ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35290—2017

信息安全技术　射频识别(RFID)系统通用安全技术要求

Information security technology—General requirement of security for radio frequency identification systems

2017-12-29 发布　　2018-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第三研究所、中国电子技术标准化研究院、北京中科国技信息系统有限公司、复旦大学、上海交通大学 RFID 与物联网研究所、江苏省质量和标准化研究院、中国科学院上海高等研究院、江苏出入境检验检疫局机电产品及车辆检测中心。

本标准主要起草人:刘彩霞、顾健、张艳、谢芳艺、张振一、范科峰、李琳、龚洁中、姚相振、周睿康、李哲、孙伟华、何蔚、邵轲、王丽娟、刘继顺、李旋、王俊宇、王东、杨迅捷、俞晓磊、张钊锋、过峰。

信息安全技术　射频识别(RFID)系统通用安全技术要求

1　范围

本标准规定了射频识别(RFID)系统安全技术相关(以下简称 RFID 系统)的基本级要求和增强级要求。

本标准适用于具有安全技术要求的 RFID 系统整体及构成 RFID 系统的各类 RFID 标签、读写器、通信链路及后端系统的安全功能的设计、开发和使用。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 20271—2006　信息安全技术　信息系统通用安全技术要求

GB/T 22239—2008　信息安全技术　信息系统安全等级保护基本要求

GB/T 29261.3—2012　信息技术　自动识别和数据采集技术　词汇　第 3 部分:射频识别

GM/T 0035.1—2014　射频识别系统密码应用技术要求　第 1 部分:密码安全保护框架及安全级别

GM/T 0035.2—2014　射频识别系统密码应用技术要求　第 2 部分:电子标签芯片密码应用技术要求

GM/T 0035.3—2014　射频识别系统密码应用技术要求　第 3 部分:读写器密码应用技术要求

GM/T 0035.4—2014　射频识别系统密码应用技术要求　第 4 部分:电子标签与读写器通信密码应用技术要求

GM/T 0035.5—2014　射频识别系统密码应用技术要求　第 5 部分:密钥管理技术要求

3　术语和定义、缩略语

3.1　术语和定义

GB/T 20271—2006 和 GB/T 29261.3—2012 界定的以及下列术语和定义适用于本文件。

3.1.1

通信链路　communication link

RFID 系统中两个节点之间的物理通道。包括读写器和标签之间的空中接口通信链路和读写器与后端系统之间的网络传输通信链路。

3.1.2

后端系统　back-end system

由中间件、计算机终端、数据库、服务器等软硬件组成的系统。

3.1.3

主动标签　active tag

自身带有内部电源供应器,用以供应内部 IC 所需电源以产生对外讯号的标签。

3.2 缩略语

下列缩略语适用于本文件。

DoS:拒绝服务(Denial of Service)

DDoS:分布式拒绝服务(Distributed Denial of Service)

SYN Flood:同步洪水攻击(Synchronize Flood)

ICMP Flood:互联网控制报文协议洪水攻击(Internet Control Message Protocol Flood)

SNMP Trap:简单网络管理协议陷阱(Simple Network Management Protocal Trap)

SMS:短信服务(Short Message Service)

4 概述

4.1 系统组成

RFID 系统由标签、读写器、通信链路及后端系统等四个部分组成,其中,通信链路又由标签与读写器之间的空中接口和读写器与后端系统之间的网络传输链路两部分组成。RFID 系统描述参见附录 A。

4.2 分类分级

依据 RFID 系统组成,本标准将 RFID 系统通用安全功能要求按标签安全、读写器安全、通信链路(空中接口)安全、通信链路(网络传输)安全及后端系统安全共五个子类给出,每个子类分别划分为两个等级:基本级和增强级。其中基本级安全功能要求应具备 GB/T 22239—2008 中第二级安全保护能力,并应同时涵盖第一级安全保护能力;增强级安全功能要求应具备 GB/T 22239—2008 中第四级安全保护能力,并应同时涵盖第三级安全保护能力。RFID 系统应至少满足基本级安全技术要求。文中增强级要求仅列出了除基本级技术要求外的增强级要求。增强级应在符合基本级安全技术要求的基础上满足增强级要求。

5 安全功能要求

5.1 标签安全功能要求

5.1.1 基本级要求

5.1.1.1 标识唯一性

标签应具有不可更改的唯一标识。

5.1.1.2 灭活(仅适用于 800/900 MHz、2.45 GHz 频段的 RFID 标签)

标签在接收到包含灭活口令的特殊指令后应进入灭活状态。灭活状态的标签应不再响应任何外部指令。灭活口令应受灭活密钥控制。

5.1.1.3 基于口令的访问控制

标签应只允许通过口令验证的读写器访问其用户区。不同标签或同一标签的不同存储区域的访问口令宜各不相同。

5.1.1.4 信息防篡改

标签应能防止其存储数据被未经授权的攻击者篡改。

5.1.1.5 防非法指令

标签应只响应协议及制造商规定的指令，对于无法识别的指令应不予响应。

5.1.1.6 具有基于算法的访问控制（仅适用于主动标签）

标签应只允许通过基于算法的身份鉴别协议验证的读写器访问其存储区。不同标签或同一标签的不同存储区域所用的密钥宜各不相同。

5.1.1.7 随机数产生

标签应具备随机数发生器。随机数发生器应能够产生安全的随机数。

5.1.1.8 片内程序更新的完整性保护（仅适用于主动标签）

标签应具备片内程序更新完整性校验功能。

5.1.2 增强级要求

5.1.2.1 完整性服务

标签应具备对其传输的数据提供完整性服务的能力。

5.1.2.2 前向安全性

标签应具备前向安全性。当标签中的密钥泄露时，前向安全性功能应能使标签之前与读写器交互的消息仍然安全。

5.1.2.3 具有基于算法的访问控制

标签应只允许通过基于算法的身份鉴别协议验证的读写器访问其存储区。不同标签或同一标签的不同存储区域的密钥宜各不相同。

5.1.2.4 敏感信息保护、销毁和管理

标签应支持加密算法加密并带校验的敏感信息存储。允许读取的敏感信息，标签应具有相应的安全机制保证敏感信息明文只在标签内部进行处理。标签清除敏感信息不得透露敏感信息本身。

5.1.2.5 基于算法的数据加密（仅适用于主动标签）

标签应对存储在标签内的敏感信息采用加密算法进行加密保护，除合法读写器外，其余任何读写器应不能获得该标签敏感信息数据。加密算法应符合 GM/T 0035.1—2014、GM/T 0035.2—2014、GM/T 0035.4—2014、GM/T 0035.5—2014 的相关技术要求及国家密码相关规定。

5.1.2.6 鉴别消息的完整性、密钥协商和读写认证等密码服务（仅适用于主动标签）

标签应对传输的数据进行校验计算，以发现数据被篡改、删除和插入等情况，达到传输过程中的数据完整性要求。

5.1.2.7 签名服务(仅适用于主动标签)

当标签作为信息的原发者时,标签应对所发送信息(数据)产生数字签名;当标签作为读写器签名信息的验证主体时,标签应能够验证读写器的签名数据。

5.2 读写器安全功能要求

5.2.1 基本级要求

5.2.1.1 基于口令的访问控制

读写器应采用口令对读写标签信息等操作设置控制权限。对不同的权限应设置不同的口令进行访问控制,应阻止非授权的访问。

5.2.1.2 基于算法的访问控制(仅适用于读取有源标签的读写器)

读写器应采用密码算法对标签信息读写、密钥存储、密钥更新等操作设置控制权限。对不同的权限应设置不同的密钥进行访问控制,应阻止非授权的访问。密码算法应符合 GM/T 0035.1—2014、GM/T 0035.3—2014、GM/T 0035.4—2014、GM/T 0035.5—2014 的相关技术要求及国家密码相关规定。

5.2.1.3 授权的程序装载与更新

读写器应具有授权的程序装载与更新功能。

5.2.1.4 初始化权限的控制

读写器应具有初始化权限的控制功能。

5.2.1.5 完整性服务

读写器对向标签传输的数据应进行自校验计算,以发现数据被篡改、删除和插入等情况,确保传输信息的完整性。

5.2.1.6 随机数产生

读写器内应具有随机数发生器。随机数发生器应能够产生安全的随机数。

5.2.1.7 敏感信息保护、销毁和管理

读写器应能正确、有效地存储、更新和销毁敏感信息。读写器应对敏感信息的访问设置相应权限。

5.2.2 增强级要求

5.2.2.1 基于算法的访问控制

读写器应采用密码算法对标签信息读写、密钥存储、密钥更新等操作设置控制权限。对不同的权限应设置不同的密钥进行访问控制,应阻止非授权的访问。密码算法应符合国家密码相关政策。

5.2.2.2 基于算法的数据加密功能

读写器应对存储的敏感信息采用密码算法进行加密保护,使得非授权访问不会导致敏感信息泄漏。读写器应对传输的敏感信息采用密码算法进行加密保护,保证该传输数据在被截获后无法得到明文数

据。加密算法应符合 GM/T 0035.1—2014、GM/T 0035.3—2014、GM/T 0035.4—2014、GM/T 0035.5—2014 的相关技术要求及国家密码相关规定。

5.2.2.3 签名服务功能

读写器应具有签名服务功能。签名服务功能应符合以下技术要求：

a) 当读写器作为信息的原发者时，读写器对向标签传输的数据产生数字签名；

b) 当读写器作为标签签名信息的验证主体时，读写器能够验证标签的签名数据。

5.3 通信链路（空中接口）安全功能要求

5.3.1 基本级要求

5.3.1.1 数据完整性

应保障通信链路（空中接口）传输过程中的数据完整性。

5.3.1.2 数据源可追溯性

应保障通信链路（空中接口）中传输的数据信息来源可追溯。

5.3.2 增强级要求

5.3.2.1 数据保密性

应对通信链路（空中接口）中传输的数据信息进行加密保护，采用的加密算法应符合 GM/T 0035.1—2014、GM/T 0035.4—2014、GM/T 0035.5—2014 的相关技术要求及国家密码相关规定。

5.3.2.2 数据时效性

通信链路（空中接口）中传输的数据信息应包含数据发布的系统时间信息，宜采用包含实时时间信息的加密技术或基于时间序列的数据加密技术来实现时间信息的防篡改保护。其中实现时间信息防篡改保障的加密算法应符合 GM/T 0035.1—2014、GM/T 0035.4—2014、GM/T 0035.5—2014 的相关技术要求及国家密码相关规定。

5.3.2.3 抗抵赖

应具有在请求的情况下为读写器或标签提供数据原发证据和接收证据的功能，以实现抗抵赖。

5.4 通信链路（网络传输）安全功能要求

5.4.1 基本级要求

5.4.1.1 数据保密性

应采用加密方法或其他措施保障通信链路（网络传输）中传输数据的保密性。

5.4.1.2 数据完整性

应能够检测到系统管理数据、鉴别信息和重要业务数据在通信链路（网络传输）中完整性受到破坏。

5.4.2 增强级要求

5.4.2.1 数据时效性

通信链路（网络传输）中传输的数据信息应包含数据发布的系统时间信息，宜采用包含实时时间信

息的加密技术或基于时间序列的数据加密技术来实现时间信息的防篡改保护。其中实现时间信息防篡改保障的加密算法应符合 GM/T 0035.1—2014、GM/T 0035.5—2014 的相关技术要求及国家密码相关规定。

5.4.2.2 数据源可追溯性

应保障通信链路(网络传输)中传输的数据信息来源可追溯,宜采用数字签名和校验机制来实现。其中数字签名算法应符合 GM/T 0035.1—2014、GM/T 0035.5—2014 的相关技术要求及国家密码相关规定。

5.4.2.3 完整性恢复机制

应能够检测到通信链路(网络传输)中完整性错误时采取必要的恢复措施。

5.4.2.4 抗抵赖

应具有在请求的情况下为数据原发者或数据接收者提供数据原发证据和接收证据的功能,以实现抗抵赖。

5.5 后端系统安全功能要求

5.5.1 基本级要求

5.5.1.1 身份鉴别

每个接入后端系统的读写器等设备应具有唯一的设备标识和身份鉴别信息。

5.5.1.2 访问控制

后端系统应能够通过访问控制列表,提供明确的访问保障能力和拒绝访问能力。

5.5.1.3 数据完整性保护

后端系统应保护储存于设备中的鉴别数据和访问控制列表等信息不受未授权查阅、修改和破坏。

5.5.1.4 状态监测

后端系统应能监测读写器等设备的在线和运行状态。

5.5.1.5 密码算法

后端系统相关功能所使用的密码算法应符合 GM/T 0035.1—2014、GM/T 0035.5—2014 的相关技术要求及国家密码相关规定。

5.5.2 增强级要求

5.5.2.1 审计日志

5.5.2.1.1 审计数据生成

后端系统应能生成读写器等设备的接入和通信日志。

5.5.2.1.2 记录内容

后端系统生成的审计日志应至少包含以下内容:

a) 事件 ID；
b) 事件主体；
c) 事件客体；
d) 事件发生的日期和时间；
e) 事件的结果；
f) 其他可审计信息。

5.5.2.1.3 可理解格式

后端系统应确保所有审计数据为管理员所理解。

5.5.2.1.4 授权查阅

后端系统应确保除授权管理员之外，其他用户无权对审计记录进行查阅。

5.5.2.1.5 可恢复性

在存储空间耗尽、遭受攻击等异常情况下，后端系统应采取措施保证已存储的审计记录的可恢复性。

5.5.2.2 数据保密

后端系统应通过加密等方式来保护包括组件之间通信数据不被非授权获取。

5.5.2.3 数据流控制

后端系统应能执行以下信息流控制功能：
a) 对接入的应用协议信息流进行合规性检查；
b) 对接入的应用协议信息流的协议信令及参数关键字进行过滤；
c) 对接入的应用协议信息流中的内容进行关键字过滤。

5.5.2.4 抗攻击

后端系统应能够抵御各种 DoS/DDoS 攻击，识别和防御 SYN Flood、ICMP Flood 等攻击。

5.5.2.5 安全报警

后端系统应能提供入侵等指定事件报警功能，报警信息应至少包括以下内容：
a) 事件主体；
b) 事件客体；
c) 事件发生的日期和时间；
d) 事件描述。

5.5.2.6 报警方式

后端系统安全功能应能够至少采用以下一种报警方式通知管理员：
a) 弹出窗报警；
b) 发送邮件报警；
c) 发送 SNMP Trap 消息；
d) 发出声光信号；
e) 发送 SMS 消息。

附 录 A
（资料性附录）
射频识别（RFID）系统描述

射频识别（RFID）系统是由 RFID 标签、读写器、后端系统、标签和读写器之间的空中接口通信链路、读写器和后端系统之间的网络传输通信链路组成的自动识别系统。通常，读写器在一个区域发射电磁场能量，RFID 标签经过这个区域时感应到读写器的信号后进行相应的反馈，读写器接收 RFID 标签发送的信号，解码和校验数据的完整性等多个交互流程后，将信息传送给后端系统完成相应的处理工作。

RFID 系统的安全防护范围如图 A.1 所示，一般包括 RFID 标签、读写器、后端系统、标签和读写器之间的空中接口通信链路、读写器和后端系统之间的网络传输通信链路。

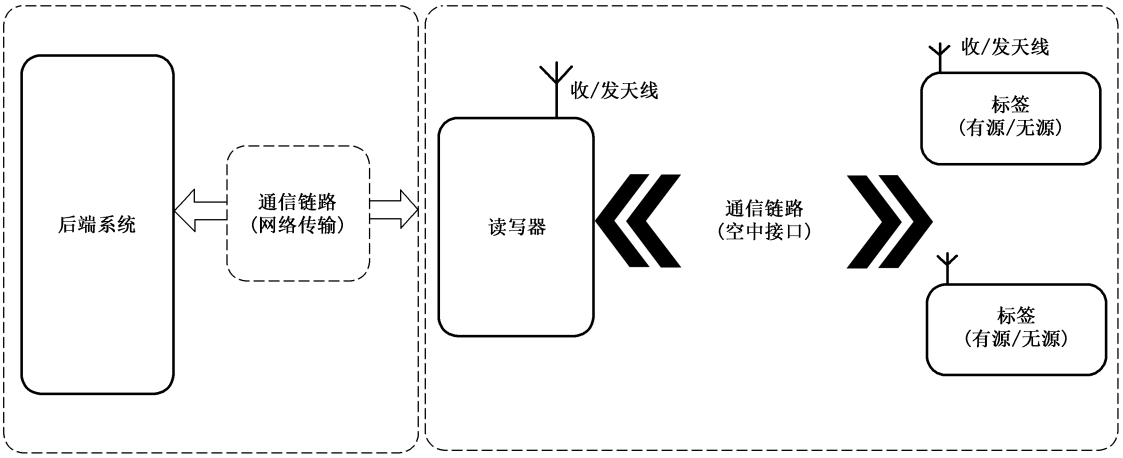

图 A.1 RFID 系统示意图