ICS

B

T/SDIOT

团　　体　　标　　准

T/SDIOT　　—2020

物联网加密通信模组技术要求

IOT Encryption Communication Module Specification

（征求意见稿）

2020－XX－XX 发布　　2020－XX－XX 实施

山东省物联网协会　　发布

目　　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由山东省物联网协会、山东省科学院新一代技术标准化研究院、厦门市物联网行业协会、河南省物联网行业协会、北京物联网智能技术应用协会、杭州市物联网行业协会、上海市物联网行业协会、中关村物联网产业联盟、宁波市物联网智能技术应用协会、　　联合提出。

本标准由山东省物联网协会标准化工作委员会归口。

本文件的有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。

本标准起草单位：天博电子信息科技有限公司、中国电子科技集团公司第二十二研究所、西安电子科技大学、河南有线电视网络集团有限公司、山东鲁源节能认证技术工程有限公司、

本标准主要起草人：丁召杰、何英杰、李启伟、董剑峰、张飞飞、张耘、侯兴鹏、孙振源、孙涵、郜迪、周道强、苏冠群、侯广尧、赵登凤、李文鹤。

物联网加密通信模组技术要求

1 范围

本标准规定了物联网加密通信模组的术语和定义、技术要求、试验方法、标志、使用说明、包装、运输及贮存。

本标准适用于物联网加密通信模组的研发设计、测试、认证和包装，其他无线通信模组的研发、测试、认证和包装可参照执行。

本标准中的加密通信模组要求除非特别规定，否则适用于具有操作系统的加密通信模组和不具有操作系统的加密通信模组。

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 17799.1-2017 电磁兼容 通用标准 居住、商业和轻工业环境中的抗扰度试验

GB/T 17799.2-2003 电磁兼容 通用标准 工业环境中的抗扰度试验

GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069-2010 信息安全技术 术语

GB/T 33745-2017 物联网 术语

3 术语和定义、缩略语

下列术语和定义、缩略语适用于本文件。

3.1 术语和定义

物联网 Internet of things

通过感知终端节点，按照约定的协议，连接人、物、系统和信息资源，进行信息处理的智能服务系统。

[GB/T 33745-2017，定义2.1.1]

加密通信模组 Encryption Communication Module

该模组为智能化模组，依靠物联网无线通信网络，实现串口设备与网络服务器传输数据的安全加密，提高目前无线通信领域数据传输的安全性，具有极高的可靠性。

3.2 缩略语

下述缩略语适用于本文件。

SOC:系统级芯片（System on Chip）

SIM:用户身份识别卡(Subscriber Identity Module)

MCU:微控制单元（Micro Control Unit）
UDP:用户数据报协议（User Datagram Protocol）
Coap:受限应用协议（The Constrained Application Protocol）
3GPP:第三代合作伙伴计划（3rd Generation Partnership Project）
GPIO:通用I/O端口（General-Purpose Input /Output Ports）
I2C:集成电路总线（Inter－Integrated Circuit）
SPI:串行外设接口（Serial Peripheral Interface）
UART:通用异步收发传输器（Universal Asynchronous Receiver/Transmitter）
SDK:软件开发工具包（Software Development Kit）
UE:用户设备（User Equipment）
NPRACH:上行物理随机接入信道（Uplink physical random access channel）
EVM:误差向量幅度（Error Vector Magnitude）
ACLR:相邻频道泄漏比（Adjacent Channel Leakage Ratio）
IMEI:国际移动设备标识（International Mobile Equipment Identity）
SN:机器码（Serial Number）
LPWAN:低功耗广域网络（Low Power Wide Area Network）
LGA:触点陈列封装（land grid array）
LCC:无引脚芯片载体（Leadless chip carrier）

4 技术要求

4.1 基本功能电路

4.1.1 模组架构：模组应采用物联网芯片，以 SOC 为核心，支持 SIM 卡，至少应集成基带电路、电源管理模块、数据存储模块、数据处理模块等软硬件设计。
4.1.2 电路设计：应对晶振、电源管理芯片、MCU 的选型要求严格。使用行业认可的开发环境进行电路设计，并完成编译仿真等简单自检任务，电路设计完成之后应进行严格的电气测试和认证，保证电路功能处于最优状态。
4.1.3 软件设计：应对物联网芯片的应用核和协议核进行嵌入式开发，应实现模组各个外设的驱动以及 UDP、Coap 等通信协议的开发;模组应支持 3GPP TS 27.007 R15 中定义的 AT 指令；模块应能够自动注网、附网。本地端口、目标服务器及端口配置均应通过简单指令完成配置。

4.2 射频电路

4.2.1 基于低功耗考虑。功放、射频开关、低噪放等有源射频器件选型时均应要求器件参数满足模组所需峰值电压、钳位电压、稳定裕度和允许误差等高效率低功耗的指标要求。
4.2.2 基于参数指标考虑。模组射频收发电路的设计应按照先仿真后实验室调测的顺序来完成，以保证发射功率、最小输出功率等射频参数性能达到要求。
4.2.3 基于通信方式考虑。模组应支持至少工作在两个频段，应至少满足可以工作在中国移动、中国联通、中国电信三家运营商网络的其中一家运营商或者工作在满足其他非授权频谱的频段。
4.2.4 基于不同的频段考虑。模组设计过程应实现两路射频信号链路的搭建，便于完成上行频段和下行频段数据的交互。

4.3 信息加密安全

4.3.1 总体要求

模组应满足GB/T 22240--2008规定的物联网信息安全系统中的通信安全要求。同时应满足GB/T 36951-2018有关物联网信息安全技术的要求。

4.3.2 接入安全

a） 模组应在接入网络中具有唯一网络身份标识；

b） 模组应具备接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证；

c） 应禁止多个模组使用同一个认证密钥；

d） 应保证模组通过受控的边界设备接入内部网络；

e） 模组应支持对基于应用协议和应用内容的访问控制；

f） 模组应支持基于对称与非对称密码机制的身份鉴别；

g） 模组应支持保证秘钥存储和交换安全。

4.3.3 通信安全

4.3.3.1 防电磁泄漏

模组应对传输数据进行加密处理，预防其衍生品信号被截获发生信息泄漏。

4.3.3.2 传输保密性与完整性

a） 应采用校验技术或密码技术保证通信过程中数据的完整性；

b） 应采用密码技术保证通信过程中数据的保密性。

4.3.3.3 身份认证与机密性

a）应基于密码技术对通信的双方进行验证或认证；

b）应基于加密算法对通信过程进行密码运算和密钥管理；

c）应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护。

4.3.4 设备安全

4.3.4.1 标识唯一与口令鉴别

a） 模组及其衍生品用户应有唯一标识；

b） 应对模组及其衍生品用户进行身份鉴别，使用口令鉴别时，口令应由字母、数字组成，且长度不小于8位。

4.3.4.2 访问权限

a） 模组及其衍生品应能控制其操作系统用户的访问权限；

b） 模组应能防护本地或远程访问数据的安全性。

4.3.4.3 失效报警

模组及其衍生品应能自检出已定义设备故障并报警，确保模组及其衍生品及时检修。

4.3.5 数据安全要求

4.3.5.1 信息数据安全

a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性；
b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性；
c）应采用密码技术保证重要数据在传输过程中的保密性；
d）应采用密码技术保证重要数据在存储过程中的保密性。

4.3.5.2 存储数据安全

a）模组上传采集数据入库时应进行加密存储；
b）保证模组的密文访问控制体系，使其非授权用户仍然无法访问密码数据；
c）确保关键信息进行加密保护，保证敏感数据以密文形式存储。

4.4 软件节能调度算法

4.4.1 应结合物联网通信应用共性，研究更加节能的软件调度算法，应将模块工作划分为Active（激活）、Idle（空闲）和PSM（深度休眠）三个状态。
4.4.2 应通过软件算法优化各个状态持续时间，模组应在无数据交互式时进入PSM状态，只有设备有数据发送时才能被激活进行数据传输，当进入到PSM状态，应不再接收来自基站的数据，但应定时的激活网络获取数据。
4.4.3 调度算法应能够保证模组处理所需发送和接收数据更加及时有效，应保证模组尽可能的处在深度休眠模式，以此来达到降低功耗的效果。

4.5 智能模块

4.5.1 在模组硬件设计时应支持常用传感器，如温湿度、粉尘颗粒等传感器。为了最大限度从硬件设计方面满足物联网应用的需求，模块应集成通用GPIO、SPI、I2C、UART等面向不同传感器通信方式的接口。
4.5.2 在软件方面。应设计最简透传系统，通过简单的AT指令完成网络接入、满足通信要求；模组应支持分等级记录日志，并提供提取日志的接口和方法；模组应支持Android 4.x及以上版本，模组应提供SDK，开放存储和处理资源，以基于模组开发外围期间的驱动程序，根据应用场景的需要开发应用程序，从而降低物联网应用系统的设计门槛、简化设计方案、缩短开发周期，降低开发成本。
4.5.3 远程升级。模组应具备远程下载和升级的通道，支持通过本地升级或远程升级的方式对模组软件进行更新，同时支持版本升级过程中的回退。

5 试验方法

测试认证工作应主要针对产品依托的网络通信特点，为保证产品满足网络通信的要求，应对模组进行多项性能测试并应经过相关认证的专业测试机构/实验室的入网测试认证，出具专业的测试认证报告。模组应进行的主要测试项目如下：

5.1 基本功能电路试验

a）测试模组正常工作电压时，判断电压范围是否在3.1~4.2VDC，满足终端设备的实际需求；
b）测试模组工作环境温度时，判断工作环境温度是否满足非消费类应用-40℃~+85℃，消费类应用-20℃~+60℃；
c）测试模组功耗时，判断测试结果是否满足省电模式和空闲模式下功耗的要求；
d）模组应达到互联互通测试的要求，使得UE能在小区正常接入、建立连接并且数据业务正常；

e）模组应达到协议一致性测试的要求，使得模组满足射频和协议标准;
f）测试模组卡接口时，判断测试结果是否符合YD/T 1763.1和YD/T 2582.1的要求；
g）测试模组可靠性时，判断测试结果是否符合YD/T 1539的要求；
h）测试模组电磁兼容性时，判断测试结果是否符合YD/T 2593.14的要求；

5.2 射频性能试验

5.2.1 发射功率

5.2.1.1 测试UE最大输出功率时，判断测试结果是否满足3GPP TS36.521-1 e20 6.2.2F的要求；
5.2.1.2 测试最大功率回退时，判断测试结果是否满足3GPP TS36.521-1 e20 6.2.3F的要求；
5.2.1.3 测试可配置的UE发射功率时，判断测试结果是否满足3GPP TS36.521-1 e20 6.2.5F的要求；

5.2.2 输出功率动态调整

5.2.2.1 测试最小输出功率时，判断测试结果是否满足3GPP TS36.521-1 e20 6.3.2F的要求；
5.2.2.2 测试通用开/关时间模板时，判断测试结果是否满足3GPP TS36.521-1 e20 6.3.4F.1的要求；
5.2.2.3 测试NPRACH时间模板时，判断测试结果是否满足3GPP TS36.521-1 e20 6.3.4F.2的要求；
5.2.2.4 测试功控绝对功率容差时，判断测试结果是否满足3GPP TS36.521-1 e20 6.3.5F.1的要求；
5.2.2.5 测试功控相对功率容差时，判断测试结果是否满足3GPP TS36.521-1 e20 6.3.5F.2的要求；
5.2.2.4 测试总功率控制容差时，判断测试结果是否满足3GPP TS36.521-1 e20 6.3.5F.3的要求；

5.2.3 发射信号质量

5.2.3.1 测试频率误差时，判断测试结果是否满足3GPP TS36.521-1 e20 6.5.1F的要求；
5.2.3.2 测试误差矢量幅度EVM时，判断测试结果是否满足3GPP TS36.521-1 e20 6.5.2.1F.1的要求；
5.2.3.3 测试载波泄露时，判断测试结果是否满足3GPP TS36.521-1 e20 6.5.2.2F的要求；
5.2.3.4 测试未分配的带内辐射时，判断测试结果是否满足3GPP TS36.521-1 e20 6.5.2.3F的要求；

5.2.4 频谱外辐射

5.2.4.1 测试占用带宽时，判断测试结果是否满足3GPP TS36.521-1 e20 6.6.1F的要求；
5.2.4.2 测试频谱辐射模板时，判断测试结果是否满足3GPP TS36.521-1 e20 6.6.2.1F的要求；
5.2.4.3 测试邻道泄漏抑制比ACLR时，判断测试结果是否满足3GPP TS36.521-1 e20 6.6.2.3F的要求；

5.2.5 接收机测试

5.2.5.1 测试无重传参考灵敏度级别时，判断测试结果是否满足3GPP TS36.521-1 e20 7.3F.1的要求；
5.2.5.2 测试最大输入电平时，判断测试结果是否满足3GPP TS36.521-1 e20 7.3F.2的要求；

5.3 信息加密安全试验

加密通信模组在物联网系统中信息安全加密发布和订阅阶段的存储开销和计算开销的技术指标至关重要，模组应满足全国信息安全标准化技术委员会通信安全标准工作组发布的《物联网安全标准化白皮书》（2019）要求，同时满足应满足GB/T 36951--2018有关物联网信息安全技术的要求。主要测试项

指标要求如下：

a）模组应达到接入安全测试的性能指标要求；

b）模组应达到通信安全测试的性能指标要求；

c）模组应达到访问权限测试的性能指标要求；

d）模组应达到失效报警测试的性能指标要求；

e）模组应达到数据安全测试的性能指标要求；

5.4 软件节能调度算法试验

a）模组应达到功耗测试的性能指标要求；

b）模组应分别满足处于激活态、空闲态、深度睡眠三个工作状态的性能指标要求。

5.5 智能模块试验

a）模组应达到业务能力测试的性能指标要求；

b）模组应能通过智能模块通信接口、不同的传输协议满足不同场景下物联网应用测试数据的指标要求；

c）模组应能通过简单指令配置，串口透传实现数据的收发，完成自动注网、附网等智能配置；

6 标志、使用说明、包装、运输和存储

6.1 标志

6.1.1 通用性标志

物联网加密通信模组的通用性标志应符合简单、清晰、辨识度高、布局合理等规格要求。此外，还应在加密通信模组及其衍生品上标注产品型号、规格、IMEI、SN等文字、字母和图片信息。

6.1.2 性能特征标志

性能特征标志作为加密模组的使用说明，应符合LPWAN的技术要求，支持平台对模组和终端设备进行管理，同时，应包含下述内容：

a） 低功耗、高安全性、可靠性、可扩展性；

b） 小尺寸、适用于需要安全性高的特殊场景，模组尺寸应尽量小于 24mm*16mm*3mm 且支持 LGA 或 LCC 封装。

6.2 使用说明

加密模组使用说明应符合其部署环境规范的要求，至少应包括：

c） 模组名称、型号；

d） 模组概述(特点、主要使用性能指标)；

e） 部署环境和使用要求、维护和保养注意事项，维护和保养注意事项包括：

——使用时的注意事项；

——闲置时的注意事项；

——其他的注意事项。

注：“使用时的注意事项”包括，加密模组使用过程中可能产生的负面影响等。

6.3 包装

模组的封装应符合满足安放、固定、密封、散热、防静电、防潮、保护模组和增强导热性能作用的有关规定。

模组应附有权威检测机构认证证书、商标注册证书和产品技术手册等说明性材料。

6.4 运输及存储

经检测认证合格后，加密模组应以真空密封袋的形式出货，防止磕碰和用手直接接触加密模组触点“金手指”。加密模组应禁止碰撞、挤压、抛扔和强烈的振动以及雨淋、受潮和暴晒，从而保证加密模组的长期可靠性，以提供完善的数据传输服务。

参 考 文 献

[1] GB/T 7665--2005 传感器通用术语

[2] GB/T 33474--2016 物联网 参考体系结构

[3] GB/T 33745--2017 物联网 术语

[4] GB/T 36951--2018 信息安全技术 物联网感知终端应用安全技术要求

[5] ITU-T Y.2060: Overview of the Internet of things

[6] ISO/IEC 20180:2012 Telecommunication and information exchange between systems -- Security framework for ubiquitous sensor networks

[7] IEC 62443-1-1:2009 Industrial communication networks -- Network and system security -- Part 1-1: Terminology, concepts and models

[8] 2020物联网白皮书：智能与安全的物联网平台

[9] 物联网白皮书（2011年）（工业和信息化部电信研究院，2011年5月）

[10] 全国信息化标准技术委员会.《信息技术 安全技术 信息技术安全评估准则》.GB/T18336--2008

[11] 物联网安全白皮书（2018年） （中国信息通信研究院，2018年12月）

[12] 物联网安全白皮书（2018年） （中国信息通信研究院，2018年9月）

[13] 物联网安全标准化白皮书（2019版）.全国信息安全标准化技术委员会通信安全标准工作组.2019年10月