



# 中华人民共和国国家标准

GB/T 38660—2020

---

## 物联网标识体系 Ecode 标识系统安全机制

Identification system for internet of things—  
Security mechanism for Ecode identification system

2020-03-31 发布

2020-10-01 实施

---

国家市场监督管理总局 发布  
国家标准化管理委员会

目 次

前言 ..... I

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 1

5 Ecode 标识系统安全一般要求 ..... 1

6 Ecode 编码数据安全要求 ..... 2

7 Ecode 标识系统身份鉴别与授权要求 ..... 3

8 Ecode 标识系统访问控制要求 ..... 4

9 Ecode 标识系统交互安全要求 ..... 4

10 Ecode 标识系统安全评估要求 ..... 4

11 Ecode 标识系统管理要求 ..... 5

参考文献 ..... 6

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国物品编码标准化技术委员会(SAC/TC 287)提出并归口。

本标准起草单位:中国物品编码中心、北京邮电大学、内蒙古自治区标准化院、中国民航信息网络股份有限公司、北京东方捷码科技开发中心、深圳市标准技术研究院、北京交通大学。

本标准主要起草人:罗秋科、韩树文、陆月明、左金鑫、李颖、郭子裕、郭哲明、李雨蓉、房艳、王佩、杜景荣、曹志伟、智慧、徐立峰、李健华、张铎、王东滨、曹若菡、李瑾、王子一。

库七七 www.k99w.com 提供下载



# 物联网标识体系

## Ecode 标识系统安全机制

### 1 范围

本标准规定了物联网标识体系中 Ecode 标识系统的一般要求、编码数据安全、鉴别与授权、访问控制、交互安全、安全评估和管理要求。

本标准适用于物联网标识体系中 Ecode 标识系统建设和应用中的信息安全保障。

### 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 2887 计算机场地通用规范
- GB/T 17963 信息技术 开放系统互连 网络层安全协议
- GB/T 22239 信息安全技术 网络安全等级保护基本要求
- GB/T 25064 信息安全技术 公钥基础设施 电子签名格式规范
- GB/T 31866 物联网标识体系 物品编码 Ecode

### 3 术语和定义

GB/T 31866 界定的以及下列术语和定义适用于本文件。

#### 3.1

**Ecode 标识系统安全机制** security mechanism for Ecode identification system

用于保障 Ecode 标识系统安全的要求集合。

### 4 缩略语

下列缩略语适用于本文件。

- MD 主码(Master Data code)
- NSI 编码体系标识(Number System Identifier)
- V 版本(Version)

### 5 Ecode 标识系统安全一般要求

#### 5.1 物理安全

Ecode 标识系统物理安全应符合以下要求：

- a) Ecode 标识系统建设、运营和使用过程中，机房、数据中心的建设应符合 GB/T 2887 的要求；
- b) 服务器与网络设备应按照安全需求配置，并通过国家认可的第三方机构的安全测评或认证；

- c) 应在数据中心或机房建设完善的电子监控和报警系统,保证 24 h 人工值守 Ecode 标识系统数据中心;
- d) 应在 Ecode 标识系统数据中心边界部署访问控制设备,安装防火墙、入侵检测系统等网络安全防护设备,启用访问控制功能,根据访问控制列表对源地址、目的地址、源端口、目的端口和协议等进行检查;
- e) 应对 Ecode 标识系统数据中心的通信流量进行安全风险监控,对异常访问进行告警。

## 5.2 系统软件安全

系统软件(包括操作系统、数据库等)应通过国家认可的第三方机构的安全测评或认证。

## 5.3 灾备中心

Ecode 标识系统灾备中心选址宜选在地质条件良好的地点。灾备中心应为异地容灾,与主用中心不宜处于同一地震带内。

## 5.4 安全审计

安全审计应包括自动响应、数据产生、审计分析、查阅、事件选择、事件存储等功能,审计的日志内容应包括安全事件的时间、类型、主体身份、结果等。

# 6 Ecode 编码数据安全要求

## 6.1 Ecode 编码数据存储

Ecode 编码数据存储安全应符合以下要求:

- a) 存储 Ecode 编码数据的介质应稳定可靠,不应受外界环境物理条件的明显影响;
- b) 不应采用移动式介质存储或转移 Ecode 编码数据;
- c) 对删除过 Ecode 编码数据的介质应进行技术处理,使删除的数据不可恢复;
- d) 应对存储介质出入库过程进行授权管理,并保留相应记录。

## 6.2 Ecode 编码数据传输

应保障 Ecode 编码数据在传输过程中的抗干扰性、私密性、完整性和正确性,具体要求如下:

- a) 应采取必要的技术和管理手段防止 Ecode 编码数据传输过程中受到干扰。
- b) 应采取必要的技术和管理手段保障 Ecode 编码数据在传输过程中的私密性。Ecode 标识系统网络传输应具备防窃听能力,宜采用 HTTPS 等安全协议,安装数字证书,传输协议安全保护机制应符合 GB/T 17963 的要求。应对传输层进行不少于 128 位加密,传输安全保护机制使用的算法应符合国家密码管理部门的相关规定。
- c) 应采取必要的技术和管理手段保障 Ecode 编码数据在传输过程中的完整性和正确性。Ecode 标识编码结构由 V+NSI+MD 组成,具体编码规则应符合 GB/T 31866 的要求,应保证 MD 编码的完整性和原有校验机制的可用性。

## 6.3 Ecode 标识系统备份与恢复

Ecode 标识系统备份与恢复应符合以下要求:

- a) 需根据 Ecode 编码信息的重要程度和信息导入的频率设定备份的频率,宜采用实时备份的方

式并按照 5.3 的要求建立系统灾备中心；

- b) 应建立异常事件紧急处理流程,以应对 Ecode 标识系统中设备失效、操作失误等造成的故障,并由运维操作员负责恢复备份数据信息；
- c) 应定期检查和测试备份介质及信息,保持其可用性和完整性,具有在规定的时间内恢复系统数据的能力；
- d) 应合理确定业务信息及其他需要永久保存的归档信息的保存期。

#### 6.4 Ecode 标识系统数据库

Ecode 标识系统数据库应符合以下要求：

- a) 应在 Ecode 标识系统中设置存取控制措施,可采取层次、分区、表格等多种方式控制用户对数据库的存取权限；
- b) 可通过实体安全、备份和恢复等多种技术手段来保护数据库的完整性；
- c) 应建立和保存日志记录,宜建立双副本日志,分别存储于磁盘等介质上以便于必要时的数据恢复；
- d) 应建立 Ecode 数据库的定期转贮制度,并根据 Ecode 编码数据交易量的大小决定转贮频度,宜采用实时转贮策略。

#### 6.5 Ecode 标识系统敏感信息保护

应采取必要的技术及管理手段保护 Ecode 标识系统敏感信息。具体要求如下：

- a) 应在 Ecode 标识系统内对身份证、营业执照等敏感信息进行存储和计算,不应在本地存储数据；
- b) 严密跟踪监控敏感信息存储介质的使用和传递过程,防止丢失和信息泄漏；
- c) 未经许可,不得超出数据服务范围,不得私自对数据进行变更和传输,禁止在 Ecode 标识系统中明文展示敏感信息；
- d) 应提供统一的介质销毁工具,包括但不限于物理摧毁、消磁设备等工具,实现各类介质的有效销毁。

#### 6.6 Ecode 编码校验

Ecode 编码校验应符合以下要求：

- a) Ecode 编码结构中,MD 编码方法应完整、准确,应采用必要的校验机制；
- b) Ecode 编码解析系统应建立 Ecode 编码对比验证机制,将解析出的 V、NSI、MD 等信息与数据库中原始码字进行对比验证,确保编码的准确性与一致性。

### 7 Ecode 标识系统身份鉴别与授权要求

#### 7.1 Ecode 标识系统身份鉴别管理

Ecode 标识系统身份鉴别应符合以下管理要求：

- a) 需建设专用登录控制模块对登录用户进行身份标识与鉴别；
- b) 应提供登录失败处理方案,可采取结束会话、限制非法登录次数、自动退出等策略；
- c) 应支持用户名/口令和数字证书两种登录认证方式,并按 GB/T 25064 要求设计数字证书；
- d) 应具有良好的可扩展性,可支持动态口令、生物识别等其他认证方式。

## 7.2 Ecode 标识系统授权管理

Ecode 标识系统授权管理应符合以下要求：

- a) 可支持用户分级授权管理；
- b) 可支持基于角色权限和业务权限的两种直接授权模型。

## 8 Ecode 标识系统访问控制要求

Ecode 标识系统中存在机构平台、企业、个人三种基本用户类型，应根据用户分类设置访问控制参数，实现用户对权限内资源的访问。

机构平台用户，是指某一行业或领域的综合性用户，在获得 Ecode 编码后，具有向企业用户下发编码的权力；企业用户，是指任何合法的生产企业、集成商、解决方案提供商等；个人用户，是指普通互联网用户。

个人用户可查询验证 Ecode 编码，企业用户可注册申请、查询验证、回传 Ecode 编码，机构平台用户可注册申请、查询验证、向企业用户下发 Ecode 编码。

## 9 Ecode 标识系统交互安全要求

应保障信息在交互过程中的一致性、完整性和不可抵赖性，具有防欺骗、重放、仿冒等攻击的机制，并保证通信双方数据的私密性。

## 10 Ecode 标识系统安全评估要求

Ecode 标识系统安全评估应符合以下要求：

- a) 应建立 Ecode 标识系统的安全评估机制；
- b) 安全评估机制应能够分析 Ecode 标识系统的安全风险，选择合理的安全功能组件，建立 Ecode 标识系统的安全轮廓；
- c) 应建立 Ecode 标识系统评估方法模型库，可采用适当的模型和方法进行评估，包括但不限于形式化、检测、专家评估等方法；
- d) 依据 Ecode 标识系统的安全轮廓和对应的评估方法，应制定 Ecode 标识系统信息安全保护及评估规范，指导 Ecode 标识系统的开发、建设、应用等；
- e) 应确保 Ecode 标识系统的保护等级符合 GB/T 22239 的要求。

Ecode 标识系统安全评估参考模型如图 1 所示，包括安全目标的确定、安全保护轮廓的形式化、安全功能组件的分解等评估流程。安全目标包括 Ecode 标识系统的机密性、可鉴别性、可控性、可用性四类。

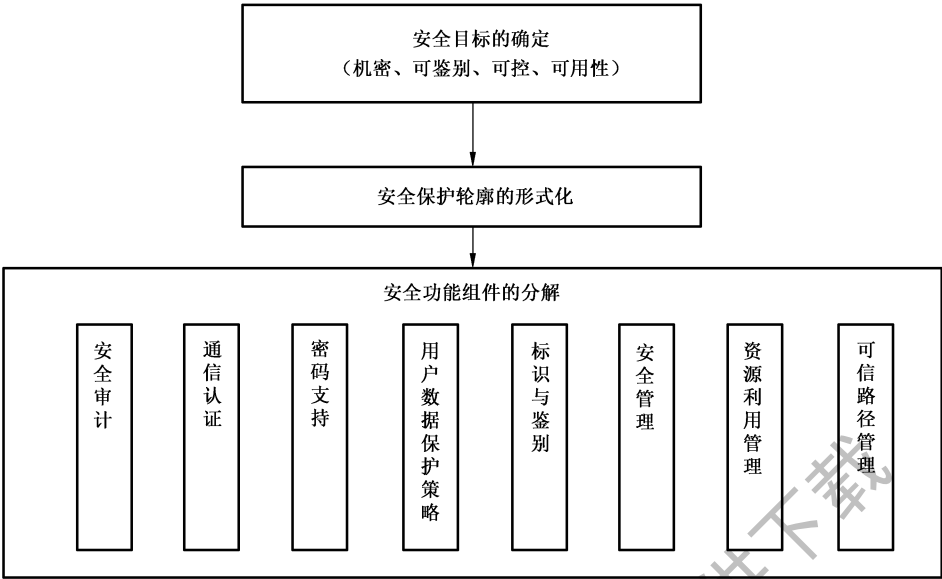


图 1 Ecode 标识系统安全评估参考模型

11 Ecode 标识系统管理要求

11.1 注册审批机制

Ecode 标识系统应增加注册审批机制，用户在网上申请编码时，应提交相应资料，用于管理机构内部审批流程。

11.2 安全管理

11.2.1 日常安全管理

Ecode 标识系统中日常安全管理应符合以下要求：

- a) 建立日常管理活动中的安全管理制度；
- b) 指定或授权专门的人员负责安全管理制度的制定、考核；
- c) 将安全管理制度以纸质文件、电子文件等多种形式发布到相关人员手中。

11.2.2 软件维护管理

Ecode 标识系统中软件维护管理应符合以下要求：

- a) 存储软件产品源文件到磁盘等介质上，并编写详细目录，以便长期保存；
- b) 将重要软件复制两份，一份作为主拷贝存档，一份作为备份；
- c) 对 Ecode 标识系统相关软件的修改保证不降低系统的安全性。

11.3 人员管理

Ecode 标识系统应建立必要的人员录用、考核、安全教育培训和外部人员访问管理制度，保证系统硬件、软件和数据不因偶然和恶意的原因遭到更改、泄漏和破坏。



参 考 文 献

- [1] GB/T 20984—2007 信息安全技术信息 安全风险评估规范
  - [2] GB/T 30269.807—2018 信息技术 传感器网络 第 807 部分:测试:网络传输安全
  - [3] GB/T 31072—2014 科技平台 统一身份认证
  - [4] GB/T 35422 物联网标识体系 Ecode 的注册与管理
- 

库七七 www.k99w.com 提供下载

