

ICS 35.040
CCS L 80

GM

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GM/T 0096-2020

Guide for RFID anti-counterfeiting cipher application

射频识别防伪系统密码应用指南

(English Translation)

Issued on: December 28, 2020

Implemented on: July 1, 2021

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative References	2
Terms and Definitions	3
Symmetric Cryptographic Algorithm	4
Asymmetric Cryptographic Algorithm / Public Key Cryptographic	5
Confidentiality	6
Cryptographic Module	7
Abbreviations	8
Overview	9
Security Level	10
Category-B System	11
System architecture	12
Tag issuance system	13
Cryptographic security requirements	14
Optional cryptographic security requirements	15
Cryptographic security requirements	16
Optional cryptographic security requirements	17
Information processing system	18
Requirements for transparent transmission channel - reader	19
System architecture	20
Tag issuance system	21
Information processing system	22
Certificate issuance and identity authentication system	23
Cryptographic security requirements	24
Sales management certificate system's issuance of sales management	25
Requirements for transparent transmission channel - reader	26
Application Scheme	27
System architecture	28
Tag issuance system	29
Information processing system	30
Certificate issuance and identity authentication system	31
Cryptographic security requirements	32

Sales management certificate system's issuance of sales management	33
Requirements for transparent transmission channel - reader	34
Application Scheme	35

1 Scope

This Standard specifies the security category, system planning and implementation of RFID anti-counterfeiting application.

This Standard is applicable to cryptographic security scheme design, cryptographic product selection and system implementation in RFID anti-counterfeiting application.

2 Normative References

The content of the following documents constitutes indispensable clauses of this document through normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 28925 Information Technology - Radio Frequency Identification - Air Interface Protocol at 2.45 GHz
 GB/T 29768 Information Technology - Radio Frequency Identification - Air Interface Protocol at 800/900 MHz
 GB/T 32915 Information Security Technology - Binary Sequence Randomness Detection Method
 GB/T 37033.1-2018 Information Security Technology - Technical Requirements for Cryptographic Application for Radio Frequency Identification Systems - Part 1.

Cryptographic Protection Framework and Security Levels
 GB/T 37033.2-2018 Information Security Technology - Technical Requirements for Cryptographic Application for Radio Frequency Identification Systems - Part 2.

Technical Requirements for Cryptographic Application for RF Tag, Reader and Communication

3 Terms and Definitions

What is defined in GB/T 37033.1-2018 and GM/Z 4001-2013 (TRANSLATOR NOTE.

it should be GM/Z 0001-2013), and the following terms and definitions are applicable to this document.

3.3 Symmetric Cryptographic Algorithm

Symmetric cryptographic algorithm refers to the cryptographic algorithm that uses the same key for encryption and decryption.

3.4 Asymmetric Cryptographic Algorithm / Public Key Cryptographic

Algorithm

Asymmetric cryptographic algorithm / public key cryptographic algorithm refers to the cryptographic algorithm that uses different keys for encryption and decryption. One of the keys (public key) may be disclosed, while the other key (private key) must be confidential, and it is infeasible to calculate the private key from the public key.

3.5 Confidentiality

Confidentiality refers to the nature of ensuring that information is not leaked to unauthorized individuals, processes and other entities.

3.10 Cryptographic Module

Cryptographic module refers to a collection of hardware, software and / or firmware that implements security functions, and is included in the cryptographic boundary.

4 Abbreviations

The following abbreviations are applicable to this document.

CA. Certificate Authority

5 Overview

The cryptographic application framework based on the RFID anti-counterfeiting system is shown in Figure 1. It is composed of tag issuance, anti-counterfeiting authentication, middleware, information processing system, gateway, key management system and CA. Among them, CA and middleware are optional parts, which may be selected in accordance with the demands of application.

6.1 Security Level

In accordance with the different requirements of RFID anti-counterfeiting system for cryptographic security technology, the security level of the anti-counterfeiting system may be divided into two categories, namely, Category-A and Category-B.

6.3 Category-B System

Category-B anti-counterfeiting cryptographic security system (hereinafter referred to as Category-B system) shall comply with the requirements of Level-4 security specified in 6.2.4 of GB/T 37033.1-2018. The random number in the system shall comply with the requirements of GB/T 32915.

7.1.1 System architecture

Category-A system adopts symmetric cryptographic algorithm, and through the authentication of the electronic tag by the reader, or through the bidirectional authentication between the reader and the electronic tag, it improves the security and anti-counterfeiting capabilities of the RFID tag.

7.1.2 Tag issuance system

Issue a key for the anti-counterfeiting tag, and after the issuance is completed, associate the commodity traceability-related information with the anti-counterfeiting tag (UID); store it in the information process system, which makes it convenient for consumers to carry out commodity traceability and anti-counterfeiting.

7.2.1.1 Cryptographic security requirements

The RFID electronic tag used in Category-A system shall satisfy the following cryptographic security requirements.

7.2.1.2 Optional cryptographic security requirements

In accordance with the demands of application, the RFID electronic tag used in Category-A system may optionally support the following cryptographic security requirements.

6.3.4 of GM/T 0040-2015.

e) Identity authentication. It may optionally support the identity authentication of the reader by the electronic tag. The mode, in which, the identity authentication of the reader by the electronic tag is realized, is shown in 8.3.2.1 of GB/T 37033.2-2018. The identity authentication of the reader by the electronic tag shall be tested in accordance with 6.2 and 6.3 of GM/T 0040-2015. The mode, in which, the bidirectional authentication between the reader and the electronic tag is realized, is shown in 8.3.3.1 of GB/T 37033.2-2018.

7.2.2.1 Cryptographic security requirements

The RF reader of cryptographic security functions used in Category-A system may satisfy the following cryptographic security requirements.