ISO/IEC JTC 1/SC 17
Cards and personal identification
Secretariat: BSI (United Kingdom)

Document type:	Disposition of Comments Report
Title:	Disposition of comments on: CD ISO/IEC 14443-3:2011/AM2 — Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision — AMENDMENT 2: Bits rates higher than fc/16 and up to fc
Status:	**Reference documents:** **Ballot is in SC17 N 4098 = WG8 N 1774** **Ballot Result is in SC17 N 4163 = WG8 N 1775**
Date of document:	2011-05-26
Expected action:	INFO
No. of pages:	31
Email of secretary:	chris.starr@ukpayments.org.uk
Committee URL:	http://isotc.iso.org/livelink/livelink/open/jtc1sc17

Disposition of comments on:
CD ISO/IEC 14443-3:2011/AM2 — Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision — AMENDMENT 2: Bits rates higher than fc/16 and up to fc

Reference documents:

Ballot is in SC17 N 4098 = WG8 N 1774
Ballot Result is in SC17 N 4163 = WG8 N 1775

Project Editor:
Reinhard Meindl, Austria

The following pages provide the details of the comments and detailed information about their resolutions, how WG8 had resolved each received comment from the CD Ballot (PDAM) at the WG8 meeting held in Ispra, Italy, on 2011-03-28/30.

The two negative votes from Germany and Japan could be resolved primarily by the WG8 Resolution 49.03, (contained in WG8 N 1796 = SC17 N 4xxx), which determines a separation of the very high bit rate options into two spectrums with one related to the ASK and the other one to the PSK technology. That decision has an impact to this amendment which will be continued as being just related to ASK furtheron. The new text of this one, as presented in WG8 N 1805, is to be processed as FCD according to the WG8 Resolution 49.07.

Template for comments

Date:	Document: **ISO/IEC 14443-3/PDAM2**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Proposed Editors Disposition**
FR1	3.4	etu definition	ED	D can have higher values		Resolved
FR2	6.1	Table 1	ED	Table 1 is very similar with the same table in 14443-2, but the table in 14443-2 contain specific names for the different types of modulation	Update table 1 (or delete it because it mainly brings the "D" definition which is not used in 14443-3)	Resolved
FR3	7.1.4	Tables 17 and 18	ED	A single line ">fc/64" can be used for fc/32, fc/16 and higher bit rates.	Group all these bit rates in a single line	accepted
FR4	7.1.5	Table 20	ED	A single line ">fc/64" can be used for fc/32, fc/16 and higher bit rates.	Group all these bit rates	accepted
FR5	7.9.4.4	Table 27	ed	clarity	Avoid breaking tables on 2 pages	accepted

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial – For technical comments, please indicate whether your comment is a MAJOR or MINOR technical comment.

NOTE Columns 1, 2, 4, 5 and 6 are compulsory.

Template for comments and secretariat observations

Date: January 20, 2011	Document: SC17 N4098 Notification of Ballot, ISO/IEC 14443-3:2010/PDAM 2 – Identification cards – Proximity Cards – Part 3: Initialization and anti-collision – Amendment 2 – Bit rates higher than fc/16 up to fc and increased frame size (ISO/IECJTC1/SC17/WG8N1734

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
US	Page 2 of the amendment	Table 1 – bit rates	Techn ical	There are many applications that demonstrate that the ISO/IEC 14443 standard does not need the complex PSK modulation approach, as proposed. Therefore, **only** ASK shall be supported. A Type B PICC can use both ASK and PSK, whereas a Type A PICC can only use PSK. This results in a disadvantage from an infrastructure point-of-view. The maximum speed supported by ASK is 6.8 Mbits, whereas the maximum speed supported by PSK is 13.56 Mbits (theoretical). PSK offers many different modes (see the table in PSK section of the 14443 standard). This high number of modes (supported by PSK) requires significant effort for testing, especially for PCD (readers). Therefore, the high number of modes supported by the PSK shall be deleted.	Delete PSK from Table 1 on Page 2 of the amendment.	Resolved by splitting the documents
US	Page 5 of the base standard	Page5 of the base standard, definition section	Techn ical	If PSK is to be included, a definition of PSK shall be added.	Add the definition of PSK to this amendment,	Resolved (definition is available in part 2)

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Template for comments and secretariat observations

Date: 08/03/10	Document: ISO/IEC 14443-3:2010/PDAM 2

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
UK1	Page 5; 6.1	Last sentence	te	If a bit rate higher than fc/16 is selected for PCD to PICC communication, then a bit rate higher than fc/128 shall be selected for PICC to PCD communication.	Either delete this sentence Or change to: If a bit rate higher than fc/16 is selected for PCD to PICC communication, then a bit rate higher than fc/16 shall be selected for PICC to PCD communication.	withdrawn
UK2	Page 45 7.10.4	Table 34	te	Why stop at frame size 4096?	Define D = 8192, E = 16384, F = 32768	Resolved by explanation

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

German comments on ISO/IEC 14443-3-PDAM2 (SC17n4098)

Date: 2011-03-22	Document: **ISO/IEC 14443-3 PDAM 2**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted **Please enter your name here**
DE 1			ge	Germany disapproves because of the following reason: Germany requests to specify only one single VHBR Mode for bitrates up to 6,78 Mbit/s, which shall be ASK. The PSK modulation scheme shall be specified for data rates greater than 6,78 Mbit/s. If the above concept will be satisfyingly considered, Germany will change its vote to "Approval".	The document shall be updated accordingly to reflect the proposed changes.	Resolved by Principal Wg8 decision
DE 2		Titel	ED	For better understanding and being clearer the title should be changed	Change title to: "Bit rates higher than *fc* / 16 up to *fc* and frame sizes higher than 256 bytes up to 4096 bytes." Same for French Title	accepted
DE 3	Page 5, 6.1	Table 1	te	Table shall be modified according DE1	Replace Table 1 by Annex 1	Resolved Add first 3 columns of last 3 rows of annex 1
DE 4	Page 7, 6.2.1.1	Table 2	te	Table shall be modified according DE1	Delete: fc/16/3, fc/8/3	Resolved Add fc/8, fc/4 and fc/2 only
DE 5	Page 9, 6.2.3	list	te	Missing link to frames for ASK modulation for bit rates higher than fc/16 up to fc/2.	Add after last dash: " – PCD standard frames for ASK modulation and bit rates higher than *fc*/16 up to *fc*/2."	Resolved " – PCD standard frames for bit rates of fc *fc*/8, fc/4 and *fc*/2."
DE 6	Page 11, end of 6.2.3.3	end of paragraph	te	Missing link to frames for ASK modulation for bit rates higher than fc/16 up to fc/2.	Add new subclause after 6.2.3.3: "**6.2.3.4 PCD standard frames for ASK modulation and bit rates higher than *fc*/16 up to *fc*/2**	Resolved *Adapt the wording* "**6.2.3.4 PCD standard frames for bit rates**

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment: ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted **Please enter your name here**
					The character transmission format and character separation is defined in 7.1.1 and 7.1.2, respectively. The frame format is defined in 7.1.3.	**of fc fc/8, fc/4 and fc/2** The character transmission format and character separation is defined in 7.1.1 and 7.1.2, respectively. The frame format is defined in 7.1.3.
DE 7	3.5	paragraph	ed	Update frame definition to match new definitions of VHBR	Replace frame definition by: " **frame** a frame is a sequence of data bits and optional error detection bits, with prefix sequence at start and a closing sequence at the end. "	Withdrawn
DE 8	6.2.3	clause	ed	Additionally list extended frame	Add another bullet at the end with: " - Extended frames "	Rejected Will be checked by TF2 for possible new amendment
DE 9	6.2.3.4	Clause	Te	Add a section introducing an extended frame format reflecting the challenges of VHBR and frame lengths up to 4kByte. The introduction of the extended frame format increases robustness in communication as the hamming code can detect and correct a single bit error within a hamming block.	See Annex 2	Rejected Will be checked by TF2 for possible new amendment
DE 10	6.2.4	title	ED	Due to the introduction of the extended frame change chapter structure of CRC	Change Clause title to: "	Rejected Will be checked by TF2 for

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted **Please enter your name here**
					6.2.4 CRC Coding "	possible new amendment
DE 11	6.2.4.1	paragraph	ED		Move CRC_A section to subclause 6.2.4.1: " 6.2.4.1 CRC_A "	Add a note: at the end of 7.9.4.5. CRC_B efficiency decreases when the frame size increases. Improved optional error detection and correction methods may defined in future
DE 12	6.2.4.2	Paragraph/ Clause	Te	Introducing CRC_32 for extended frames. The probability of an undetected error for frame lengths exceeding 256Bytes is in the range of a BER of 10^-5. This means we cannot be sure if we do not encounter an error or if the CRC16 is not detecting this error. Therefore, CRC_32 is introduced for extended frames.	ADD new subclause : "6.2.4.2 CRC_32 A frame that includes CRC_32 shall only be considered correct if it is received with a valid CRC_32 value. The frame CRC_32 is a function of k data bits, which consist of all the data bits in the frame, excluding parity bits, SOC and EOC, and the CRC_32 itself. For error checking, the four CRC_32 bytes are sent in the extended frame after the data bytes. The CRC_32 is as defined in ISO/IEC 13239. The initial register content shall be '0xffffffff' and the register content	Rejected Will be checked by TF2 for possible new amendment

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted **Please enter your name here**
					shall be inverted after calculation. For examples refer to Annex B.”	
DE 13	7.1.3.1	title	ed	Shift Clause of 7.1.3 to subclause 7.1.3.1 and rename title	New title of subclause: “ Standard Frame “	Rejected Will be checked by TF2 for possible new amendment
DE 14	7.1.3	title	ed	Due to the introduction of extended frames change title	Change Title: “ Frame Format “	Rejected Will be checked by TF2 for possible new amendment
DE 15	7.1.3.2	clause	TE	Add new clause for extended frames	Add subclause “ 7.1.3.2 Extended frame See 6.2.3.5 ”	Rejected Will be checked by TF2 for possible new amendment
DE 16	7.2.1	clause	ed	Due to the introduction of the CRC_32 for extended frames:	Move content of sub clause 7.2 to new sub clause 7.2.1	Rejected Will be checked by TF2 for possible new amendment

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted **Please enter your name here**
DE 17	7.2	title	ed	Due to the introduction of the CRC_32 introduce new clause title	Change title of Clause 7.2 to: " 7.2. CRC Coding "	Rejected Will be checked by TF2 for possible new amendment
DE 18	7.2.2	New clause	TE	See comments for 6.2.4.2	Add new sub clause: " 7.2.2 CRC_32 As defined in 6.2.4.2 "	Rejected Will be checked by TF2 for possible new amendment
DE 19	Annex B	Title	ED	Due to CRC_32 change title:	New Title: "CRC_A, CRC_B an CRC_32 encoding"	Rejected Will be checked by TF2 for possible new amendment
DE 20	Annex B4	Clause	ED	Due to CRC_32 introduction. Shift Clause Annex B3 to Annex B4		Rejected Will be checked by TF2 for possible new amendment
DE 21	Annex B3	Clause	TE	CRC_32 encoding example in C language for explanatory purpose	New Clause: "Annex B.3 CRC_32 encoding This Annex is provided for explanatory purposes and indicates the bit patterns that will exist in the physical layer. It is included for the	Rejected Will be checked by TF2 for possible new amendment

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted **Please enter your name here**
					purpose of checking an ISO/IEC 14443-3 implementation of CRC_32 encoding. The CRC_32 uses polynomial = 0x04c11db7 with, initial Value = 'FFFFFFFF' and reflected bit order (LSB first). The final CRC value is inverted before transmission. Refer to ISO/IEC 13239 for further details. **Example** Transmission of first byte = '12', second byte = '34', third byte = '56', fourth byte = '78', CRC_32 appended. Calculated CRC_32 = '4A090E98' (transmitted as '98', '0E', '09', '4A'). "	
DE 22	Annex B4	clause	Te	Replace C language code for CRC Type A and Type calculation by a C language additionally calculating CRC_32. See Annex A.2 below. (parts in red are new for CRC_32 calculation)	See Annex 3 below	Rejected Will be checked by TF2 for possible new amendment

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

Annex 1:

Divisor D	etu	Bit rate		
		1 bit / etu	2 bits / etu	3 bits / etu
1	**128 / *fc* (~ 9,4 µs)**	***fc* / 128 (~ 106 kbit/s)**		
2 (optional)	**128 / (2 *fc*) (~ 4,7 µs)**	***fc* / 64 (~ 212 kbit/s)**		
4 (optional)	**128 / (4 *fc* (~ 2,4 µs)**	***fc* / 32 (~ 424 kbit/s)**		
8 (optional)	**128 / (8 *fc*) (~ 1,2 µs)**	***fc* / 16 (~ 848 kbit/s)**		
16 (optional)	**128 / (16 *fc*) (~ 0,6 µs)**	***fc* / 8 (~ 1,7 Mbit/s)**		
32 (optional)	**128 / (32 *fc*) (~0,3 µs)**	***fc* / 4 (~ 3,39 Mbit/s)**		***fc* / 4/3 (~ 10,17 Mbit/s)**
64 (optional)	**128 / (64 *fc*) (~0,15 µs)**	***fc* / 2 (~ 6,78 Mbit/s)**	***fc* (~ 13,56 Mbit/s)**	

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted **Please enter your name here**

Annex 2:

"

6.2.3.4 Extended frames

Format

Extended frames are used for data exchange data and consist of, in the following order

— Start of Communication (SOC)

— Data bytes (= *n* * 8 data bits), where the first 2 bytes shall contain the length (in bytes) of all data bytes. The data bytes are encoded using Hamming(63,57) blocks as follows:

  — the first group of 57 data bits (bits 1..57) are encoded in the first Hamming block of 63 bits.

  — the second group of 57 data bits (bits 58..114) is encoded in the second Hamming block of 63 bits.

  — the third group of 57 data bits (bits 115..171) is encoded in the third Hamming block of 63 bits.

  — ...

The last Hamming block may be incomplete, i.e. it may contain less than 57 data bits. So, the total number of Hamming blocks is ceil((n × 8) / 57).

NOTE The first Hamming block shall always be a complete Hamming block. Zero-Padding shall be used to achieve a complete Hamming block.

NOTE The data is transmitted as a sequence of symbols. Depending on the selected transmission scheme a symbols can contain more than 1 bit.

Hamming Code

The Hamming Block Structure is defined as follows:

Each (complete) Hamming block consists of 57 data bits ($d_1..d_{57}$) and 6 parity bits ($p_1..p_6$). So, the length of each (complete) Hamming block is 63 bits.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted **Please enter your name here**

Let b_i denote the bit in the Hamming block at position i (i = 1..63). Furthermore, let $j = \log_2(i)$ and $k = \text{floor}(\log_2(i))$. Bit b_i then represents:

— parity bit p_{k+1} if j = k

— data bit $d_{i-(k+1)}$ if j ≠ k

The structure of a Hamming (63,57) block is illustrated in Figure AA:

Bit position	1	2	3	4	5	6	7	8	9	10	…	14	15	16	17	18	…	30	31	32	33	34	…	62	63
Encoded bit	p_1	p_2	d_1	p_3	d_2	d_3	d_4	p_4	d_5	d_6	…	d_{10}	d_{11}	p_5	d_{12}	d_{13}	…	d_{25}	d_{26}	p_6	d_{27}	d_{28}	…	d_{56}	d_{57}

Figure AA -- structure of a Hamming(63,57) block.

Calculation of the parity bits

Parity bit p_x (x = 1..6) is calculated over the bits in the bit set $\{b_y \mid y \neq 2^{(x-1)}$ and $(y \,\&\, 2^{(x-1)}) \neq 0\}$ with y = 1..63. (Note that & is the bitwise AND operator.)

-- if the number of bits with value 1 in the bit set is even, the parity bit has value 0

-- if the number of bits with value 1 in the bit set is odd, the parity bit has value 1

In other words: the value of parity bit p_x (x = 1..6) is such that the number of bits with value 1 in the bit set $\{b_y \mid (y \,\&\, 2^{(x-1)}) \neq 0\}$ with y = 1..63 -- which includes parity bit p_x itself -- is even.

Error correction

One single-bit error can be corrected per Hamming block. The position of the bit error (the *error syndrome*) can be calculated by taking the binary XOR of all bit positions for which the received bit has value 1. If the result of the calculation is 0, the Hamming block does not contain a single-bit error. Otherwise, the result indicates the position of the bit in error and the error can be fixed by inverting that bit.

Incomplete Hamming block

As mentioned, the last Hamming block may be incomplete, i.e. it may contain less than 57 data bits. In that case, the Hamming block is simply truncated after the last data bit. For example, assume that only 13 data bits ($d_1..d_{13}$) are encoded in the last Hamming block. Then, this block will be truncated after bit d_{13} at position 18 (see figure AA). Note: for the calculation of the parity bits, one can simply assume here that $b_y = 0$ for $y > 18$.

Padding with zero-bits

If symbols are coded with N bits, where N is larger than 1, then the following rules shall be applied.

The data, consisting of *n* Bytes that are encoded using *m* Hamming(63,57) blocks, is padded with 0-bits as follows:

-- 4PSK modulation: up to 1 bit is appended to the data, such that the total number of bits is an integer multiple of 2.

-- 8PSK modulation: up to 2 bits are appended to the data, such that the total number of bits is an integer multiple of 3.

-- 16PSK modulation: up to 3 bits are appended to the data, such that the total number of bits is an integer multiple of 4.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted **Please enter your name here**

NOTE These bits can easily be removed again after transmission, since in all cases less than 8 bits (i.e. less than a complete Byte) are appended.

"

Annex 3:

"

Annex B4: Code sample written in C language for CRC calculation

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <ctype.h>

#define CRC_A 1
#define CRC_B 2
#define BYTE unsigned char

unsigned int ComputeCrc32(unsigned char *Data, unsigned int Length, unsigned int init, unsigned int xor) {

 unsigned int c;
 unsigned char d, e, f;

 unsigned int i;

 // init
 c = init;
 // compute CRC
 for (i = 0; i < Length; i++) {
          d = Data[i];

          e = c ^ d;
          f = e ^ (e << 6);
          c = (c >>  8) ^ (f << 24) ^ (f << 23) ^ (f << 22) ^
              (f << 20) ^ (f << 19) ^ (f << 17) ^ (f << 16) ^
              (f << 14) ^ (f << 13) ^ (f << 12) ^ (f << 8) ^
              (f <<  2) ^ (f <<  1) ^ (f >>  2);
```

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted **Please enter your name here**

```
  }
  // final xor
  c = c ^ xor;
  return c;
}

unsigned short UpdateCrc(unsigned char ch, unsigned short *lpwCrc)
{
  ch = (ch^(unsigned char)((*lpwCrc) & 0x00FF));

  ch = (ch^(ch<<4));

  *lpwCrc = (*lpwCrc >> 8)^((unsigned short)ch << 8)^((unsigned short)ch<<3)^((unsigned short)ch>>4);

  return(*lpwCrc);
}

void ComputeCrc(int CRCType, char *Data, int Length,
  BYTE *TransmitFirst, BYTE *TransmitSecond)
{
  unsigned char chBlock;
  unsigned short wCrc;

  switch(CRCType) {
          case CRC_A:
                  wCrc = 0x6363; /* ITU-V.41 */
                  break;
          case CRC_B:
                  wCrc = 0xFFFF; /* ISO/IEC 13239 (formerly ISO/IEC 3309) */
                  break;
          default:
                  return;
  }

  do {
          chBlock = *Data++;
          UpdateCrc(chBlock, &wCrc);
  } while (--Length);
  if (CRCType == CRC_B)
          wCrc = ~wCrc; /* ISO/IEC 13239 (formerly ISO/IEC 3309) */

  *TransmitFirst = (BYTE) (wCrc & 0xFF);
```

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted **Please enter your name here**

```
  *TransmitSecond = (BYTE) ((wCrc >> 8) & 0xFF);

  return;
}

BYTE BuffCRC_A[10] = {0x12, 0x34};
BYTE BuffCRC_B[10] = {0x0A, 0x12, 0x34, 0x56};
BYTE BuffCRC_32[10] = {0x12, 0x34, 0x56, 0x78};
unsigned int Crc32;
BYTE First, Second;
FILE *OutFd;
int i;

int main(void)
{
  printf("CRC-16 reference results ISO/IEC 14443-3\n");
  printf("Crc-16 G(x) = x^16 + x^12 + x^5 + 1\n\n");
  printf("CRC_A of [ ");
  for(i=0; i<2; i++) printf("%02X ",BuffCRC_A[i]);
  ComputeCrc(CRC_A, BuffCRC_A, 2, &First, &Second);
  printf("] Transmitted: %02X then %02X.\n", First, Second);
  printf("CRC_B of [ ");
  for(i=0; i<4; i++) printf("%02X ",BuffCRC_B[i]);
  ComputeCrc(CRC_B, BuffCRC_B, 4, &First, &Second);
  printf("] Transmitted: %02X then %02X.\n", First, Second);
  printf("\n");
  printf("CRC-32 reference results ISO/IEC 14443-3\n");
  printf("Crc-32 G(x) = x^32 + x^26 + x^23 + x^22 + x^16 + x^12 + x^11 + x^10 + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1\n\n");
  printf("CRC_32 of [ ");
  for(i=0; i<4; i++) printf("%02X ",BuffCRC_32[i]);
  Crc32 = ComputeCrc32(BuffCRC_32, 4, 0xFFFFFFFF, 0xFFFFFFFF);
  printf("] Transmitted: %02X then %02X then %02X then %02X.\n", (Crc32 & 0xFF), ((Crc32 >> 8) & 0xFF), ((Crc32 >> 16) & 0xFF), ((Crc32 >> 24) & 
0xFF));

  return(0);
}
```

"

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

Template for comments and secretariat observations

Date: 2011-03-15	Document: JTC1/SC17N4098 ISO/IEC 14443-3(2010)/PDAM 2

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
JP1	Whole documents		GE	JNB's (Japan National Body) stances for VHBR are shown in the following. JNB's comments on JTC 1/SC 17 N3925 JNB supports the rational of VHBR (Very High Bit Rate). JNB's positioning and requirements for this project are as follows. (1) Single method - JNB requires that SC 17 should adopt single method for this newly developed VHBR before going to PDAM ballot in order to improve interoperability and to avoid possible market confusion. - Though several methods for VHBR have been contributed in the previous SC 17/WG 8 Meetings, JNB does not support the idea of specifying two or more methods for VHBR. This is because JNB cannot see the purpose, the necessity, the market needs or the users' merits for specifying two or more methods. (2) Backward compatibility with ISO/IEC 14443 series - JNB supports the positioning of VHBR (amendments to ISO/IEC 14443 series, according to the Resolutions 47.02 and 47.03 of Summary Report of the 47th meeting of ISO/IEC JTC 1/SC 17/WG 8). *47.02 NP for Very High Bit Rate* *WG8 instructs its Secretariat to forward the NP for Very High Bit Rate, as laid down in N 1683, to the SC 17 Secretariat for NP balloting process.* *47.03 Project Editor for Very High Bit Rate* *WG 8 appoints Messr. Caruana, Meindl and Raggam, the Project Editors for the amendments to 14443-x and*	Make the standards which are satisfied all following requests (1) to (4).	Resolved resolved

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
				10373-6 regarding Very High Bit Rate. - JNB requires that the bit rates for VHBR should be OPTIONAL as higher bit rates (212k, 424k and 848 kbps) are optional in ISO/IEC 14443-3:2010. (3) Higher layer compatibility - JNB is of the opinion that application based on ISO/IEC 7816 series shall not be excluded even when using VHBR protocol because ISO/IEC 7816-4 (Organization, security and commands for interchange) is one of the normative references for ISO/IEC14443-4. (4) Parameter confirmation "after" the development of test method - JNB requires that the each parameter for VHBR should be fixed after the test method		Resolved by explanation Any APDU of 7816 can also be transmitted by VHBR Postponed and To be checked in TF2 meeting JP1 Resolved in general by discussion at WG8 meeting
JP2	Whole documents		TE	ISO/IEC 14443-3/Amd.2 is related closely with (ISO/IEC14443-2/Amd.1, ISO/IEC 14443-4/Amd.2 and ISO/IEC 10373-6/Amd.x) However, there are many lots of problems in ISO/IEC14443-2/Amd.1 and that technical contents are fixed is premature (see the ballot comments of ISO/IEC14443-2/Amd.1). If proceeding with the other part as it left an un- reviewed part, it is a fear to bring mismatch among the parts. Also, for test methods not to be established, there is not a means of confirming the validity and the reproducibility of the proposal contents in every national bodies.	Synchronize discussion with other parts of 14443 (include test methods).	JP2 Resolved in general by decision at WG8 meeting and test method to be checked in TF2 meeting Resolution 49.03

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

Template for comments and secretariat observations

Date: 2011-03-15	Document: JTC1/SC17N4098 ISO/IEC 14443-3(2010)/PDAM 2

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
JP3	Whole documents		TE	The close inspection whether or not which uses S(PARAMETER) is insufficient. It depend on about whether or not to set bit durations in the ATTRIB command that it can do the squeezing of the parameter of RF in Part 2.	Judge the validity of the revision of Part 3.After deciding the whole mechanism of switching to VHBR.	Resolved by Adding a note: In 7.9.4.6

JP3
Activation of High bit rates
Type A: 106 -> PPS -> 212,424,848
S(Param)

Type B 106 -> ATTRIB -> 212,424,848
S(Param)

Activation of very High bit rates
Type A: 106 -> S(Param) -> 1,7 … 13,56

Type B 106 -> S(Param) -> 1,7 … 13,56

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

[BE] comments on ISO/IEC 14443-3:2010/PDAM 2

Date: 2011-03-23	Document: **SC 17 N4098**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
[BE] 1			Te	BE requires 2 RF methods for modulation of VHBR which is in-line with current CDs. In terms of different FCC regulations which will become a critical obstacle for VHBR deployment and in terms of even higher speed PSK is regarded as more promising method whereas ASK will allow fast deployment of prototype systems.		Resolved
[BE] 2						
[BE] 3						
[BE] 4						
[BE] 5						
[BE] 6						
[BE] 7						
[BE] 8						
[BE] 9						
[BE] 10						
[BE] 11						
[BE] 12						
[BE] 13						
[BE] 14						
[BE] 15						
[BE] 16						
[BE] 17						

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

ISO electronic balloting commenting template/version 2001-10

[BE] comments on ISO/IEC 14443-3:2010/PDAM 2

Date: 2011-03-23	Document: **SC 17 N4098**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com- ment**[2]	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
[BE] 18						
[BE] 19						
[BE] 20						
[BE] 21						
[BE] 22						
[BE] 23						
[BE] 24						

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
NL1	3.5	paragraph	ed	Update frame definition to match new definitions of VHBR	Replace frame definition by: " **frame** a frame is a sequence of data bits and optional error detection bits, with prefix sequence at start and a closing sequence at the end. "	Rejected Will be checked by TF2 for possible new amendment
NL2	6.2.3	clause	ed	Additionally list extended frame	Add another bullet at the end with: " - Extended frames "	Rejected Will be checked by TF2 for possible new amendment
NL3	6.2.3.4	Clause	Te	Add a section introducing an extended frame format reflecting the challenges of VHBR and frame lengths up to 4kByte. The introduction of the extended frame format increases robustness in communication as the hamming code can detect and correct a single bit error within a hamming block.	See Annex 1	Rejected Will be checked by TF2 for possible new amendment
NL4	6.2.3.2	Paragraph	ED	Describe Zero padding of PSK symbols for standard frames in order to have an integer number of symbols .	Add after Figure 3 "<u>Padding with zero-bits</u> If symbols are coded with N bits, where N is larger than 1, then the following rules shall be applied. -- 4PSK modulation: up to 1 bit is appended to the data, such that the total number of bits is an integer multiple of 2.	Rejected Will be checked by TF2 for possible new amendment

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
					-- 8PSK modulation: up to 2 bits are appended to the data, such that the total number of bits is an integer multiple of 3. -- 16PSK modulation: up to 3 bits are Rejected Will be checked by TF2 for possible new amendment appended to the data, such that the total number of bits is an integer" multiple of 4. "	
NL5	6.2.4	title	ED	Due to the introduction of the extended frame change chapter structure of CRC	Change Clause title to: " 6.2.4 CRC Coding "	Rejected Will be checked by TF2 for possible new amendment
NL6	6.2.4.1	paragraph	ED		Move CRC_A section to subclause 6.2.4.1: " 6.2.4.1 CRC_A "	Rejected Will be checked by TF2 for possible new amendment
NL7	6.2.4.2	Paragraph/ Clause	Te	Introducing CRC_32 for extended frames. The probability of an undetected error for frame lengths exceeding 256Bytes is in the range of a BER of 10^-5. This means we cannot be sure if we do not encounter an error or if the CRC16 is not detecting this error. Therefore, CRC_32 is introduced for	ADD new subclause : "6.2.4.2 CRC_32 A frame that includes CRC_32 shall only be considered correct if it is received with a valid CRC_32 value.	Rejected Will be checked by TF2 for possible new amendment

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
				extended frames.	The frame CRC_32 is a function of k data bits, which consist of all the data bits in the frame, excluding parity bits, SOC and EOC, and the CRC_32 itself. For error checking, the four CRC_32 bytes are sent in the extended frame after the data bytes. The CRC_32 is as defined in ISO/IEC 13239. The initial register content shall be '0xffffffff' and the register content shall be inverted after calculation. For examples refer to Annex B."	
NL8	7.1.3.1	title	ed	Shift Clause of 7.1.3 to subclause 7.1.3.1 and rename title	New title of subclause: " Standard Frame "	Rejected Will be checked by TF2 for possible new amendment
NL9	7.1.3	title	ed	Due to the introduction of extended frames change title	Change Title: " Frame Format "	Rejected Will be checked by TF2 for possible new amendment
NL10	7.1.3.2	clause	TE	Add new clause for extended frames	Add subclause " 7.1.3.2 Extended frame	Rejected Will be checked by TF2 for possible new amendment

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment: ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com- ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
					See 6.2.3.5 ”	
NL11	7.2.1	clause	ed	Due to the introduction of the CRC_32 for extended frames : Shift Clause of 7.2. to subclause 7.2.1		Rejected Will be checked by TF2 for possible new amendment
NL12	7.2	title	ed	Due to the introduction of the CRC_32 introduce new clause title	Add title: “ 7.2. CRC Coding “	Rejected Will be checked by TF2 for possible new amendment
NL13	7.2.2	New clause	TE	See comments for 6.2.4.2	Add new clause: “ CRC_32 As defined in 6.2.4.2 “	Rejected Will be checked by TF2 for possible new amendment
NL14	Annex B	Title	ED	Due to CRC_32 change title:	New Title: “CRC_A, CRC_B an CRC_32 encoding”	Rejected Will be checked by TF2 for possible new amendment
NL15	Annex B4	Clause	ED	Due to CRC_32 introduction. Shift Clause Annex B3 to Annex B4		Rejected Will be checked by TF2 for possible new amendment
NL16	Annex B3	Clause	TE	CRC_32 encoding example in C language for explanatory purpose	New Clause: “Annex B.3 CRC_32 encoding This Annex is provided for explanatory purposes and indicates the bit patterns that will exist in the	Rejected Will be checked by TF2 for possible new amendment

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
					physical layer. It is included for the purpose of checking an ISO/IEC 14443-3 implementation of CRC_32 encoding. The CRC_32 uses polynomial = 0x04c11db7 with, initial Value = 'FFFFFFFF' and reflected bit order (LSB first). The final CRC value is inverted before transmission. Refer to ISO/IEC 13239 for further details. **Example** Transmission of first byte = '12', second byte = '34', third byte = '56', fourth byte = ‘78’, CRC_32 appended. Calculated CRC_32 = '4A090E98’ (transmitted as ‘98’, ‘0E’, ‘09’, ‘4A’). “	
NL17	Annex B4	clause	Te	Replace C language code for CRC Type A and Type calculation by a C language additionally calculating CRC_32. See Annex A.2 below. (parts in red are new for CRC_32 calculation)	See Annex 2 below	Rejected Will be checked by TF2 for possible new amendment

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

Annex 1:

“

6.2.3.4 Extended frames

Format

Extended frames are used for data exchange data and consist of, in the following order

— Start of Communication (SOC)

— Data bytes (= *n* * 8 data bits), where the first 2 bytes shall contain the length (in bytes) of all data bytes. The data bytes are encoded using Hamming(63,57) blocks as follows:

  — the first group of 57 data bits (bits 1..57) are encoded in the first Hamming block of 63 bits.

  — the second group of 57 data bits (bits 58..114) is encoded in the second Hamming block of 63 bits.

  — the third group of 57 data bits (bits 115..171) is encoded in the third Hamming block of 63 bits.

  — ...

The last Hamming block may be incomplete, i.e. it may contain less than 57 data bits. So, the total number of Hamming blocks is ceil((n × 8) / 57).

NOTE The data is transmitted as a sequence of symbols. Depending on the selected transmission scheme a symbols can contain more than 1 bit.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

Hamming Code

The Hamming Block Structure is defined as follows:

Each (complete) Hamming block consists of 57 data bits ($d_1..d_{57}$) and 6 parity bits ($p_1..p_6$). So, the length of each (complete) Hamming block is 63 bits. Let b_i denote the bit in the Hamming block at position i (i = 1..63). Furthermore, let $j = \log_2(i)$ and $k = \text{floor}(\log_2(i))$. Bit b_i then represents:

— parity bit p_{k+1} if j = k

— data bit $d_{i-(k+1)}$ if j ≠ k

The structure of a Hamming (63,57) block is illustrated in Figure AA:

Bit position	1	2	3	4	5	6	7	8	9	10	…	14	15	16	17	18	…	30	31	32	33	34	…	62	63
Encoded bit	p_1	p_2	d_1	p_3	d_2	d_3	d_4	p_4	d_5	d_6	…	d_{10}	d_{11}	p_5	d_{12}	d_{13}	…	d_{25}	d_{26}	p_6	d_{27}	d_{28}	…	d_{56}	d_{57}

Figure AA -- structure of a Hamming(63,57) block.

Calculation of the parity bits

Parity bit p_x (x = 1..6) is calculated over the bits in the bit set $\{b_y \mid y \neq 2^{(x-1)}$ and $(y \,\&\, 2^{(x-1)}) \neq 0\}$ with y = 1..63. (Note that & is the bitwise AND operator.)

-- if the number of bits with value 1 in the bit set is even, the parity bit has value 0

-- if the number of bits with value 1 in the bit set is odd, the parity bit has value 1

In other words: the value of parity bit p_x (x = 1..6) is such that the number of bits with value 1 in the bit set $\{b_y \mid (y \,\&\, 2^{(x-1)}) \neq 0\}$ with y = 1..63 -- which includes parity bit p_x itself -- is even.

Error correction

One single-bit error can be corrected per Hamming block. The position of the bit error (the *error syndrome*) can be calculated by taking the binary XOR of all bit positions for which the received bit has value 1. If the result of the calculation is 0, the Hamming block does not contain a single-bit error. Otherwise, the result indicates the position of the bit in error and the error can be fixed by inverting that bit.

Incomplete Hamming block

As mentioned, the last Hamming block may be incomplete, i.e. it may contain less than 57 data bits. In that case, the Hamming block is simply truncated after the last data bit. For example, assume that only 13 data bits ($d_1..d_{13}$) are encoded in the last Hamming block. Then, this block will be truncated after bit d_{13} at position 18 (see figure AA). Note: for the calculation of the parity bits, one can simply assume here that $b_y = 0$ for $y > 18$.

Padding with zero-bits

If symbols are coded with N bits, where N is larger than 1, then the following rules shall be applied.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

The data, consisting of *n* Bytes that are encoded using *m* Hamming(63,57) blocks, is padded with 0-bits as follows:
-- 4PSK modulation: up to 1 bit is appended to the data, such that the total number of bits is an integer multiple of 2.
-- 8PSK modulation: up to 2 bits are appended to the data, such that the total number of bits is an integer multiple of 3.
-- 16PSK modulation: up to 3 bits are appended to the data, such that the total number of bits is an integer multiple of 4.

NOTE These bits can easily be removed again after transmission, since in all cases less than 8 bits (i.e. less than a complete Byte) are appended.

"

Annex 2:

"

Annex B4: Code sample written in C language for CRC calculation

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <ctype.h>

#define CRC_A 1
#define CRC_B 2
#define BYTE unsigned char

unsigned int ComputeCrc32(unsigned char *Data, unsigned int Length, unsigned int init, unsigned int xor) {

 unsigned int c;
 unsigned char d, e, f;

 unsigned int i;

 // init
 c = init;
 // compute CRC
 for (i = 0; i < Length; i++) {
         d = Data[i];

         e = c ^ d;
         f = e ^ (e << 6);
```

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

```
          c = (c >>  8) ^ (f << 24) ^ (f << 23) ^ (f << 22) ^
              (f << 20) ^ (f << 19) ^ (f << 17) ^ (f << 16) ^
              (f << 14) ^ (f << 13) ^ (f << 12) ^ (f << 8) ^
              (f <<  2) ^ (f <<  1) ^ (f >>  2);
 }
 // final xor
 c = c ^ xor;
 return c;
}

unsigned short UpdateCrc(unsigned char ch, unsigned short *lpwCrc)
{
 ch = (ch^(unsigned char)((*lpwCrc) & 0x00FF));

 ch = (ch^(ch<<4));

 *lpwCrc = (*lpwCrc >> 8)^((unsigned short)ch << 8)^((unsigned short)ch<<3)^((unsigned short)ch>>4);

 return(*lpwCrc);
}

void ComputeCrc(int CRCType, char *Data, int Length,
 BYTE *TransmitFirst, BYTE *TransmitSecond)
{
 unsigned char chBlock;
 unsigned short wCrc;

 switch(CRCType) {
         case CRC_A:
                 wCrc = 0x6363; /* ITU-V.41 */
                 break;
         case CRC_B:
                 wCrc = 0xFFFF; /* ISO/IEC 13239 (formerly ISO/IEC 3309) */
                 break;
         default:
                 return;
 }

 do {
         chBlock = *Data++;
         UpdateCrc(chBlock, &wCrc);
 } while (--Length);
 if (CRCType == CRC_B)
```

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted

```
            wCrc = ~wCrc; /* ISO/IEC 13239 (formerly ISO/IEC 3309) */

     *TransmitFirst = (BYTE) (wCrc & 0xFF);
     *TransmitSecond = (BYTE) ((wCrc >> 8) & 0xFF);

     return;
    }

    BYTE BuffCRC_A[10] = {0x12, 0x34};
    BYTE BuffCRC_B[10] = {0x0A, 0x12, 0x34, 0x56};
    BYTE BuffCRC_32[10] = {0x12, 0x34, 0x56, 0x78};
    unsigned int Crc32;
    BYTE First, Second;
    FILE *OutFd;
    int i;

    int main(void)
    {
     printf("CRC-16 reference results ISO/IEC 14443-3\n");
     printf("Crc-16 G(x) = x^16 + x^12 + x^5 + 1\n\n");
     printf("CRC_A of [ ");
     for(i=0; i<2; i++) printf("%02X ",BuffCRC_A[i]);
     ComputeCrc(CRC_A, BuffCRC_A, 2, &First, &Second);
     printf("] Transmitted: %02X then %02X.\n", First, Second);
     printf("CRC_B of [ ");
     for(i=0; i<4; i++) printf("%02X ",BuffCRC_B[i]);
     ComputeCrc(CRC_B, BuffCRC_B, 4, &First, &Second);
     printf("] Transmitted: %02X then %02X.\n", First, Second);
     printf("\n");
     printf("CRC-32 reference results ISO/IEC 14443-3\n");
     printf("Crc-32 G(x) = x^32 + x^26 + x^23 + x^22 + x^16 + x^12 + x^11 + x^10 + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1\n\n");
     printf("CRC_32 of [ ");
     for(i=0; i<4; i++) printf("%02X ",BuffCRC_32[i]);
     Crc32 = ComputeCrc32(BuffCRC_32, 4, 0xFFFFFFFF, 0xFFFFFFFF);
     printf("] Transmitted: %02X then %02X then %02X then %02X.\n", (Crc32 & 0xFF), ((Crc32 >> 8) & 0xFF), ((Crc32 >> 16) & 0xFF), ((Crc32 >> 24) &
    0xFF));

     return(0);
}
```

"

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.