatRevision	2	See note
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 in Table 62 below. However, Shell Owners may override the default values with a permitted geometry as defined in Table 62a 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

Table 62a - Permitted data element values

Profile	B	S	E
Permitted Profile 1	64	16	8
Permitted Profile 2	80	16	8
Permitted Profile 3	128	16	8
Permitted Profile 4	140	16	8
Permitted Profile 5	160	16	8
Permitted Profile 6	180	16	8
Permitted Profile 7	200	16	8
Permitted Profile 8	220	16	8
Permitted Profile 9	240	16	8

Note:

Customer media certified to this version of the Specification shall only use supported profile geometries as defined in Table 62a. POST devices certified to this version of the Specification are permitted to support acceptance of Customer Media configured with alternate geometries certified to earlier versions of this Specification and using SFR=1.

Permitted Profile 1 indicates the original (default) DESfire geometry.

8.7.1.4.3 Shell Environment detailed layout

Table 63 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[34]	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).

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.

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

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'[35]	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

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

Note that the 13 files 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-1)[36] (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 Backup 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 and comply with the Permitted Profile values defined in Table 62a.

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

[36] Default value of E is 8

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.

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.

Note: As a standard practice, all deployed POSTS must utilise two records to ensure interoperability, irrespective of file size.

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 7816-5]. Only 3 bytes are available for coding of the AID, as opposed to the 6 to 16 bytes required by [ISO 7816-5] for a registration category 'A' AID[37].

The ITSO AID in accordance with [ISO 7816-5] 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, 16A 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.

[37] Which ITSO is

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.

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[38].

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)

[38] Showing the read of the entire Shell

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.

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[39].

[39] Showing the read of the entire Directory

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[40], 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.

8.11.2 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.

[40] A data frame can hold up to 59 bytes. See the Mifare DESFire specifiaction for further details

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[41].

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[42], 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.

[41] Showing the read of the entire IPE file

[42] 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[43].

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

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.

8.13.1.4 Response data

The response to the ReadData command for the entire Value Record file will consist of 2 data frames[44], 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.

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

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

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[45].

[45] Showing the read of an entire TT record of 48 bytes

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.

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[46], 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
- 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

[46] Where this is taken to mean the creation of the ITSO Shell on the customer media

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 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. CMD8 - RFU-Obsolete

Clause retained for numbering.

10. CMD9 - NTAG215/216 – NFC Forum Type 2 Tag compliant IC

10.1 General description

This clause briefly defines the NFC Forum Type 2 compliant IC before any customisation or adaptation by ITSO. The specific tags described in this clause are NTAG215/216 – NFC Forum Type 2 Tag compliant IC variants by NXP Semiconductors, however, you may wish to use any compatible NFC tag with similar specification.

NTAG215/216 are only appropriate for low-value products and should not be used for high-value items, such as Annual Passes. Additionally, space-saving IPEs (Types 27, 28, 29_1, and 29_2) must not be used on CMD9. For further information, consult the manufacturer's datasheet.

The NTAG215/216 – NFC Forum Type 2 Tag compliant IC variants are designed to fully comply with NFC Forum Type 2 Tag (NFC Forum Tag 2 Type Operation, Technical Specification — NFC Forum, 31/05/2011, Version 1.1) and ISO/IEC14443 Type A. Please refer to the technical specification for detailed information.

10.2 Data transfer rate

NTAG215/216 IC is positioned in the RF field, the high speed RF communication interface allows the transmission of the data with a baud rate of 106 kbit/s.

10.3 Pre-programmed security options

NTAG215/216 – NFC Forum Type 2 Tag compliant IC variants offer various manufactured programmed security options by default out of which only the following are relevant:

- A number of pre-programmed one time programmable bits
- 32-bit Password protected to prevent unauthorised memory operations
- Contactless transmission of data and supply energy
- Operating frequency of 13.56 MHz
- Data integrity of 16-bit CRC, parity, bit coding, bit counting
- Operating distance up to 100 mm (depending on various parameters as e.g. field strength and antenna geometry)
- 7-byte serial number (cascade level 2 according to ISO/IEC 14443-3)
- MID ASCII mirror for automatic serialization of NDEF messages
- Fast read command
- True anticollision
- 50 pF input capacitance

10.4 Memory features

10.4.1 NTAG215

- 540 bytes, organized in 135 pages of 4 byte per page
- 26 bytes reserved for manufacturer and configuration data
- 28 bits used for the read-only locking mechanism
- 504 bytes user programmable read/write memory
- Field programmable read-only locking function per page for the first 16 pages

- Configurable password protection with optional limit of unsuccessful attempts
- Anti-tearing support for OTP memory and lock bits
- Data retention time of 10 years
- Write endurance 100.000 cycles

10.4.2 NTAG216

- 924 bytes, organized in 231 pages of 4 byte per page.
- 26 bytes reserved for manufacturer and configuration data
- 37 bits used for the read-only locking mechanism
- 4 bytes available as capability container
- 888 bytes user programmable read/write memory
- Field programmable read-only locking function per page for the first 16 pages
- Configurable password protection with optional limit of unsuccessful attempts
- Anti-tearing support for OTP memory and lock bits
- Data retention time of 10 years
- Write endurance 100.000 cycles

10.5 Memory organisation

The EEPROM memory is organised in pages with 4 bytes per page. The figure below shows the memory mapping for NTAG215/216 – NFC Forum Type 2 Tag compliant IC variants.

Page Address								
NTAG215		NTAG216		**Byte number within a page**				
Dec	Hex	Dec	Hex	0	1	2	3	**Description**
0	0h	0	0h	serial number				Manufacturer data & static lock bytes
1	1h	1	1h	serial number				
2	2h	2	2h	serial number	internal	lock bytes	lock bytes	
3	3h	3	3h	Capability Container (CC)				Capability Container
4	4h	4	4h	user memory				User memory pages
5	5h	5	5h					
...	...	...	...					
128	80h	224	E0h					
129	81h	225	E1h					
130	82h	226	E2h	dynamic lock bytes			RFUI	Dynamic lock bytes
131	83h	227	E3h	CFG 0				Configuration pages
132	84h	228	E4h	CFG 1				
133	85h	229	E5h	PWD				
134	86h	230	E6h	PACK		RFUI		

Figure 3 - Memory organisation

10.5.1 Unique serial number

Each device has a 7 byte manufacturer defined unique ID. It's delivered as the MID during ISO/IEC 14443-3 anti-collision and can also be read from the first two memory pages.

10.5.2 Dynamic lock bytes

The dynamic lock bytes enable password protected updates to the memory beyond page 10 for NTAG215/216 variants. The dynamic lock bytes are located at page 82h for NTAG215 and at E2h for NTAG216. The three lock bytes cover the memory area of 456 data bytes.

10.5.3 OTP memory

Some are programmed during the IC production and therefore pre-configured by the manufacturer whereas the others are available for and used by ITSO.

10.5.4 Data pages

Pages 04h to E1h for NTAG215 and 04h to 81h for NTAG216 are the user memory read/write area. The access to a part of the user memory area can be restricted using a password verification.

10.5.5 Configuration pages

Pages E3h to E6h for NTAG215 whereas pages 83h to 86h for NTAG216 are used to configure the memory access restriction and to configure the MID ASCII mirror feature.

10.6 Password verification protection

NTAG215/216 both provide a 32-bit password mechanism to protect memory access and a password acknowledgement mechanism to help detect emulated cards.

10.7 NTAG commands

There are a number of NTAG commands prescribed by the manufacturer by default, however only those relevant to ITSO are outlined below. Please refer to NFC Forum Tag 2 Type Operation, Technical Specification — NFC Forum, 31/05/2011, Version 1.1 for further details and other commands.

Table 103 - NTAG Commands

Command	ISO/IEC 14443	NFC FORUM	Command code (Hex)
READ	-	READ	30h
FAST_READ	-	-	3Ah
WRITE	-	WRITE	A2h
PWD_AUTH	-	-	1Bh

10.7.1 READ

This command essentially reads four consecutive four-byte words from the device's memory.

10.7.2 FAST_READ

The command offers extended read capability to read larger memory blocks.

10.7.3 WRITE

The WRITE command requires a block address, and writes a single 4 bytes of data into the memory.

10.7.4 PWD_AUTH

This command must be performed before protected memory on the device can be accessed. Access is granted only after a successful password verification using the PWD_AUTH command. It is a password presentation and acknowledgement delivery.

Note that NTAG215/216 also supports other commands such as COMP_WRITE, READ_CNT and READ_SIG which are not relevant for ITSO implementation but may be of interest to the supplier.

10.8 Anti-collision

NTAG215/216 – NFC Forum Type 2 Tag compliant IC variants have an intelligent anti-collision function. The capability allows it to operate more than one tag in the field simultaneously. Media can be identified from parameters (SAK, ATQA, MID) collected during the media’s anti-collision and selection phase.

The SAK byte will be 0x000 indicating the cascade is complete and the device is not ISO/IEC 14443-4 compliant whereas the MID-length will be ’double size’ (7 bytes) with bit-3 of the bit-frame anti-collision value set. This can be recognized as ATQA = 0x0044.

Please refer to Identification cards — Contactless integrated circuit cards — Proximity cards, Part 3: Initialization and anticollision. ISO/IEC, 2016-06-01, BS ISO/IEC 14443-3, (3rd Edition), which prescribes how anti-collision is performed in principle. However, another option could be to convert the IPE to read only as opposed to write-with-password.

10.9 NTAG215/216 - NFC Forum Type 2 Tag compliant IC adaptation

10.9.1 Scope

This clause defines the CMD for platforms based on NTAG215/216 - NFC Forum Type 2Tag compliant IC. This platform is capable of supporting the full range of ITSO IPE types, Value Record groups and ITSO's Log file mechanism. However, due to restricted security, this platform shall be limited to the hosting of a single IPE instance.

10.9.2 Terminology

Throughout this clause reference will be made to terms defined within the NFC Forum Tag 2 Type operation, Technical Specification - NFC Forum, 31/05/2011, Version 1.1, where applicable. Please refer to the technical specification for further details.

10.9.3 Platform capability

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

• Shell Environment	*With all optional elements present*
• Directory	*Two instances (Anti-tear support)*
• IPE	*One instance*
• Value Record	*May be associated with IPEs subject to overall memory limits*
• Cyclic Log	*Support for Basic and Normal mode logging*

10.9.4 ISO/IEC 14443 compliance

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

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

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

10.9.5 Format Version Code

Platforms that conform to this CMD shall use the Format Version Code (FVC) of 09.

10.9.6 Definition support

This definition supports One IPE and both Basic and Normal Logs.

- Permitted Shell Geometries
- Sector mapping to Addresses
- ITSO data structure mapping to Sectors

10.10 CMD 9 Media

10.10.1 ITSO Shell properties

The tables below summarises the ITSO shell organisation of CMD9 on NTAG215/216 – NFC Forum Type 2 Tag compliant IC variants. See clause 10.4 and 10.11.3 for more details on each property.

Table 104 - Shell properties

		NTAG215	**NTAG216**
Property	**Shell Parameter**	**Value**	**Value**
Format Revision Code	FVC	9	9
Key Strategy Code	KSC	1	1
Key Version Code	KVC	1	1
Sector Chain Table Length	SCTL	3	3
ITSO Block Size	B	64	128
Sector Count	S	9	9
Directory Entries	E#	2	2

10.10.2 Memory Mapping

The figures below provide a memory mapping overview of NTAG215/216 – NFC Forum Type 2 Tag compliant IC variants. Please refer to clause 10.4 and 10.11.3 for more details on each property.

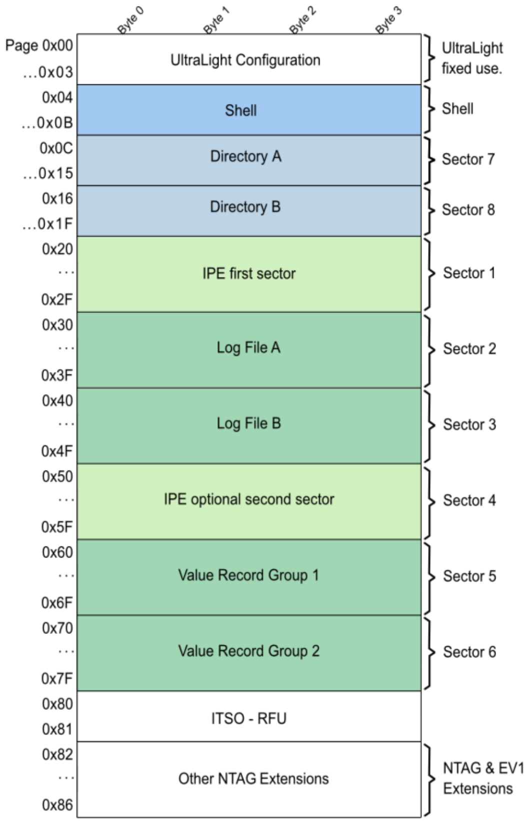


Figure 4.1 - NTAG215

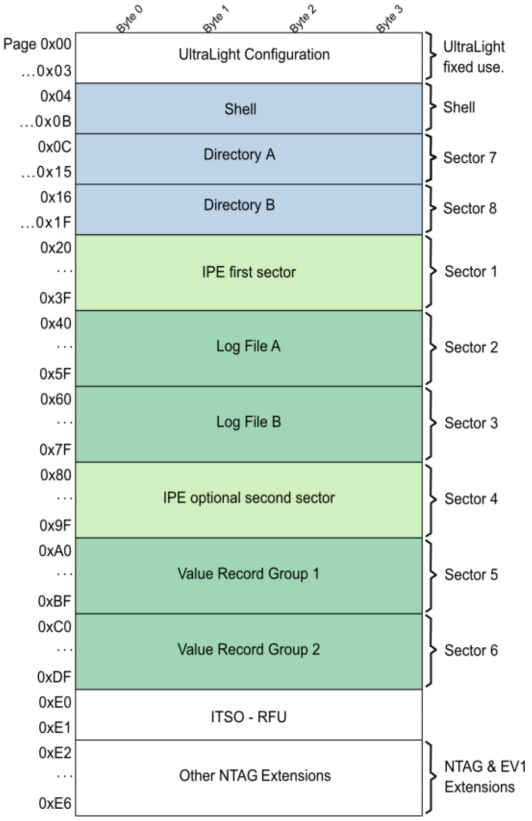


Figure 4.2 - NTAG216

10.11 CMD 9

10.11.1 Scope

This clause 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 components are described only in terms of their interfaces, where applicable.

10.11.2 Platform capability

This platform is capable of supporting a full ITSO shell as defined in ITSO TS 1000-2. The supported Data Groups and all optional elements are stated 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)

10.11.3 ITSO control structures

This CMD has the full data structure which shall be found at fixed address and the shell environment data group shall be mapped to page 0x04. The sector contents of the shell (page 0x04 to 0x0B) shall rotate to allow the FVC (0x06 in Byte 2) to align with the same address as FVC definitions within the same chip family which makes FVC identification quicker for POSTs.

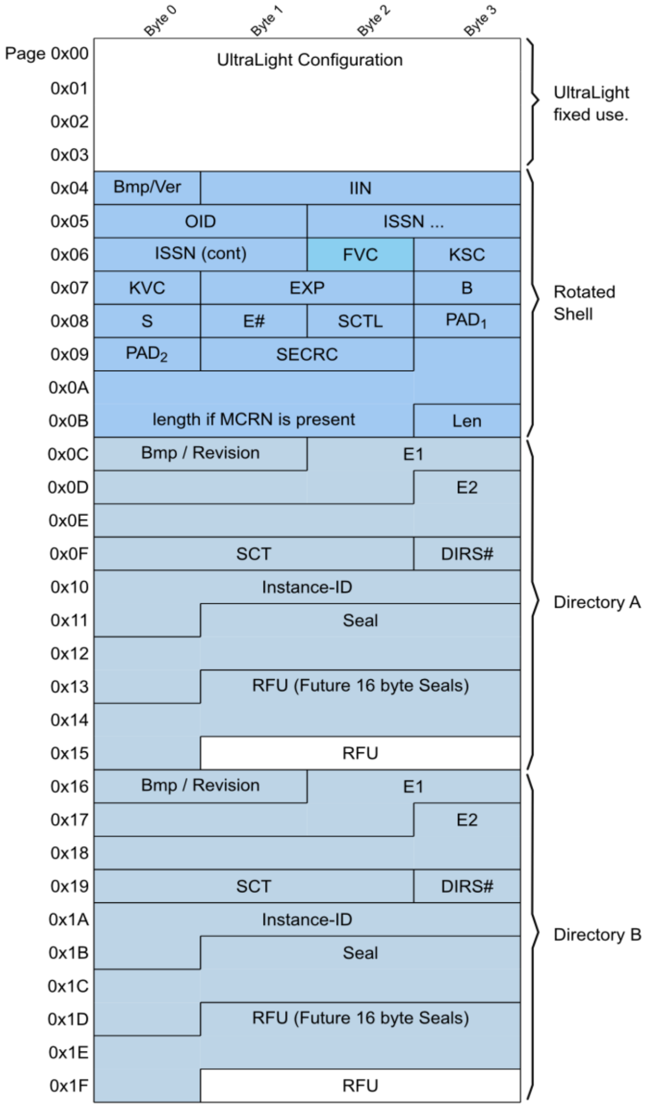


Figure 5 - Control structure

The ITSO logical sectors are not ordered sequentially in memory, see Figure 4.1 and 4.2. The ITSO Shell Environment Data Group and Directory Data Group are placed adjacent to each other and at the low end of the address map to ensure that the same data will be at the same address across all members of this family of media (CMDs 4, 9 & 10). Only the IPE/Log storage sectors have variable physical addresses.

The said arrangement also puts the memory allocated for ITSO's logical sectors at a 16 (0x10) page boundary. The dynamic Lock bytes protection mechanism (password protected updates to the memory beyond 0x10 on NTAG215/216 variants) works on 16 page blocks. This ensures that each sector can be locked independently.

The Shell length and most significant two bits of the bitmap field occupy a single byte. This part of the bitmap always equals zero and the Shell length value can be inferred from the section of bitmap found in the second byte of the Shell. The first byte of the Shell structure can therefore be omitted as its value can be inferred from the remaining data. If there is no MCRN present then the first byte of the Shell will be 0x18, if MCRN is present the first byte will be 0x20.

The omitted Shell Len byte has been copied to the end of the Shell storage block. Thus a POST can reconstruct the expected Shell data without needing to infer it from theBmp/Ver field. The intention is to future proof the structure and assist POSTs in case future versions of the Shell structure result in shells of alternative sizes. The Shell component is large enough to support the optional MCRN field.

The Directories are fixed size supporting two entries; one IPE and one Log. Fixed size deliberately restricts the platform to two entries thus preventing extending the capacity of this platform. It also optimises the read time for POSTs and simplifies the logic for determining which of the pair is the active copy and which is the backup copy.

10.11.4 Platform parameters with fixed values

The platform parameter data elements within the ITSO Shell Environment Data Group shall have the fixed values specified herein for all implementations of this CMD. Shading in Table 105 indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Table 105 - Platform parameters

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	9	Format Version Code for this CMD
KSC	1	For this version of the Specification
B	64 128	Size of logical sector For NTAG215 For NTAG216
S	9	This gives a Ψ of 4
E	2	Number of Directory Entries
SCTL	3	Length of Sector Chain Table

Note:

The number of bits needed to encode the SCT data element. The default value of Ψ is 4 for this CMD. If an alternate Ψ is used, then the SCT value(s) shall be adjusted accordingly (as defined in ITSO TS 1000 -2).

10.11.5 Overriding default platform parameter values

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

10.12 FVC/KSC/KAS in POST application

This CMD shall use the Key Strategy Code (KSC) value as defined in clause 10.11.4. The ISAM shall use this to determine the appropriate cryptographic processes to be applied to such media platforms.

For each combination of the values of FVC and KSC shown in ITSO TS 1000-8 Annex C Table C1, the POST application shall use the Key Aliases (KAS) shown as stored in the CM Codes Table for each command listed in column 2 of ITSO TS 1000-8 Annex C, Table C1.

The ISAM shall mechanise the diversification and cryptographic algorithms in accordance with the value of the key flags as listed in ITSO TS 1000-8 Annex C Table C1.

10.13 FVC/KSC/KAS in PERSO-POST application

For each combination of the values of FVC and KSC shown in ITSO TS 1000- 8 Annex C Table C2, the PERSO/POST application shall use the Key Aliases (KAS) shown as stored in the CM Codes Table for each command listed in column 2 of ITSO TS 1000-8 Annex C, Table C2. The ISAM shall mechanise the diversification and cryptographic algorithms in accordance with the value of the key flags as listed in Access Keys Table as shown in ITSO TS 1000-8 Annex C Table C2.

10.14 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 whereas all pages that have not been locked shall have password protected write access.

The PWD and PACK blocks are write-only. PWD defines the password required to gain access to the media’s memory. The PACK defines a value to be returned in acknowledgement of a successful password presentation.

10.15 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).

10.16 Delivered conditions

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

— Page 0 MID and BCC0

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

10.17 POST-issue conditions

After the ITSO Shell Environment, Directory and IPE Data Groups have been loaded onto the media as per Figure 4.1 (NTAG215) and Figure 4.2 (NTAG216).

10.18. 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;

10.19 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 106 - Manufacturer's ID

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

10.19.1 Verification of the serial number

POSTs shall verify that the serial number data in pages 0 and 1 corresponds to the MID (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 MID data.

10.20 Detection of the ITSO Shell

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

- If a NTAG215/216 platform is detected then the POST shall read page 6.
- The POST shall read and confirm that all required data Elements have the specified values. If this check passes then this is a strong suspicion that an ITSO Shell of FVC = 09 is present.
- The trust relationship for IPEs and directories is still subject to confirmation of seals by the ISAM.

10.21 Benchmark transaction

10.21.1 IPE with Transient Ticket creation

The benchmark transaction for this CMD shall comprise:

- Detection of a platform carrying a valid ITSO Shell with FVC = 09 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.

10.21.2 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 = 09 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 the 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…)

10.22 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 = 09, then it shall use ITSO Shell Referencing as defined in ITSO TS 1000-3.

10.23 Configuration pages

The device provides memory access protection through several configuration registers. In particular, they define the area of memory requiring password verification before access is permitted; the permitted number of password failures before the media will lock itself; and access control to the configuration pages themselves.

To the effect of this media definition (CMD 9), the specific configurations of each register is described below.

10.23.1 Static Lockbytes (NTAG215/216)

This controls access to the first 32 bytes of the tag.

The bits of byte 2 and byte 3 of page 02h as shown in Figure 3 represent the field programmable read-only locking mechanism. Each page from 03h (CC) to 0Fh can be individually locked by setting the corresponding locking bit Lx to logic 1 to prevent further write access. After locking, the corresponding page becomes read-only memory.

Recommended settings:

(Page 2, bytes 2 & 3) = F70F. The pages 4...B should be Locked because it contains the shell and it never changes.

Pages C...F holds part of the first directory and therefore should be modifiable, therefore 0xF00F. No changes should be made to these lock bytes. 0x07000xF00F+0x0700=F70F.

The default value of the static lock bytes is 00 00h. Any write operation to the static lock bytes is tearing-proof.

10.23.2 Dynamic lock bytes

This permits all the pages to be modified such as the Dirs, IPE, VRDGs, & Log. It also prevents the modification of these lock bits. However, operators may choose to lock some of the pages. For example, if an operator issued a period pass, the IPE body will not change. It could safely be locked to further resist attempts to invalidate or recycle media.

The dynamic lock bytes are located at page 82h for NTAG215 and at page E2h for NTAG216. These lock bytes cover the memory area of 456 data bytes for NTAG215 and 840 data bytes for NTAG216.

Recommended settings:

(Page 0x82 / 0xE2, bytes 0,1,2) = 0x00000F / 0x00007F.

The default value of the dynamic lock bytes is 00 00 00h. The value of Byte 3 is always BDh when read. Any write operation to the dynamic lock bytes is tearing-proof.

10.23.3 CFG0/CFG1 configurations

Pages 83h to 86h for NTAG215 and pages E3h to E6h for NTAG216 are used to configure the memory access restriction.

Recommended settings (CFG0)(Page 0x83 / 0xE3, bytes 0...3)= 0x0000000C. This translates to all pages above page 12 (0x0C) requiring password permission to modify them.

Recommended settings (CFG1)

(Page 0x84 / 0xE4, bytes 0...3)= 0x47000000 (Locking the configuration, 0x40000000)

Password retry limit = max value of 7, 0x07000000 (0x40000000 + 0x07000000 = 0x47000000)

10.24 POST behaviour

10.24.1 Media recognition

Anti-Collision shall be performed upon placing the media on the POST which shall result in the collection of three essential elements of information described as follows:

- **SAK:** 8 bits of data indicating the completion of the anti-collision cascade and the communication protocol supported by this medium.
- **ATQA:** 16 bits of data indicating proprietary data and the size of the MID.
- **MID:** The Unique Identifier assigned to this medium by the manufacturer.

If the SAK byte bit b6 = 0, and the ATQA word equals 0x0044 then the media is likely to be a member of the UltraLight Family.

The media shall go through further clearing process by using READ command which is common to all members of the UltraLight Family. Byte 2 of Page 6 (See Figure 5) indicates the FVC of the medium’s Shell. This value is used to establish which CMD type to be used for further processing. Note however that this test may give a false-positive in the case of non-ITSO media and it is important to verify the full details of the Shell before relying on this observation.

10.24.2 Media verification

The POST will read and verify the integrity of the Shell.

The POST will identify the most recent directory, and verify its integrity via the ISAM.

A single execution of the UltraLight FAST READ command (see Table 103) with StartPage = 0x04 and EndPage = 0x1F can be used to retrieve the Shell and directories (see Figure 5). The SECRC value of the Shell on page 0x09 should be verified before selecting the medium as being a genuine ITSO medium.

The POST must read the Abacus (Table 107) to determine if the medium is already blocked or retired. However, this can only be executed after the Shell has been read because the Abacus location changes with NTAG215/216 hardware.

Note that the ISAM commands for BEGIN and WDIR will be used as per normal ITSO media to validate the authenticity of the medium.

10.24.3 IPE verification

The process of IPE verification on the medium is carried out in the usual way whereby the sectors containing the IPE and Log are pointed via the directory's SCT, see ITSO TS 1000-2 clause 2.4.3.
This media definition mandates one further step when verifying VRDGs. The Transaction Sequence Number (TS#) of the latest Value Record (VR) must be greater than or equal to the number represented by the Abacus value.

10.24.4 Use of ITSO Abacus

The abacus is stored in the OTP memory of NTAG215/216 media.

The abacus has 16 bits formed by the concatenation of byte 1 and byte 3 from memory Page 0x03 of the medium. The initial delivery state of raw media gives an initial Abacus value of 0x1000. See Table 107 for abacus values and the states they represent.

Table 107 - ITSO Abacus

Abacus				
OTP1	***OTP3***	***HEX***	***TS#***	***Remaining Uses***
00010000	00000000	1000	1	14
10010000	00000000	9000	2	13
11010000	00000000	D000	3	12
11110000	00000000	F000	4	11
11111000	00000000	F800	5	10
11111100	00000000	FC00	6	9
11111110	00000000	FE00	7	8
11111111	00000000	FF00	8	7
11111111	10000000	FF80	9	6
11111111	11000000	FFC0	10	5
11111111	11100000	FFE0	11	4
11111111	11110000	FFF0	12	3
11111111	11111000	FFF8	13	2
11111111	11111100	FFFC	14	1
11111111	11111110	FFFE	15	0
11111111	11111111	FFFF	16	Retired

To accommodate future variants of NTAG that may contain differing initial values for bytes 1 & 3 the State value is calculated by counting the number of bits set in the two bytes. This gives a maximum life of a product as 14 uses. After 14 uses the abacus will indicate a VR with TS#=15. At the end of the last journey permitted by the product the POST should advance the abacus value to 16 (Retired).

Scheme operators should not use State 15 to indicate the 15th use of the product because POSTs will recognize state 16 as retired and will therefore not be able to validate the IPE mid-journey, making inspection impossible.

10.24.5 VRG read and verification

The interpretation of Value Records and their manipulation is performed in the usual ITSO IPE/VRDG processing but with an additional requirement that the abacus is updated to reflect the up-to-date TS# value. The abacus must be updated immediately once the modification VRDG and directory have been written to the medium. This sequence ensures consistency and safe method in the event of card tear during the update process.

10.24.5.1 VRG writing

This media type shall hold a single full-sized ITSO Product Entity (IPE) along with its value groups. When creating a new VRDG, the ISAM ensures that the TS#=0. Writing such a VRDG onto the media would contradict the assertion that the TS# must be greater than or equal to the Abacus's value. Therefore, when creating an IPE containing VRDGs, one or more empty MODIFY_VALUE_IPE actions may need to be executed to synchronise the latest TS# with the Abacus. The TransactionType 00 (Not Specified) must be used for such empty operations.

The messages to the HOPS relating to the creation of the IPE shall indicate a TransactionType 00 and TS#=x. These may be accompanied by additional messages assigning value to the VRDG where the TS#=x+1. At this point, the TS# equals the Abacus value and it can be written to the medium. Upon reception of a Create IPE Transaction Record message (with TransactionType 00), the HOPS shall accept the TS# value presented as the initial value for monitoring consecutive transactions.

To avoid unnecessary increments of the Abacus counter, it is recommended that the new IPEs are created with any relevant initial value before being written to the medium.

10.25 Password/key

The WDIR will not only reseal the directory but it will also return keys that are diversified by Manufacturer's Identification Number (MID) + ISRN.

The first 4 bytes of the first returned key are used as the media write PWD whereas the fifth and sixth bytes are used as the PACK value (see clause 10.14). This means that the POST will receive the medium's write key if, and only if, it performs an action that will update the directory. These actions are creating an IPE and updating a VRDG or the Log records.

11. CMD10 - Mifare Ultralight EV1 (Extended Memory) MF0UL51

Throughout this clause reference will be made to terms defined within the NXP Mifare® Ultralight EV1 - Contactless ticket IC MF0UL51 Data Sheet (11 April 2014).

11.1 General description

This clause briefly defines the CMD for platforms based on the Mifare Ultralight EV1 MF0UL51 by NXP Semiconductors prior to any customisation or adaptation by ITSO.

The Mifare Ultralight EV1 MF0UL51 is designed to work in an ISO/IEC14443 Type A compliant environment. Please refer to the technical specification for detailed information. The target applications include single trip or limited use tickets in public transportation networks or loyalty cards and is intended for low-value single use products.

11.2 Data transfer rate

The MF0UL51 chip allows the transmission of the data with a baud rate of 106 kbit/s.

11.3 Pre-programmed security options

The MF0UL51 provides the following security-related options by default:

- Manufacturer programmed 7-byte MID for each device
- 32-bit user definable One-Time programmable (OTP) area
- 3 independent 24-bit true one-way counters
- Field programmable read-only locking function per page (per 2 pages for the extended memory section)
- ECC based originality signature
- 32-bit password protection to prevent unintended memory operations
- Data integrity of 16-bit CRC, parity, bit coding, bit counting
- Operating distance up to 100 mm (depending on various parameters as e.g. field strength and antenna geometry)
- 7-byte serial number (cascade level 2 according to ISO/IEC 14443-3)
- True anticollision

11.4 Memory features - EEPROM

- 924 bytes organized in 231 pages with 4 bytes per page
- 888 bytes freely available user Read/Write area (222 pages)
- First 512 bits compatible to MF0ICU1
- Field programmable read-only locking function per page for the first 512 bits
- Field programmable read-only locking function per 16 pages above page 15
- 32-bit user definable One-Time Programmable (OTP) area
- 3 independent, true one-way 24-bit counters on top of the user area
- Anti-tearing support for counters, OTP area and lock bits
- Configurable password protection with optional limit of unsuccessful attempts
- ECC based originality signature

- Data retention time of 10 years
- Write endurance 100,000 cycles
- Write endurance for one-way counters 1,000,000 cycles

11.5 Memory organisation

The EEPROM memory is organised in pages with 4 bytes per page. The MF0UL51 has 231d pages in total. The memory organisation can be seen in Figure 6 below.

Figure 6 - Memory organisation MF0UL51

Page Address		Byte number within a page				
Dec	Hex	0	1	2	3	**Description**
0	0h	serial number				Manufacturer data & static lock bytes
1	1h	serial number				
2	2h	serial number	internal	lock bytes		
3	3h	OTP	OTP	OTP	OTP	One Time Programmable
4	4h	user memory				User memory pages
5	5h					
...	...					
224	E0h					
225	E1h					
226	E2h	lock bytes			RFUI	Lock bytes
227	E3h	CFG0				Configuration pages
228	E4h	CFG1				
229	E5h	PWD				
230	E6h	PACK		RFUI		
		One-way counters (only accessible with READ_CNT & INCR_CNT commands)				Counter pages

11.5.1 Unique serial number

The unique 7-byte serial number (MID) and its two check bytes are programmed into the first 9 bytes of memory covering page addresses 00h, 01h and the first byte of page 02h. It is delivered as the MID during ISO/IEC 14443-3 anti-collision and can also be read from the first two memory pages.

11.5.2 Lock bytes

11.5.2.1 Lock byte 0 and byte 1

The bits of byte 2 and byte 3 of page 02h represent the field programmable read-only locking mechanism. Each page from 03h (OTP) to 0Fh can be individually to prevent further write access.

11.5.2.2 Lock byte 2 to byte 4

To lock the pages of the MF0UL51 starting at page address 10h onwards, the lock bytes 2-4 located in page E2h are used. Those three lock bytes cover the memory area of 840 data bytes. The granularity is generally 16 pages, compared to a single page for the first 512 bits. The last two pages of the user memory on addresses E0h and E1h are locked with a single locking bit.

11.5.3 OTP memory

Some are programmed during the IC production and therefore pre-configured by the manufacturer whereas the others are available for and used by ITSO. Any write operation to the OTP bytes features anti-tearing support.

11.5.4 Data pages

Pages 04h to E1h of the MF0UL51 are the user memory read/write area. The access to a part of the user memory area can be restricted using a password verification.

11.5.5 Configuration pages

Pages E3h to E6h of the MF0UL51 are used to configure the memory access restriction of the ML0UL51.

11.5.6 Counter functionality

The MF0UL51 features three independent 24-bit one-way counters. These counters are located in a separate part of the NVM which is not directly addressable using READ, FAST_READ, WRITE or COMPATIBILITY_WRITE commands.

11.6 Password verification protection

The MF0UL51 provides a 32-bit secret password mechanism to protect memory access and a password acknowledgement mechanism to help detect emulated cards.

11.7 Mifare Ultralight EV1 commands

There are a number of MF0UL51 commands prescribed by the manufacturer by default. However, only those relevant to ITSO are outlined below – see Table 108 below. Please refer to NXP Mifare® Ultralight EV1 - Contactless ticket IC MF0UL51 Data Sheet (11 April 2014) for further details regarding other commands.

Table 108 – Mifare Ultralight EV1 Commands

Command	ISO/IEC 14443	NFC FORUM	Command code (Hex)
READ	-	READ	30h
FAST_READ	-	-	3Ah
WRITE	-	WRITE	A2h
PWD_AUTH	-	-	1Bh
READ_CNT	-	-	39h
INCR_CNT	-	-	A5h

11.7.1 READ

This command essentially reads four consecutive four-byte words from the device's memory.

11.7.2 FAST_READ

The command offers extended read capability to read larger memory blocks.

11.7.3 WRITE

The WRITE command requires a block address and writes a single 4 bytes of data into the memory.

11.7.4 PWD_AUTH

This command must be performed before protected memory on the device can be accessed. Access is granted only after a successful password verification using the PWD_AUTH command. It is a password presentation and acknowledgement delivery.

Note that MF0UL51 also supports other commands such as COMP_WRITE, READ_CNT and READ_SIG which are not relevant for ITSO implementation but may be of interest to the supplier.

11.7.5 READ_CNT

The READ_CNT command is used to retrieve the actual counter value.

11.7.6 INCR_CNT

This command is used to increment the counters.

11.8 Anti-collision

MF0UL51 has an intelligent anti-collision function. The capability allows it to operate more than one tag in the field simultaneously. Media can be identified from parameters (SAK, ATQA, MID) collected during the media's anti-collision and selection phase.

The SAK byte will be 0x00 indicating the cascade is complete and the device is not ISO/IEC 14443-4 compliant whereas the MID-length will be ’double size’ (7 bytes) with bit-3 of the bit-frame anti-collision value set. This can be recognized as ATQA = 0x0044.

Please refer to Identification cards — Contactless integrated circuit cards — Proximity cards, Part 3: Initialization and anticollision. ISO/IEC, 2016-06-01, BS ISO/IEC 14443-3, (3rd Edition), which prescribes how anti-collision is performed in principle. However, another option could be to convert the IPE to read only as opposed to write-with-password.

11.9 Mifare Ultralight EV1 Scope

This clause defines the CMD for platforms based on the MF0UL51 contactless ticket IC. This platform is capable of supporting the full range of ITSO IPE types, Value Record groups and ITSO's Log file mechanism.

11.9.1 Terminology

Throughout this clause reference will be made to terms defined within the NXP Mifare® Ultralight EV1 - Contactless ticket IC MF0UL51 Data Sheet - 11 April 2014, where applicable. Please refer to the technical specification for further details.

11.10 Platform Capability

11.10.1 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 Two instances (Anti-tear support)
- IPE One instance
- Value Record May be associated with IPEs subject to overall memory limits
- Cyclic Log Support for Basic and Normal mode logging

11.10.2 Memory architecture

The memory architecture of this platform is summarised below:

- 924 bytes of EEPROM, organised in 231 pages of 4 bytes each
- *8 bytes are reserved for manufacturer data*
- *37 bit used for the read-only locking mechanism*
- *32 bit available as OTP area*
- Storage capacity of 888 bytes is available for the ITSO Application
- *128 bytes are used for the ITSO Shell Environment and Directory Data Groups*
- *760 bytes are available for IPE instance, Value Record and Cyclic Log storage*

11.10.3 ISO/IEC 14443 compliance

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

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

11.11 Format Version Code

Platforms that conform to this CMD shall use the Format Version Code (FVC) of 10.

11.12 Definition support

This definition supports One IPE and both Basic and Normal Logs.

- Permitted Shell Geometries
- Sector mapping to Addresses
- ITSO data structure mapping to Sectors

11.13 ITSO Shell Environment Data Group

The elements and layout of this data structure are fully defined in ITSO TS 1000-2.

11.13.1 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 109– 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	10 (0A hex)	See section11.11
KSC	1	For this version of the Specification
B	128 (80 hex)	Size of memory Sector
S	9	This gives a Ψ of 4
E#	2	Number of Directory Entries
SCTL	3	Length of SCT

11.13.2 Memory Mapping

The figure below provides a memory mapping overview of the MF0UL51. Please refer to clause 11.5 for more details on each property.

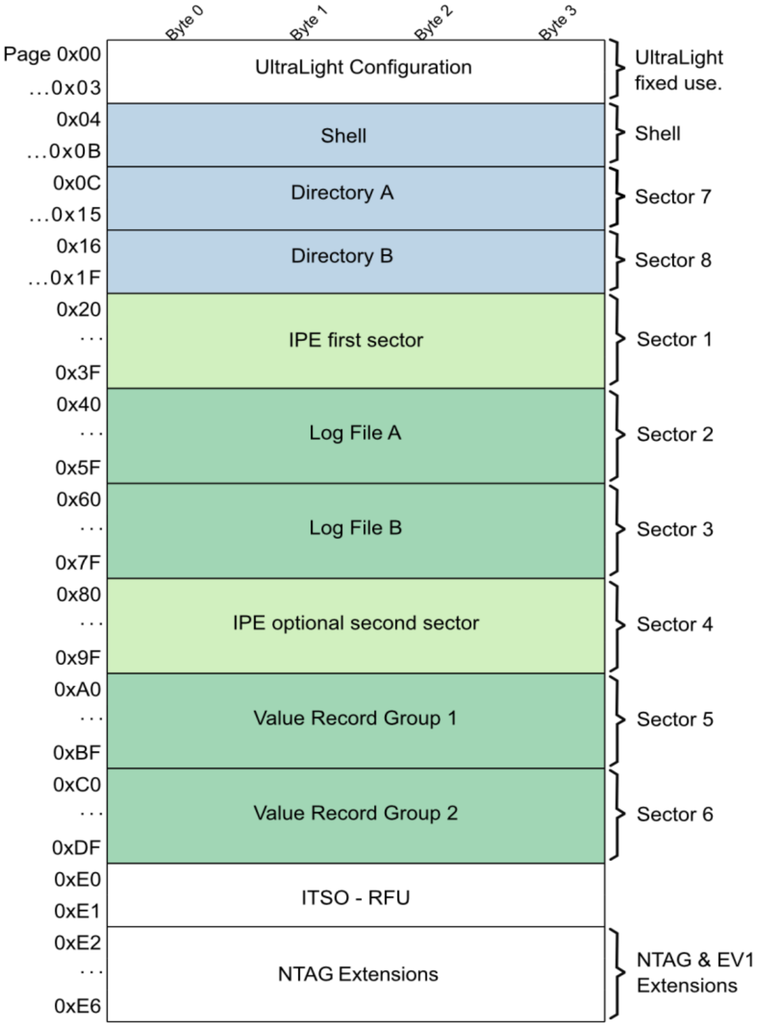


Figure 7 - Memory mapping

11.14 CMD 10

11.14.1 Scope

This clause 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 components are described only in terms of their interfaces, where applicable.

11.14.2 Platform capability

This platform is capable of supporting a full ITSO shell as defined in ITSO TS 1000-2. The supported Data Groups and all optional elements are stated 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)

11.14.3 ITSO control structures

This CMD has the full data structure which shall be found at fixed address and the shell environment data group shall be mapped to page 0x04. The sector contents of the shell (page 0x04 to 0x0B) shall rotate to allow the FVC (0x06 in Byte 2) to align with the same address as FVC definitions within the same chip family which makes FVC identification quicker for POSTs.

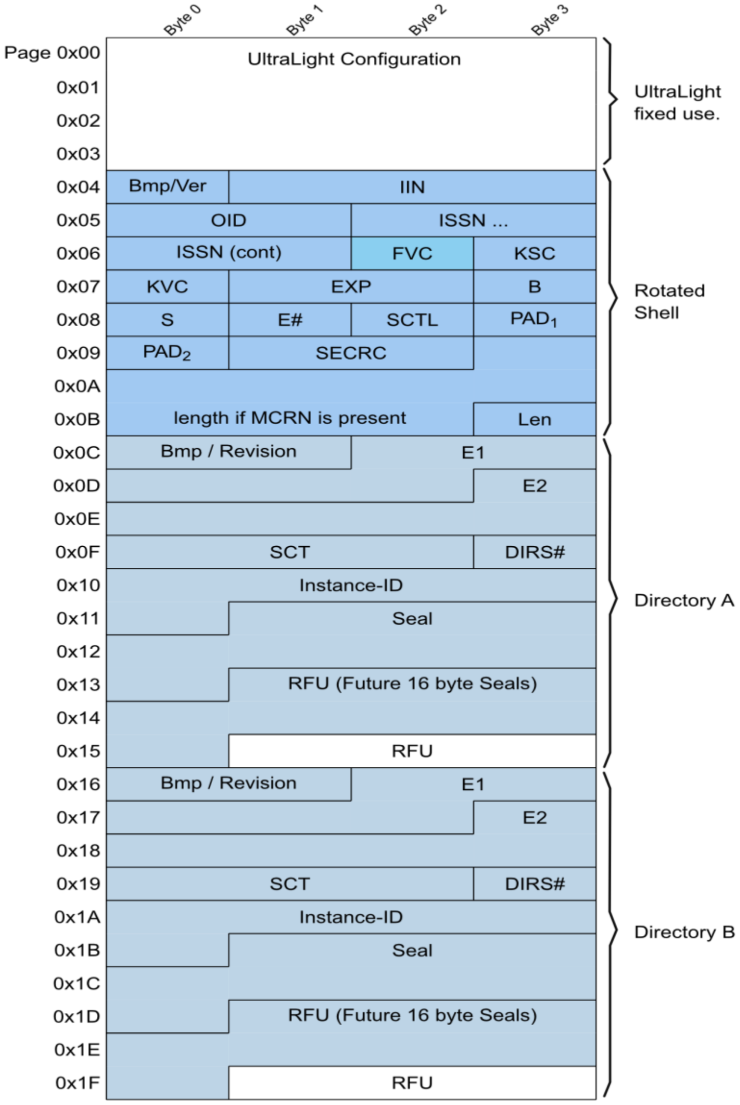


Figure 8 - Control structure

Note the ITSO logical sectors are not ordered sequentially in memory, see Figure7 .

The ITSO Shell Environment Data Group and Directory Data Group are placed adjacent to each other and at the low end of the address map to ensure that the same data will be at the same address across all members of this family of media (CMDs 4, 9 & 10). Only the IPE/Log storage sectors have variable physical addresses.

This arrangement puts the memory allocated for ITSO's logical sectors at a 16 (0x10) page boundary. The dynamic Lock bytes protection mechanism (password protected updates to the memory beyond 0x10 works on 16 page blocks. This ensures that each sector can be locked independently.

The Shell length and most significant two bits of the bitmap field occupy a single byte. This part of the bitmap always equals zero and the Shell length value can be inferred from the section of bitmap found in the second byte of the Shell. The first byte of the Shell structure can therefore be omitted as its value can be inferred from the remaining data. If there is no MCRN present then the first byte of the Shell will be 0x18, if MCRN is present the first byte will be 0x20.

The omitted Shell Len byte has been copied to the end of the Shell storage block. Thus a POST can reconstruct the expected Shell data without needing to infer it from the BMP/VER field. The intention is to future proof the structure and assist POSTs in case future versions of the Shell structure result in shells of alternative sizes. The Shell component is large enough to support the optional MCRN field.

The Directories are fixed size supporting two entries; one IPE and one Log. Fixed size deliberately restricts the platform to two entries thus preventing extending the capacity of this platform. It also optimises the read time for POSTs and simplifies the logic for determining which of the pair is the active copy and which is the backup copy.

11.14.4 Platform Parameters with fixed values

The platform parameter data elements within the ITSO Shell Environment Data Group shall have the fixed values specified herein for all implementations of this CMD. Shading in Table 110 indicates the main Data Structures and is as defined and used in ITSO TS 1000-2.

Table 110 - Platform parameters

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	10	Format Version Code for this CMD
KSC	1	For this version of the Specification
B	128	Size of logical sector
S	9	This gives a Ψ of 4
E	2	Number of Directory Entries
SCTL	3	Length of Sector Chain Table

Note:

The number of bits needed to encode the SCT data element. The default value of Ψ is 4 for this CMD. If an alternate Ψ is used, then the SCT value(s) shall be adjusted accordingly (as defined in ITSO TS 1000 -2).

11.14.5 Overriding default platform parameter values

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

11.15 FVC/KSC/KAS in POST application

This CMD shall use the Key Strategy Code (KSC) value as defined in clause 11.14.4. The ISAM shall use this to determine the appropriate cryptographic processes to be applied to such media platforms.

For each combination of the values of FVC and KSC shown in ITSO TS 1000-8 Annex C Table C1, the POST application shall use the Key Aliases (KAS) shown as stored in the CM Codes Table for each command listed in column 2 of ITSO TS 1000-8 Annex C, Table C1.

The ISAM shall mechanise the diversification and cryptographic algorithms in accordance with the value of the key flags as listed in ITSO TS 1000-8 Annex C Table C1

11.16 FVC/KSC/KAS in Perso-POST application

For each combination of the values of FVC and KSC shown in ITSO TS 1000-8 Annex C Table C2, the PERSO/POST application shall use the Key Aliases (KAS) shown as stored in the CM Codes Table for each command listed in column 2 of ITSO TS 1000-8 Annex C, Table C2.

The ISAM shall mechanise the diversification and cryptographic algorithms in accordance with the value of the key flags as listed in ITSO TS 1000-8 Annex C Table C2.

11.17 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 whereas all pages that have not been locked shall have password protected write access.

The PWD and PACK blocks are write-only. PWD defines the password required to gain access to the media’s memory. The PACK defines a value to be returned in acknowledgement of a successful password presentation.

11.18 Key strategy

This CMD shall use the Key Strategy Code (KSC) value as defined in clause 11.14.4. The ISAM shall use this to determine the appropriate cryptographic processes to be applied to such media.

11.19 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).

11.19.1 Delivered conditions

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

— Page 0 MID and BCC0
— Page 1 MID;
— Page 2 (bytes 0 and 1) BCC1 and reserved.

11.19.2 Post-issue conditions

After the ITSO Shell Environment, Directory and IPE Data Groups have been loaded onto the media as per Figure 6.

11.20 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;

11.21 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 111 – 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

11.21.1 Verification of the serial number

POSTs shall verify that the serial number data in pages 0 and 1 corresponds to the MID (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 MID data.

11.22 Detection of the ITSO Shell

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

- If a MF0UL51 platform is detected then the POST shall read page 6.
- The POST shall read and confirm that all required data Elements have the specified values. If this check passes then this is a strong suspicion that an ITSO Shell of FVC = 10 is present.
- The trust relationship for IPEs and directories is still subject to confirmation of seals by the ISAM.

11.23 Benchmark transaction

11.23.1 IPE with Transient Ticket creation

The benchmark transaction for this CMD shall comprise:

- Detection of a platform carrying a valid ITSO Shell with FVC = 10 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.

11.23.2 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 = 10 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 the 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…)

11.24 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 = 10, then it shall use ITSO Shell Referencing as defined in ITSO TS 1000-3.

11.25 Configuration pages

The device provides memory access protection through several configuration registers. In particular, they define the area of memory requiring password verification before access is permitted; the permitted number of password failures before the media will lock itself; and access control to the configuration pages themselves.

To the effect of this media definition (CMD10) the specific configuration of each register is described below.

11.25.1 Static Lockbytes

This controls access to the first 32 bytes of the tag.

The bits of byte 2 and byte 3 of page 02h as shown in Figure 6 represent the field programmable read-only locking mechanism. Each page from 03h (CC) to 0Fh can be individually locked by setting the corresponding locking bit Lx to logic 1 to prevent further write access. After locking, the corresponding page becomes read-only memory.

Recommended settings:

(Page 2, bytes 2 & 3) = F70F. The pages 4...B should be Locked because it contains the shell and it never changes.

Pages C...F holds part of the first directory and therefore should be modifiable, therefore 0xF00F. No changes should be made to these lock bytes. 0x07000xF00F+0x0700=F70F.

The default value of the static lock bytes is 00 00h. Any write operation to the static lock bytes is tearing proof.

11.25.2 Dynamic lock bytes

This permits all the pages to be modified such as the DIRs, IPE, VRDGs, & Log. It also prevents the modification of these lock bits. However, operators may choose to lock some of the pages. For example, if an operator issued a period pass, the IPE body will not change. It could safely be locked to further resist attempts to invalidate or recycle media.

The dynamic lock bytes are located at page E2h. These lock bytes cover the memory area of 840 data bytes

Recommended settings:

(Page 0x82 / 0xE2, bytes 0,1,2) = 0x00000F / 0x00007F.

The default value of the dynamic lock bytes is 00 00 00h. The value of Byte 3 is always BDh when read. Any write operation to the dynamic lock bytes is tearing-proof.

11.25.3 CFG0/CFG1 configurations

Pages E3h to E6h are used to configure the memory access restriction.

Recommended settings (CFG0)

(Page 0x83 / 0xE3, bytes 0...3)= 0x0000000C. This translates to all pages above page 12 (0x0C) requiring password permission to modify them.

Recommended settings (CFG1)

(Page 0x84 / 0xE4, bytes 0...3)= 0x47000000 (Locking the configuration, 0x40000000)

Password retry limit = max value of 7, 0x07000000 (0x40000000 + 0x07000000 = 0x47000000)

11.26 POST behaviour

The clause describes the process by which the media shall be verified by a POST.

11.26.1 Media recognition

Anti-Collision shall be performed upon placing the media on the POST which shall result in the collection of three essential elements of information described as follows:

- **SAK:** 8 bits of data indicating the completion of the anti-collision cascade and the communication protocol supported by this medium.
- **ATQA:** 16 bits of data indicating proprietary data and the size of the MID.
- **MID:** The Unique Identifier assigned to this medium by the manufacturer.

If the SAK byte bit b6 = 1 then the media supports the APDU based command protocol.

If the SAK byte bit b6 = 0, and the ATQA word equals 0x0044 then the media is likely to be a member of the UltraLight Family.

The media shall go through further clearing process by using READ command which is common to all members of the UltraLight Family. Byte 2 of Page 6 (See Figure 8) indicates the FVC of the medium’s Shell. This value is used to establish which CMD type to be used for further processing. Note however that this test may give a false-positive in the case of non-ITSO media and it is important to verify the full details of the Shell before relying on this observation.

11.26.2 Media verification

The POST will read and verify the integrity of the Shell.

The POST will identify the most recent directory and verify its integrity via the ISAM.

A single execution of the UltraLight FAST READ command with StartPage = 0x04 and EndPage = 0x1F can be used to retrieve the Shell and directories (see Figure 8). The SECRC value of the Shell on page 0x09 should be verified before selecting the medium as being a genuine ITSO medium.

The POST must read the counter to determine if the medium is already blocked or retired. However, this can only be executed after the Shell has been read because the counter location changes with MF0UL51 hardware.

Note that the ISAM commands for BEGIN and WDIR will be used as per normal ITSO media to validate the authenticity of the medium.

11.26.3 IPE verification

The process of IPE verification on the medium is carried out in the usual way whereby the sectors containing the IPE and Log are pointed via the directory's SCT, see ITSO TS 1000-2 clause 2.4.3.

This media definition mandates an additional step when verifying Value Record Data Groups (VRDGs). The Transaction Sequence Number (TS#) of the latest Value Record (VR) must be greater than or equal to the number represented by the Counter.

11.26.4 Use of one-way counter #1

The MF0UL51 features three independent 24-bit one-way counters. These counters are located in the Counter pages in a separate part of the NVM which is not directly addressable using READ, FAST_READ, WRITE or COMPATIBILITY_WRITE commands.

The actual value can be retrieved by using the READ_CNT command. The counters can be incremented with the INCR_CNT command. The INCR_CNT command features anti-tearing support, thus no undefined values originating from interrupted programming cycles are possible. Either the value is unchanged or the correct, incremented value is correctly programmed into the counter. The occurrence of a tearing event can be checked using the CHECK_TEARING_EVENT command.

In the initial state, the counter values are set to 000000h. If the counter reports 0xFFFFFF then the medium has been retired and is no longer valid. This can be achieved by reading the current value of counter #1 (READ CNT), inverting the value (i.e. xor with 0xFFFFFF) and using this number as the increment value for INCR CNT command.

The maximum life of a product shall be at the discretion of the Product Owner and governed or stipulated by the product business rules.

Scheme operators should take note and not use State 0xFFFFFF to indicate the final use of the product because POSTs will recognize the 0xFFFFFF state as retired and will therefore not be able to validate the IPE mid-journey, making inspection impossible.

11.26.5 VRG read and verification

The interpretation of Value Records and their manipulation is performed in the usual ITSO IPE/VRDG processing but with an additional requirement that the counter #1 is updated to reflect the up-to-date TS# value. The counter must be updated immediately once the modification VRDG and directory have been written to the medium. This sequence ensures consistency and safe method in the event of card tear during the update process.

The process of IPE verification on the medium is carried out in the usual way whereby the sectors containing the IPE and Log are pointed via the directory's SCT, see ITSO TS 1000-2 clause 2.4.3. This media definition mandates one further step when verifying VRGs. The TS# of the latest VR must be greater than or equal to the number represented by the Counter.

11.26.5.1 VRG writing

This media type shall hold a single full-sized ITSO Product Entity (IPE) along with its value groups.

To prevent the replaying of old products on this medium, the TS# value must be synchronised with the value of the medium’s Counter. When this medium is being re-used, this Counter may not necessarily be zero. In this case, the TS# of a newly created VRDG shall need to be advanced to match the value held in the Counter. This can be achieved by executing one or more MODIFY_VALUE_IPE actions until the respective counters are equal. The TransactionType 00 (Not Specified) must be used for such empty operations.

The messages to the HOPS relating to the creation of the IPE shall consist of the following:

- The IPE creation message (0005).
- Optionally, an IPE owner IPE creation message with TransactionType 00 (Not Specified) and the relevant value for TS#. The HOPS shall accept this TS# value as the starting point for monitoring consecutive transactions. In the absence of this message the initial value of TS# shall be zero.

- Optionally, an Amend IPE Transaction Record message indicating the addition of value to the VRDG.

11.27 Password/key

The WDIR will not only reseal the directory but it will also return keys that are diversified by Manufacturer's Identification Number (MID) + ISRN.

The first 4 bytes of the first returned key are used as the media write PWD whereas the fifth and sixth bytes are used as the PACK value. This means that the POST will receive the medium's write key if, and only if, it performs an action that will update the directory. These actions are creating an IPE and updating a VRDG or the Log records.

12. CMD11 - ITSO Programmable Intelligent Media (PIM)

12.1 Scope

This clause defines programmable intelligent media for microprocessor-based platforms. The design of this CMD allows for the hosting of an ITSO specific Application on a single or multi-application microprocessor-based CM platform that:

— Supports the standard ISO/IEC 7816-4;

— Compliance to the standard ISO/IEC 14443-3;

— Supports application selection via AID

This medium supports all ITSO functions currently supported by CMD2 and CMD7. These key functions and features are:

1. ITSO data structures - Maintain compatibility with ITSO data structures for Shell Environment Data Group (Shell), Directory (Dir), IPE, and Transient Ticket Record (TTR).
2. Mutual Authentication - Provide proof of identity and resistance to cloning.
3. Secure Messaging - Provide proof of message integrity, but not necessarily secrecy.
4. Transaction Protection - Guarantee that incomplete message exchanges can be detected, either by the POST and the media. Additionally, incomplete transactions must not leave the medium in an indeterminate state.
5. Application Clash - The same instance of the application should be selectable via more than one Application Identifier (AID). This will enable compatibility with Proximity Payment System Environment (PPSE) or Ticket Reader Interface Protocol (TRIP) like mechanisms in future
6. More memory capacity
7. Improved transaction speed
8. Enhanced security
9. No additional hardware costs

12.1.1 Terminology

Throughout this clause reference will be made to terms defined within ISO/IEC 7816-4 and ISO/IEC 14443-3.

12.2 Platform capability

12.2.1 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	*One directory with hardware 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.*

12.2.2 Security requirements

This CMD shall be capable of using Advanced Encryption Standard (AES) and modern MAC algorithms should be adopted.

The temporary co-existence with the current ISAM means that the application shall also work with Data Encryption Standard (DES) and basic CBC MAC algorithms.

All ITSO transactions, whether they are just checking a card, marking the TTL or manipulating an IPE, must read the Shell and Dir. Mutual Authentication (MA) between CM and ISAM is always required in order to ensure the data transferred is live as opposed to a replay of recorded data.

12.2.3 Application Family Identifier usage

ISO/IEC 14443-3 provides support for 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 (0x10 hex) is recommended.

POSTs shall not assume that media uses AFI coding, and shall default to using the Select All code of 0x00 (hex).

12.2.4 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 and / or Type B requirements;
- Part 3: Initialisation & anticollision Compliance with ISO/IEC 14443 Type A and / or Type B requirements;
- Part 4: Transmission protocol Compliance with ISO/IEC 14443 Type A and / or Type B requirements.

12.3 Format Version Code

Platforms that conform to this CMD shall use the Format Version Code (FVC) of 0x0B (11).

12.4 Media Command set

These commands are defined by ISO/IEC 7816-4. The following APDU/command set shall be used within the Live environment. The detailed usage of these commands will be defined in subsequent sections of this document.

Table 112 - APDUs

Command	CLA	INS	P1	P2		Data	Description
Select	0x00	0xA4	0x04	0x00	⇒ ⇐ ⇐	ITSO AID FCI Status Word	A0000002164954534f2d3100 TLV structured data
Authenticate	0x90	0x10	0x00	0x00	⇒ ⇒ ⇐ ⇐	Response Challenge Response Status Word	ISAM's response to the CM's challenge ISAM's challenge to the CM CM's response to the ISAM's challenge
ReadIPE	0x90	0x12	ipe#	0x00	⇒ ⇐ ⇐	IPE Status Word	Read length = *Lc*. *Lc* = 0 is the size of the IPE and its seal. If issued prior to establishing a secure session, the CMD 11 applet will redact the IPE InstanceID and

							Seal (a total of 16 bytes), replacing them with 0xFF to prevent digital fingerprinting and unauthorised tracing. After mutual authentication and during a secure session, the correct IPE InstanceIDand Seal will be returned to allow successful IPE verification.
ReadVRG	0x90	0x14	ipe#	0x00	⇒ ⇐ ⇐	VRG Status Word	VRG data indicated by *Lc* If issued prior to establishing a secure session, the CMD 11 applet will redact the IPE InstanceID and Seal (a total of 16 bytes), replacing them with 0xFF to prevent digital fingerprinting and unauthorised tracing. After mutual authentication and during a secure session, the correct Value Record InstanceID and Seal will be returned to allow successful Value Group verification.
ReadLog	0x90	0x16	0x00	0x00	⇒ ⇐ ⇐	TTL Status Word	Log data indicated by *Lc*
UpdateIpe	0x90	0x18	ipe#	0x00	⇒ ⇒ ⇐	password data Status Word	Sector Password Data to write at offset
UpdateVrg	0x90	0x1A	ipe#	0x00	⇒ ⇐ ⇐	password data Status Word	Sector Password Data to write
UpdateLog	0x90	0x1C	0x00	0x00	⇒ ⇐ ⇐	password data Status Word	Sector Password Data to write
UpdateDir	0x90	0x1E	0x00	0x00	⇒ ⇐ ⇐	password data Status Word	Sector Password Data to write
EndSession	0x90	0x20	0x00	0x00	⇒ ⇐ ⇐	ts ccs Status Word	POST and ISAMs calculated TS value CM's CCS
Reselect	0x90	0x22	0x00	0x00	⇒ ⇐ ⇐	FCI Status Word	Reselection, FCI update TLV structured data

12.4.1 Selection

Selection shall be via the standard ITSO AID. The CM shall respond to a SELECT() command with Tag-Length-Value (TLV) formatted File Control Information (FCI), see 12.4.6 for details. The tagged data elements are described below.

12.4.2 Media using static MIDs

For media using a static MID, the FCI shall be composed of the following mandatory components:

- C0: **Shell** — This is the medium’s unique Shell. Along with the MID (retrieved during anti-collision), and Tag C5 (Challenge), it forms part of the MA exchange.
- C1: **Capabilities** -The value of zero here indicates that the default command set is supported. All other values are reserved for future extensions to this CM.
- C2: **Dir** — The directory indicates the medium’s state, i.e. Whether the Shell is Blocked or Active, what IPEs are present, and their state, Virgin, Used, or Expired. This enables a POST to quickly decide if the medium is of interest. Its presence here pre-empts the need for the POST to issue a separate command to retrieve this data.
- C3: **OID List** — This list removes the need to read the IPEs when looking for candidate IPEs to use in a transaction.
- C4: **MAC** — This data enables a POST to quickly determine the medium’s end state after a card tear
- C5: **Challenge** — This data replaces the need to perform a GETCHALLENGE() APDU when starting the MA exchange.

12.4.3 Media using random MIDs

For media using a random MID, the FCI will be composed of the following mandatory components:

- C0 : **Pseudo-Shell** — This is a shared constant Shell structure to be used in a first level MA.
- C1 : **Capabilities** — Zero for this specification indicating that the default command set is supported. All other values are reserved for future extensions to this CM
- C2 : **Dir** — The directory indicates the medium’s state, i.e. Whether the Shell is Blocked or Active, what IPEs are present, and their state, Virgin, Used, or Blocked. This enables a POST to quickly decide if the medium is of interest. Its presence here also pre-empts the need for the POST to issue a separate command to retrieve this data.
- C3: **OID List** —This list removes the need to read the IPEs when looking for candidate IPEs to use in a transaction.
- C4 : **MAC** — This data enables a POST to quickly determine the medium’s end state after a card tear
- C5 : **Challenge** — This data replaces the need to perform a GETCHALLENGE() APDU when starting the MA exchange
- C6 : **Pseudo-MID** — This is a constant value to use in place of the MID in the first level MA process

The **Pseudo-Shell**, **Pseudo-MID** and **Challenge** will be used as components in an ISAM BEGIN command and enable MA to proceed between the ISAM and the medium. This secure session will be generic for media issued by a particular operator.

The **MAC**’s presence shall ensure the efficient tear detection mechanism is not compromised by the use of random MIDs.

A new RESELECT command is only executable from within a secure session, and will deliver a replacement FCI. This replacement FCI will be composed of the following mandatory components.

- C0 : **Shell** — This is the medium's unique Shell. Along with the Tag C8 (MID) and Tag C5 (Challenge), it forms part of the MA exchange.
- C2 : **Dir** — The directory indicates the medium's state, i.e. Whether the Shell is Blocked or Active, what IPEs are present, and their state, Virgin, Used, or Blocked. This enables a POST to quickly decide if the medium is of interest. Its presence here also pre-empts the need for the POST to issue a separate command to retrieve this data.
- C3 : **OID List** — This list removes the need to read the IPEs when looking for candidate IPEs to use in a transaction[47].
- C5 : **Challenge** — This data replaces the need to perform a GETCHALLENGE() APDU when starting the MA exchange.
- C7 : **MID** — The real unique identifier for this medium.

The Shell, MID and Challenge will be used as components in an ISAM BEGIN() command and enable MA to proceed between the ISAM and the medium. This secure session will be medium specific. The ITSO sealed structures on the medium are bound to this medium by keys generated by this re-selection process.

Table 113 - FCI tag summary

Tag	Element	Description
C0	**Shell**	The Shell is required to identify the CMD and for presentation to the ISAM as part of the BEGIN() command.
C1	**Capabilities**	A data structure that indicates the commands supported by the medium. When/if new commands are introduced in future, POSTs may choose to use either the old way or the new way.
C2	**Dir**	The Dir is required to identify Shell and IPE states. It is also passed to the ISAM for processing via the VERIFY_ITSO() command and a necessary step in any ITSO transaction.
C3	**OID List**	This is a list of the 16-bit OIDs of the entries within the DIR. The DIR's 'E' records only uniquely identify 13-bit OIDs. Longer OIDs assigned to other operators can only be determined after the IPE's Instance ID has been recovered.
C4	**MAC**	The MAC of the last session. In the unlikely event of a tear during an ENDSESSION() command this value uniquely identifies the last successful transaction to the POST. A POST may then discover whether the recent torn transaction was committed or rolled back.
C5	**Challenge**	If the CM is of interest to the POST then MA will need to be performed to establish a Secure Channel (SC). This data replaces the need to perform a GETCHALLENGE() APDU when starting the MA exchange.
C6	**Pseudo-MID**	An eight byte constant value used by the operator for all of their CMD11 media. This tag is only present in the FCI if the medium uses Randomised MIDs and is used to indicate the two-pass authorization process is required.
C7	**MID**	The real unique identifier for this medium. This tag is only ever returned by the RESELECT() command.

[47] Where multiple IPEs using the same "OID + TYP + PTYP" combination coexist on a single medium, for example, Single trip rail tickets, it may still be necessary to read their contents to determine which one amongst the set of candidates is the appropriate one to use.

12.4.4 Authentication and Secure Channel Management

A single AUTHENTICATE() command shall receive the POST's response to the CM's challenge, issued within the SELECT()'s FCI response, and a reciprocal challenge from the POST. The reply data shall be the CM's response to the POST's challenge.

After a successful MA an ephemeral SC key shall be constructed by both parties.

Individual MACs do not need to be appended to each APDUs. Instead, both parties maintain their own version of the session's MAC and a transaction is terminated by both parties agreeing on the final MAC value.

The session MAC covers all the APDUs and responses, including the status words, exchanged between the POST and the CM, starting with the first APDU after a positive outcome of the mutual authentication. A Secure Hash Algorithm (SHA), SHA-256, of the exchanged data is calculated and this hash is signed by the ISAM to generate a Transaction Signature (TS). The TS is delivered in the ENDSESSION command. This mechanism reduces the ISAM communication overhead associated with the alternative secure messaging protocols. The POST can calculate the session MAC and only one exchange with the ISAM is required to generate the TS and prove the integrity of the whole exchange. Data corruption shall be detectable when the CM fails to verify the TS and all of the session's updates shall be rolled-back in this scenario.

The ENDSESSION command, if successful, shall reply with a signature of the TS. This Committal Confirmation Signature (CCS) is a simple encryption of the TS and is quick to perform and verify via the ISAM. It is calculated using the Session Key, and only returned if the TS was successfully verified. The CCS indicates to the POST that the CM has committed the data and efficiently neutralises attacks based in delaying the committal of a transaction.

If the ENDSESSION command itself is torn then the POST shall receive no response. In this scenario the POST needs to determine whether the transaction was committed or rolled-back by the CM. To accelerate recovery from this scenario, the CCS of the last transaction is included in the SELECT() command's FCI response. This provides a fast mechanism for a POST to reacquire a torn CM and identify if the recently torn transaction had completed prior to the tear event.

The precise mechanisms used in the Session Key derivation and the underlying cryptographic algorithm remain unknown to the POST. The Keys and algorithm are identified in the Shell parameters and mutually understood by the CM and ISAM. The algorithm can be updated in future without affecting the required behaviour of the POST. Early incarnations of this CM shall use the mechanisms implemented in the current generation of ISAMs. Future versions of this CM are not restricted to this limited set of options.

12.4.5 Transaction Management

All media updates shall be cached and only applied after the receipt of an ENDSESSION() command.

When processing the ENDSESSION() command, the CM shall compare the delivered TS with an internally calculated version of the same. If they match, it shall generate the CCS and commit the proceeding memory updates to Non-Volatile Memory (NVM).

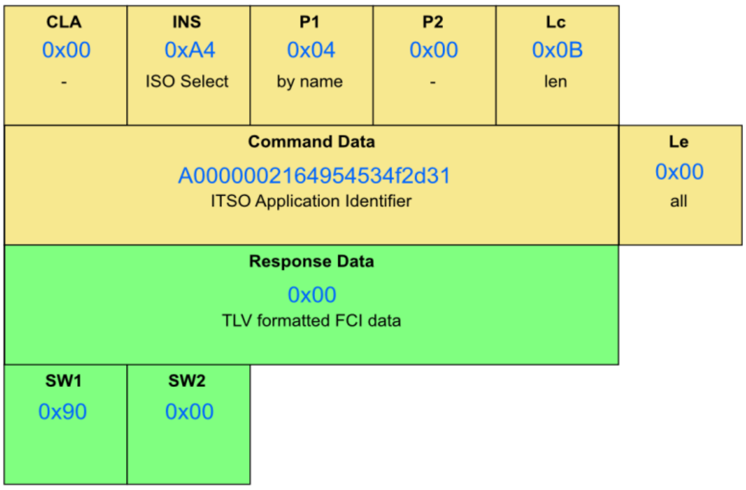
Any corrupt APDUs, missing APDUs, or additional APDUs, cryptographic failures, or incomplete exchanges shall result in the CM being unmodified.

ENDSESSION() shall invalidate the session keys and the application shall await reselection. If a tear occurs during the processing of ENDSESSION() then the POST shall not receive confirmation of either success or failure. To discover whether a transaction needs to be repeated the CCS from the last successful ENDSESSION() is included in the FCI response. A POST can reselect the application and by checking this value it shall discover if the transaction needs to be repeated or was complete. In the absence of a tear, the ENDSESSION() shall respond with the CCS and the POST can confirm either success or failure. Success does not require reverification via the reselection mechanism.

This CCS in the FCI mechanism can also be used to detect the continued presence of a CM. This mechanism is a more reliable substitute for the use of the CM's MID, which may be random on some CM.

12.4.6 Select

This command selects the application using the ITSO AID, [A0, 00, 00, 02, 16, 49, 54, 53, 4f, 2d, 31, 00].



CLA	INS	P1	P2	Lc
0x00 -	0xA4 ISO Select	0x04 by name	0x00 -	0x0B len

Command Data	Le
A0000002164954534f2d31 ITSO Application Identifier	0x00 all

Response Data
0x00 TLV formatted FCI data

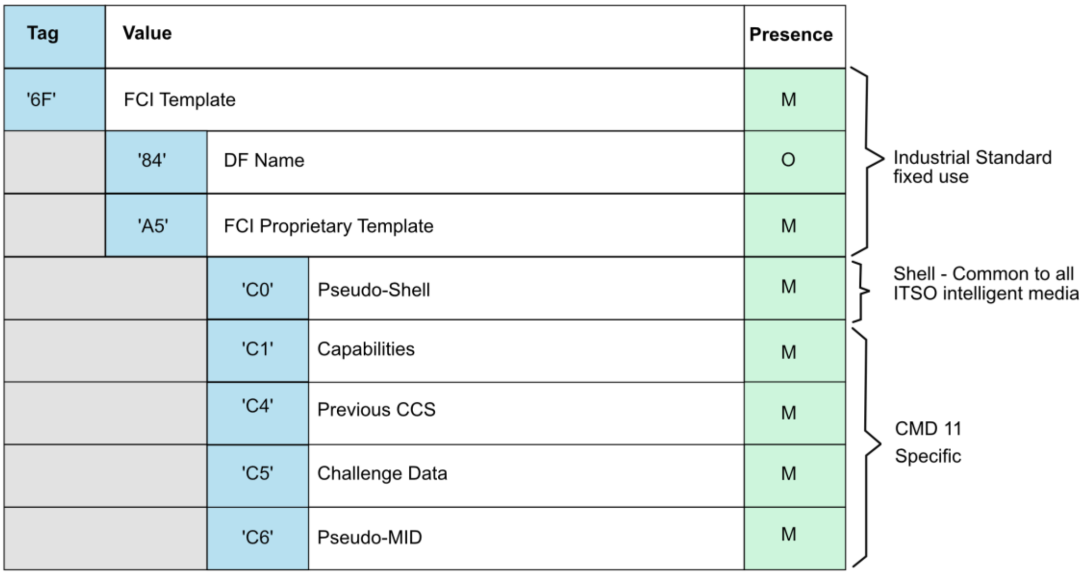
SW1	SW2
0x90	0x00

The command as defined by ISO/IEC 7816-4.

The returned FCI data is mandatory and its contents are defined here below. If the medium uses a static MID then the data shown in Figure 9 - FCI Data Structure (Static MID) will be returned. If the medium uses a random MID then the data shown in Figure 10 - FCI Data Structure (Random MID) will be returned. The latter variant contains no static information that would potentially identify the card holder.

This application shall respond to the same SELECT APDU as CMD2 and CMD12. Thus, the caller can distinguish the CM type from the Shell within the FCI response. Therefore, this media definition does not add additional command and polling delays to the existing POST behaviour.

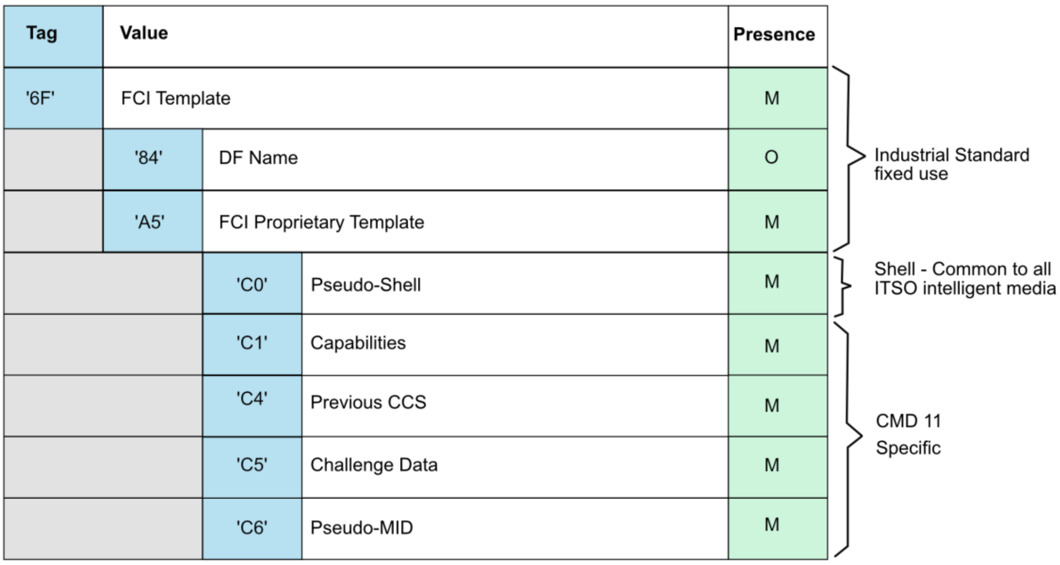
All fields are mandatory for this definition. See clause 12.4.2 for details on components required for static MIDs and clause 12.4.3 for random MIDs.



Tag	Value				Presence
'6F'	FCI Template				M
	'84'	DF Name			O
	'A5'	FCI Proprietary Template			M
		'C0'	Pseudo-Shell		M
		'C1'	Capabilities		M
		'C4'	Previous CCS		M
		'C5'	Challenge Data		M
		'C6'	Pseudo-MID		M

Industrial Standard fixed use
Shell - Common to all ITSO intelligent media
CMD 11 Specific

Figure 9 - FCI Structure (Static MID)



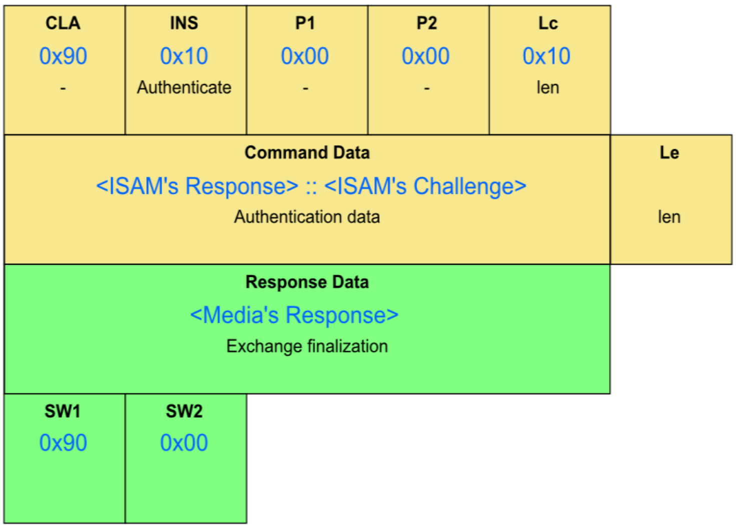
Tag			Value	Presence
'6F'			FCI Template	M
	'84'		DF Name	O
	'A5'		FCI Proprietary Template	M
		'C0'	Pseudo-Shell	M
		'C1'	Capabilities	M
		'C4'	Previous CCS	M
		'C5'	Challenge Data	M
		'C6'	Pseudo-MID	M

Industrial Standard fixed use
Shell - Common to all ITSO intelligent media
CMD 11 Specific

Figure 10 - FCI Structure (Random MID)

12.4.7 Authenticate

The ISAM’s Response is the value returned by the ISAM when processing the BEGIN() command.



CLA	INS	P1	P2	Lc
0x90	0x10	0x00	0x00	0x10
-	Authenticate	-	-	len

Command Data	Le
<ISAM's Response> :: <ISAM's Challenge> Authentication data	len

Response Data
<Media's Response> Exchange finalization

SW1	SW2
0x90	0x00

The ISAM’s Challenge is returned as part of the same processing. The two 8-byte fields are aligned in the same way as they are delivered from the ISAM; the POST does not need to process or restructure this data when passing it from the ISAM to the CM. The Media’s Response is the value to be delivered to the ISAM via the EXTERNAL_AUTHENTICATE() command.

After completing this command, the CM will construct the ephemeral Session Key. The CM’s internal session hash accumulator is initialised at this point. The data, both received and sent, for all subsequent APDUs, up until a the ENDSESSION() command will be added to this hash accumulator. If the POST intends writing to the CM it must mirror this behaviour and calculate its own version of the session hash. The hash algorithm used is SHA-256 [5].

12.4.8 ReadIPE

P1 indicates the IPE to be read; range 1 . . . *E − 1*.

CLA	INS	P1	P2	Lc	Le
0x90	0x12	NN	0x00	--	0x00
-	ReadIpe	IPE #	-	absent	len = all

Response Data
<IPE>
The full contents of the IPE with its seal.

SW1	SW2
0x90	0x00

The returned data comprises the concatenation of the IPE's five byte directory entry, the IPE body & its Instance ID with Seal. This is the same data structure that the POST shall need to construct for delivery to the ISAM prior to verifying the seal.

The size of the IPE data body is determined from the Length field present in byte zero of all IPEs.

Partial read is not supported because there are no circumstances that require it. The historical need to quickly read just the OID data has been removed by its inclusion in the FCI.

If issued prior to establishing a secure session, the CMD 11 applet will redact the IPE InstanceID and Seal (a total of 16 bytes), replacing them with 0xFF to prevent digital fingerprinting and unauthorised tracing.

After mutual authentication and during a secure session, the correct IPE InstanceIDand Seal will be returned to allow successful IPE verification.

12.4.9 ReadVRG

P1 indicates the IPE whose VRG is to be read; range 1 . . . *E − 1.*

CLA	INS	P1	P2	Lc	Le
0x90	0x14	NN	0x00	--	0x00
-	ReadVrg	IPE #	-	absent	len = all

Response Data
<VRG>
The full contents of the VRG with its seal.

SW1	SW2
0x90	0x00

The behaviour of this command is the same as that of the READIPE() command. The returned data is pre-formatted ready for presentation to the ISAM for verification.

This definition supports one VRG per IPE. It uses the familiar CMD7 mechanism of a single VRG holding up to four VRs and an optional single Value Group Extension (VGX). This simplified mechanism takes advantage of the medium's hardware memory transaction protection to simplify the record processing.

If issued prior to establishing a secure session, the CMD 11 applet will redact the IPE InstanceID and Seal (a total of 16 bytes), replacing them with 0xFF to prevent digital fingerprinting and unauthorised tracing.

After mutual authentication and during a secure session, the correct IPE InstanceIDand Seal will be returned to allow successful IPE verification.

12.4.10 ReadLog

The LOG holds 5×48 byte transaction records. They are sorted by the medium and returned in age order, newest record first.

CLA	INS	P1	P2	Lc	Le
0x90	0x16	N	0x00	--	0x00
-	ReadLog	Record count	-	absent	len = all

Response Data
<LOG>
multiple 48 byte records.

SW1	SW2
0x90	0x00

P1 expects a record count value in the range 1 . . . 5.

- 1 returns the single most recent 48 byte record.
- 2 returns the most recent and its immediate predecessor.
- etc up to 5, where all five of the LOG's transaction records are returned, sorted in increasing age order.

12.4.11 UpdateIPE

P1 indicates the IPE to be updated; range 1 . . . E − 1.

CLA	INS	P1	P2	Lc
0x90	0x18	NN	00	XX
-	UpdateIpe	IPE #	-	8 + IPE Data length

Command Data	Le
<Password> :: <IPE>	--
The sector password and the sector contents. Writes the IPE #NN.	absent

SW1	SW2
0x90	0x00

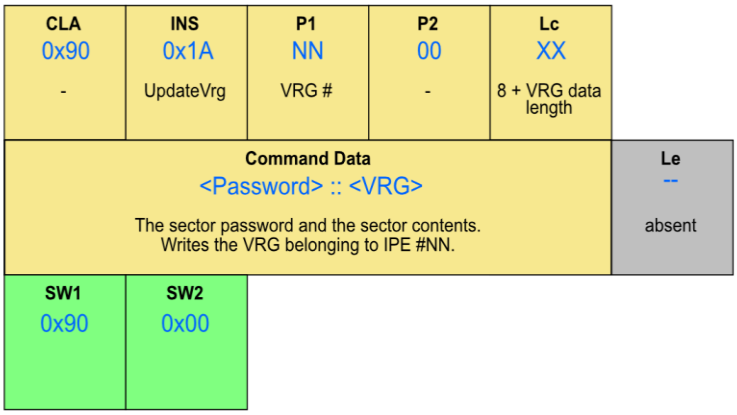
The sector password, concatenated with the IPE and its seal, is delivered to the medium is this single command. Inclusion of the sector password corresponding to the directory entry number helps guard against accidental overwriting of the wrong IPE.

The update itself will not occur until the end of the session. Thus, multiple updates of IPEs, VRGs, LOG records and the Dir may be sent to the medium to be committed on-mass; all or nothing. This atomic update prevents the scenario of partial updating of data prior to a card tear and leaving the medium in a logically inconsistent state.

Combining the password delivery with the IPE's data limits the maximum size of an IPE, including its seal to 247 bytes. The maximum size of the IPE itself is therefore 231 bytes after accounting for the InstanceID and Seal components. This limit is not considered to impose any realistic limitations on range of practical IPE definitions.

12.4.12 UpdateVRG

P1 indicates the IPE whose VRG is to be updated; range 1 . . . E − 1



CLA	INS	P1	P2	Lc
0x90	0x1A	NN	00	XX
-	UpdateVrg	VRG #	-	8 + VRG data length

Command Data	Le
<Password> :: <VRG>	--
The sector password and the sector contents. Writes the VRG belonging to IPE #NN.	absent

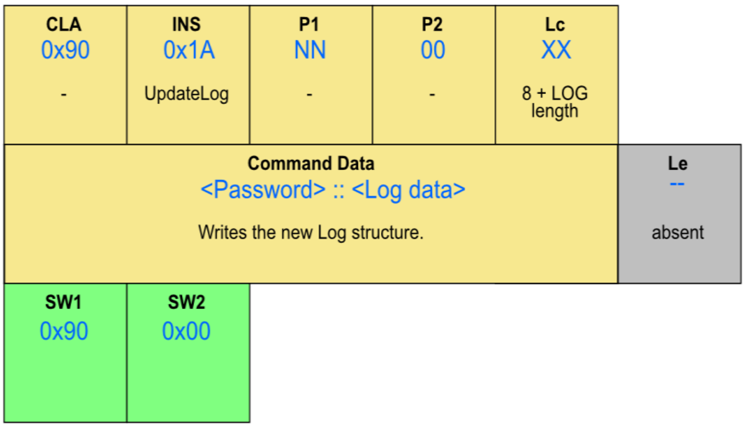
SW1	SW2
0x90	0x00

The command behaviour is the same as that of UPDATEIPE(). The single VRG shall be replaced as part of the transaction protected atomic update.

With the exception of the IPE state transitions (Virgin ⇒ Used ⇒ Expired), this mechanism means the Dir does not always need to be updated after a VRG update.

12.4.13 UpdateLog

The LOG data consists of up to 48 bytes, making 8 ≤ Le ≤ 58.7



CLA	INS	P1	P2	Lc
0x90	0x1A	NN	00	XX
-	UpdateLog	-	-	8 + LOG length

Command Data	Le
<Password> :: <Log data>	--
Writes the new Log structure.	absent

SW1	SW2
0x90	0x00

The new data is added to the LOG as the first (most recent) record. The old records 1 . . . 4 are copied to the new records 2 . . . 5 and the old record 5 is lost. This process maintains the chronological ordering of the records and maintains an efficient structure for the READLOG() command to process.

The Password, for sector No. E# is used for this command.

12.4.14 UpdateDir

This command updates the Dir record. The mechanism is the same as the UPDATEIPE() & UPDATEVRG() commands.

<table>
<tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th></th></tr>
<tr><td>0x90
-</td><td>0x1E
UpdateDir</td><td>00
-</td><td>00
-</td><td>XX
8 + DIR length</td><td></td></tr>
<tr><td colspan="5">Command Data
<Password&gt; :: &lt;Directory&gt;
Writes the new Directory to the media.</td><td>Le
--
absent</td></tr>
<tr><td>SW1
0x90</td><td>SW2
0x00</td><td></td><td></td><td></td><td></td></tr>
</table>

The Password, for sector No. E# + 1, is used for this command.

12.4.15 EndSession

<table>
<tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th></th></tr>
<tr><td>0x90
-</td><td>0x20
EndSession</td><td>0x00
-</td><td>XX
0: Normal
1: Debug</td><td>0x08
len</td><td></td></tr>
<tr><td colspan="5">Command Data
<Transaction Signature (TS)>
Session key signature of the MAC of the session’s APDU</td><td>Le
0x08
len</td></tr>
<tr><td colspan="5">Response Data
<Committal Confirmation Signature (CSS)&gt;
Session key signature of &lt;TS&gt;</td><td></td></tr>
<tr><td>SW1
0x90</td><td>SW2
0x00</td><td></td><td></td><td></td><td></td></tr>
</table>

The Session MAC is the SHA256 [5] of the APDU data transmitted since the secure session was established; (not including this command). Transaction Signature (TS) is the session key signature of this MAC. Committal Confirmation Signature (CCS) is the session key signature of TS. If the CCS returned by this command matches the value calculated via the ISAM, the transaction was successful.

All memory updates from this session shall be committed if the medium verifies TS. On verification failure, all updates shall be lost/aborted. The CCS value provides proof that the updates were performed.

The P2 value of 1 makes this command deliver the Hash of the preceding transaction. This feature enables developers to verify their Hash calculation. Doing so breaks the secure session and aborts any pending memory updates.

12.4.16 Reselect

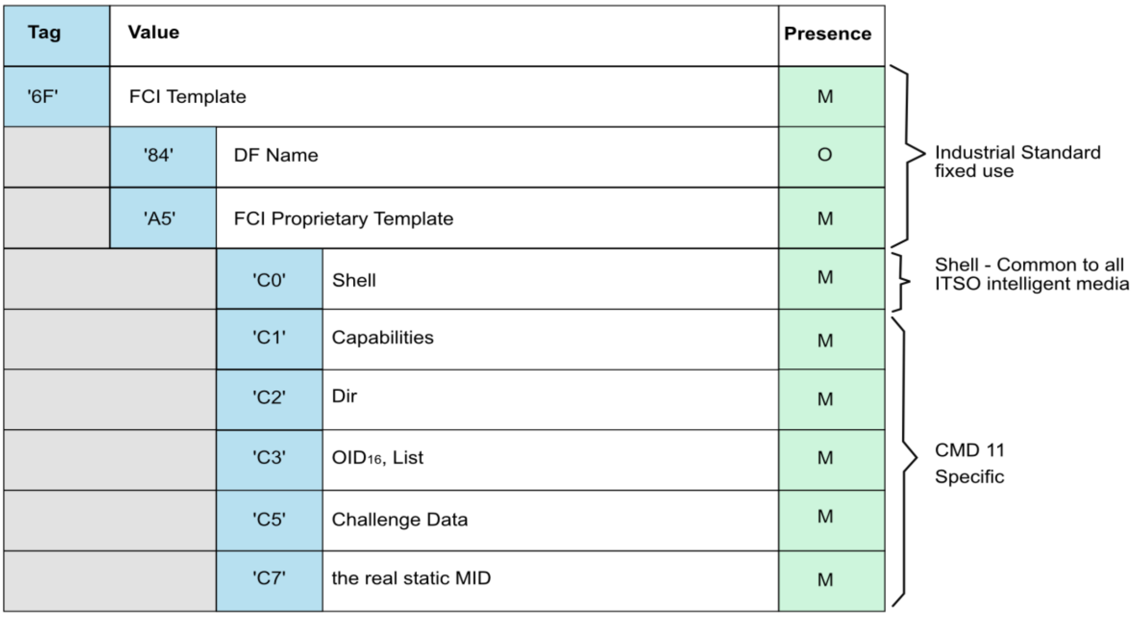
CLA	INS	P1	P2	Lc	Le
0x90	0x22	00	0x00	--	0x00
-	Reselect	-	-	absent	all

Response Data
--
TLV formatted FCI data

SW1	SW2
0x90	0x00

This command only works after successful completion of MA.

The primary use of this command is for media that use random MIDs. The initial session, established using the pseudo-Shell and pseudo-MID, proves that the terminal has authority (via the ISAM) to use the medium. This RESELECT() command then recovers the real Shell and the static MID required to establish MA and perform the usual ITSO product manipulation.



Tag	Value			Presence
'6F'	FCI Template			M
	'84'	DF Name		O
	'A5'	FCI Proprietary Template		M
		'C0'	Shell	M
		'C1'	Capabilities	M
		'C2'	Dir	M
		'C3'	OID$_{16}$, List	M
		'C5'	Challenge Data	M
		'C7'	the real static MID	M

Industrial Standard fixed use
Shell - Common to all ITSO intelligent media
CMD 11 Specific

Figure 11 - FCI Structure (Reselect)

12.5 POST Media behaviour

12.5.1 Media Identification and IPE Recognition

On media using static MIDs, IPEs can be identified (but not verified) using a single standard APDU to Select ITSO, see Figure 12.

On media using random UIDs, the same process for IPEs identification is shown in Figure 13.

The Dir record and the list of extended OID values provides all the information necessary for a POST to identify all IPEs on the media, their expiry dates and their lifecycle states. A decision to continue with the CM or not can be made very efficiently.

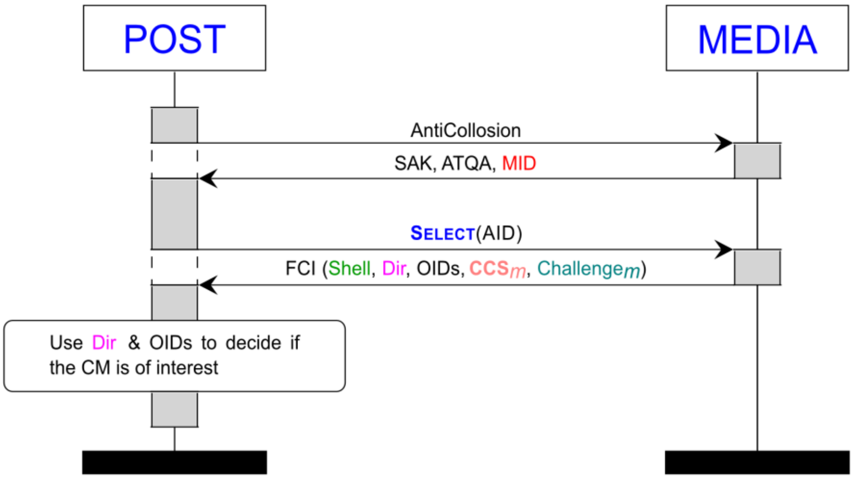

POST
MEDIA
AntiCollision
SAK, ATQA, MID
SELECT(AID)
FCI (Shell, Dir, OIDs, CCS$_{m}$, Challenge$_{m}$)
Use Dir & OIDs to decide if the CM is of interest

Figure 12 - IPE Detection - Static MID

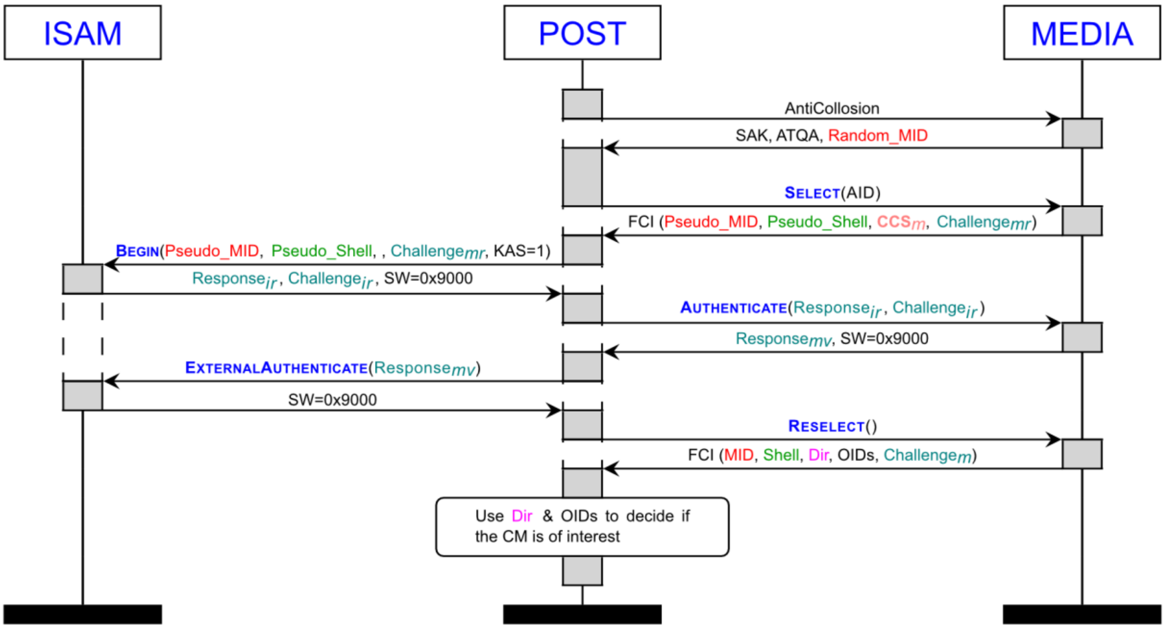

ISAM
POST
MEDIA
AntiCollision
SAK, ATQA, Random_MID
SELECT(AID)
FCI (Pseudo_MID, Pseudo_Shell, CCS$_{m}$, Challenge$_{mr}$)
BEGIN(Pseudo_MID, Pseudo_Shell, , Challenge$_{mr}$, KAS=1)
Response$_{ir}$, Challenge$_{ir}$, SW=0x9000
AUTHENTICATE(Response$_{ir}$, Challenge$_{ir}$)
Response$_{mv}$, SW=0x9000
EXTERNALAUTHENTICATE(Response$_{mv}$)
SW=0x9000
RESELECT()
FCI (MID, Shell, Dir, OIDs, Challenge$_{m}$)
Use Dir & OIDs to decide if the CM is of interest

Figure 13 - IPE Detection (Random MID)

12.5.2 Mutual authentication

If the media is of interest to the POST, Mutual Authentication must be performed, see Figure 14.

Only one additional command is sent to the CM. This command, AUTHENTICATE(), verifies the ISAM's response to the challenge delivered as part of the SELECT() command's response.

It simultaneously receives the ISAM's challenge and returns with the response to that challenge. The ISAM can now verify the CM's authenticity. Both the ISAM and the CM shall generate a session key from the exchanged challenges. The POST and the CM initialise their respective MAC accumulators.

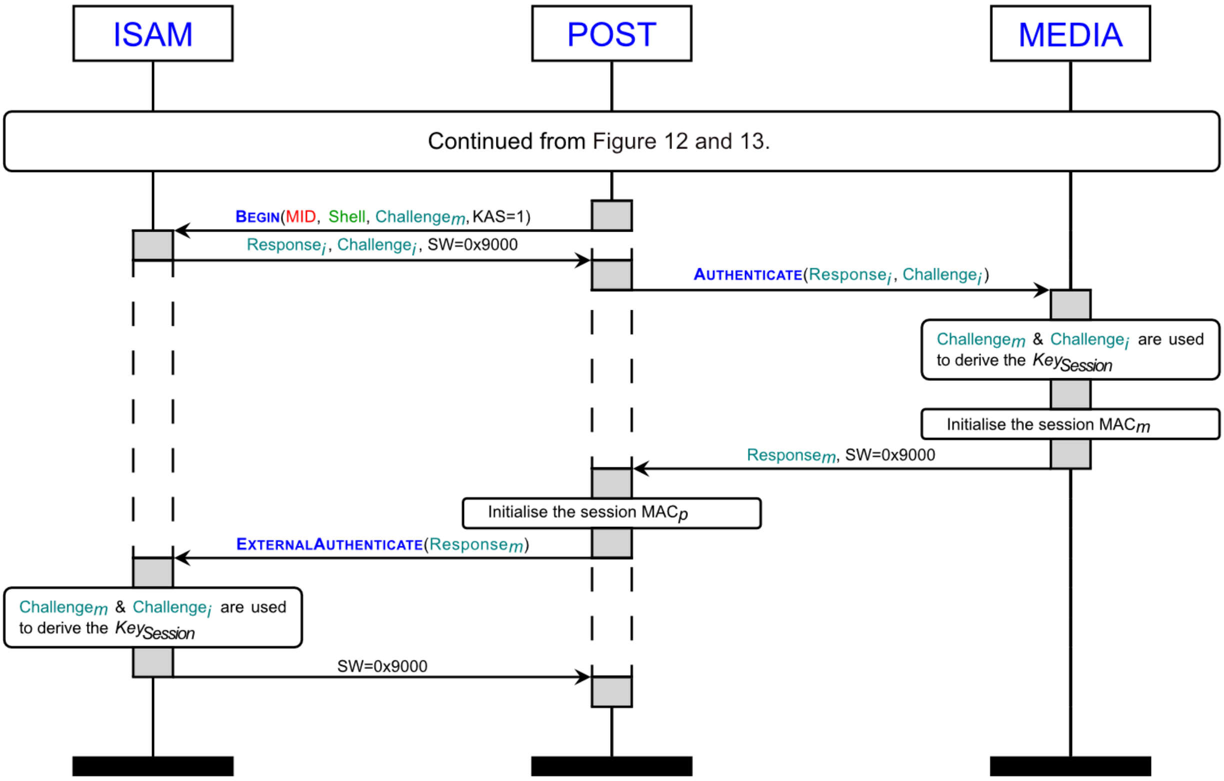

ISAM
POST
MEDIA
Continued from Figure 12 and 13.
BEGIN(MID, Shell, Challenge$_m$, KAS=1)
Response$_i$, Challenge$_i$, SW=0x9000
AUTHENTICATE(Response$_i$, Challenge$_i$)
Challenge$_m$ & Challenge$_i$ are used to derive the Key$_{Session}$
Initialise the session MAC$_m$
Response$_m$, SW=0x9000
Initialise the session MAC$_p$
EXTERNALAUTHENTICATE(Response$_m$)
Challenge$_m$ & Challenge$_i$ are used to derive the Key$_{Session}$
SW=0x9000

Figure 14 - Mutual Authentication

12.5.3 Message exchange

Message exchange between the POST and CM takes place without interaction with the ISAM, see Figure 15. Each party maintains its own version of the session MAC. No secrets are required at this stage. This enables the POST to perform the operations without sending APDUs to the ISAM.

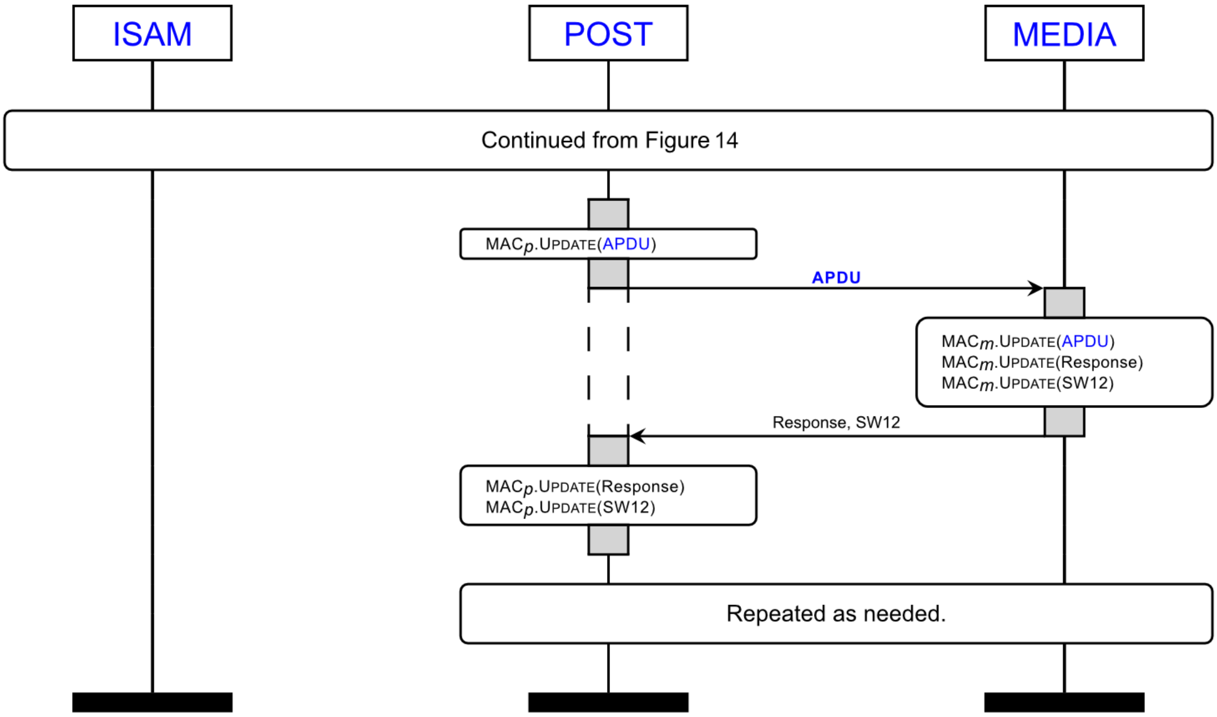


Figure 15 - Message Exchange

12.5.4 Transaction commit

Transaction committal requires interaction with the ISAM, see Figure 16.

The PIMO() command is used to sign the POST's version of the transaction MAC generating TS. A further call to PIMO() is used to generate CCS, a signature of the TS.

The POST's TS is delivered to the CM as part of the ENDSESSION() command. If the CM's own calculation of TS matches the delivered version, the conversation was complete and uncorrupted. The CM generates the CCS and commits all the preceding memory updates to non-volatile storage. CCS is returned as a receipt to confirm the memory has been fully written. The POST can verify the CCS to ensure the receipt originated from the CM and relates to the proceeding transaction.

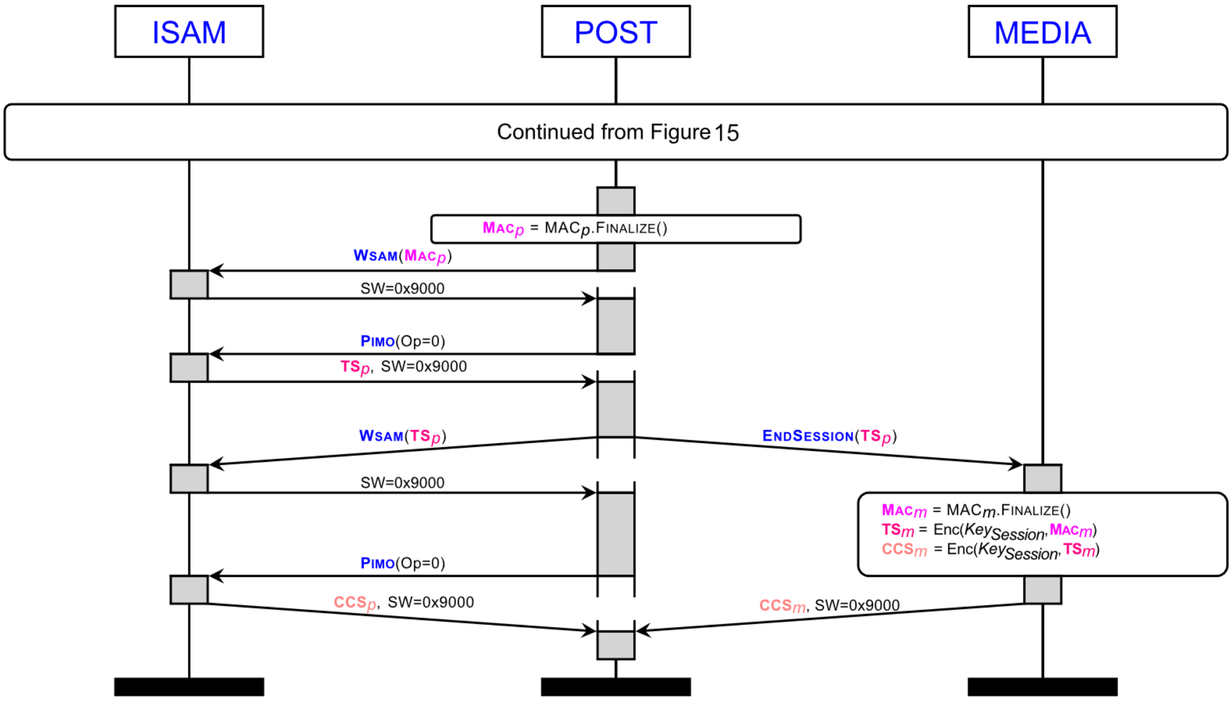


Figure 16- Transaction Commit

12.6 ITSO Shell Environment layout

The tables below summarise the ITSO shell data content. Shading indicates the main Data Structures.

Table 114 - Default ITSO Shell Environment data content - no MCRN present

Data Element Label	# of bits	# 1 Small	#2 Normal	#3 Large	#4 Extra Large
ShellLength	6	0x18/24	0x18/24	0x18/24	0x18/24
ShellBitMap	6	1	1	1	1
ShellFormatRevision	4	1	1	1	1
IIN	24	633597	633597	633597	633597
OID	16	Assigned by ITSO			
ISSN	28	Issuer defined			
CHD	4	Calculated from above			
FVC (Hex/Dec)	8	0X0B/11	0X0B/11	0X0B/11	0X0B/11
KSC	8	1 or 2 (dependent upon cryptographic capabilities)			
KVC	8	1	1	1	1
RFU	2	Padding for optimal data alignment			
EXP	14	DATE (Shell Expiry Date)			
B	8	0	0	0	0
S (Hex/Dec)	8	7	0X0B/11	0X0F/15	0X13/19

E#	8	4	8	0X0C/12	0X10/16
SCTL	8	2	4	6	0X0A/10
PAD	16	0	0	0	0
SECRC	16	Padding			
FCI Size (bytes) **Memory (bytes)**	-	**0x73/115** **3.7k**	**0X93/147** **5.8k**	**0xBb1/177** **7.9k**	**0xD1/209** **10.0k**

Table 115 - Default ITSO Shell Environment data content - MCRN present

Data Element Label	# of bits	# 1 Small	#2 Normal	#3 Large	#4 Extra Large
ShellLength	6	0x18/24	0x18/24	0x18/24	0x18/24
ShellBitMap	6	3	3	3	3
ShellFormatRevision	4	1	1	1	1
IIN	24	633597	633597	633597	633597
OID	16	Assigned by ITSO			
ISSN	28	Issuer defined			
CHD	4	Calculated from above			
FVC (Hex/Dec)	8	0X0B/11	0X0B/11	0X0B/11	0X0B/11
KSC	8	1 or 2 (dependent upon cryptographic capabilities)			
KVC	8	1	1	1	1
RFU	2	Padding for optimal data alignment			
EXP	14	DATE (Shell Expiry Date)			
B	8	0	0	0	0
S (Hex/Dec)	8	7	0X0B/11	0X0F/15	0X13/19
E#	8	4	8	0X0C/12	0X10/16
SCTL	8	2	4	6	0X0A/10
PAD	16	0	0	0	0
MCRN	80	Issuer defined			
SECRC	16	Padding			
FCI Size (bytes) **Memory (bytes)**	-	**0x73/115** **3.7k**	**0X93/147** **5.8k**	**0xBb1/177** **7.9k**	**0xD1/209** **10.0k**

12.7 Key Usage

The master key shall be generated at the time of CM personalisation. It 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.

12.8 Key strategy

This CMD shall use the Key Strategy Code (KSC) value as defined in clause 12.6. The ISAM shall use this to determine the appropriate cryptographic processes to be applied to such media.

12.9 Anti-tear

The tear is handled automatically by the platform by virtue of the exchange protocol. See clause 12.4.15 and 12.5.4 on the FCI data and how the CSS value is used.

12.10 Manufacturer’s ID - MID

ISO/IEC 7816 does not provide for access to the MID in a standardised manner. However, it is required as per authentication exchange.

12.11 Benchmark transaction

12.11.1 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 = 0x0B 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 (i.e. one EF).
- Creation of a sealed Transient Ticket Record.
- Update of the log entry and modification of the Directory.
- Perform and verify the results of the Commit command.

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

12.11.2 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 = 0x0B 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 of the IPE’s latest Value Record and update of its oldest Value Record within the Value Record Data Group, where the Value Record Data Group resides in a single Sector.
- Update of the Basic log record and write back of the modified Directory.
- Perform and verify the results of the Commit command.

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

12.12 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 = 0x0B, then it shall use ITSO Shell Referencing as defined in ITSO TS 1000-3.

13. CMD12 - MIFARE DESfire

13.1 Scope

The design of this CMD allows for the hosting of an ITSO Application on NXP's DESFire[48] or compatible specification CM that;

— Supports the standard ISO/IEC 7816-4;
— Compliance to the standard ISO/IEC 14443-3; and
— Supports application selection via AID

This medium supports all ITSO functions currently supported by CMD7 and utilises the existing features and capabilities of DESFire;

1. Chained secure messaging
2. Medium identification without the need to reset the NFC session
3. Secret key cryptography to be performed within the ISAM
4. Standard DESfire and Mobile phone emulated DESfire to use the same CMD
5. Random MID support as part of the ISO 14443-3 [2] type-A anti-collision processing
6. High capacity medium
7. Card availability from various channels
8. Long-life in service
9. Enhanced security

13.1.1 Terminology

Throughout this clause reference shall be made to terms defined within ISO/IEC 7816-4 and ISO/IEC 14443-3.

13.2 Platform capability

13.2.1 General

This platform is capable of supporting a full set of ITSO Data Groups as defined below and further explained in clause:

● ITSO 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*

13.2.2 Security provisions

The platform provides the following security-related features:

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

— DES and AES protocol support

[48] MF3Dx2 - MIFARE DESFire EV2 - contactless multi-application IC, NXP Semiconductors, 25 April 2017, rev. 3.1.

— Support for plain, MACed and enciphered air communication between POST and media

— Support for native Anti-tear protection.

This definition utilises DESFire's DES authentication features for compatibility with the current ISAM. This definition anticipates the use of AES in the future and enables a seamless transition to AES in the future.

13.2.3 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 and / or Type B requirements;
- Part 3: Initialisation & anticollision Compliance with ISO/IEC 14443 Type A and / or Type B requirements;
- Part 4: Transmission protocol Compliance with ISO/IEC 14443 Type A and / or Type B requirements.

13.2.4 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 secures 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.

13.3 Format Version Code

Platforms that conform to this CMD shall use the Format Version Code (FVC) of 0x0C (12).

13.4 ITSO Shell

The platform supports full shell and Dir structures.

This platform supports the atomic update of file data therefore a single copy of the directory is maintained and managed as per CMD 7.

13.4.1 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.

13.4.2 Platform parameters with fixed values

The 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 116 - Parameters with Fixed 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 (Hex/Dec)	0x0C/12	-

13.4.3 Shell Environment detailed layout

The table below details the location of the data elements when the default platform parameter values are used. Shading indicates the main Data Structures.

Table 117 - Default ITSO Shell Environment data content - no MCRN present

Data Element Label	# of bits	Generic Value
ShellLength (Hex/Dec)	6	0x18/24
ShellBitMap	6	1
ShellFormatRevision	4	1
IIN	24	633597
OID	16	Assigned by ITSO
ISSN	28	Issuer defined
CHD	4	Calculated from IIN+OID+ISSN
FVC (Hex/Dec)	8	0X0C/12
KSC	8	5
KVC	8	1
RFU	2	Padding for optimal data alignment
EXP	14	DATE (Shell Expiry Date)
B	8	Refer to Permitted Fixed geometries Table 120
S (Hex/Dec)	8	
E#	8	
SCTL	8	
PAD	16	0
SECRC	16	Padding

Table 118 - Default ITSO Shell Environment data content - MCRN present

Data Element Label	# of bits	Generic Value
ShellLength (Hex/Dec)	6	0x24/32
ShellBitMap	6	3
ShellFormatRevision	4	1
IIN	24	633597
OID	16	Assigned by ITSO
ISSN	28	Issuer defined
CHD	4	Calculated from IIN+OID+ISSN
FVC (Hex/Dec)	8	0X0C/12
KSC	8	5

KVC	8	1
RFU	2	Padding for optimal data alignment
EXP	14	DATE (Shell Expiry Date)
B	8	Refer to Permitted Fixed geometries Table 120
S (Hex/Dec)	8	
E#	8	
SCTL	8	
PAD	16	0
MCRN	80	Issuer defined
SECRC	16	Padding

13.5 ITSO Application

ITSO CMD12 is implemented as a single application within DESFire.

Two variants of the application are defined below.

Standard — This variant is identified by the presence of a static/fixed Manufacturer’s Identification Number (MID). As per other ITSO media definitions, all files are freely readable.

Anonymous — This variant is identified by the delivery of a randomised MID. It is used primarily in mobile phone media where the device, and by implication the holder, must not be identifiable without deliberate interaction on the part of the holder. Randomisation of the MID is used to prevent unauthorised readers recognising or tracking a device by using the MID as a digital fingerprint. Similarly files containing card-unique invariant data have restricted access (Shell and IPE storage files). The Directory and Log contain dynamic data and cannot be used to fingerprint a device. These files retain free read permission, thus enabling ISAM-less ticket inspection devices to verify the existence of ticket types and the holder’s check-in/check-out status.

13.6 Application Keys

Three 16-byte keys are needed.

Key0 — Is the application master key. It is not used by ITSO. It is set by the CM owner/manufacturer and permits them to manage the application’s settings.

Key1 — This is the ITSO MID diversified CM key. It is generated by the ISAM and is unique to the CM. ITSO file operations are performed using a secure session key derived from this key as a side effect of the ISAM–CM mutual authentication exchange.

Key2 — This key is only required for the Anonymous variants of this CMD. This key is derived by the ISAM via the pseudo-MID & pseudo-Shell data retrieved as part of application selection. It is generated by the ISAM and is unique to the operator. It is used to establish a temporary secure session to enable the collection of the true MID on media that use a random MID during card selection. Section 13.8.1 provides details of the pseudo-MID.

13.6.1 Applications Files

The application consists of up to 32 files. Their configuration and roles are described here in Table 119, and Table 120 shows the permitted variants of the Shell’s B, S & E parameters.

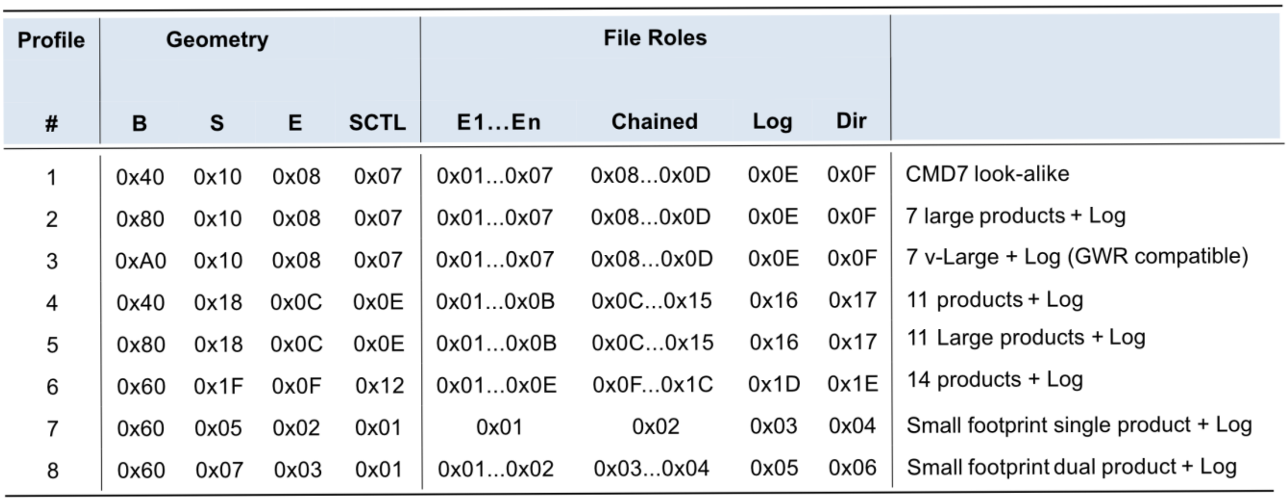
Table 119 - Application Files

File		Std	Anon	Description
0				**Shell**
	Communications mode	`0x00`	`0x01`	**Std:** Reading can be performed without an active SM session. **Anon:** Data read from this file will be Message Authentication Code (MAC)'ed using the current SM session key.
	Access Permission	`0xE00F`	`0x200F`	Reading is free on **Std** media and requires Key$_2$ authentication for **Anon** media. Updating requires authentication with Key$_0$, and these permissions cannot be changed.
	File Size	32	32	The file size is 32 bytes
1..*S*-3				**Sector Storage Files**, File$_x$ stores Sector$_x$. These files contain the IPE data.
	Communications mode	`0x01`	`0x01`	Data read from this file will be MAC'ed using the current SM session key.
	Access Permission	`0xE11F`	`0x111F`	Reading is free on **Std** media and requires Key$_1$ authentication for **Anon** media. Updating requires authentication with Key$_1$, and these permissions cannot be changed.
	File Size	*B*	*B*	The file size is *B*, as indicated within the Shell data structure.
S-2				**Log**, Record management is performed as per the identical structure in CMD7.
	Communications mode	`0x01`	`0x01`	Data read from this file will be MAC'ed using the current SM session key.
	Access Permission	`0xE11F`	`0xE11F`	Reading is free, updating requires authentication with Key$_1$, and these permissions cannot be changed.
	File Size	192	192	The ITSO LOG data structure, comprising of 4 48 byte records.
S-1				**Directory**, It contains the ITSO Dir data structure.
	Communications mode	`0x01`	`0x01`	Data read from this file will be MAC'ed using the current SM session key.
	Access Permission	`0xE11F`	`0xE11F`	Reading is free, updating requires authentication with Key$_1$, and these permissions cannot be changed.
	File Size	*X*	*X*	File size depends on the Shell's geometry.
31				**FCI**
	Communications mode	`0x00`	`0x00`	Reading can be performed without an active SM session.
	Access Permission	`0xE00F`	`0xE00F`	Reading is free, updating requires authentication with Key$_0$, and these permissions cannot be changed.
	File Size	*X*	*X*	The file size depends on the size of the FCI data structure it contains.

13.7 Permitted Fixed Geometries

There are 8 permitted variants of the Shell's B, S & E parameters, see Table 120.

Table 120 - Permitted fixed geometries



Profile	Geometry				File Roles				
#	B	S	E	SCTL	E1…En	Chained	Log	Dir	
1	0x40	0x10	0x08	0x07	0x01...0x07	0x08...0x0D	0x0E	0x0F	CMD7 look-alike
2	0x80	0x10	0x08	0x07	0x01...0x07	0x08...0x0D	0x0E	0x0F	7 large products + Log
3	0xA0	0x10	0x08	0x07	0x01...0x07	0x08...0x0D	0x0E	0x0F	7 v-Large + Log (GWR compatible)
4	0x40	0x18	0x0C	0x0E	0x01...0x0B	0x0C...0x15	0x16	0x17	11 products + Log
5	0x80	0x18	0x0C	0x0E	0x01...0x0B	0x0C...0x15	0x16	0x17	11 Large products + Log
6	0x60	0x1F	0x0F	0x12	0x01...0x0E	0x0F...0x1C	0x1D	0x1E	14 products + Log
7	0x60	0x05	0x02	0x01	0x01	0x02	0x03	0x04	Small footprint single product + Log
8	0x60	0x07	0x03	0x01	0x01...0x02	0x03...0x04	0x05	0x06	Small footprint dual product + Log

13.8 Media Command set

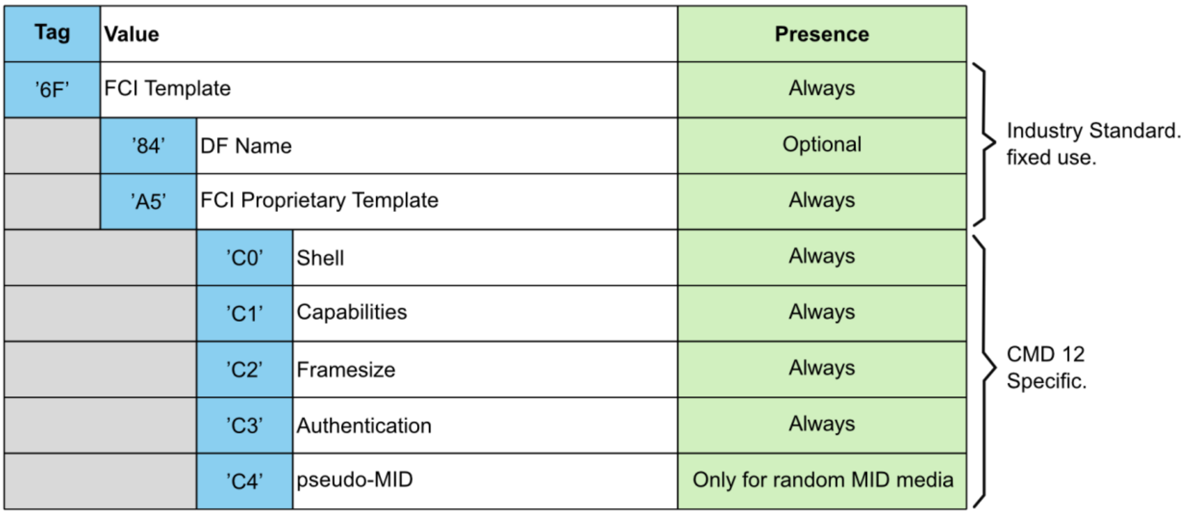
This section describes the subset of commands that a POST needs to use to utilise CMD12 within the live environment. These commands are defined by ISO/IEC 7816. The detailed usage of these commands shall be defined in subsequent sections.

Table 121 - Media Command set

Command	**CLA**	**INS**	**P1**	**P2**	**Description**
Select ITSO	0x00	0xA4	0x04	0x00	This command selects the application using the ITSO AID.
Authenticate	0x90	xx (FCI Tag C3: Authentication)	0x00	0x00	ISAM's response to the CM's challenge ISAM's challenge to the CM CM's response to the ISAM's challenge
Recover MID	0x90	0x51	0x00	0x00	This command retrieves the CM's true MID encrypted by the current session.
Read File	0x90	0xBD/0xAD	0x00	0x00	DESFire ISO wrapped command / Read Data
Update File	0x90	0x3D/0x8D	0x00	0x00	DESFire ISO wrapped command / Write Data
Commit Transaction	0x90	0xC7	0x00	0x00	DESFire ISO wrapped command / Commit Transaction.
Last Command	0x90	0xEE	0x00	0x00	Proprietary extension to the DESFire command. Marks the end of POST - CM communication.

13.8.1 Selection

Selection shall be via the standard ITSO AID. The CM shall respond to a SELECT ITSO() command with Tag-Length-Value (TLV) formatted File Control Information (FCI), see Figure 17 for structure of the FCI data;



Tag			Value	Presence
’6F’			FCI Template	Always
	’84’		DF Name	Optional
	’A5’		FCI Proprietary Template	Always
		’C0’	Shell	Always
		’C1’	Capabilities	Always
		’C2’	Framesize	Always
		’C3’	Authentication	Always
		’C4’	pseudo-MID	Only for random MID media

Industry Standard. fixed use.

CMD 12 Specific.

Figure 17 - FCI Structure

The FCI tags described above have the following structure and use;

- C0: **Shell** - This must be present on CMs. On CMs that use static-MIDs, this is the real-Shell that can be used in the ISAM mutual authentication process. In this case this record contains a duplicate of the Shell data from File0.

  On media using random-MIDs, this is an operator specific pseudo-shell common to all CMs issued by that operator. This pseudo-shell must use the issuer’s ITSO Operators Identification Number (OID) and it is recommended that an ITSO Shell Serial Number (ISSN) of zero is also used. Multi-application CM Reference Number (MCRN) data must not be included. Its size shall therefore be 0x18 bytes.

  The pseudo-shell (and the pseudo-MID, delivered in the C4 tag) are used to establish a temporary secure session via the usual ISAM mutual authentication commands. This temporary secure session permits the recovery of the CM’s unique real-MID, and the CM specific real Shell from File0. These can then be used to repeat the ITSO mutual authentication, thus enabling the verification and manipulation of stored IPEs.

- C1: **Capabilities** - Size 1 byte.

  bit 0 is set to indicate the CM supports the EV1 command set.
  bit 1, ditto EV2.
  bit 2, ditto EV3.
  bit 6 is set to indicate the LAST COMMAND (see Figure 36) APDU extended behaviour is required.

- C2: **FrameSize** - Size 1 byte.

  This byte indicates the maximum size of the DESFire frames supported by this CM. Different versions of DESFire support differing frame sizes and optimal data delivery is achievable if the POST uses the largest possible frame size when delivering data to the CM.

- C3: **Authentication** - Size 3 byte.

  This tag provides support for the adoption of alternative DESFire authentication algorithms in future.
  Byte:1 indicates the DESFire instruction code for the appropriate AUTHENTICATE command.
  Byte:2 indicates the block size operated on by the identified algorithm.
  Byte:3 indicates the size of the key used by the identified algorithm.

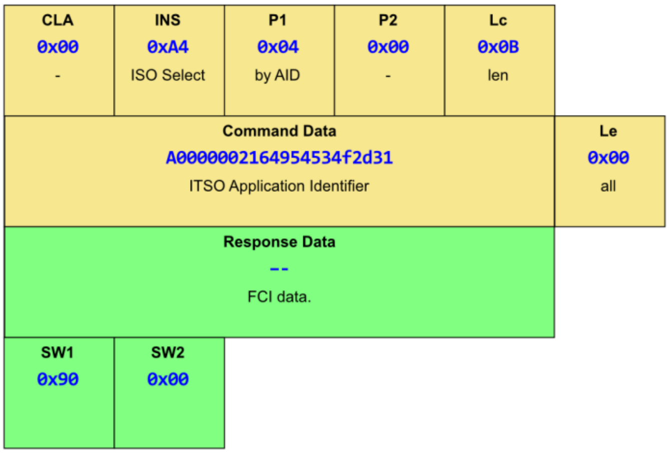
The combination of these three parameters enables the POST to blindly exchange the appropriate volume of data between the indicated DESFire AUTHENTICATE command and the ISAM's BEGIN and EXTERNAL AUTHENTICATE.

- C4: **Pseudo-MID** - This field must be present on CMs that use random-MIDs and must not be present on CMs that use static-MIDs.

  Size = 8 bytes.
  This record contains the pseudo-MID. The value is arbitrary and must be constant for all CM issued by an individual operator.

13.8.2 Select ITSO

This command selects the application using the ITSO AID, [A0, 00, 00, 02, 16, 49, 54, 53, 4f, 2d, 31] and the returned FCI data is mandatory, which is defined in 13.8.1.



CLA	INS	P1	P2	Lc
0x00	0xA4	0x04	0x00	0x0B
-	ISO Select	by AID	-	len

Command Data	Le
A0000002164954534f2d31	0x00
ITSO Application Identifier	all

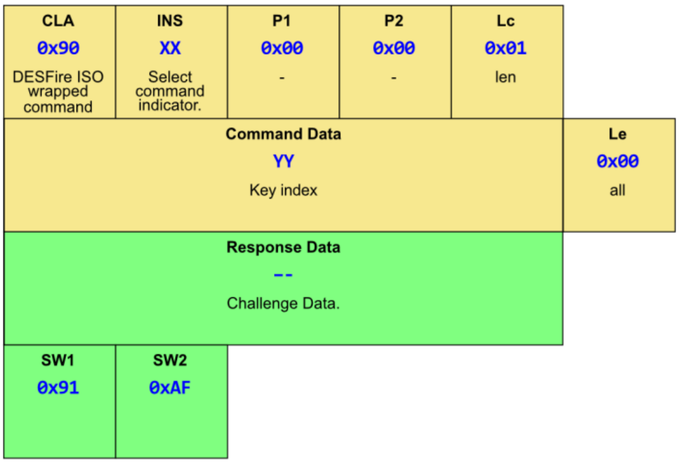
Response Data
--
FCI data.

SW1	SW2
0x90	0x00

The command as defined by ISO/IEC 7816 (Part 4 (4)).

This command selects the application using the ITSO AID.

13.8.3 Authenticate



CLA	INS	P1	P2	Lc
0x90	XX	0x00	0x00	0x01
DESFire ISO wrapped command	Select command indicator.	-	-	len

Command Data	Le
YY	0x00
Key index	all

Response Data
--
Challenge Data.

SW1	SW2
0x91	0xAF

The INS value, Select command indicator XX, was delivered to the POST in the FCI data retrieved during application selection (see section 13.8.2). The Command data, Key Index YY, shall be 0x01 when authenticating with the CM's real MID, or 0x02 when authenticating with the pseudo MID.

The size of the response, Challenge Data, depends on the cryptographic keys personalised into the ISAM. For DES keys this shall be 16 bytes of data. This is two times the BLOCKSIZE indicated in the FCI.

The POST is expected to deliver the Challenge Data to the ISAM and collect the ISAM's response. This response is then delivered to the CM using the following ADDITIONAL FRAME APDU.

CLA	INS	P1	P2	Lc
0x90	0xAF	0x00	0x00	0x10 / 0x20
Authenticate, Additional Frame	DESFire additional frame.	-	-	len

Command Data	Le
ISAM's response	0x00
ISAM's response	all

Response Data
--
Media's response.

SW1	SW2
0x91	0x00

Le, is determined by the ISAM's response size.

The ISAM's Response is the value returned by the ISAM when processing the BEGIN() command.

The Media's response shall be delivered to the ISAM in an EXTERNALAUTHENTICATE command. This completes the process of mutual authentication between the CM and the ISAM.

13.8.4 Recover MID

CLA	INS	P1	P2	Lc	Le
0x90	0x51	0x00	0x00	--	0x00
DESFire ISO wrapped command	Get Card MID.	-	-	absent	all

Response Data
--
Encrypted MID.

SW1	SW2
0x91	0x00

The command retrieves the CM's true-MID encrypted by the current session key. This command should be performed when the CM indicates it uses a random MID.

The POST should first authenticate with the CM using the pseudo-MID and pseudo-Shell from the FCI data.

The PIMO command, (see section 13.8.9) can be used to decrypt and retrieve the clear text true-MID.

13.8.5 Read File

CLA	INS	P1	P2	Lc
0x90	0xBD/0xAD	0x00	0x00	0x07
DESFire ISO wrapped command	Read Data	-	-	len

Command Data	Le
Read parameters	0x00
File[1], Offset[3], Length[3]	all

Response Data
--
Collected data.

SW1	SW2
0x91	0x00

If the Capabilities Indicator indicates EV2 or above, then the ISO framed 0xAD READDATA command should be used. This provides a faster mechanism for retrieving data. EV1 does not support this optimization and the POST must use the legacy 0xBD READDATA command and manage the DESFire 0xAF framing.

13.8.6 Update File

CLA	INS	P1	P2	Lc
0x90	0x3D/0x8D	0x00	0x00	0x??
DESFire ISO wrapped command	Write Data	-	-	len

Command Data	Le
Write parameters	0x00
File[1], Offset[3], Length[3], Data[], Delivery MAC[8]	all

Response Data
--
Response MAC[8]

SW1	SW2
0x91	0x00

If the Capabilities Indicator indicates EV2 or above, then the ISO framed 0x8D WRITEDATA command should be used. This provides a faster mechanism for delivering data. EV1 does not support this optimization and the POST must use the legacy 0x3D WRITEDATA command and manage the DESFire 0xAF framing. The maximum size of an individual Frame is given by the FCI's Tag-C2.

13.8.7 Commit Transaction

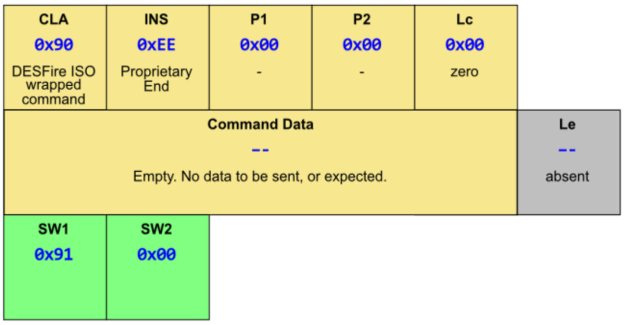
CLA	INS	P1	P2	Lc
0x90	0xC7	0x00	0x00	0x00
DESFire ISO wrapped command	Commit Transaction	-	-	all

Command Data	Le
--	--
Response MAC[8]	absent

SW1	SW2
0x91	0x00

This command is only needed if one or more WRITEDATA commands (see 13.8.6) have been executed. It is important to verify the returned MAC. This provides evidence that the updates have been committed to memory and prevents attacks that exploit delayed delivery of this command.

13.8.8 Last command



CLA	INS	P1	P2	Lc
0x90	0xEE	0x00	0x00	0x00
DESFire ISO wrapped command	Proprietary End	-	-	zero

Command Data	Le
--	--
Empty. No data to be sent, or expected.	absent

SW1	SW2
0x91	0x00

This command is a proprietary extension to the DESFire command set. It is used to mark the end of a POST – CM conversation.

The rules for using the command are:

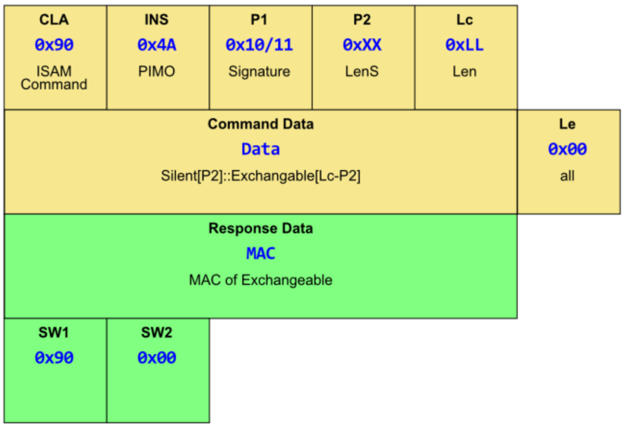
- Only use the command if the Capabilities identifier (FCI Tag C1) indicates the CM supports it.
- When the CM indicates it implements it, then it must be used and must be the last APDU in the message exchange.
- Failure to respond on the part of the CM should not be interpreted as an error.

13.8.9 ISAM APDU Commands

13.8.9.1 PIMO

Three variants of the PIMO command support CMD12.

These variants offer an alternative approach by bypassing the use of ITSOBuffer, removing the necessity for WSAM and RSAM commands to handle its contents. Instead, all relevant data are integrated within the PIMO command itself.



CLA	INS	P1	P2	Lc
0x90	0x4A	0x10/11	0xXX	0xLL
ISAM Command	PIMO	Signature	LenS	Len

Command Data	Le
Data	0x00
Silent[P2]::Exchangable[Lc-P2]	all

Response Data
MAC
MAC of Exchangeable

SW1	SW2
0x90	0x00

13.8.9.2 PIMO for Signature

Signature generation is required for DESFire commands that expect delivery of a MAC as part of the command body.

This calculates the CMAC of the Exchangeable and returns it to the caller.

When P1 == 0x11, the whole process is preceded by a CMAC generation over a single byte of 0x00.

13.8.9.3 Processing, P1=0x10

```
if ($P2 \neq 0$)      $IV' = CMAC(IV, Silent\_Data)$
else                  $IV' = IV$
if ($P2 \neq Lc$)     $IV'' = CMAC(IV', Exchangeable\_Data)$
else                  $IV'' = IV'$
return ($IV''$)
```

13.8.9.4 Processing, P1 = 0X11

```
                      $IV' = CMAC(IV; 0x00)$
if ($P2 \neq 0$)      $IV'' = CMAC(IV'; Silent\_Data)$
else                  $IV'' = IV'$
if ($P2 \neq Lc$)     $IV''' = CMAC(IV''; Exchangeable\_Data)$
else                  $IV''' = IV''$
return ($IV'''$)
```

13.8.9.5 Behaviour

Table 122 - Signature behaviour

P2		Lc	Operation
0		0	No operation, Return nothing.
0		X	MAC of X bytes, Return MAC.
X	<	Y	Silent MAC of first X bytes, MAC of the remaining Y-X bytes, Return MAC.
X	=	Y	Silent MAC X bytes, Return nothing.
X	>	Y	Error.

Table 123 - PimoForSignature - Status Words

StatusWord		Meaning
9000	No Error	Normal processing.
6A86	Incorrect P1 P2	P1 < 0x10 or 0x15 < P1
6700	Wrong Length	P2 > Lc

13.8.9.6 Pimo for Verification

CLA	INS	P1	P2	Lc	
0x90 ISAM Command	0x4A PIMO	0x12/13 Verification	0xXX LenS	0xLL Len	
Command Data Data Silent[P2]::Exchangable[Lc-P2]::MAC[8]					Le -- absent
SW1 0x90	SW2 0x00				

Verification of signatures becomes necessary for DESFire commands that provide a MAC as part of their response data.

This specific version of the PIMO command receives the Customer Medium (CM)'s MAC and contrasts it with an internally generated version of the same for comparison and validation purposes.

13.8.9.7 Processing, P1=0x12

```
1:  $if(P2 \neq 0)$              $IV' = CMAC(IV; Silent\_Data)$
    $else$                       $IV' = IV$
2:  $if(P2 \neq Lc \quad 8)$     $IV'' = CMAC(IV'; Exchangeable\_Data)$
    $else$                       $IV'' = IV'$
3:  $return \quad (IV'' == \quad MAC)$
```

13.8.9.8 Processing, P1=0x13

```
1:                               $IV' = CMAC(IV; 0x00)$
2:  $if(P2 \neq 0)$              $IV'' = CMAC(IV'; Silent\_Data)$
    $else$                       $IV'' = IV'$
3:  $if(P2 \neq Lc \quad 8)$     $IV''' = CMAC(IV''; Exchangeable\_Data)$
    $else$                       $IV''' = IV''$
4:  $return \quad (IV''' == \quad MAC)$
```

13.8.9.9 Behaviour

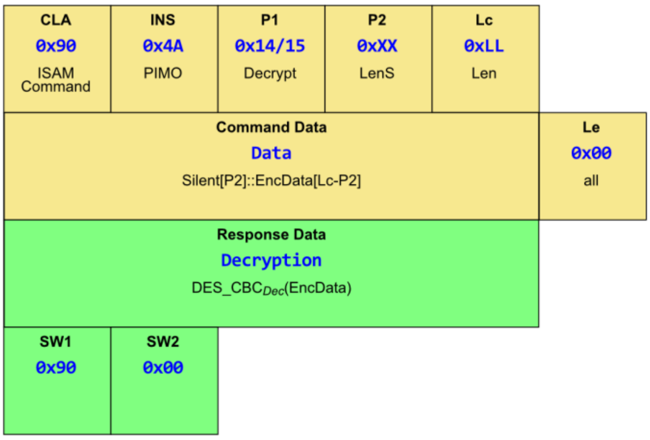
Table 124 - Verification Behaviour

P2		Lc	Operation
X		0…7	Error.
0		8	Return IV == MAC.
0		Y+8	MAC of Y bytes, Return IV == MAC.
X	<	Y+8	Silent MAC of first X bytes, MAC of the remaining Y-X bytes, Return IV == MAC.
X	=	Y+8	Silent MAC X bytes, Return nothing.
X	>	Y+8	Error.

Table 125 - PimoForVerification - Status Words

StatusWord		Meaning
9000	No Error	Normal processing.
6A86	Incorrect P1 P2	P1 < 0x10 or 0x15 < P1
6700	Wrong Length	P2 > Lc - 8
6300	Host Cryptogram Failed	MAC verification failure

13.8.9.10 Pimo for Decryption



CLA	INS	P1	P2	Lc
0x90	0x4A	0x14/15	0xXX	0xLL
ISAM Command	PIMO	Decrypt	LenS	Len

Command Data	Le
Data	0x00
Silent[P2]::EncData[Lc-P2]	all

Response Data
Decryption
DES_CBC$_{Dec}$(EncData)

SW1	SW2
0x90	0x00

If the Silent data component exists, it undergoes processing initially. The subsequent data is decrypted, and the resulting information is then sent back to the requester. Unlike other commands, in this scenario, the Initialization Vector (IV) is the outcome of this Cipher Block Chaining (CBC) operation, distinct from the usual CMAC process.

13.8.9.11 Processing, P1=0X14

```
1:  $if(P2 \neq 0)$                          $IV' = CMAC(IV; Silent\_Data)$
    $else$                                   $IV' = IV$
2:  $if(P2 \neq Lc)$       $ClearData; IV'' = DES\_CBC_{Dec}(IV'; EncData)$
    $else$                 $ClearData; IV'' = 0/; IV'$
3:  $return\ (ClearData)$
```

13.8.9.12 Processing, P1=0X15

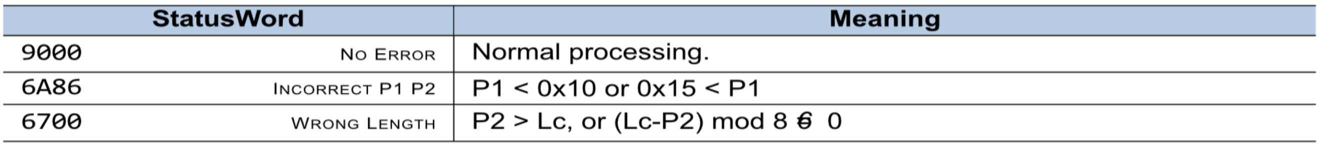
```
1:                                           $IV' = CMAC(IV, 0x00)$
2:  $if(P2 \neq 0)$                          $IV'' = CMAC(IV', Silent\_Data)$
    $else$                                   $IV'' = IV'$
3:  $if(P2 \neq Lc)$       $ClearData; IV''' = DES\_CBC_{Dec}(IV'', EncData)$
    $else$                 $ClearData; IV''' = \emptyset, IV''$
4:  $return\ (ClearData)$
```

13.8.9.13 Behaviour

Table 126 - Decryption Behaviour

P2		Lc	Operation
0		0	No operation, Return nothing.
0		X	Decrypt X bytes, Return decrypted data.
X	<	Y	Silent MAC of first X bytes, Decrypt the remaining Y-X bytes, Return decrypted data.
X	=	Y	Silent MAC X bytes, Return nothing.
X	>	Y	Error

Table 127 - PimoForDecryption - Status Words



StatusWord		Meaning
9000	No Error	Normal processing.
6A86	Incorrect P1 P2	P1 < 0x10 or 0x15 < P1
6700	Wrong Length	P2 > Lc, or (Lc-P2) mod 8 6̸ 0

13.9 POST Media behaviour

13.9.1 Media detection and IPE recognition Process

After card detection, Selection and Authentication must be performed. This establishes a secure session and verifies the authenticity of the CM. If the card detection process retrieved a static-MID as part of the ISO 14443-3 anti-collision processing, then the procedure described by Figure 18 (Static) should be used. If a random-MID was retrieved, then the process described by Figure 19 (Media selection - Random MID) should be use.

After authentication files may be read and updated as per Figure 20 (Read File) and Figure 21-22 (Write File). These commands can be interleaved and repeated as often as required to perform the transaction.

If the transaction involves writing data to one or more files, the data changes need to be committed, as shown in Figure 23 (Commit Transaction). Failure to perform the process results in the changes being lost, and the card shall be restored to its pre- transaction state. This ensures incomplete transactions do not leave the card in indeterminate intermediate states in the event of a card tear.

Finally, if the CM’s Capabilities byte (Section 13.8 Tag C1) indicates the requirement to use the LASTCOMMAND APDU (Section 13.8.8), the process described in Figure 24 (Section 13.9.1.5 - Last Command) must be performed.

13.9.1.1 Selection and Authentication - Static MID

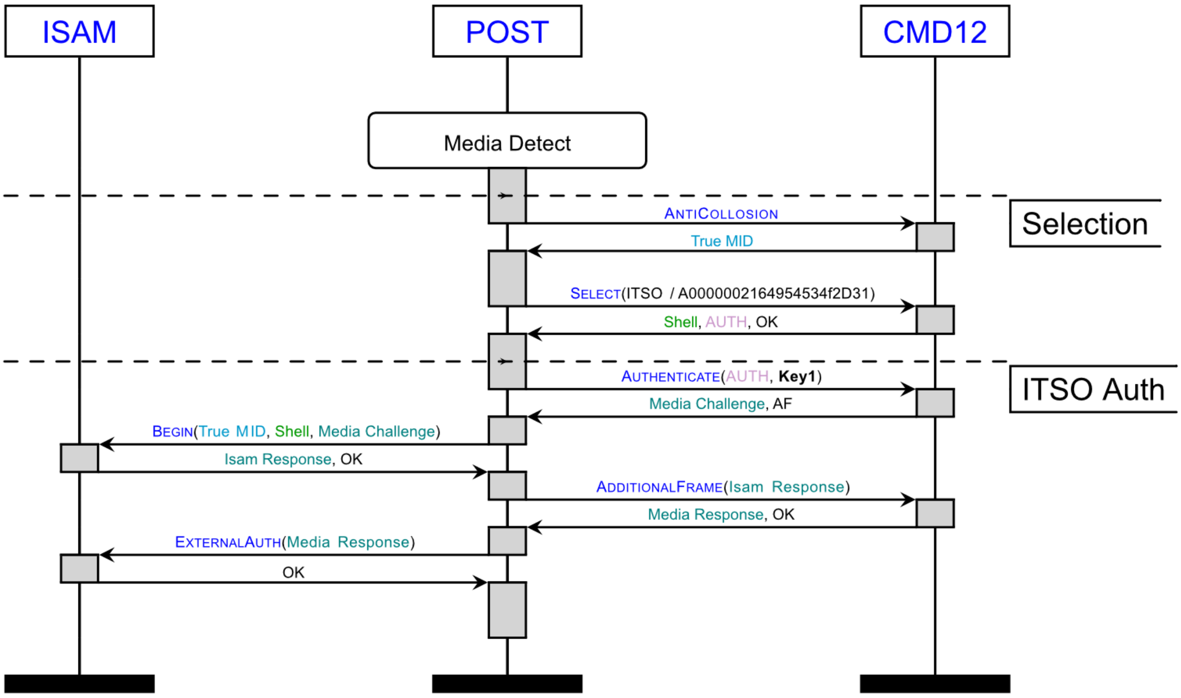


Figure 18 - Media selection, Static MID

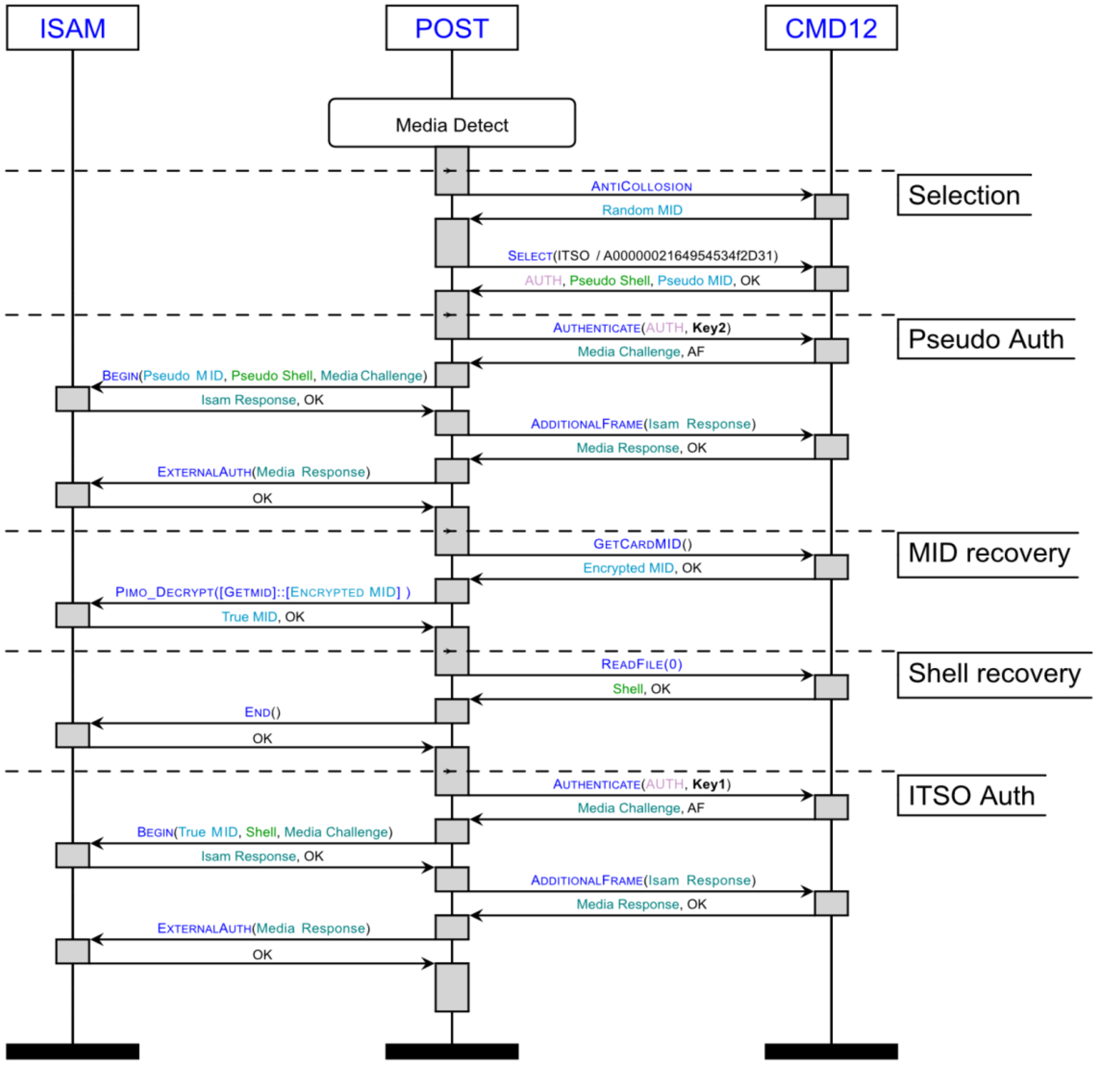


Figure 19 - Media selection, Random MID

13.9.1.2 Reading Files

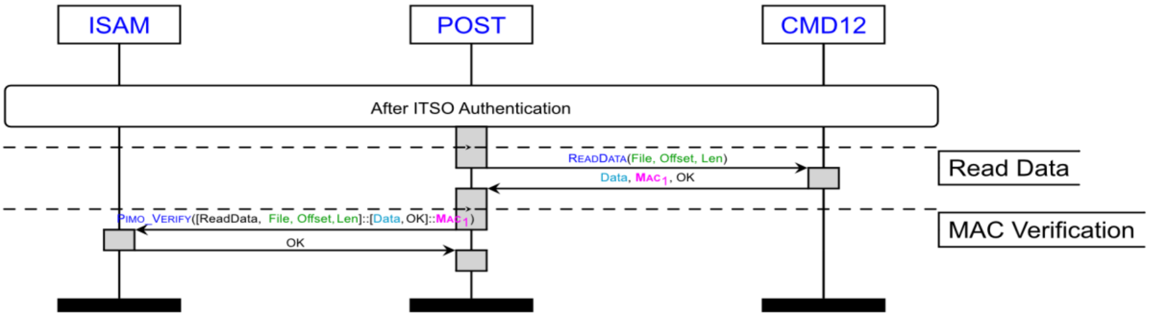

ISAM
POST
CMD12
After ITSO Authentication
Read Data
ReadData(File, Offset, Len)
Data, Mac1, OK
MAC Verification
Pimo_Verify([ReadData, File, Offset, Len]::[Data, OK]::Mac1)
OK

Figure 20 - Reading Files

13.9.1.3 Writing Files

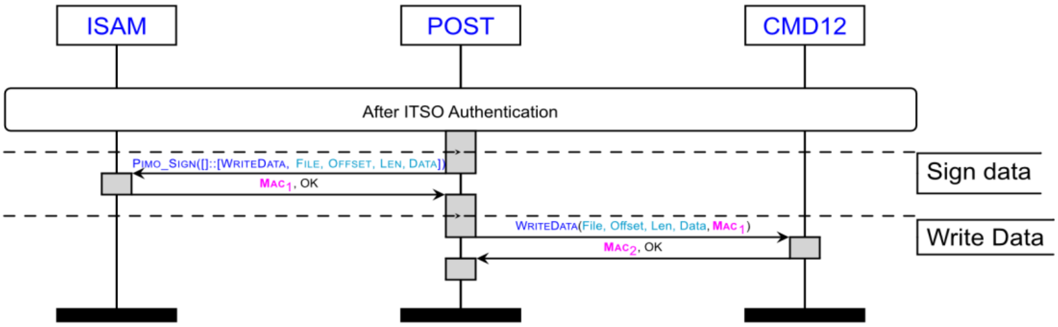

ISAM
POST
CMD12
After ITSO Authentication
Sign data
Write Data
PIMO_SIGN([]::[WRITEDATA, FILE, OFFSET, LEN, DATA])
MAC1, OK
WRITEDATA(File, Offset, Len, Data, MAC1)
MAC2, OK

Figure 21 - Write File - (after ReadFile)

Note: The final OK is unverified/unprocessed at this point.

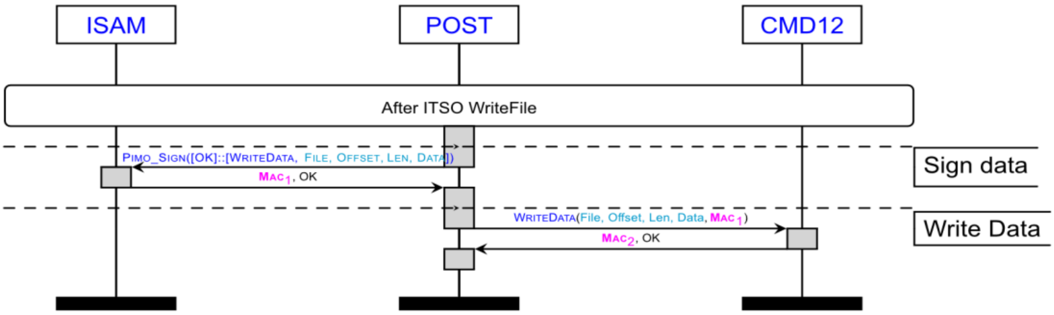

ISAM
POST
CMD12
After ITSO WriteFile
Sign data
Write Data
PIMO_SIGN([OK]::[WRITEDATA, FILE, OFFSET, LEN, DATA])
MAC1, OK
WRITEDATA(File, Offset, Len, Data, MAC1)
MAC2, OK

Figure 22 - Write File (after WriteFile)

Note: This processes the missing OK while collecting another (as of yet) unverified OK.

Note: MAC2 does not need to be verified. It will be the IV resulting from the CMAC of the OK. If it is faulty then the subsequent commands will fail and abort the transaction.

13.9.1.4 Committing Updates

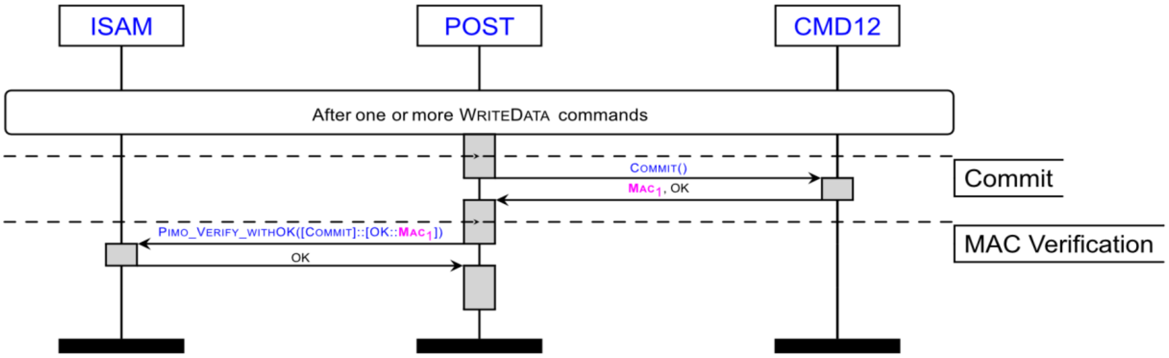

ISAM
POST
CMD12
After one or more WRITEDATA commands
Commit
COMMIT()
MAC1, OK
MAC Verification
PIMO_VERIFY_WITHOK([COMMIT]::[OK::MAC1])
OK

Figure 23 - Commit Transaction

Note: This uses the odd numbered P1 version of the PimoForVerification. It processes the unhandled OK from the preceding WriteDate, processes the Commit message and finally verifies the Commit's MAC to prove the command was successful.

13.9.1.5 Last command

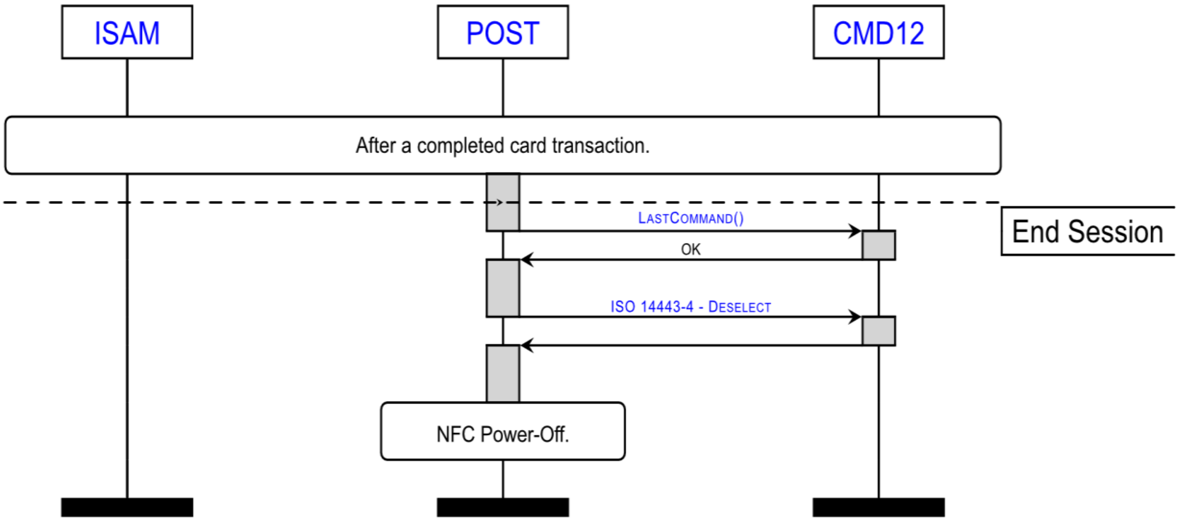


Figure 24 - Last Command

13.10 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.

13.11 Shell access

The file containing the ITSO Shell shall be accessed by use of the ReadData command. The Shell is free on static MID otherwise it needs Key2. All other files (except FCI/31) need Key1 authentication. Update access to this file is not allowed.

13.12 Access Files - Directory/IPE/Value Record & Cyclic

The IPE access, Value Record and Cyclic Log access files shall be accessed by use of the ReadData and WriteData commands. The Shell is free on static MID otherwise it needs Key2. All other files (except FCI/31) need Key1 authentication. Update access to these files shall require a valid mutual authentication session to have taken place. Updates to these files need the use of the CommitTransaction command.

13.13 Key Usage

The master key shall be generated at the time of CM personalisation. It 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.

13.14 Key strategy

This CMD shall use the Key Strategy Code (KSC) value as defined in clause 13.4.3. The ISAM shall use this to determine the appropriate cryptographic processes to be applied to this medium.

13.15 Anti-tear

The tear is handled automatically by the platform by virtue of the exchange protocol.

13.16 Manufacturer’s ID - MID

ISO/IEC 7816 does not provide for access to the MID in a standardised manner. However, it is required as per authentication exchange.

13.17 Benchmark transaction

13.17.1 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 = 0x0C/12 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 (i.e. one EF).
- Creation of a sealed Transient Ticket Record.
- Update of the log entry and modification of the directory.
- Issue the Commit command and Last Command if its use was indicated by the Capabilities flag.

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

13.17.2 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 = 0x0C/12 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 the data group and product above.
- Update of the log entry within the directory.
- Issue the Commit command and Last Command if its use was indicated by the Capabilities flag.

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

13.18 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 = 0x0C/12, then it shall use ITSO 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.

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 copy[49] 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.

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

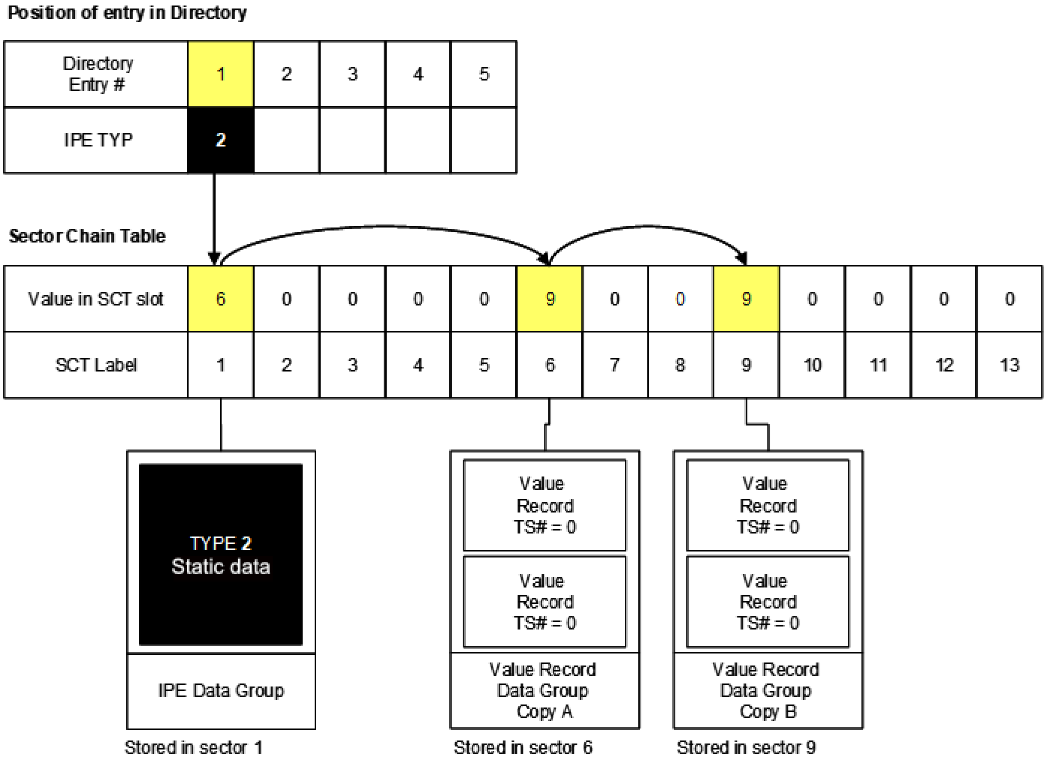
Where an IPE Data Group is associated with a Value Record Data Group, there shall be two copies of the Value Record Data Group. These two Value Record Data Groups shall be labelled Copy A and Copy B respectively.

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.

[49] i.e a copy held within the POSTs memory



Position of entry in Directory

Directory Entry #	1	2	3	4	5
IPE TYP	2				

Sector Chain Table

Value in SCT slot	6	0	0	0	0	9	0	0	9	0	0	0	0
SCT Label	1	2	3	4	5	6	7	8	9	10	11	12	13

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.

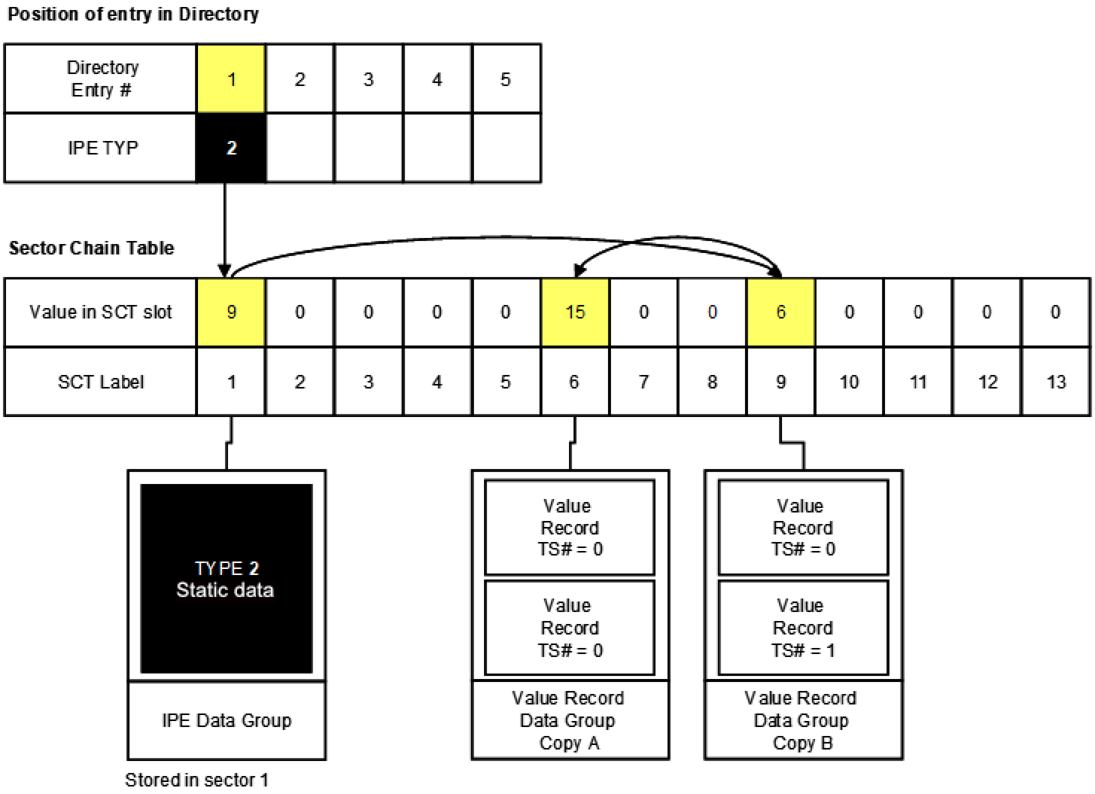
When a Value Record Data Group is created, sufficient memory space shall be allocated for the number of Value Records supported. The VGBitMap Data Element indicates how many Records a Value Record Dataset supports and the A and B copies of the Data Group shall support the same number. The minimum number 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.



Position of entry in Directory

Directory Entry #	1	2	3	4	5
IPE TYP	2				

Sector Chain Table

Value in SCT slot	9	0	0	0	0	15	0	0	6	0	0	0	0
SCT Label	1	2	3	4	5	6	7	8	9	10	11	12	13

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.

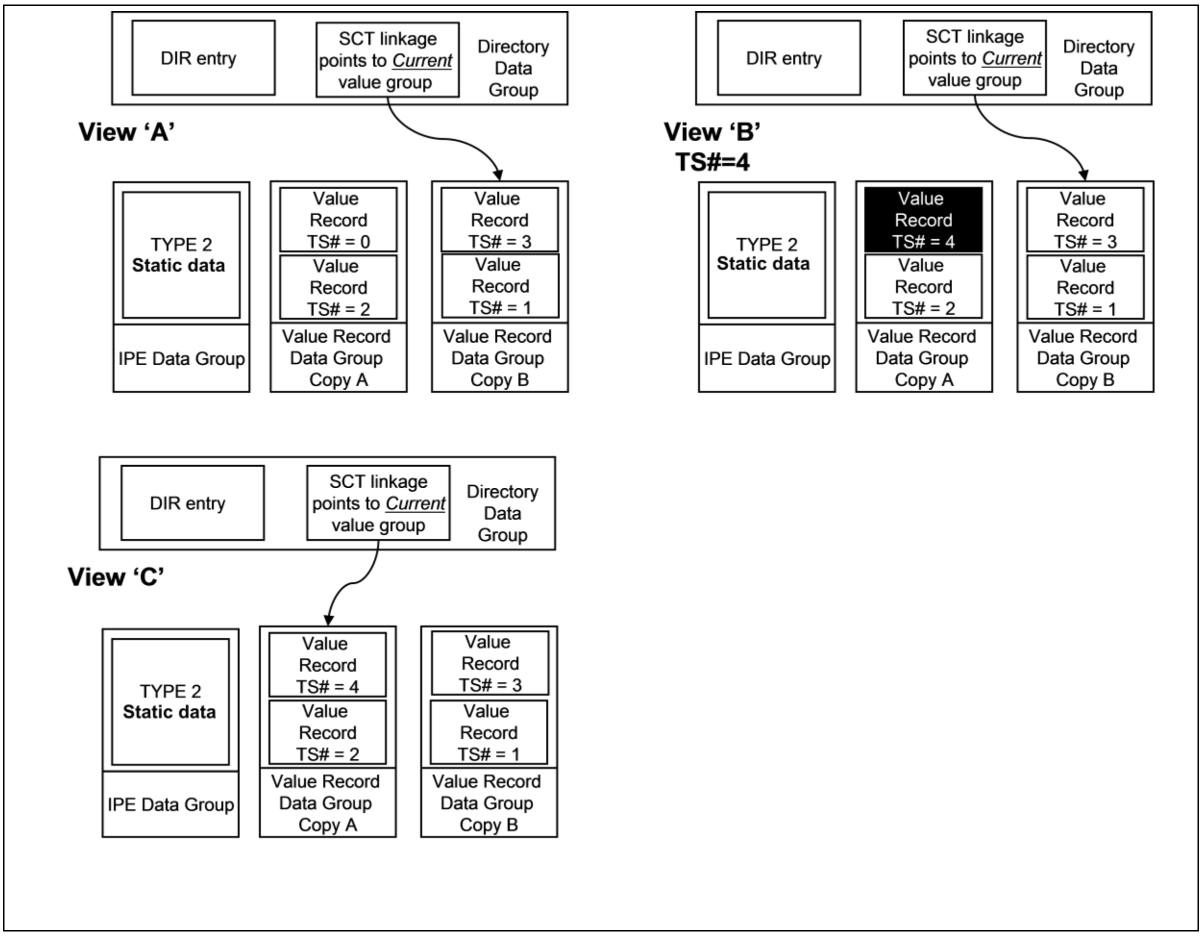


Figure A.3 - Value Record updating

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.

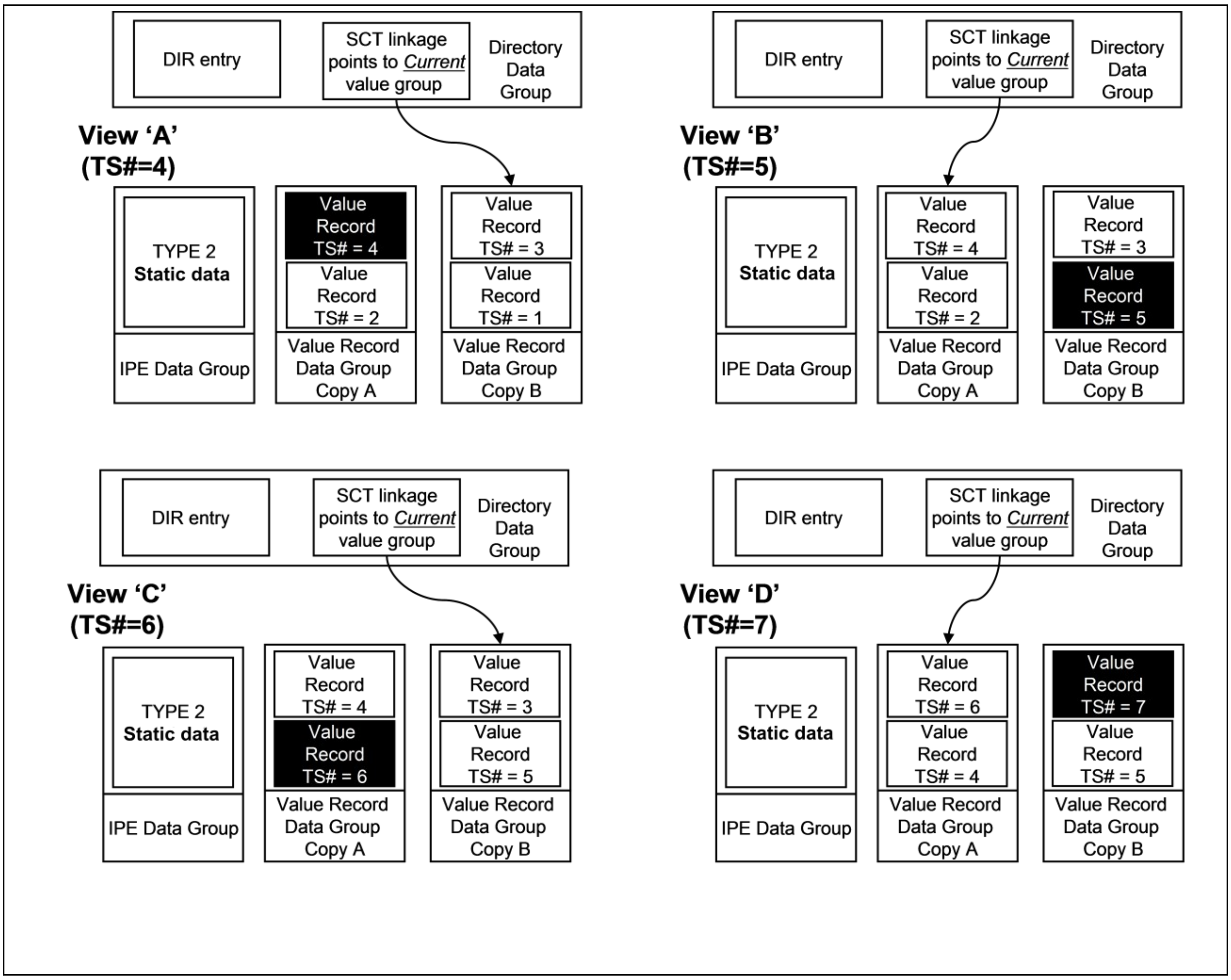


Figure A.4 - Value Record updating

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[50]. The SCT link order in the Directory has not been correctly updated to point to Copy B as Current.

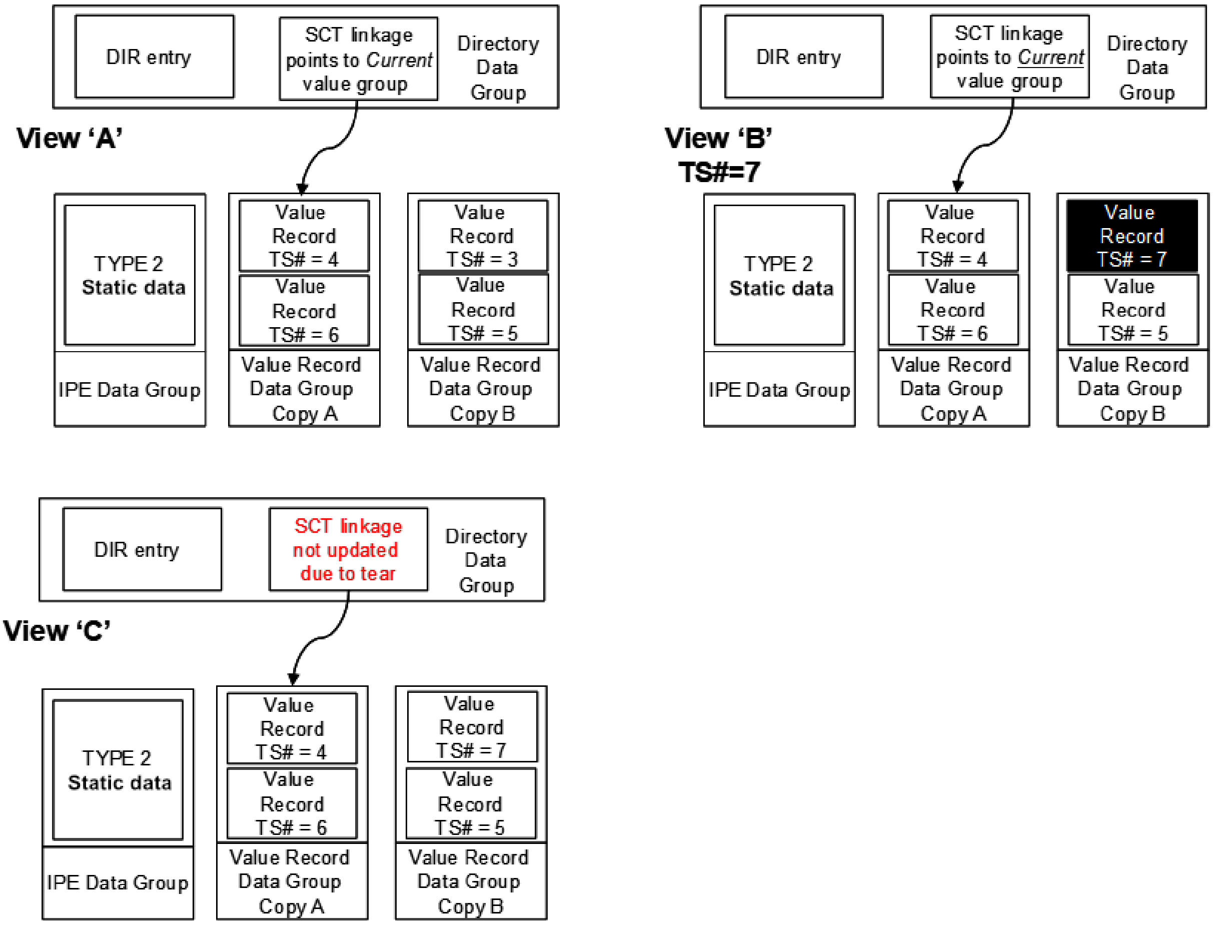


Figure A.5 - Torn transaction (Directory write)

[50] Note: As defined in ITSO TS 1000-3, the POST must check for such tearing and must take appropriate actions to 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*.

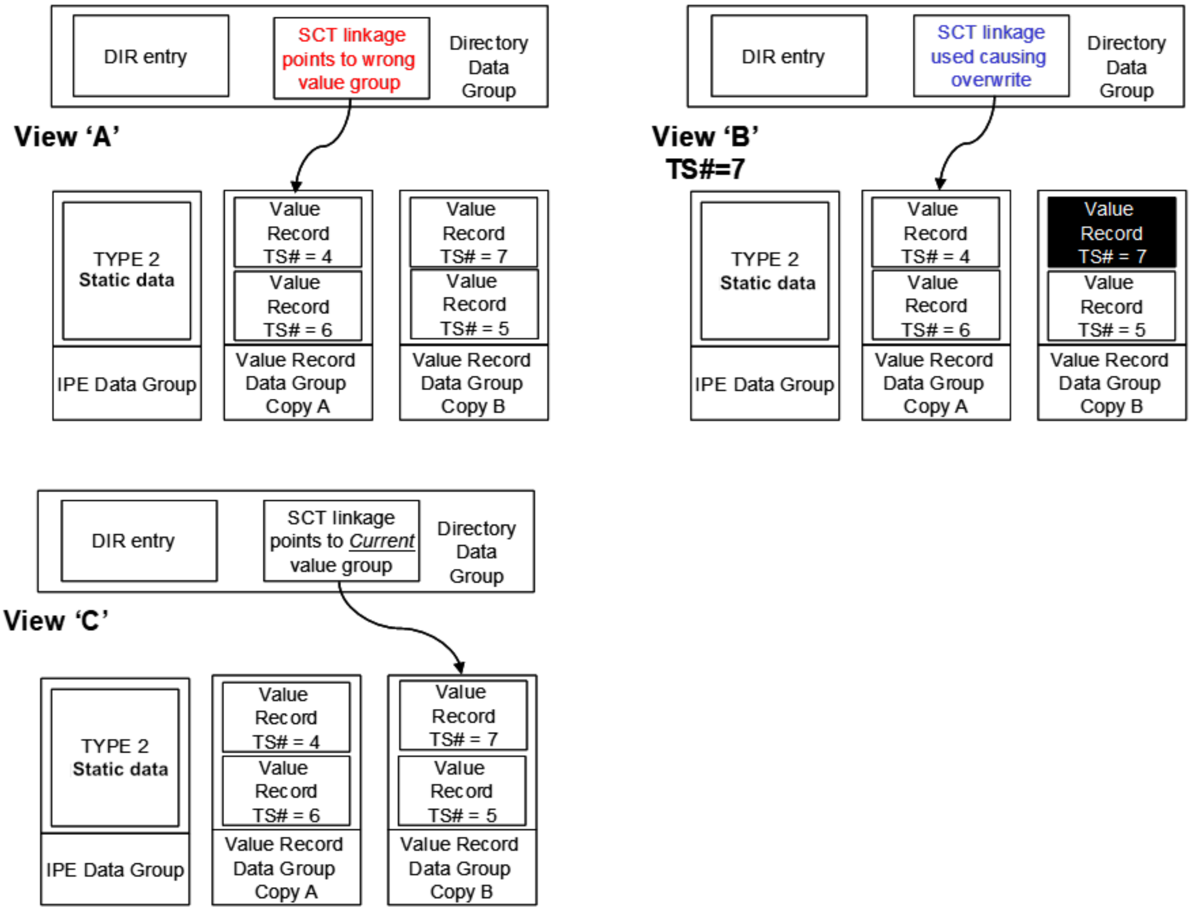


Figure A.6 - Processing after torn Directory write

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.

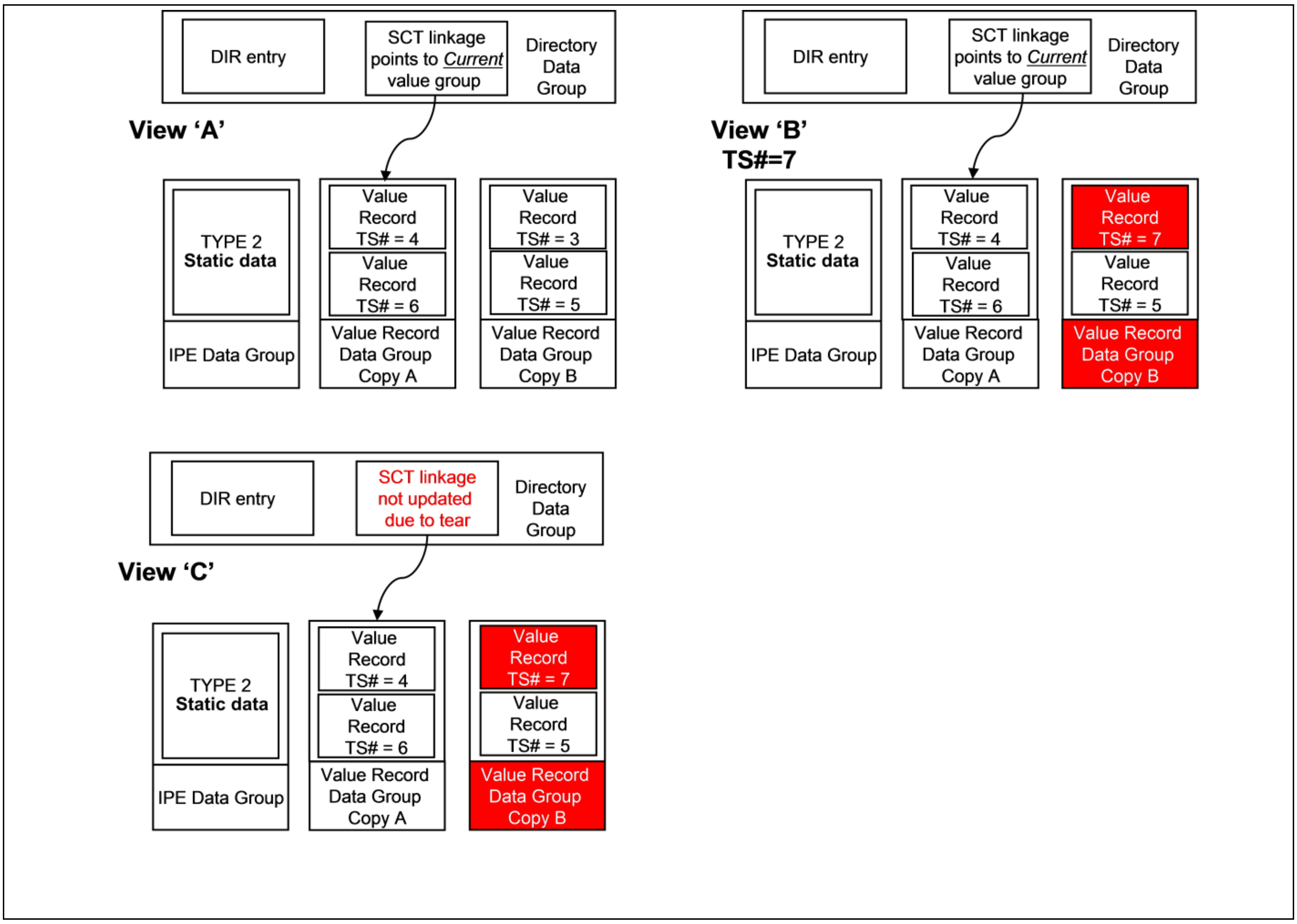


Figure A.7 - Torn transaction (Value Record write)

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*.

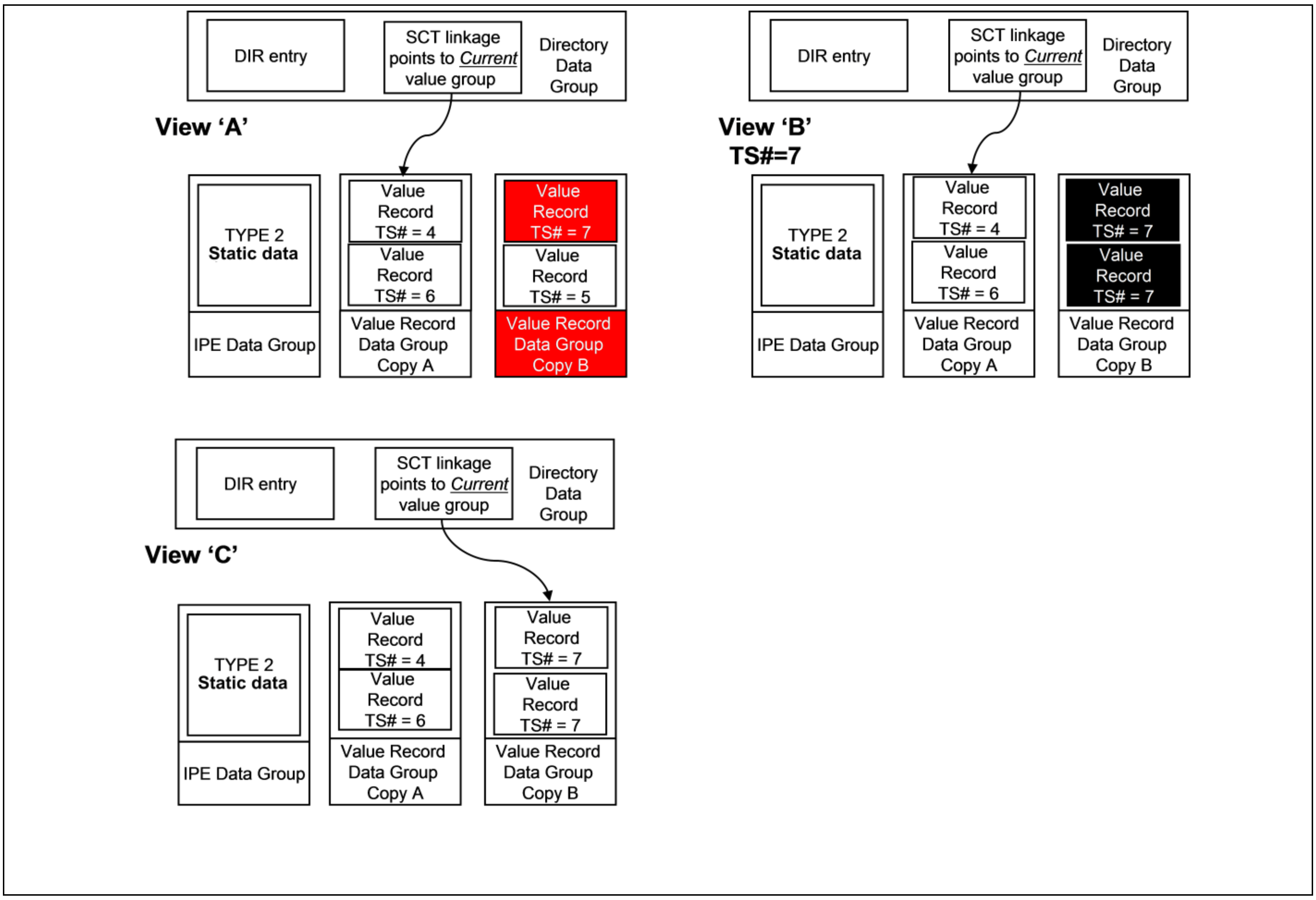


Figure A.8 - Processing after torn Value Record write

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)

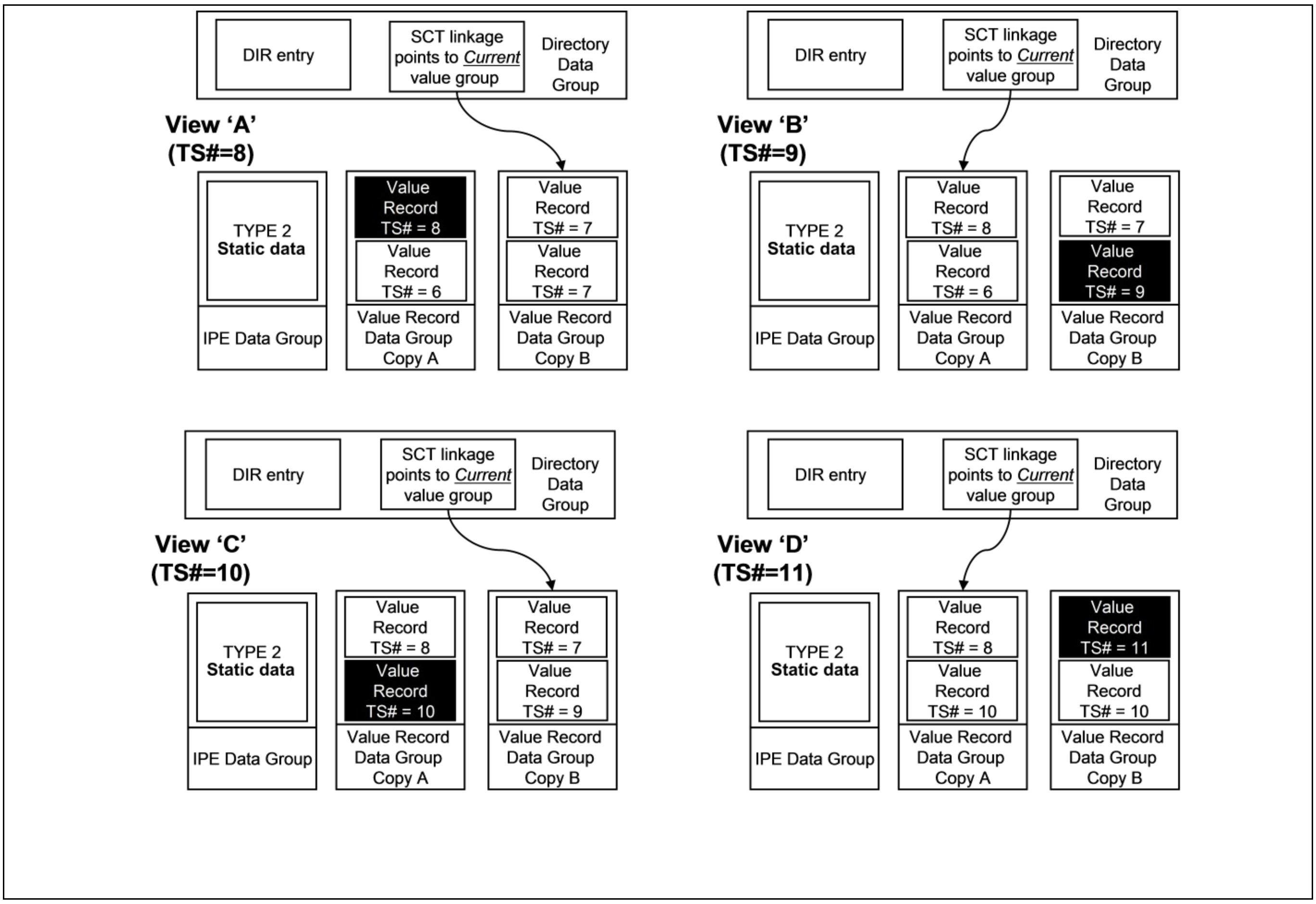


Figure A.9 - Overwriting where there are multiple records with same TS#

A.3.2.4.3 Corrupt Current copy

Under normal operation the *Current* copy of the Value Record Dataset should not become corrupted[51] 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.

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*.

[51] Where corrupt is taken to mean that the Seal is not correct

Figure A.10 - Processing when *Current* copy is corrupt. 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.

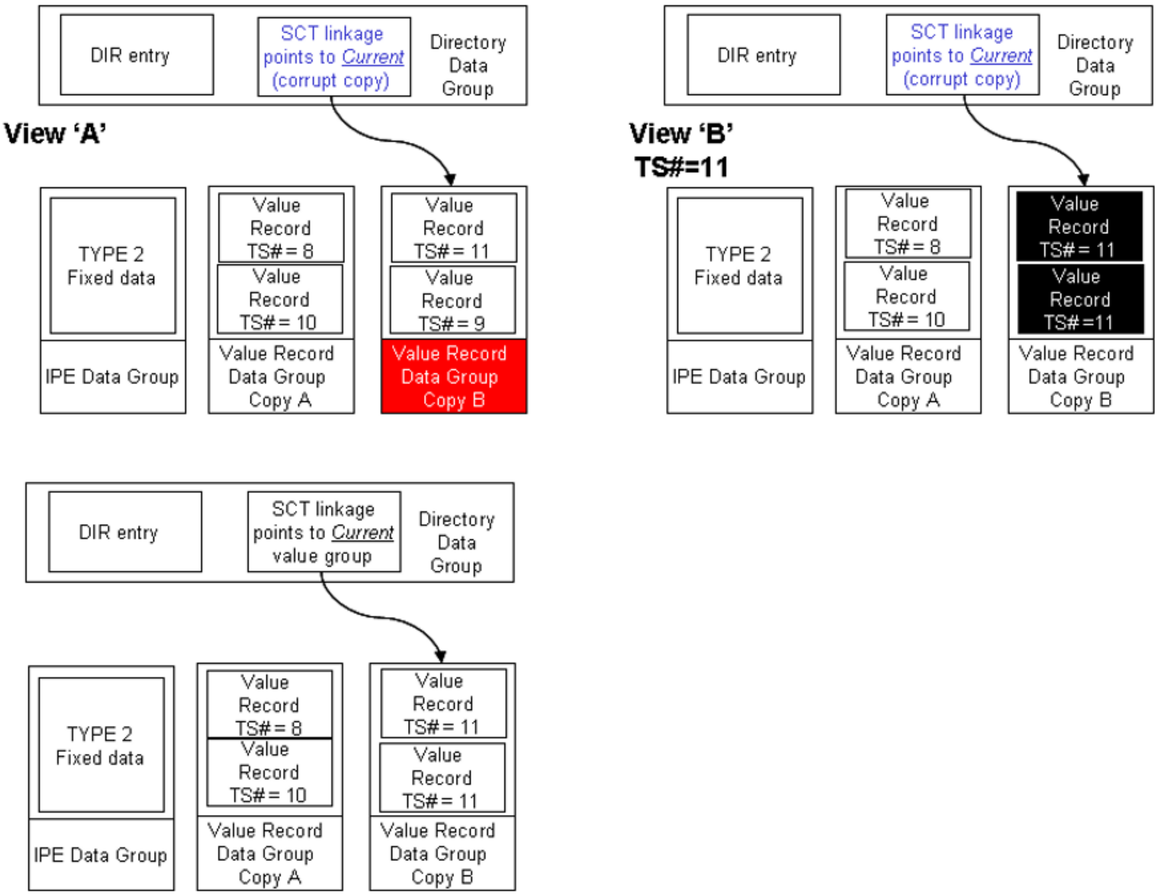


Figure A.10 - Processing when Current copy is corrupt

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 than 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 copy[52] 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.

[52] i.e. a copy held within the POSTs 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