ICS 35.020
CCS I 6450

T/（ZPMA）

团 体 标 准

T/ZPMA 0002—2024

RFID 技术物联网应用与数据安全技术规范

RFID Technology Application in the Internet of Things and Data Security Technical Specification

2024－07－05 发布 2024－08－05 实施

浙江省职业经理人协会 发 布

目 次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由美思特射频技术科技（长兴）有限公司提出。

本文件由浙江省职业经理人协会归口。

本文件起草单位：美思特射频技术科技（长兴）有限公司、宁波迪泰科技股份有限公司、捷信（浙江）通信技术有限公司、浙江浙大网新软件产业集团有限公司、杭州瀚融信息技术有限公司、浙江诺盾消防科技有限公司、杭州感想科技有限公司、浙江金惠科技有限公司、维灵（杭州）信息技术有限公司、浙江城安大数据有限公司、浙江黎阳网络科技有限公司、丽水华数广电网络有限公司、浙江桃科智能科技有限公司、杭州穿石物联科技有限责任公司、杭州日报报业集团（杭州日报社）、杭州欣美成套电器制造有限公司、杭州阳斯信息技术有限公司、杭州市融资担保集团有限公司、浙江省通信产业服务有限公司宁波市分公司（集体）。

本文件主要起草人：胡日红、陈宇峰、刘建军、高春林、徐科峰、王正勇、陈洁涵、汤秀燕、杨波、王珺、陈吉、范全龙、金礼杨、何文武、陶勇、王铤慧、许雪娟、戴建刚、俞志彦、俞皓凡、韩鑫。

RFID技术物联网应用与数据安全技术规范

1 范围

本文件规定了RFID产品的分类与要求，包含外观要求、气候环境、功能要求、性能要求及检验规则。

本标准规定了RFID技术的数据安全，包含威胁与技术要求。

本文件适用于具有安全技术要求的应用RFID技术的各类电子标签、读写器安全、通信链路安全、管理单元安全及测试环境要求、测试评价方法。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 5170 环境试验设备检验方法

GB/T 10593.2-2023 电工电子产品环境参数测量方法 第2部分：盐雾

GB/T 17626 电磁兼容 试验和测量技术

GB/T 20271 信息安全技术 信息系统通用安全技术要求

GB/T 28925 信息技术 射频识别 2.45GHz 空中接口协议

GB/T 33848.3 信息技术 射频识别 第3部分：13.56MHz 的空中接口通信参数

GB/T 35290-2023 信息安全技术 射频识别（RFID）系统安全技术规范

GB/T 36365-2018 信息技术 射频识别 800/900MHz无源标签通用规范

GB/T 37033-2018（所有部分） 信息安全技术 射频识别系统密码应用技术要求

GB/T 42025-2022 智能制造 射频识别系统 超高频RFID系统性能测试方法

WB/T 1121-2022 仓储管理射频识别技术应用要求

YZ/T 0180-2021 寄递包装射频识别（RFID）应用技术要求

ISO/IEC 18000（所有部分） 信息技术 物品管理用射频识别

3 术语和定义

下列术语和定义适用于本文件。

3.1

射频识别 radio frequency identification（RFID）

是一项利用射频信号通过空间耦合（交变磁场或电磁场）实现无接触信息传递并通过所传递信息达到识别目的的技术。

3.2

电子标签 electronic tag

用于目标物信息的识别或物品的跟踪、负责信息的存储与处理、能接收阅读器/读写器的射频信号，并返回响应信号的数据载体。

3.3

RFID读写器 RFID， Radio Frequency Identification

又称为“RFID 阅读器”，即无线射频识别阅读器，采用射频识别信号自动辨识目标对象和获取相关数据，无需人工干预，能快速便捷地识别高速运动物体以及同时识别多个RFID 标签。

3.4

射频天线 radio frequency antenna

无线收发设备的基本单元，用于向空中辐射或从空中接收射频信号。

3.5

距离 distance

特指电子标签与读写器之间有效读写及识别的距离。

3.6

管理单元 management unit

射频识别系统中的应用管理部分，由中间件、计算机终端或移动智能终端、网络通信设备、数据库、服务器以及系统管理软件等硬件和软件构成。

3.7

通信链路 communication link

射频识别系统中的传输通信信道，包括阅读器/读写器与电子标签之间的空中接口通信信道以及阅读器/读写器与管理单元之间的网络传输通信信道。

4 符号和缩略语

下列符号和缩略语适用于本文件。

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

DoS：拒绝服务（Denial of Service）

HMAC：采用密码杂凑函数生成的消息鉴别码（Hash Message Authentication Code）

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

K_{TR}：传输密钥（Key for Transport）

MAC：消息鉴别码（Message Authentication Code）

RFID：射频识别（Radio Frequency Identification）

SMS：短信服务（Short Message Service）

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

SYN Flood：同步洪水攻击（Synchronize Flood）

TID：电子标签标识符（Tag Identifier）

UID：唯一标识符（Unique Identifier）

5 RFID 物联网应用

5.1 在公安领域中的应用

5.1.1 交通管控上的 RFID：

——应用场景：ETC 系统，即不停车收费系统；

——工作原理：装有 RFID 标签的车辆在 0～10 m 范围内，接近 ETC 读写器时，读写器发出微波查询信号，电子标签将信号与数据信息（如高速里程）反馈回读写器；

——优势：减少人为乱收费现象，提高通关速度，防止堵车；

——技术特点：利用现代通信技术、电子技术、自动控制技术、计算机和网络技术实现车辆不停车自动收费。

5.1.2 车辆识别上的 RFID：

——应用场景：车辆进出管理、车辆追踪、车辆信息收集等；

——工作原理：通过无线射频方式获取车辆相关数据，实现车辆识别；

——优势：提高车辆监控和管理的效率和准确性；

——技术特点：车辆在通过 RFID 读取区域时，无需停车即可被自动识别，提高了车辆监控和管理的准确性和效率。

5.1.3 交通流量管理：

——应用场景：交通规划、拥堵分析、交通信号控制等；

——工作原理：RFID 设备检测车辆数量、速度和方向，提供数据给交通管理部门；

——优势：帮助交通管理部门实时了解交通状况，采取有效管理措施；
——技术特点：通过在关键交通节点部署 RFID 设备，实时收集并分析车辆流量数据。

5.1.4 违章处罚：
——应用场景：交通违章监控、违章车辆追踪、罚款通知等；
——工作原理：RFID 设备自动检测违章车辆信息，与黑名单比对，自动发送罚款通知；
——优势：实现违章检测和处罚的自动化，提高效率；
——技术特点：车辆违章时，RFID 设备自动检测并记录违章信息，与数据库比对后，自动向车主发送罚款通知。

5.1.5 电子车牌：
——应用场景：车辆身份验证、交通管理、车辆追踪等；
——工作原理：车辆通过读取区域时，系统自动识别电子车牌信息；
——优势：简化交通管理流程，提高监控准确性；
——技术特点：电子车牌包含 RFID 芯片，车辆通过读取区域时，系统自动识别车牌信息。

5.1.6 监狱司法上的 RFID：
——应用场景：监狱人员管理、感应式电子巡更等；
——工作原理：服刑人员佩戴腕式标签，定位器发送位置信息给标签，标签传递信息给阅读器，系统分析并发出警报；
——优势：提高监狱管理信息化水平，确保人员安全；
——技术特点：服刑人员佩戴腕式 RFID 标签，监狱出入口安装阅读器和定位器，实现人员定位和监控。

5.2 在防伪领域中的应用

5.2.1 流通领域：
——应用场景：RFID 技术在物流行业，用于产品从出厂到最终销售的整个流程；
——工作原理：产品出厂时附上电子标签，写入唯一识别代码，并将信息录入数据库，通过读写器在各个环节反复读写标签；
——优势：
- 实现了产品全流程的实时监控和管理；
- 提高了物品分拣的自动化程度，降低了差错率。

——技术特点：电子标签作为物品的“身份证”，在装箱销售、出口验证、到港分发、零售上架等环节发挥关键作用。

5.2.2 特殊物品监管：
——应用场景：用于药品、食品、危险品等特殊物品的防伪和跟踪追溯；
——工作原理：利用 RFID 技术对特殊物品进行全程电子监控和管理；
——优势：确保特殊物品从生产到消费的每个环节都可追踪，提高安全性；
——技术特点：
- RFID标签的UID为每件特殊物品提供了独一无二的身份标识；
- 标签的防篡改特性增强了监管力度，确保了特殊物品的真实性和合法性；
- 实时监控能力允许监管机构快速响应潜在的安全问题，如产品召回；
- 配合数据库和分析工具，RFID技术能够提供详细的物流和供应链数据，辅助决策制定。

5.2.3 证件防伪：
——应用场景：护照防伪、电子钱包以及国内二代身份证等证件防伪领域；
——工作原理：在证件中嵌入 RFID 标签，提供安全功能并支持硬件加密；
——优势：提高了证件管理的效率，如快速验证和身份确认，同时增强了防伪能力；
——技术特点：
- RFID标签集成在证件中，不易被察觉或移除，增加了伪造难度；
- 支持硬件加密的芯片提供了高级的数据保护，防止未授权访问和数据泄露。

5.3 在智能停车场中的应用

5.3.1 停车管理：

——应用场景：停车场；

——工作原理：停车场部署 RFID 读写器，车辆携带 RFID 标签，系统自动读取标签信息，计算停车时间和费用；系统整合物联网 RFID 技术、计算机局域网技术、语音提示技术、短程微波通信技术、图像数字处理技术和自动控制技术；

——优势：

- 提高车辆通行效率和安全性；
- 减轻管理人员劳动强度，有效防止收费漏洞；
- 实现车辆出入数据的实时统计和管理。

——技术特点：

- 电子闸栏：根据系统判断控制开启或关闭；
- 车辆检测器：确保车辆在闸栏下方时安全；
- 车辆远距离读写设备：与电子标签配合，实现约10米的有效读取距离；
- 出入口控制主机：在非常规情况下允许手动控制；
- 车辆电子标签：具有防水、防磁、大容量存储、高保密度、多用途等特点；
- 管理系统：提供实时系统管理、卡片数据管理，以及车辆信息统计分析功能，支持统计报表的显示和打印；
- 数据库系统：作为智能停车场系统的核心，支持业务主机的运行。

6 RFID 产品分类与要求

6.1 产品分类

6.1.1 按工作频率分类：

——低频：125 kHz～134.2 kHz；

——高频：13.56 MHz；

——超高频：860 MHz～960 MHz；

——微波：2.45 GHz～5.0 GHz。

6.1.2 按标签供电方式分类：

——被动式：无内置电源，由读写器提供能量；

——主动式：内置电源，可主动发射信号。

6.1.3 按标签存储信息方式分类：

——只读：信息写入后不可更改；

——读写：信息可被读写和更新。

6.1.4 按标签形态分类：

——标签：通常为薄片状，可附着在物品上；

——卡片：如智能卡，具有一定的刚性；

——嵌入型：嵌入在物品内部，不易察觉。

6.1.5 按封装后的物理特性分类：

——柔性标签：采用柔软基材（如纸）封装的射频标签；

——硬性标签：采用具有一定硬度基材（如 PVC、金属等）封装的射频标签。

6.1.6 按读写器类型分类：

——手持式读写器：便携，用于现场操作；

——固定式读写器：安装在特定位置，如门禁系统。

6.2 产品要求

6.2.1 电子标签要求

6.2.1.1 外观要求

电子标签外观至少应符合以下要求：

a) 标签表面应平整光滑，无明显的凹凸不平或损伤；
b) 印刷图案或文字应清晰可辨，无模糊或重影现象；
c) 标签尺寸应精确，边缘整齐，无毛刺或锐边；
d) 色彩应均匀一致，无色差或褪色现象。

6.2.1.2 气候环境

电子标签温、湿度和大气压环境适应性应符合表1的规定。

表 1 温、湿度和大气压环境适应性

气候条件		参数
温度	工作	-10℃～80℃
	贮存运输	-40℃～150℃
相对湿度	工作	5%～95%
	贮存运输	20%～93%(40℃)
大气压		86kPa～106kPa

6.2.1.3 功能要求

6.2.1.3.1 空中接口

应符合GB/T 28925、GB/T 29768、GB/T 33848.3的规定。

6.2.1.3.2 访问功能

应正常清点标签，宜有读取、改写及锁死标签芯片中数据的功能。

6.2.1.3.3 加密功能

应具备数据加密功能，确保信息传输的安全性。

6.2.1.3.4 多标签识别功能

标签应具备基本的应答功能，能够正确响应符合标签相关通讯协议的读写器发出的信号。

6.2.1.4 性能要求

6.2.1.4.1 读写距离

标签的读写距离应在适合工人操作的范围内，且电子标签间不易形成干扰。

6.2.1.4.2 抗干扰能力

标签应能在复杂的电磁环境中稳定工作，不受其他信号的干扰。

6.2.1.4.3 耐久性

标签应能承受日常使用中的物理冲击和磨损。

6.2.1.4.4 快速响应

标签应具备快速的数据处理和响应能力，以适应高速移动物品的识别。

6.2.1.4.5 兼容性

标签应与市场上主流的读写器兼容，支持多种通信协议。

6.2.1.4.6 粘接于金属表面的读写性能

电子标签粘接于各种金属材料上，其标签读性能等于或优于置于空气中的读性能，或满足应用的读写距离需求。

6.2.1.4.7 金属环境中的读写性能

将电子标签置于周围分布有金属的环境下，其标签读性能等于或优于空气中读写性能，或满足应用的读写距离需求。

6.2.1.5 检验规则

6.2.1.5.1 外观检测

目测和手动检查电子标签的外观，应满足6.1.2的要求。

6.2.1.5.2 物理性能试验

6.2.1.5.3 工作温度上下限试验

测试步骤如下：

a) 在低温试验中按照 GB/T 2423.1-2008 的规定进行测试，确保环境温度稳定 2h 后，对标签进行连续读写程序 2h，受试样品应能与读写设备正常信息通信；
b) 在高温试验按 GB/T 2423.2-2008 的规定进行测试，确保环境温度稳定 2h 后，对标签连续读写程序 2h，受试样品应能与读写设备正常信息通信。

6.2.1.5.3.1 恒定湿热

恒定湿热试验应遵循GB/T 2423.3-2016标准进行测试，并需满足以下要求：

a) 试验样品放入温度为室室温的试验箱中，试验箱温度调节至 40℃±2℃、相对湿度控制在 93%±3%，试验持续 24h；
b) 试验结束后，取出试验样品 2h 后，应能正常与读写设备进行信息通信。

6.2.1.5.3.2 随机振动

按照GB/T2423.10-2008要求测试后，结构没有损伤，仍可正常工作。

6.2.1.5.3.3 盐雾

按GB/T 2423.17-2008标准规定的条件进行，盐雾测试后应没有湿气引发的损伤，应能正常工作。

6.2.1.5.4 电气性能

6.2.1.5.4.1 一般要求

电子标签应符合ISO/IEC 18000-63：2013空中接口规定，应支持该标准中的所有强制指令和访问指令，并遵循ISO/IEC 18000-63：2013的多标签防冲突规定。

6.2.1.5.4.2 通信帧格式

电子标签应遵循ISO/IEC 18000-63：2013规定的数据帧格式进行通信，同时支持对标签中不同区域的数据进行读写操作，包括整个或部分保留区、物品标识区、标签标识区以及用户数。

6.2.1.5.4.3 射频一致性要求

电子标签的射频性能应满足ISO/IEC 18000-63：2013中技术条件的要求，包括频率范围、解调能力、占空比以及前导码等方面。

6.2.1.5.4.4 协议一致性要求

电子标签的协议应遵循ISO/IEC 18000-63：2013中技术规范，具体包括标签频偏、时序、响应状态以及标签数据等方面的规定。

6.2.1.5.4.5 静电放电抗扰度

在遵循GB/T 17626.2-2006标准进行测试后，电子标签仍能保持正常工作状态。

6.2.1.5.4.6 射频电磁场抗扰度

在遵循GB/T 17626.3-2016标准进行测试后，电子标签仍能保持正常工作状态。

6.2.1.5.4.7 工频磁场抗扰度

在遵循GB/T 17626.8-2006标准进行测试后，电子标签仍能保持正常工作状态。

6.2.1.5.4.8 粘接于金属表面的读写性能

随机选取50枚电子标签，分别粘接于各种金属材料（纯金属、合金、金属材料金属间化合物和特种金属材料等）上，置于2.0 A/m～7.5 A/m场强内，按厂家给定的读写距离标准，对每个标签进行400次的标签读写测试，总的正确率不低于99.995%。

6.2.1.5.4.9 金属环境中的读写性能

随机选取50枚电子标签，置于周围分布有规则或不规则金属环境下，且分布场强为2.0 A/m～7.5 A/m，按厂家给定的读写距离标准，对每个标签进行400次的标签读写测试，总的正确率不低于99.995%。

6.2.2 读写器要求

6.2.2.1 外观要求

读写器外观至少应符合以下要求：

a) 表面应无显著的凹陷、划痕或裂纹，整体应无变形和污渍；
b) 涂层应平滑且完整，不得有气泡、裂纹、剥落或过度磨损的现象；
c) 金属组件不应有锈蚀及其他机械损伤；
d) 各部件应紧固无松动，确保按钮、开关及其他可动部件操作顺畅且反应灵敏；
e) 产品的标志、铭牌以及功能说明的文字和图标应设计得简洁明了、易于辨认且布局工整。

6.2.2.2 气候环境

读写器温、湿度和大气压环境适应性应符合表2的规定。

表 2 温、湿度和大气压环境适应性

气候条件		参数
温度	工作	-20℃～65℃
	贮存运输	-30℃～70℃
相对湿度	工作	30%～80%
	贮存运输	20%～93%(40℃)
大气压		86kPa～106kPa

6.2.2.3 功能要求

6.2.2.3.1 空中接口

应符合GB/T 28925、GB/T 29768、GB/T 33848.3的规定。

6.2.2.3.2 访问功能

应正常清点标签，宜有读取、改写及锁死标签芯片中数据的功能。

6.2.2.3.3 多标签识别功能

读写器应具备多标签识别能力。

6.2.2.3.4 脱机工作能力

脱机工作方式下的读写器，从标签中读取的信息应能保存在读写器的存储器中。

6.2.2.3.5 显示输出

对于手持式读写器应能处理GB/T 1988和GB/T 2312-1980规定的全部字符。当GB/T 2312-1980不能满足使用时，读写器应支持GB 18030-2005强制部分的要求并应与GB/T 13000-2010相应部分建立映射关系。

6.2.2.3.6 按键

对于手持式读写器，应按功能要求设置必要的工作键。

6.2.2.3.7 通信接口

读写器的串行通信接口应符合GB/T 6107-2000的规定读写器如有USB等其他接口，则该接口应符合相关标准的规定。

6.2.2.3.8 其他要求

移动式读写器还应具有数据存储、导入和导出等功能。

6.2.2.4 性能要求

6.2.2.4.1 存储器

读写器的存储容量应符合应用要求。

6.2.2.4.2 最大发射功率

读写器最大发射功率为100mW(EIRP)。

6.2.2.4.3 接收灵敏度

在误码率为10^{-5}的条件下，读写器接收信号的最小功率应＜-60dBm。

6.2.2.5 检验规则

6.2.2.5.1 检验分类

RFID读写器的检验分为出厂检验和型式检验。

6.2.2.5.2 出厂检验

RFID读写器必须经过出厂检验合格，并且由企业质量管理部门出具合格证明后，方可出厂。出厂检验的抽检项目包括传输功能与性能、结构尺寸与外观、抗电强度、接触电流与保护导体电流检测、保护接地措施检测、贮存与运输环境要求等，以确保产品的质量符合要求。

RFID读写器的出厂检验抽样应遵循GB/T 2828.1-2012的统计抽样检验规定，采用正常检验一次抽样方案。不同项目的检查水平与合格质量水平应符合相应的成品检验标准。

定期检验合格的产品如超过贮存期，应尽快处理并考虑促销方案以促进及时出货（RFID读写器额定使用寿命为1年，超过贮存期的产品可能存在失效风险）；对于检验不合格的产品应进行评审并报废处理。

6.2.2.5.3 型式试验

6.2.2.5.3.1 RFID 读写器处于以下任一情况时，应进行型式检验：

a) 在产品试制定型或定型鉴定时；
b) 在正式生产后，当产品的结构、材料、工艺等发生较大改变并可能影响性能时；
c) 当产品长期停产后重新恢复生产时；
d) 当出厂检验结果与上次型式检验结果有较大差异时；
e) 根据国家或公司有关产品质量监督机构的要求或合同规定等。

6.2.2.5.3.2 检验内容

型式检验是对样品进行全面质量考核的试验，涵盖常温性能、电磁兼容性和环境适应性等方面的测试。

6.2.2.5.3.3 检验判定

定型检验中，如果各检验项目出现故障或某项无法通过时，应立即停止试验，并查明故障原因，提出故障分析报告，并在故障排除后重新进行该项试验。如果在后续的检验中再次遇到故障或某项无法通过时，应在查明故障原因，排除故障并提交故障分析报告后，重新进行定型试验。完成检验后，应提交定型检验报告。

6.2.2.5.3.4 检验样品处理

经过出厂检验后，合格样品可作为合格产品交付给订货方。而经型式检验的样品则不能作为合格产品交付给订货方。

6.2.3 射频天线要求

6.2.3.1 技术要求

6.2.3.1.1 外观质量要求

射频天线的连接线条应均匀、平整，无白斑、明显拖影和水渍等残留物，并且应无明显毛边和缺口等现象。见表3。

表 3 外观质量

项目	指标
外观	无明显毛边，缺口
残留物	无白斑及明显拖影，水渍等
连接线条	无短路和开路
针眼	单个针眼直径小于0.2mm，分布在0.03mm-0.2的针眼≤8个

6.2.3.1.2 尺寸偏差

6.2.3.1.2.1 宽度偏差

宽度尺寸允许公差要求为±0.2mm。

6.2.3.1.2.2 天线线宽偏差

天线线宽的公差范围为±0.08mm。

6.2.3.1.2.3 剥离强度

使用百格刀进行测试，剥离强度等级需达到1级或以上。

6.2.3.1.2.4 热收缩率

热收缩率要求纵向不超过2.0%，横向不超过2.0%。

6.2.3.1.2.5 拉伸强度

拉伸强度方面，纵向≥160MPa，横向≥160MPa。

6.2.3.1.3 直流电阻

直流电阻≤3Ω。

6.2.3.2 环境条件

试验应在温度23±2℃和相对湿度50±10%的环境下进行，并在此条件下对样品进行至少16h以上的预处理。

6.2.3.3 检验规则

6.2.3.3.1 外观检查

在自然光线或40w日光灯下用目测方法进行，应符合6.3.1.1的要求。

6.2.3.3.2 尺寸测量

6.2.3.3.2.1 宽度

使用分度值为0.01mm的读数显微镜分别测量受检产品的天线线宽。

6.2.3.3.2.2 线宽测量

使用分度值为0.01mm的读数显微镜分别测量受检产品的天线线宽。

6.2.3.3.2.3 天线线间距及绑定间距测量

使用分度值为0.01mm的读数显微镜分别测量受检产品的天线线间距及绑定间距。

6.2.3.3.3 剥离强度测试

射频天线的剥离强度测试按照、GB/T 9286规定的方法，在平衡过的试样上用百格刀进行测试。

注：平衡方法为对成卷的产品应先弃去片卷外层至少2～3层，然后剪去150mm的全宽样片作为试样，并按6.3.2规定的条件进行平衡15h以上。

6.2.3.3.4 拉伸强度测试

按GB/T 1040.3规定进行试验，试验采用2型试样，从5.1平衡过的试样中剪切成150mm×15mm的长条形，夹具间距为100mm，试验速度为100mm/min±10%。分别测试纵向、横向试验条5条，各取其平均值。

6.2.3.3.5 直流电阻测试

将测试导线连接至天线和直流电阻电桥，对电桥进行机械和电气调零，以确保测量的准确性。这一过程需持续至表头指针精确对准0刻度线，标志着调零完成。进入读数盘的调节阶段。初始步骤是将测量读数盘定位至被测电阻的预估值附近。通过细致旋转读数盘，使指零仪表的指针向左偏移，直至接近0刻度。若指针向左偏离，这表明当前刻度盘的读数偏高，需要向下微调一格以校准。继续这一过程，依次对每一个读数盘进行精细调节，直至表头指针完美指向0刻度，确保了测量的精确性。最终，将所有读数盘上的示值进行累加，并乘以相应的倍率，从而得出天线的直流电阻值。

6.2.3.3.6 盐雾试验

射频天线的盐雾试验按GB/T 10125中规定的中性盐雾进行测试。

7 数据安全

7.1 安全威胁

射频识别（RFID）技术因其开放架构而具有固有的脆弱性，容易受到外部威胁。这些威胁贯穿了整个系统，包括数据的收集、传输、处理和存储等关键环节。RFID系统由电子标签、读写设备、管理组件以及它们之间的通信路径组成，这些组件在无线通信和网络传输过程中都可能遭遇安全问题。

7.2 安全技术要求

7.2.1 电子标签安全

7.2.1.1 基本级要求

7.2.1.1.1 标签唯一性

电子标签应具有不可更改的唯一标识。

7.2.1.1.2 灭活（仅适用于 800/900 MHz、2.45 GHz 频段的电子标签）

电子标签应具有灭活功能。灭活应符合以下技术要求：

a） 电子标签在接收到包含灭活口令的特殊指令后进入灭活状态；
b） 灭活状态的电子标签不再响应任何外部指令；
c） 灭活口令受灭活密钥控制。
注：不适用于125 kHz、133 kHz、13.56 MHz频段的电子标签。

7.2.1.1.3 基于口令验证的访问控制

电子标签应具备基于口令验证的访问控制。基于口令验证的访问控制应符合以下要求：
a） 仅允许通过口令验证的阅读器/读写器访问其用户区；
b） 口令具有复杂度策略要求；
c） 同一电子标签的不同存储区域的访问口令各不相同；
d） 不同电子标签的访问口令各不相同。

7.2.1.1.4 信息防篡改

电子标签应能防止其存储数据被未经授权的攻击者篡改。

7.2.1.1.5 防非法指令

电子标签应仅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。

7.2.1.1.6 随机数产生

电子标签应具备随机数发生器。随机数发生器应能够产生长度与密码算法分组长度一致的随机数且随机数二元序列随机性符合GB/T 32915中的符合性结果判定。

7.2.1.1.7 基于密码技术验证的访问控制（仅适用于主动标签）

电子标签应仅允许通过密码技术验证的阅读器/读写器访问其存储区。不同电子标签或同一电子标签的不同存储区域所用的密钥宜各不相同。

7.2.1.1.8 片内程序更新的完整性保护（仅适用于主动标签）

电子标签应具备片内程序更新完整性校验功能。

7.2.1.2 增强级要求

7.2.1.2.1 完整性服务

电子标签应具备对其传输的数据提供完整性服务的能力。

7.2.1.2.2 前向安全性

电子标签应具备前向安全性。当电子标签中的密钥泄露时，前向安全性功能应能使电子标签之前与阅读器/读写器交互的消息仍然安全。

7.2.1.2.3 具有基于算法的访问控制

电子标签应仅允许通过基于算法的身份鉴别协议验证的阅读器/读写器访问其存储区。不同电子标签或同一电子标签的不同存储区域的密钥宜各不相同。

7.2.1.2.4 敏感信息保护、销毁和管理

电子标签应具有敏感信息保护、销毁和管理功能。敏感信息保护、销毁和管理应符合以下技术要求：
a） 支持带校验的敏感信息加密存储；
b） 对允许读取的敏感信息，提供安全机制保证敏感信息明文只在电子标签内部进行处理；
c） 清除标签内敏感信息时不透露敏感信息本身。

7.2.1.2.5 基于算法的数据加密（仅适用于主动标签）

电子标签应对存储在内的敏感信息采用加密算法进行加密保护。加密算法应符合GB/T 37033—2018（所有部分）中的规定。

7.2.1.2.6 数据校验（仅适用于主动标签）

电子标签应对传输的数据进行完整性校验，防止数据被篡改、删除或插入。

7.2.1.2.7 签名服务（仅适用于主动标签）

当电子标签作为数据的原发方时，应能够对所发送数据生成数字签名；当电子标签作为阅读器/读写器数据的接收方时，应能够验证阅读器/读写器的签名数据。

7.2.2 读写器安全

7.2.2.1 基本级要求

7.2.2.1.1 标识唯一性

读写器应具有不可更改的唯一性标识。

7.2.2.1.2 基于口令验证的身份鉴别

读写器应采用具有复杂度策略要求的口令验证对读写电子标签信息等操作进行身份鉴别。对不同的操作权限应设置不同的口令。

7.2.2.1.3 基于密码技术验证的访问控制（仅适用于读写半主动标签和主动标签的读写器）

读写器应采用密码技术验证对电子标签信息读写、密钥存储与更新等操作设置控制权限不同权限需分配独立密钥，防止未授权访问。加密算法应符合GB/T 37033—2018（所有部分）中的规定。

7.2.2.1.4 授权的程序装载与更新

阅读器/读写器应具有授权的程序装载与更新功能。

7.2.2.1.5 初始化权限控制

读写器应对电子标签的初始化信息设定控制权限。

7.2.2.1.6 完整性服务

读写器对与电子标签之间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。

7.2.2.1.7 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长度与密码算法分组长度一致的随机数且随机数二元序列随机性符合GB/T 32915中的符合性结果判定。

7.2.2.1.8 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。阅读器/读写器应对敏感信息的访问设置相应权限。

7.2.2.1.9 审计日志

7.2.2.2 增强级要求

7.2.2.2.1 基于算法的访问控制

阅读器/读写器应具有基于算法的访问控制功能。基于算法的访问控制应符合以下要求：

a) 阅读器/读写器采用加密算法对读写标签信息、密钥存储、密钥更新等操作设置控制权限；
b) 对不同的权限设置不同的密钥进行访问控制；
c) 能阻止所有非授权的访问；
d) 加密算法符合 GB/T 37033-2018（所有部分）中的规定。

7.2.2.2.2 基于算法的数据加密功能

阅读器/读写器应具有基于算法的数据加密功能。基于算法的数据加密应符合以下要求：

a) 采用加密算法对存储的敏感信息进行加密保护，防止敏感信息非授权泄露；
b) 采用加密算法对传输的敏感信息进行加密保护；
c) 加密算法符合 GB/T 37033-2018（所有部分）中的规定。

7.2.2.2.3 签名服务功能

阅读器/读写器应具有签名服务功能。签名服务应符合以下技术要求：

a) 当阅读器/读写器作为信息的原发者时，阅读器/读写器对向电子标签传输的数据产生数字签名；
b) 当阅读器/读写器作为电子标签签名信息的验证主体时，阅读器/读写器能够验证电子标签的签名数据。

7.2.2.2.4 审计日志机密性保护

阅读器/读写器应采用安全的加密算法对存储的审计日志进行加密保护。加密算法应符合 GB/T 37033-2018（所有部分）中的规定。

7.2.2.2.4.1 审计数据生成

读写器应能生成电子标签的读取或写入及管理单元接入情况等审计数据。

7.2.2.2.4.2 日志内容

读写器生成的审计日志应至少包含以下内容：

a) 电子标签的读取或写入日期或时间；
b) 配置管理；
c) 阅读器/读写器的注册、注销；
d) 阅读器/读写器的在线、离线状态；
e) 设备故障；
f) 设备更新；
g) 其他可审计信息。

7.2.2.2.4.3 授权查阅

读写器应设置审计日志查阅权限，确保仅授权人员能对审计日志进行查阅。

7.2.2.2.4.4 数据完整性保护

读写器应具备数据完整性保护机制，确保存储的日志信息不被篡改、伪造和恶意删除。

7.2.3 通信链路（空中接口）安全

7.2.3.1 基本级要求

7.2.3.1.1 数据完整性

系统应采用数字校验技术保证通信链路（空中接口）传输过程中的数据完整性。

7.2.3.1.2 数据源可追溯性

系统应保障通信链路（空中接口）中传输的数据信息来源可追溯。

7.2.3.2 增强级要求

7.2.3.2.1 数据完整性

系统应采用密码算法保证通信链路（空中接口）传输过程中的数据完整性。

7.2.3.2.2 数据保密性

系统应对通信链路（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GB/T 37033—2018（所有部分）中的规定。

7.2.3.2.3 数据时效性

系统应具有通信链路（空中接口）数据时效性。通信链路（空中接口）数据时效性应符合以下要求：

a) 通信链路（空中接口）中传输的数据信息包含数据发布的系统时间信息；
b) 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；
c) 实现时间信息防篡改保护的加密算法符合 GB/T 37033—2018（所有部分）中的规定。

7.2.3.2.4 抗抵赖

系统通信链路（空中接口）传输的数据应具有抗电子标签抵赖、抗电子标签原发抵赖、抗读写器抵赖功能。

7.2.4 通信链路（网络传输）安全

7.2.4.1 基本级要求

7.2.4.1.1 数据保密性

系统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。

7.2.4.1.2 数据完整性

系统应具有通信链路（网络传输）数据完整性。通信链路（网络传输）数据完整性应符合以下要求：

a) 采用校验技术保证通信链路（空中接口）传输过程中的数据完整性；
b) 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）中的完整性受到破坏时能够检测到并发出提示。

7.2.4.2 增强级要求

7.2.4.2.1 数据时效性

系统应具有通信链路（网络传输）数据时效性。通信链路（网络传输）数据时效性应符合以下要求：

a) 通信链路（网络传输）中传输的数据信息包含数据发布的系统时间信息；
b) 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；
c) 实现时间信息防篡改保护的密码算法符合国家密码有关标准。

7.2.4.2.2 数据源可追溯性

系统应具有通信链路（网络传输）数据源可追溯性。通信链路（网络传输）数据源可追溯性应符合以下要求：

a) 采用数字签名和校验机制来实现保障通信链路（网络传输）中传输的数据信息来源可追溯；
b) 数字签名算法符合国家密码有关标准。

7.2.4.2.3 抗抵赖

系统通信链路（网络传输）传输的数据应具有抗读写器抵赖功能。

7.2.5 管理单元安全

7.2.5.1 基本级要求

7.2.5.1.1 身份鉴别

管理单元应具备身份鉴别功能。身份鉴别应符合以下技术要求：

a) 采用唯一标识符对每个接入的阅读器/读写器进行身份鉴别，通过身份鉴别的阅读器/读写器才能接入管理单元；
b) 对登录系统管理软件的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
c) 具有登录失败处理功能，配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

7.2.5.1.2 访问控制

管理单元应具有访问控制功能。访问控制应符合以下要求：

a) 通过访问控制列表对登录系统管理软件的用户分配账户和权限，提供明确的访问保障能力和拒绝访问能力；
b) 支持重命名或删除默认账户，修改默认账户的默认口令；
c) 支持及时删除或停用多余的、过期的账户，避免共享账户的存在。

7.2.5.1.3 授权的程序装载与更新

管理单元应具有授权的程序装载与更新功能。

7.2.5.1.4 数据完整性保护

管理单元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。

7.2.5.1.5 状态监测

管理单元应能监测阅读器/读写器等设备的在线和运行状态。

7.2.5.1.6 密码算法

管理单元相关功能所使用的密码算法应符合国家密码有关标准。

7.2.5.1.7 恶意代码防范

管理单元应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

7.2.5.1.8 可信验证

管理单元应可基于可信根对计算设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

7.2.5.1.9 数据备份恢复

管理单元应提供重要数据的本地数据备份与恢复功能。

7.2.5.1.10 审计日志

7.2.5.1.10.1 审计数据生成

管理单元应能对阅读器/读写器的接入操作、运行情况、操作事件、用户行为记录等生成审计日志。

7.2.5.1.10.2 记录内容

管理单元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。

7.2.5.1.10.3 授权查阅

管理单元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。

7.2.5.2 增强级要求

7.2.5.2.1 访问控制

管理单元应具有访问控制功能。访问控制应符合以下要求：

a) 在网络边界根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
b) 删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
c) 对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
d) 能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

7.2.5.2.2 数据完整性

管理单元应采用校验技术保证组件之间通信过程中的数据完整性。

7.2.5.2.3 数据保密

管理单元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。

7.2.5.2.4 可信验证

管理单元应可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

7.2.5.2.5 数据流控制

管理单元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。

7.2.5.2.6 抗攻击

管理单元应具备DoS/DDoS攻击防护功能并识别和防御SYN Flood、ICMP Flood等攻击。

7.2.5.2.7 安全报警

管理单元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。

7.2.5.2.8 报警方式

管理单元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。

7.2.5.2.9 入侵防范

管理单元应在关键网络节点处监视网络攻击行为。

7.2.5.2.10 恶意代码防范

管理单元应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

7.2.5.2.11 可恢复性

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

7.2.5.2.12 安全审计

管理单元应具备安全审计功能。安全审计应符合以下要求：

a) 在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b) 审计记录包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

附 录 A
（规范性附录）
测试环境要求

A.1 一般要求

射频识别安全性测试应遵循以下要求：

a) 测试过程中涉及 13.56 MHz 频段射频识别系统的，空中接口协议默认按照 GB/T 33848.3 的要求；
b) 测试过程中涉及 800/900 MHz 频段射频识别系统的，空中接口协议默认按照 GB/T 29768 的要求；
c) 测试过程中涉及 2.45 GHz 频段射频识别系统的，空中接口协议默认按照 GB/T 28925 的要求；
d) 测试前先确认进行安全符合性测试所需的指令和通信参数；
e) 符合国家密码有关标准的密码算法包括但不限于符合 GB/T 37033.1、GB/T 37033.2、GB/T 37033.3 的射频识别系统密码；
f) 电子标签安全要求测试优先选择基准阅读器/读写器作为测试设备；
g) 阅读器/读写器安全要求测试优先选择基准电子标签作为测试设备；
h) 当 f）、g）项条件不具备时，采用射频信号发生器向被测电子标签或被测阅读器/读写器发射模拟基准阅读器/读写器或模拟基准电子标签射频信号，采用射频分析仪或频谱分析仪接收被测电子标签或被测阅读器/读写器发射的射频信号方式进行测试。

A.2 测试环境

除气候环境适应性试验外，所有试验均在下述环境条件下进行：

——环境温度：15℃～35℃；

——相对湿度：45%～85%；

——大气压力：86 kPa～106 kPa。

A.3 测试条件

除另有规定外，电子标签、阅读器/读写器测试应在电波暗室中进行。当且仅当电波暗室限制了被测件的摆放和测试距离时，允许测试在开阔测试环境下进行。开阔测试环境下选择测试位置时应预先排除杂散辐射影响。在测试场地中，所选择的测试位置的噪声电平需符合以下要求：

a) 10 kHz 测试带宽下，0.5 GHz～2 GHz 频率范围内的噪声电平≤-60 dBm；
b) 在 2 MHz 测试带宽下，0.5 GHz～5 GHz 频率范围内的噪声电平≤-60 dBm；

c） 800 MHz～960 MHz 工作频率范围内的噪声电平≤-90 dBm；
d） 2.4 GHz～2.5 GHz 工作频率范围内的噪声电平≤-101 dBm。

A.4 通用测试设备

A.4.1 基准阅读器/读写器

基准阅读器/读写器应符合以下要求：
a） 支持对应频段的相关协议及制造商规定的空中接口指令；
b） 支持编辑相关协议及制造商规定的命令序列；
c） 支持相关加密命令以及密钥的输入。

A.4.2 基准电子标签

基准电子标签应符合以下要求：
a） 支持对应频段的相关协议及制造商规定的空中接口指令响应；
b） 支持相关加密命令以及密钥的输入。

A.4.3 射频信号发生器

射频信号发生器应符合以下要求：
a） 能够发射至少包括用于射频识别技术的 13.56 MHz 频段、800 MHz～960 MHz 频段、2.4 GHz～2.5 GHz 频段的任意射频信号；
b） 能够和频谱分析仪同步；
c） 在接收到触发射频信号时立即发送相应频段射频信号；
d） 相位噪声优于-95 dBc/Hz（10 kHz 频偏）；
e） 数字量化不低于 14 位；
f） 谐波和杂散不高于-30 dBc。

A.4.4 射频分析仪

测试用射频分析仪应符合以下要求：
a） 至少内置频谱分析仪、干扰分析仪和天馈线分析仪；
b） 内置频谱分析仪工作频率范围支持用于射频识别技术的 13.56 MHz 频段、800 MHz～960 MHz 频段、2.4 GHz～2.5 GHz 频段，输入频率范围 100 kHz～3 GHz 内的平均噪声电平小于等于-10 dBm，分析带宽小于等于 25 MHz；
c） 内置干扰分析仪可追踪的指定频点覆盖用于射频识别技术的 13.56 MHz 频段、800 MHz～960 MHz 频段、2.4 GHz～2.5 GHz 频段，能定位和识别正常工作的周期性或突发性信号，并给出干扰信号的信号带宽和波形轮廓；
d） 内置天馈线分析仪支持用于射频识别技术的 13.56 MHz 频段、800 MHz～960 MHz 频段、2.4 GHz～2.5 GHz 频段，频率分辨率小于等于 100 kHz，驻波比范围：1～65 dB。

A.4.5 频谱分析仪

测试用频谱分析仪应符合以下要求：
a） 工作频率范围支持用于射频识别技术的 13.56 MHz 频段、800 MHz～960 MHz 频段、2.4 GHz～2.5 GHz 频段；
b） 支持时域分析和 I/Q 分析模式；
c） 分析带宽小于等于 25 MHz；
d） 采样时间大于 80 ms；
e） 普通攻击持续输出核心（ADC）采样率至少 90 MSa/s，分辨率至少 10 位；
f） 10 MHz～3.6 GHz 频率范围内的平均噪声电平（DANL）≤-120 dBm。

附 录 B
（规范性附录）
测试评价方法

B.1 电子标签安全测试评价

B.1.1 基本级要求测试评价

B.1.1.1 标识唯一性测试

标识唯一性的测试评价方法如下：

a) 测试方法：
   1) 控制基准阅读器/读写器读取被测电子标签 TID 数据；
   2) 控制基准阅读器/读写器向被测电子标签写入新 TID 数据；
   3) 控制基准阅读器/读写器再次读取被测电子标签 TID 数据。
b) 预期结果：
   1) 读取出被测电子标签 TID 数据；
   2) 无法往被测电子标签写入新 TID 数据；
   3) 再次读取被测电子标签 TID 数据与首次读取相同。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.1.2 灭活测试（仅适用于 800/900 MHz、2.45 GHz 频段的电子标签）

灭活的测试评价方法如下：

a) 测试方法：
   1) 控制基准阅读器/读写器读取被测电子标签，确认电子标签工作正常；
   2) 输入错误的灭活密钥获取口令；使用所获取的口令控制基准读写器灭活被测电子标签；
   3) 输入正确的灭活密钥获取口令；使用所获取的口令控制基准读写器灭活被测电子标签；
   4) 控制基准阅读器/读写器读取被测电子标签，确认电子标签是否响应指令。
b) 预期结果：
   1) 使用错误灭活密钥获取口令灭活失败；
   2) 使用正确灭活密钥获取口令灭活成功；
   3) 灭活成功后再次读取被测电子标签，电子标签不响应指令。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.1.3 基于口令验证的访问控制测试

基于口令验证的访问控制的测试评价方法如下：

a) 测试方法：
   1) 控制基准阅读器/读写器向至少 2 只被测电子标签各个存储区域写入非 0 数据；
   2) 分别使用正确口令和错误口令擦除、写入和读取存储区域 1 数据，检验执行结果是否成功或失败；
   3) 如果有多个用户存储区域，对其他各个用户存储区域重复步骤1）、2）。
b) 预期结果：
   1) 使用正确口令擦除、写入和读取电子标签用户区数据成功；
   2) 使用错误口令擦除、写入和读取电子标签用户区数据失败；
   3) 使用各不相同的口令才能擦除、写入和读取同一电子标签的不同存储区域；
   4) 使用各不相同的口令才能擦除、写入和读取电子标签的用户区数据。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.1.4 信息防篡改测试

信息防篡改的测试评价方法如下：

a) 测试方法：

1） 控制基准阅读器/读写器对被测电子标签进行安全鉴别，采用正确口令读取用户区数据备用；
2） 下电－上电或发送休眠－唤醒命令，上电或唤醒前等待时间大于被测电子标签空口协议规定的状态复位时间，如无规定，时间不小于2 s；
3） 控制基准阅读器/读写器命令电子标签进入确认模式或会话模式；
4） 不进行安全鉴别，采用正确口令对用户区数据擦除和写入，检验操作是否失败；
5） 进行安全鉴别，采用正确口令读取用户区数据与步骤 1）数据比较是否相同。

b） 预期结果：
1） 不进行安全鉴别对用户区数据擦除、写入失败；
2） 擦除、写入失败后数据信息保持不变。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.1.5 防非法指令测试

防非法指令的测试评价方法如下：

a） 测试方法：
1） 向被测电子标签供应商获取空口协议符合性申明，包括是否设计了私有指令集；
2） 控制基准阅读器/读写器向被测电子标签发送不符合GB/T 33848.3、GB/T 29768、GB/T 28925及私有指令集的非法指令，检验被测电子标签是否响应。

b） 预期结果：

被测电子标签对全部非法指令都不响应。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.1.6 随机数产生测试

随机数产生的测试评价方法如下：

a） 测试方法：
1） 控制基准阅读器/读写器使用正确口令和身份鉴别协议读取被测电子标签存储区，获取被测电子标签随机数；
2） 重复步骤1）直到采集到至少1000个样本；
3） 检查随机数长度与密码算法分组长度的一致性；
4） 按照GB/T 32915检测随机数发生器产生的二元序列的随机性。

b） 预期结果：
被测电子标签产生的随机数长度与密码算法分组长度一致且随机数二元序列的随机性符合GB/T 32915中的符合性结果判定。

c） 结果判定：上述预期结果满足判定为符合，其他情况判定为不符合。

B.1.1.7 具有基于密码技术验证的访问控制测试（仅适用于主动标签）

具有基于密码技术验证的访问控制的测试评价方法如下：

a） 测试方法：
1） 控制基准阅读器/读写器不使用身份鉴别协议读取被测电子标签存储区；
2） 控制基准阅读器/读写器使用身份鉴别协议，使用错误密码读取电子标签存储区；
3） 控制基准阅读器/读写器使用身份鉴别协议，使用正确密码读取电子标签存储区。

b） 预期结果：
1） 不使用身份鉴别协议无法读取电子标签存储区；
2） 使用身份鉴别协议，使用错误密码无法读取电子标签存储区；
3） 使用身份鉴别协议，使用正确密码可以读取电子标签存储区。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.1.8 片内程序更新的完整性保护测试（仅适用于主动标签）

片内程序更新的完整性保护的测试评价方法如下：

a) 测试方法：
   1) 向被测电子标签供应商获取片内程序数据包，修改该数据包内容，可以在任意位置修改一个字节；
   2) 控制基准阅读器/读写器向被测电子标签发起程序更新，下载修改过的数据包，检验程序更新是否失败；
   3) 控制基准阅读器/读写器向被测电子标签发起程序更新，下载原版数据包，检验程序更新是否成功。
b) 预期结果：
   1) 下载修改过的数据包，程序更新失败；
   2) 下载原版数据包，程序更新成功。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.2 增强级要求测试评价

B.1.2.1 完整性服务测试

完整性服务的测试评价方法如下：

a) 测试方法：
   1) 控制基准阅读器/读写器向被测电子标签数据区写入测试数据；
   2) 遍历被测电子标签读取信息的指令，检验被测电子标签传输回应的校验码和数据是否正确。
b) 预期结果：
   1) 每个指令对应的被测电子标签传输回应的数据正确；
   2) 被测电子标签传输回应的校验码正确。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.2.2 前向安全性测试

前向安全性的测试评价方法如下：

a) 测试方法：
   1) 控制基准阅读器/读写器向被测电子标签用户数据区写入测试数据；
   2) 读取被测电子标签用户区数据并采集电子标签应答数据包；
   3) 控制基准阅读器/读写器向被测电子标签发送下电－上电或休眠－唤醒命令，上电或唤醒前等待时间大于被测电子标签空口协议规定的状态复位时间，如无规定，时间不小于2秒；
   4) 再次读取被测电子标签用户区数据并采集被测电子标签应答数据包；
   5) 比对两次被测电子标签应答数据包内容，检验是否相同。
b) 预期结果：
   被测电子标签两次应答返回相同信息数据所对应的物理层数据不同。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.2.3 具有基于算法的访问控制测试

具有基于算法的访问控制的测试评价方法如下：

a) 测试方法：
   1) 控制基准阅读器/读写器向至少2只被测电子标签各个存储区域写入非0的数据；
   2) 进入会话状态后，使用错误的加密算法进行身份鉴别，检验是否鉴别失败；
   3) 使用正确密钥和算法进行身份鉴别，建立安全会话，并读取存储区域1数据，检验是否执行成功、读取数据是否正确，采集分析会话密钥物理层数据；
   4) 如果有多个用户存储区域，对其他各个用户存储区域重复步骤1）、2）、3）。
b) 预期结果：
   1) 错误加密算法鉴别失败；
   2) 正确加密算法鉴别成功；

3） 读取存储区域正确；
4） 会话密钥物理层数据不同。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.2.4 敏感信息保护、销毁和管理测试

敏感信息保护、销毁和管理的测试评价方法如下：

a） 测试方法：
1） 控制基准阅读器/读写器向被测电子标签用户区的敏感数据区域写入预先设定的数据，监听记录被测电子标签回应的物理层数据，检验物理层数据是否为明码原始数据；
2） 控制基准阅读器/读写器从被测电子标签读取上一步骤写入的数据，监听记录被测电子标签回应的物理层数据，检验物理层数据是否为明码原始数据；
3） 控制基准阅读器/读写器将被测电子标签上述被检验区域数据删除，监听记录被测电子标签回应的物理层数据，检验物理层数据是否包含明码原始数据；
4） 对被测电子标签中的所有敏感数据区域重复步骤1）、2）、3）。

b） 预期结果：
被测电子标签所有敏感数据区域的写入、读取、删除会话中，监听记录被测电子标签回应的物理层数据均不是明码原始数据。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.2.5 基于算法的数据加密测试（仅适用于主动标签）

基于算法的数据加密的测试评价方法如下：

a） 测试方法：
1） 向被测电子标签供应商获取基准阅读器/读写器或者和基准阅读器/读写器兼容的加密算法计算装置；
2） 进入安全会话状态后，控制安装加密算法计算装置的合法基准阅读器/读写器读取被测电子标签敏感信息；
3） 修改被测电子标签加密密钥，再控制合法阅读器/读写器读取被测电子标签敏感信息；
4） 控制非合法阅读器/读写器读取被测电子标签敏感信息；
5） 控制射频分析仪或频谱分析仪采集合法基准阅读器/读写器和被测电子标签之间的空中传输数据。

b） 预期结果：
1） 合法基准阅读器/读写器可读取被测电子标签敏感信息；
2） 修改被测电子标签加密密钥后，合法基准阅读器/读写器无法读取被测电子标签敏感信息；
3） 非合法阅读器/读写器无法读取被测电子标签敏感信息；
4） 采集的合法基准阅读器/读写器和被测电子标签之间的空中传输数据经过加密算法加密。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.2.6 数据校验测试（仅适用于主动标签）

数据校验的测试评价方法如下：

a） 测试方法：
1） 控制基准读写器向被测电子标签用户区写入数据，并读取数据，检验写入和读出指令是否成功，数据是否一致；
2） 控制基准读写器向被测电子标签写入另一组数据，同步用射频信号发生器发送与写入数据包同步的一个干扰脉冲，使得被测电子标签接收到的数据有一个比特误码，用射频分析仪分析应答过程，确认干扰是否有效，被测电子标签是否返回校验失败回应。

b） 预期结果：
1） 基准读写器向被测电子标签写入和读取数据指令成功，数据一致；
2） 干扰有效，被测电子标签返回校验失败回应。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.1.2.7 签名服务测试（仅适用于主动标签）

签名服务的测试评价方法如下：

a) 测试方法：
   1) 控制基准阅读器/读写器读取被测电子标签；
   2) 用射频分析仪分析会话过程，检查被测电子标签接收基准阅读器/读写器的读取指令时，是否验证基准阅读器/读写器的签名数据，并检查被测电子标签回应的原发数据中是否包含数字签名信息；
   3) 当电子标签作为数据的原发方时，应能够对所发送数据生成数字签名；当电子标签作为阅读器/读写器数据的接收方时，应能够验证阅读器/读写器的签名数据。
b) 预期结果：
   1) 被测电子标签接收基准阅读器/读写器的读取指令时，验证了基准阅读器/读写器的签名数据；
   2) 被测电子标签回应的原发数据中包含数字签名信息；
   3) 基准阅读器/读写器和被测电子标签的会话过程包含数字签名发送与验证。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

B.2 阅读器/读写器安全测试评价

阅读器/读写器安全测试方法按照GB/T 35290-2023第9.2节的规定实施。

B.3 通信链路（空中接口）安全测试评价

通信链路（空中接口）安全测试方法按照GB/T 35290-2023第9.3节的规定实施。

B.4 通信链路（网络传输）安全测试评价

通信链路（网络传输）安全测试方法按照GB/T 35290-2023第9.4节的规定实施。

B.5 管理单元测试评价

管理单元测试方法按照GB/T 35290-2023第9.5节的规定实施。