• mifare® DESFire Type ID
• mifare® DESFire ATQA
• mifare® DESFire SAK
• mifare® DESFire UID
• ISO14443A RATS & PPS
• mifare® DESFire (R)ATS
• mifare® DESFire PPS (Request)
• Block Exchange via „T=CL“
mifare® DESFire Type ID

PCD

Start

Anticollision Loop

ISO 14443-4 (T=CL)

SAK bit 6 = 1?

YES

NO

SAK bit 6 = 1?

Anticollision Loop

NO

YES

MIFARE® Classic

Proprietary frames and protocol

Bit frame anticollision supported?

NO

PCD

REQA

ATQA

PICO

ATQA

SAK

UID

Proprietary frames and protocol

UID + SAK

NO

ISO 14443-3 A

Semiconductors
### ATQA of mifare® ICs

<table>
<thead>
<tr>
<th>MIFARE® IC</th>
<th>MSB ATQA</th>
<th>LSB ATQA</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIFARE® UL (0x0044)</td>
<td>0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0</td>
<td></td>
</tr>
<tr>
<td>MIFARE® 1K (0x0004)</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0</td>
<td></td>
</tr>
<tr>
<td>MIFARE® 4K (0x0002)</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0</td>
<td></td>
</tr>
<tr>
<td>MIFARE® DESFire (0x0344)</td>
<td>0 0 0 0 0 1 1 0 1 0 0 0 1 0 0 0</td>
<td></td>
</tr>
<tr>
<td>MIFARE® ProX</td>
<td>0 0 0 0 0 0 X² X² X² 0 0 0 0 X² X² X² X²</td>
<td></td>
</tr>
</tbody>
</table>

1. All RFU bits shall be set to '0'
2. Depends on OS
### SAK bit values as defined in the ISO/IEC 14443A-3

<table>
<thead>
<tr>
<th>Bit no.</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cascade bit set: UID not complete</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UID complete, PICC compliant with ISO/IEC 14443-4</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UID complete, PICC not compliant with ISO/IEC 14443-4</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### SAK of mifare® ICs

<table>
<thead>
<tr>
<th>mifare® ICs</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIFARE® ultralight (0x04) – cascade level 1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MIFARE® ultralight (0x00) – cascade level 2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MIFARE® 1K (0x08)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MIFARE® 4K (0x18)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MIFARE® DESFire (0x24) – cascade level 1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MIFARE® DESFire (0x20) – cascade level 2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MIFARE® ProX</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

1 Depend on OS
Double or Triple Size UIDs:

<table>
<thead>
<tr>
<th>ISO 14443</th>
<th>UID0</th>
<th>UID1 – UID6 (resp. UID1 - UID9)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Manufacturer ID according to the ISO/IEC 7816-6/AM1</td>
<td>Each manufacturer is responsible for the uniqueness of the value of the other bytes of the unique number.</td>
</tr>
<tr>
<td>Philips</td>
<td>0x04</td>
<td>x</td>
</tr>
</tbody>
</table>

mifare® DESFire UID Coding
ISO 14443 - 4

mifare® DESFire PICC selected

Request for Answer to Select (RATS)
Answer To Select (ATS)
PPS Request
PPS Response
Exchange Transparent Data

NO
PCS supported?
YES
Reader PPS?
YES
Set parameter
NO

PPS = Protocol Parameter Select

PCD
PICC
Request for Answer To Select (RATS)

FSD: Maximum frame size supported by the PCD:

<table>
<thead>
<tr>
<th>FSDI</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9-F</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSD</td>
<td>16</td>
<td>24</td>
<td>32</td>
<td>40</td>
<td>48</td>
<td>64</td>
<td>96</td>
<td>128</td>
<td>256</td>
<td>RFU</td>
</tr>
</tbody>
</table>

CID: Logical number of the addressed PICC (0 – 14)

ATS (next slides)

Note: Times units are not drawn to scale!
ATS 1: Length Byte

Length Byte

Format Byte

Interface Bytes
Optional

Historical Bytes
Optional
ISO/IEC 7816-4 specifies the content

TL Interface Bytes
Optional

Historical Bytes
Optional
ISO/IEC 7816-4 specifies the content
ATS 2: Format Byte T0

FSCI to FSC conversion

<table>
<thead>
<tr>
<th>FSCI</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9 – F</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSC</td>
<td>16</td>
<td>24</td>
<td>32</td>
<td>40</td>
<td>48</td>
<td>64</td>
<td>96</td>
<td>128</td>
<td>256</td>
<td>RFU &gt; 256</td>
</tr>
</tbody>
</table>

FSC defines the maximum size of the PICC receive buffer.

FSCI … Frame Size for proximity Card Integer
FSC … Frame Size for proximity Card
ATS 3: Interface Byte TA(1)

- **Bit 7**: 0 .. Different D for each direction supported
  1 .. Only the same D for both directions supported.

- **Bit 6**: DS=8 (848 kBaud) supported, if bit is set to 1
- **Bit 5**: DS=4 (424 kBaud) supported, if bit is set to 1
- **Bit 4**: DS=2 (212 kBaud) supported, if bit is set to 1
- **Bit 2**: DR=8 (848 kBaud) supported, if bit is set to 1
- **Bit 1**: DR=4 (424 kBaud) supported, if bit is set to 1
- **Bit 0**: DR=2 (212 kBaud) supported, if bit is set to 1

- **DR**: Divisor Receive (PCD -> PICC)
- **DS**: Divisor Send (PICC -> PCD)
ATS 4: Interface Byte TB(1)

Frame Waiting Time:

Frame sent by PCD

Frame sent by PICC

t < FWT

Frame Waiting Time: $FWT = (256 \times 16 / fc) \times 2^{FWI}$

Example:

FWT$_{\text{MIN}}$ = 0: $(256 \times 16 / 13,56 \times 10^6) \times 1 \approx 302$ µs

FWT = 4: $(256 \times 16 / 13,56 \times 10^6) \times 2^4 \approx 4833$ µs

FWT = 9: $(256 \times 16 / 13,56 \times 10^6) \times 2^9 \approx 154$ ms

FWT$_{\text{MAX}}$ = 14: $(256 \times 16 / 13,56 \times 10^6) \times 2^{14} \approx 4949$ ms

FWI … Frame Waiting Time Integer

FWT … Frame Waiting Time
ATS 5: Interface Byte TA(1)

Start-up Frame Guard Time:

\[ SFG = \left( \frac{256 \times 16}{fc} \right) \times 2^{SFGI} \]

ATS sent by PICC

Frame sent by PCD

\[ t > SFG \]

SFGI …Start-up Frame Guard Time Integer
SFG …Start-up Frame Guard Time
ATS 6: Interface Byte TC(1)

CID … Card Identifier
NAD … Node Address

Bit 0  NAD supported, if bit is set to 1
Bit 1  CID supported, if bit is set to 1
Answer To Select (ATS)

<table>
<thead>
<tr>
<th>TL</th>
<th>T0</th>
<th>TA(1)</th>
<th>TB(1)</th>
<th>TC(1)</th>
<th>T1</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>'06'</td>
<td>'75'</td>
<td>'33'</td>
<td>'62'</td>
<td>'02'</td>
<td>'XX'</td>
<td>C0</td>
</tr>
</tbody>
</table>

**T1: ‘Historical character’**: shall be *ignored* by the application software.

**‘Interface byte TC(1)’**: CID supported, NAD not supported

**‘Interface byte TB(1)’**:  
High Nibble: Frame Waiting Time (FWT) (77.33 ms)  
Low Nibble: Start-up frame guard time (SFGT) (604 μs)

**‘Interface byte TA(1)’**: possible data rates supported by the PICC.  
(The DESFire supports up to 424 kbaud in both directions.)

**T0: ‘Format Byte’**  
High Nibble: presence of TA(1), TB(1) and TC(1)  
Low Nibble: ‘FSCI’ (maximum accepted size of a frame)

**TL: ‘Length Byte’** of the transmitted ATS  
(including itself, but excluding the two CRC bytes)
**Protocol Parameter Selection Request**

### Command Table

<table>
<thead>
<tr>
<th>RFU</th>
<th>CID</th>
</tr>
</thead>
<tbody>
<tr>
<td>b8</td>
<td>b7</td>
</tr>
<tr>
<td>b6</td>
<td>b5</td>
</tr>
<tr>
<td>b4</td>
<td>b3</td>
</tr>
<tr>
<td>b2</td>
<td>b1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

**Notes:**
- CMD (PPS): Command
- RFU (Request Field Use)
- CID (Command Identification)
- PPS0: PPS1 follows

---

**Table: Divisor and Baudrate**

<table>
<thead>
<tr>
<th>Divisor</th>
<th>DSI</th>
<th>DRI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00*</td>
<td>01</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>10</td>
</tr>
</tbody>
</table>

**Divisor:**
- 1: 106kBd
- 2: 212kBd
- 4: 424kBd

---

* '00' (106 kbaud in both directions) is the default if no PPS command is sent.
### Block Structure of T=CL

#### Application Protocol Data Unit (APDU)

<table>
<thead>
<tr>
<th>Prologue field</th>
<th>Information field</th>
<th>Epilogue field</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCB</td>
<td>[CID]</td>
<td>EDC</td>
</tr>
<tr>
<td>1 byte</td>
<td>[NAD]</td>
<td>2 bytes</td>
</tr>
<tr>
<td>1 byte</td>
<td>[INF]</td>
<td>up to 253 bytes</td>
</tr>
<tr>
<td>1 byte</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **FSD** ... Frame Size for PCD
- **FSC** ... Frame Size for PICC
• Information Block (I-Block)
  – Exchange of Application Data Units (APDUs)

• Receive Ready Block (R-Block)
  – ACK or NACK (containing no INF Field)

• Supervisor Block (S-Block)
  – Waiting Time Extension (contains 1 INF Field)
  – Deselect (containing no INF Field)
I-Block \((0)_{X}\) ... I-Block with chaining bit not set and block number \(X\)

I-Block \((1)_{X}\) ... I-Block with chaining bit set and block number \(X\)
Example of Block Exchange

<table>
<thead>
<tr>
<th>Prologue Field</th>
<th>Information Field</th>
<th>Epilogue Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCB [CID] [NAD] [INF]</td>
<td>[INF]</td>
<td>EDC</td>
</tr>
<tr>
<td>no of bytes:</td>
<td>1 1 0</td>
<td>max. 60</td>
</tr>
<tr>
<td>no of bytes:</td>
<td>1 0</td>
<td>max. 61</td>
</tr>
</tbody>
</table>

1 If CID = 0, no CID byte is sent

“0a 02 6a xx xx”

PCB
CID
CMD: GetApplicationIDs()

EDC: CRC according to ISO14443A
Example: - Write 2 Bytes of „0x ff ff“ into a
- DES encrypted DataFile with
- File number 1
- CID 4

Assumption:
The DESFire PICC is selected, RATS is performed with CID = 4. The according application
(whatever number) is selected, and the authentication with the according key is performed.

Example:
- Write 2 Bytes of „0x ff ff“ into a
- DES encrypted DataFile with
- File number 1
- CID 4

Assumption:
The DESFire PICC is selected, RATS is performed with CID = 4. The according application
(whatever number) is selected, and the authentication with the according key is performed.

CMD: WriteData(FileNo, Offset, Length)

EDC (CRC)

(3)DES
deciphered data

Offset Length