# Research on the Security Authentication Mode of MF1 S50 Electronic Tag

**Xiao Zhiliang**

Foshan Polytechinc., Foshan, Guangdong, China, 528137

***Abstract:*** This paper expatiates the security authentication mechanism of the MF1 S50 electronic tag most widely used at present, and flexibly sets its keys and access bits to meet different application environment requirements. On this basis, this paper further discusses the basic types and setting methods of the security authentication mode of the electronic tag, so as to provide guidance for the application developers to choose different security authentication modes according to different requirements.

***Keywords:*** Electronic Tag, Security Authentication, Mode

## 1. Background

Mifare one S50 (hereinafter referred to as S50) electronic tag is a high frequency RFID passive IC developed by Philips based on the ISO/IEC 14443 type/A protocol, is one of the most widely used electronic tags in the world, and is commonly used in the fields, such as the city card, electronic ticket, ID card, campus card, parking lot management, etc. S50 electronic tag has a communication frequency of 13.56 MHz, a read-write distance of less than 10 cm, and a data transfer rate of 106 kbit/s, is provided with a multi-tag collision prevention function, has a greatest characteristic of having a perfect security authentication mechanism, and is suitable for a closed-loop system with high security authentication requirements, such as an electronic wallet, etc.

S50 security authentication mechanism is complete and strict, but in the face of a large number of application requirements in different forms, system developers need to design an applicable and reliable authentication scheme with strong operability for the users flexibly using the S50 security mechanism. Excessively strict authentication mode may lead to complex user operations, while excessively simple authentication mode may pose a potential safety hazard to the application and cause losses to the users. Therefore, designing an appropriate security authentication mode is the key to the application of the S50 electronic tag, and is also the dreamboat pursued by the application system.

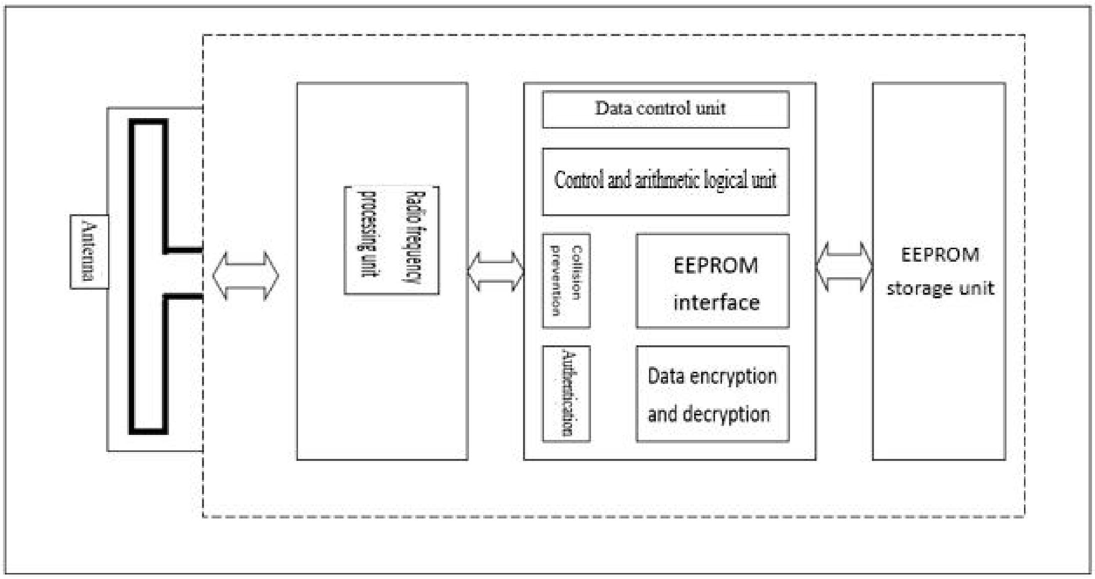
## 2. Security mechanism of the S50 electronic tag

### 2.1 S50 electronic tag structure

S50 electronic tag consists of two parts: a chip and an antenna. A S50 chip is divided into three units: a radio frequency processing unit (responsible for transmitting and receiving signals), a data control unit (responsible for data conversion, calibration, storage and other processing), and a storage unit (saving data, keys, access bits, UID codes, etc.). The S50

doi: 10.18686/esta.v4.42

antenna is made up of a number of closed-loop coils, is responsible for transmitting and receiving electromagnetic waves whilst generating inductive current, and provides energy for the chip. The structure of the S50 electronic tag is shown in Figure 1:



Antenna
Radio frequency processing unit
Data control unit
Control and arithmetic logical unit
Collision prevention
EEPROM interface
Authentication
Data encryption and decryption
EEPROM storage unit

Figure 1 Structure of the S50 electronic tag

## 2.2 Structure of the S50 electronic tag storage

The S50 electronic tag often uses EEPROM storage with a storage capacity of 8 kbits, i.e. 1024 bytes. The storage includes 16 sectors with the address code of 0 to 15, each sector includes 4 blocks with the relative address of 0 to 3, the whole storage totally includes 64 blocks with the absolute address code of 0 to 63, and each block includes 16 bytes, totally including 1024 bytes.

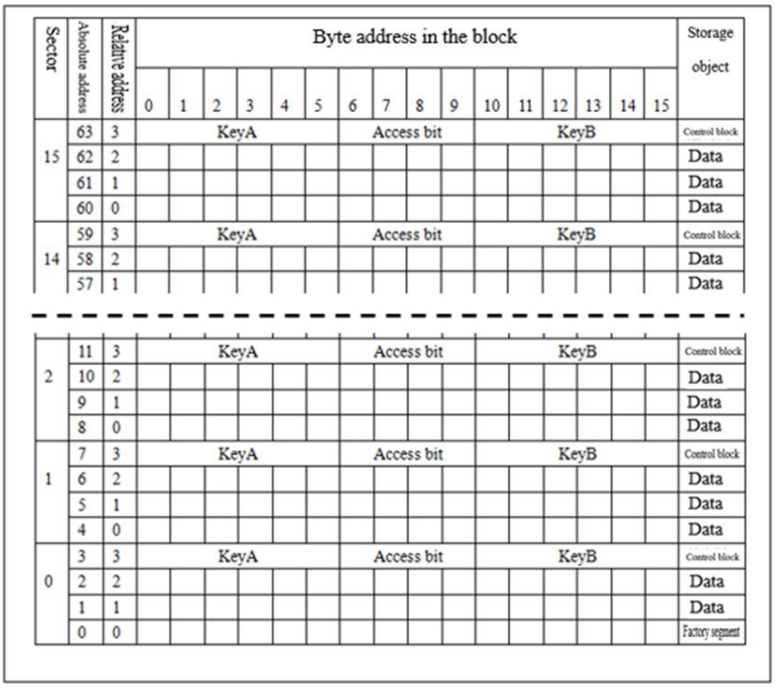
It is worth noting that the S50 storage block is a basic storage unit, which means that the reading or writing operation of the S50 must be done by reading or writing the whole block. The S50 storage block is subdivided into a data block and a control block. The data block is provided for users to store data information, while the control block is used to store sector keys and access bits, and cannot be used to store the user data. In addition, the 0th block of the 0th sector is used to store the UID code (a unique code in the world) and factory information of the chip, has been solidified before leaving the factory, and can only be read. Therefore, S50 electronic tag storage totally includes 47 data blocks actually used to store user data information, and each block includes 16 bytes, totally including 752 bytes. 752 characters or 376 Chinese characters (double byte) can be stored. The structure of the S50 electronic tag storage is shown in Figure 2:

## 2.3 Security mechanism of the S50 electronic tag

### 2.3.1 Control block structure

As can be easily seen from the structure of the S50 electronic tag storage, each sector includes a control block, stores two keys (keyA and keyB) and access bits, the length of keyA and keyB is respectively 6 bytes, and their initial key is respectively 0 XFFFFFFFFFFFF, wherein the 0th to 5th bytes are keyA, and the 10th to 15th bytes are keyB. The two keys control the operations of four blocks of the sector, and are not associated with the operations of other sectors. The

6th to 9th bytes are access bits, the setting of which determines how keyA and keyB control the operations of this sector. The structure of the control block is shown in Figure 3:



| Sector | Absolute address | Relative address | Byte address in the block | | | | | | | | | | | | | | | | Storage object |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | |
| 15 | 63 | 3 | KeyA | | | | | | Access bit | | | | KeyB | | | | | | Control block |
| | 62 | 2 | | | | | | | | | | | | | | | | | Data |
| | 61 | 1 | | | | | | | | | | | | | | | | | Data |
| | 60 | 0 | | | | | | | | | | | | | | | | | Data |
| 14 | 59 | 3 | KeyA | | | | | | Access bit | | | | KeyB | | | | | | Control block |
| | 58 | 2 | | | | | | | | | | | | | | | | | Data |
| | 57 | 1 | | | | | | | | | | | | | | | | | Data |
| 2 | 11 | 3 | KeyA | | | | | | Access bit | | | | KeyB | | | | | | Control block |
| | 10 | 2 | | | | | | | | | | | | | | | | | Data |
| | 9 | 1 | | | | | | | | | | | | | | | | | Data |
| | 8 | 0 | | | | | | | | | | | | | | | | | Data |
| 1 | 7 | 3 | KeyA | | | | | | Access bit | | | | KeyB | | | | | | Control block |
| | 6 | 2 | | | | | | | | | | | | | | | | | Data |
| | 5 | 1 | | | | | | | | | | | | | | | | | Data |
| | 4 | 0 | | | | | | | | | | | | | | | | | Data |
| 0 | 3 | 3 | KeyA | | | | | | Access bit | | | | KeyB | | | | | | Control block |
| | 2 | 2 | | | | | | | | | | | | | | | | | Data |
| | 1 | 1 | | | | | | | | | | | | | | | | | Data |
| | 0 | 0 | | | | | | | | | | | | | | | | | Factory segment |

Figure 2 Structure of the S50 electronic tag storage

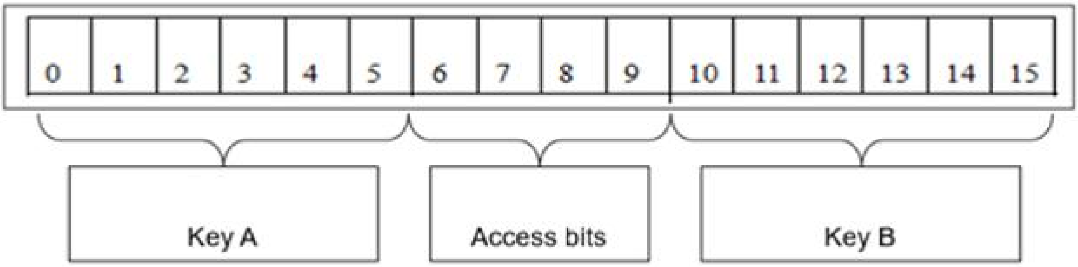


Figure 3 Structure of the S50 storage control block

### 2.3.2 Structure of the access bit

The access bit determines how keyA and keyB control the operation of this sector, which is closely related to the operation type and the security authentication state of the S50.

The operation types of the S50 are divided into 6 types:

1) Read: reading data from a block;

2) Write: Writing data into a block;

3) Increment: Increasing value of data in a block;

4) Decrement: Decreasing value of data in a block;

5) Transfer: Transferring data in a block to a register;

6) Restore: Restoring data in a register to a block.

The security authentication state of the S50 is divided into four categories:

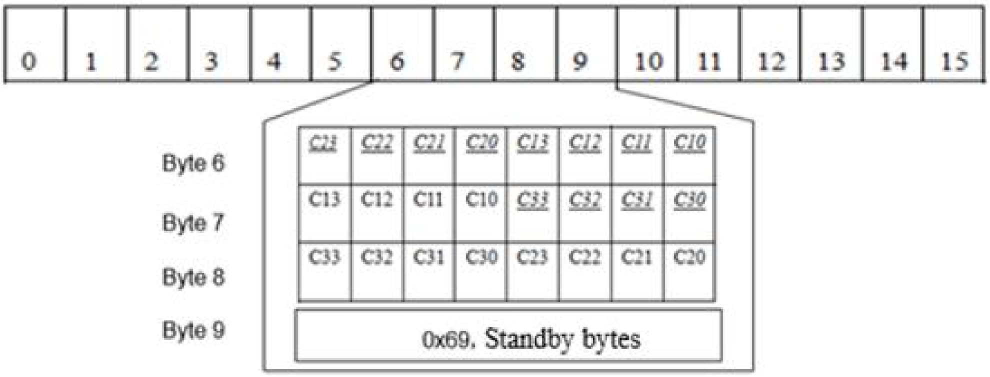
1) Never: Non-operable in any case;

2) Key A: Operable after Key A passes authentication;

3) Key B: Operable after Key B passes authentication;

4) Key A | B: Operable after Key A or Key B passes authentication.

As stated above, the access bit is located in 6th to 9th bytes of the control block, wherein 9th byte is a reserved byte with a value of 0x69 before leaving the factory. The actual access bit only includes 3 bytes, totally including 24 bits (6th to 8th bytes). Its structure is shown in Figure 4:



| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

|  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|
| Byte 6 | $\underline{C23}$ | $\underline{C22}$ | $\underline{C21}$ | $\underline{C20}$ | $\underline{C13}$ | $\underline{C12}$ | $\underline{C11}$ | $\underline{C10}$ |
| Byte 7 | C13 | C12 | C11 | C10 | $\underline{C33}$ | $\underline{C32}$ | $\underline{C31}$ | $\underline{C30}$ |
| Byte 8 | C33 | C32 | C31 | C30 | C23 | C22 | C21 | C20 |
| Byte 9 | 0x69, Standby bytes |  |  |  |  |  |  |  |

Figure 4 Structure of the S50 access bit

As can be seen from the above figure, the access bit of the control block totally includes 3 bytes and 24 bits, which are distributed in 6th to 8th bytes of the control block according to certain rules. For convenience, we assume that each bit is expressed as C××, and its meaning is shown in Figure 5:

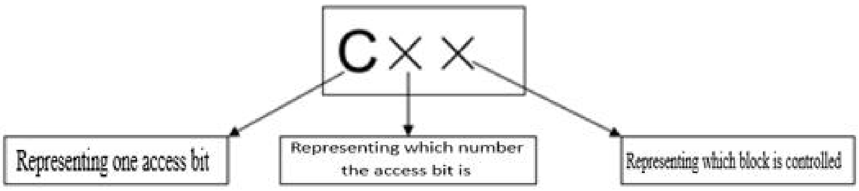

C××
Representing one access bit
Representing which number the access bit is
Representing which block is controlled

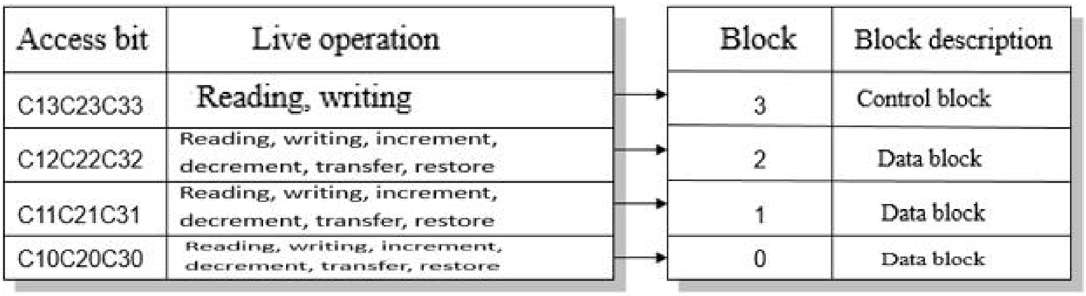
Figure 5 Meaning of the symbols expressed as the access bits

For example, C12=1 represents that the first control code of the second block is 1; and C33=0 represents that the third control code of the third block is 0. For another example, C10=0, C20=1 and C30=0 represent that the three-bit access control code of 0th block 0 is "010".

In Figure 4, the underlined italic bit represents inversion. For example, *C11* represents inversion of C11.

### 2.3.3 S50 security authentication mechanism

S50 electronic tag stipulates that a security access mechanism can be separately set for each block of each sector, the security access mechanism of each block is determined by 3 bits (access bits), which are respectively located in 6th to 8th bytes of the control block, and inverted result and uninverted result are respectively saved once. In this way, 3-bit access bits of each block occupy 6-bit storage space, and 4 blocks just need 24 bits, namely 3 bytes. The correspondence relationship between the S50 access bits, operation types and corresponding block addresses are shown in Figure 6:

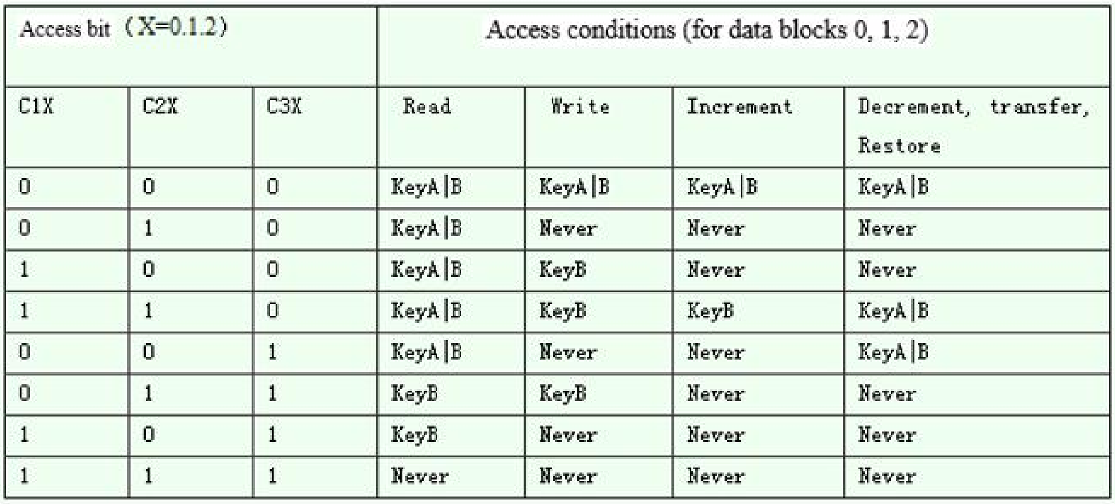


| Access bit | Live operation | Block | Block description |
|---|---|---|---|
| C13C23C33 | Reading, writing | 3 | Control block |
| C12C22C32 | Reading, writing, increment, decrement, transfer, restore | 2 | Data block |
| C11C21C31 | Reading, writing, increment, decrement, transfer, restore | 1 | Data block |
| C10C20C30 | Reading, writing, increment, decrement, transfer, restore | 0 | Data block |

Figure 6 Correspondence relationship between the S50 access bits, operation types and corresponding block addresses.

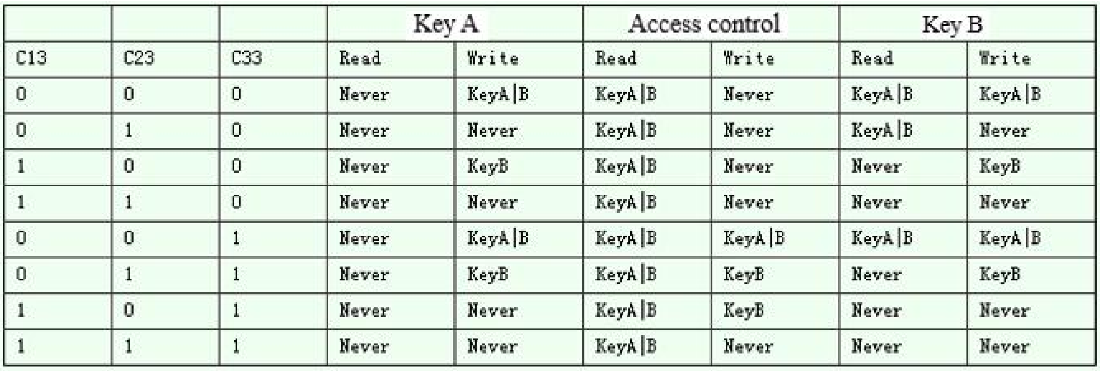
In fact, besides the data block, the control block of S50 also needs to design a security mechanism, which means that permissions to set and modify key A/B are defined. S50 provides that the setting of the operation security mechanism of the control block itself is independent of the setting of the operation security mechanism of the data block, which greatly improves the safety performance of the S50 electronic tag. The security mechanism setting mode of the data block access bit is shown in Table 1, and that of the control block access bit is shown in Table 2:

Table 1 Security mechanism setting mode of the data block access bit



| Access bit （X=0.1.2） | | | Access conditions (for data blocks 0, 1, 2) | | | |
|---|---|---|---|---|---|---|
| C1X | C2X | C3X | Read | Write | Increment | Decrement, transfer, Restore |
| 0 | 0 | 0 | KeyA\|B | KeyA\|B | KeyA\|B | KeyA\|B |
| 0 | 1 | 0 | KeyA\|B | Never | Never | Never |
| 1 | 0 | 0 | KeyA\|B | KeyB | Never | Never |
| 1 | 1 | 0 | KeyA\|B | KeyB | KeyB | KeyA\|B |
| 0 | 0 | 1 | KeyA\|B | Never | Never | KeyA\|B |
| 0 | 1 | 1 | KeyB | KeyB | Never | Never |
| 1 | 0 | 1 | KeyB | Never | Never | Never |
| 1 | 1 | 1 | Never | Never | Never | Never |

Table 2 Security mechanism setting mode of the control block access bit



| | | | Key A | | Access control | | Key B | |
|---|---|---|---|---|---|---|---|---|
| C13 | C23 | C33 | Read | Write | Read | Write | Read | Write |
| 0 | 0 | 0 | Never | KeyA\|B | KeyA\|B | Never | KeyA\|B | KeyA\|B |
| 0 | 1 | 0 | Never | Never | KeyA\|B | Never | KeyA\|B | Never |
| 1 | 0 | 0 | Never | KeyB | KeyA\|B | Never | Never | KeyB |
| 1 | 1 | 0 | Never | Never | KeyA\|B | Never | Never | Never |
| 0 | 0 | 1 | Never | KeyA\|B | KeyA\|B | KeyA\|B | KeyA\|B | KeyA\|B |
| 0 | 1 | 1 | Never | KeyB | KeyA\|B | KeyB | Never | KeyB |
| 1 | 0 | 1 | Never | Never | KeyA\|B | KeyB | Never | Never |
| 1 | 1 | 1 | Never | Never | KeyA\|B | Never | Never | Never |

In order to facilitate understanding the setting of the S50 security mechanism mode, we illustrate this using two simple user demand cases.

Case 1: It is requested to write personal information of a person in the 0th block of the 2nd sector. This information can only be read and cannot be rewritten. The book borrowing information written by the 1st block can be read and written, can be read after verifying the key A, and can be written only after verifying the key B. The top-up data written by the 2nd block into the student's meal cards can only be rewritten after verifying the key B. Consumption (decrement) can be achieved after verifying the key A or B. How to set the access bit?

1) Set 3 access bits of the 0th block: As can be found by looking up Table 1, the access bit "010" is suitable for the user demand, and is designed as: C10=0, C20=1 and C30=0.

2) Set 3 access bits of the 1st block: As can be found by looking up Table 1, the access bit "100" is suitable for the user demand, and is designed as: C11=1, C21=0 and C31=0.

3) Set 3 access bits of the 2nd block: As can be found by looking up Table 1, the access bit "110" is suitable for the user demand, and is designed as: C12=1, C22=1 and C32=0.

Case 2: The key A can be rewritten only after verifying the key B; the access bits can be read, but cannot be changed; the key B cannot be read, but the key B can be reset after verifying the key B. How to set the access bit?

Obviously, this is a safe mode setting for the control block itself. As can be found by looking up Table 2, the access bit "100" is suitable for the user demand, and is designed as: C13=1, C23=0 and C33=0.

## 3. Security certification mode of the S50 electronic tag

As can be seen from the foregoing description, S50 electronic tag itself provides a very perfect security authentication mechanism. But in actual development and application, the situation is far from so simple, and the developers need to deal with a lot of practical problems and contradictions. Based on the practical application case over the years, I summarize the security authentication mechanism of the S50 electronic tag as an internal authentication mechanism and an external authentication mechanism, which need to be subdivided into different security authentication modes based on the user demand. The problem is discussed below.

### 3.1 Internal authentication mechanism

The internal authentication mechanism of S50 means independent security authentication using the keys and access bits provided by the S50 chip itself. Its encryption process can be done by user's subjective consciousness without the help of an external intelligent device. The keys are controlled by the user, and maintained by the system administrator. This security authentication method is influenced and limited by human factors, and its security also depends on the professional ethics and moral accomplishment of the operator.

### 3.1.1 Parallel limitation mode

The parallel limitation mode means that a plurality of operators has equal permission to control the same operation of the S50 electronic tag, and there is no hierarchy of permission between them. As we know, security authentication of the S50 electronic tag is conducted for a single sector, and the parallel limitation mode is also operated in the same sector. A sector has two sets of keys: keyA and keyB. It is necessary to adopt the "keyA|keyB" mode, so that the operators have equal operation permission, which means that operation can be made after comparison of the key A or key B is successful.

For the operation of the data block, as can be seen from comparison of the “Security mechanism setting mode of the data block access bit” in Table 1 of 2.3.3, the access bit of this sector should be set as: C1X=0, C2X=0 and C3X=0. However, for the control block itself, as can be seen from comparison of the “Security mechanism setting mode of the control block access bit” in Table 2 of 2.3.3, the access bit of this sector should be set as: C13 0, C23=0 and C33=0.

For example, for the bus card top-up operation of a bus company, the staff during day shift is Zhang San, the staff during night shift is Li Si, and both of them have equal operation permission. However, neither of them would like the other person to know about his key, and then this mode is a good choice. The keyA is assigned to Zhang San, the keyB is assigned to Li Si, and then setting a 3-bit Access Bit as "000" is OK.

It is worth noting that the parallel limitation mode is for a block of a sector, which doesn't mean that each block of this sector shall adopt the parallel limitation mode. Other blocks can also use a stepped limitation mode.

### 3.1.2 Stepped limitation mode

The stepped limitation mode is that a plurality of operators has different hierarchies of permission to control the operation of the S50 electronic tag, and different operators have different permissions of the operation type of S50. Like the parallel limitation mode, the stepped limitation mode is also operated in the same sector, and a sector has two sets of keys: keyA and keyB, which play different roles, and do not have a parallel relationship. The stepped limitation mode does not completely represent the relationship between the superior and the inferior, and more precisely represents different labor divisions of operators.

For the operation of the data block, as can be seen from comparison of the “Security mechanism setting mode of the data block access bit” in Table 1 of 2.3.3, the access bits "100" and "110" belong to the stepped limitation mode, "100" means that the operator controlling the keyA can only read data, and only the operator controlling the keyB can read and write data.

### 3.1.3 One-card mode

One-card mode means that various business types use a same electronic tag as a support carrier, each business type is carried out in different sectors, and various business types can be run separately without the hierarchy of membership and permission. With 16 sectors, the MF1 S50 electronic tag can theoretically manage 16 business types. The UID code of the electronic tag is solidified in the 0th sector, is a unique electronic tag can theoretically manage 16 business types. The UID code of the electronic tag is solidified in the 0th sector, is the unique identification code of the whole electronic tag, and may be used for the operation of every sector. Therefore, usually, the 0th sector is used as a public sector to manage and assign all kinds of business types and address information of the sector. The 1st sector to the 15th sector can be operated as 15 separate business types.

The one-card mode is very widely used, and a typical case is the campus card, which assigns various business types to different sectors for separate security authentication, so that various business management departments do not interfere with each other, and business operators operate independently. For example, for the logistics department (dining hall), borrowing books from the library, teaching attendance, leasing sports facilities, paying for utilities, and so on, each business is managed by a sector, and a security authentication mode is separately set for each sector without interfering with each other.

### 3.2 External authentication mechanism

The MF1 S50 electronic tag provides flexible and diverse internal security authentication mechanisms. The internal security authentication mechanism is a mode based on keys artificially set for sectors, wherein the security authentication management greatly depends on the responsibility and morality of the operator, and once an operator reveals the keys or leaves office, it will seriously affect the card security. Based on this, introducing an external security authentication mechanism can better solve this problem.

External security authentication mechanism operates keys using an external hardware device, and then sets or compares keys. In this mode, the operator does not know specific content of the keys, and achieves isolation of operators from the keys. The external hardware operating the keys may be a PSAM card (built in the reader-writer), and may also be a U-KEY (inserted in a USB interface).

In order to achieve different keys for different electronic tags, usually keys of 16 sectors of an S50 electronic tag can be operated through external encryption operation using the UID code of the electronic tag as an operational factor and using a long string as a divergent factor. Different divergent factors may also be used in different sectors to calculate the keys for each sector. In this way, the keys for each electronic tag and for different sectors of the same electronic tag are completely different, thereby breaking through the limitations of internal logic security authentication of the MF1 S50 electronic tag, and greatly improving the safety performance of electronic tags.

## 4. Conclusions

MF1 S50 electronic tag is very widely used, and is not only used as an identity authentication medium, but also usually has a function of an alternative electronic currency, such as consumption, top-up, integral, etc. Therefore, its security appears to be particularly important. Because the storage structure and security authentication mechanism of the MF1 S50 electronic tag are complex and flexible, how to choose an appropriate security authentication mode and hierarchy according to user demand needs to be summarized and explored in a lot of practice. The various security authentication modes explored herein are summarized and concluded by the author in abundant applications and development, and are expected to provide reference for application developers of the MF1 S50 electronic tag.

## Reference

1. Yu Lei. Logistics Management System of Internet of Things based on RFID electronic tags [J]. Microcomputer Information, 2006 (02).
2. Ma Yujian. Design and implementation of the signature system based on the electronic tag system [D]. Masters' Theses of North China University of Technology, 2009CNKI
3. Ouyang Changqing, Huang Sheng Ye & Liu Wanfang. Overview of security problems of low cost RFID [J]. Network Security Technology & Application, 200
4. Xiao Feng. Research and design of the security protocol for electronic tags of Internet of Things [D]. Masters' Theses and Doctoral Theses of Beijing University of Posts and Telecommunications, 2013CNKI
5. Tian Yun. Research on some problems in the identification of passive electronic tags. [D]. Doctoral Theses of Shanghai Jiao

tong University, 2013CNKI

6. Zhao Kewen. Research on security of electronic tags and applications thereof in logistics [D]. Masters' Theses of Xidian University, 2006CNKI
7. Wang Lung & Peng Sheqiang. Research on RFID multi-authentication protocol and security analysis [J]. Journal of Computer Applications, 2013, (S2)
8. Xiao Feng. Research on anti-collision algorithm and security authentication protocol in RFID system. Masters' Theses of Beijing Institute of Technology, 2014CNKIHammond DC. Neuro feedback with anxiety an ad affective disorders. J Child Adolesc Psychiatr Clin N Am, 2005, 14:105-123.