Specification for the use of Mifare® 4K

Version: 2.3

28’th May 2007

Revision History

Ver	Date	Author	Description of Changes
2.3	28/05/07	Owen Mc Laughlin	Adopted by LASSeO
2.2	10/12/06	Owen Mc Laughlin	Addition of CRC algorithms
2.1	10/02/06	Owen Mc Laughlin	Corrected GPB error Clarified Mifare AID format
2.0	08/09/05	Euan Tennant	Version signed off by SmartConnect User Group Meeting on 8th September 2005.
1.2	02/08/05	Euan Tennant	Enhancements: 1. Use different AIDs for NSCP Directory / NSCP Services Directory and USID Data Sectors 2. Service Labels (Tag '50') are now Mandatory 3. Add USID '9999' – Reserved 4. Add reference to NSCP Services and Data Objects document
1.1	15/06/05	Euan Tennant	Initial version for review.
1.0	10/06/05	Euan Tennant	Initial version for release.

Preface

Scope

This document is intended as specification for the provision of local authority services on a Mifare® 4K Classic card.

Intended Readership

Developers requiring to integrate with a Mifare® 4K card encoded in accordance with this specification.

Related Documents

[1] Mifare® Standard 4kByte Card IC MF1 IC S70 Functional Specification (m043531)
[2] Mifare® Standardisation Group – Mifare® Application Directory Specification Standardisation Note (m001824)
[3] Mifare® Interface Platform Type Identification Procedure (m018411)
[4] ITSO Technical Specification 1000-2 – Interoperable public transport ticketing using contactless smart customer media – Part 2: Customer Media data and Customer Media architecture (ITSO TS 1000-2)
[5] ITSO Technical Specification 1000-10 – Interoperable public transport ticketing using contactless smart customer media – Part 10: Customer Media definitions (ITSO TS 1000-10)
[6] Smart Card Systems: Interoperable Citizen Services: Extended User Related Information: Part 1 – Definition of User Related Information and Implementation (CWA 13987-1)
[7] Information technology – Telecommunications and information exchange between systems – High level data link control (HDLC) procedures (ISO/IEC 13239 previously ISO/IEC 3309)
[8] NSCP “Services and Data Definitions” version 0.5
[9] NSCP “Specifications for Javacard Implementations” version 0.4

Glossary

Term	*Definition*
AID	Application Identifier
CCDA	Common Cardholder Data Application
CPS	Card Publisher Sector
CRC	Cyclic Redundancy Check
GPB	General Purpose Byte
IPE	ITSO Product Entity
ITSO	Integrated Transport Smartcard Organisation
MAD	Mifare® Application Directory
NSCP	National Smartcard Project
RFU	Reserved For Future Use
SAK	Select Acknowledgement
NSCP	Generic product name for outputs from the NSCP
SUG	NSCP User Group
TLV	Tag, Length, Value
UCI	Universal Card Holder Information
USID	Unique Services Identifier
‘XY’	Notation using the hexadecimal digits ‘0’ to ‘9’ and ‘A’ to ‘F’, equal to XY to the base 16

Contents

1 Introduction 1

2 Mifare® 4K Classic Memory Architecture 3

3 Mifare® 4K Classic Security Provisions 4

4 Mifare® 4K Classic ISO/IEC 14443 compliance 5

5 Mifare® Application Directory 6

6 NSCP Directory 7

7 NSCP Services Directory 8

8 USID Data Sectors 9

8.1 USID '9999' Reserved 10

9 Key Strategy 11

10 ITSO™ 12

10.1 Profile A 13
10.2 Profile B 14
10.3 Profile C 15
10.4 Profile E 15
10.5 Directory Data Group 16

11 Support for Mifare® 1K Classic Legacy Applications 18

11.1 Profile D 19

12 CRC Calculations 20

12.1 CRC 8 20
12.2 CRC16 20

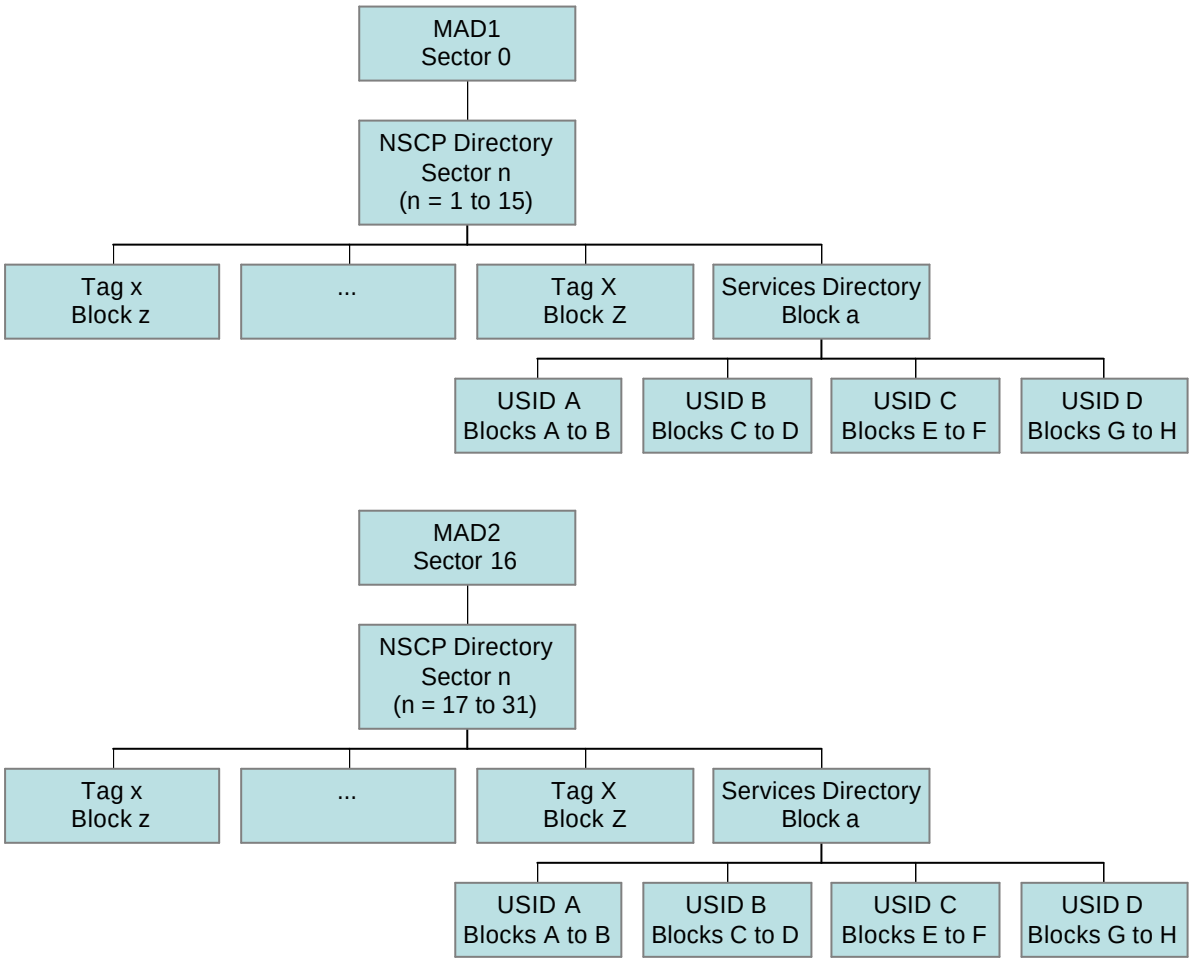
1 Introduction

This is a specification for the mapping of NSCP CCDA services data onto a Mifare® 4K Classic platform.

The Mifare® 4K platform is a low-end memory technology and should be considered to provide only minimal security. As such only free-read data elements should be held on this platform.

The mapping detailed in this specification allows gives flexibility for locating services data in indirectly addressed contiguous memory areas.

The top level addressing mechanism utilises the MAD standard with additional directory layers detailed below:



For MAD1 the NSCP Directory must be located within the first 1K of the Mifare® 4K platform.

For MAD2 the NSCP Directory must be located within the second 1K of the Mifare® 4K platform.

The Tags, Services Directory and USID data can be located anywhere within full 4K of memory.

2 Mifare® 4K Classic Memory Architecture

A Mifare® 4K Classic memory is divided as follows:

4096 bytes of EEPROM divided into 2 main areas:

- An area of 32 Sectors of 64 bytes (4 blocks) each (zone A)
- An area of 8 Sectors of 256 bytes (16 blocks) each (zone B)

Within zone A:

- 16 bytes are reserved for manufacturer data
- 512 bytes are reserved for keys and access control settings
- 1520 bytes are available for general storage of user data

Within zone B:

- 128 bytes are reserved for keys and access control settings
- 1920 bytes are available for general storage of user data

Refer to related document [3] for details of how to differentiate between the various Mifare® variants. Note that Philips makes proprietary use of certain bits in the SAK byte.

3 Mifare® 4K Classic Security Provisions

The platform provides the following security-related features:

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

4 Mifare® 4K Classic ISO/IEC 14443 compliance

This platform complies 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;

Note that tear prevention mechanisms will have to be implemented when writing to or updating data on this platform. These are required to protect the integrity of the data in situations where the card is removed from the card acceptor's RF field before all of the data is written.

It is recommended that where data is written the card is physically held in place to ensure that it cannot be removed from the RF field before all of the data is written.

CRCs are defined to span all NSCP data structures and allow card acceptors to detect torn cards.

5 Mifare® Application Directory

The MAD is simply a partition table rather than a directory.

The MAD1 is located in Sector 0 with the following structure:

Block 0	Manufacturers Data							
Block 1	CRC / Info	AID Sector 1	AID Sector 2	AID Sector 3	AID Sector 4	AID Sector 5	AID Sector 6	AID Sector 7
Block 2	AID Sector 8	AID Sector 9	AID Sector 10	AID Sector 11	AID Sector 12	AID Sector 13	AID Sector 14	AID Sector 15
Block 3	Key A			Access Conditions	GPB	Key B		

- See related document [2] and section 12 of this document for further details of CRC calculation.
  Please note the seed value for NSCP is 'C7' for all CRC 8 bit calculations.
- The Info byte contains the CPS if required. See related document [2] for further details
- The AIDs allocated for NSCP are '4011', '4012' and '4013'.
  - '4011' is used for the NSCP Directory
  - '4012' is used for the NSCP Services Directory and USID Data Sectors

  Mifare AIDs are stored little-endian, ie the NSCP AID '4011' would be stored with '11' at the lower memory address.
- The GPB is set to 'C1' for MAD1 and 'C2' for MAD2
- The Access Conditions are set to '787788'. This setting has the effect of:
  - Allowing read access with key A or key B.
  - Allowing write access with key B.
  - Not allowing the use of the increment command.
  - Not allowing the use of the decrement command.
  - Not allowing the use of the transfer command.
  - Not allowing the use of the restore command.

To minimise data usage it is recommended that only MAD1 is utilised.

6 NSCP Directory

The NSCP AID points to the NSCP Directory occupying one sector within Zone A. The NSCP Directory has the following structure:

Block 0	CRC / RFU	Tag / Block 1	Tag / Block 2	Tag / Block 3	Tag / Block 4	Tag / Block 5	Tag / Block 6	Tag / Block 7
Block 1	Tag / Block 8	Tag / Block 9	Tag / Block 10	Tag / Block 11	Tag / Block 12	Tag / Block 13	Tag / Block 14	Tag / Block 15
Block 2	Tag / Block 16	Tag / Block 17	Tag / Block 18	Tag / Block 19	Tag / Block 20	Tag / Block 21	Tag / Block 22	Tag / Block 23
Block 3	Key A			Access Conditions	GPB	Key B		

- The CRC is calculated as for a MAD2 structure. See related document [2] and section 12 of this document for further details of the CRC calculation.
- RFU is set to ‘00’
- The GPB is set to ‘00’
- The Access Conditions are set to ‘787788’. This setting has the effect of:
  - Allowing read access with key A or key B.
  - Allowing write access with key B.
  - Not allowing the use of the increment command.
  - Not allowing the use of the decrement command.
  - Not allowing the use of the transfer command.
  - Not allowing the use of the restore command.

In order to maintain some degree of interoperability with existing Mifare® 1K Classic acceptance network this directory allows existing data items contained in the current NSCP 1K mapping to be addressed.

The structure for each Tag / Block field is a 1 byte Tag followed by a 1 byte absolute block offset. Unused Tag / Block fields should contain the value ‘0000’.

The tags for these data elements and default absolute block offsets are as follows:

Data Item	**Tag**	**NSCP Mifare® 1K Classic Block Offset**
Cardholder Number	‘C0’	‘34’ (Sector 13, Block 0)
Leisure Number	‘C1’	‘2C’ (Sector 11, Block 0)
Library Number	‘C2’	‘24’ (Sector 9, Block 0)
Purse Sector	‘C3’	‘20’ (Sector 8)
Purse Transaction Sector	‘C4’	‘1C’ (Sector 7)
Access Number	‘C5’	‘28’ (Sector 10, Block 0)
Card Expiry Date	‘C6’	‘35’ (Sector 13, Block 1)
Purse Top-up Sector	‘C7’	-
Scheme Specific Data Sector	‘CE’	‘30’ (Sector 12)
NSCP Services Directory	‘CF’	-

7 NSCP Services Directory

The NSCP Services Directory Tag points to the NSCP Services Directory occupying one sector within Zone A. The NSCP Services Directory has the following structure:

Block 0	CRC / RFU		USID 1	Start Block / Block Len	USID 2	Start Block / Block Len	USID 3	Start Block / Block Len
Block 1	USID 4	Start Block / Block Len	USID 5	Start Block / Block Len	USID 6	Start Block / Block Len	USID 7	Start Block / Block Len
Block 2	USID 8	Start Block / Block Len	USID 9	Start Block / Block Len	USID 10	Start Block / Block Len	USID 11	Start Block / Block Len
Block 3	Key A			Access Conditions	GPB	Key B		

- The CRC is calculated as for a MAD2 structure. See related document [2] and section 12 of this document for further details of the CRC calculation.
- RFU is set to ‘000000’
- The GPB is set to ‘00’
- The Access Conditions are set to ‘787788’. This setting has the effect of:
  - Allowing read access with key A or key B.
  - Allowing write access with key B.
  - Not allowing the use of the increment command.
  - Not allowing the use of the decrement command.
  - Not allowing the use of the transfer command.
  - Not allowing the use of the restore command.

Valid USIDs (2 bytes) are as follows:

USID	Service
‘0001’	CCDA
‘0002’	Health
‘0003’	Organ Donor
‘0004’	Leisure
‘0005’	Trust
‘0006’	Sure Start
‘0007’	Special Needs
‘0065’	UCI
‘9999’	Reserved

Unused USID fields should contain the value ‘0000’.

The structure for each Start Block / Block Len field is a one byte absolute block start offset followed by a one byte length defining the number of contiguous blocks (excluding sector trailer blocks) occupied by the USID data. Unused Start Block / Block Len fields should contain the value ‘0000’.

8 USID Data Sectors

USID data can span multiple contiguous sectors.

USID data will be encoded using constructed BER-TLV data objects of format {T-L-{T1-L1-V1} … -{Tn-Ln-Vn}} stored across a number of contiguous blocks as indicated for each USID in the NSCP Services Directory.

The initial constructed tag field T will be as follows:

USID	Service	Constructed Tag
'0001'	CCDA	'E0'
'0002'	Health	'E0'
'0003'	Organ Donor	'E0'
'0004'	Leisure	'E0'
'0005'	Trust	'E0'
'0006'	Sure Start	'E0'
'0007'	Special Needs	'E0'
'0008'	T-Scheme Authentication	'E0'
'0009'	Membership	'E0'
'000A'	Employment	'E0'
'000B'	Driver Permit	'E0'
'000C'	UCI	'65'

The following length field L will be 1 or 2 bytes in length.

Tag fields T1 … Tn will be 1 or 2 bytes in length. Each length field L1 … Ln includes the length of the data format field contained with the value field and will be 1 or 2 bytes in length. Each value field V1 … Vn will contain as the first byte the data format followed by the variable length data element.

The USID data constructed BER-TLV data object will then be followed by a mandatory primitive data object of format T-L-V containing a two byte checksum. This checksum uses CRC_B encoding using initial value 'FFFF'. See related document [7] and section 12 of this document for further details. The tag field of the checksum data object will be 'C0'.

The checksum is calculated on all of the bytes of the USID data up to and including the tag and length fields of the checksum data object.

The most significant byte of the checksum shall be encoded first in the value field, also known as "big endian".

Any unutilised memory after the checksum data object will be padded with '00'.

See related document [8] for all the supported tags for each USID. Note that the Max Length does not include the data format field.

Each sector trailer block will be encoded as follows:

- The GPB is set to ‘00’
- The Access Conditions are set to ‘787788’. This setting has the effect of:
  - Allowing read access with key A or key B.
  - Allowing write access with key B.
  - Not allowing the use of the increment command.
  - Not allowing the use of the decrement command.
  - Not allowing the use of the transfer command.
  - Not allowing the use of the restore command.

8.1 USID ‘9999’ Reserved

Extra ‘reserved’ blocks can be allocated to allow for other services data to grow in the future. All bytes in these blocks will be set to ‘00’.

9 Key Strategy

The following table defines which keys will be used to access directories and data items:

Directory / Data Item	Key A (read only)	Key B (read / write)
MAD1	MAD Public Read Key	Issuer Scheme Key
MAD2	MAD Public Read Key	Issuer Scheme Key
NSCP Directory	NSCP Default Read Key	Issuer Scheme Key
Cardholder Number	MAD Public Read Key	Issuer Scheme Key
Leisure Number	NSCP Default Read Key	Issuer Scheme Key
Library Number	NSCP Default Read Key	Issuer Scheme Key
Purse Sector	Purse Read Key	Purse Write Key
Purse Transaction Sector	NSCP Default Read Key	Purse Write Key
Access Number	Access Read Key	Access Write Key
Card Expiry Date	MAD Public Read Key	Issuer Scheme Key
Scheme Specific Data	NSCP Default Read Key	Issuer Scheme Key
NSCP Services Directory	NSCP Default Read Key	Issuer Scheme Key
USID Data Sectors	NSCP Default Read Key	Issuer Scheme Key

The MAD Public Read Key will allow read access to appropriate MAD and cardholder sectors. It shall be the non-diversified MAD Key ('A0A1A2A3A4A5'). See related document [2] for further details.

The NSCP Default Read Key will allow read access to appropriate sectors. It shall be the non-diversified NSCP Default Key ('1494E81663D7').

The Issuer Scheme Key will allow read / write access to appropriate sectors The card issuer will determine what diversification mechanisms shall be employed for this key.

The Purse Read Key will allow read access to appropriate purse sectors. The purse owner will determine what diversification mechanisms shall be employed for this key.

The Purse Write Key will allow read / write access to appropriate purse sectors. The purse owner will determine what diversification mechanisms shall be employed for this key.

The Access Read Key will allow read access to appropriate access system sectors. The access system operator will determine what diversification mechanisms shall be employed for this key.

The Access Write Key will allow read / write access to appropriate access system sectors. The access system operator will determine what diversification mechanisms shall be employed for this key.

10 ITSO™

Local Authority issuers who are also ITSO™ issuers should be able to issue cards to hold both NSCP data and an ITSO™ shell. The following section describes a method for doing this devised after lengthy consultations with the Association of ITSO Licenced Operators.

Care must be taken to ensure that sectors occupied by MAD1, NSCP Directories and Data are referenced in the Sector Chain Table contained in the ITSO™ Data Directory Group as a Private Application. This is to ensure that ITSO™ shells and NSCP data do not overlap and will not interfere with each other.

The mapping below shows the mandatory allocation of sectors for NSCP (Red) and ITSO (Green) usage.

<table>
<tr><th colspan="4">Zone A</th><th colspan="4">Zone B</th></tr>
<tr><td>Sector 0</td><td>MAD1</td><td>Sector 16</td><td>ITSO Shell Environment Data Group</td><td rowspan="4">Sector 32</td><td rowspan="4"></td><td rowspan="4">Sector 36</td><td rowspan="4"></td></tr>
<tr><td>Sector 1</td><td></td><td>Sector 17</td><td></td></tr>
<tr><td>Sector 2</td><td></td><td>Sector 18</td><td></td></tr>
<tr><td>Sector 3</td><td></td><td>Sector 19</td><td></td></tr>
<tr><td>Sector 4</td><td></td><td>Sector 20</td><td></td><td rowspan="4">Sector 33</td><td rowspan="4"></td><td rowspan="4">Sector 37</td><td rowspan="4"></td></tr>
<tr><td>Sector 5</td><td></td><td>Sector 21</td><td></td></tr>
<tr><td>Sector 6</td><td></td><td>Sector 22</td><td></td></tr>
<tr><td>Sector 7</td><td></td><td>Sector 23</td><td></td></tr>
<tr><td>Sector 8</td><td></td><td>Sector 24</td><td></td><td rowspan="4">Sector 34</td><td rowspan="4"></td><td rowspan="4">Sector 38</td><td rowspan="4"></td></tr>
<tr><td>Sector 9</td><td></td><td>Sector 25</td><td></td></tr>
<tr><td>Sector 10</td><td></td><td>Sector 26</td><td></td></tr>
<tr><td>Sector 11</td><td></td><td>Sector 27</td><td></td></tr>
<tr><td>Sector 12</td><td></td><td>Sector 28</td><td></td><td rowspan="4">Sector 35</td><td rowspan="4"></td><td rowspan="4">Sector 39</td><td rowspan="4">ITSO Directory Data Group</td></tr>
<tr><td>Sector 13</td><td></td><td>Sector 29</td><td></td></tr>
<tr><td>Sector 14</td><td></td><td>Sector 30</td><td></td></tr>
<tr><td>Sector 15</td><td></td><td>Sector 31</td><td></td></tr>
</table>

3 possible scenarios are envisaged for cards requiring NSCP and ITSO™ to co-exist.

10.1 Profile A

<table>
<tr><th colspan="4">Zone A</th><th colspan="4">Zone B</th></tr>
<tr><td>Sector 0</td><td>MAD1</td><td>Sector 16</td><td>ITSO Shell Environment Data Group</td><td rowspan="4">Sector 32</td><td rowspan="4">Reserved for ITSO</td><td rowspan="4">Sector 36</td><td rowspan="4">Reserved for ITSO</td></tr>
<tr><td>Sector 1</td><td>NSCP Directory</td><td>Sector 17</td><td>Reserved for ITSO</td></tr>
<tr><td>Sector 2</td><td>NSCP Services Directory</td><td>Sector 18</td><td>Reserved for ITSO</td></tr>
<tr><td>Sector 3</td><td>Reserved for NSCP</td><td>Sector 19</td><td>Reserved for ITSO</td></tr>
<tr><td>Sector 4</td><td>Reserved for NSCP</td><td>Sector 20</td><td>Reserved for ITSO</td><td rowspan="4">Sector 33</td><td rowspan="4">Reserved for ITSO</td><td rowspan="4">Sector 37</td><td rowspan="4">Reserved for ITSO</td></tr>
<tr><td>Sector 5</td><td>Reserved for NSCP</td><td>Sector 21</td><td>Reserved for ITSO</td></tr>
<tr><td>Sector 6</td><td>Reserved for NSCP</td><td>Sector 22</td><td>Reserved for ITSO</td></tr>
<tr><td>Sector 7</td><td>Reserved for NSCP</td><td>Sector 23</td><td>Reserved for ITSO</td></tr>
<tr><td>Sector 8</td><td>Reserved for NSCP</td><td>Sector 24</td><td>Reserved for ITSO</td><td rowspan="4">Sector 34</td><td rowspan="4">Reserved for ITSO</td><td rowspan="4">Sector 38</td><td rowspan="4">Reserved for ITSO</td></tr>
<tr><td>Sector 9</td><td>Reserved for NSCP</td><td>Sector 25</td><td>Reserved for ITSO</td></tr>
<tr><td>Sector 10</td><td>Reserved for NSCP</td><td>Sector 26</td><td>Reserved for ITSO</td></tr>
<tr><td>Sector 11</td><td>Reserved for NSCP</td><td>Sector 27</td><td>Reserved for ITSO</td></tr>
<tr><td>Sector 12</td><td>Reserved for NSCP</td><td>Sector 28</td><td>Reserved for ITSO</td><td rowspan="4">Sector 35</td><td rowspan="4">Reserved for ITSO</td><td rowspan="4">Sector 39</td><td rowspan="4">ITSO Directory Data Group</td></tr>
<tr><td>Sector 13</td><td>Reserved for NSCP</td><td>Sector 29</td><td>Reserved for ITSO</td></tr>
<tr><td>Sector 14</td><td>Reserved for NSCP</td><td>Sector 30</td><td>Reserved for ITSO</td></tr>
<tr><td>Sector 15</td><td>Reserved for NSCP</td><td>Sector 31</td><td>Reserved for ITSO</td></tr>
</table>

This profile allocates a maximum of 624 bytes for NSCP data structures.

The NSCP Directory and NSCP Services Directory may be located in any of the NSCP sectors from 1 to 15.

10.2 Profile B

Zone A				Zone B			
Sector 0	MAD1	Sector 16	ITSO Shell Environment Data Group	Sector 32	Reserved for ITSO	Sector 36	Reserved for ITSO
Sector 1	NSCP Directory	Sector 17	Reserved for ITSO				
Sector 2	NSCP Services Directory	Sector 18	Reserved for ITSO				
Sector 3	Reserved for NSCP	Sector 19	Reserved for ITSO				
Sector 4	Reserved for NSCP	Sector 20	Reserved for ITSO	Sector 33	Reserved for ITSO	Sector 37	Reserved for ITSO
Sector 5	Reserved for NSCP	Sector 21	Reserved for ITSO				
Sector 6	Reserved for NSCP	Sector 22	Reserved for ITSO				
Sector 7	Reserved for NSCP	Sector 23	Reserved for ITSO				
Sector 8	Reserved for NSCP	Sector 24	Reserved for ITSO	Sector 34	Reserved for ITSO	Sector 38	Reserved for ITSO
Sector 9	Reserved for NSCP	Sector 25	Reserved for NSCP				
Sector 10	Reserved for NSCP	Sector 26	Reserved for NSCP				
Sector 11	Reserved for NSCP	Sector 27	Reserved for NSCP				
Sector 12	Reserved for NSCP	Sector 28	Reserved for NSCP	Sector 35	Reserved for ITSO	Sector 39	ITSO Directory Data Group
Sector 13	Reserved for NSCP	Sector 29	Reserved for NSCP				
Sector 14	Reserved for NSCP	Sector 30	Reserved for NSCP				
Sector 15	Reserved for NSCP	Sector 31	Reserved for NSCP				

This profile allocates a maximum of 960 bytes for NSCP data structures.

The NSCP Directory may be located in any of the NSCP sectors from 1 to 15.

The NSCP Services Directory may be located in any of the NSCP sectors from 1 to 15 and 25 to 31.

10.3 Profile C

Sector 0	MAD1	Sector 16	ITSO Shell Environment Data Group	Sector 32	Reserved for NSCP	Sector 36	Reserved for NSCP
Sector 1	NSCP Directory	Sector 17	Reserved for ITSO				
Sector 2	NSCP Services Directory	Sector 18	Reserved for ITSO				
Sector 3	Reserved for NSCP	Sector 19	Reserved for ITSO				
Sector 4	Reserved for NSCP	Sector 20	Reserved for ITSO	Sector 33	Reserved for NSCP	Sector 37	Reserved for NSCP
Sector 5	Reserved for NSCP	Sector 21	Reserved for ITSO				
Sector 6	Reserved for NSCP	Sector 22	Reserved for ITSO				
Sector 7	Reserved for NSCP	Sector 23	Reserved for ITSO				
Sector 8	Reserved for NSCP	Sector 24	Reserved for ITSO	Sector 34	Reserved for NSCP	Sector 38	Reserved for ITSO
Sector 9	Reserved for NSCP	Sector 25	Reserved for ITSO				
Sector 10	Reserved for NSCP	Sector 26	Reserved for ITSO				
Sector 11	Reserved for NSCP	Sector 27	Reserved for ITSO				
Sector 12	Reserved for NSCP	Sector 28	Reserved for ITSO	Sector 35	Reserved for NSCP	Sector 39	ITSO Directory Data Group
Sector 13	Reserved for NSCP	Sector 29	Reserved for ITSO				
Sector 14	Reserved for NSCP	Sector 30	Reserved for ITSO				
Sector 15	Reserved for NSCP	Sector 31	Reserved for ITSO				

This profile allows a maximum of 2064 bytes for NSCP data structures.
The NSCP Directory may be located in any of the NSCP sectors from 1 to 15.
The NSCP Services Directory may be located in any of the NSCP sectors from 1 to 15.

10.4 Profile E

Sector 0	MAD1	Sector 16	ITSO Shell Environment Data Group	Sector 32	Reserved for NSCP	Sector 36	Reserved for ITSO
Sector 1	NSCP Directory	Sector 17	Reserved for ITSO				
Sector 2	NSCP Services Directory	Sector 18	Reserved for ITSO				
Sector 3	Reserved for NSCP	Sector 19	Reserved for ITSO				
Sector 4	Reserved for NSCP	Sector 20	Reserved for ITSO	Sector 33	Reserved for NSCP	Sector 37	Reserved for ITSO
Sector 5	Reserved for NSCP	Sector 21	Reserved for ITSO				
Sector 6	Reserved for NSCP	Sector 22	Reserved for ITSO				
Sector 7	Reserved for NSCP	Sector 23	Reserved for ITSO				
Sector 8	Reserved for NSCP	Sector 24	Reserved for ITSO	Sector 34	Reserved for NSCP	Sector 38	Reserved for ITSO
Sector 9	Reserved for NSCP	Sector 25	Reserved for ITSO				

Sector 10	Reserved for NSCP	Sector 26	Reserved for ITSO				
Sector 11	Reserved for NSCP	Sector 27	Reserved for ITSO				
Sector 12	Reserved for NSCP	Sector 28	Reserved for ITSO	Sector 35	Reserved for NSCP	Sector 39	ITSO Directory Data Group
Sector 13	Reserved for NSCP	Sector 29	Reserved for ITSO				
Sector 14	Reserved for NSCP	Sector 30	Reserved for ITSO				
Sector 15	Reserved for NSCP	Sector 31	Reserved for ITSO				

This profile allows a maximum of 1712 bytes for NSCP data structures.
The NSCP Directory may be located in any of the NSCP sectors from 1 to 15.
The NSCP Services Directory may be located in any of the NSCP sectors from 1 to 15.

10.5 Directory Data Group

The Directory Data Group located in Sector 39 must have a Directory Entry E1 indicating the presence of a Private Application in accordance with related documents [4] and [5]:

- IPE Type (TYP) = 0
- IPE Sub Type (PTYP) = 0
- Value Group Present flag (VGP) = 0
- Expiry (EXP) = 0

The Sector Chain Tables required to support the above 4 profiles are as follows:

SCT Label	Media Sector	Profile A SCT Entry Value	Profile B SCT Entry Value	Profile C SCT Entry Value	Profile E SCT Entry Value
SCT1	Sector 1	14	14	14	14
SCT2	Sector 17				
SCT3	Sector 18				
SCT4	Sector 19				
SCT5	Sector 20				
SCT6	Sector 21				
SCT7	Sector 22				
SCT8	Sector 23				
SCT9	Sector 24				
SCT10	Sector 32			11	11
SCT11	Sector 33			12	12
SCT12	Sector 34			13	13
SCT13	Sector 35			35	14
SCT14	Sector 2	15	15	15	15
SCT15	Sector 3	16	16	16	16
SCT16	Sector 4	17	17	17	17
SCT17	Sector 5	18	18	18	18
SCT18	Sector 6	19	19	19	19
SCT19	Sector 7	20	20	20	20
SCT20	Sector 8	21	21	21	21
SCT21	Sector 9	22	22	22	22
SCT22	Sector 10	23	23	23	23
SCT23	Sector 11	24	24	24	24
SCT24	Sector 12	25	25	25	25
SCT25	Sector 13	26	26	26	26
SCT26	Sector 14	27	27	27	27
SCT27	Sector 15	27	28	10	10
SCT28	Sector 25		29		
SCT29	Sector 26		30		
SCT30	Sector 27		31		
SCT31	Sector 28		32		
SCT32	Sector 29		33		
SCT33	Sector 30		34		
SCT34	Sector 31		34		
SCT35	Sector 36			36	
SCT36	Sector 37			36	
SCT37	Sector 38				

Undefined entries will be utilised for the ITSO™ defined IPEs.

There will be no IPE Data Group defined for this Private Application.

11 Support for Mifare® 1K Classic Legacy Applications

Local Authority issuers may wish to issue cards to hold both NSCP data and other legacy applications currently hosted on Mifare® 1K Classic platforms. These legacy applications may not utilise MAD1 e.g. Oyster so a MAD2 will be used to partition the last 3K for NSCP usage.

A MAD2 is located in Sector 16 with the following structure:

Block 0	CRC / Info	AID Sector 17	AID Sector 18	AID Sector 19	AID Sector 20	AID Sector 21	AID Sector 22	AID Sector 23
Block 1	AID Sector 24	AID Sector 25	AID Sector 26	AID Sector 27	AID Sector 28	AID Sector 29	AID Sector 30	AID Sector 31
Block 2	AID Sector 32	AID Sector 33	AID Sector 34	AID Sector 35	AID Sector 36	AID Sector 37	AID Sector 38	AID Sector 39
Block 3	Key A			GPB	Access Conditions	Key B		

- See related document [2] for further details of CRC calculation
- The Info byte contains the CPS if required. See related document [2] for further details
- The AIDs allocated for NSCP are ‘4011’, ‘4012’ and ‘4013’.
  - ‘4011’ is used for the NSCP Directory
  - ‘4012’ is used for the NSCP Services Directory and USID Data Sectors
- The GPB is set to ‘C1’ for MAD1 and ‘C2’ for MAD2
- The Access Conditions are set to ‘787788’. This setting has the effect of:
  - Allowing read access with key A or key B.
  - Allowing write access with key B.
  - Not allowing the use of the increment command.
  - Not allowing the use of the decrement command.
  - Not allowing the use of the transfer command.
  - Not allowing the use of the restore command.

In this scenario the following profile will be utilised.

11.1 Profile D

Zone A				Zone B			
Sector 0	Reserved for legacy	Sector 16	MAD2	Sector 32	Reserved for NSCP	Sector 36	Reserved for NSCP
Sector 1	Reserved for legacy	Sector 17	NSCP Directory				
Sector 2	Reserved for legacy	Sector 18	NSCP Services Directory				
Sector 3	Reserved for legacy	Sector 19	Reserved for NSCP				
Sector 4	Reserved for legacy	Sector 20	Reserved for NSCP	Sector 33	Reserved for NSCP	Sector 37	Reserved for NSCP
Sector 5	Reserved for legacy	Sector 21	Reserved for NSCP				
Sector 6	Reserved for legacy	Sector 22	Reserved for NSCP				
Sector 7	Reserved for legacy	Sector 23	Reserved for NSCP				
Sector 8	Reserved for legacy	Sector 24	Reserved for NSCP	Sector 34	Reserved for NSCP	Sector 38	Reserved for NSCP
Sector 9	Reserved for legacy	Sector 25	Reserved for NSCP				
Sector 10	Reserved for legacy	Sector 26	Reserved for NSCP				
Sector 11	Reserved for legacy	Sector 27	Reserved for NSCP				
Sector 12	Reserved for legacy	Sector 28	Reserved for NSCP	Sector 35	Reserved for NSCP	Sector 39	Reserved for NSCP
Sector 13	Reserved for legacy	Sector 29	Reserved for NSCP				
Sector 14	Reserved for legacy	Sector 30	Reserved for NSCP				
Sector 15	Reserved for legacy	Sector 31	Reserved for NSCP				

This profile allocates a maximum of 2544 bytes for NSCP data structures.

The NSCP Directory and NSCP Services Directory may be located in any of the NSCP sectors from 17 to 31.

This profile cannot support an ITSO format.

12 CRC Calculations

The following C code shows examples for software generated 8 bit and 18 bit CRC values.

12.1 CRC 8

C routine for MAD and NSCP Directories

```
CRC 8bit
BYTE CalcCRC8(BYTE* byData, int nLength )
{
    int i,j;
    BYTE out;

    out = 0xC7;
    for (j = 0; j < nLength; j++)
    {
        out = out ^ byData[j];
        for (i = 0; i < 8; i++)
        {
            if ((out & 0x80) == 0x80)
            {
                out = (out << 1) ^ 0x1D;
            }
            Else
            {
                out = out << 1;
            }
        }
    }
    return (out);
}
```

12.2 CRC16

C routine for Service Data

```
CRC 16bit
WORD CalcCRC16(BYTE* byData, int nLength )
{
   int i,j;
   unsigned int;
   unsigned int crc16;

   out = 0xffff;

   for (j = 0; j  < nLength; j++
   {
      out = out  ^ ((unsigned int) byData[j] << 8);
      for (i = 0; i < 8; i++)
      {
            if((out & 0x8000) == 0x8000)
            {
                  out = (out << 1) ^ 0x1021;
```

```
            }
            else
            {
                  out = out << 1;
            }
      }
   }
   return (out);
}
```

** End of Document **