ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 35290-2023

Replacing GB/T 35290-2017

Information security technology-Security technical specification for radio frequency identification (RFID) systems

信息安全技术 射频识别（RFID）系统安全技术规范

Issued on: December 28, 2023 **Implemented on: July 1, 2024**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document complies with the provisions of GB/T 1:1-2020 "Standardization Work

Guidelines Part 1: Structure and Drafting Rules of Standardization Documents" Drafting:

This document replaces GB/T 35290-2017 "General Security Technical Requirements for Radio Frequency Identification (RFID) Systems in Information Security Technology" and is consistent with Compared with GB/T 35290-2017, in addition to structural adjustments and editorial changes, the main technical changes are as follows:

- Changed the scope (see Chapter 1, Chapter 1 of the:2017 edition);

- Added and changed terms and definitions (see Chapter 3, 3:1 of the:2017 edition);

- Changed symbols and abbreviations (see Chapter 4, 3:2 of the:2017 edition);

- Changed the system composition (see 5:1, 4:1 of the:2017 version);

- Increased system security risks (see 5:2);

- Changed the system security classification (see Chapter 6,:2017 version 4:2);

- Changed the data verification requirements for electronic label security requirements (see 7:1:2:6, 5:1:2:6 of the:2017 version);

- Added identification uniqueness, security audit and security audit confidentiality protection requirements for reader/reader writer security technology requirements (see 7:2:1:1, 7:2:1:9, 7:2:2:4);

- Added data integrity requirements for air interface communication link security technical requirements (see 7:3:2:1);

- Deleted the integrity recovery mechanism requirements for network transmission communication link security technical requirements (see 5:4:2:3 of the:2017 version);

- Added management unit security related to authorized program loading and updating, malicious code prevention, trusted verification, data backup and recovery, Basic level requirements for security audits (see 7:5:1:3, 7:5:1:7, 7:5:1:8, 7:5:1:9, 7:5:1:10), as well as information on access control, data Enhanced requirements for data integrity, data confidentiality, trusted verification, intrusion prevention, malicious code prevention, recoverability, and security auditing (See 7:5:2:1, 7:5:2:2, 7:5:2:3, 7:5:2:4, 7:5:2:9, 7:5:2:10, 7:5:2:11, 7:5:2:12), understandable format removed Enhanced level requirements (see 5:5:2:1:3 of the:2017 version);

- Added test environment requirements (see Chapter 8);

- Added test evaluation method (see Chapter 9):

Please note that some content in this document may be subject to patents: The publisher of this document assumes no responsibility for identifying patents:

This document is proposed and coordinated by the National Information Security Standardization Technical Committee (SAC/TC260):

This document was drafted by: The Third Research Institute of the Ministry of Public Security, China Electronics Technology Standardization Institute, Beijing Zhongke Guoji Information System Co:, Ltd:

Company, Shanghai Yishi Intelligent Technology Co:, Ltd:, Shanghai Lingang Power Electronics Research Co:, Ltd:, Tencent Cloud Computing (Beijing) Co:, Ltd:, Zhuhai Haifudan Innovation Research Institute, Zhengzhou Xinda Ji'an Information Technology Co:, Ltd:, Shanghai Institute of Chemical Industry Testing Co:, Ltd:, Changyang Technology (Beijing) Co:, Ltd:, Xi'an Jiaotong University Jabil Network Technology Co:, Ltd:, China Automotive Engineering Research Institute Co:, Ltd:, China Network Security Review Technology Technology and Certification Center, Guangdong Ji'an Technology Co:, Ltd:, Zhejiang University of Technology:

The main drafters of this document: Liu Caixia, Gu Jian, Xie Fangyi, Zhang Yan, Liu Dandan, Jiao Zhihao, Li Lin, Li Zhe, Dai Jie, Liu Hong, Zhang Dongju, Liu Yucheng, Li Jianhui, Liu Haitao, Wang Junyu, Liu Weihua, Wang Siyi, Zhao Hua, He Jianfeng, Liu Chong, Shen Yongbo, He Hongliang, Gu Guomin:

The previous versions of this document and the documents it replaces are as follows:

- First published as GB/T 35290-2017 in:2017;

- This is the first revision:

Information Security Technology Radio Frequency Identification (RFID) System Safety technical specifications

1 Scope

This document specifies the security technical requirements for radio frequency identification (RFID) systems, including electronic tags, readers/readers, and air interface communications The security requirements for links, network transmission communication link management units, etc: are given, and test conditions and test evaluation methods are given:

This document applies to the design, development, use, testing and evaluation of security functions of radio frequency identification (RFID) systems:

This document does not apply to radio frequency identification (RFID) systems in the 5:8GHz band:

Note: This document does not involve security functional requirements or security performance requirements for physical attack security risks:

2 Normative reference documents

GB/T 20271

GB/T 28925

GB/T 29261

GB/T 29768

GB/T 32915

GB/T 33848

GB/T 37033

GB/T 37033

GB/T 37033

3 Terms and definitions

GB/T 20271, GB/T 29261:3, GB/T 28925, GB/T 29768, GB/T 37033:1-2018, GB/T 37033:2- 2018, GB/T 37033:3-2018 and the following terms and definitions apply to this document: 3:1 In the radio frequency part of the spectrum, electromagnetic coupling or inductive coupling is used to interactively communicate with electronic tags through various modulation and coding schemes:

A technology that obtains the unique identity of electronic tags:

[Source: GB/T 29261:3-2012,05:01:01] 3:2 Using radio frequency identification technology, including one or more readers/readers, one or more electronic tags, readers/readers and The air interface communication link between electronic tags, the network transmission communication link between the reader/reader and the management unit, and the management unit