电 信 终 端 产 业 协 会 标 准

TAF-WG4-AS0027-V1.0.0:2018

面向低功耗广域网的物联网终端安全能力技术要求

Technical Requirements for Security Capability of Internet of Things Terminal Equipment for Low Power Wide Area Network

2018-09-03 发布　　2018-09-03 实施

电信终端产业协会　　发 布

目 次

前　　言

本标准按照GB/T 1.1-2009给出的规则起草。
本标准由电信终端产业协会提出并归口。

请注意本文件的某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：中国信息通信研究院；中国移动通信集团公司；华为技术有限公司；高通无线通信技术(中国)有限公司；

本标准主要起草人：刘陶、潘娟、宁华、张玉玲、潘凯、杜志敏

引　言

基于低功耗广域网的物联技术已经成为万物互联的重要分支，其远距离、大连接、广覆盖、低功耗等特性能够满足行业、公共、个人、家庭等多领域应用。低功耗广域物联网的广泛应用将大幅改变当前的工作模式、客户体验以及人们的日常生活，给各行业发展带来新的商机。然而快速应用发展的同时，其信息安全问题也日益突显，伪造终端、应用篡改、中间人攻击、数据泄露、漏洞被利用变为僵尸终端执行DDoS攻击等安全威胁频繁爆出，并逐渐成为制约应用发展的关键问题之一。本标准的制定，旨在规范广域物联网终端的安全防护能力，通过提高终端自身的安全防护水平，以防范各类安全威胁，避免用户的利益受到损害，同时防止低功耗广域物联网终端应用对网络安全产生不利影响。

本标准并不规定具体的实现方法和措施，以利于创新和发展。本标准从硬件安全能力要求、系统安全能力要求、应用安全能力要求、接入安全能力要求、传输安全能力要求、用户数据安全能力要求6个层面对低功耗广域物联网终端的安全能力提出要求，并从基本的安全保障、实现难度等层面出发对安全防护能力进行了分级，以便于产品具有特定品质，便于消费者选择。

通过本标准的制定能够为广域物联网终端设备采购者、生产厂商、评估机构提供了一个多方认可的，通用的安全规范，终端厂商可参考本标准进行设计、开发，评估机构可依据本标准开展对终端设备的安全测评。本标准将更好地服务于提高广域物联网终端安全防护水平，提升物联网整体信息安全保障能力。

面向低功耗广域网的物联网终端安全能力技术要求

1 范围

本标准规定了面向低功耗广域网的物联网终端安全能力技术要求，包括终端硬件安全能力、系统安全能力、应用安全能力、接入安全能力、传输安全能力、用户数据安全能力等方面要求，并对安全能力要求进行了分级。

本标准适用于各种制式的低功耗广域网物联网终端，个别条款不适用于特殊行业、专业应用，其他类型物联网终端也可参考使用。

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，仅所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。

YD/T 3228-2017 《移动应用软件安全评估方法》

YD/T 3082-2016 《移动智能终端上的个人信息保护技术要求》

YD/T 1811T-2016《面向物联网的蜂窝窄带接入(NB-IoT) 安全技术要求和测试方法》

YD/T 2407-2013《移动智能终端安全能力技术要求》

3 术语、定义、符号和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

低功耗广域网 low power wide area network

低功耗广域网是一种针对低功耗终端场景设计的无线通信广域网。常见的低功耗广域网包括NB-IoT网络和eMTC网络。

3.1.2

面向低功耗广域网的物联网终端 Internet of Things terminal equipment for LPWAN能对物进行信息采集和/或执行操作，并能通过低功耗广域网进行通信的装置。后文简称为低功耗广域网终端。

3.1.3

安全能力 security capability

在低功耗广域网终端上可实现的，能够防范安全威胁的技术手段。

3.1.4

用户 user

使用低功耗广域网终端资源的对象，包括人或第三方应用程序。

3.1.5

用户数据 user data

低功耗广域网终端采集、存储或传输的用户相关信息，包括由用户在本地生成的数据、为用户在本地生成的数据、在用户许可后由外部进入用户数据区的数据等。

3.2 符号和缩略语

下列符号和缩略语适用于本文件。

CNNVD	中国国家信息安全漏洞库	China National Vulnerability Database of Information Security
CNVD	国家信息安全漏洞共享平台	China National Vulnerability Database

4 总体安全技术要求

4.1 安全能力框架

低功耗广域网终端安全能力主要由硬件安全能力、系统安全能力、应用安全能力、接入安全能力、传输安全能力和用户数据安全能力六部分构成，具体如图1所示。

图1 低功耗广域网终端安全能力框架

接入安全能力涉及系统和硬件，传输安全能力涉及系统和应用，用户数据安全能力涉及全部其它5个层面。

4.2 安全目标

4.2.1 硬件安全目标

低功耗广域网终端硬件安全目标是在芯片和硬件接口层保证终端内部基带、存储器和接口的安全，确保系统程序、终端参数、安全数据、用户数据不被篡改或非法获取。

4.2.2 系统安全目标

低功耗广域网终端系统安全目标是达到固件系统对系统资源调用的监控、保护和提醒，确保涉及安全的系统行为总是在受控的状态下，不会出现用户在不知情情况下某种行为的执行，或者用户不可控行为的执行。另外，固件系统还应保证自身的升级是受控的。

4.2.3 应用安全目标

低功耗广域网终端应用安全目标是要保证终端对应用软件可进行授权安装和更新。另外，还要确保已经安装在终端上的应用软件无损害用户利益和危害网络安全的行为。

4.2.4 接入安全目标

低功耗广域网终端接入安全目标是确保终端网络接入时的安全可鉴别。

4.2.5 传输安全目标

低功耗广域网终端传输安全目标是确保数据传输的可知、可控、安全和完整。

4.2.6 用户数据安全目标

低功耗广域网终端用户数据安全目标是要保证用户数据的安全收集、存储、转移和删除，确保用户数据不被非法访问、获取和篡改，同时能够通过掉电保护等方式保证用户数据的可用性。

5 终端安全能力技术要求

5.1 硬件安全要求

5.1.1 芯片安全

应满足如下芯片安全要求：

a) 应具备芯片固件的物理写保护的功能，防止固件被篡改；
b) 芯片的硬件特征信息应与芯片固件绑定，如果芯片固件程序被篡改或更换，终端应能够停止加载芯片固件程序并反馈异常信息。

5.1.2 接口安全

5.1.2.1 调试接口安全

应满足如下调试接口安全要求：

a) 调试接口配置为限制使用；
b) 通过授权的方式管理调试端口的打开、关闭；
c) 终端调试接口默认配置为禁用；

5.1.2.2 闲置端口安全

应满足如下闲置端口安全要求：

a） 具备物理端口的授权使用功能，物理端口包括但不限于通信端口、外部设备接口等；
b） 禁用终端的外接存储设备自启动功能；
c） 禁用闲置的物理端口。

5.1.3 防止物理攻击

低功耗广域网终端应满足如下防止物理攻击要求：

a） 终端密码模块应具备抵抗物理攻击能力，防止敏感信息泄漏。攻击手段包括但不限于旁路攻击和故障注入攻击；

b） 对于需要获取时钟源的终端，应支持与授权时钟源的同步；

c） 对于特殊行业（比如电力、石油炼化、煤炭、化工、核工业等）的物联网终端，应满足国家和行业制定的相关物理安全标准和产品认证，比如防爆、防尘、防泄漏等。

5.1.4 根密钥生成与保护

低功耗广域网终端如存在根密钥，应满足如下要求：

a） 根密钥应随机生成，随机数熵值应不低于128比特；

b） 根密钥应存储并运行于安全区域，无法被外部获取。

5.1.5 加密运算安全

在整个加密周期中应保持加密运算的机密性，满足以下要求：

a） 本地加密密钥应置于安全存储区域；

b） 非本地加密密钥应在业务结束时应从本地销毁；

c） 加密运算过程中应防止密钥信息的泄露，确保密钥信息安全。

5.1.6 启动安全

5.1.6.1 授权验证

应满足如下授权验证要求：

a） 终端安全启动代码应进行完整性验证，当验证通过后执行安全启动过程；

b） 终端安全启动代码应采用签名的方式进行完整性和授权验证，当验证通过后执行安全启动过程。

5.1.6.2 FLASH 启动

应满足如下FLASH启动要求：

a） FLASH未加密存储固件的启动受限；

b） FLASH加密存储固件的启动受限；

5.1.7 安全运行区域

应满足如下安全运行区域要求：

a） 可通过加密的方式实现安全存储；

b） 具备独立的安全运行区域，不与非安全运行区域共享存储空间，防止篡改或非法获取；

c） 具备硬件独立的安全运行区域，通过物理隔离防止篡改或非法获取。

5.2 系统安全要求

5.2.1 标识与鉴别

终端应满足如下标识与鉴别要求：

a） 终端应具备唯一标识；

b） 应对终端进行身份鉴权；

c） 终端应能鉴别执行指令的来源。

5.2.2 访问控制

终端应满足如下访问控制要求：

a） 对具有通用操作系统的终端，对不同任务应具有权限管理功能；

b） 对具有通用操作系统的终端，不同任务应仅被授予完成任务所需的最小权限；

c） 终端应提供安全措施控制对其远程配置；

d） 终端系统访问控制范围应覆盖所有主体、客体以及它们之间的操作。

5.2.3 日志审计

对于具备日志审计功能的终端，应满足如下日志审计要求：

a） 应能为操作系统事件生成审计记录，审计记录应包括日期、时间、操作类型等信息；

b） 应保护已存储的操作系统审计记录，以避免未授权的修改、删除、覆盖等。

5.2.4 系统更新

5.2.4.1 更新安全防护

应提供远程固件更新功能，并满足以下要求：

a） 在远程固件更新时，终端应对固件的来源和完整性进行验证；

b） 在远程固件更新时，终端应对固件采用签名的方式进行来源和完整性验证；

5.2.4.2 更新失败处理

应满足如下更新失败处理要求：

a) 在远程固件更新失败时，应具备报警功能，支持手动恢复；

b) 在远程固件更新失败时，应保持在可用状态，并能重新接受平台的指令；

5.2.5 系统漏洞修补

终端系统应具备通过补丁或软件升级的方式消除重要安全漏洞的能力,发现系统漏洞应及时进行修补。

终端系统应保证不含有CNVD与CNNVD6个月前公布的高危漏洞。

5.2.6 失效保护

终端应能自检出已定义的设备故障并进行告警，确保设备未受故障影响部分的功能正常。

5.3 预置应用安全要求

5.3.1 应用认证签名

如果终端采用认证签名机制，在此情况下，预置应用软件应包含签名信息，且签名信息真实可信，具体可参考YD/T 3228-2017《移动应用软件安全评估方法》。

5.3.2 升级更新要求

预置应用软件更新，应在用户授权的情况下进行，当升级行为不能保证终端系统、其他应用软件、软件本身的安全时，应在说明中明示用户可能带来的安全风险。

当预置应用软件升级失败时，应保证应用软件能保持在可用状态。

5.3.3 应用软件漏洞要求

终端预置应用应保证不含有CNVD与CNNVD6个月前公布的高危漏洞。

5.4 接入安全要求

5.4.1 网络接入认证

接入网络时，终端应满足如下要求：

a) 应在接入网络中具有唯一终端标识；

b) 应支持低功耗广域网的接入认证机制，如 YD/T 1811T-2016《面向物联网的蜂窝窄带接入（NB-IoT）安全技术要求和测试方法》中定义的 NB-IoT 网络的接入认证机制；

c) 应能向物联网应用服务器或物联网管理平台证明其网络身份，支持基于 TLS/DTLS 等协议的身份鉴别机制。

5.4.2 网络接入控制

终端应满足如下网络访问控制要求：

a) 应设置网络接入控制策略，限制对终端的网络访问；

b) 终端多次连接网络失败，应设置延迟或中断连接尝试，避免反复尝试对网络造成影响；

c） 终端应具有随机接入机制，即各终端初始部署或重启之后随机延迟一段时间接入，使同一区域终端错峰接入避免对网络造成冲击；

d） 应在满足应用要求前提下，限制单个终端数据包发送频率。

5.5 传输安全要求

5.5.1 传输完整性

终端应启用通信完整性校验机制，实现生存信息、鉴别信息、隐私性数据和重要业务数据等数据传输的完整性保护；

终端应具有通信延时和中断恢复后继续处理业务的处理机制。

5.5.2 传输保密性

终端传输鉴别信息、隐私数据和重要业务数据等敏感信息时应进行加密。

5.6 用户数据安全要求

5.6.1 用户数据的收集

终端设备采集用户信息在提供相应服务的同时进行。若出于业务需要收集用户个人信息，应在收集前明示收集的目的和范围，并且只有在用户同意的情况下方可继续，且应提供关闭数据收集功能。

5.6.2 用户数据的存储

未经授权的任何实体应不能从终端的加密存储区域的数据中还原出用户数据的真实内容。

当用户个人信息存储在终端内部时，应为数据文件提供访问控制机制，防止未授权访问。存储账户设置类、金融支付类数据时，应采用密文方式存储。个人信息定义参考YD/T 3082-2016《移动智能终端上的个人信息保护技术要求》。

5.6.3 用户数据的授权访问

终端应提供本地存储的用户数据的授权访问能力，当第三方实体访问被保护的用户数据时，应在用户确认的情况下才能访问。

5.6.4 用户数据的转移

终端进行用户数据转移应按照约定目的和用途进行，传输数据之前应对双方进行身份认证和授权。若通过公共网络传输账户设置类、传感采集类、金融支付类用户个人信息时，应采用数字签名等技术手段保证数据的完整性和抗抵赖性，同时应采用密文方式传输。宜先对用户个人信息进行脱敏加工，消除能够识别特定个体的所有数据字段后再进行转移。

5.6.5 用户数据的删除

如终端对用户数据有本地存储操作，应提供用户数据彻底删除功能，以保证被删除的用户数据不可再恢复出来。一般的删除功能仅会删除数据在存储器件中放置位置的索引，而该区域内实际存储的数据没有完全清空，在数据被删除之后，非法程序通过读取该区域的内容，仍有可能从读取到的数据中恢复

被删除的私密数据。彻底删除功能应把该区域内实际存储的数据彻底消除。例如，当终端用户数据被删除时，在该数据对应的存储区域使用全“0”或全“1”进行多次填充。

6 终端安全能力分级

6.1 概述

低功耗广域网终端所支持的安全能力划分为五个等级，第五级是最高等级。终端可选支持到不同的等级，达到相应等级的终端可在说明书上进行明确的标识。

6.2 安全能力分级

根据低功耗广域网终端所支持的安全能力的程度，将终端安全能力自低到高划分为五个等级。在每一等级定义了低功耗广域网终端在相应等级对应的安全能力的最小集合，也就是终端必须支持该集合中的所有安全能力才能标识为该级别，例如：达到第三级的低功耗广域网终端应支持本标准第5章所定义的所有第三级安全能力要求。具体的等级划分详见表1。

表1 低功耗广域网终端安全能力分级

安全能力		安全能力等级				
		一级	二级	三级	四级	五级
1.	5.1.1 芯片安全 a)		√	√	√	√
2.	5.1.1 芯片安全 b)			√	√	√
3.	5.1.2.1 调试接口安全 a)	√	√	√	√	√
4.	5.1.2.1 调试接口安全 b)			√	√	√
5.	5.1.2.1 调试接口安全 c)					√
6.	5.1.2.2 闲置端口安全 a)	√	√	√	√	√
7.	5.1.2.2 闲置端口安全 b)			√	√	√
8.	5.1.2.2 闲置端口安全 c)					√
9.	5.1.3 防止物理攻击 a)					√
10.	5.1.3 防止物理攻击 b)		√	√	√	√
11.	5.1.3 防止物理攻击 c)	√	√	√	√	√
12.	5.1.4 根密钥生成与保护 a)			√	√	√
13.	5.1.4 根密钥生成与保护 b)				√	√
14.	5.1.5 加密运算安全 a)	√	√	√	√	√
15.	5.1.5 加密运算安全 b)		√	√	√	√
16.	5.1.5 加密运算安全 c)		√	√	√	√
17.	5.1.6.1 授权验证 a)	√	√	√	√	√
18.	5.1.6.1 授权验证 b)			√	√	√
19.	5.1.6.2 FLASH 启动 a)		√	√	√	√
20.	5.1.6.2 FLASH 启动 b)			√	√	√
21.	5.1.7 安全运行区域 a)		√	√	√	√
22.	5.1.7 安全运行区域 b)				√	√
23.	5.1.7 安全运行区域 c)					√

24.	5.2.1 标识与鉴别 a)	√	√	√	√	√
25.	5.2.1 标识与鉴别 b)	√	√	√	√	√
26.	5.2.1 标识与鉴别 c)				√	√
27.	5.2.2 访问控制 a)		√	√	√	√
28.	5.2.2 访问控制 b)			√	√	√
29.	5.2.2 访问控制 c)				√	√
30.	5.2.2 访问控制 d)					√
31.	5.2.3 日志审计 a)				√	√
32.	5.2.3 日志审计 b)					√
33.	5.2.4.1 更新安全防护 a)	√	√	√	√	√
34.	5.2.4.1 更新安全防护 b)			√	√	√
35.	5.2.4.2 更新失败处理 a)	√	√	√	√	√
36.	5.2.4.2 更新失败处理 b)			√	√	√
37.	5.2.5 系统漏洞修补		√	√	√	√
38.	5.2.6 失效保护			√	√	√
39.	5.3.1 应用认证签名			√	√	√
40.	5.3.2 升级更新要求	√	√	√	√	√
41.	5.3.3 应用软件漏洞要求		√	√	√	√
42.	5.4.1 网络接入认证	√	√	√	√	√
43.	5.4.2 网络接入控制			√	√	√
44.	5.5.1 传输完整性			√	√	√
45.	5.5.2 传输保密性	√	√	√	√	√
46.	5.6.1 用户数据的收集	√	√	√	√	√
47.	5.6.2 用户数据的存储		√	√	√	√
48.	5.6.3 用户数据的授权访问				√	√
49.	5.6.4 用户数据的转移	√	√	√	√	√
50.	5.6.5 用户数据的删除			√	√	√

参 考 文 献