电 信 终 端 产 业 协 会 标 准

TAF-WG4-AS0054-V1.0.0:2020

NB-IoT 终端安全测试细则和送检指引

2020-04-09 发布　　2020- 04-09 实施

电 信 终 端 产 业 协 会　发 布

目　　次

前　　言

本标准由电信终端产业协会协会提出并归口。

本标准起草单位：中国信息通信研究院
本标准主要起草人：刘陶、詹维骁、宁华、王嘉义、路晔绵、王剑

NB-IoT 终端安全测试细则和送检指引

一、 适用范围

本文件适用电信终端设备中能够独立接入我国公用电信网的“移动用户终端”NB-IoT 制式网络信息安全能力（通信安全部分除外），包括 NB-IoT 制式的无线数据终端等。

二、 检验依据

1.	YD/T 2408-2013 《移动终端安全能力测试方法》
2.	YD/T 3228-2017 《移动应用软件安全评估方法》

注 1：除以上标准外，产品应符合“电信条例”的相关要求；

三、 检测项目一览表

序号	检测项目	测试项数	备注
网络信息安全			
1、	操作系统安全能力测试	1	
2、	应用安全保护能力测试	4	

注 2：本文档不包含网络信息安全中的“通信安全”测试项。

四、 测试项目

1、操作系统安全能力测试

（标准依据：YD/T 2408-2013）

序号	检验项目	标准与要求
1	4.3.1.3 操作系统的更新	终端提供操作系统的更新机制时，应保证执行授权的操作系统更新；终端不能保证操作系统安全的更新时，应在说明书中明示用户可能带来的安全风险。

2、应用安全保护能力测试

（标准依据：YD/T 3228-2017）

序号	检验项目	标准与要求
2	6.2.1.1　签名规范	应用软件应包含供应者或开发者的数字签名信息和软件属性信息（如名称、版本信息和描述等），且签名信息应真实、规范。
3	6.3.1.5　升级行为	应用软件的升级前应明示用户,且用户可有效的确认或取消继续升级；升级前应对升级可能带来的安全风险进行明示，且用户可有效确认或拒绝继续升级；如果取消升级应用软件或者升级失败时，软件能回到更新前的版本且能正常使用。
注：第 2 项适用于承载可安装的业务应用程序的终端； 第 3 项适用于承载可安装的业务应用程序且具备应用界面的终端；		

（标准依据：YD/T 3228-2017）

序号	检验项目	标准与要求
4	6.4.1.7.2 个人信息的加密传输	如果应用软件涉及个人信息（金融支付类，信息通信类，账户设置类，传感采集类信息）等，应用软件应无敏感信息明文传输的行为。
5	6.5.3.1 身份认证机制	厂商提供的文档中应包含用户身份认证机制，且应用的用户身份认证机制与文档中一致。
注：第 4 项适用于具备业务应用程序，且传输敏感个人信息的终端； 第 5 项适用于具备业务应用程序的终端；		

五、　判定原则

1、操作系统安全能力测试

该项测试目的是为了检测在被测设备固件或操作系统升级过程中是否提供了相应的安全措施以保证授权更新，升级过程应满足以下要求：

1) 设备应可判断升级包是否来源于设备生产厂商官方，拒绝刷入非官方来源的包，或即使能刷入，设备识别来源不正确后也不会进行实际的升级操作，而是依旧运行旧版本。（来源验证）
2) 设备应可判断升级包的完整性是否遭到破坏，拒绝刷入经过篡改后的升级包，或即使能刷入，设备识别升级包完整性被破坏后也不会进行实际的升级操作，而是依旧运行旧版本。（完整性保护）

2、应用安全保护能力测试

该项测试目的是为了检测被测设备上所运行业务应用的安全保护能力，以保证设备身份认证安全和数据传输安全，业务应用应满足以下要求：

1) 用户信息加密传输
被测终端应采用传输加密，并以实际上传明密文数据截图为例详细阐述终端上传的所有数据类型，加密方式，以及明密文对应关系。
注：只进行编码不进行加密，例如只采用 HEX 编码、Base64 编码、ASCII 码转换等，本项判定不合格。
2) 身份认证机制
通过运营商平台进行身份认证的，应明确标注在运营商 IOT 平台进行设备注册，并附上平台接收到终端发出信息的截图。
通过自有平台进行身份认证的，身份信息要进行加密传输，方式合理，并附上平台接收到终端发出信息的截图。

本要求仅含移动用户终端 NB-IoT 终端网络信息安全部分要求，其中一项不合格时，本部分综合判定结论为不合格。

六、 测试送检指引

1、 操作系统安全能力测试

1.1 不支持更新时的需提供的材料

出厂后不支持固件更新或操作系统更新的被测终端，送测时需提供下述材料：

	内容说明	备注
不支持说明文档	说明送检设备不支持任何固件或操作系统升级	需加盖公章（可在文档经检测实验室审核确定内容无误后再盖章）

1.2 未全部提供安全措施时的需提供的材料

在固件或操作系统升级过程中未采用完整性保护或来源验证等安全措施，或仅支持其中一种安全措施，或相关安全措施无法达到安全要求的被测终端，送测时需提供下述材料：

	内容说明	备注
产品说明书	内容中应提示固件或操作系统更新存在安全风险，提示用户不要私自刷机等。	不需盖章，只需提供电子版留档。也可以在其他提供给用户查看的文档资料中进行风险声明，将该文档电子版发送检测实验室留档。

风险声明示例文字：

固件更新存在安全风险，仅支持用户使用官方渠道进行固件更新，如用户使用非官方发布的固件包升级，导致的安全风险和损失由用户负责。

注：如采用说明书明示方式，除说明书外无需提供其他材料，若说明书审核通过，则进网检验“操作系统更新”项判定为“未见异常”，但正式报告中会备注此项存在风险。

1.3 提供安全措施时的需提供的材料

根据升级方式，终端升级可分为本地升级和在线 FOTA 升级两种情况，若两种情况都支持，则两种情况下的相关材料都需提供。

1.3.1 本地升级的需提供的材料

分为文档审核及方案验证两个步骤。需提供材料如下：

1.3.1.1 文档材料

至少应包含以下文档：

	内容说明	备注
安全说明文档	针对固件或操作系统更新过程的安全校验和完整性保护方面进行说明，内容包括但不限于采用何种加密方法，刷写时如何进行版本控制等。 **系统安全文档书写建议请参考 1.4 小节。**	需加盖公章（可在文档经检测实验室审核确定内容无误后再盖章）；需同时提供相关技术人员的联系方式，以便测试人员沟通咨询安全方案中的相关问题。
驱动安装及接线指导文档	介绍与送检设备配套的驱动如何进行安装，包括系统环境要求和配置、安装流程、安装过程中是否需要操作设备的某些开关等，需详尽且可操作。	

	需提供所用驱动的版本号。 若有驱动卸载流程，需一并提供。	
升级过程操作指导文档	介绍如何对送检设备进行固件或操作系统升级操作，包括操作过程中所需软件列表（包括名称、版本号等信息）、具体操作流程（包括操作过程中是否需要在某一步操作设备的某些开关等）、查看设备系统版本号的方式（不限于专门的查看工具或 AT 命令等方式）、确认升级后的系统是否可正常运行的方式等。 若提供系统降级操作，还需提供相应的降级操作流程指导说明。	
操作指导书（选）	模块的操作指导（包括但不限于开关机，RESET 等基本操作），如 NB-IoT 设备需要拆机，需提供具体拆机步骤图解等。	
物品清单	送检的所有软硬件清单，请见 1.3.1.2 及 1.3.1.3	

1.3.1.2 硬件

（1）送检的 NB-IoT 终端设备
（2）设备与电脑通信所需的特殊连接设备
（3）送测方认为设备进行系统升级过程中所需的其他设备

1.3.1.3 软件

应至少包括以下内容：

	说明
驱动	与送检设备版本对应的驱动程序
刷写工具	固件刷写工具，即将升级包刷入送检设备的软件工具
固件更新包	需提供升级和降级两个包，若无法提供可仅提供升级包
串口工具（选）	若升级过程中需使用，或查看设备系统版本号时需使用，则应提供
其他软件	在“驱动安装及接线指导文档”和“升级过程操作指导文档”中使用到的其他软件工具或系统插件、补丁等。

注：在送检之前，需确保送检设备版本与各文档描述中使用的设备版本一致，且与驱动等各软件版本匹配。

1.3.2 在线 FOTA 升级的需提供的材料

分为文档审核及方案验证两个步骤。需提供材料如下：

	内容说明	备注
系统安全说明文档	针对固件更新过程的安全校验和完整性保护方面进行说明，内容包括但不限于采用何种加密方法，FOTA 传	需加盖公章（可在文档经检测实验室审核确定内容无误后再

	输时如何进行加密，刷写时如何进行版本控制等。 **系统安全文档书写建议请参考 1.4 小节。**	盖章）；需同时提供相关技术人员的联系方式，以便测试人员沟通咨询安全方案中的相关问题。
不支持说明文档	**若仅支持 FOTA 升级，请提供该文档**，说明仅支持 FOTA 升级，不支持其余方式升级	需加盖公章（可在文档审核确定内容无误后再盖章）

1.4 系统安全文档内容建议

安全说明文档建议包含以下几部分内容：

（1）升级包生成过程

i. 说明在升级包生成过程中使用到的安全措施，包括完整性保护和来源验证两方面。
ii. 若安全措施中使用了密码算法，请注明具体算法名称、运行模式及密钥保护方式（即密钥的使用阶段、存储位置等信息）。
iii. 若使用计算哈希值的方式进行完整性保护，需说明是否是将升级包作为一个整体计算哈希值，若不是，需说明是否存在未计算哈希值的部分，以及这部分内容在固件升级过程中的作用。

例：升级包为一个整包，使用 RSA+SHA1 进行完整性及来源保护，首先计算整个升级包的 sha1 值，之后使用 RSA 的私钥对 sha1 值进行签名，RSA 的私钥保存在厂商私有工具中，不对外公开，RSA 的公钥在设备出厂前内置在设备 XX 区域中，不会被篡改。

（2）升级包验证过程

i. 说明设备收到升级包之后在升级过程中如何进行验证
ii. 验证失败如何处理

例：设备下载升级包后，使用 RSA+SHA1 进行签名及完整性验证，验签公钥为预先存储于设备中的公钥。若升级包验证不通过，则放弃此次升级，设备重启并删除该升级包，继续运行旧版本系统。

（3）若使用升级工具进行升级包来源的判断及升级包完整性的判断，需说明如何保证设备只能通过官方提供的升级工具刷入升级包，而不能通过其他方式（如直接使用 AT 命令等）刷入升级包。

（4）若使用 FOTA 升级，请说明传输过程中如何对数据进行安全保护。

注：系统安全文档内容可能涉及底层芯片设计，设备厂商可联系底层芯片厂商共同撰写。

1.5 常见问题及解答

Q1： 送检产品中的部分模块已经通过检测实验室的 NB-IoT 进网检测，那么请问该产品是否还需要进行检测？

A：实验室是以最终产品形态作为进网检测对象的，所以仍需要进行检测。

Q2： 送检产品的相应文档是否直接发送盖章后的版本？是否需要纸质版本？

A： 所有提供的说明文档需要经过检测实验室审阅合格后，厂商再对该文档进行盖章，通过邮件的方

式提供电子版即可，不需要提供纸质版本。

Q3： 操作系统授权更新需要提供的文档是什么？
A： 如果送检产品不支持更新，请提供该产品不支持出厂后升级的声明；如果送检产品无法满足完整性或来源验证的安全机制，请在说明书上添加“风险声明”（详情请见 Q5），将说明书的电子版通过邮件的方式发送；如果送检产品支持完整性与来源验证（详情请见 Q4）的安全机制，请提供固件包、刷写工具、升级过程操作指导文档、更新安全过程说明、固件签名信息及查看方法、驱动安装及接线指导文档。

Q4： 来源认证和完整性保护分别指的是什么？
A： 来源认证：设备可判断升级包是否是设备生产厂商官方提供的，拒绝刷入非官方来源的升级包，或即使能刷入进去，设备识别来源不正确后也不会进行实际的升级操作，而是依旧运行旧版本。
完整性保护：设备可判断升级包的完整性是否遭到破坏，拒绝刷入经过篡改后的升级包，或即使固件包能刷入设备，设备识别升级包完整性被破坏后也不会进行实际的升级操作，而是依旧运行旧版本。

Q5： 说明书上的风险声明指的是什么？
A： 需要在用户说明书上添加“固件更新存在安全风险，仅支持用户使用官方渠道进行固件更新，如用户使用非官方发布的固件包升级，导致的安全风险和损失由用户负责”，描述可不完全一致，意思相同即可。

2、 应用安全保护能力测试

2.1 需提供的材料

2.1.1 文档材料

至少应包含以下文档：

	内容说明	备注
应用安全说明文档	1、针对终端与后台服务的身份认证机制进行说明，内容包括但不限于终端识别信息、终端注册流程、非法终端连接的处理方式等。 2、说明终端传输的用户信息种类，例如 IMEI 信息、温湿度等传感类信息、报警类信息等。 说明用户信息在传输过程中的安全防护（加密）方法，包括但不限于加密的数据对象，加密方法（无需详述具体加密算法）等。 **应用安全文档书写建议请参考 2.2 小节。**	文档经检测实验室审核确定内容无误后需加盖公章；需同时提供相关技术人员的联系方式，以便测试人员沟通咨询安全方案中的相关问题。

2.1.2 测试条件

（1）送检的 NB-IoT 终端设备（需配备现网上网卡）

（2）至少一台终端焊接射频线

（3）提供串口板，调试工具

（4）后台终端管理平台测试账号，可实现对送测终端对应记录的增添、修改和删除（在送检之前，请确保送检终端已在后台进行注册）

2.2 应用安全说明文档内容建议

1、 范围 (需说明本文档适用的设备型号，设备的使用场景，适用范围，并说明文档中内容与上市产品在身份认证机制和个人信息加密传输方面保持一致)

2、 终端识别 （需说明通过何种手段识别唯一设备，如：通过IMEI号或其他方式）

3、 终端注册流程 （需说明设备的注册过程，需截图（包含平台LOGO，以及一条设备上报的数据），必要时可配流程图；如设备在自有平台注册，身份信息（如IMEI号）还需要进行加密传输或安全校验，请配合截图说明）

4、 终端身份认证过程

4.1 、过程描述（需说明终端身份认证过程，可综合终端识别和终端注册流程进行简述）

4.2 、异常处理方式（需详述，平台如何识别，如何处理设备信息被修改的终端，如IMEI号被修改，加密格式不正确，未注册设备上传信息等）

5、 终端信息传输种类（应包含设备上传的所有种类的个人信息）

5.1 、身份标识类（如：IMEI 信息等，如没有可写“无”）

5.2 、传感采集类（如：温度、湿度、火警、烟感、流量、水压、位置、阀门状态、锁状态等，如没有可写“无”）

5.3 、账户设置类（如：用户名、密码等，如没有可写“无”）

5.4 、金融支付类（如没有可写“无”）

5.5 、信息通信类（如：短消息等，如没有可写“无”）

5.6 、其它类别用户数据（如：远程控制数据，如没有可写“无”）

6、 终端用户数据加密方式

6.1 、加密数据包结构（应包含“5、 终端信息传输种类”中的各种数据，请根据上报数据类型，每一条逐一分析，切勿仅用一张大图举例，分析格式如下）

上报数据：在此处说明上报的数据类型，如上电包，心跳包，报警包，并分别举例

密文截图：在此处附上通过设备串口线或log抓包的密文截图

平台截图：在此处附上对应的平台接收的数据截图，最好是密文

分析说明：在此处附上解析出明文的截图（需包含网站或工具解析的过程），对明文和密文进行对比分析说明，解析过程应包含完整步骤（如解密、转码、进制转换），使解析结果与明文一一对应；请说明加密方式（如整包加密、仅对个人信息加密），哪些字段对应哪些信息（如0代表正常，1代表报警），数据上传周期等，说明应根据截图，清晰详细

6.2 、加密方法（无需提供具体算法，陈述加密方式即可）

需说明加密算法，如AES，可配合在线解析网站或其他自由工具截图说明，HEX编码、BASE64编码以及ASCII码转换等编码方式不算做加密方式

7、 现场测试截图

此部分为现场配合之后填写，需将现场配合测试的截图，按照6.1加密数据包结构的格式进行数据解析。测试截图请与当天被测设备的测试结果保持一致，之前的举例截图请不要修改。

2.3 常见问题及解答

Q1： 设备简介中哪些信息必须填写？

A： IMEI 号需与测试设备一致，若 IMEI 号暂未申请下来，只需内外号码一致。（会在现场测试中进行验证）

此外“设备简介”中“是否已承载业务应用”、“是否承载可安装的业务应用程序”、“是否传输用户信息”三项需如实填写，如有疑问，可向实验室咨询。

Q2： 若设备不具备业务应用程序，是否还需提供安全说明文档？

A： 实验室检测后若发现设备不具备业务应用程序会联系厂商，厂家需提供相关的盖章声明。

Q3： 安全说明文档只用提交一个就够了吗？

A： 应用安全说明文档和系统安全说明文档两部分都应包含在提交的文档中，应分开提交。

Q4： 应用安全说明文档需要包含哪些信息？

A： 需要按照模板逐项填写，重点阐述身份认证过程和信息加密方式，标明是通过自有平台还是运营商 IOT 平台进行身份认证，若使用自有平台，则身份信息也要进行加密传输，对自有平台与终端间身份信息传输的安全性进行详细分析；加密传输采用 AES128 算法或是其他自有算法加密即可。

Q5： 现场测试需要看到哪些信息？

A： 测试时需要查看设备串口上报密文，需要登录平台查看接收信息，需要看到明文以及各个字段含义，且与文档中加密手段一致。以此判断终端数据与平台间通信是否采用应用层加密，终端身份认证机制是否合规，IMEI 号是否正确，传输的数据种类是否已全部包含在提交的文档中，明密文对应关系是否与文档中一致等，对应信息需要截图。

Q6： 现场测试前需要准备些什么？实验室可否提供测试用现网上网卡？

A： 实验室不提供 NB-IoT 频段上网卡，请厂家自备兼容测试终端的 NB-IoT 上网卡；此外还需要至少一台终端连接串口线，请厂家提供调试工具用来读取终端对外传输的密文；提供后台终端管理平台测试

账号，用来观察平台接收到的被测终端信息种类；请在测试前将设备调试好。

Q7： 现场测试结束后还需要做什么？应用安全说明文档可否最后再盖章？
A： 等现场测试通过后，将现场测试截图补充到应用安全说明文档中，标注测试相关数据后（如被测终端串口发出密文对应平台上接收到的哪条信息，明密文对应方法等）再次提交，实验室检查无误后，请将盖章安全文档整合成清晰的单个扫描版 PDF 提交。

七、 更新说明

序号	文件编号	制修订日期	版本主要变化
1	--	2019 年 7 月首次制定本文件	