GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
File No.: 44641-2014

GM/T 0036-2014

Technical guidance of cryptographic application for access control system based on contactless smart card

采用非接触卡的门禁系统密码应用技术指南

Issued on: February 13, 2014 **Implemented on: February 13, 2014**

Issued by: State Cryptography Administration

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This Standard was proposed by and shall be under the jurisdiction of Cryptography Industry Standardization Technical Committee.

Main drafting organizations of this Standard: Shanghai Fudan Microelectronics Group Co., Ltd, Shanghai Huahong Integrated Circuit Co., Ltd, Xing Tang Communication Technology Co., Ltd, Beijing CEC Huada Electronics Design Co., Ltd, Shanghai Huashen Smart Card Application System Co., Ltd, Tongfang Microelectronics Co., Ltd, Aerospace Information Co., Ltd, Beijing Huada Chi Po Electronic Systems Co., Ltd, Fudan University.

Main drafters of this Standard: Yu Jun, Dong Haoran, Liang Shaofeng, Wu Xingjun, Zhou Jiansuo, Wang Junfeng, Xie Wenlu, Liu Xun, Chen Yue, Gu Zhen, Wang Yunsong, Xu Shumin, Wang Junyu.

Technical guidance of cryptographic application for access control system based on contactless smart card

1 Scope

This Standard specifies the related requirements of encryption device, cryptographic algorithm, cryptographic protocol and key management which are applied for access control system using cryptographic security technology based on contactless smart card.

This Standard is applicable to guide the research, usage and management of products related to access control system based on contactless smart card.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GM/T 0002-2012 SM4 block cipher algorithm

GM/T 0035.4-2014 Specifications of cryptographic application for RFID systems - Part 4: Specification of cryptographic application for communication between RFID tag and reader

3 Terms and definitions

The following terms and definitions apply to this document.

3.1 Secure access module

Cryptography module built in the reader to provide security services.

3.2 RFID tag

A carrier for radio frequency identification containing electronic identification information relevant to the intended application. Each tag has a unique electronic code which usually consists of coupled components and chips, including contactless CPU card and contactless memory card.

Management of key generation, distribution, storage, update, archiving, revocation, backup, recovery and destruction of keys throughout the life cycle according to security policy.

3.15 Radio frequency identification

The radio frequency signal that is used to achieve the contactless transmission of information through space coupling (alternating magnetic field or electromagnetic field), and the purpose of identification by the transmitted information.

3.16 Audit

Independent observation and assessment of the records and activities of the information system.

3.17 Data integrity

The nature of data not being tampered with or compromised in an unauthorized manner.

3.18 SM1 algorithm

A block cipher algorithm, with a block length of 128 bits and a key length of 128 bits.

3.19 SM4 algorithm

A block cipher algorithm, with a block length of 128 bits and a key length of 128 bits.

3.20 SM7 algorithm

A block cipher algorithm, with a block length of 64 bits and a key length of 128 bits.

3.21 Random number

A data sequence that is unpredictable and has no periodicity.

3.22 Message authentication code

Also known as message verification code. It is the output of message authentication algorithm.

3.23 Unique identifier

A unique identifier that is solidified in the tag chip by the tag chip manufacturer, containing unique information such as the chip production serial number, the registered manufacturer code, and so on.

3.24 Subject

6.5.1 Key generation

The key should be generated by random numbers that meet the requirements of national cryptography management, and the confidentiality and randomness of the generated keys shall be guaranteed. Ensure the process of key generation is non-predictable, and any two keys generated in the key space have the same probability.

6.5.2 Key injection

The following two points of key injection should be noted when issuing the access card and the cryptographic module:

a) No part of the plaintext key shall be disclosed during key injection;

b) The key can only be injected into the cryptographic device when the cryptographic device, interface, and transmission channel are not subjected to any situation that may cause the key or sensitive data to be compromised or tampered with.

6.5.3 Other requirements

Throughout the whole process of key generation, injection, update and storage, make sure that the key is not disclosed.

7 Cryptographic application solution reference

This standard provides the following cryptographic application solutions as reference:

a) The contactless logic encryption card solution based on the national cryptographic algorithm SM7, see Appendix A;

b) The contactless CPU card solution (including scheme 1 and scheme 2) based on the national cryptographic algorithm SM1/SM4, see Appendix B.

8 Other security factors to be considered

This standard only stressed on the security requirements for cryptographic applications. The following factors should be taken into account in the implementation of the system for the overall security of the system:

a) Management requirements of background management system;

b) Security of access card reader and background management system;

c) Other management and technical measures not related to cryptographic security, such as code recognition, biometric identification, personnel guard and so on.

Figure B.3 -- Schematic block diagram of contactless CPU card solution based on SM1/SM4 algorithm scheme 2

In the scheme, the radio frequency interface module is responsible for radio frequency communication between the card reader and the access card; the MCU controls the communication between the radio frequency interface module and the access card AND is responsible for realizing the data transfer inside the card reader and the communication with the background management system.

B.3 Cryptographic security application process

B.3.1 Key management and card issuing system

a) Security module distribution

The background management system of access control uses the key management subsystem cryptographic device to generate the access system derivation key, which must be securely transferred to the security module.

b) Access card issuing

The background management system uses the SM1/SM4 algorithm to distribute the system derivation key and achieve one cipher for one key. Through a card issuing reader, the background management system carries out card identification, directory application and initialization of data structure such as document system using the SM1/SM4 algorithm and process key AND completes downloading of the card key (Keyc). It also writes in the card the user information and information of the issuing agency. The process uses the CPU card issuing process to ensure the security of the information writing and confidentiality of data.

B.3.2 Access control system

The two schemes described in B.2 are explained as follows.

a) Scheme 1

In scheme 1, the access card reader directly authenticates the access card and controls the implementation of the access control function according to the result. This process is similar to that of the logic encryption card using the SM7 algorithm, so it will not be discussed here. The difference is using the internal authentication command of CPU card to authenticate the identity of CPU access card rather than the special command of logic encryption card.

b) Scheme 2

In mode 2, the access card reader does not directly authenticate the access card BUT uses the background management system (through a secure access module supporting the SM1/SM4 algorithm) to authenticate the card AND controls the implementation of access control function according to the identification results.

The specific methods of identification are as follows:

-- The access card reader reads the unique identification number(UID) of the card and apply to the specific distribution information Ci (if any) for one-card-one-code distribution;

-- The access card reader sends an internal authentication command to the access card, that is, to send a random number R (The generation of random numbers is discussed below.) to the access card. The access card uses the one-card-one-code key Keyc, which is used in the card, to encrypt the random number by the SM1/SM4 algorithm and generate the result R'_a=Enc(Keyc, R_a) and send it back to the access control reader;

-- One access card reader transmits the R_a (or not), R'_a, UID, Ci (if any) to the background management system;

-- When the background management system obtains information uploaded from the third step, it can carry out the authentication of the access card. First it uses distribution factor such as UID, Ci (if any) and the system derivation key Keyr stored in the security module to get one-cipher-one card key Keyc by SM1/SM4 algorithm, namely Keyc=Enc(Keyr, UID, Ci). Then encrypt R_a (recorded in the system or uploaded by the card reader) with the one-card-one-code by the SM1/SM4 algorithm key, which means R''_a=Enc(Keyc, R'_a). If R'_a= R''_a, the identity is authentic; and if not, the identity is not authorized;

-- The background management system compares whether the card unique identification number is a blacklist, and if not, the card is a legitimate access card within the system. It sends an open message to the access execution unit to open. At the same time, it uses the security module to generate a random number R_{a+1} for the reader to use next time and send, together with R_{a+1}, the authentication result (whether authorized or not) to the access card reader. The access card reader receives and stores the random number for the next authentication process of the internal authentication command of access control.

The authentication process is shown in figure B.4.

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

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