GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.220.01

L 64

GB/T 29768-2013

Information technology - Radio frequency identification - Air interface protocol at 800/900 MHz

信息技术 射频识别 800/900 MHz 空中接口协议

Issued on: September 18, 2013 **Implemented on: May 01, 2014**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine;

Standardization Administration of PRC.

Table of Contents

Information technology - Radio frequency identification - Air interface protocol at 800/900 MHz

1 Scope

This standard specifies the physical layer and media access control layer parameters and protocol working methods of the air interface in 840 MHz ~ 845 MHz and 920 MHz ~ 925 MHz radio frequency identification system.

This standard applies to the design, production, testing, use of tags and readers for radio frequency identification systems in the frequency bands of 840 MHz ~ 845 MHz and 920 MHz ~ 925 MHz.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB/T 29261.3-2012 Information technology - Automatic identification and data capture (AIDC) techniques - Vocabulary - Part 3: Radio-frequency identification

3 Terms and definitions

The terms and definitions as defined in GB/T 29261.3-2012 as well as the following terms and definitions apply to this document.

3.1

Response data pack

The data as sent by the tag in the specified format to the reader according to the reader command.

4 Symbols and abbreviations

The following symbols and abbreviations apply to this document.

TR_{ext} - Indication of leading signal;

$XXXX_b$ - Binary data identification;

$XXXX_h$ - Hexadecimal data identification;

|| - Tandem.

4.2 Abbreviations

AK - Authentication key;

ASK - Amplitude shift keying;

BLF - Backscatter link frequency;

CRC - Cyclic redundancy check;

DDS-BT - Dynamic disperse shrink binary tree;

DSB-ASK - Double-sideband amplitude shift keying;

FHSS - Frequency-hopping spread spectrum;

FT - Frequency tolerance;

LSB - Least significant bit;

MSB - Most significant bit;

PSK - Phase shift keying;

PW - Pulse width;

RDP - Response data pack;

RK - Root key;

SK - Session key;

SSB-ASK - Single-sideband amplitude shift keying;

TID - Tag identifier;

TPP - Truncated pulse position encoding.

c) The maximum value of T_2 only applies to tags in the reply state and acknowledged state. If T_2 reaches its maximum value, the tag shall jump to the arbitrate state. The maximum range of the tag's judgment of T_2 timeout shall be 20 T_{pri} ~ 32 T_{pri}.

d) FT is the frequency tolerance as specified in Table 4.

e) $T_1 + T_3$ shall not be less than T_4.

6 Working method of protocol

6.1 Anti-collision mechanism

Multi-tag anti-collision uses the DDS-BT mechanism, as shown in Figure 15. In this mechanism, the initial value of the tag time slot counter is set to 0. The time slot counter is gradually adjusted according to subsequent commands. When the time slot counter is 0, the tag jumps from the Arbitrate state to the reply state and starts to respond to the reader:

a) When the tag has no response:

1) When the reader cannot receive the tag response, it first judges whether to end the checking. If the criterion is true, the checking is considered to be completed. Refer to Appendix A for the judgment method;

2) If it does not end the checking, it needs to determine whether the number of consecutive idle time slots reaches CIN (continuous idle threshold, typical value is 4). If the number of consecutive idle time slots is not less than CIN, then the shrink command is sent; the tag time slot counter values of all arbitrate state and reply state are divided by 2 and rounded;

3) If the number of consecutive free time slots is less than CIN, meanwhile the previous time slot reader sends a divide command, the reader sends a divide command with the divide position "1", meanwhile all tags with a slot counter value of 1 are divide;

4) If the number of consecutive idle time slots is less than CIN, meanwhile the previous time slot reader sends a divide command, the reader will send a repeat query command, meanwhile the tag time slot counter value of all arbitrate state and reply state is reduced by 1.

b) When the tag responds correctly:

Tags that support security authentication leave the factory with a security mode of 01_b; tags that do not support security authentication leave the factory with a security mode of 00_b, which cannot be changed. When security authentication is not required, the security mode shall be kept as 01_b; when security authentication is required but no secure communication is required, write the security mode as 10_b; when security authentication is required and secure communication is required, write the security mode as 11_b. If the tag does not require security authentication, then secure communication is not required.

b) Security function: It is used to indicate the security function supported by the tag, which is defined as follows:

1) 82_h: XOR one-way authentication of the tag to the reader, 0_b means not supported, 1_b means supported;

2) 83_h: Symmetric encryption one-way authentication of the tag to the reader, 0_b means not supported, 1_b means supported;

3) 84_h: XOR one-way authentication of the tag by the reader, 0_b means not supported, 1_b means supported;

4) 85_h: Symmetric encryption one-way authentication of the tag by the reader, 0_b means not supported, 1_b means supported;

5) 86_h: XOR two-way authentication, 0_b means not supported, 1_b means supported;

6) 87_h: Symmetric encryption two-way authentication, 0_b means not supported, 1_b means supported;

7) 88_h: Secure communication, 0_b means not supported, 1_b means supported.

c) Encryption algorithm: It indicates the encryption algorithm used, 0_h represents encryption algorithm 1, 1_h represents encryption algorithm 2, and so on. The cryptographic algorithms and random numbers involved in this standard shall follow the relevant national provisions on commercial cryptography.

d) Key length: The length of the authentication key, in words.

e) T_{sec}: After the reader sends an authentication command, a one-way authentication command, a two-way authentication command or a secure communication command, the reference time for waiting for the tag response, with a unit of 10 ms.

The tag shall maintain a separate checking flag for each session. The checking flag for 4 sessions can be 0_b or 1_b. At the beginning of each checking cycle, the reader chooses to count the tags with the 0_b or 1_b value checking flag under one of the four sessions. The tags that are participating in the checking cycle of a certain session can no longer be used or modified for other sessions. The checking flag is the only resource provided by the tag to a given session independently, the other tag resources are shared by each session. After the tag is singularized, the reader can issue a command to make the tag a conversion checking flag for this session.

The checking flag retention time of the tag shall be as shown in Table 7. The checking flag when the tag is energized shall be set as follows:

a) The S0 checking flag shall be set to 0_b.

b) The S1 checking flag shall be set to 0_b or 1_b, depending on its stored value. If the retention time is exceeded after the tag setting takes effect, the tag shall set its S1 checking flag to 0_b when it is energized. Since the S1 checking flag is not automatically refreshed, it can be restored from 1_b to 0_b even when the tag is energized.

c) The S2 checking flag shall be set to 0_b or 1_b, depending on the value stored. If the tag's power-off time exceeds its retention time, the S2 checking flag when the tag is powered-on is automatically set to 0_b.

d) The S3 checking flag shall be set to 0_b or 1_b, depending on the value stored. If the tag power-off time exceeds its retention time, the S3 checking flag when the tag is powered-on is automatically set to 0_b.

When the initial state of the tag is any value, the tag will be set to 0_b or 1_b within a time less than or equal to 2 ms. The tag shall refresh its S2 and S3 checking flags when it is energized, which means that every time the tag is powered off, its S2 and S3 checking flags shall have a retention time as shown in Table 7. When a tag is participating in a certain checking cycle, the value of its S1 checking flag shall not be changed due to exceeding the retention time. In an checking cycle, if the S1 retention time is exceeded, the tag will modify the S1 checking flag to 0_b at the end of the checking cycle.

data field of $11XXXX_b$, if the length data field is not 0, the tag does not match. Tags that require security authentication do not respond to the sorting command with the storage area data field of $11XXXX_b$.

If the logical storage area is locked as unreadable, the tag does not respond to the sorting command.

For tags that support security authentication, the tag does not respond to the sorting command with the storage area data field of $11XXXX_b$.

c) Target: Instruct the tag to set a matching flag or checking flag.

d) Rules: Instruct the tag to set the matching flag or checking flag rules. The meaning of the four values is explained as follows:

1) 00_b: The matched tag will set the flag to 1_b; the unmatched tag will set the flag to 0_b;

2) 01_b: The flag of the matched tag remains unchanged; the flag of the unmatched tag is set to 0_b;

3) 10_b: The matched tag will set the flag to 1_b; the flag of the unmatched tag will remain unchanged;

4) 11_b: The matched tag will set the flag to 0_b; the unmatched tag will set the flag to 1_b.

e) Pointer: Point to the bit address of the logical storage area to start matching. If the pointer exceeds the logical storage area, the tag does not match.

f) Length: The bit length to be matched. If the length is 0 and the storage area data field is not 100000_b, the tag matches. If the matching length exceeds the logical storage area, the tag does not match.

g) Mask: The data that needs to be matched. If the length data field is an odd number, add a 0 to the lowest bit of the mask. When the tag receives a sorting command with an odd length data field, the lowest bit of the mask is ignored.

h) Check: CRC-16 calculation includes command code, storage area, target, rule, pointer, length and mask data field. See Appendix D for the calculation of CRC-16. If the check included in the command received by the tag is wrong, the tag does not respond to the command.

After the tag receives the sorting command, it changes the matching flag or checking flag according to the rules; it does not send a response data pack

1) 0_b: The checking flag is 0_b;

2) 1_b: The checking flag is 1_b.

e) TR_{ext}: Leading signal indication, the meaning of the two values is explained as follows:

1) 0_b: Backscatter-link preamble without preamble;

2) 1_b: The backscatter-link preamble has a preamble signal.

f) Backscatter-link rate factor: Determine BLF, as shown in Table 4.

g) Coding selection: Specifies the coding method of the backscatter-link; the meanings of the 4 values are explained as follows:

1) 00_b: FM0;

2) 01_b: Miller-coding, the subcarrier coefficient M is 2;

3) 10_b: Miller-coding, the subcarrier coefficient M is 4;

4) 11_b: Miller-coding, the subcarrier coefficient M is 8.

h) Check: CRC-16 calculation includes command code, condition, session, target, TR_{ext}, backscatter-link rate factor and code selection data field. See Appendix D for the calculation of CRC-16. If the check included in the command received by the tag is wrong, the tag does not respond to the command.

For tags in the ready state, arbitrate state, reply state, after receiving the start query command, if their matching flag meets the conditional data field requirements in the start query command, meanwhile the checking flag and the target data field in the start query command are equal, then set the time slot counter to 0, jump to the reply state, send a response data pack to the reader. The format of the response data pack is as shown in Table 11. If the tag in the ready state, arbitrate state, or reply state, if its matching flag does not meet the requirements of the conditional data field in the start query command, or its checking flag and the target data field are not equal, it will not respond to the start query command.

In the acknowledged state, authentication state, open state and security state, after receiving the start query command, if its matching flag meets the requirement of the conditional data field in the start query command, the flag is reversed. If the reversed checking flag is equal to the target data field in the start query command, set its time slot counter to 0, jump to the reply state, immediately send a response data pack to the reader. The format of the

sends a response data pack to the reader according to the format of Table 11. If the value of the changed time slot counter is not 0, the tag jumps to the arbitrate state and does not send response data packs to the reader;

3) 10_b: Reserved. If the divide location data field is 10_b, the tag does not respond to the divide command;

4) 11_b: Reserved. If the divide location data field is 11_b, the tag does not respond to the divide command.

c) Session: The session number where the checking cycle is located. If the session number of the tag that received the divide command is different from the session number that has started the cycle, the command will not be executed.

When the tags in the acknowledged state, authentication state, open state and security state receive the divide command, reverse the checking flag and jump to the ready state.

6.5.6 Disperse commands

The disperse command is used to disperse tags. The disperse command has no parameters. The frame format of the disperse command is as shown in Table 14.

Table 14 -- Frame format of disperse commands

Data field	Command code	Session
Length	4-bit	2-bit
Description	1000_b	00_b: S0 01_b: S1 10_b: S2 11_b: S3

The definition of each data field in the frame format is as follows:

a) Command code: 1000_b, disperse command's code;

b) Session: The session number where the checking cycle is located. If the session number of the tag that received the disperse command is different from the session number that has started the cycle, the command will not be executed.

The tag in the arbitrate state and the reply state, after receiving the disperse command, generates a random number, the value of the time slot counter is multiplied by 2 and the random number is added. If the value of the changed time slot counter is 0, the tag jumps to the reply state and sends a response

a) Command code: 10110110_b, the code of XOR identification command;

b) $SORN_t$: The reader calculates $SORN_t = RN_t' \oplus (AK' + O_n)$;

c) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

d) Check: CRC-16 calculation includes command code, $SORN_t$ and handle data fields. See Appendix D for the calculation of CRC-16. If the check included in the command received by the tag is wrong, the tag does not respond to the command.

6.5.12.2 Response data pack

After the tag in the authentication state receives the XOR authentication command, it compares whether the $SORN_t \oplus RN_r'$ and $AK' + O_n$ are equal. If they are equal, the tag considers that the reader has passed the authentication, sends a response data pack to the reader, jumps to the open state. If they are not equal, the tag considers that the reader has not passed the authentication, sends a response data pack to the reader, jumps to the arbitrate state. The format of the response data pack is as shown in Table 24.

Table 24 -- Response data pack format of XOR authentication command

Data field	Command code	Handle	Check
Length	8-bit	16-bit	16-bit
Description	Command operating state	handle	CRC-16

The definition of each data field in the response data pack is as follows:

a) Operating state: See Appendix E for the specific meaning of operating state;

b) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

c) Check: CRC-16 calculation includes operating state and handle data field. See Appendix D for the calculation of CRC-16.

6.5.13 One-way XOR authentication command

6.5.13.1 Command frame format

The one-way XOR authentication command is used to initiate the one-way authentication protocol flow based on the XOR operation of the reader to the tag. The frame format of the one-way XOR authentication command is as

shown in Table 25.

Table 25 -- Frame format of one-way XOR authentication command

Data field	Command code	SRN_t	Handle	Check
Length	8-bit	16-bit	16-bit	16-bit
Description	10110111_b		handle	CRC-16

The definition of each data field in the frame format is as follows:

a) Command code: 10110111_b, One-way XOR identification command code;

b) SRN_r: The reader generates the XOR value of the 16-bit random number RN_r and the authentication key AK, that is, $SRN_r = (RN_r + O_n) \oplus AK$;

c) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

d) Check: CRC-16 calculation includes command code, SRN_r, handle data fields. See Appendix D for the calculation of CRC-16. If the check included in the command received by the tag is wrong, the tag does not respond to the command.

6.5.13.2 Response data pack

After the tag receives the one-way XOR authentication command, it may need to send a response data pack to the reader according to the state it is in. The format of the response data pack is as shown in Table 26; meanwhile it jumps to the open state.

Table 26 -- Response data pack format of one-way XOR authentication command

Data field	$SORN_r$	Handle	Check
Length	16-bit	16-bit	16-bit
Description		handle	CRC-16

The definition of each data field in the response data pack is as follows:

a) $SORN_r$: Tag calculation $SORN_r = RN_r' \oplus (AK' + O_n)$, wherein RN_r' and AK' respectively represent the value of RN_r and AK after cyclic shifting to the left by n bits, the value of n is the number of the bits whose value is 1 in RN_r;

b) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

c) Check: CRC-16 calculation includes $SORN_r$ and handle data field. See Appendix D for the calculation of CRC-16.

The reader compares whether $SORN_r \oplus RN_r'$ is equal to $AK' + O_n$. If they are equal, the reader considers the tag to pass the authentication; if they are not equal, the reader considers the tag to fail the authentication.

6.5.14 Two-way XOR authentication command

6.5.14.1 Command frame format

The two-way XOR authentication command is used to initiate the two-way authentication protocol process based on the XOR operation. The frame format of the two-way XOR authentication command is as shown in Table 27.

Table 27 -- Frame format of two-way XOR authentication command

Data field	Command code	SRN_t	Handle	Check
Length	8-bit	16-bit	16-bit	16-bit
Description	10111000_b		handle	CRC-16

The definition of each data field in the frame format is as follows:

a) Command code: 10111000_b, the code of request XOR authentication command;

b) SRN_r: The reader generates a 16-bit random number RN_r, calculates the XOR value $SRN_r = (RN_r + O_n) \oplus AK$ of RN_r and the authentication key AK;

c) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

d) Check: CRC-16 calculation includes command code, SRN_r, handle data fields. See Appendix D for the calculation of CRC-16. If the check included in the command received by the tag is wrong, the tag does not respond to the command.

6.5.14.2 Response data pack

After the tag receives the two-way XOR authentication command, it may need to send a response data pack to the reader according to its state. The format of the response data pack is as shown in Table 28.

Table 28 -- Response data pack format of two-way XOR authentication command

Data field	$SORN_r$	SRN_t	Handle	Check
Length	16-bit	16-bit	16-bit	16-bit
Description			handle	CRC-16

The definition of each data field in the response data pack is as follows:

a) $SORN_r$: Tag calculates $RN_r = SRN_r \oplus AK - O_n$; calculates $SORN_r$: Tag calculates $SORN_r = RN_r' \oplus (AK' + O_n)$, wherein RN_r' and AK' respectively indicate that RN_r and AK are cyclically shifted to the left by n bits. The value of n is the number of bits with a value of 1 in RN_r;

b) SRN_t: The tag generates the XOR value of the 16-bit random number RN_t and the authentication key AK, that is, $SRN_t = (RN_t + O_n) \oplus AK$;

c) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

d) Check: CRC-16 calculation includes $SORN_r$, SRN_t, handle data fields. See Appendix D for the calculation of CRC-16.

The reader compares whether $SORN_r \oplus RN_r'$ and $AK' + O_n$ are equal. If they are equal, the reader considers the tag to pass the authentication; if they are not equal, the reader considers the tag to fail the authentication.

6.5.15 Request authentication command

6.5.15.1 Command frame format

The request authentication command is used to initiate the symmetric encryption authentication process of the tag to the reader. The frame format of the request authentication command is as shown in Table 29.

Table 29 -- Frame format of request authentication command

Data field	Command code	Handle	Check
Length	8-bit	16-bit	16-bit
Description	10100000_b	handle	CRC-16

The definition of each data field in the frame format is as follows:

a) Command code: 10100000_b, the code of request identification command;

b) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

a) Command code: 10110011_b, the code of authentication command;

b) Authentication data: including the encryption result of RN_t and the reader, that is, $RN_t \| E_{AK}(RN_t \| SK)$, see 6.6.2 for details. If the length of the encryption result generated by the reader is an odd number, add a bit of 0 to the lowest bit of the encryption result, that is, the authentication data is encrypted data after adding 0;

c) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

d) CRC-16: CRC-16 calculation includes command code, authentication data and handle data fields. See Appendix D for the calculation of CRC-16. If the check included in the command received by the tag is wrong, the tag does not respond to the command.

6.5.16.2 Response data pack

After the tag in the authentication state receives the authentication command, it first judges whether the received RN_t is equal to the RN_r it generated. If it is equal, use the authentication key AK to decrypt $E_{AK}(RN_t \| SK)$ to get $RN_t' \| SK$, compare RN_t' and RN_t; if equal, the tag considers that the reader has passed authentication, the session key is SK, sends a response data pack to the reader, jumps to the open state; if it is not equal, the tag considers that the reader has not passed authentication, sends a response data pack to the reader and jumps to the arbitrate state. The format of the response data pack is as shown in Table 32.

Table 32 -- Response data pack format of authentication command

Data field	Random number	Handle	Check
Length	8-bit	16-bit	16-bit
Description	Operating state of command	handle	CRC-16

The definition of each data field in the response data pack is as follows:

a) Operating state: See Appendix E for the specific meaning of operating state;

b) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

c) Check: CRC-16 calculation includes operation state and handle data field. See Appendix D for the calculation of CRC-16.

b) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

c) Check: CRC-16 calculation includes authentication data and handle data fields. See Appendix D for the calculation of CRC-16;

d) The reader first judges whether the received RN_r is equal to the RN_r generated by itself. If they are equal, use the authentication key AK to decrypt E_{AK} (RN_r ‖ SK) to get RN_r' ‖ SK, compare RN_r' and RN_r, if they are equal, then reader considers that the tag passes the authentication and the session key is SK; if it is not equal, the reader considers that the tag has not passed the authentication.

6.5.18 Two-way authentication command

6.5.18.1 Command frame format

The two-way authentication command is used to complete the symmetric encryption two-way authentication process of the reader and the tag. The frame format of the two-way authentication command is as shown in Table 35.

Table 35 -- Frame format of two-way authentication command

Data field	Command code	Authentication data	Handle	Check
Length	8-bit	Determined based on encryption algorithm	16-bit	16-bit
Description	10100001_b	The encryption result of the random number used for authentication and the session key, that is, RN_t ‖ E_{AK} (RN_r ‖ RN_t ‖ SK)	handle	CRC-16

The definition of each data field in the frame format is as follows:

a) Command code: 10100001_b, the code of the two-way authentication command;

b) Authentication data: Including the encryption result of RN_t and the reader, that is, RN_t ‖ E_{AK} (RN_r ‖ RN_t ‖ SK), see 6.6.4 for details. If the length of the encryption result generated by the reader is odd, add a bit of 0 to the lowest bit of the encryption result, that is, the authentication data is encrypted data after supplementing with 0;

c) Handle: the 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

d) Check: CRC-16 calculation includes command code, authentication data, handle data fields. See Appendix D for the calculation of CRC-16. If the check included in the command received by the tag is wrong, the tag does

The definition of each data field in the frame format is as follows:

a) Command code: 10101101_b, the code of the secure communication command;

b) Length: The bit length of the encrypted data;

c) Encrypted data: Encrypted command data, see 6.7 for details. If the length of the encrypted command data generated by the reader is odd, add a bit 0 to the lowest bit of the encrypted command data, that is, the encrypted data the encrypted command data after adding 0;

d) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

e) Check: CRC-16 calculation includes command code, length, encrypted data and handle data fields. See Appendix D for the calculation of CRC-16. If the check included in the command received by the tag is wrong, the tag does not respond to the command.

6.5.19.2 Response data pack

The format of the response data pack of the tag to the secure communication command is as shown in Table 38.

Table 38 -- Response data pack format of secure communication command

Data field	Command code	Authentication data	Handle	Check
Length	16-bit	Determined based on encryption algorithm	16-bit	16-bit
Description	Bit length of encrypted data	Encrypted response data	handle	CRC-16

The definition of each data field in the response data pack is as follows:

a) Length: The bit length of the encrypted data;

b) Encrypted data: The encrypted response data, see 6.7 for details;

c) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

d) Check: CRC-16 calculation includes length, encrypted data and handle data fields. See Appendix D for the calculation of CRC-16.

6.5.20 Handle refresh command

6.5.20.1 Command frame format

write permissions, erase permissions, lock permissions, kill permissions. In which, the erase permissions and write permissions are the same. Before the reader sends an access command, it shall send a random number acquisition command. The frame format of the access command is as shown in Table 43.

When accessing the tag information area and the coding area, the password is set to 0; when accessing the security subarea field, it is sufficient to compare the contents of the security subarea field to be accessed; when accessing the user subarea, it is necessary to compare the read and write password of the user subarea.

Table 43 -- Frame format of access command

Data field	Command code	Storage area	Command type	Command	Handle	Check
Length	8	6-bit	4-bit	16-bit	16-bit	16-bit
Description	10100011_b	000000_b: Tag information area 010000_b: Coding area 100000_b: Secure area $11XXXX_b$: User area	Type of command	The result of bitwise XOR of password and RN16	Handle	CRC-16

The definition of each data field in the frame format is as follows:

a) Command code: 10100011_b, the code of access command.

b) Storage area: Specify the logical storage area where the data is located. The meanings of the 4 values are explained as follows:

1) 000000_b: Tag information area;

2) 010000_b: Coding area;

3) 100000_b: secure area;

4) $11XXXX_b$: User area. "XXXX" means the user subarea number 0 ~ 15.

c) Password type: See Table 44 for details.

d) Password: This data field is the result of bitwise XOR between the password indicated by the password type and RN16. Among them, RN16 is the 16-bit random number obtained after the reader sends the random number acquisition command for the last time.

e) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command.

f) Check: CRC-16 calculation includes command code, storage area,

d) Length: The number of words to be read.

1) If the read address exceeds the range of the logical storage area, the tag returns the error code of the storage area overflow;

2) If the length is 0, when the access storage area is the tag information area and the user area, the tag returns all data from the start address to the end of the storage area;

3) If the length is 0, the access storage area is a coding area, meanwhile the starting word address is within the range indicated by the code length, then the data from the starting address to the code length indication is returned;

4) If the length is 0, the access storage area is a coding area, meanwhile the start word address exceeds the range indicated by the code length, all data from the start address to the end of the code area will be returned.

e) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command.

f) Check: CRC-16 calculation includes command code, storage area, pointer, length, handle data field. See Appendix D for the calculation of CRC-16. If the check included in the command received by the tag is wrong, the tag does not respond to the command.

6.5.23.2 Response data pack

After the tag receives the read command, it may need to send a response data pack to the reader according to its state. The format of the response data pack is as shown in Table 47.

Table 47 -- Response data pack format of the read command

Data field	Operating state	Data	Handle	Check
Length	8-bit	Corresponding to the length in read command	16-bit	16-bit
Description	Operating state of command	Actual-read data	handle	CRC-16

The definition of each data field in the response data pack is as follows:

a) Operating state: See Appendix E for the specific meaning of operating state;

b) Data: Return the data in the corresponding logical storage area. If the reading fails, the data field does not exist;

command.

e) Data: The data actually needs to be written.

f) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command.

g) Check: CRC-16 calculation includes command code, storage area, pointer, length, data, handle data fields. See Appendix D for the calculation of CRC-16. If the check included in the command received by the tag is wrong, the tag does not respond to the command.

After the reader sends the write command, it must continue to send the carrier wave to the tag. If the response data pack sent by the tag is still not received for more than 20 ms, the reader considers that this write operation has failed.

6.5.24.2 Response data pack

After the tag receives the write command, it performs the corresponding operation according to its state; it may need to send a response data pack to the reader. The format of the response data pack is as shown in Table 49. When the tag responds to the write command, the preamble uses the form of TR_{ext} = 1_b in Figure 9 or Figure 13.

Table 49 -- Response data pack format of write command

Data field	Operating state	Handle	Check
Length	8-bit	16-bit	16-bit
Description	Operating state of command	handle	CRC-16

The definition of each data field in the response data pack is as follows:

a) Operating state: See Appendix E for the specific meaning of operating state;

b) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

c) Check: CRC-16 calculation includes operation state and handle data field. See Appendix D for the calculation of CRC-16.

6.5.25 Erase command

6.5.25.1 Frame format

The erase command is used to erase the data in the logical storage area of the tag. Before the reader sends the erase command, it shall send the handle

After the reader sends the erase command, it must continue to send the carrier wave to the tag. If the response data pack sent by the tag is still not received for more than 20 ms, the reader considers that this erasing operation has failed.

6.5.25.2 Response data pack

After the tag receives the erase command, it performs the corresponding operation according to its state; it may need to send a response data pack to the reader. The format of the response data pack is as shown in Table 51. When the tag responds to the erase command, the preamble uses the form of TR_{ext} = 1_b in Figure 9 or Figure 13.

Table 51 -- Response data pack format of the erase command

Data field	Operating state	Handle	Check
Length	8-bit	16-bit	16-bit
Description	Operating state of command	handle	CRC-16

The definition of each data field in the response data pack is as follows:

a) Operating state: See Appendix E for the specific meaning of operating state;

b) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

c) Check: CRC-16 calculation includes operation state and handle data field. See Appendix D for the calculation of CRC-16.

6.5.26 Lock command

6.5.26.1 Command frame format

The lock command is used to lock the tag logic storage area or configure the security mode of the tag. The frame format of the lock command is as shown in Table 52. When the field is locked as unreadable and unwritable, the access command shall respond with an error code.

3) Other: reserved.

d) Action: If the configuration field is 00_b, it indicates the lock operation of the specified logical storage area. The meanings of the 4 values are explained as follows:

1) 00_b: The corresponding logic storage area is locked as readable and writable;

2) 01_b: The corresponding logical storage area is locked as readable and unwritable;

3) 10_b: The corresponding logical storage area is locked as unreadable and writable;

4) 11_b: The corresponding logical storage area is locked as unreadable and unwritable.

If the configuration field is 01b, it indicates the configuration operation of the security mode. The meanings of the four values are explained as follows:

1) 00_b: Reserved;

2) 01_b: No identification required;

3) 10_b: Authentication required, secure communication not required;

4) 11_b: Authentication required, secure communication required.

e) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command.

f) Check: CRC-16 calculation includes command code, storage area, configuration, action, handle data fields. See Appendix C for the calculation of CRC-16. If the check included in the command received by the tag is wrong, the tag does not respond to the command.

6.5.26.2 Response data pack

After the tag receives the lock command, it performs corresponding operations according to its state. It may need to send a response data pack to the reader. The format of the response data pack is as shown in Table 53. When the tag responds to the lock command, the preamble uses the form of TR_{ext} = 1 in Figure 9 or Figure 13.

wave to the tag. If the response data pack sent by the tag is not received for more than 20 ms, the reader considers the kill operation failed.

6.5.27.2 Response data pack

After the tag receives the kill command, it performs corresponding operations according to its state; it may need to send a response data pack to the reader. The format of the response data pack is as shown in Table 55. When the tag responds to the kill command, the preamble uses the form of $TR_{ext} = 1_b$ in Figure 9 or Figure 13.

Table 55 -- Response data pack format of kill command

Data field	Operating state	Handle	Check
Length	8-bit	16-bit	16-bit
Description	Operating state of command	handle	CRC-16

The definition of each data field in the response data pack is as follows:

a) Operating state: See Appendix E for the specific meaning of operating state;

b) Handle: The 11-bit random number and CRC-5 sent by the tag during the checking process, or the 11-bit random number and CRC-5 sent after receiving the handle refresh command;

c) Check: CRC-16 calculation includes operation state and handle data field. See Appendix D for the calculation of CRC-16.

The killed tags no longer respond to any commands from the reader.

6.6 Security authentication protocol

6.6.1 Overview

Tags that need security authentication can use the following security authentication protocol.

6.6.2 One-way authentication protocol of tag to reader

6.6.2.1 One-way authentication protocol based on XOR operation

For tags working in security mode, the one-way authentication protocol flow based on the XOR operation of the tag to the reader is as shown in Figure 24.

a) The reader sends a security parameter acquisition command.

b) The tag sends security parameters.

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------