



中华人民共和国密码行业标准

GM/T 0097—2020

射频识别电子标签统一名称 解析服务安全技术规范

Security technical specifications for unified name resolution
service of RFID

2020-12-28 发布

2021-07-01 实施

国家密码管理局 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号和缩略语	2
4.1 符号	2
4.2 缩略语	2
5 电子标签编码	3
6 ONS 系统架构	3
7 ONS 系统关键业务流程	3
7.1 ONS 服务器注册	3
7.2 安全查询处理	4
8 安全性要求	5
8.1 密码算法	5
8.2 随机数安全	5
8.3 密钥管理安全	5
8.3.1 总体要求	5
8.3.2 密钥种类及用途	5
8.3.3 密钥结构	6
8.3.4 密钥生成	6
8.3.5 密钥分发	6
8.3.6 密钥存储	6
8.3.7 密钥更新	7
8.3.8 密钥备份和恢复	7
8.3.9 密钥销毁	7
8.4 硬件安全	7
8.5 软件安全	7
附录 A (资料性附录) 射频识别电子标签统一编码规则	8
附录 B (规范性附录) ONS 服务器注册流程	9
附录 C (规范性附录) 消息协议规范	11
附录 D (规范性附录) 安全查询处理流程	15

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：中国电力科学研究院有限公司、成都卫士通信息产业股份有限公司、北京智芯微电子科技有限公司、上海复旦微电子集团股份有限公司、北京中电华大电子设计有限责任公司、南方电网科学研究院。

本标准主要起草人：赵兵、许斌、梁晓兵、吕英杰、翟峰、刘鹰、李保丰、曹永峰、孔令达、徐萌、冯云、罗俊、胡川、付建峰、绍兴、杨祎巍、兰天。

射频识别电子标签统一名称 解析服务安全技术规范

1 范围

本标准规定了射频识别电子标签统一名称解析服务的系统架构、关键业务流程和安全性要求,定义了名称解析服务器的注册流程、产品电子代码的安全查询流程及相应消息报文格式。

本标准适用于射频识别电子标签统一名称解析服务系统的开发和使用的。

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 17901.1 信息技术 安全技术 密钥管理 第1部分:框架
 GB/T 32905 信息安全技术 SM3 密码杂凑算法
 GB/T 32907 信息安全技术 SM4 分组密码算法
 GB/T 32915 信息安全技术 二元序列随机性检测方法
 GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法
 GB/T 35276—2017 信息安全技术 SM2 密码算法使用规范
 GM/Z 4001—2013 密码术语

3 术语和定义

GM/Z 4001—2013 界定的以及下列术语和定义适用本文件。

3.1

产品电子代码 electronic product code

存储在 RFID 标签上,为物品提供唯一标识。

3.2

产品电子代码应用系统 electronic product code application system

为访问和持久保存产品电子代码相关数据提供了一个标准的接口,已授权用户可以通过它来读写产品电子代码相关数据,具有高度复杂的数据存储与处理过程,支持多种查询方式。

3.3

产品电子代码信息服务器 electronic product code information service server

保存物品详细信息的服务器,一般由生产商或者产品使用者管理和维护。

3.4

名称解析服务 object name service

提供产品电子代码与存放物品具体信息的服务地址之间的映射关系。

3.5

密钥 key

控制密码变换操作的关键信息或参数。