

ICS 35.040

GM

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

GM/T 0097-2020

**Security technical specifications for unified name resolution
service of RFID**

射频识别电子标签统一名称解析服务安全技术规范

(English Translation)

Issued on: December 28, 2020

Implemented on: July 1, 2021

Issued by: State Administration of Cryptography

Table of Contents

Foreword	1
Scope	2
Normative References	3
Terms and Definitions	4
Electronic Product Code	5
Electronic Product Code Application System	6
Object Name Service	7
Key	8
Key Management	9
Symbols	10
Coding of Electronic Tags	11
ONS System Architecture	12
ONS Server Registration	13
Security Query Processing	14
Cryptographic Algorithm	15
Random Number Security	16
General requirements	17
Key distribution	18
Key storage	19
Key update	20
Key backup and recovery	21
Hardware Security	22
Software Security	23
Foreword	24
Cryptographic Algorithm	25
Random Number Security	26
General requirements	27
Key distribution	28
Key storage	29
Key update	30
Key backup and recovery	31
Hardware Security	32

Foreword

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

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

1 Scope

This Standard specifies the system architecture, key business process and security requirements for unified name resolution service of RFID; defines the registration process of name resolution server, the security query process of electronic product code and corresponding information message format.

This Standard is applicable to the development and application of unified name resolution service system of RFID.

2 Normative References

The following documents are indispensable to the application of this document. 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 17901.1 Information Technology - Security Techniques - Key Management - Part 1: Framework
GB/T 32905 Information Security Techniques - SM3 Cryptographic Hash Algorithm
GB/T 32907 Information Security Technology - SM4 Block Cipher Algorithm
GB/T 32915 Information Security Technology - Randomness Test Methods for Binary Sequence
GB/T 32918 (all parts) Information Security Technology - Public Key Cryptographic Algorithm
SM2 Based on Elliptic Curves
GB/T 35276-2017 Information Security Technology - SM2 Cryptographic Algorithm Usage Specification
GM/Z 4001-2013 Cryptology Terminology (TRANSLATOR NOTE. it should be GM/Z 0001-2013)

3 Terms and Definitions

What is defined in GM/Z 4001-2013 (TRANSLATOR NOTE. it should be GM/Z 0001-2013), and the following terms and definitions are applicable to this document.

3.1 Electronic Product Code

Electronic product code is stored on RFID tag to provide unique identification for an object.

3.2 Electronic Product Code Application System

Electronic product code application system provides a standard interface for accessing and persistently storing electronic product code-related data.

3.4 Object Name Service

Object name service provides the mapping relationship between the electronic product code and the service address where the detailed information of the object is stored.

3.5 Key

Key refers to the key information or parameters that control the password conversion operation.

3.6 Key Management

Key management refers to the management of the processes of key generation, storage, usage, update, import, export and destruction, etc.

4.1 Symbols

The following symbols are applicable to this document.

5 Coding of Electronic Tags

Please refer to Appendix A for the coding rules of electronic tags.

6 ONS System Architecture

ONS system is composed of six parts. electronic tag, tag reader, ONS client-side, local ONS server, ONS infrastructure server and EPCIS server, in which, the elliptical area is ONS infrastructure server, which adopts three-level deployment. The ONS servers at all levels provide the address mapping of electronic product code to EPCIS server, as it is shown in Figure 1.

7.1 ONS Server Registration

When the local ONS server joins the system, it shall register with the Level-1 ONS server. The device certificates of both parties shall be used to verify the legitimacy of the identity, and a session key shall be obtained through negotiation.

7.2 Security Query Processing

When the local ONS server receives the query request of electronic product code from the ONS client-side, firstly, it searches for the corresponding EPCIS server information in the local cache. If such information is not found, then, starting from the Level-1 ONS server, it conducts resolution in the mode of iterative query, until the query result is obtained. In the end, it returns the query result to the ONS client-side.

8.1 Cryptographic Algorithm

The cryptographic algorithm used by the ONS system shall comply with the requirements of national and industry standards on cryptography.

8.2 Random Number Security

The random number used by the ONS system shall comply with the requirements of national and industry standards on cryptography.

The inspection of random number shall comply with the requirements of GB/T 32915.

8.3.1 General requirements

The ONS system shall be equipped with complete key management measures. The contents of key generation, storage, distribution, backup, update and destruction shall comply with the relevant requirements of GB/T 17901.1.

8.3.5 Key distribution

The device public key of the ONS servers at all levels shall be able to be exported. It is imported into the device after the key management system issues the device certificate. The device private key does not need to be distributed.

8.3.6 Key storage

The device key shall be stored in the non-volatile storage unit of the device, in which, the device private key shall have security protection measures, and cannot appear outside the device in plain text under any circumstances.

8.3.7 Key update

Generally speaking, the validity period of the device certificate is not more than 5 years.

Before the device certificate expires, the device certificate shall be re-issued by the digital certificate system in advance.