Country **国家**	Greater China 大中华区
Mark: **标志:**	TÜV Rheinland China Mark TÜV 莱茵中国标志
Procedure Author: **程序作者:**	Ivan Deng TUV Rheinland (China) Ltd. 莱茵检测认证服务(中国)有限公司
Approved **批准**	Matthias Liebscher TUV Rheinland (China) Ltd. 莱茵检测认证服务(中国)有限公司
Revision date: **修订日期:**	2021-06-07

1 Purpose 目的

本文件阐述了莱茵检测认证服务(中国)有限公司（TRCHN）中国标志认证产品范围内规定的准备、提交、评估和认证程序。

2 Scope 范围

本规则适用于通过网络连接相关服务来实现其完整功能的消费类电子 产品（消费类 IoT 产品）的信息安全及个人数据保护的安全认证。消费类 IoT 产品尤指在居家使用或消费者可穿戴的联网电子产品。根据认证业务范围分类符合标准的部分产品类型，产品类型包括但不局限于下述：

- 联网电子电器消费品（智能家电，智能照明装置，智能电视及视频监视器等）
- 联网网络设备（网关，路由器）
- 联网家用安防设备（家庭联网式火灾报警器，防入侵报警器）
- 联网家用电源控制器 （智能插座，智能墙壁开关，智能定时器）
- 联网可穿戴电子设备（智能手表及类似产品）

3 Type of Approval 认证模式

IoT 产品进行的安全认证模式为：型式测试+初始工厂检查+获证后监督

认证的基本环节包括：

4 The application of Certification 认证的申请

4.1 Unit partition of the certified products 认证产品单元划分

原则上按组成IoT产品的软件、硬件和配置等申请认证。同一名称的IoT产品，不同制造商，不同版本号的软件或配置不同时，一般应分为不同申请单元。IoT产品的主要组成结构相同、制造工艺相同、软件相同可作为一个申请单元。

4.2 Application documents 申请材料

A、 申请表

B、 营业执照

C、 TÜV莱茵测试报告或任何其他的TÜV莱茵指定的符合ISO/IEC 17025要求的实验室出具的型式试验报告

D、 关键零部件数据表（CDF）

E、 产品有关信息安全的技术配置表

F、 IoT产品软件及硬件架构图

G、 中文或英文产品说明书

H、 中文或英文产品用户手册

I、 照片文件（如果试验报告中未包括）

5 Products testing 型式测试

5.1 Sample 样品

TRCHN从申请认证单元中抽取代表性样品。申请单元中只有一个型号的，送本型号的样品。以系列产品申请认证时，应从系列产品中选取具有代表性的产品作为主检产品，主检产品应该是该系列产品中对性能影响最不利的产品，其余型号产品为附检产品，附检样品送样要求见附件1。

5.1.1 Send sample 送样原则

从申请认证单元中抽取代表性样品。申请单元中只有一个型号的，送本型号的样品。以系列产品申请认证时，应从系列产品中选取具有代表性的产品作为主检产品，主检产品应该是该系列产品中对性能影响最不利的产品，其余型号产品为附检产品，附检样品送样要求按和主检产品实际差异评估后在作决定。

5.1.2 Sample quantity 样品数量

申请人负责把样品送到TÜV莱茵实验室或任何其他的TÜV莱茵指定的实验室。样品数量见附件1。

5.1.3 Disposition of the sample and records 样品及记录处置

试验结束并出具实验报告后，有关试验记录和相关材料由实验室保存，样品按照TÜV莱茵有关规定处置。

5.2 Products testing 产品测试

适用于产品测试的认证标准为以下标准的技术测试章节：ETSI EN 303 645 V2.1.1 （2020-06）EUROPEAN STANDARD CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements 物联网消费品的网络安全：基本要求

ETSI TS 103 701 V1.1.1 （2021-08）

Cyber Security for Consumer Internet of Things:Conformance Assessment of Baseline Requirements

物联网消费品的网络安全: 基本要求的符合性评估

5.2.1 Acc. Standards 依据标准

对获认可范围内的 IoT 产品适用技术测试标准如下：

ETSI EN 303 645 V2.1.1 （2020-06）

ETSI TS 103 701 V1.1.1 （2021-08）

5.2.2 Testing items and requirements 试验项目及要求

IoT 产品应满足 5.2.1 标准中的技术测试适用的项目及要求。

5.2.3 Testing method 试验方法

按照 5.2.1 标准中的建议的技术测试方法并结合实际的技术发展进行试验。

5.2.4 Period of Products testing产品测试周期

产品测试周期从收到样品和检测费用算起，通常不超过 3 个月（因检测项目不合格，企业进行整改和重新检验的时间不计算在内）。

5.2.5 Testing result evaluation 测试结果判定

产品测试应符合 5.2.1 标准的技术要求，产品如有部分试验项目不符合标准的要求，允许申请人整改后重新提交样品进行试验。重新试验的样品数量和试验项目视不合格情况决定，整改期限不超过 6 个月。如仍有任何 1 项不符合标准要求时，则判定该认证单元产品不符合认证要求。

5.2.6 Testing report 产品测试报告

由 TÜV 莱茵实验室或任何其他的 TÜV 莱茵指定的实验室对样品进行试验，并按规定格式出具测试报告。认证批准后，为申请人提供一份测试报告。

5.3 CDF 关键零部件要求

为确保获证产品的一致性，关键零部件/材料的技术参数、规格型号、制造商、生产厂发生变化时，持证人应及时提出变更申请，并送样进行试验（或提供书面材料确认），经批准后方可在获证产品中使用。

6. Initial factory inspection 初始工厂检查

6.1 Compliance of Standard 认证标准

适用于初始工厂检查标准为以下标准的流程审核章节：

ETSI TS 103 701 V1.1.1 （2021-08）

Cyber Security for Consumer Internet of Things:Conformance Assessment of Baseline Requirements

物联网消费品的网络安全: 基本要求的符合性评估

6.2 Inspection content 检查内容

初始工厂检查的内容为工厂质量保证能力和产品依据 6.1 的流程检查要求的一致性检查进行检查。

6.2.1 Inspection of the factory quality assurance 工厂质量保证能力检查

按《TÜV 莱茵中国标志认证工厂质量保证能力要求》和附件 2 中工厂质量流程检查要求进行检查。

6.2.2 Inspection of the products compliance 产品一致性检查

现场检查时，应在生产现场检查申请认证产品的一致性，重点核查以下内容：

A. 认证产品的标识应与申请表上所标明的信息一致；

B. 认证产品的结构应与申请表中的一致；

C. 认证产品所用的关键零部件/材料应与申请表中的一致；

D. 应至少抽取一个规格型号做一致性检查。一致性检查时，工厂应保证申请认证的产品在生产状态，对产品安全性能采取现场见证试验。

6.2.3 工厂质量保证能力检查和产品一致性检查应覆盖申请认证的所有产品和加工场所。

6.3 The man-day of initial factory inspection 初始工厂检查人天数

工厂检查人日数依据申请认证产品的工厂生产规模来确定，具体人天数如下：

生产规模	300 人以下	300 人及 300 人以上
人日数	1	2

6.4 The result of initial factory inspection 初始工厂**检查结论**

检查组（检查员）负责报告检查结论。现场检查结论为不通过的，检查组（检查员）直接向项目助理和 TRCHN 报告。初始工厂检查存在不符合项时，工厂应在规定期限内完成整改，TRCHN 采取适当方式对整改结果进行验证。未能按期完成整改的或整改不通过的，按现场检查不通过处理。

7 Evaluation and approval of the certification 认证结果评价与批准

7.1 Evaluation and approval of the certification 认证结果评价与批准

TR CHN莱茵中国根据申请资料、产品测试报告和初始工厂检查结论进行综合评价。评价合格后，向申请人颁发认证证书，并授权获证组织使用规定的认证标志。每一个申请认证单元颁发一份认证证书。

7.2 Lead-time 交付周期

完成型式试验和工厂检查后，对符合认证要求的，批准时间、证书制作时间一般不超过15个工作日。

7.3 Stop the certification 认证终止

当型式试验不合格或工厂检查不通过，TRCHN做出不合格决定，终止认证。终止认证后，如要继续申请，按新申请进行。

8 Follow-up surveillance 获证后监督

获证后监督的内容包括工厂产品质量保证能力的监督检查和获证产品一致性检查。

8.1 Surveillance 监督检查时间

8.1.1 Surveillance frequency 监督检查频次

一般情况下，初始工厂检查结束后，12 个月内应安排监督检查，每次监督检查间隔不超过 12 个月。

认证机构可依据产品生产的实际情况，按年度调整监督检查时间。若发生下述情况之一可增加频次：

A、获证产品出现严重质量问题或用户提出严重投诉并经查实为产品问题的；

B、TRCHN 有足够理由对获证产品与认证依据标准的符合性提出质疑时；

C、有足够信息表明制造商、生产厂由于变更组织机构、生产条件、质量管理体系等而可能影响产品符合性或一致性时；

8.1.2 The man-day of follow-up inspection 监督检查人天数

数依据申请认证产品的工厂生产规模来确定，具体人天数如下：

生产规模	300 人以下	300 人以上
人日数	1	2

8.2 Follow-up surveillance content 监督检查的内容

监督检查的内容为工厂质量保证能力和产品一致性检查。依据《TÜV 莱茵中国标志认证工厂质量保证能力要求》和附件 2 中关键流程检查要求对工厂进行监督检查。

前次现场检查不符合项的整改情况是每次监督检查的必查内容。

8.3 The result of follow-up inspection 监督检查结论

检查组（检查员）负责报告检查结论。工厂 检查结论为不通过的，检查组（检查员）直接向项目助理和 TRCHN 报告。工厂检查存在不符合项时，工厂应在规定期限内完成整改，TRCHN 采取适当方式对整改结果进行验证。未能按期完成整改的或整改不通过的，按工厂检查不通过处理。

8.4 Result evaluation 结果评价

TRCHN 组织对监督检查结论进行评价，评价合格的，颁发工厂检查通过证书，认证证书保持有效。当监督检查不通过时，按照 9.3 规定执行。

9 Maintain, Change, suspend, restore, cancel and withdraw the certification 认证证书保持，变更，暂停，恢复，注销和撤销

9.1 Maintain the certification 保持认证

9.1.1 Certificate cycle 证书的有效性

本方案覆盖产品的认证周期是三年，三年有效期满后，需进行再认证。

9.1.2 Certified products changing 认证产品的变更

9.1.2.1 Application for Changing 变更的申请

证书上的内容发生变化时，或产品中涉及安全和/或性能的设计、机构参数、外观、关键零部件/材料发生变更时，证书持有者应向 TRCHN 提出变更申请。

9.1.2.2 Evaluate and approve the changing 变更的评价和批准

TRCHN 根据变更的内容和提供的资料进行评价，确定是否可以变更。如需安排文件评审和/或工厂检查，则评审合格和/或工厂检查通过后方能进行变更。原则上，应以最初进行认证产品为变更评价的基础。评审和工厂检查按照 TRCHN 的规定执行。

对符合要求的，批准变更，并换发新的认证证书。

9.2 Extending scope of certification 扩大认证范围

9.2.1 Extending process 扩大的流程

认证证书持有者需要增加与已获得认证的产品为同一认证单元的产品认证范围时，应从认证申请开始办理手续，并说明扩大要求。TRCHN 核查扩大范围产品与原认证产品的一致性，确认原认证结果对扩大范围产品的有效性，针对差异和/或扩大的范围做文件审核和/或工厂检查，对符合要求的，依据认证证书持有者的要求换发证书。

原则上，应以最初进行认证产品为扩展评价的基础。

9.2.2 Sample 样品要求

持证人应先提供扩大范围产品的有关技术资料，需要送样时，按本方案第 5 章的要求选送样品或进行差异试验。

9.3 Suspension, Withdrawal and Restoring of certification 认证暂停、撤销和恢复

无论通过何种方式发现认证产品不符合中国标志认证方案和/或检测认证条例规定的基本要求，TRCHN 签证官将暂停或撤销相应证书。

在 TRCHN 签证官允许恢复认证状态和使用认证标志前，证书持有者必须报告并完成纠正行动。签证官依照中国标志认证流程规定，将证书恢复为有效状态。对于暂停超过 6 个月，将撤销相应证书；未完成纠正的，视为自愿放弃，对相应证书予以撤销。如果撤销，需要及时将原证书退回给 TRCHN。

当证书暂停或撤销时，相关证书持有者将得到书面通知，说明暂停或撤销的原因，并在记录中标记该证书无效。自暂停或撤销日期起，不得将认证标志用于所制造的产品上，且在所述期限内，不得继续销售认证产品。对可能存在缺陷的认证产品应立即采取纠正行为，包括召回（如果适用）。

10 Certification mark 认证标志

本规则覆盖产品的认证证书无认证标志。

11 Cost 收费

认证费用按TRCHN有关规定收取。

附件1

IoT产品工厂质量控制检验要求

依据标准	送样数量	工厂质量控制检验要求	
		试验项目	例行检验
ETSI EN303645	IoT产品release版本1件 IoT产品debug版本1件	1、产品外观检查	必须
		2、关键流程抽样检查	必须
		3、关键管理变更检查	必须
		4、其他经营风险分析	可选

附件2

No.	Reference Table B.1	Status	Technical /Process
5.1	**5.1 No universal default passwords 没有通用默认密码**		
5.1.1	Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user. (MC, in the case passowords are used)如果使用密码，并且在除工厂默认之外的任何状态下，所有消费者 IoT 设备密码应是每个设备唯一的或由用户定义的。	M C	P+T
5.1.2	Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device. (MC, in the case pre-installed passwords are used)如果使用预先安装的每个设备唯一密码，则应使用一种机制生成这些密码，以减少自动攻击某一类或某一类型设备的风险。	M C	T
5.1.3	Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage. (M)用于针对设备技术属性、风险和使用，对用户进行身份验证的身份验证机制应使用最佳实践和最适合的密码学。	M	T
5.1.4	Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used. (MC, in the case the device allowing user authentication) 如果用户可以对设备进行身份验证，设备应向用户或管理员提供一个简单的机制来更改所使用的身份验证值。（例如：设备可提供修改密码）	M C	P
5.1.5	When the device is not a constrained device, it shall have a mechanism available which makes bruteforce attacks on authentication mechanisms via network interfaces impracticable.(MC，in the case the device is not constrained)当设备不是受约束的设备时（有限制的网络访问），它应具有一种机制抵御通过网络接口对身份验证机制进行攻击（暴力攻击是不可能实现的）	M C	T
5.2	**5.2 Implement a means to manage reports of vulnerabilities 实现管理漏洞报告的手段**		

5.2.1	The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum: • contact information for the reporting of issues; and • information on timelines for: 1) initial acknowledgement of receipt; and 2) status updates until the resolution of the reported issues.(M)制造商应公布脆弱性披露政策，政策包括报告问题的初步确认状态，状态更新，直到解决。	M	P
5.2.2	Disclosed vulnerabilities should be acted on in a timely manner.(R)披露的漏洞过程应包括限时采取的行动	R	P
5.2.3	Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period.(R)制造商应不断监测、查明和纠正其销售、生产、生产和在规定的支助期间运作的产品和服务中的安全漏洞。	R	P
5.3	**5.3 Keep software updated 不断更新软件**		
5.3.1	All software components in consumer IoT devices should be securely updateable.(R)设备上的软件应保持开发和部署安全更新	R	P
5.3.2	When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates. (MC, in the case the device the device is not constrained)当设备不是受约束的设备时，它应具有用于安全安装更新的更新机制	M C	P+T
5.3.3	An update shall be simple for the user to apply. (MC, in the case an update mechanism is implemente)更新应简单地供用户应用。	M C	P
5.3.4	Automatic mechanisms should be used for software updates. (RC, in the case an update mechanism is implemented)软件更新应使用自动机制	R C	P+T
5.3.5	The device should check after initialization, and then periodically, whether security updates are available. (RC, in the case an update mechanism is implemented) 设备应在初始化后检查自动更新，然后定期检查是否有安全更新。	R C	P
5.3.6	If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications. (RC, in the case the device supports automatic updates and/or update notifications and an update mechanism is implemented)如果设备支持自动更新和/或更新通知，则应在初始化状态下启用和可配置功能，以便用户能够启用、禁用或推迟安装安全更新和/或更新通知。	R C	P

5.3.7	The device shall use best practice cryptography to facilitate secure update mechanisms. (MC，In the case an update mechanism is implemented) 设备应使用最佳做法加密技术，以便利安全的更新机制	M C	P+T
5.3.8	Security updates shall be timely. (MC, in the case an update mechanism is implemented)安全更新应及时	M C	P
5.3.9	The device should verify the authenticity and integrity of software updates. (RC, in the case an update mechanism is implemented) 设备应验证软件更新的真实性和完整性	R C	P+T
5.3.10	Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship. (M, updates are delivered over a network interface and an update mechanism is implemented)如果更新通过网络接口传递，设备应通过信任关系验证每次更新的真实性和完整性	M	P+T
5.3.11	The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update. (RC, in the case an update mechanism is implemented) 制造商应以可识别和明显的方式通知用户，需要进行安全更新，并提供关于该更新所减轻的风险的信息。	R C	P
5.3.12	The device should notify the user when the application of a software update will disrupt the basic functioning of the device. (RC, in the case an update mechanism is implemented) 当应用软件更新将中断设备的基本功能时，设备应通知用户。（关联服务更新失败不适用）	R C	P
5.3.13	The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period. (M)制造商应以用户清楚和透明的可访问方式公布规定的支持期	M	P
5.3.14	For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user. (RC, in the case software components are not updateable and the device is constrained)对于无法更新其软件的受限设备，制造商应以用户清楚和透明的方式公布没有软件更新的理由、硬件更换支持的期限和方法以及规定的支持期限	R C	P
5.3.15	For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable. (RC, in the case software components are not updateable and the device is constrained)对于无法更新其软件的受限设备，产品应是可隔离的，硬件应可更换	R C	P
5.3.16	The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.	M	P

	(M)消费者物联网设备的型号名称应通过设备上的标签或通过物理接口清楚地识别。		
5.4	**5.4 Securely store sensitive security parameters 安全地存储敏感安全参数**		
5.4.1	Sensitive security parameters in persistent storage shall be stored securely by the device.(M)持久存储中的敏感安全参数（token,key）应由设备保护并安全存储。	M	P+T
5.4.2	Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software. (MC, in the case of a hard-coded unique per device identity is used for security purposes)如果为安全目的而在设备中使用的硬件编码形成的每个设备标识，应以防止通过物理、电气或软件等手段篡改的方式实施。	M C	T
5.4.3	Hard-coded critical security parameters in device software source code shall not be used.(M)不得使用设备软件源代码中的硬编码关键安全参数。	M	T
5.4.4	Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.(M)为了降低设备受到自动攻击的风险，任何关键安全参数用于完整性校验，真实性检查，软件更新和保护通信的密钥，及相关服务软件应当每个设备和独特的生产机制产生	M	T
5.5	**5.5 Communicate securely 安全地沟通**		
5.5.1	The consumer IoT device shall use best practice cryptography to communicate securely.(M)消费者 IoT 设备应使用最佳做法密码学进行安全通信	M	P+T
5.5.2	The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.(R)消费者物联网设备应使用经过审查或评估的方式实现来提供网络和安全功能，特别是在密码学领域。审查和评价应由独立的内部或外部组织输出。	R	P
5.5.3	Cryptographic algorithms and primitives should be updateable.(R)密码算法和基体应可更新	R	P
5.5.4	Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.(R)在初始化状态下通过网络接口访问设备的功能（模块），只有在该接口上进行身份验证后才可进行	R	T
5.5.5	Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate.(M)设备功能，只有在认证后才能访问，和允许通过网络接口对配置进行安全相关的更改。例外情况：网络服务协议所依赖的就是这个设备，而制造商不能保证设备被正确配置。	M	T
5.5.6	Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and	R	P

	usage.(R)在传输过程中应加密关键安全参数，并应根据技术特性、风险和使用情况进行加密。		
5.5.7	The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.(M)消费者物联网设备应保护通过远程访问网络接口通信的关键安全参数的机密性。	M	T
5.5.8	The manufacturer shall follow secure management processes for critical security parameters that relate to the device.(M)制造商应遵循与设备相关的关键安全参数的安全管理流程。	M	P
5.6	**5.6 Minimize exposed attack surfaces 尽量减少暴露的攻击表面**		
5.6.1	All unused network and logical interfaces shall be disabled.(M)所有未使用的网络和逻辑接口应禁用	M	T
5.6.2	In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.(M)在初始化状态下，设备的网络接口应尽量减少未经认证的安全相关信息的披露。	M	T
5.6.3	Device hardware should not unnecessarily expose physical interfaces to attack. (R)设备硬件不应该不必要地暴露物理接口以受攻击	R	T
5.6.4	Where a debug interface is physically accessible, it shall be disabled in software. (MC, in the case a debug interface is physically accessible)如果调试接口是物理可访问的，则应在软件中禁用	M C	T
5.6.5	The manufacturer should only enable software services that are used or required for the intended use or operation of the device.(R)制造商只应启用用于或要求用于设备的预期用途或操作的软件服务	R	T
5.6.6	Code should be minimized to the functionality necessary for the service/device to operate.(R)应尽量减少服务或设备运行所需的功能	R	T
5.6.7	Software should run with least necessary privileges, taking account of both security and functionality.(R)软件应以最不必要的特权运行，同时考虑到安全性和功能	R	T
5.6.8	The device should include a hardware-level access control mechanism for memory.(R)#该设备应包括用于内存的硬件级访问控制机制.	R	T

5.6.9	The manufacturer should follow secure development processes for software deployed on the device.(R)制造商应遵循设备上部署的软件的安全开发过程	R	P
5.7	**5.7 Ensure software integrity 确保软件的完整性**		
5.7.1	The consumer IoT device should verify its software using secure boot mechanisms. (R)消费者物联网设备应使用安全引导机制验证其软件	R	T
5.7.2	If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.(R)如果检测到软件发生未经授权的更改，设备应提醒用户和/或管理员注意此问题，并且不应连接到比执行警报功能所需的网络更宽的网络	R	T
5.8	**5.8 Ensure that personal data is secure 确保个人资料安全**		
5.8.1	The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.(R) 在设备和服务之间传输的个人数据，特别是相关服务，应通过最佳做法加密加以保护	R	P+T
5.8.2	The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.(M)应保护设备与相关服务之间通信的敏感个人数据的机密性，并采用适合技术和使用性质的密码。	M	P+T
5.8.3	All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.(M)设备的所有外部传感能力应以用户清晰透明的可访问方式记录下来	M	P
5.9	**5.9 Make systems resilient to outages 使系统能够适应中断**		
5.9.1	Resilience should be built in to consumer IoT devices and services, taking into account the possibility of outages of data networks and power.(R)应在考虑到数据网络和电力中断可能性的情况下，为消费者物联网设备和服务提供复原	R	P
5.9.2	Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.(R)消费者物联网设备应在失去网络接入的情况下保持运行和本地功能，并应在恢复电力的情况下“清洁恢复”服务。	R	P
5.9.3	The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.(R)消费者物联网设备应以预期的、可操作的和稳定的状态并有序地连接到网络，同时考虑到基础设施的能力。	R	P
5.10	**5.10 Examine system telemetry data 检查系统遥测数据**		

5.10.1	If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies. (RC, in the case of telemetry data being collected)如果遥测数据是从消费者物联网设备和服务中收集的，如使用和测量数据，则应检查其是否存在安全异常。	R C	P
5.11	**5.11 Make it easy for users to delete user data 使用户方便删除用户数据**		
5.11.1	The user shall be provided with functionality such that user data can be erased from the device in a simple manner.(M)应向用户提供功能，使用户数据能够以简单的方式从设备中擦除	M	P
5.11.2	The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner. (R)应向消费者提供设备上的功能，以便可以简单地从相关服务中删除个人数据	R	P
5.11.3	Users should be given clear instructions on how to delete their personal data.(R)应向用户明确说明如何删除其个人资料	R	P
5.11.4	Users should be provided with clear confirmation that personal data has been deleted from services, devices and applications.(R)应向用户明确确认个人数据已从服务、设备和应用程序中删除。	R	P
5.12	**5.12 Make installation and maintenance of devices easy 使装置安装和维护方便**		
5.12.1	Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.(R)消费者物联网的安装和维护应涉及用户的最小决策，并应遵循安全性最佳可用性实践	R	P
5.12.2	The manufacturer should provide users with guidance on how to securely set up their device.(R)制造商应向用户提供如何安全设置其设备的指导。	R	P
5.12.3	The manufacturer should provide users with guidance on how to check whether their device is securely set up.(R)制造商应向用户提供如何检查其设备是否安全设置的指导。	R	P
5.13	**5.13 Validate input data 验证输入数据**		
5.13.1	The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.(M)消费者物联网设备软件应验证通过用户接口或通过应用程序编程接口(API)或在服务和设备中的网络之间传输的数据输入。	M	T
6	**6 Data protection provisions for consumer IoT 消费者物联网的数据保护规定**		

6.1	The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.(M)制造商应向消费者提供明确和透明的信息，说明个人数据是如何处理的，如何使用，由谁使用，以及用于什么目的，每个设备和服务。这也适用于可以参与的第三方，包括广告商。	M	P
6.2	Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way. (MC, in the case personal data is processed on the basis of consumers' consent)在消费者同意的基础上处理个人资料的，应以有效方式取得这种同意。	M C	P
6.3	Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.(M)同意处理个人资料的消费者应有能力随时撤回	M	P
6.4	If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality. (RC, in the case telemetry data being collected)如果遥测数据是从消费者物联网设备和服务收集的，个人数据的处理应保持在预期功能所需的最低限度。	R C	P
6.5	If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes. (MC, telemetry data being collected)如果遥测数据是从消费者物联网设备和服务中收集的，应向消费者提供信息，说明收集了哪些遥测数据、如何使用遥测数据、由谁使用遥测数据以及用于何种目的。	M C	P

Status	Description
M	the provision is a mandatory requirement
R	the provision is a recommendation
M C	the provision is a mandatory requirement and conditional
R C	the provision is a recommendation and conditional