NFC Forum Type 4A & 4B Tag Platform Operations with the TRF7970A

NFC/RFID Training Module (2014)

S2 MCU NFC/RFID Applications Team

Overview of NFC Forum Type 4 Tag Platform Operations

- TRF7970A being used with NFC Forum Type 4A & 4B Tag Platforms operation is possible using Direct Mode 2 (default mode of the TRF7970A)
- TRF7970A will be configured for ISO14443 operations by MCU
- TRF7970A (+ MCU) will activate and select the Type 4 tag platforms using ISO14443 standard command flow
- After activation and selection, the NDEF message will be selected.
  - If tag is not previously NDEF Formatted, then obviously this would be the first step after activating and selecting it.
- Then the reading or writing of the NDEF Message is possible using the Read_Binary and Update_Binary commands.

ISO14443B

ISO14443-2 , -3 for Type B

- **ISO14443-3 Type B Command Set**:
  - More efficient than ISO14443A, only four primitive commands are needed to manage the multi-node communication channels in this sub-protocol of ISO14443:
  - **REQB** & **WUPB**
    - The REQB and WUPB Commands sent by the PCD are used to probe the field for PICCs of Type B. In addition, WUPB is particularly used to also wake up PICCs which are in HALT state.

1st byte	2nd byte	3rd byte	4th, 5th bytes
APf (1 byte)	**AFI** (1 byte)	**PARAM** (1 byte).	**CRC_B** (2 bytes)
MSB LSB	MSB LSB	MSB LSB	MSB LSB

    - Response is called: Answer to Request B (ATQB)
    - Inside the ATQB response is the PUPI, Application and Protocol Data Bytes

1st byte	2nd, 3rd, 4th, 5th bytes	6th, 7th, 8th, 9th, bytes	10th, 11th, 12th, bytes	13th, 14th bytes
'50' (1 byte)	**PUPI** (4 bytes)	**Application Data** (4 bytes)	**Protocol Info** (3 bytes)	**CRC_B** (2 bytes)
MSB LSB	MSB LSB	MSB LSB	MSB LSB	MSB LSB

ISO14443-2 , -3 for Type B

- **ISO14443-3 Type B Command Set (cont.)**:
  - **ATTRIB**
    - The ATTRIB Command sent by the PCD includes information required to select a single PICC.
    - A PICC receiving an ATTRIB Command with its identifier becomes selected and assigned to a dedicated channel. After being selected, this PICC only responds to commands defined in ISO/IEC 14443-4 which include its unique CID.
    - This command is also used to change data rate of the PCD ←→ PICC communications.

1st byte	2nd, 3rd, 4th, 5th bytes	6th byte	7th byte	8th byte	9th byte	10th,…….bytes	
'1D' (1 byte)	**Identifier** (4 bytes)	**Param 1** (1 byte)	**Param 2** (1 byte)	**Param 3** (1 byte)	**Param 4** (1 byte)	**Higher layer - INF** (optional – 0 or more bytes)	**CRC_B** (2 bytes)

MSB LSB MSB LSB MSB LSB MSB LSB MSB LSB MSB LSB MSB LSB MSB LSB LSB MSB LSB

    - If the higher layer INF field in the command request is empty (normal), then the Answer to ATTRIB response will be:

1st byte		2nd, 3rd bytes
MBLI	**CID**	**CRC_B**
(1 byte)		(2 bytes)

MSB LSB MSB LSB

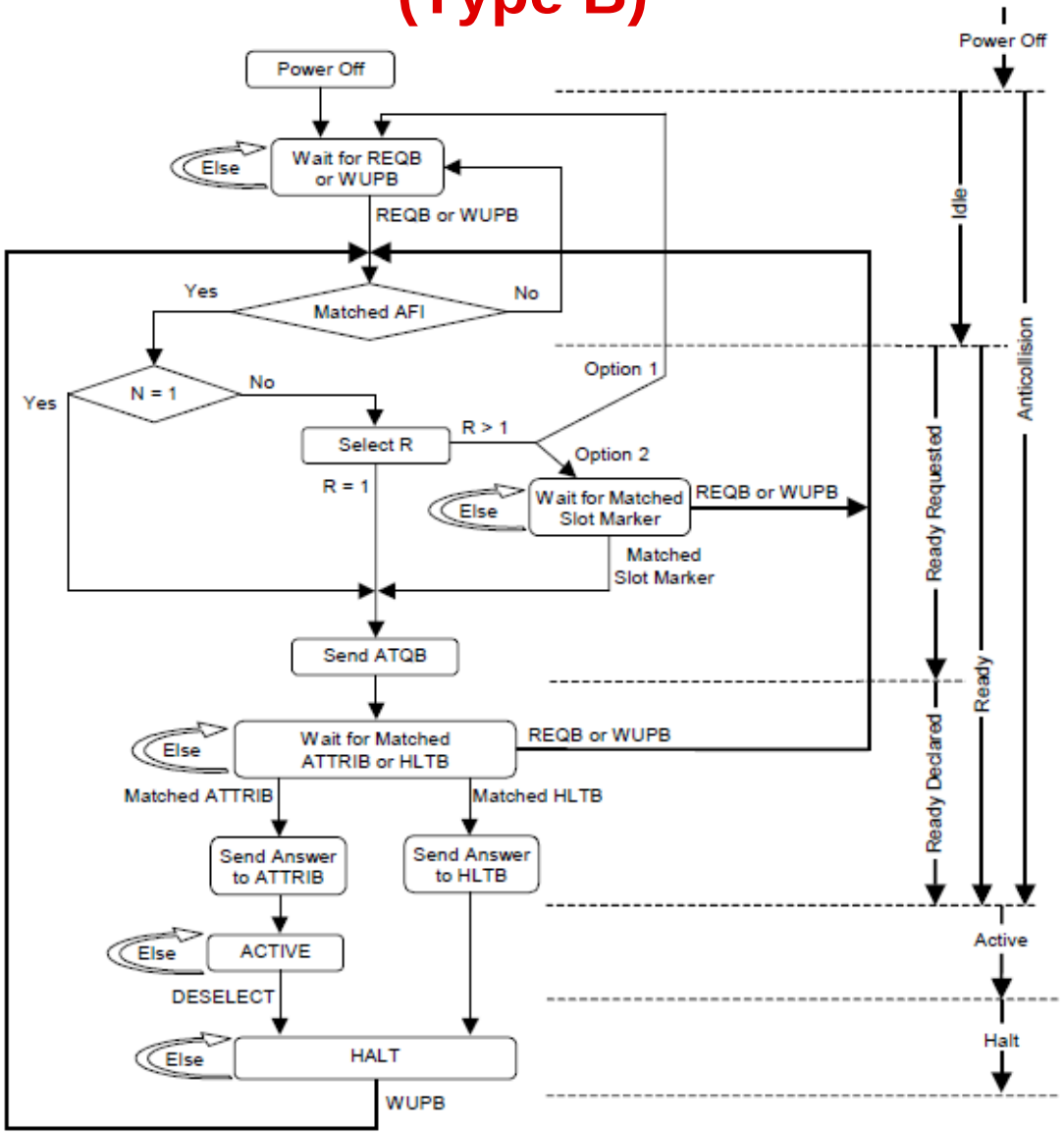
    - When this response is received, the card will be in Layer 4 and ready for transparent data exchange.

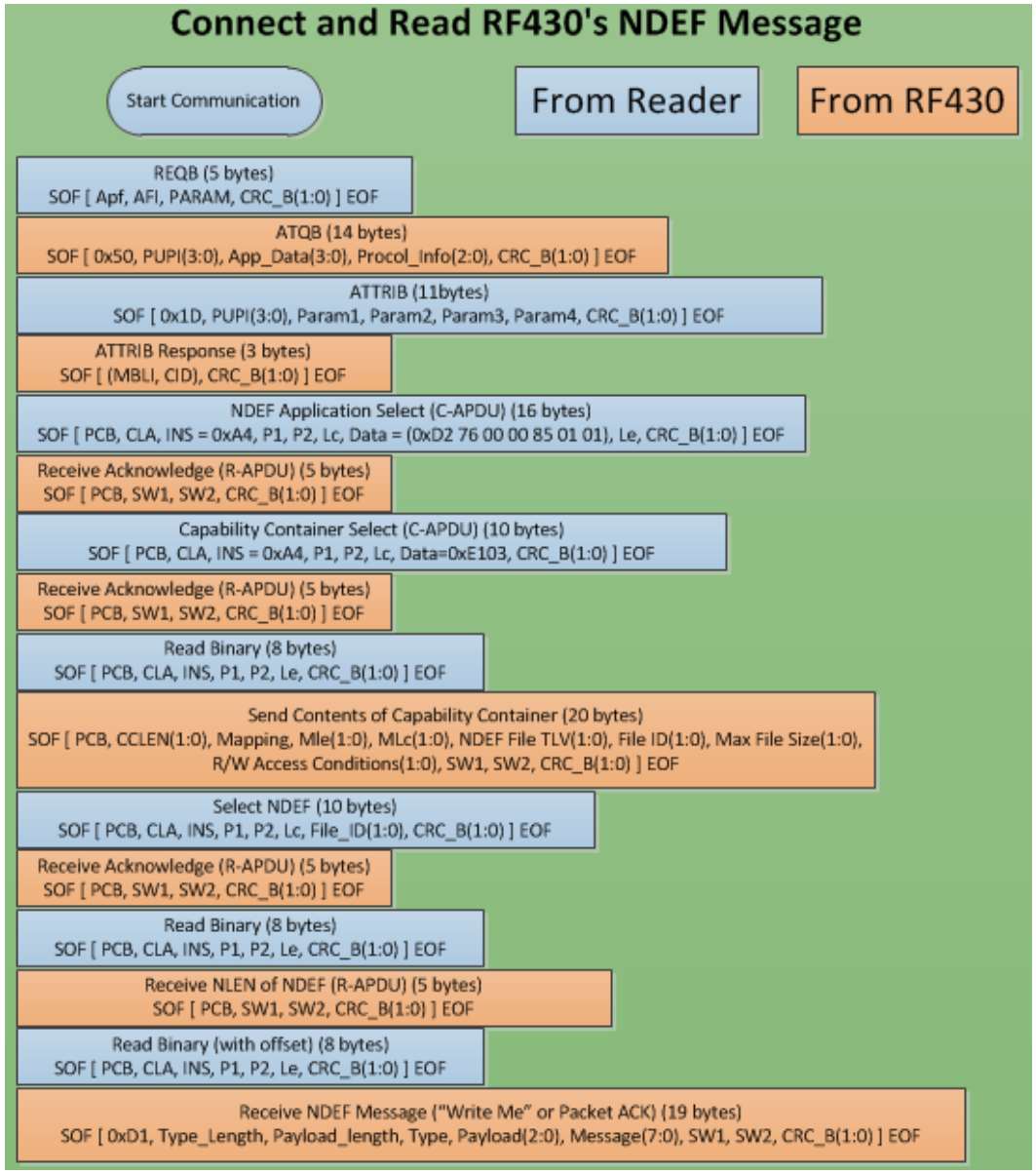
ISO14443-2 , -3 for Type B

- **ISO14443-3 Type B Command Set (cont.)**:
  - **Slot-MARKER**
    - After a REQB/WUPB Command, the PCD **may** send up to (N-1) Slot-MARKER Commands to define the start of each timeslot. (**it's not mandatory, like Type A**)
      - Slot-MARKER Commands **can** be sent :
        - » after the end of an ATQB message received by the PCD to mark the start of the next slot or earlier if no ATQB is received (no need to wait until the end of a slot, if this slot is known to be empty).
        - » It is not mandatory for a PICC to support this command. In this case, the PICC shall ignore any Slot-MARKER Command. The PICC may only send its ATQB after REQB (in the first slot) in a probabilistic approach.
  - **HLTB**
    - The HLTB Command is used to set a PICC in HALT state and stop responding to a REQB. After answering to this command the PICC shall ignore any commands except the WUPB Command.
    - The four byte Identifier is the PUPI, retrieved from the REQB command.

1st byte	2nd, 3rd, 4th, 5th bytes	6th, 7th bytes
'50' (1 byte)	**Identifier** (4 bytes)	**CRC_B** (2 bytes)
MSB LSB	MSB LSB	MSB LSB

ISO14443-3 Activation and Selection Logic Loop (Type B)

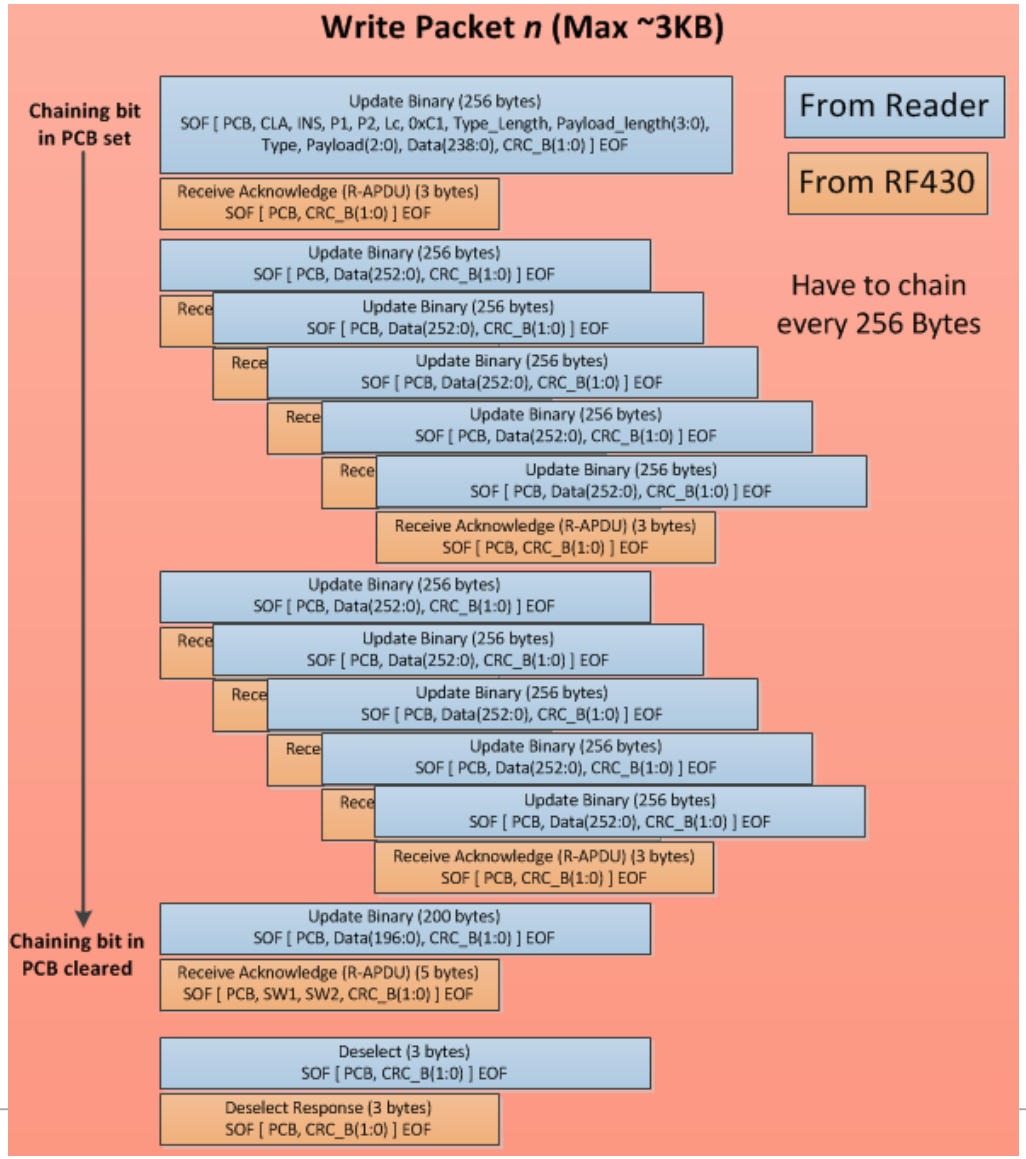




ISO14443B Selection Process

- Once we get to NDEF Application Select, the commands are the exact same for both ISO14443A & B.
- Let's follow this in code & on the LSA.

Writing Packet with Chaining



- Notice there is some overhead in every packet.
- There is much less over head in chained packets.

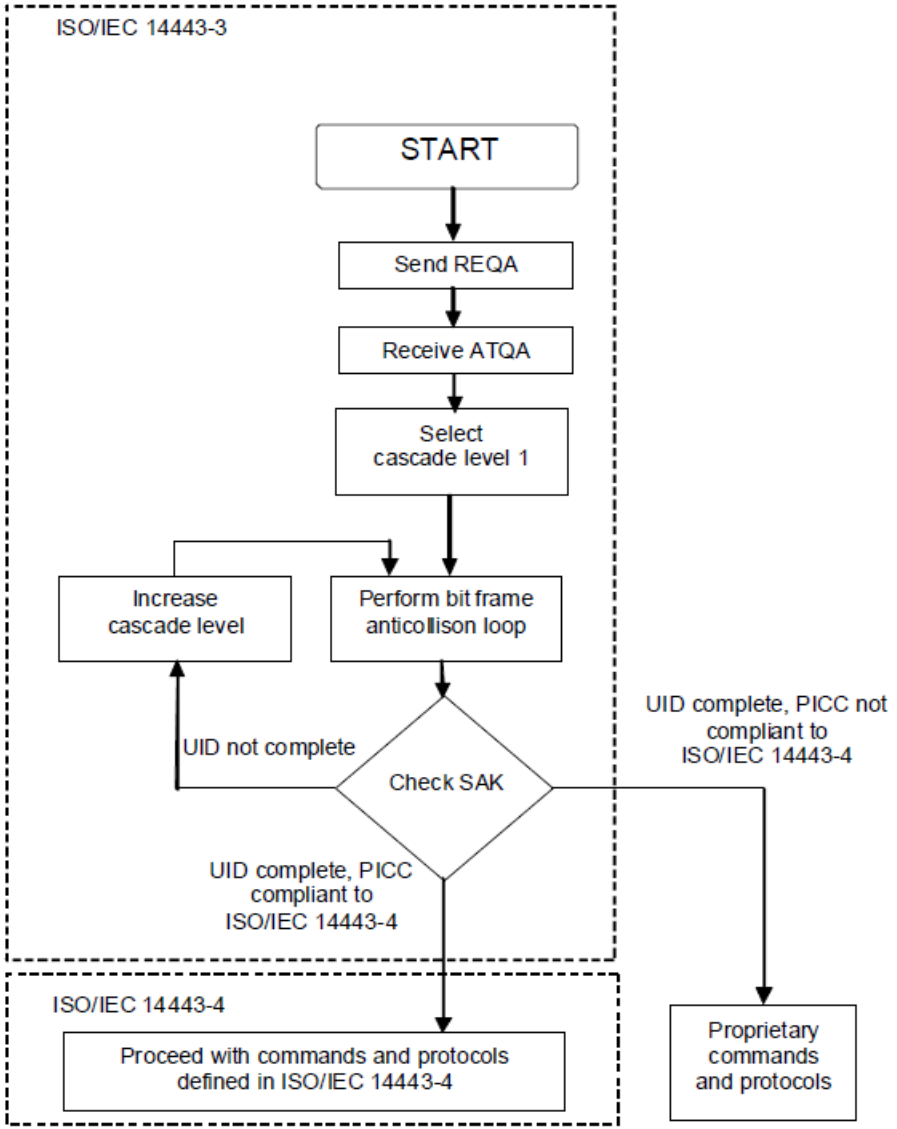
ISO14443A

ISO14443-2 , -3 for Type A

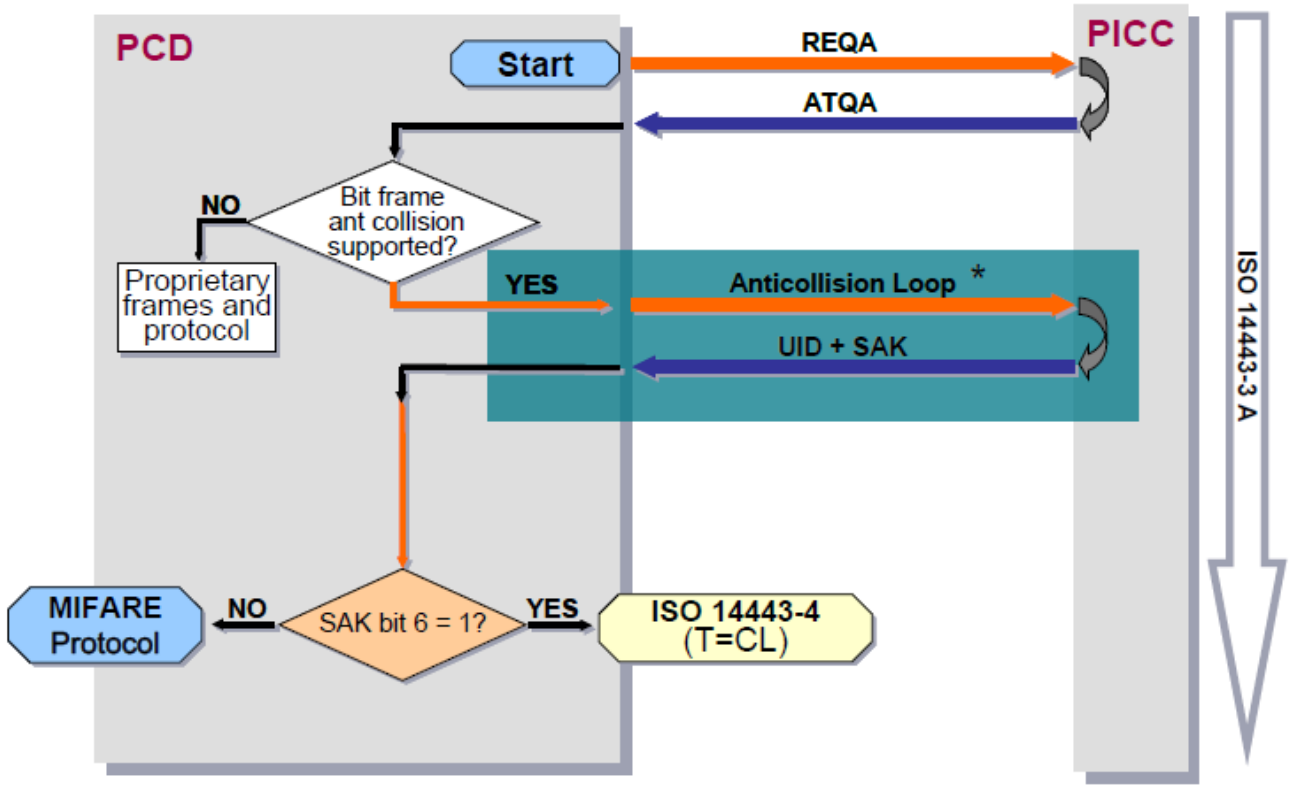
- **ISO14443-3 Type A Command Set**:
  - **REQA** (0x26) & **WUPA** (0x52)
    - These two commands are issued as broken byte (7 bits) command with no CRC
      - Used for Activation of the card
        - » REQA is activation command, WUPA is used after a HALTA.
    - PICC response is called ATQA (go to ISO14443-3, section 6.5.2 for details)
  - **ANTICOLLISION** & **SELECT**
    - The anti-collision and selection for Type A is done inside a cascaded loop. (go to ISO14443-3, section 6.5.1 for details.)
    - The main output of this loop is the complete UID of the card, which can be 4, 7 or 10 bytes long. (called single, double or triple size UIDs)
  - Cards which are not Layer 4 compliant are identified at end of this loop by their response.
    - B6 in **SAK** (go to Table 9 in ISO14443-3)
    - If card **is** compliant, proceed to -4 commands
      - Popular examples are: NFC Type 4A (MIFARE™ DESFire EV1) cards.
    - If card **is not** compliant, proceed to using that cards' specific document(s)
      - Popular examples are: NFC Type 2 (MFUL/MFULC) and MIFARE™ Classic cards.
        - » These card types are specifically covered in other training modules
  - **HLTA** (0x50, 0x00, CRC_A)
    - Used to stop communication with the card while still in the PCD field (i.e. put it to sleep)

ISO14443-3 Activation and Selection Logic Loop (Type A)

Step 1	The PCD shall assign SEL with the code for the selected anticollision cascade level.
Step 2	The PCD shall assign NVB with the value of '20'. NOTE This value defines that the PCD will transmit no part of UID CL*n*. Consequently this command forces all PICCs in the field to respond with their complete UID CL*n*.
Step 3	The PCD shall transmit SEL and NVB.
Step 4	All PICCs in the field shall respond with their complete UID CL*n*.
Step 5	If more than one PICC responds, a collision may occur. If no collision occurs, steps 6 to 10 shall be skipped.
Step 6	The PCD shall recognize the position of the first collision.
Step 7	The PCD shall assign NVB with a value that specifies the number of valid bits of UID CL*n*. The valid bits shall be part of the UID CL*n* that was received before a collision occurred followed by a (0)b or (1)b, decided by the PCD. A typical implementation adds a (1)b.
Step 8	The PCD shall transmit SEL and NVB, followed by the valid bits.
Step 9	Only PICCs of which the part of UID CL*n* is equal to the valid bits transmitted by the PCD shall transmit their remaining bits of the UID CL*n*.
Step 10	If further collisions occur, steps 6 to 9 shall be repeated. The maximum number of loops is 32.
Step 11	If no further collision occurs, the PCD shall assign NVB with the value of '70'. NOTE This value defines that the PCD will transmit the complete UID CL*n*.
Step 12	The PCD shall transmit SEL and NVB, followed by all 40 bits of UID CL*n*, followed by CRC_A.
Step 13	The PICCs which UID CL*n* matches the 40 bits shall respond with their SAK.
Step 14	If the UID is complete, the PICC shall transmit SAK with cleared cascade bit and shall transit from READY state to ACTIVE state or from READY* state to ACTIVE* state.
Step 15	The PCD shall check if the cascade bit of SAK is set to decide whether further anticollision loops with increased cascade level shall follow.



ISO14443A Activation Sequence

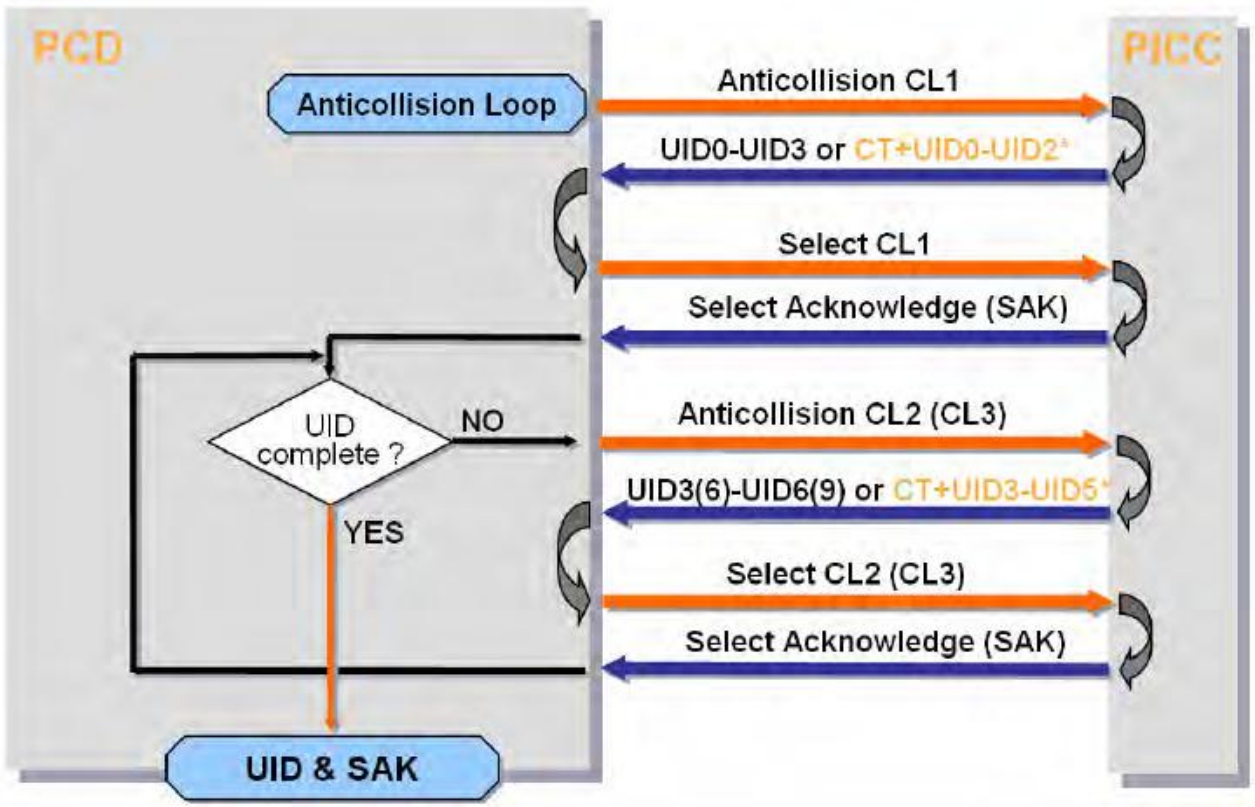


(1) Details of the Anticollision Loop see Fig 2.

Fig 1. Principle of the Card Activation Sequence

- The bit 6 in the SAK indicates, whether the PICC is compliant to the ISO/IEC14443-4 or not. However, it does not necessarily indicate, whether the PICC supports the MIFARE Protocol or not.

ISO14443A Anti-collision Loop



(3) CT = Cascade Tag

(4) CL = Cascade Level

Fig 2. Anticollision sequence

- Mifare tags recently started being released with double sized (7 byte) UID's. Mifare 4 byte UID's are now labeled "non-unique". Currently there are no triple sized UID Mifare tags.

ISO14443A Selection Process

ISO14443A Anti-Collision Double Sized UID and SAK retrieval example (no collisions)

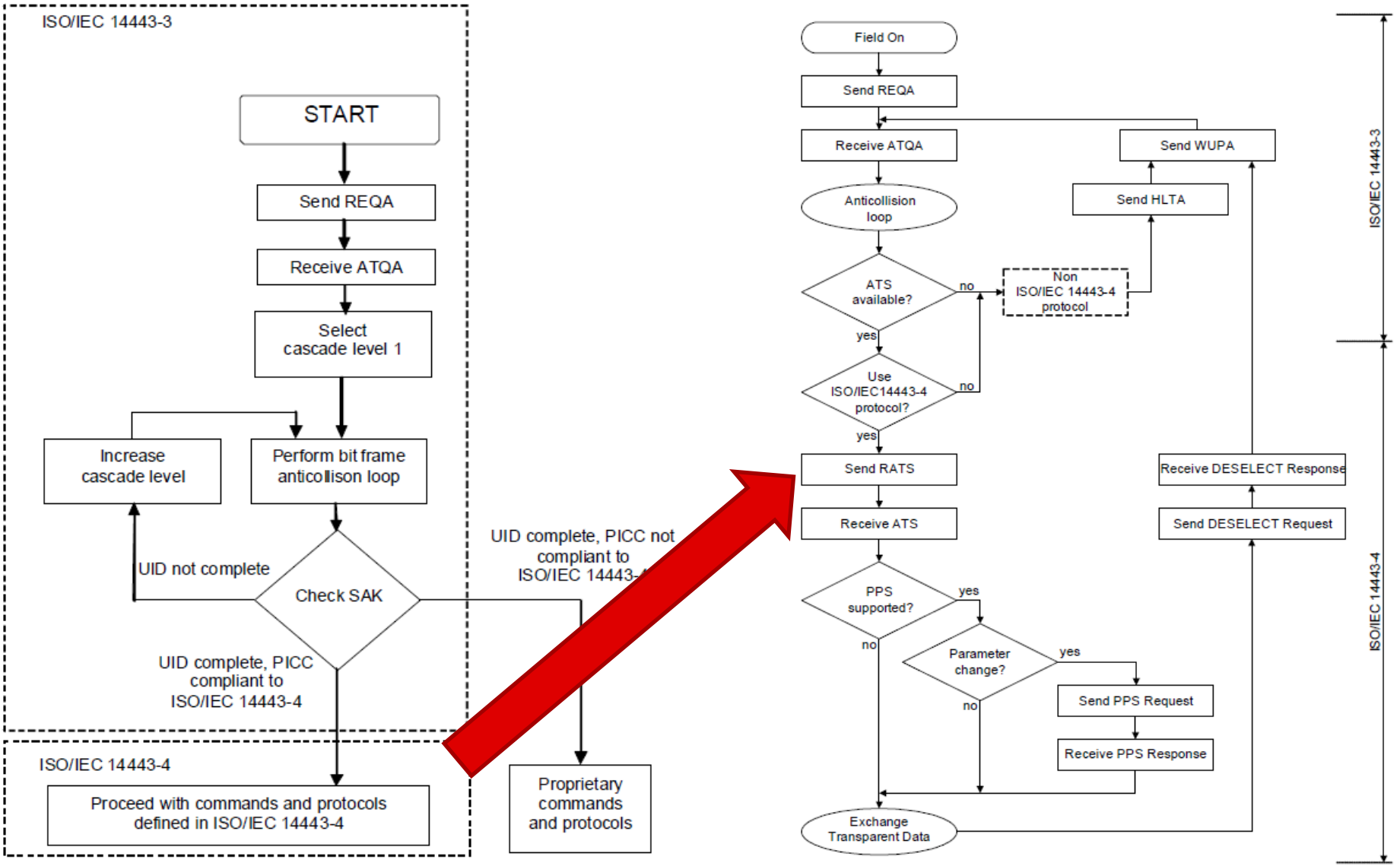
Reader		Tag	Notes
1 93 20 2	3	LSByte of UID	SEL = 93, NVB = 20
	4	88 04 DA E9 BF	88 = Double Size (or greater) UID; 04, DA, E9 are first three bytes of UID; BF = BCC of the string.
1 11 93 70 88 04 DA E9 BF	12		SEL = 93, NVB = 70
	13	04 B3	Cascade Bit set in SAK response (B3) = UID not Complete
1 95 20 2	3	MSByte of UID	SEL = 95, NVB = 20 (Increase Cascade Level)
	4	CA B5 28 80 D7	CA B5 28 80 = last four bytes of UID, D7 = BCC of the string
1 11 95 70 CA B5 28 80 D7	12		SEL = 95, NVB = 70
	13	00	UID Complete, Transponder not Compliant to ISO14443-4
			(this is a Mifare Classic with Double Sized UID)

Complete UID for this 7 byte (double size) tag is:
04 DA E9 CA B5 28 80

These UID Bytes coming in need to be stored in a buffer and then concatenated for further use.

For triple size UID, these steps would be taken, but the first byte would again be 0x88 and the SAK response would be 04. The cascade level would be incremented to 0x97 to get last four bytes of the 10 byte (or triple size) UID transponder.

Going from ISO14443-3 into ISO14443-4A Logic Loop



ISO14443-4 for Type A

- **Advanced Commands (used for -4, aka “Layer 4” compliant cards)**
  - **RATS** (used to select a -4 compliant card)
    - Response is Answer to Select (**ATS**)
  - **PPS** (optional command used to change data rate, issued after **RATS/ATS** command/response)
- After Layer 4 is entered, commands and protocols are used to exchange data transparently.
  - This is the Data Link (MAC + LLC) & Application layers shown previously as represented in the OSI model concept.
  - ISO14443-4 provides a “framework structure” and scenario handling rules for these layers, ISO17816-4 provides Commands and Error Codes
  - Together, ISO14443-4 + ISO7816-4 make no distinction between Type A or Type B, data is sent or received according to the same protocol rules for both cards types in this layer.
  - Details on Type 4A and Type 4B data/error handling will be covered in detail inside another training module of this series.