附件1

物联网基础安全标准体系建设指南

（征求意见稿）

2021年1月

目录

[前言 - 1 -](#_Toc49958223)

[一、建设思路及目标 - 2 -](#_Toc49958224)

[（一）总体思路 - 2 -](#_Toc49958225)

[（二）基本原则 - 2 -](#_Toc49958226)

[（三）建设目标 3](#_Toc49958227)

[二、建设内容 - 3 -](#_Toc49958228)

[（一）标准体系框架 - 3 -](#_Toc49958229)

[（二）重点标准化领域及方向 - 4 -](#_Toc49958230)

[1.总体安全要求 - 4 -](#_Toc49958231)

[2.终端安全标准 6](#_Toc49958232)

[3.网关安全标准 8](#_Toc49958233)

[4.平台安全标准 1](#_Toc49958234)0

[5.安全管理标准 - 11 -](#_Toc49958235)

[三、组织实施 - 12 -](#_Toc49958236)

[附件：物联网基础安全相关标准项目明细表 - 14 -](#_Toc49958237)

前言

物联网是新一代信息技术的高度集成和综合运用，是新型基础设施建设的重要组成部分。与传统互联网相比，物联网“无缝连接、全面感知、智能处理、虚实交织”的特点突出，行业安全需求多样。随着5G网络覆盖日益完善，物联网产品应用日益丰富，行业渗透日益加深，物联网关键基础环节的一些安全风险将更为突出，加快构建物联网基础安全保障体系，保障物联网安全健康发展尤为重要。

“安全发展，标准先行”。标准化工作是保障物联网安全发展的重要基础。按照《中华人民共和国网络安全法》等相关法律规定，工业和信息化部组织制定了《物联网基础安全标准体系建设指南》（以下简称《建设指南》），加强物联网安全标准顶层设计和方向引领，推动构建系统、科学、规范的物联网基础安全标准体系，指导物联网安全工作的有序开展，支撑经济社会数字化转型和高质量发展。

一、建设思路及目标

**（一）总体思路**

以习近平新时代中国特色社会主义思想为指导，坚持总体国家安全观，以筑牢物联网基础安全、防范公共网络安全风险为目标，着力构建物联网基础安全标准体系，指导标准统筹规划，系统推进标准研制，促进标准落地实施，做好与国家标准、国际标准以及相关领域行业标准的有效衔接，加强国际交流合作，保障物联网安全发展。

**（二）基本原则**

基础支撑，统筹规划。结合物联网行业的发展现状及特点，发挥行业主管部门在顶层设计、组织协调和政策制定等方面的重要作用，形成政府引导、市场主导、社会参与的行业标准建设体系，促进物联网产业安全发展。

急用先行，注重实效。从物联网基础安全的重点难点工作出发，聚焦物联网基础设施和重点行业应用领域，加快基础共性、关键技术、基础通用协议类标准的研究制定，并在此基础上，结合重点行业应用的安全风险，协同推进重点标准的研究制定。

广泛参与，加强落实。在标准制定过程中加强与设备厂商、电信企业、安全企业、互联网企业、科研单位、高校等产业界和学术界各方充分沟通，凝聚共识，统筹运用行业资源，发挥头部企业在产品研发、示范引领等方面的作用，加强重点标准在行业中贯彻应用。

**（三）建设目标**

到2022年，初步建立物联网基础安全标准体系，研制重点行业标准10项以上，明确物联网终端、网关、平台等关键基础环节安全要求，满足物联网基础安全保障需要，促进物联网基础安全能力提升。

到2025年，推进形成完善的物联网基础安全标准体系，研制行业标准30项以上，提升标准对细分行业及领域的覆盖程度，提高跨行业物联网应用安全水平，保障消费者安全使用。

二、建设内容

**（一）标准体系框架**

物联网基础安全标准主要是指物联网终端、网关、平台等关键基础环节的安全标准。物联网基础安全标准体系包括总体安全要求、终端安全、网关安全、平台安全、安全管理五大类标准。物联网基础安全标准体系框架如图1所示。

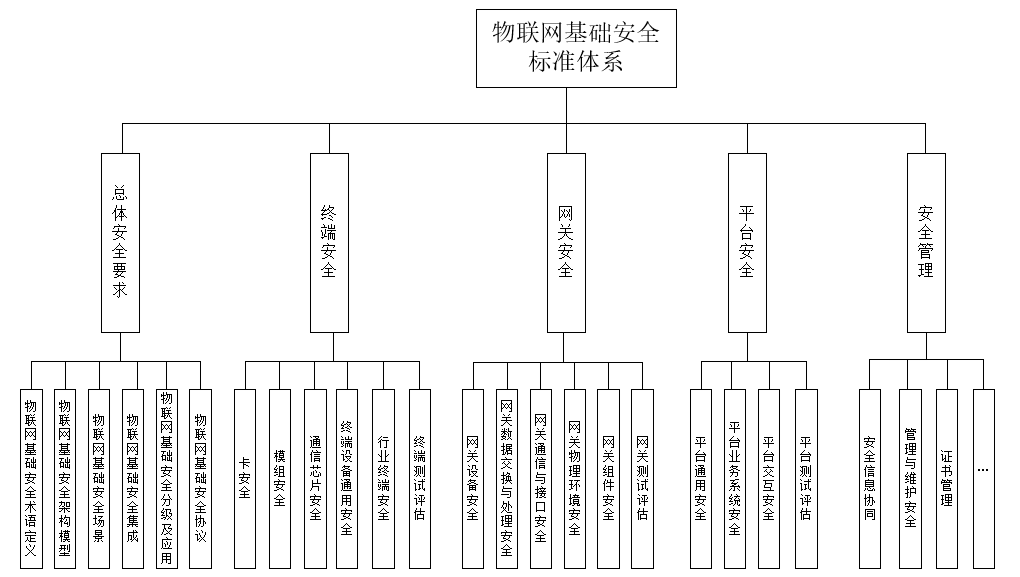


图1 物联网基础安全标准体系框架

**（二）重点标准化领域及方向**

**1.总体安全要求**

总体安全要求是物联网基础安全的基础性、指导性和通用性标准，包括物联网基础安全术语定义、架构模型、安全场景、安全集成、安全分级及应用等方面标准。总体安全要求子体系如图2所示。

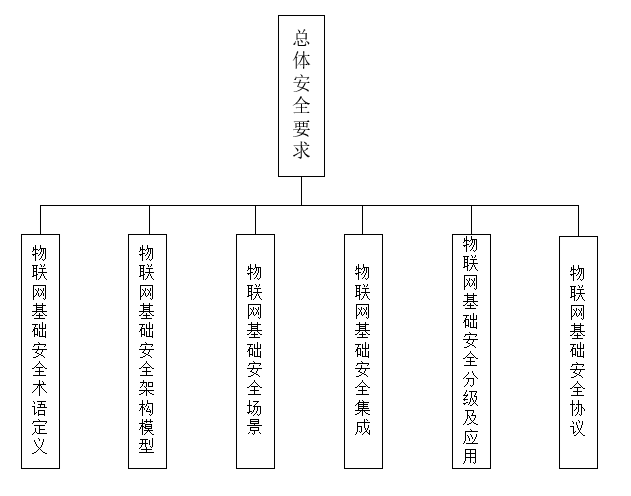


图2 总体安全要求子体系

（1）物联网基础安全术语定义：主要规范物联网基础安全的概念和关键术语，包括技术、规范、应用领域的相关术语，实现统一标准体系内的语义理解。

（2）物联网基础安全架构模型：主要提出物联网基础安全体系框架以及各部分参考模型，以明确和界定云、管、端各层面功能、关系、角色、边界、责任等内容。

（3）物联网基础安全场景：明确物联网基础安全体系的主要安全场景，对不同类型的场景中的安全需求进行示例和规范的标准。

（4）物联网基础安全集成：在物联网系统规划、集成、实施等过程中，保障系统各层级对象安全性和可靠性的相关标准。

（5）物联网基础安全分级及应用：明确物联网基础安全分级分类的基本原则、维度、方法、示例、建议场景等要求，为实施分级分类安全管理提供基础支撑。

（6）物联网基础安全协议：针对物联网平台、网关、终端之间及其他组网模式的通信需求，规范通信协议和接口规范等安全要求，包括有线协议安全、无线协议安全等标准。

**2.终端安全标准**

终端安全标准是物联网基础安全体系中感知层面的标准，包括卡安全、模组安全、通信芯片安全、终端设备通用安全、行业终端安全、终端测试评估等标准。终端安全标准子体系如图3所示。

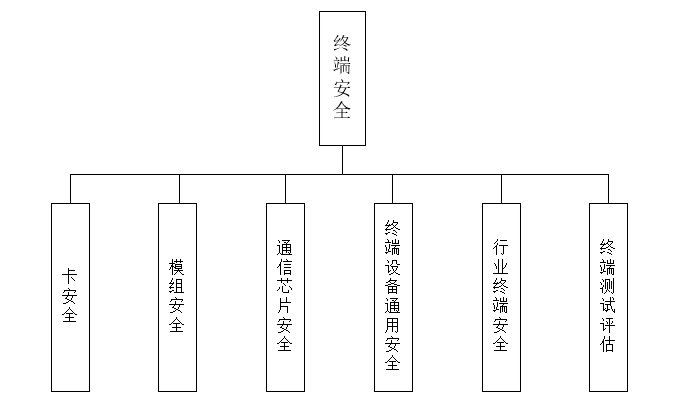


图3 终端安全标准子体系

（1）卡安全：细化落实相关法律法规和政策文件对物联网卡安全管理的要求，规范物联网卡销售、登记、使用管理等具体流程以及技术要求。包括物联网卡安全分类管理规范、物联网卡技术手段建设标准等。

（2）模组安全：规范物联网终端通信模组安全要求，细化不同通信协议、网络制式的通信模组在接入认证、数据交互、数据传输、抗电磁干扰等方面的安全要求，包括蜂窝通信模组和其他类型通信模组安全标准。

（3）通信芯片安全：规范通信芯片的基础安全要求，包括通信加密算法、秘钥管理、加解密能力、签名验签、数据存储等。

（4）终端设备通用安全：规范物联网终端基线安全要求，包括物联网终端硬件安全、操作系统安全、软件安全、接入认证、数据安全、协议安全、隐私保护、接口互通、证书规范、固件升级等通用安全标准。

（5）行业终端安全：主要包括与各垂直行业密切相关的、具有特定功能的物联网终端安全要求，如智能门锁、监控设备等特定行业终端的特有安全要求。

（6）终端测试评估：主要用于规范物联网终端软硬件安全评估及测试方法，包括物联网卡安全测试、硬件安全测试、操作系统安全测试、软件安全测试、接入认证安全测试、数据安全测试、通信协议安全测试等标准。

**3.网关安全标准**

网关安全标准包括物联网网关设备安全、网关数据交换与处理安全、网关通信与接口安全、网关物理环境安全、网关组件安全、网关测试评估等内容。网关安全标准子体系如图4所示。

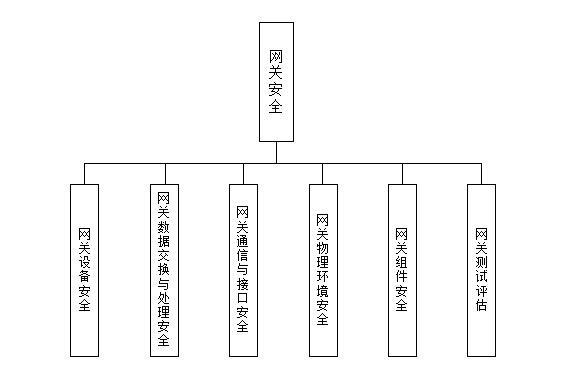


图4 网关安全标准子体系

（1）网关设备安全：规范网关设备系统级的功能架构、安全协议、安全防护能力等方面技术要求，主要包括网关设备安全架构、安全功能、安全性能、安全协议等标准。

（2）网关数据交换与处理安全：规范网关在传输、处理网络感知数据、业务管理平台数据过程中数据安全传输、安全处理和安全存储等方面技术要求，主要包括数据安全模型、安全计算、处理算法、数据存储、数据溯源等标准。

（3）网关通信与接口安全：规范网关与其他设备互联时通信接口和管理接口的安全通信协议、黑白名单、鉴权认证等方面技术要求，主要包括网关南向、北向接口安全规程、安全协议流程、端口防护等标准。

（4）网关物理环境安全：规范网关贮存、运输和使用环境条件下电磁辐射、防电磁干扰、抗硬力破坏、温湿盐雾环境适应能力等方面技术要求，提高网关产品环境适应性能力，主要包括网关设备电磁兼容、机械环境适应性、气候环境适应性等标准。

（5）网关组件安全：规范网关功能服务、数据采集、数据传输处理等软硬件组件的安全设计、功能等方面技术要求，主要包括网关设备组件安全架构、开源组件安全、应用启动安全等标准。

（6）网关测试评估：规范网关设备安全、组件安全、接口安全、管理维护安全、数据传输处理安全、环境安全等方面的评估测试方法和分级分类评估方法，主要包括设备安全测试、组件安全测试、接口安全测试、安全管理维护测试、数据传输处理安全测试、环境适应性测试、分级分类评估测试等标准。

**4.平台安全标准**

物联网平台包括不限于设备管理平台、连接管理平台、应用使能平台、业务分析平台、态势感知平台等。物联网平台安全标准包括平台通用安全、平台业务系统安全、平台交互安全、平台测试评估等。平台安全标准子体系如图5所示。

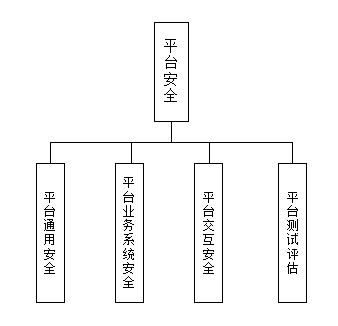


图5 平台安全标准子体系

（1）平台通用安全：规范各类物联网平台通用数据安全、通信安全、身份鉴别、安全监测、物理安全、安全可信等方面安全要求，包括通用安全框架、平台可信计算等标准。

（2）平台业务系统安全：规范基于物联网平台开发的行业业务系统自身和对外的访问控制、防代码逆向、安全审计、篡改和注入防范等方面安全要求，包括业务系统基础安全、跨系统访问以及业务系统与用户交互等标准。

（3）平台交互安全：规范不同物联网平台之间、平台与上层业务系统、平台与下层设备（主要是接入平台的网关和终端）之间的数据交互、加密传输、交互接口配置和审计等方面的安全要求，包括不同物联网平台之间交互、平台与南向和北向之间交互的安全标准。

（4）平台测试评估：规范物联网平台的通用安全、业务系统安全、平台内部和平台之间交互安全、安全管理等方面的评估测试方法和分级分类评估方法，包括物联网平台通用安全测试、业务系统安全测试、交互安全测试和安全管理测试等标准。

**5.****安全管理标准**

安全管理标准主要用于指导行业落实通用安全管理要求，包括安全信息协同、管理与维护安全、证书管理等。安全管理子体系如图6所示。

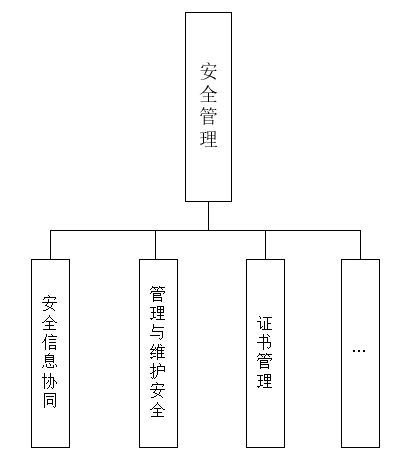


图6 安全管理子体系

（1）安全信息协同：针对物联网协议类型众多，明确物联网基础安全相关数据互联互通标准，实现跨协议安全互联互通，包括接口规范、测试方法等标准。

（2）管理与维护安全：规范不同物联网场景下终端、网关、平台的运维管理等方面安全要求，支撑物联网业务的安全运行及有效监测，包括制度建设、安全组织、人员管理、运行安全、资产管理、配置管理、应急响应、灾备恢复等标准。

（3）证书管理：规范不同类型的物联网终端、网关、平台的认证管理，用于不同类型设备的安全认证互通互认，包括证书生成、证书管理、证书更换等标准。

三、组织实施

**一是加快标准研制。**在工业和信息化部的指导下，按照《建设指南》明确的标准研制路径，有序推进行业标准研制工作，注重物联网基础安全标准化工作与行业发展实际结合，尽快制定发布一批产业急需、贴近应用的标准。

**二是实施动态更新。**紧盯物联网新技术、新应用的发展趋势，加强标准体系的科学规划和动态更新，做好与产业各方的工作协同，在物联网安全发展水平的不同阶段，补充完善适应产业发展的安全标准。

**三是深化标准应用。**充分发挥地方主管部门、行业协会的作用，通过培训、论坛、研讨等方式，加大标准普及推广力度，强化标准应用落地，积极推进重点行业领域安全标准的试点示范，快速提升物联网安全整体水平。

**四是加大交流合作。**组织做好物联网基础安全标准跨行业交流以及国际合作，积极参与物联网安全国际标准制定，促进行业标准向国家标准、国际标准转换。

附件：物联网基础安全相关标准项目明细表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **总序号** | **分序号** | | **标准名称** | **标准号/计划号** | | **状态** |
| **A总体安全要求** | | | | | | |
| **A.1 物联网基础安全术语定义** | | | | | | |
|  |  | | 物联网基础安全术语定义 |  | | 待制定 |
| **A.2 物联网基础安全架构模型** | | | | | | |
|  |  | | 物联网安全参考模型及通用要求 | GB/T 37044-2018 | | 已发布 |
|  |  | | 信息安全技术 网络安全等级保护基本要求 | GB/T 22239-2019 | | 已发布 |
| **A.3 物联网基础安全场景** | | | | | | |
|  |  | | 安全应用场景 |  | | 待制定 |
| **A.4 物联网基础安全集成** | | | | | | |
|  |  | | M2M技术要求（第一阶段） 安全解决方案 | T/CCSA 215-2018 | | 已发布 |
| **A.5 物联网基础安全分级及应用** | | | | | | |
|  |  | | 物联网分级分类安全 总则 |  | | 待制定 |
| **A.6 物联网基础安全协议** | | | | | | |
|  | 7. | | 物联网感知层协议安全技术要求 | YDB 171-2017 | | 已发布 |
|  | 8. | | 物联网感知层协议安全性要求 | 2012B106 | | 制定中 |
| **B终端安全** | | | | | |  |
| **B.1卡安全** | | | | | |  |
|  |  | 智能卡通用安全检测指南 | | | GB/T 31507-2015 | 已发布 |
|  |  | 智能卡安全技术要求（EAL4+） | | | GB/T 36950-2018 | 已发布 |
|  |  | 嵌入式通用集成电路卡（eUICC）及其远程管理的安全技术要求 | | | YD/T 2845-2015 | 已发布 |
|  |  | 物联网卡安全风险监测技术要求 | | | 2019-0740T-YD | 制定中 |
|  |  | 物联网卡日志留存技术要求 | | | 2019-0300T-YD | 制定中 |
|  |  | 面向消费电子设备的嵌入式通用集成电路卡（eUICC）安全能力技术要求 | | | 2019-1272T-YD | 制定中 |
|  |  | 面向物联网设备的嵌入式通用集成电路卡（eUICC）安全能力技术要求 | | | 2019-1271T-YD | 制定中 |
|  |  | 移动通信智能终端卡接口安全技术要求 | | | 2016-0442T-YD | 制定中 |
|  |  | 基于安全平台的eSIM安全技术要求和测试方法 | | | 2019-1274T-YD | 制定中 |
|  |  | 基于eSIM安全架构的车辆紧急救援系统 网络部分 | | | 2018B46 | 制定中 |
|  |  | 基于SIM卡的物联网安全服务技术要求 | | | 2019-0995T-YD | 制定中 |
|  |  | 物联网基础安全 物联网卡安全分类管理规范 | | |  | 制定中 |
|  |  | 物联网分级分类基础协议安全规范 物联网卡安全监测与管理平台数据采集接口规范 | | | 2019-0739T-YD | 制定中 |
|  |  | 物联网分级分类基础协议安全规范 物联网卡安全监测与管理平台协同处置接口规范 | | |  | 制定中 |
| **B.2模组安全** | | | | | | |
|  |  | 网络电子身份标识eID载体安全技术要求 | | | YD/T 3456-2019 | 已发布 |
| **B.3通信芯片安全** | | | | | | |
|  |  | 智能家居终端安全芯片接口技术要求 | | | 2017-YDB-38 | 制定中 |
| **B.4终端设备通用安全** | | | | | | |
|  |  | 物联网感知设备安全技术要求 | | | 20152007-T-469 | 已发布 |
|  |  | 物联网感知终端应用安全技术要求 | | | GB/T 36951-2018 | 已发布 |
|  |  | 物联网感知层接入通信网的安全要求 | | | GB/T 37093-2018 | 已发布 |
|  |  | 物联网终端嵌入式操作系统安全技术要求 | | | YDB 173-2017 | 已发布 |
|  |  | 物联网终端操作系统安全性技术要求 | | | 2012B105 | 制定中 |
|  |  | 面向低功耗蜂窝网的物联网终端安全能力技术要求 | | | 2018-1629T-YD | 制定中 |
|  |  | 泛在网感知延伸层的物理层安全技术研究 | | | 2015B39 | 制定中 |
|  |  | 基于信任根的物联网设备系统安全技术要求 | | |  | 立项中 |
|  |  | 物联网终端通用安全防护要求 | | | YDCPZT0312-2020 | 立项中 |
|  |  | 物联网基础安全 蜂窝物联网终端安全分级分类管理技术要求 | | |  | 立项中 |
| **B.5行业终端安全** | | | | | | |
|  |  | 公安物联网感知终端安全防护技术要求 | | | GB/T 35318-2017 | 已发布 |
|  |  | 公安物联网感知终端接入安全技术要求 | | | GB/T 35592—2017 | 已发布 |
|  |  | 智能家居终端设备通用安全能力技术要求 | | | YDB 201-2018 | 已发布 |
|  |  | 电信网视频监控系统 第7部分：安全要求 | | | YD/T 2455.7-2016 | 已发布 |
|  |  | 用于煤矿安全生产与监控及应急救援的信息系统总体技术要求 | | | 20150034-T-339 | 制定中 |
|  |  | 基于oneM2M的物联网服务层 安全 | | | 2018-0146T-YD | 制定中 |
|  |  | MTC安全关键技术研究 | | | 2015B67 | 制定中 |
|  |  | 智能家居终端安全 通用安全能力技术要求 | | | 2019-0998T-YD | 制定中 |
| **B.6终端测试评估** | | | | | | |
|  |  | | 智能家居终端设备通用安全能力测试方法 | | 2018-CCSA-24 | 制定中 |
|  |  | | 移动通信智能终端信息安全风险评估方法 | | 2016-0419T-YD | 制定中 |
|  |  | | 移动通信智能终端卡接口安全测试方法 | | 2016-0417T-YD | 制定中 |
|  |  | | 基于物联网的智能锁系统 第5部分：终端安全技术要求和测试方法 | | 2019-CCSA-51 | 制定中 |
|  |  | | 智能家居终端安全 智能音箱安全能力技术要求和测试方法 | | 2019-CCSA-23 | 制定中 |
|  |  | | 智能家居终端安全 智能电视安全能力技术要求和测试方法 | | 2019-CCSA-24 | 制定中 |
|  |  | | 物联网基础安全 蜂窝物联网终端安全分级分类管理评估方法 | |  | 立项中 |
|  |  | | 物联网类终端通用安全技术要求和测试方法 | | YDCPZT0326-2020 | 立项中 |
| **C网关安全** | | | | | |  |
| **C.1网关设备安全** | | | | | |  |
|  |  | | 物联网感知层网关安全技术要求 | GB/T 37024-2018 | | 已发布 |
| **C.2网关数据交换与处理安全** | | | | | | |
|  |  | | 感知层通信系统安全等级保护基本要求 | YDB 172-2017 | | 已发布 |
|  |  | | 基于公用电信网的宽带客户智能网关 第12部分：家庭用智能网关设备安全技术要求 |  | | 立项中 |
|  |  | | 基于公用电信网的宽带客户智能网关 第13部分：企业用智能网关设备安全技术要求 |  | | 立项中 |
|  |  | | 物联网基础安全 基于公用电信网的宽带客户智能网关安全分级分类管理技术要求 |  | | 立项中 |
|  |  | | 物联网基础安全 基于公用电信网的宽带客户智能子网关安全分级分类管理技术要求 |  | | 立项中 |
| **C.3网关通信与接口安全** | | | | | | |
|  |  | | 为移动通信终端提供互联网接入的设备安全能力技术要求 | YD/T 3530-2019 | | 已发布 |
|  |  | | 无线传感器网络与移动通信网络融合的安全技术要求 | YDB 131-2013 | | 已发布 |
| **C.4网关物理环境安全** | | | | | | |
|  |  | | 面向物联网的蜂窝窄带接入（NB-IoT） 安全技术要求 | YD/T 3339-2018 | | 已发布 |
| **C.5网关组件安全** | | | | | | |
|  |  | | 网关插件安全 |  | | 待制定 |
| **C.6网关测试评估** | | | | | | |
|  |  | | 物联网基础安全 基于公用电信网的宽带客户智能网关安全分级分类管理评估方法 |  | | 立项中 |
|  |  | | 物联网基础安全 基于公用电信网的宽带客户智能子网关安全分级分类管理评估方法 |  | | 立项中 |
| **D平台安全** | | | | | |  |
| **D.1平台通用安全** | | | | | | |
|  |  | | 物联网卡安全监测与管理平台总体技术要求 | 2019-0738T-YD | | 制定中 |
|  |  | | 物联网管理平台安全防护要求 | 2019-0734T-YD | | 制定中 |
|  |  | | 物联网信息系统安全运维通用要求 第2部分：管理平台 | 2018-1803T-YD | | 制定中 |
|  |  | | 物联网信息系统安全运维通用要求 第1部分：总体要求 | 2018-1802T-YD | | 制定中 |
|  |  | | 物联网服务平台安全防护要求 | YDCPZT0311-2020 | | 立项中 |
|  |  | | 物联网基础安全 物联网平台安全分级分类管理技术要求 |  | | 立项中 |
| **D.2平台业务系统安全** | | | | | | |
|  |  | | 基于物联网的智能锁系统 第3部分：平台安全技术要求和测试方法 | 2019-CCSA-49 | | 制定中 |
| **D.3平台交互安全** | | | | | | |
|  |  | | 平台交互安全技术要求 |  | | 待制定 |
| **D.4平台测试评估** | | | | | | |
|  |  | | 物联网云平台能力评估方法 第2部分：安全要求 | 2019-0996T-YD | | 制定中 |
|  |  | | 物联网基础安全 物联网平台安全分级分类管理评估方法 |  | | 立项中 |
| **E安全管理** | | | | | |  |
| **E.1安全信息协同** | | | | | | |
|  |  | | 物联网数据传输安全技术要求 | GB/T 37025-2018 | | 已发布 |
|  |  | | 物联网标识解析安全技术要求 |  | | 立项中 |
| **E.2管理与维护安全** | | | | | | |
|  |  | | 物联网信息安全管理系统接口规范 | 2019-0737T-YD | | 制定中 |
|  |  | | 物联网信息安全管理系统技术要求 | 2019-0736T-YD | | 制定中 |
|  |  | | 物联网终端账号管理系统安全要求 | 2018-1394T-YD | | 制定中 |
| **E.3证书管理** | | | | | | |
|  |  | | 通用证书认证和终端技术要求 |  | | 待制定 |