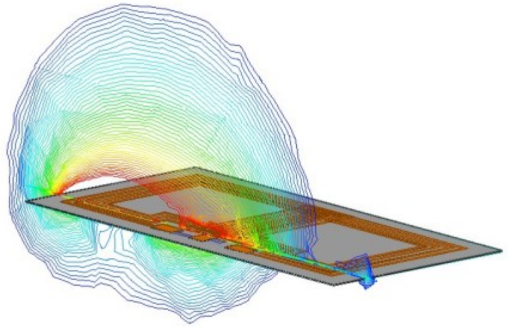
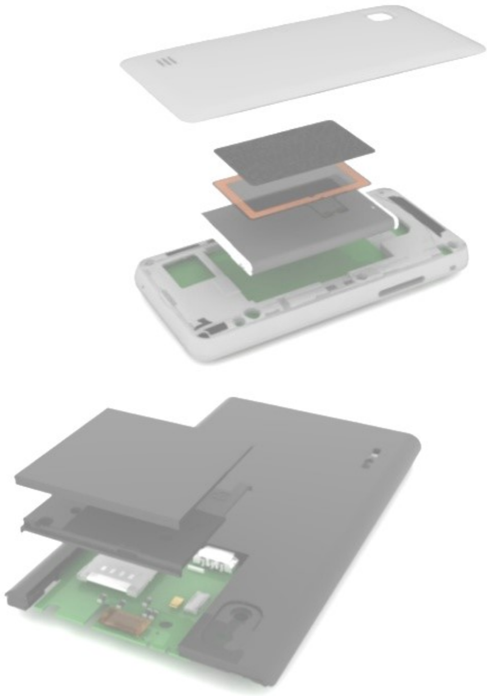


04 HF Protocols

4^{th} unit in course 451.417, RFID Systems, TU Graz

Dipl.-Ing. Dr. Michael Gebhart, MSc

RFID Systems, Graz University of Technology
SS 2023, March 06^{st}

rfid-systems.at
Advancing Technology

Content

- Proximity (ISO/IEC14443)
  - Data interface Type A
    - Communication Reader ➔ Transponder
    - Communication Transponder ➔ Reader
- FeliCa
- Vicinity (ISO/IEC15693)
- NFC

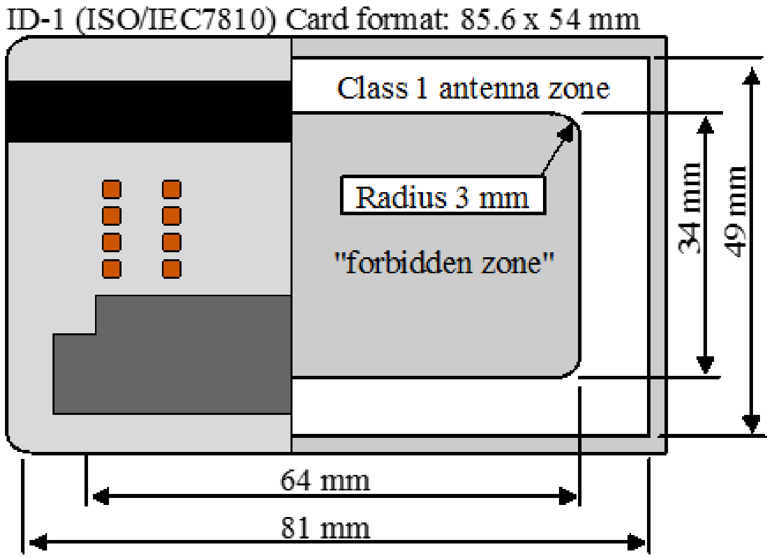
Proximity (ISO/IEC14443)

13,56 MHz person-related Standard (secure applications)

The world of Smartcards

- **ISO/IEC14443**.........The **Contactless Proximity Air Interface** for **person-related applications** was standardized at the end of the 1990ies.
- Applications in **Government** (e-Passports, driver license, health card...), **Payment** (Contactless Credit Cards), **Public Transport** (Ticketing), **Secure Access Control**, etc. are successfully deployed.
- The **battery-less**, field-proven secure chip technology did migrate into objects e.g. watches, rings, SD-Cards, USB-Sticks, which require small antennas. This requires **more accurate characterization and production tolerance consideration**.

- **Related ISO/IEC Standards**
  - 7810...........Card geometry (e.g. ID-1 format) and physical properties
  - 7811-3/-3...Embossing (letters raised in relief)
  - 7811...........magnetic stripe cards
  - 7812...........optical character recognition cards
  - 7813...........bank cards
  - 7816...........contact cards with ICs
  - 10373.........test methods



Card geometry specifications.

ISO/IEC14443 (Proximity) (formerly Philips, Motorola, Infineon,...)

– **Carrier frequency:**	13,56 MHz (+/- 7 kHz)	
– ***H*-field strength:**	1,5 – 7,5 A/m(rms)	
– **Distance:**	~ < 10 cm (depends on reader / transponder, not specified)	
– **Data transmission:**	Data frames (start-bit and stop-bit)	
– **Protocol principle:**	Reader Talks First	
– **Anti-collision:**	Mandatory implemented. UID and Binary Search Tree.	
● **Comm. Interface:**	Typ A (Licence Philips)	Typ B (License Novatron et al.)
Data link Reader ➔ Transponder (Reader supports both Interfaces)		
– **Modulation**	ASK, 100 % (106), < 60 % high bit rates	ASK, 10 % (8 - 14 %)
– **Channel coding**	Modified Miller	NRZ
– **Data rate**	~ 106 kbit/s (fc/128), 212, 424, 848 kbit/s	
Data link Transponder ➔ Reader (Reader supports both Interfaces)		
– **Subcarrier**	847,5 kHz (fc/16)	847,5 kHz
– **Modulation**	Load modulation (external AM/PM)	
– **Channel coding**	Manchester (106), BPSK (212-848)	NRZ-L (106), BPSK (212-848)
– **Data rate**	~ 106 kbit/s, 212, 424, 848 kbit/s	

The Proximity Card Standard (14443)

Definitions in the **Proximity-Base Standard** (ISO/IEC)

14443-4 — Protocol 2 (state diagrams, error correction)

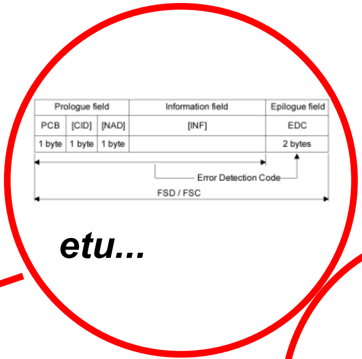
14443-3 — Protocol 1 (data frame, initialization and anticollision)

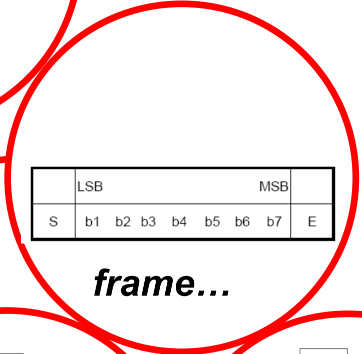
14443-2 — Air Interface (power and signal transmission, modulation)

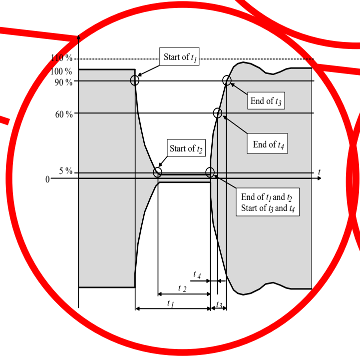
14443-1 — Physical Layer (Card geometry, limits)

10373-6 — Measurement set-up and test methods for Proximity-Cards

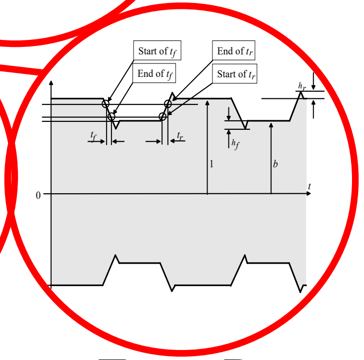
Measurement of properties in Test Standard / Lab Standard (ISO/IEC)



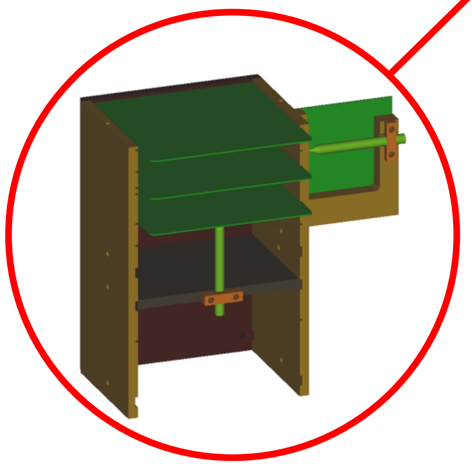


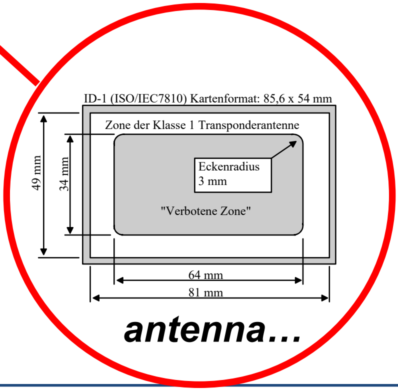


Type A



Type B





Proximity Data Interface Type A

Communication link Reader → Transponder

Short frame command set

- Data transmission in the Type A Interface is bit oriented.
- A specific Short Frame is used for a few reader commands, e.g. for fast anti-collision handling.
  - Commands consist of 2 hexadecimal digits (value 1…F), means 8 binary digits.
  - The most significant binary digit is not transmitted, so 2^7 = 128 different commands are possible.

Command	hexadecimal Code	binary Code
Request A (REQA)	26	0 0 1 0 0 1 1 0
Wake up A (WUPA)	52	0 1 0 1 0 0 1 0
Optional Time Slot Method	35	0 0 1 1 0 1 0 1
Propritary Commands	40 … 4F	0 1 0 0 x x x x
Proprietary Commands	70 ... 7F	0 1 1 1 1 x x x
Reserved for future use (RFU)	all other	

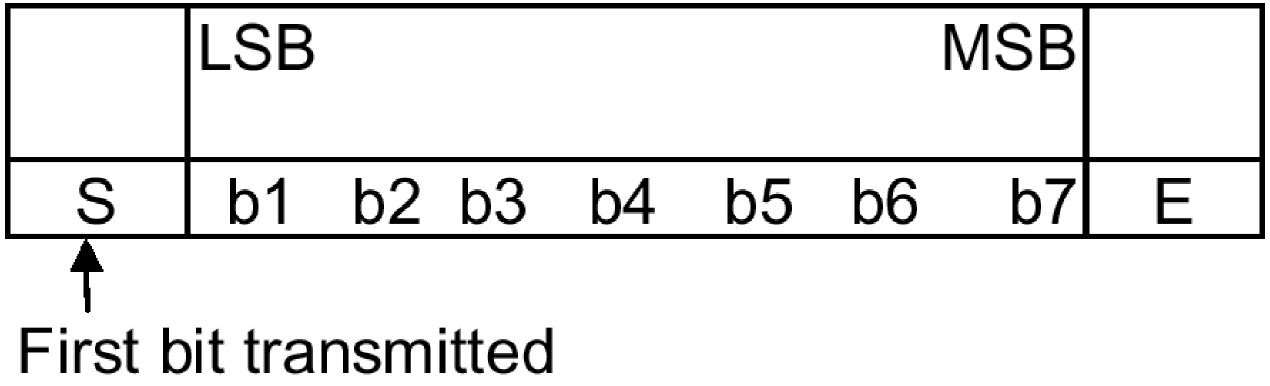
Least significant bit (LSB)

Most significant bit (MSB)

Reference: ISO/IEC 14443-3

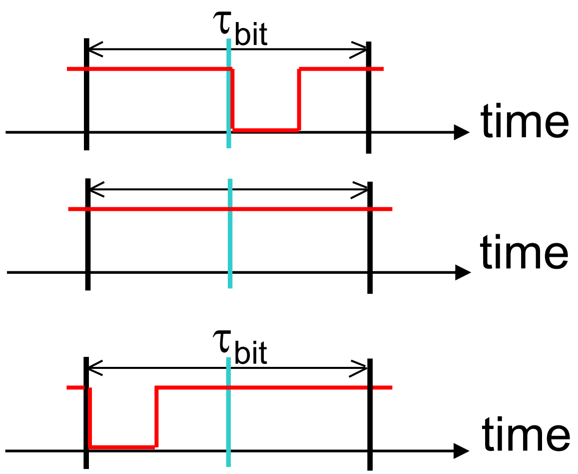
Short frame for first Reader Commands

- Commands are transmitted in frames, delimited by a start-bit and a stop-bit.
- The least significant bit is transmitted first, this means start-bit, then binary digit b1 = 2^0, b2 = 2^1,…, (b8 = 2^7 is not transmitted), then stop-bit.



Bit duration and channel encoding

- The base data rate (BDR) is given by the reader carrier frequency divided by factor 128, so this means 105,9375 kbit/s or ~ 106 kbit/s.
- So the bit duration or elementary time unit (etu) is 128 carrier periods.
- Modified Miller channel coding is used (energy efficient transmission). For binary logical data encoding the following 3 sequences are defined:
  - **Sequence X**: Modulation in second half-etu
  - **Sequence Y**: No modulation during one etu (bit duration)
  - **Sequence Z**: Modulation at the start of etu



Bit and channel coding

- The information content in bits is encoded to the sequences as follows:
  - **Start bit: Z**
  - **Logic 1: X**
  - **Logic 0: Y**, with the following exception:
    - If two or more 0´s follow consequently, sequence Z is used from the 2nd 0 onwards, and
    - If the first bit after the start bit is zero, sequence Z is used for this bit and all following zeros.
  - **Stop-bit:** Logic 0, followed by sequence Y
  - **No information:** At least two subsequent Y

Example for a Type A short-frame coding

- The defined **REQA** command is **26**$_{hex}$.

  E.g. conversion into decimal gives…

  $2 \times 16^1 + 6 \times 16^0 = 32 + 6 = 38_{dec}$.

  Conversion into **binary** gives…

38 : 2^7 = 0, remains 38 0

38 : 2^6 = 0, remains 38....................0

38 : 2^5 = 1 remains 6....................1

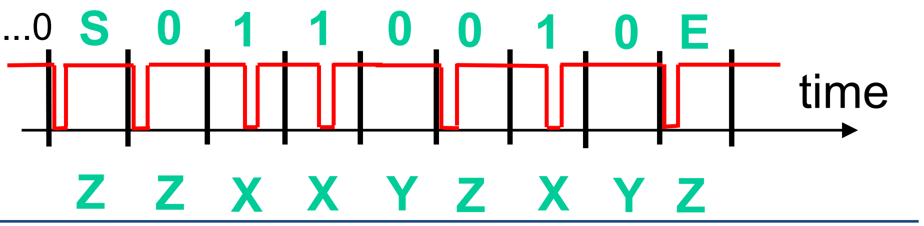
6 : 2^4 = 0 remains 6....................0

6 : 2^3 = 0 remains 6....................0

6 : 2^2 = 1 remains 2....................1

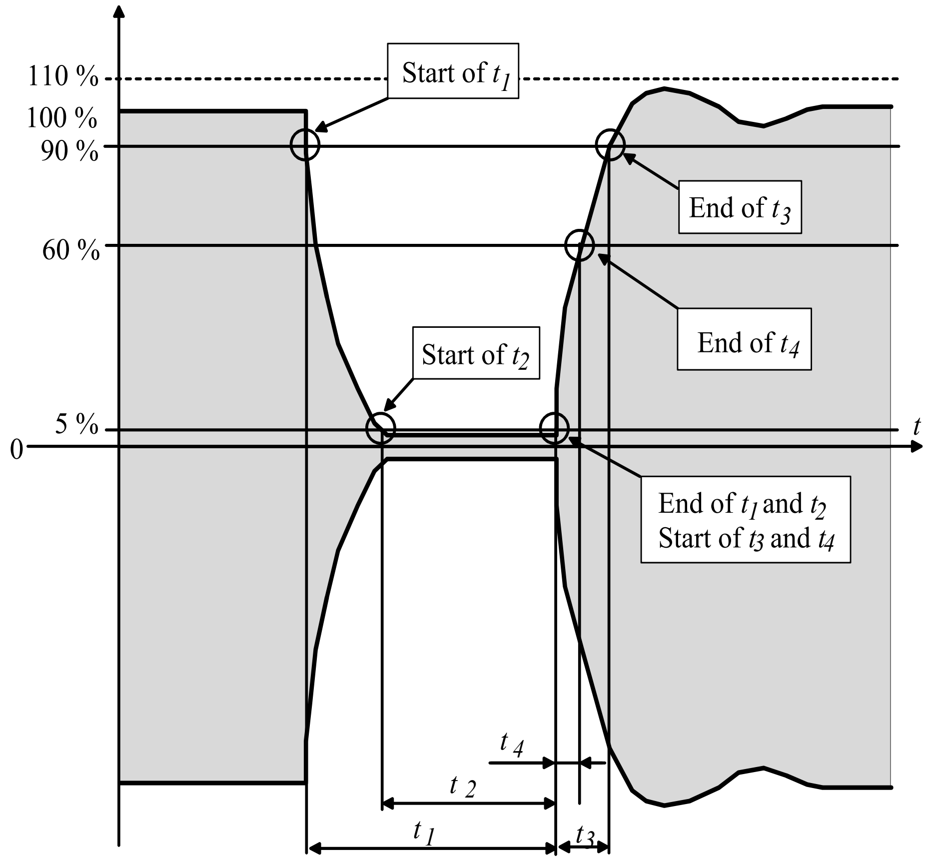
2 : 2^1 = 1 remains 0....................1

0 : 2^0 = 0 remains 0....................0



The result is 0 0 1 0 0 1 1 0

Modulation on *H*-field alternating with RF carrier



- Modulation is ASK 100 % index, nominally
- Properties are defined at the air interface (specified in time domain, residual carrier, overshoot).
- Parameters are specified in value ranges, individual for reader and transponder, to allow signal distortion by coupling of resonant antenna circuits.
- E.g. off-keying 2 – 3 µs duration, 10 % overshoot acceptable, ringing can be accepted to a certain amount.

- (Residual carrier, overshoots, ringing)
- Time parameters t_1, t_2, t_3, t_4

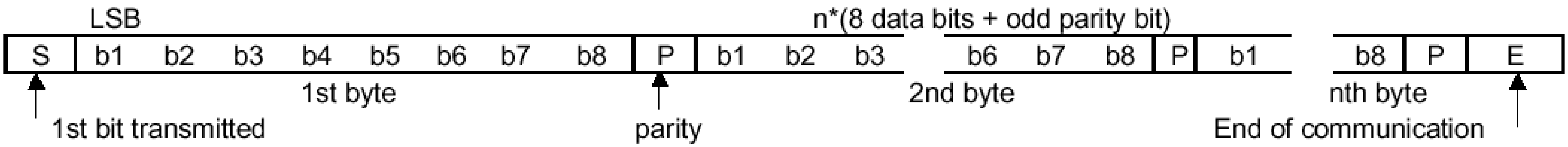
Reference: Specification in ISO/IEC14443-2, Measurement in ISO/IEC10373-6

Summary of properties

Principle	Reader talks first (~ master to slave)
Data rate	~ 106 kbit/s
Data format	Frame with start- and stop-bit, 7 data bits
Error correction	No, transparent
Bit order	Least significant bit is transmitted first
Channel coding	Modified Miller
Modulation	ASK with 100 % index (means off-keying of the carrier)

Standard frame

- Standard frames consist of several (n) bytes (8 bit) followed by a parity bit.
  - Odd parity (means that the parity is 1, if the sum of 9 bits is odd).
  - One byte means 8 binary digits, 256 bit information content.
- The frame is delimited by a start-bit and a stop-bit.
- Maximum length (was 256 bytes until 2012) is 4048 bytes.



Example for a Standard frame

- The Halt A (**HLTA**) command consists of two data bytes and a cyclic redundancy check (**CRC_A**).

First bit transmitted
↓

S	‘50’	‘00’	CRC_A	E

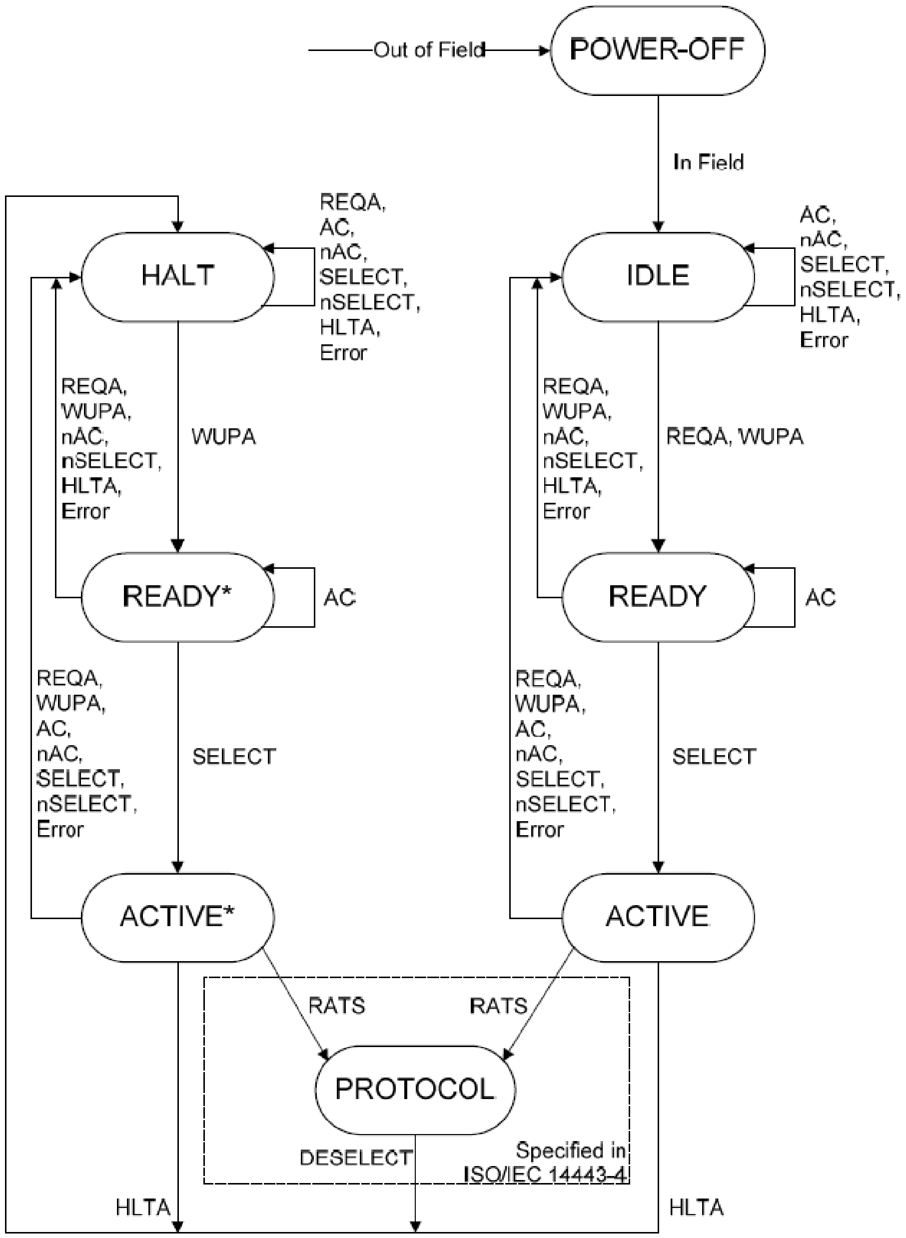
- The CRC_A is calculated over all data bits of the frame (n x 8 bit), except for start-bit, stop-bit, parity bits and the CRC16 content itself.
- Calculation is done over a cyclic shift register with XOR feedback and a start value “6363” (as specified in ISO/IEC13239).

First bit transmitted
↓

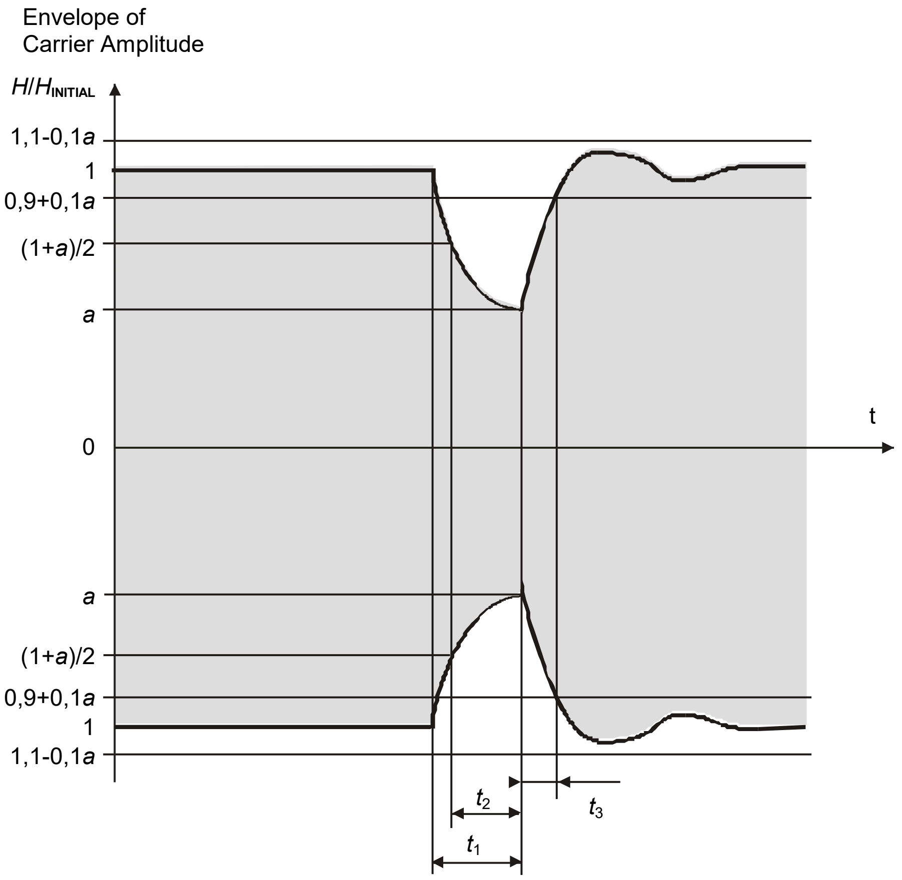
S	0000 0000	1	0000 0000	1	0000 0101	1	0111 1000	1	E
	‘00’	P	‘00’	P	‘A0’	P	‘1E’	P	

Some states and state transitions

- Reader commands can bring the transponder from one state to another.
- Some basic states:
  - Power off: The transponder is reset (no supply power)
  - Idle state: The transponder is power supplied via reader carrier, and ready to receive REQA or WUPA commands.
  - READY state: The transponder is awaiting anti-collision
  - Active: The transponder is in the operating system, awaiting application specific commands
  - HALT state: The transponder waits for the Wake-up A (WUPA) command. In case there are several transponders in the field, the reader can set all but one to HALT, and then communicate with one after the other.
  - Ready* and Active* are similar to READY and ACTIVE, but starting from HALT, not from IDLE.



Higher data rates



- As the duration of off-keying gets shorter than time constants of the resonant reader antennas, a different modulation parameter specification is required:
  - Residual carrier *a,* (and overshoots, ringing)
  - Time parameters t_5, t_6, t_7

Timing parameter	Bit rate					
	fc/64		*fc*/32		*fc*/16	
	Min	Max	Min	Max	Min	Max
t_1	15/*fc*	20/*fc*	8/*fc*	10/*fc*	4/*fc*	5/*fc*
t_2	8/*fc*	t_1	4/*fc*	t_1	2/*fc*	t_1
t_3	0	12/*fc*	0	10/*fc*	0	8/*fc*

Summary of properties

Principle	Reader talks first (~ master to slave)
Data rate	~ 106 kbit/s (BDR)
	212, 424, 848 kbit/s (optional HDR – reader can choose)
Data format	Frame with start- and stop-bit, up to 4 kbytes data
Error correction	Parity bit for each byte, optional CRC16
Bit order	Least significant bit is transmitted first
Byte order	Least significant byte is transmitted first
Channel coding	Modified Miller
Modulation	ASK (off-keying of the carrier)

Proximity Data Interface Type A

Communication link Transponder → Reader

Bit duration and channel encoding

- Base data rate is ~ 106 kbit/s, one etu (bit duration) is 128 carrier cycles
- Data is transmitted in frames of n bytes
- Channel encoding is Manchester coding for BDR. A sub-carrier frequency is gated with this signal.
- The sub-carrier frequency is the carrier divided by 16, so 847,5 kHz
- In BDR, one etu takes 8 sub-carrier periods, 8 x 16 = 128 carrier cycles

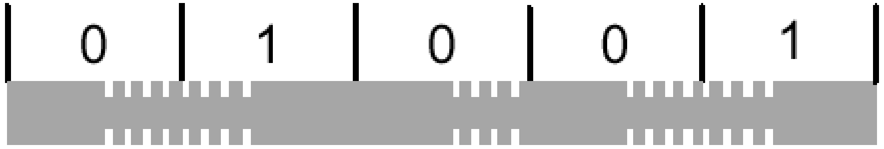
  - **Sequence D**: Modulation in first half-etu

  - **Sequence E**: Modulation in second half-etu

  - **Sequence F**: No modulation during one etu

Bit and channel coding

- In the transmitted frame logical information appears as Manchester encoded sub-carrier load modulation of the reader carrier.
- We differentiate the following conditions:
  - Start bit: Sequence **D**,
  - Logic 1: Sequence **D**,
  - Logic 0: Sequence **E**,
  - Stop bit: Sequence **F**,
  - No information: Sequence **F**



- The Standard frame is used. Each byte is followed by odd parity, data length can be 1 … 4096 bytes.

Reference: ISO/IEC14443-2 for modulation, ISO/IEC14443-3 for frame

Proximity Data Interface Type A

Communication flow – up to individual applications

Sequential communication

- **Reader talks first**
  - The communication flow is sequential (half-duplex), the reader sends a command and the transponder responds (master-slave).
- The reader defines the time reference of communication via carrier frequency.
- For some commands in BDR, the transponder replies in a bit-grid, defined by the reader command (response comes after Frame Delay Time, FDT). This is used for the anti-collision mechanism for Type A, BDR.
- For subsequent commands there is only a minimum FDT and a bit grid, the transponder response may start at a multiple of the time value.

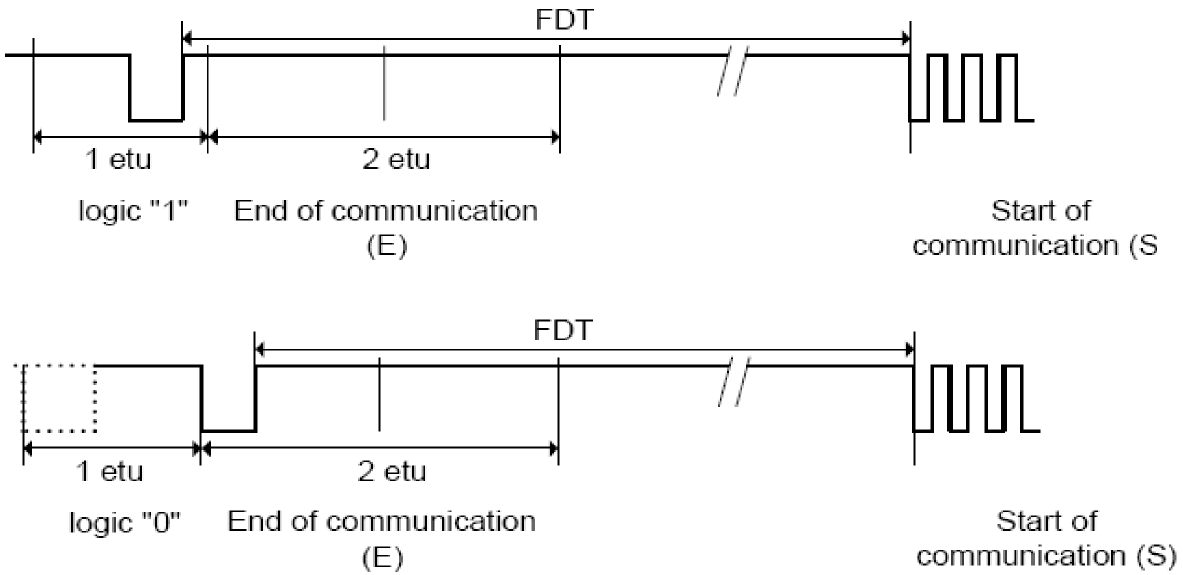
Command type	n (integer value)	FDT	
		last bit = (1)b	last bit = (0)b
REQA Command WUPA Command ANTICOLLISION Command SELECT Command	9	1236 / fc	1172 / fc
All other commands	≥ 9	(n * 128 + 84) / fc	(n * 128 + 20) / fc

Reference: ISO/IEC14443-3

Frame Delay Time Reader ➔ Transponder

- Time unit for the transponder response are carrier periods, $1/f_C$ ~ 73 ns.
- FDT is measured from the end of the last edge of the reader command to the start of the transponder back modulation.

  Due to channel coding, there are two duration options, depending on the information content:
- Last command-bit "**1**": FDT = $(n \times 128 + 84)/f_C$ (~ 91,15 µs for n = 9)
- Last command-bit "**0**": FDT = $(n \times 128 + 20)/f_C$ (~ 86,43 µs for n = 9)



Reference: ISO/IEC14443-3

Frame Delay Time Transponder ➔ Reader

- Also the reader may transmit the next command not earlier than after a minimum delay time after the transponder response.
- **FTD transponder ➔ reader** is measured from the last edge of back modulation to the first edge of the following reader command.
- The minimum FDT transponder ➔ reader is 1172 carrier periods (~ 86,43 µs).
- The reader may wait longer (no limit).

- E.g. two subsequent REQA commands must be separated by at least 7000 carrier periods ~ 0,5 ms (**Request guard time**)

Reference: ISO/IEC14443-3

Anti-collision mechanism (I)

- Before any application may start, it is mandatory to run an anti-collision sequence in base data rate.
- In case, more than one transponder compliant to the ISO/IEC14443 protocol is in the operating volume of a reader, at the beginning all are set to HALT, then one after the other is selected and an application / transaction is completed.

- Main commands are
  - REQA — Short frame (26h)
  - WUPA — Short frame (52h)
  - ANTICOLL — bit oriented anti-collision
  - SELECT — Standard frame (93h = Level 1, 95h = Level 2, 97h = Level 3)
  - HLTA — Standard frame (50 00h)

Reference: ISO/IEC14443-3

Anti-collision mechanism (II)

- The **Unique Identifier (UID)**, the serial number of a Type A transponder, may consist of 4, 7 or 10 bytes.

  According to this single, double or triple UID the anti-collision is done in up to 3 steps: **Cascade Level** 1, 2 and 3.

UID size	Number of UID bytes	Cascade levels
single	4	1
double	7	2
triple	10	3

- The transponder announces the size of its UID in Answer to Request (ATQA).

8	b7	Meaning
0	0	UID size: single
0	1	UID size: double
1	0	UID size: triple
1	1	RFU

Reference: ISO/IEC14443-3

Anti-collision mechanism (III)

- The UID may be ROM programmed, or random generated (e.g. Passport). The first byte announces the content of the following n x 3 bytes of the UID. For single UID, the first byte allows following options:

uid0	Description
'08'	uid1 to uid3 is a random number which is dynamically generated
'x0' - 'x7', 'x9' - 'xE'	Proprietary number
'18', '28', '38', '48', '58', '68', '78', '98', 'A8', 'B8', 'C8', 'D8', 'E8', 'F8'	RFU
'xF'	Fixed number, non-unique

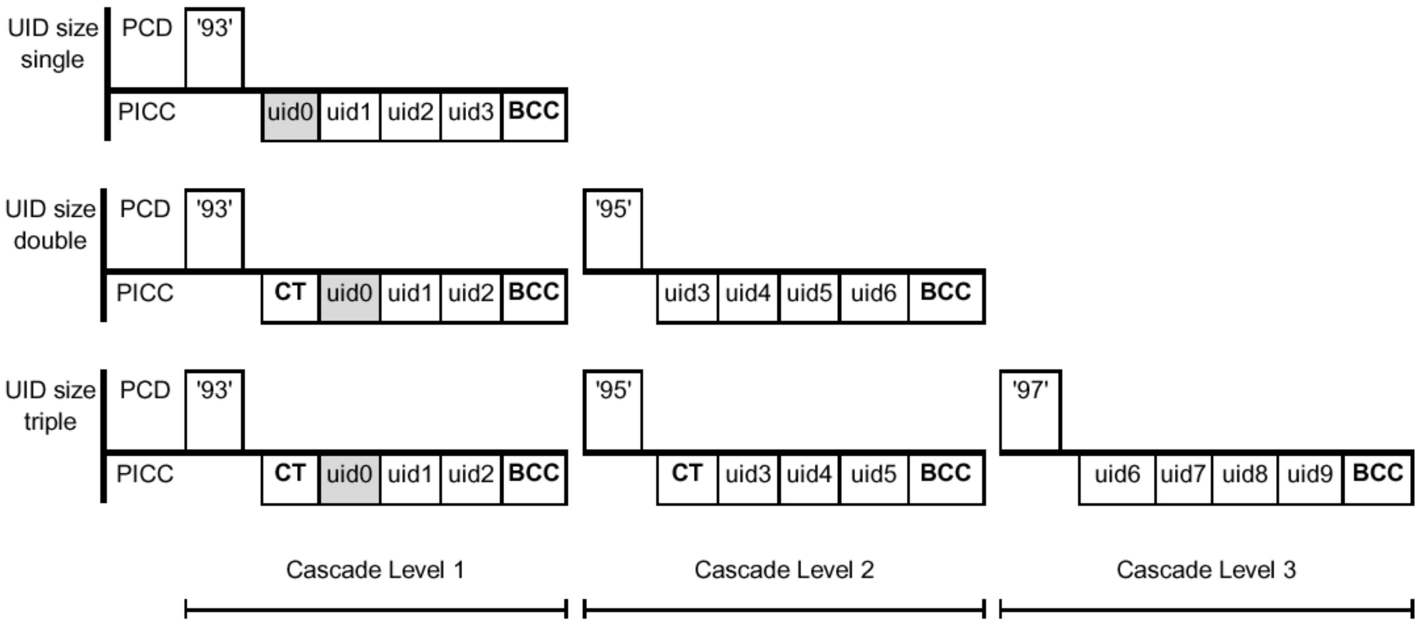
- For double (2 x 3 bytes) or triple UID (3 x 3 Bytes) following options are specified for the first byte:

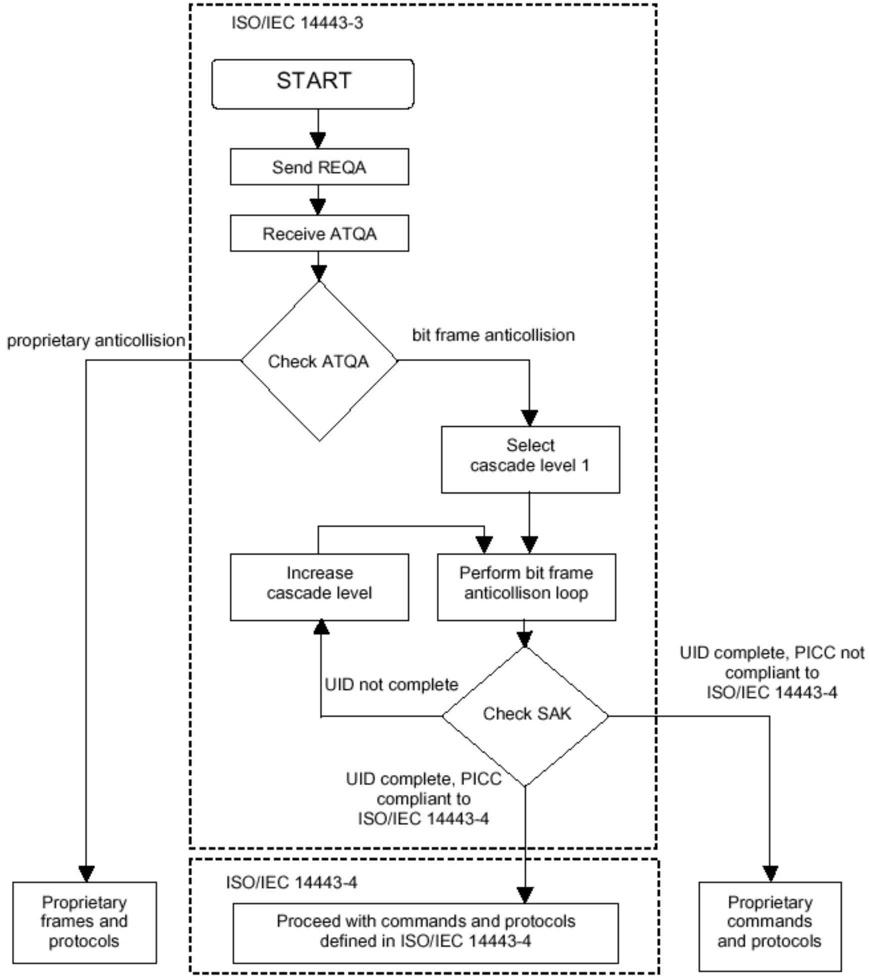
uid0	Description
Manufacturer ID according to ISO/IEC 7816-6*	Each manufacturer is responsible for the uniqueness of the value of the other bytes of the unique number.
* The values '81' to 'FE', which are marked for "Proprietary" in ISO/IEC 7816-6 shall not be allowed in this context.	

Reference: ISO/IEC14443-3

Anti-collision mechanism (IV)

- The first transponder response (ATQA) contains information, if single, dual, or triple UID is used. Accordingly the anti-collision is done up to Cascade Level 1 (always), 2 or 3.

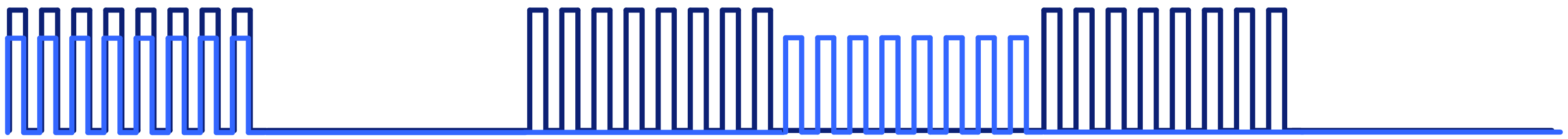




Reference: ISO/IEC14443-3

Anti-collision mechanism (V)

- All Type A transponders in the reader **Operating Volume** start their response at the same time, in the bit grid. The reader can detect a collision as a Manchester code violation, if two half-bits are sub-carrier modulated. This can happen at any digit of the UID, where the first difference between UIDs appears.

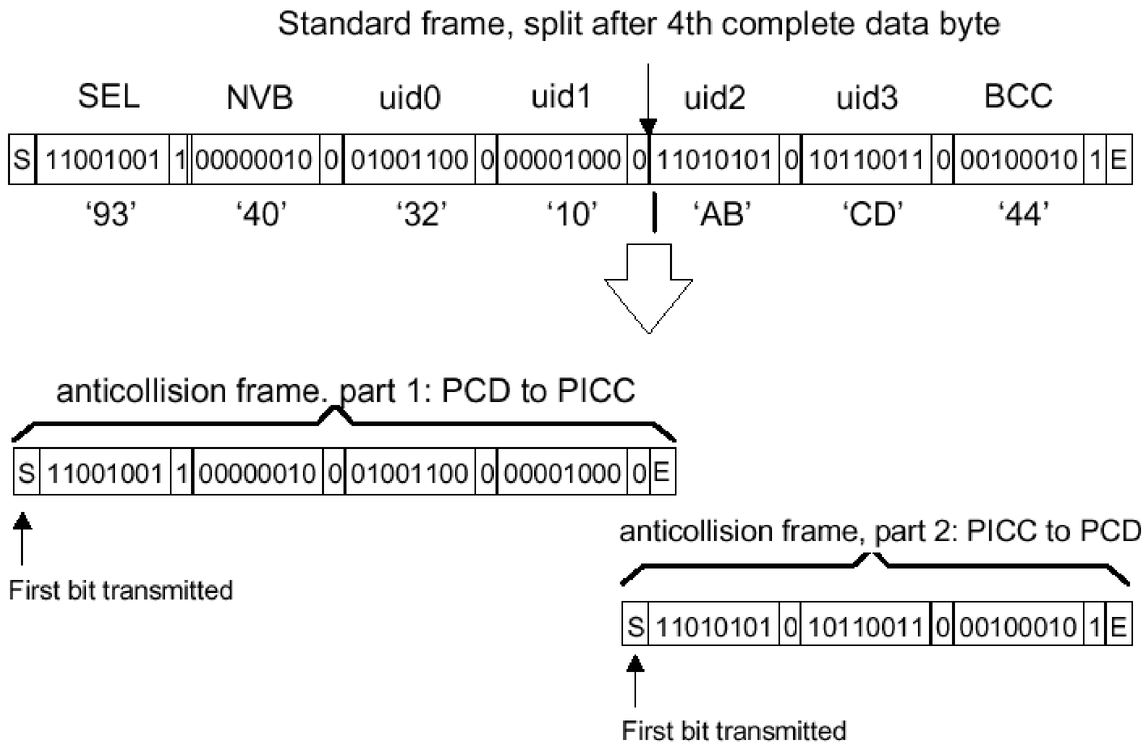


- The reader has two options to solve that: **Full-byte** and s**plit-byte**.
- These can be applied at any Cascade Level.

Reference: ISO/IEC 14443-3

Full-Byte method

- Is used, if the collision appears at the first digit of a byte.
- After the collision has been detected, the reader sends back a complete standard frame containing UID until the last correctly received byte, incl. parity. Only the transponder with a logic “1” at the collision bit responds. It sends the missing parts of its UID starting with the first complete byte.



Reference: ISO/IEC14443-3

FeliCa

Contactless personal Card System from Japan

FeliCa (FeliCa consortium, formerly Sony, Panasonic,...)

– **Carrier frequency:** 13,56 MHz
– ***H*-field strength:** ~ 1,5 – 12 A/m(rms) (depends on reader, not specified)
– **Distance:** ~ < 15 cm (not specified)
– **Data transmission:** Data packets (preamble, sync., length, data content, CRC)
– **Protocol principle:** Reader Talks First
– **Anti-collision:** Mandatory implemented. Polling and response with UID in time-slots.

- **Comm. Interface:**

Data link Reader ➔ Transponder

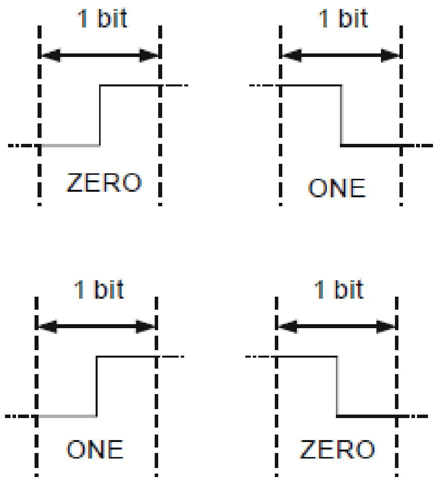
– **Modulation** ASK, 10 % (8 - 14 %)
– **Channel coding** Manchester (each polarity permitted – reader selects)
– **Data rate** 212 kbit/s, 424 kbit/s

Data link Transponder ➔ Reader

– **Subcarrier** No
– **Modulation** Load modulation (external AM/PM)
– **Channel coding** Manchester (each polarity supported)
– **Data rate** 212 kbit/s, 424 kbit/s

Bit-duration and channel coding

- For channel encoding, Manchester Coding is used (each polarity permitted).
- Data rates of 212 and 424 kbit/s are supported. One transmitted symbol has the information content of 1 bit and a duration of 4,72 or 2,36 µs.



Bit-coding obverse.

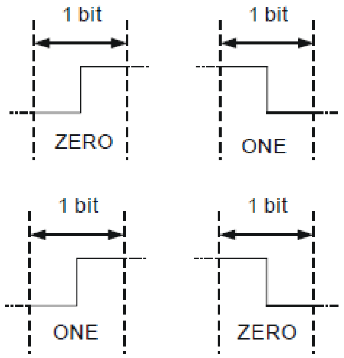
Bit-coding reverse.

- The reader decides, if obverse of reverse coding is used. At the start of the first command, a known, universal SYNC-byte is transmitted, which assigns to the transponder, in which coding it has to send back its data to the reader.
- Specific for FeliCa is, the data transmission is equal for both directions. So, Manchester coding is also used for the transponder ➔ reader link.

Reference: JIS X 6319-4:2005

Bit-duration and channel coding

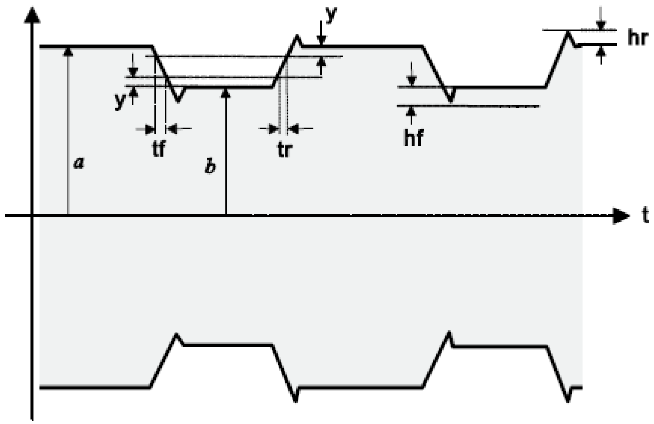
- Modulation of the HF carrier is Amplitude Shift Keying (ASK) for the reader, and load modulation for the transponder (seen as complex AM / PM modulation)



So the minimum duration of a modulation pulse is half a bit duration, for 212 kbit/s ~ 4,72 µs.

Permitted is AM with nominally 10 % modulation index, rise and fall times as well as overshoots are defined as follows:

10 % Modulation Index

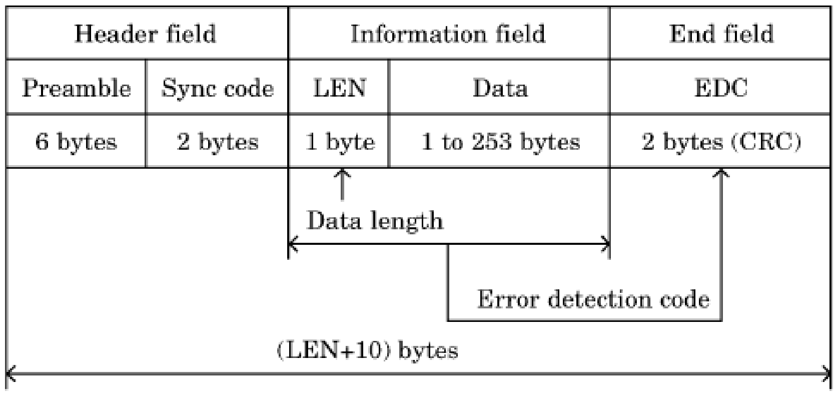


	212 kbps	424 kbps
tf	2,0 µs max	1,0 µs max
tr	2,0 µs max	1,0 µs max
y	0,1 (*a* – *b*)	0,1 (*a* – *b*)
hf, hr	0,1 (*a* – *b*) max	0,1 (*a* – *b*) max

Reference: JIS X 6319-4:2005

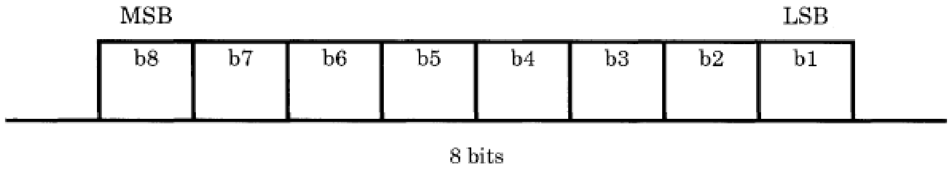
Bit-duration and channel coding

- Data is transmitted in packets. Each packet contains 3 main fields:
  - **Header**, consists of Preamble (to synchronize), and Sync Code
  - **Information field**, contains 1 byte to specify the length (2...254 bytes), and application data
  - **End field**, contains the error recognition mechanism (cyclic redundancy check sum)



- Preamble: 0x00 0x00 0x00 0x00 0x00 0x00
- Sync: 0xB2 0x4D
- LEN: min. value 0x02, max. value 0xFD
- EDC: contains CRC with start value “0000” and generator polynomial

  - Information data is transmitted in form of bytes. One byte is built up as shown:

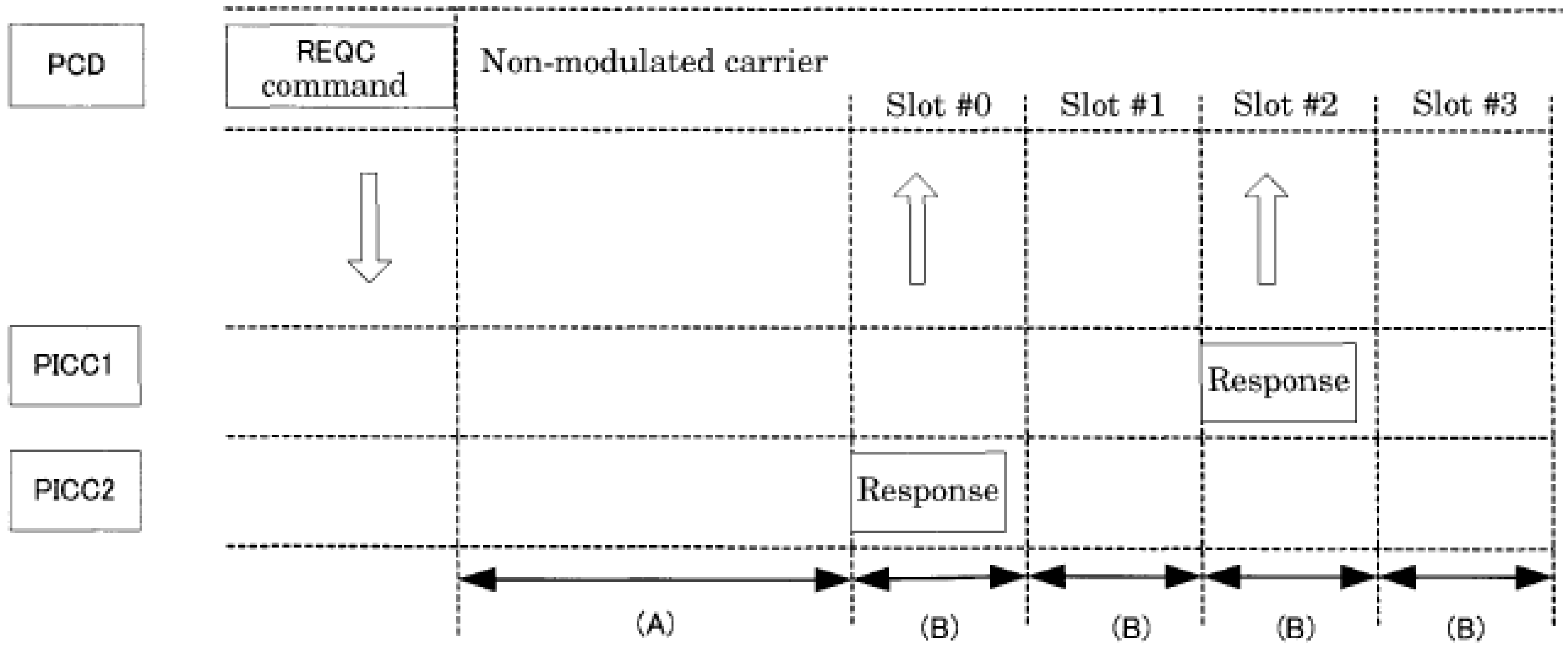


MSB first

Reference: JIS X 6319-4:2005

Anti-collision mechanism

- Initially, the reader sends a REQUEST command, by determining a number of 1…16 time slots for the card response.
- A FeliCa transponder responds in one of the time slots (selected by the first digits of it´s UID).



PICC processing time (A): 512 × 64/fc (approximately 2.417 ms)

Time slot duration (B): 256 × 64/fc (approximately 1.208 ms)

Reference: JIS X 6319-4:2005

Vicinity (ISO/IEC15693)

13,56 MHz object-related Standard (logistics applications, sensors,…)

ISO/IEC15693 (Vicinity) (formerly Philips Semiconductors & Texas Instruments)

– **Carrier frequency:**	13,56 MHz (+/- 7 kHz)	
– ***H*-field strength:**	~ 0,15 – 5 A/m(rms)	
– **Distance:**	~ < 150 cm (depends on reader / transponder, not specified)	
– **Data transmission:**	Data frames (start-bit and stop-bit)	
– **Protocol principle:**	Reader Talks First	
– **Anti-collision:**	Mandatory implemented. Polling and response with UID in time-slots.	

- **Comm. Interface:**

Data link Reader ➔ Transponder (transponder supports both interface options)

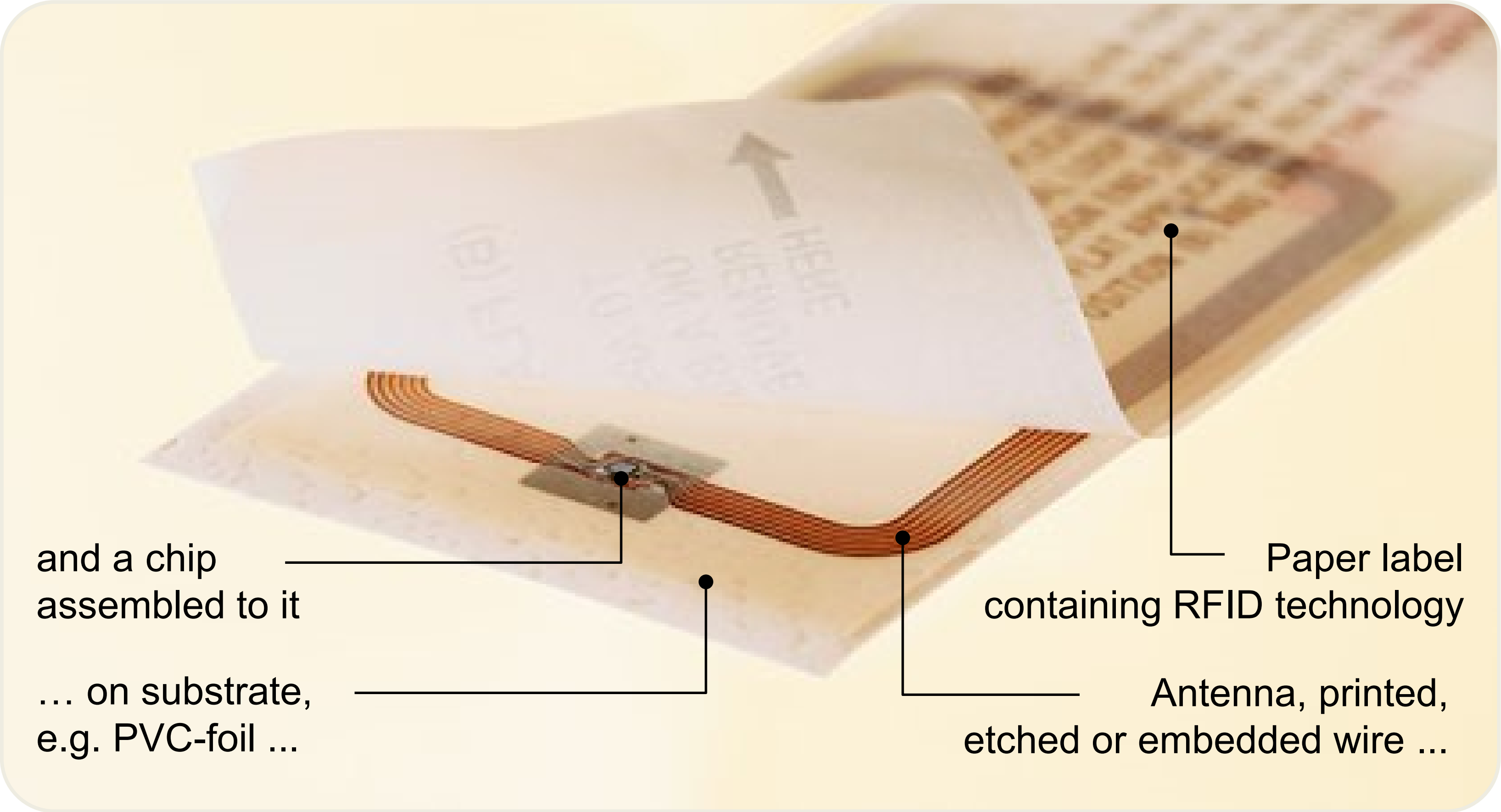
– **Modulation**	ASK, 10 % or 100 %	
– **Channel coding**	256PPM, 4PPM (Pulse Position Modulation), pulse in 2nd half-bit	
– **Data rate**	~ 1,65 kbit/s, ~ 26,48 kbit/s	

Data link Transponder ➔ Reader

– **Subcarrier**	423,75 kHz (fc/32)	or 424 / 484 kHz
– **Modulation**	Load modulation (external AM/PM)	
– **Channel coding**	Manchester (for single Subcarrier)	FSK (for dual Subcarrier)
– **Data rate**	6,62 kbit/s, 26,48 kbit/s	or 6,67 kbit/s and 26,69 kbit/s

What is a “Smart Label”?

- The contactless transponder is the electrically functional part.
- “Label” refers to object-oriented tagging (e.g. logistics).

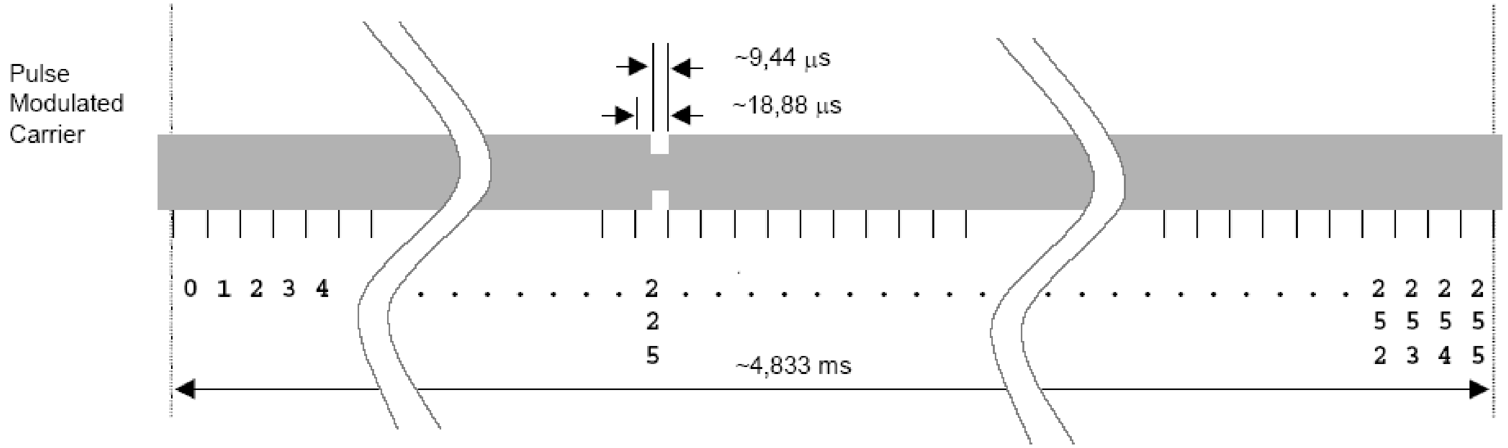


Vicinity (ISO/IEC15693)

Communication link Reader → Transponder

Low data rate: Bit duration and channel coding

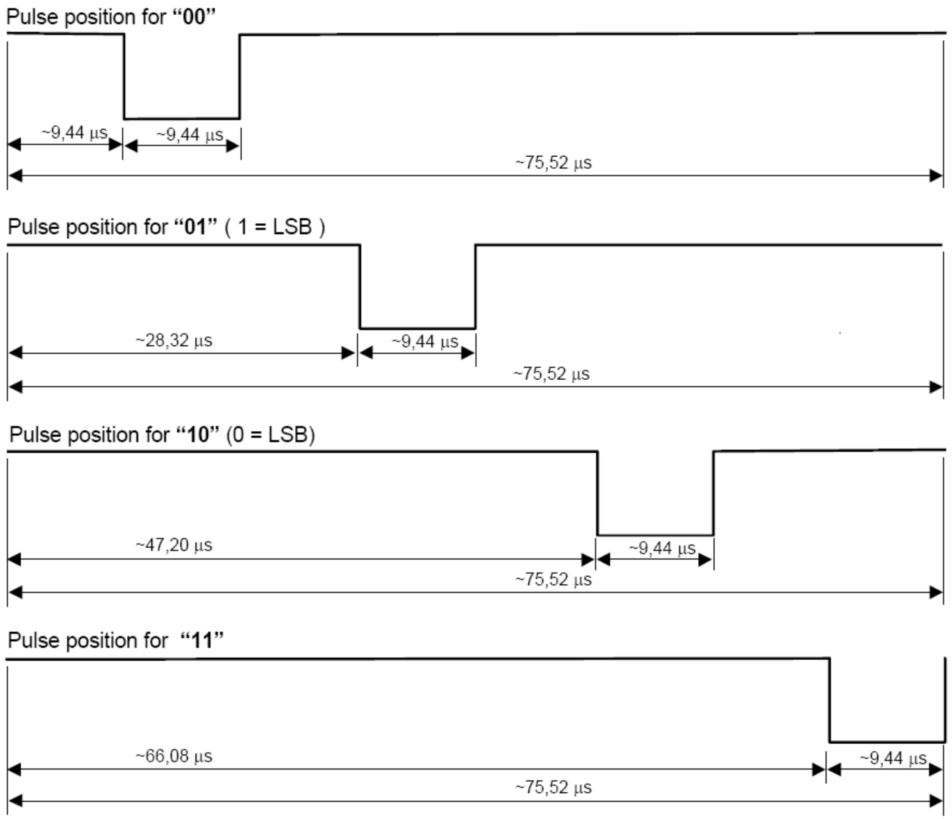
- Channel coding is done by 256 pulse-position modulation (PPM). Symbols of the information content 1 byte = 8 bit are encoded by a single, short modulation pulse in one of 256 time slots.



  – One time-slot is defined by 256 carrier periods (~ 18,88 µs).
  – The duration to transmit one byte is ~ 4,883 ms or 8 x 256 x 256 carrier periods.
  – The base data rate is ~ 165 kbit/s, means the carrier frequency divided by 8192.
  – The example shows the information E1(hex) = 11100001_{bin} = 225_{dec}.

High data rate: Bit duration and channel coding

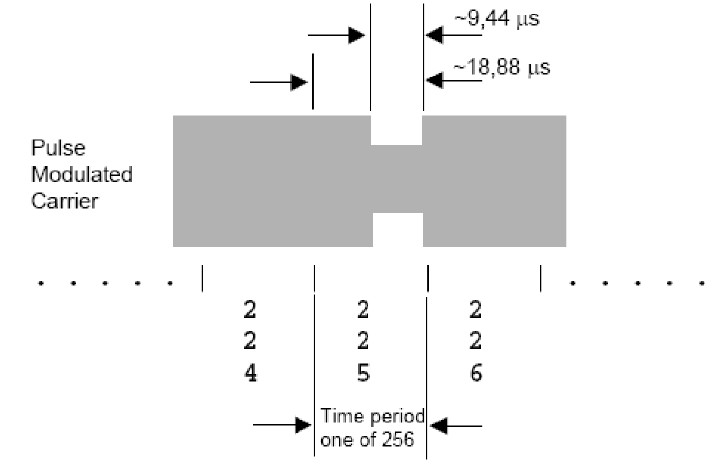
- Alternatively, 4 PPM is used for channel encoding. Symbols of an information content of 2 bits are transmitted by a short pulse (ASK) in one of 4 time-slots.



- One time-slot is again defined by 256 carrier periods (~ 18,88 µs).
- Information of one byte is encoded in 4 symbols of 2 bit information content
- Duration to transmit 1 byte is 4 x 256 carrier cycles (~75,52 µs).
- The data rate is ~ 26,48 kbit/s, means the carrier frequency divided by 512.

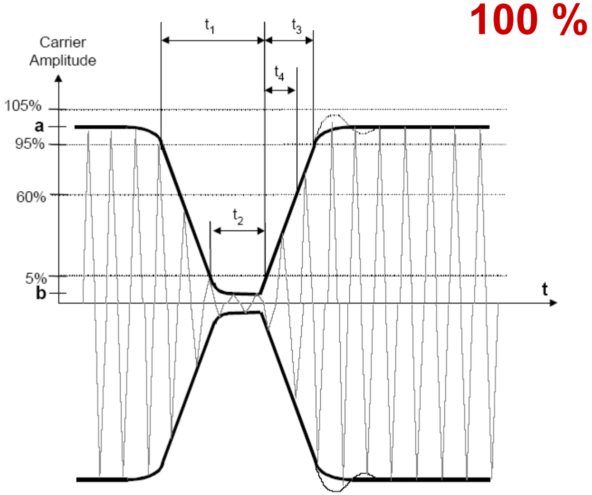
Modulation on the 13,56 MHz carrier

- Modulation of the RF carrier is done in pulses, which are applied in 2nd half-bit.



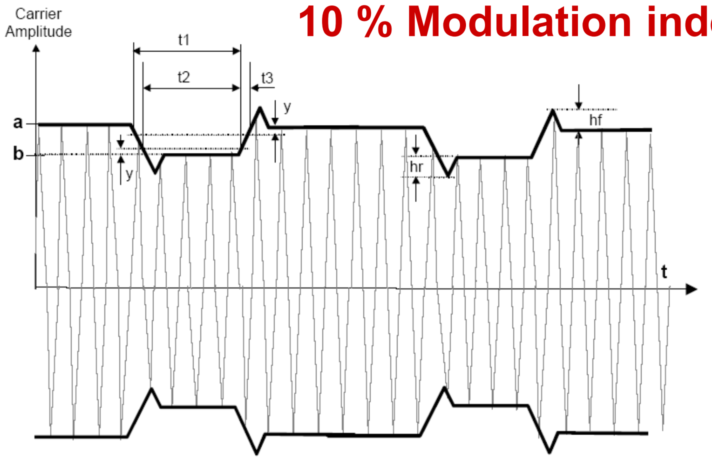
- The maximum pulse duration is half the duration of a time-slot, 9,44 µs.
- For modulation, AM of nominally 100 % and 10 % modulation index is permitted, according to the following specification:

100 % Modulation index



	Min (µs)	Max (µs)
t1	6,0	9,44
t2	2,1	t1
t3	0	4,5
t4	0	0,8

10 % Modulation index



y	0,05 (a-b)
hf, hr	0,1 (a-b) max

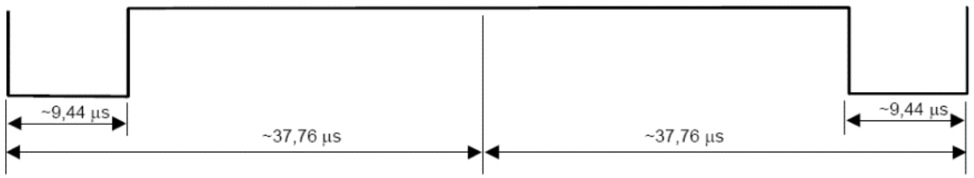
	Min	Max
t1	6,0 µs	9,44 µs
t2	3,0 µs	t1
t3	0	4,5 µs
Modulation Index	10%	30%

Reference: Specification in ISO/IEC 15693-2, Measurement in ISO/IEC10373-7

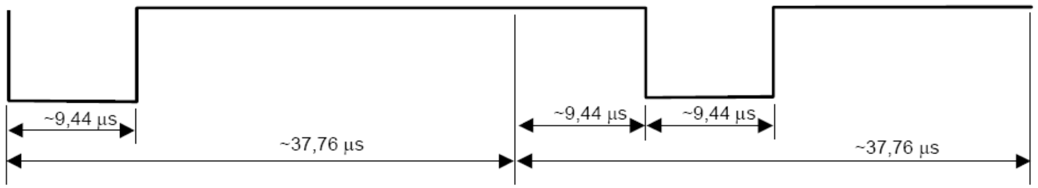
Data frame

- Data is transmitted in frames, initiated by a start-of-frame (SOF) symbol, and completed by an end-of-frame (EOF) symbol.
- This SOF symbol announces also the data rate (256 PPM or 4 PPM).

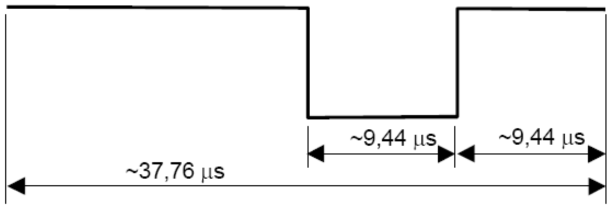
SOF-Symbol for 256 PPM:



SOF-Symbol for 4 PPM:



- The EOF symbol is equal for both data rates (1,65 kbit/s using 256 PPM, or 26,48 kbit/s using 4 PPM), as follows:

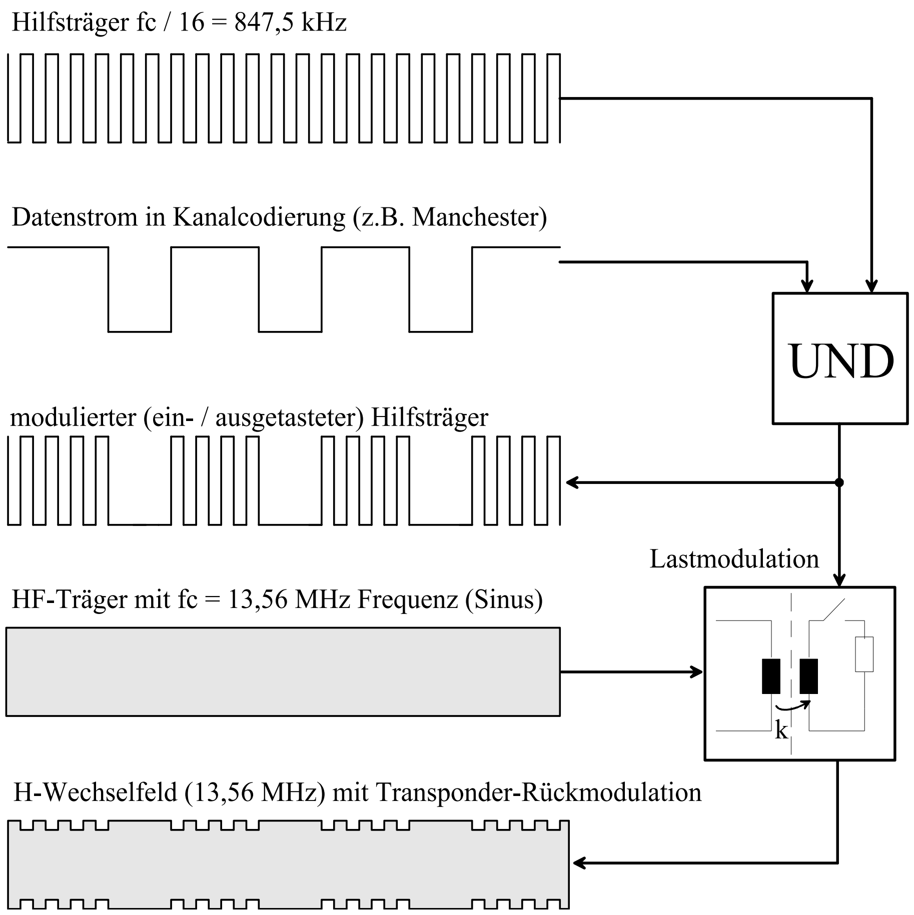


Vicinity (ISO/IEC15693)

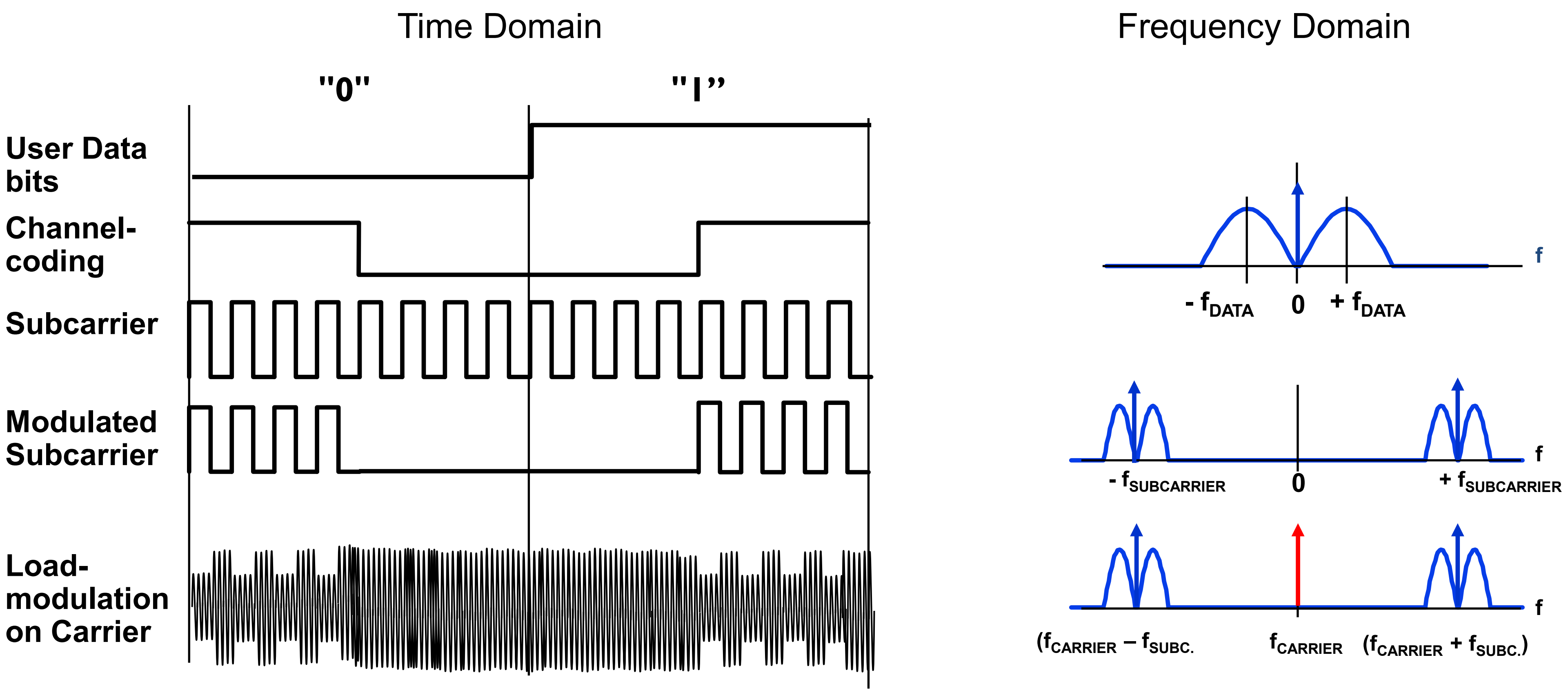
Communication link Transponder → Reader

Principle of Load modulation

- The ISO/IEC15693 sub-carrier of 423,75 kHz in is generated in the transponder by dividing the reader carrier frequency by 32.
- The data frame in channel coding (Manchester for single SC or NRZ for FSK) is logically combined with the sub-carrier.
- Result is a binary 424 kHz signal, which can be used for digital modulation.
- Logic levels of this signal control a switch, which changes the transponder antenna resonant circuit properties (Q, or f_{RES}).
- Vicinity coupling (in the near-field) modulates the impedance of the reader antenna circuit, consequently the reader antenna voltage. This can also be understood as external AM/PM (modulation index depends on coupling and resonance properties!)



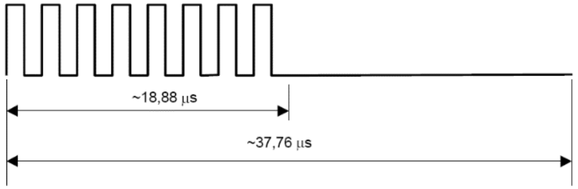
Load modulation in Time- and Frequency Domain



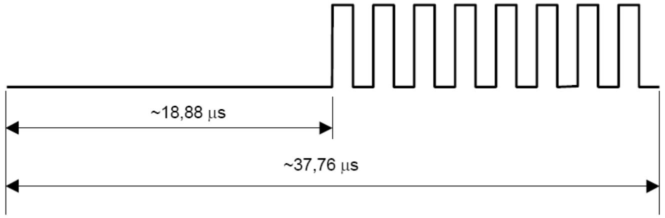
High rate: Bit duration, Coding and Modulation

- Single sub-carrier:
  - Load modulation using one sub-carrier at ~ 424 kHz (32 carrier periods) and Manchester channel encoding (only one half bit-duration is modulated. 1 bit = 16 subcarrier cycles, 16 x 32 = 512 carrier cycles, ➔ ~ 26,48 kbit/s

logic 0 - first half bit duration modulated

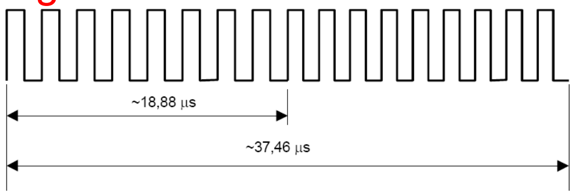


logic 1 – second half is modulated

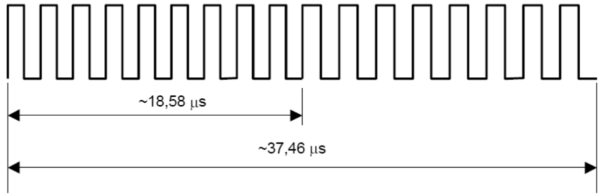


- Two sub-carriers:
  - Load modulation using two sub-carriers at 423.75 kHz (32) and 484.28 kHz (28) and non return to zero (NRZ) channel encoding. 1 bit = 480 carrier cycles, ➔ ~ 26,69 kbit/s

logic 0 – first half 424 kHz



logic 1 – second half 424 kHz



For low data rate all times x 4.

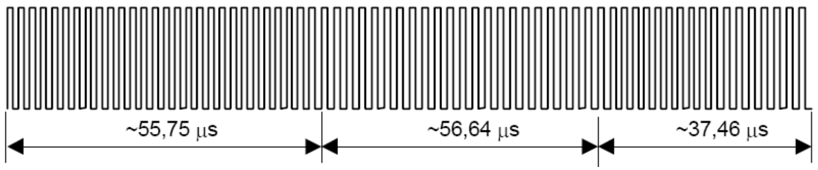
Data frame

- Data is transmitted in frames, starting with an SOF and completed with an EOF symbol. These symbols both provide an intentional channel code violation.

SOF symbol, operation at 1 sub-carrier:

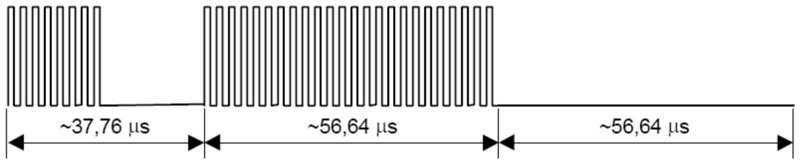
non-modulated, 424 kHz (24 periods), logic 1

SOF symbol, operation at 2 sub-carriers:



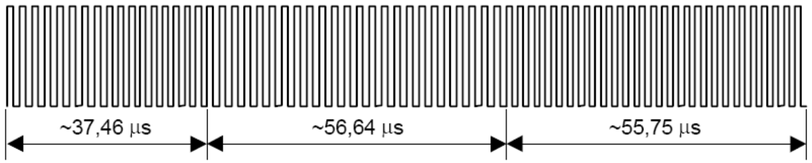
~484 kHz (9 periods), ~424 kHz, logic 1

EOF symbol, operation at 1 sub-carrier:



logic 0, ~ 424 kHz (24 periods), non-modulated

EOF symbol, operation at 2 sub-carriers:



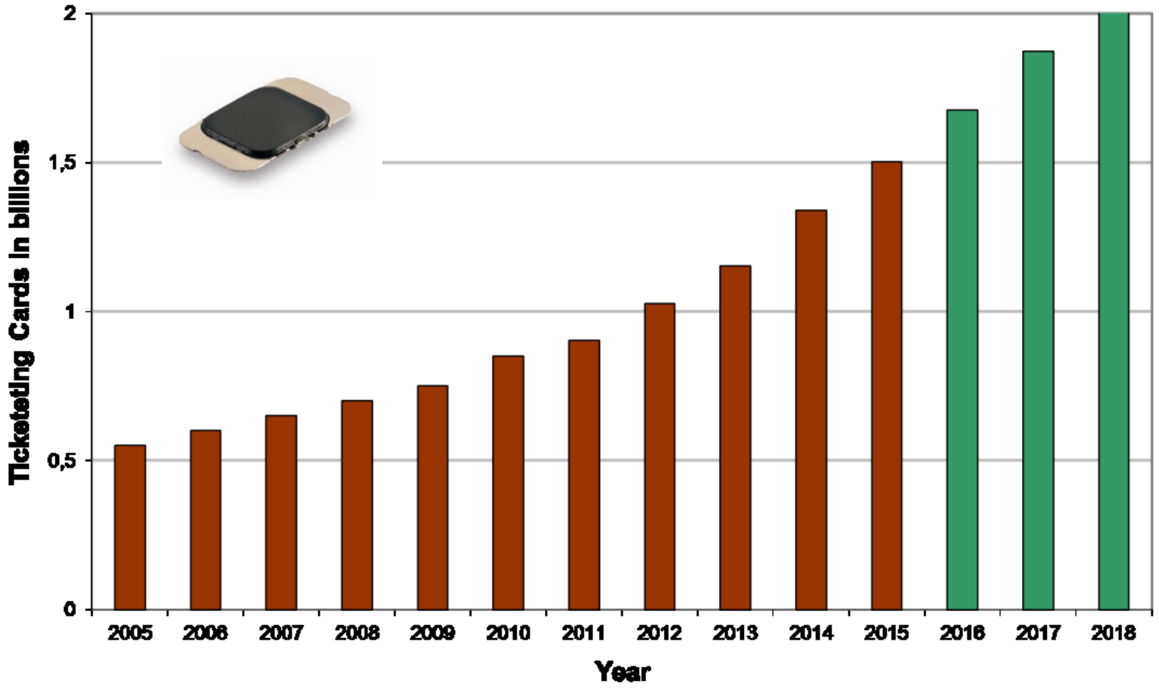
logic 0, ~ 424 kHz, 484 kHz (27 periods)

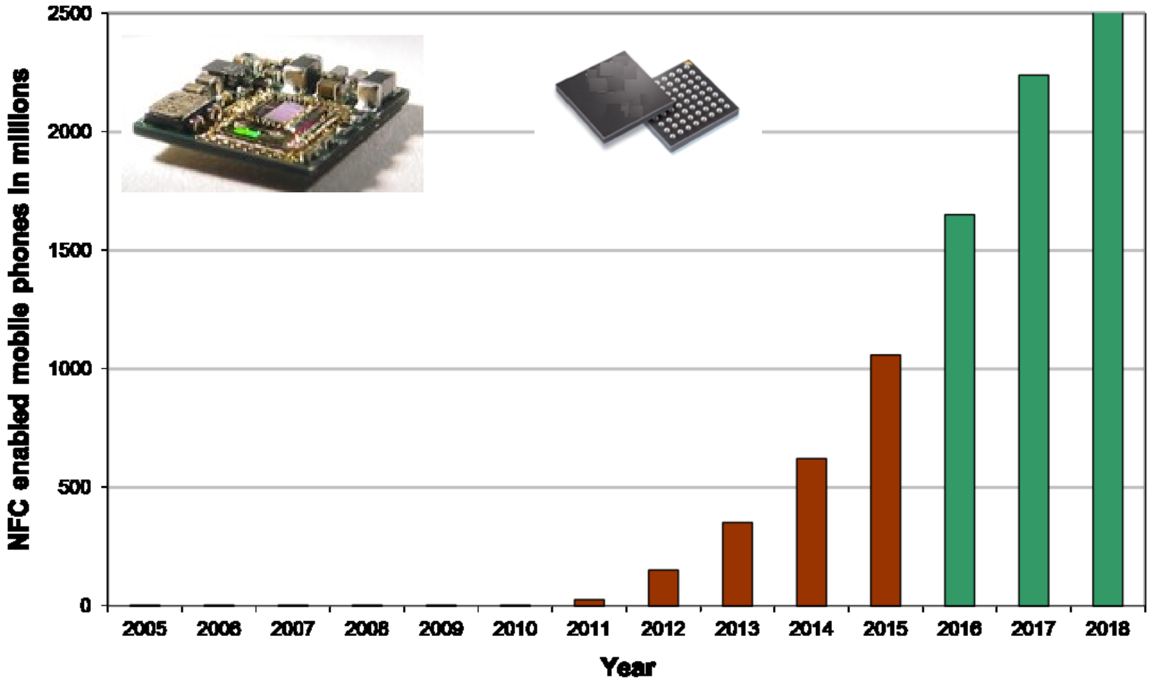
- Transponder must be ready (to receive) 1 ms after Reader *H*-field carrier power-on.
- Transponder must be ready (to receive) 300 µs after sending a response.

Additional Specifications

In the context of NFC

NFC – Some Market figures

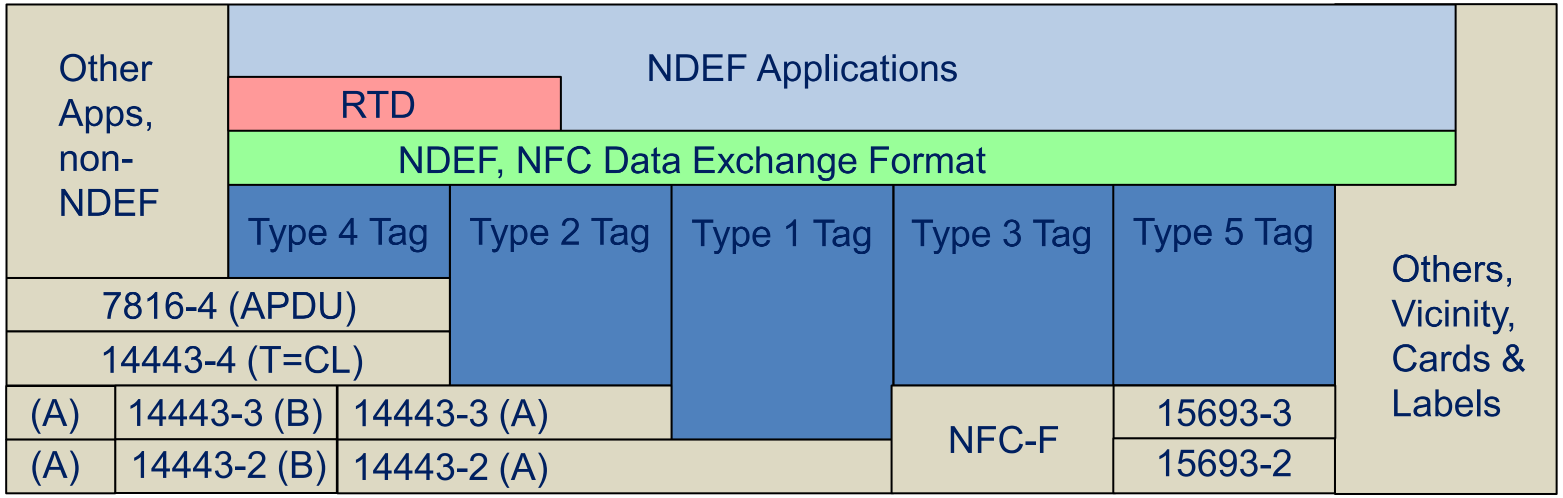




Batteryless, contactless tickets & NFC tags

Devices with NFC interface (incl. reader mode option)

NFC Tag Types



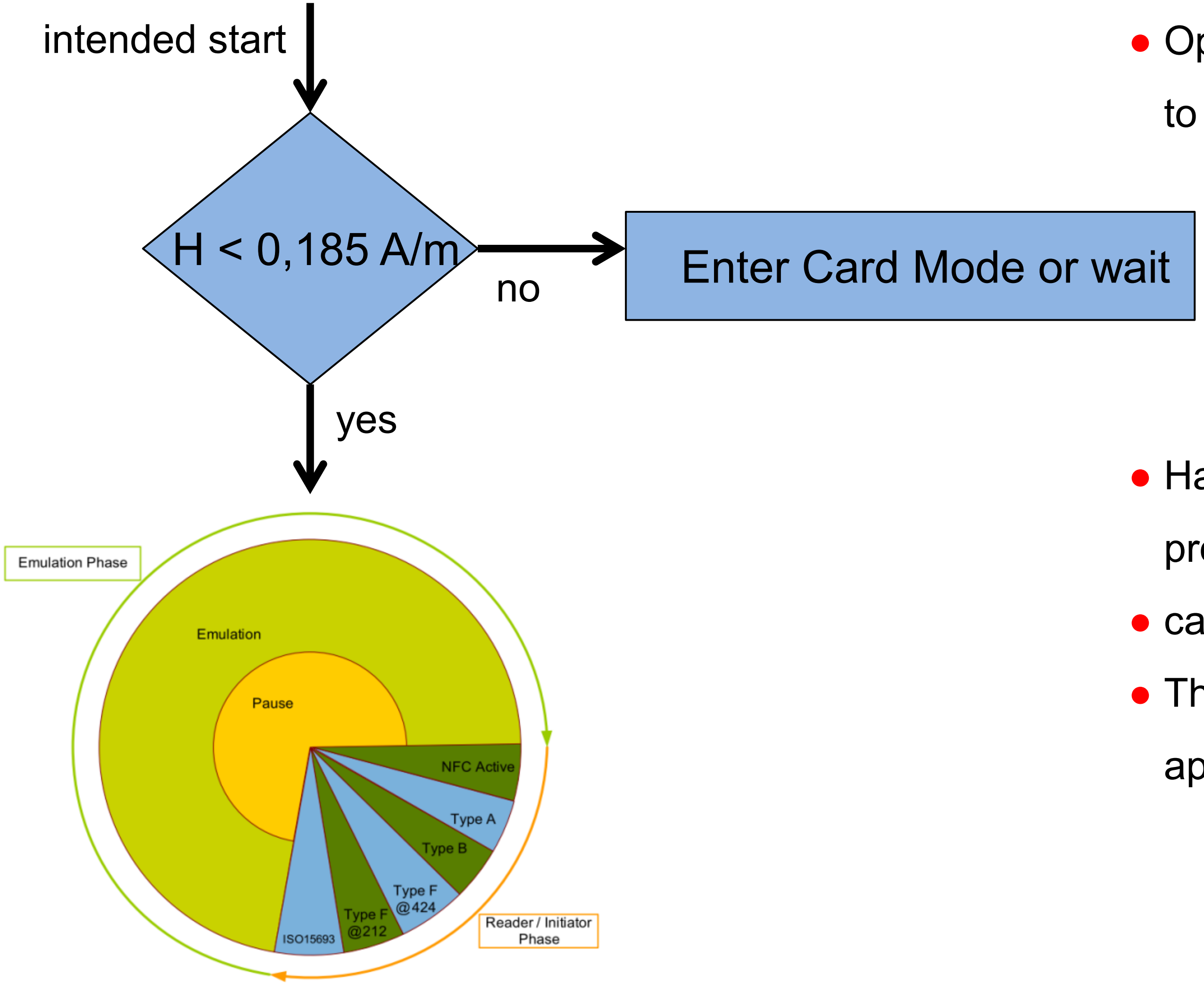
NDEF….NFC Data Exchange Format

RTD….Record Type Definition

APDU….Application Protocol Data Unit (contact cards, ISO/IEC7816)

T=CL….Transport layer is contactless, protocol for contactless cards

Handling of different Modes and Protocols



- Operation of the NFC Interface in **reader mode** requires first to check if the channel is free ("listen before talk").
- Handling of contactless cards and tags using different protocols requires an initial Polling Loop.
- carrier on – polling A – polling B – polling F – ….
- The implementation can be optimized for the intended application or based on geographic information.

NFC interface implementation in a Device

NCI…..NFC Controller Interface

SWP….Single Wire Protocol
ETSI TS 102 613 & 102 694-1

HCI…..Host Controller Interface
ETSI TS 102 622 & 102 695-1

MN….Impedance Matching Network loop antenna

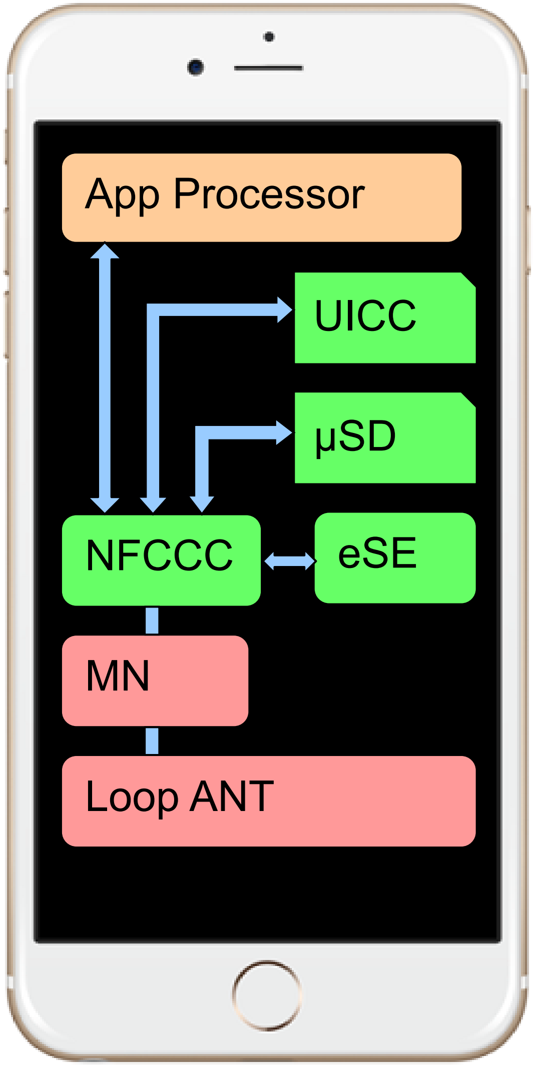
Proximity A & B, ISO/IEC14443 & 10373-6 (Test)

FeliCa, JIS X 6319-4

Vicinity, ISO/IEC15693 & 10373-7

NFCIP-1, ECMA340, ISO/IEC18092
NFCIP-2, ECMA354, ISO/IEC21481

Mifare, HID, Calypso, Topaz,….



NFCC…NFC Controller

UICC….Universal Integrated Chip Card

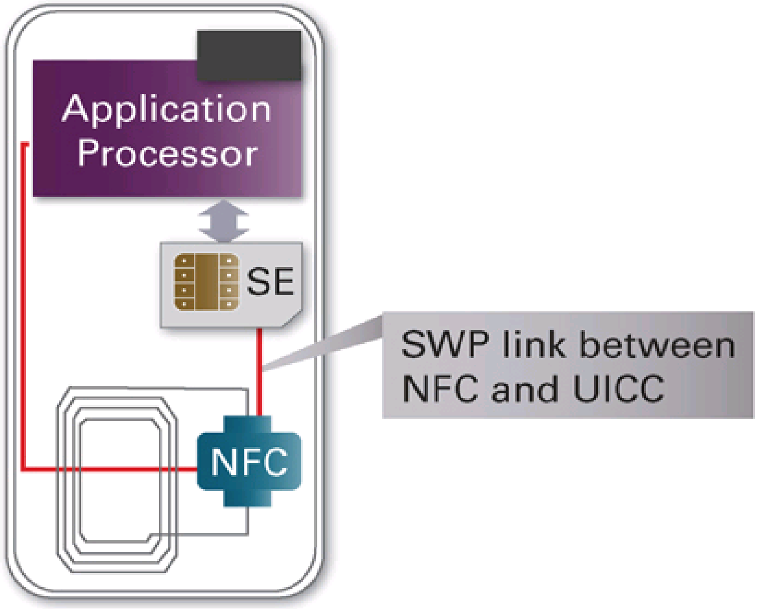
µSD…..Micro Secure Device

eSE…..embedded Secure Element

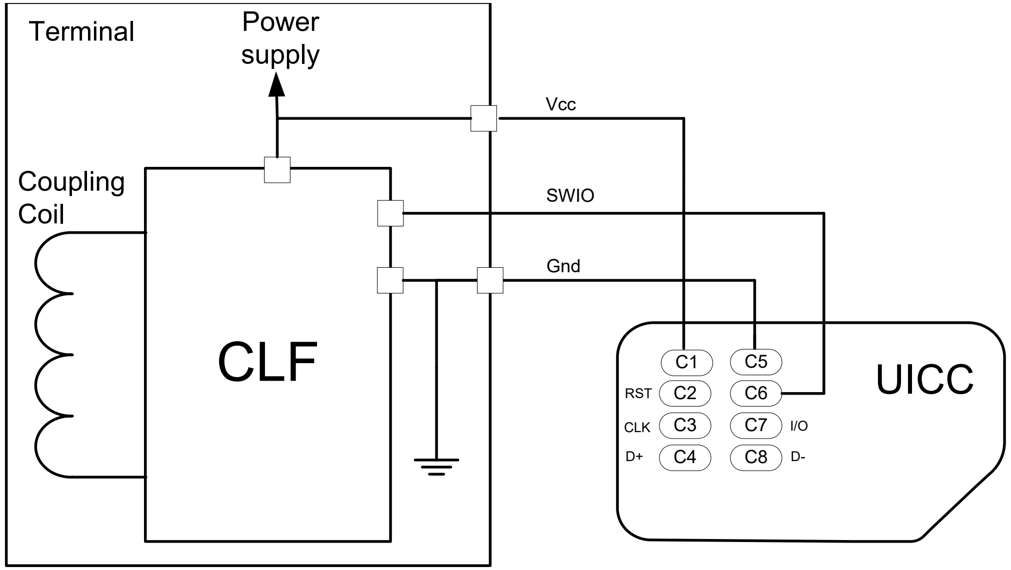
NFC enabled Device

NFC Connections – Single Wire Protocol usage

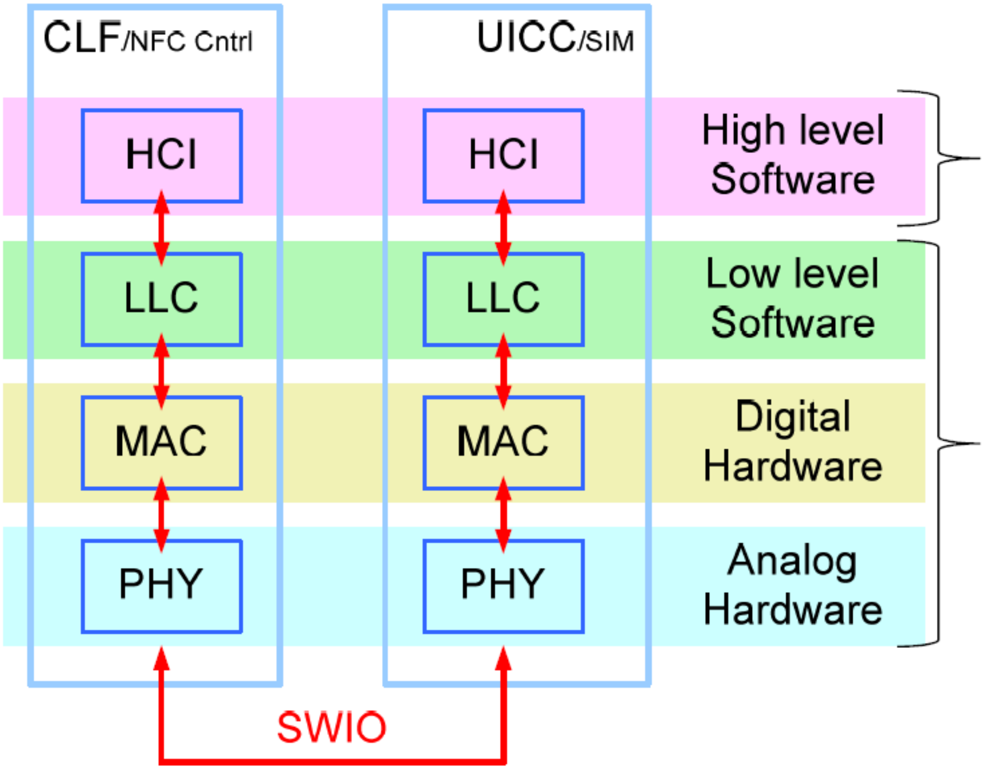
- Single wire protocol offers
  - one data connection between UICC (SimCard) and CLF (PN5xx)
  - two supply power connections (GND and UCC)
- All secure applications can be stored on the UICC (De-)Ciperhing is done on the UICC so the SWP data transfer is already encrypted.



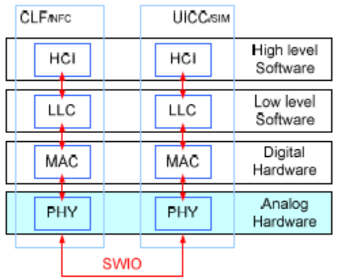
NFC CLF + SIM (SE)



SWP – Physical Interface

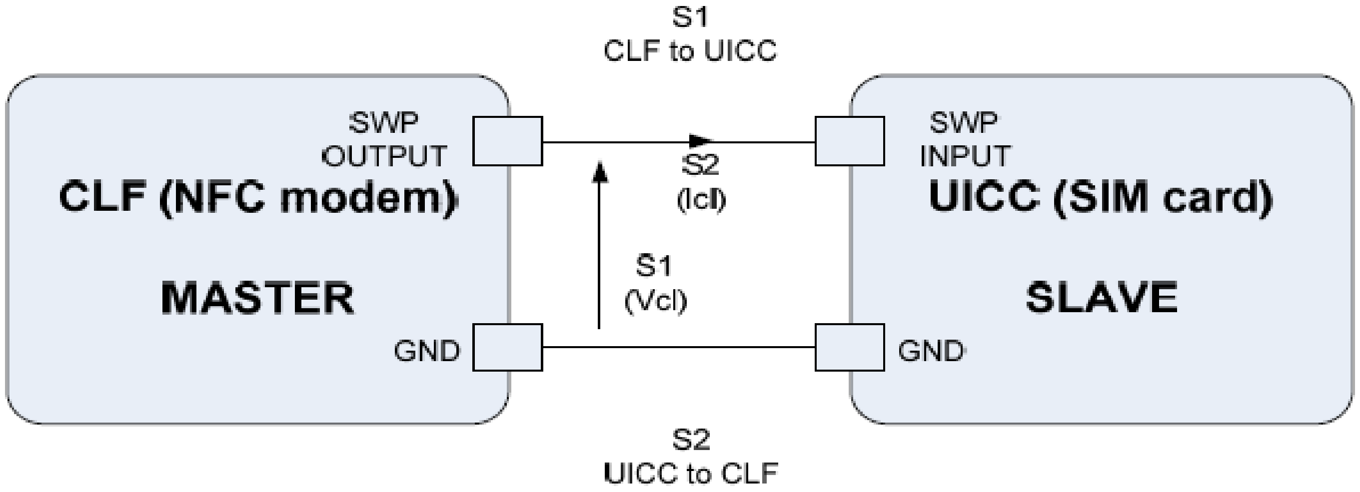


Layer (s) defined in	Tests defined in
TS 102 622	TS 102 695
TS 102 613	TS 102 694



SWP – Functional Overview

- SWP is based on master-slave principle
  - CLF is master
  - UICC is slave
- SWP is based on voltage – current transmission
  - Master uses the voltage to modulate the signal (S1 signal)
  - Slave draws current to modulate the signal (S2 signal)
- SWP is full-duplex compatible
  - S1 and S2 can be simultanously transmitted



Thank you for your Audience!

Please feel free to ask questions...

Hinweise – Notizen

Questions for self-evaluation

- Give an overview of main properties specified in the product standards for Proximity, Vicinity, FeliCa and NFC!
- For ISO/IEC14443 A (or NFC-A), explain, how a Proximity reader command is constituted and how it is modulated at the air interface. Also explain, how a Proximity card response is built, and how it appears at the air interface.
- Explain differences of Proximity ISO/IEC14443 and other relevant protocols!
- Explain the meaning of NFC, which main protocols it can handle. Explain reader mode, card mode, and peer-to-peer mode. How can an NFC device switch on in reader mode and differentiate between different protocols?
- Give examples and explain, how an anti-collision mechanism works!

References

- ISO/IEC14443-1: Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics, second edition, June 2008.
- ISO/IEC14443-2: Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface, second edition, Sept. 2010.
- ISO/IEC14443-3: Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision, second edition, Nov. 2009.
- ISO/IEC14443-4: Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol, second edition, July 2008.
- ISO/IEC10373-6: Identification cards – Test methods – Part 6: Proximity cards, second edition, Jan. 2011.
- ISO/IEC15693-1:
- ISO/IEC15693-2:
- ISO/IEC10373-7
- ISO/IEC18092:2013 Information Technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)
- JIS X 6319-4:2005 (E), Specification of Implementation for integrated circuit(s) cards – Part 4: High Speed proximity cards, first English edition, 2007.
- EMVCo, “Book D – EMV Contactless Communication Protocol Specification”, in EMV Contactless Specifications for Payment Systems, v. 2.2, June 2012

References

- www.nfc-forum.org/ NFC Forum Homepage
- www.emvco.com/ EMVCo Contactless Payment
- www.discover.com Discover (Contactless Card System)