# GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L80

File No.: 49739-2015

# GM/T 0040-2015

# Cipher test specification of radio frequency identification tag module

射频识别标签模块密码检测准则



**Issued on: April 1, 2015** **Implemented on: April 1, 2015**

**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.

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. The issuing authority shall not be held responsible for identifying any or all such patent rights.

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

Main drafting organizations of this Standard: CEC Huada Electronic Design Co., Ltd., Commercial Cryptography Testing Center of State Cryptography Administration, Shanghai Huahong Integrated Circuit Co., Ltd., Beijing Tongfang Microelectronics Company, Shanghai Fudan Microelectronics Group Co., Ltd., Shanghai Hsic Application System Co., Ltd., Aisino Corporation, Nation Technologies Inc.

Main drafters of this Standard: Dong Haoran, Luo Peng, Zhou Jiansuo, Lan Tian, Fei Du, Mao Yingying, Mo Fan, Deng Kaiyong, Gu Zhen, Yang Xianwei, Shao Bo, Liu Xun, Liu Ying, Yue Chao.

# Cipher test specification of radio frequency identification tag module

## 1 Scope

This standard specifies the test content and requirements for cipher test of RFID (Radio Frequency Identification) tag module product by using cryptographic techniques.

This standard applies to cipher test and security function test of RFID tag module. It can also be used to meet the requirements of GB/T 28925-2012 and GB/T 29768-2013 for the cipher test of RFID air interface protocol product.

The algorithm described in this standard is the cryptographic algorithm which is approved by state cryptography administration competent department.

## 2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this document. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 28925-2012 Information technology - Radio frequency identification - Air interface protocol at 2.45 GHz

GB/T 29768-2013 Information technology - Radio frequency identification - Air interface protocol at 800/900 MHz

GM/T 0005-2012 Randomized test specification

GM/T 0008-2012 Cipher test specification of security chip

GM/T 0035.1-2014 Technical requirements for cryptographic application of radio frequency identification system – Part 1: Cryptographic security protection framework and security level

GM/T 0035.2-2014 Technical requirements for cryptographic application of radio frequency identification system - Part 2: Technical requirements for cryptographic applications of electronic tag chip

GM/T 0035.4-2014 Technical requirements for cryptographic application of

radio frequency identification system - Part 4: Technical requirements for cryptographic application of electronic tag and reader-writer communication

GM/Z 4001 Cipher terms

# 3 Terms and definitions

The terms defined in GM/Z 4001 AND the following terms and definitions apply to this document.

**3.1**

**Symmetric cryptographic algorithm**

It is a cryptographic algorithm which uses the same key in encryption-decryption.

**3.2**

**Unidirectional authentication**

It is an identity authentication for tag which is initiated by reader-writer.

**3.3**

**Confidentiality**

It is the nature which guarantees information not to be leaked to entities such as unauthorized individuals and processes.

**3.4**

**Non-repudiation of origin**

It is a cryptographic method which is used to prevent the originator of a message from denying its creation and having sent the message.

**3.5**

**Kill**

It is an operation instruction to tag module; after successfully executed, the tag module will no longer respond to any command.

**3.6**

**Radio frequency identification**

command and mechanism specified in the standard; if it selects and uses the products of security authentication protocols in GM/T 0035.4-2014, it shall implement the security mechanism specified in the standard; If it selects and uses the products of security authentication protocols in other security standards or user-defined, it shall implement the corresponding security mechanism.

#### 6.3.1.2 Category-I tag module

The identity authentication test mode of Category-I tag module is as follows:

a) Test requirements

Use unidirectional authentication mode. The unidirectional authentication process shall use cipher, and its cipher function shall be correct and valid. The test environment needs to design valid and invalid test cases. The tag module shall respond correctly to the authentication request which is issued by the reader-writer.

b) Decision criteria

The unidirectional authentication mechanism of tag module is valid.

#### 6.3.1.3 Category-II tag module

The identity authentication test mode of Category-II tag module is as follows:

a) Test requirements

Use bidirectional authentication mode. The bidirectional authentication process shall use cipher, and its cipher function shall be correct and valid.

The test environment needs to design valid and invalid test cases. The tag module shall respond correctly to the bidirectional authentication between the reader-writer.

b) Decision criteria

The bidirectional authentication mechanism of tag module is valid.

### 6.3.2 Data-transmission confidentiality test

#### 6.3.2.1 Category-I tag module

No requirement.

#### 6.3.2.2 Category II-A tag module

No requirement.

The tag module can use cryptographic algorithm to protect the confidentiality of the stored sensitive information data.

#### 6.3.4 Data-transmission integrity test (This item is optional)

##### 6.3.4.1 Category-I tag module

No requirement.

##### 6.3.4.2 Category II-A tag module

No requirement.

##### 6.3.4.3 Category II-B tag module

The data-transmission integrity test mode of Category II-B tag module is as follows:

a) Test requirements

The tag module can provide correct and effective data-transmission integrity service for sensitive information that is allowed to be transmitted as required.

When the tag module communicates with the reader-writer, the tag module uses cryptographic algorithm to perform verification calculation on the transmitted data to find out that the data has been tampered with, deleted and inserted, etc., in order to achieve data integrity requirements during transmission.

b) Decision criteria

The data which is transmitted on the channel can use cryptographic algorithm for integrity protection during transmission.

#### 6.3.5 Data-storage integrity test (This item is optional)

##### 6.3.5.1 Category-I tag module

No requirement.

##### 6.3.5.2 Category II-A tag module

No requirement.

##### 6.3.5.3 Category II-B tag module

The data-storage integrity test mode of Category II-B tag module is as follows

Send the undefined or incorrect instructions of products to the tested tag module; the tag module shall report errors or produce no response.

#### 6.7.2.2 Category-II tag module

It is the same as Category-I tag module.

### 6.7.3 Anti-initial right of use deception test

#### 6.7.3.1 Category-I tag module

The anti-initial right of use deception test mode of Category-I tag module is as follows:

a) Test requirements

The tag module does not provide initialization permission; perform initialization operation for the tested tag module; test whether the tag module has the anti-initialization function.

b) Decision criteria

Do not perform initialization operation on the tested tag module.

#### 6.7.3.2 Category-II tag module

It is the same as Category-I tag module.

### 6.7.4 Anti-life-cycle cross-border test

#### 6.7.4.1 Category-I tag module

Anti-life-cycle cross-border test mode of Category-I tag module is as follows:

a) Test requirements

Use non-current instructions of life-cycle phase; test the anti-life-cycle cross-border function of tag module.

b) Decision criteria

Send the non-current instructions of life-cycle phase to the tested tag module; the tag module shall report errors or produce no response.

#### 6.7.4.2 Category-II tag module

It is the same as Category-I tag module.

It shall meet the requirements of 7.3.1of GM/T 0008-2012.

#### 6.9.3.2 Category-II tag module

It is the same as Category-I tag module.

### 6.9.4 Key update

#### 6.9.4.1 Category-I tag module

If the tag module has the key update function, it shall comply with the provisions of 7.4.1 of GM/T 0008-2012.

#### 6.9.4.2 Category-II tag module

It is the same as Category-I tag module.

### 6.9.5 Key import

#### 6.9.5.1 Category-I tag module

It shall meet the requirements of 7.5.1 of GM/T 0008-2012.

#### 6.9.5.2 Category-II tag module

It is the same as Category-I tag module.

### 6.9.6 Key clearing

#### 6.9.6.1 Category-I tag module

If the tag module has the key clearing function, it shall comply with the provisions of 7.7.1 of GM/T 0008-2012.

#### 6.9.6.2 Category-II tag module

It is the same as Category-I tag module.

## 6.10 Development environment protection

### 6.10.1 Document management

#### 6.10.1.1 Category-I tag module

The document management mode of Category-I tag module is as follows:

a) Various types of documents such as development process, configuration management, delivery operation, algorithm function development and tool technology of tag module are complete;

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

Full-copy PDF can be purchased from 1 of 3 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

3. https://www.google.com/search?tbm=bks&q=ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Google Books -- Select your currency.
- Processed by Google (delivery, tax invoice etc.). Delivered in 9 seconds by Google.
- Tips: Download an unprotected True-PDF (text-editable) from Google-Books:
  1. https://play.google.com/books → 2. Sign in → Google account
  3. Find the BOOK you bought → 4. Click "3-dots" → Export
  5. Save as "*.pdf" (Save True-PDF to your local computer for offline reading/printing)

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

Accountable person and shareholder: Wayne Zheng

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

**------ The End ------**