ETSI EN 303 645 V2.1.1 (2020-06) 译本

网络；

消费级物联网产品的网络安全：基线要求

参考资料

REN/CYBER-0048

关键词

网络安全、物联网、隐私

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel：+33 4 92 94 42 00 传真：+33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

重要通知

本文件可从以下网址下载：
http://www.etsi.org/standards-search

本文件可提供电子版和/或印刷版。未经 ETSI 事先书面授权，不得修改本文件任何电子版和/或印刷版的内容。如果电子版和/或印刷版之间存在或被认为存在内容差异，ETSI 可交付文件的现行版本为以 PDF 格式公开提供的版本，网址为 www.etsi.org/deliver。

本文件使用者应了解，本文件可能会进行修订或更改。
有关本文件和其他 ETSI 文件的现状信息，请访问
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx。

如果您发现本文件存在错误，请将您的意见发送至以下服务机构之一：
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

版权通知

免责声明

1、本免责声明系为保证本文档被正确使用、规避意外风险而设，其初衷在于为读者提供中文参考，促进沟通交流。

2、本文档由高维密码测评技术（山东）有限公司翻译，仅供交流学习使用，不得用于商业用途，转载或传播请注明出处。

3、我司仅出于交流学习之目的制作本文档，因此对于文档中的翻译不当之处，我司不担任任何法律责任或道德谴责。然若读者发现任何翻译错误，请不吝指正，欢迎将相关问题发送至邮箱：**shenglin.xu@gwst.cn**。

目 录

知识产权

重要专利

对规范性交付品至关重要或潜在至关重要的知识产权可能已向 ETSI 申报。ETSI 成员和非成员均可公开获取与这些基本知识产权有关的信息（如有），这些信息可在 ETSI SR 000 314 中找到：ETSI SR 000 314：*"知识产权 (IPR)；就 ETSI 标准通知 ETSI 的重要或潜在基本知识产权"*，可向 ETSI 秘书处索取。最新更新可在 ETSI 网络服务器 (https://ipr.etsi.org/) 上查阅。

根据 ETSI 知识产权政策，ETSI 没有进行任何调查，包括知识产权检索。对于 ETSI SR 000 314（或 ETSI Web 服务器上的更新）中未提及的、对本文件至关重要或可能至关重要的其他知识产权，不作任何保证。

商标

本文件可能包含由其所有者主张和/或注册的商标和/或商号。除标明属于 ETSI 所有的商标和/或商号外，ETSI 对这些商标和/或商号不拥有所有权，也不授予使用或复制任何商标和/或商号的权利。本文件中提及的这些商标并不构成 ETSI 对与这些商标相关的产品、服务或组织的认可。

前言

本欧洲标准 (EN) 由 ETSI 网络安全技术委员会 (CYBER) 制定。

国家转换日期	
本 EN 的通过日期：	2020 年 6 月 19 日
本 EN 的最新宣布日期（doa）	2020 年 9 月 30 日
新国家标准的最新发布日期或本 EN 的认可日期 (dop/e)：	2021 年 3 月 31 日
任何与之冲突的国家标准的撤销日期 (dow)：	2021 年 3 月 31 日

情态动词术语

在本文件中，“应”、“不应”、“可”、“不必”、“将”、“将不”、“能”和“不能”应按照《ETSI起草规范》第 3.2 条（条款表达的口头形式）进行解释。

ETSI 可交付成果中不允许使用“必须”和“禁止”，直接引用时除外。

导言

随着越来越多的家庭设备连接到互联网，物联网 (IoT) 的网络安全问题日益受到关注。人们将个人数据托付给越来越多的在线设备和服务。传统上离线的产品和设备现在都已联网，因此在设计上必须能够抵御网络威胁。

本文件汇集了在联网消费类设备安全方面广受认可的良好做法，形成了一套注重成果的高级规定。本文件旨在为参与消费类物联网产品开发和制造的各方提供产品安全指南。

这些规定主要以结果为重点，而不是规定性的，使各组织能够灵活地创新和实施适合其产品的安全解决方案。

本文件无意解决与消费级物联网产品相关的所有安全挑战。本文件的重点也不在于防范长期/复杂的攻击，或需要对设备进行持续物理访问的攻击。相反，重点在于技术控制和组织政策，这对解决最重要和最普遍的安全缺陷最为重要。总体而言，考虑的是基线安全级别；其目的是防止针对基本设计缺陷（如使用容易猜到的口令）的初级攻击。

本文件提供了一套适用于所有消费类物联网设备的基线规定。本文件旨在由其他标准加以补充，这些标准定义了更具体的规定以及针对特定设备的完全可测试和/或可验证的要求，与本文件一起将促进保证方案的开发。

许多消费类物联网设备及其相关服务都会处理和存储个人数据，本文件有助于确保这些设备符合《一般数据保护条例》（GDPR）[i.7]。设计安全是本文件认可的一项重要原则。

ETSI TS 103 701[i.19]为如何根据本文件中的规定评估和保证物联网产品提供了指导。

本文件中的规定是在对已发布的物联网安全和隐私标准、建议和指南进行审查后制定的，这些标准、建议和指南包括ETSI TR 103 305-3 [i.1], ETSI TR 103 309 [i.2]、ENISA 基线安全建议 [i.8]、英国数字、文化、媒体和体育部 (DCMS) 安全设计报告 [i.9]、物联网安全基金会合规框架 [i.10]、GSMA 物联网安全指南和评估 [i.11]、ETSI TR 103 533 [i.12]、DIN SPEC 27072 [i.20] 和 OWASP 物联网 [i.23]。

注：关于物联网安全标准、建议和指导的映射，可查阅 ENISA Baseline Security Recommendations for IoT - Interactive Tool [i.15] 和 Copper Horse Mapping Security & Privacy in the Internet of Things [i.14]。

随着消费类物联网产品的安全性不断提高，预计本文件今后的修订版将对本文件目前的建议条款做出规定。

1 范围

本文件规定了与网络基础设施（如互联网或家庭网络）连接的消费类物联网设备及其与相关服务交互的高级安全和数据保护条款。相关服务不在此范围内。消费类物联网设备示例的不完全列表包括：

- 连接儿童玩具和婴儿监视器；
- 连接烟雾探测器、门锁和窗户传感器；
- 连接多台设备的物联网网关、基站和集线器；
- 智能摄像头、电视和扬声器；
- 可穿戴健康追踪器；
- 联网的家庭自动化和报警系统，特别是其网关和集线器；
- 联网电器，如洗衣机和冰箱；以及
- 智能家居助手

此外，本文件还涉及受限设备特有的安全考虑因素。

例如： 窗户接触传感器、水浸传感器和能源开关是典型的受限设备。

本文件通过示例和说明性文字，为参与开发和制造消费类物联网的组织如何实施这些规定提供了基本指导。表B.1提供了一个示意图，供读者提供有关条款实施的信息。

非消费级物联网设备，例如主要用于制造、医疗保健或其他工业应用的设备，不在本文件的范围之内。

本文件的制定主要是为了帮助保护消费者，但消费者物联网的其他用户也同样可以从本文件规定的实施中受益。

本文件的附件 A（信息性）旨在为第 4、5 和 6 条（规范性）提供上下文。附件 A 包含设备和参考架构示例以及设备状态示例模型，包括每种状态的数据存储。

2 参考资料

2.1 规范性参考资料

参考文献或具体（以出版日期和/或版次号或版本号标明），或非特定。对于特定参考文献，只适用引用的版本。对于非特定参考文献，引用文件的最新版本（包括任何修订）适用。

未在预期位置公开的参考文件可在 https://docbox.etsi.org/Reference/ 上找到。

注：虽然本条款中包含的任何超链接在发布时有效，但 ETSI 无法保证其长期有效性。下列参考文件对本文件的应用是必要的。

不适用。

2.2 信息参考

参考文献或具体（以出版日期和/或版次号或版本号标明），或非特定。对于特定参考文献，只适用引用的版本。对于非特定参考文献，引用文件的最新版本（包括任何修订）适用。

注： 虽然本条款中包含的任何超链接在发布时有效，但 ETSI 无法保证其长期有效性。

下列参考文件对于本文件的应用并非必要，但它们有助于用户了解特定主题领域。

[i.1] ETSI TR 103 305-3: “CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations”

[i.2] ETSI TR 103 309: “CYBER; Secure by Default - platform security technology”

[i.3] NIST Special Publication 800-63B: “Digital Identity Guidelines - Authentication and Lifecycle Management”

注： 见 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[i.4] ISO/IEC 29147：“信息技术--安全技术--漏洞披露”。

注：见https://www.iso.org/standard/45170.html。

[i.5] OASIS：“CSAF 通用漏洞报告框架 (CVRF)”。

注：见http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/csaf-cvrf-v1.2.html

[i.6] ETSI TR 103 331: “CYBER; Structured threat information sharing”

[i.7] 2016年4月27日欧洲议会和欧盟理事会关于在个人数据处理方面保护自然人以及关于此类数据自由流动的第2016/679号条例（欧盟），并废除第95/46/EC号指令（《通用数据保护条例》）。

[i.8] ENISA：《关键信息基础设施背景下的物联网基线安全建议》，2017 年 11 月，ISBN：978-92-9204-236-3，doi：10.2824/03228。

注 ： 见 https://op.europa.eu/en/publication-detail/-/publication/c37f8196-d96f-11e7a506- 01aa75ed71a1/language-en/format-PDF/source-117211901

[i.9] 英国数字、文化、媒体和体育部：“Secure by Design：改善消费级物联网产品网络安全报告》”，2018 年 3 月。

注：见 https://www.gov.uk/government/collections/secure-by-design。

[i.10] 物联网安全基金会："物联网安全合规框架"，2018年12月第2版。

注 ： 可 登 录 https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf.

[i.11] GSMA：“GSMA 物联网安全指南和评估”。

注： 见 https://www.gsma.com/iot/iot-security/iot-security-guidelines/。

[i.12] ETSI TR 103 533：“SmartM2M；Security；Standards Landscape and Best Practices”。

[i.13] Commission Notice：2016 年欧盟产品规则实施 "蓝色指南"（与欧洲经济区相关的文本），2016/C 272/01。

注： 见《欧洲联盟公报》，https://eur-lex.europa.eu/legal- content/EN/ALL/?uri=OJ:C:2016:272:TOC

[i.14] Copper Horse：《绘制物联网中的安全与隐私》。

注： 见https://iotsecuritymapping.uk/

[i.15] ENISA：“物联网基线安全建议--互动工具”。

注 ： 见 https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/baseline-security- recommendations-for-iot-interactive-tool

[i.16] 物联网安全基础：“了解消费级物联网产品公司对漏洞披露的最新应用”。

注：见https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/Vulnerability- Disclosure-Design-v4.pdf

[i.17] F-Secure：“物联网威胁：家庭中随处可见的‘智能’设备爆炸性增长导致风险不断增加》。

注：见 https://blog.f-secure.com/iot-threats/

[i.18] W3C：“Web of Things at W3C”

注：见 https://www.w3.org/WoT/

[i.19] ETSI TS 103 701：“CYBER；消费类物联网产品的网络安全评估”。

注： 正在开发中。

[i.20] DIN SPEC 27072：“信息技术 - 物联网设备 - 信息安全的最低要求”。

[i.21] GSMA: “Coordinated Vulnerability Disclosure (CVD) Programme”

注：见 https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

[i.22] IoT Security Foundation：“漏洞披露--最佳实践指南”。

注：见https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability- Disclosure_WG4_2017.pdf

[i.23] OWASP物联网（IoT）2018年十大事件。

注： 见https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10。

[i.24] IEEE 802.15.4™-2015：“IEEE 低速率无线网络标准”。

注： 见 https://standards.ieee.org/content/ieee-standards/en/standard/802_15_4-2015.html。

[i.25] ETSI TS 102 221：“智能卡；UICC-终端接口；物理和逻辑特性”。

[i.26] GSMA:“SGP.22 Technical Specification v2.2.1”.

[i.27] ISO/IEC 27005:2018：“信息技术--安全技术--信息安全风险管理”。

注：见 https://www.iso.org/standard/75281.html。

[i.28] Microsoft® Corporation："STRIDE威胁模型"。

注： 见 https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[i.29] ETSI TR 121 905："数字蜂窝电信系统（2+阶段）（GSM）；通用移动电信系统（UMTS）；LTE；3GPP 规范词汇表（3GPP TR 21.905）"。

3 术语、符号和缩写的定义

3.1 条款

为本文件之目的，适用下列术语：

管理员：拥有设备用户最高权限级别的用户，这意味着他们可以更改与预期功能相关的任何配置

相关服务：与设备一起成为整个消费级物联网产品一部分的数字服务，通常需要这些服务来提供产品的预期功能。

例 1： 相关服务可包括移动应用程序、云计算/存储和第三方应用程序编程接口 (APIs)。

例 2： 设备向设备制造商选择的第三方服务传输遥测数据。该服务属于关联服务。

认证机制：用于证明实体真实性的方法 注：“实体”可以是用户或机器。

例：认证机制可以是请求口令、扫描二维码或使用生物指纹扫描仪。

认证值：认证机制使用的属性的个别值。

例：当认证机制要求输入口令时，认证值可以是字符串。当身份验证机制是生物指纹识别时，身份验证值可以是左手的食指指纹。

最佳实践密码学：适用于相应用例的密码学，且没有迹象表明可利用现有技术进行攻击注 1： 这不仅指所使用的加密基元，还包括实施、密钥生成和密钥处理。

注 2：多个组织（如 SDO 和公共机构）维护可用的加密方法指南和目录。

例：设备制造商使用物联网平台提供的通信协议和加密库，并且该库和协议已针对可行的攻击（如重放）进行了评估。

受限设备：由于预期用途的限制，在数据处理能力、数据通信能力、数据存储能力或与用户交互能力方面受到物

理限制的设备。

注 1：物理限制可能是由于电源、电池寿命、处理能力、物理访问、有限的功能、有限的内存或有限的网络带宽造成的。这些限制可能要求受限设备由其他设备（如基站或配套设备）提供支持。

例 1：窗户传感器的电池不能由用户充电或更换；这是一个受限设备。

例 2： 由于存储限制，设备无法更新软件，因此硬件更换或网络隔离是管理安全漏洞的唯一选择。

例 3：低功率设备使用电池，可在多个地点部署。
执行高功率加密操作会迅速缩短电池寿命，因此它依赖基站或集线器对更新进行验证。

例 4：设备没有显示屏来验证蓝牙配对的绑定代码。

例 5：设备无法输入（如通过键盘）验证信息。

注 2：具有有线电源并能支持基于 IP 的协议和这些协议所使用的加密原语的设备不受限制。例 6： 某设备由电源供电，主要使用 TLS（传输层安全）进行通信。

消费者：为其贸易、商业、手工业或职业以外的目的行事的自然人 。

注：包括任何规模的企业在内的组织都会使用消费者物联网。例如，智能电视就是家庭安全套件可以保护小型企业的场所。

消费者物联网设备：与相关服务有联系的网络连接（和网络可连接）设备，消费者通常在家中使用，或作为电子可穿戴设备使用。

注 1：消费类物联网设备通常也用于商业环境。这些设备仍归类为消费类物联网设备。

注 2：消费者通常可在零售环境中购买消费类物联网设备。消费者物联网设备也可以委托专业人员安装和/或调试。

关键安全参数：与安全有关的秘密信息，泄露或修改这些信息会危及安全模块的安全。例：加密密钥、认证值（如口令、PIN 码）、证书的私密部分。

调试接口：制造商用于在开发过程中与设备通信或对设备问题进行分流的物理接口，不作为面向消费者功能的一部分使用。

例：测试点、UART、SWD、JTAG。

确定的支持期：制造商提供安全更新的最短期限，以期限或结束日期表示。

注： 本定义侧重于安全方面，不包括与产品支持有关的其他方面，如保修。

设备制造商：制造组装好的最终消费级物联网产品的实体，该产品可能包含许多其他供应商的产品和组件.

出厂默认设置：设备出厂重置后或最终生产/组装后的状态。

注： 这包括组装后的物理设备和软件（包括固件）。

初始化：激活设备网络连接的操作，并为用户或网络访问设置认证功能的过程。

初始化状态：设备初始化后的状态。

物联网产品：消费类物联网设备及其相关服务

可隔离：能够从其所连接的网络中移除，所造成的任何功能损失仅与其连接有关，而与其主要功能无关；或者能够与其他设备一起放置在一个独立的环境中，前提是能够确保该环境中设备的完整性。

例：智能冰箱有一个与网络连接的触摸屏界面。该界面可以拆卸，但不会影响冰箱对冰箱内物品的冷藏。

逻辑接口：利用网络接口通过通道或端口进行网络通信的软件应用。

制造商：供应链中的相关商业运营商（包括设备制造商）。

注：本定义承认消费级物联网产品生态系统中涉及的参与者种类繁多，分担责任的方式复杂。除设备制造商外，这些实体还可以是：进口商、分销商、集成商、组件和平台提供商、软件提供商、IT 和电信服务提供商、

管理服务提供商和相关服务提供商。

网络接口：可用于通过网络访问消费级物联网产品功能的物理接口。

所有者：拥有或购买设备的用户。

个人数据：与已识别或可识别的自然人有关的任何信息。

注：使用该术语是为了与熟知的术语保持一致，但在本文件中没有法律意义。

物理接口：用于在物理层与设备通信的物理端口或空中接口（如无线电、音频或光接口）。

例：无线电、以太网端口、USB 等串行接口以及用于调试的接口。

公共安全参数：与安全相关的公共信息，修改这些信息会危及安全模块的安全。

例 1：用于验证软件更新真实性/完整性的公开密钥。

例 2：证书的公共部分。

远程访问：可从本地网络以外访问。

安全模块：实现安全功能的一套硬件、软件和/或固件。

例： 一台设备包含一个硬件信任根、一个在可信执行环境中运行的加密软件库，以及操作系统中用于执行安全（如用户分离和更新机制）的软件。这些都构成了安全模块。

安全更新：针对制造商发现或报告的安全漏洞的软件更新。

注：如果漏洞的严重程度需要更高的优先级修复，软件更新可以是纯粹的安全更新。

敏感安全参数：关键安全参数和公共安全参数。

软件服务：设备中用于支持功能的软件组件。

例：设备软件内使用的编程语言的运行时间，或暴露设备软件使用的 API（如加密模块的 API）的守护进程。

遥测：来自设备的数据，可提供信息帮助制造商识别与设备使用相关的问题或信息。

例：消费级物联网设备向制造商报告软件故障，使其能够识别并纠正故障原因。

每个设备的唯一性：特定产品类别或类型的每个设备的唯一性。

用户：自然人或组织。

3.2 符号

空白。

3.3 缩略语

本文件使用以下缩写：

API 应用程序接口

ASLR 地址空间布局随机化

CVD 协调漏洞披露

CVRF 通用漏洞报告框架

DDoS 分布式拒绝服务攻击

DSC 专用安全组件

ENISA 欧盟网络和信息安全局

EU 欧盟

GDPR 通用数据保护条例

GSM 全球移动通讯系统

GSMA GSM 协会

IEEE 电气和电子工程师学会

IoT 物联网

IP 互联网协议

ISO 国际标准化组织

JTAG 联合测试行动小组

LAN 局域网

LoRaWAN 远程广域网

MAC 介质访问控制

NIST 国家标准与技术研究所

NX 不执行

OTP 一次性口令

QR 快速反应

SBOM 软件物料清单

SDO 标准开发组织

SE 安全元素

SSID 服务设备标识符

STRIDE 欺骗，篡改，拒绝，信息披露，拒绝服务，提升特权

SWD 串行线调试

TEE 可信执行环境

TS 技术规范

UART 通用异步收发两用机

UI 用户交互界面

UK 联合王国（英国）

USB 通用串行总线

WAN 广域网

4 报告实施情况

风险评估和威胁建模（如 ISO/IEC 27005:2018 [i.27] 和 STRIDE 威胁模型 [i.28]）为本文件条款的实施提供了信息；这由设备制造商和/或其他相关实体执行，不在本文件的范围内。对于某些用例，在进行风险评估后，除了本文件中包含的规定外，也可以适用于其他规定。

本文件设定了一个安全基线；但是，由于消费级物联网产品的范围很广，我们认识到条款的适用性取决于每个设备。本文件通过使用非强制性语气的“应”（建议），提供了一定程度的灵活性。

规定 4-1 对于本文件中认为不适用于消费级物联网设备或消费级物联网设备无法满足的每项建议，应记录其理由。

表 B.1 提供了以结构化方式记录这些理由的模式。这样做是为了让其他利益相关方（如保证评估员、供应链成员、安全研究人员或零售商）确认规定是否得到了正确和适当的应用。

例 1： 制造商在其网站上公布表 B.1 的完整版本，并附上产品说明。

例 2： 制造商填写表 B.1 以供内部记录保存使用。之后，外部保证机构根据本文件对产品进行评估，并要求与产品安全设计相关的信息。制造商可以很容易地提供这些信息，因为它们都包含在表 B.1 中。

消费级物联网设备不适用或不履行条款的情况包括：

- 当设备属于受限设备，无法实施某些安全措施，或不适合已识别的风险（安全或隐私）时；
- 不包括规定中所述功能的设备（例如，只提供数据而不要求验证的设备）。

例 3： 电池寿命有限的窗户传感器在触发时通过远程相关服务发送警报，并通过集线器进行控制。与其他消费类物联网设备相比，它的电池寿命和处理能力有限，因此是一种受限设备。此外，由于用户通过集线器控制设备，因此用户无需使用口令或其他身份验证机制直接对设备进行身份验证。

5 消费级物联网产品的网络安全规定

5.1 不使用通用默认口令

规定 5.1-1 在使用口令的情况下，除出厂默认设置外，所有消费类物联网设备的口令必须是每个设备唯一的或由用户定义的。

注意：有许多机制可用于执行身份验证，口令不是验证用户身份进入设备的唯一机制。但是，如果要使用口令，则应遵循 NIST 特别出版物 800-63B [i.3] 中有关口令的最佳做法。在机器对机器验证中使用口令通常是不合适的。

许多消费类物联网设备在销售时，从用户界面到网络协议都使用通用默认用户名和口令（如 “admin，admin”）。继续使用通用默认值是物联网中许多安全问题的根源[i.17]，因此必须停止这种做法。上述规定可通过以下方式实现：使用每个设备都独一无二的预装口令，和/或要求用户在初始化时选择一个符合最佳实践的口令， 或使用其他不使用口令的方法。

例 1： 在初始化过程中设备会生成证书，用于验证用户通过相关服务（如移动应用程序）进入设备。

为了提高安全性，可以使用多因素认证（如使用口令加 OTP 程序）来更好地保护设备或相关服务。拥有唯一且不可更改的身份可进一步加强设备的安全性。

规定 5.1-2 在使用每个设备预装的唯一口令时，这些口令的生成机制应能降低针对某类或某型设备的自动攻击风险。

例 2： 预装口令具有足够的随机性。

举个反例，带有递增计数器的口令（如 "password1"、"password2 "等）很容易被猜到。此外，使用与公共信息（在空中或网络内发送）（如 MAC 地址或 Wi-Fi® SSID）明显相关的口令，可以通过自动方式检索口令。

规定 5.1-3 用于对用户进行设备身份验证的验证机制应使用与技术特性、风险和使用情况相适应的最佳加密方法。

规定 5.1-4 如果用户可以对设备进行验证，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认证值。

例 3： 对于生物识别认证值，设备制造商允许通过针对新的生物识别技术进行再训练来改变认证值。

例 4：父母在设备上为子女创建一个帐户，并选择和管理子女使用的 PIN 或口令。家长是设备的管理员，可以限制孩子更改 PIN 或口令。

例 5：为使用户更改口令简单易行，制造商在设计口令更改程序时，将所需步骤减至最少。制造商应在用户手册和视频教程中说明这一过程。

用于验证用户身份的认证机制，无论是指纹、口令还是其他令牌，其值都需要可以更改。当这种机制是设备正常使用流程的一部分时，更改就比较容易。

规定 5.1-5 当设备不是受限设备时，应具备一种机制，使通过网络接口对验证机制的暴力攻击变得不可行。

例 6： 设备对一定时间间隔内的身份验证尝试次数有限制。并且会延长每次尝试之间的时间间隔。

例 7： 客户端应用程序可以锁定账户，或在一定次数的身份验证尝试失败后延迟其他身份验证尝试。

该条款针对的是执行“凭证填充”或耗尽整个密钥空间的攻击。重要的是，消费类物联网设备能检测到这些类型的攻击并进行防御，同时防范相关的“资源耗尽”和拒绝服务攻击威胁。

5.2 实施管理漏洞报告的方法

规定 5.2-1 制造商应公开漏洞披露政策。该政策至少应包括：

- 报告问题的联系信息；以及
- 有关以下方面时间表的信息：
  1) 初步确认收到；以及
  2) 报告的问题得到解决之前的状态更新。

漏洞披露政策明确规定了安全研究人员和其他人员报告问题的程序。这种政策可根据需要进行更新，以进一步确保制造商与安全研究人员之间交往的透明度和清晰度，反之亦然。

协调漏洞披露（CVD）是一套处理潜在安全漏洞披露并支持漏洞修复的流程。国际标准化组织（ISO）在关于漏洞披露的 ISO/IEC 29147 [i.4] 中将 CVD 标准化，并已在全球一些大型软件公司中获得了成功案例。

在物联网行业，CVD 目前还没有得到很好的发展[i.16]，因为一些公司对与安全研究人员打交道持保留态度。在这里，CVD 为公司提供了管理这一过程的框架。这为安全研究人员提供了一个向公司通报安全问题的渠道，使公司能够提前应对恶意利用的威胁，并有机会在公开披露之前应对和解决漏洞问题。

规定 5.2-2 对披露的漏洞应及时采取行动。

对不同漏洞采取行动的“及时性”定义差别很大，要视具体事件而定；但按照惯例，软件解决方案的漏洞处理过程应在90天内完成，包括提供补丁和通知问题。硬件修复可能比软件修复需要更长的时间。此外，与服务器软件修复相比，必须部署到设备上的修复可能需要更多时间。

规定 5.2-3 在规定的支持期内，制造商应持续监控、识别和纠正其销售、生产、已生产的产品和服务以及其运营的服务中的安全漏洞。

注 1：制造商应对产品中使用的所有软件和硬件组件采取适当的谨慎措施，包括对提供相关服务以支持产品功能的第三方采取适当的谨慎措施。

软件解决方案通常包含开放源代码和第三方软件组件。创建和维护所有软件组件及其子组件的列表是监控产品漏洞的前提条件。
有各种工具可以扫描源代码和二进制文件，并建立所谓的“软件物料清单”（SBOM），以识别第三方组件和产品中使用的版本。然后利用这些信息监控每个已识别软件组件的相关安全和许可风险。

首先应直接向受影响的利益相关方报告漏洞。如果无法做到这一点，可向国家当局报告漏洞。我们还鼓励制造商与相关行业机构共享信息，如 GSMA [i.21] 和物联网安全基金会。物联网安全基金会[i.22]提供了协调漏洞披露指南，其中参考了 ISO/IEC 29147 [i.4]。

预计将在规定的支持期限内对设备执行此操作。不过，制造商可以在支持期外继续执行，并发布安全更新来修正漏洞。

提供物联网产品的制造商有责任关心消费者和第三方，因为他们可能会因为没有实施 CVD 计划而受到伤害。此外，通过行业机构分享这些信息的公司还能帮助其他面临同样问题的公司。

根据具体情况，披露可以包括不同的方法：

- 与单个产品或服务相关的漏洞：预计问题会直接报告给受影响的利益相关方（通常是设备制造商、物联网服务提供商或移动应用程序开发商）。这些报告的来源可以是安全研究人员或业内同行。
- 系统漏洞：设备制造商等利益相关者可能会发现潜在的系统性问题。虽然在设备制造商自己的产品中修复该问题至关重要，但共享该信息对行业和消费者都有很大好处。同样，安全研究人员也可以报告此类系统漏洞。对于系统性漏洞，相关的行业主管机构可以协调更大规模的应对措施。

注 2：通用漏洞报告框架（CVRF）[i.5] 也可用于交换安全漏洞信息。

根据 ETSI TR 103 331 [i.6]，网络安全威胁信息共享可支持各组织开发和生产安全产品 。

5.3 不断更新软件

及时开发和部署安全更新是制造商为保护其客户和更广泛的技术生态系统所能采取的最重要行动之一。良好的做法是对所有软件进行更新和维护。

5.3-3 至 5.3-12 的每一条规定都取决于根据规定 5.3-1 或 5.3-2 实施的更新机制。

规定 5.3-1 消费级物联网设备中的所有软件组件都应可安全升级。

注 1：成功管理软件更新通常依赖于设备与制造商之间软件组件版本信息的通信。

并非设备上的所有软件都可以更新。

例 1： 设备上的第一阶段引导加载程序只写入设备存储空间一次，从此不可更改。

例 2： 在有多个微控制器的设备上（如一个用于通信，一个用于应用程序），其中一些微控制器可能无法更新。

规定 5.3-2 当设备不是受限设备时，应具有安全安装更新的更新机制。

注 2：在某些情况下，即使 5.3-2 不适用，规定 5.3-1 也适用。

“可安全更新”和“安全安装”意味着有足够的措施防止攻击者滥用更新机制。

例 3： 措施可包括使用真实的软件更新服务器、受完整性保护的通信渠道、验证软件更新的真实性和完整性。需要认识到软件更新机制和“安装”在定义上存在很大区别。

例 4：基于版本检查的防回滚策略可用于防止降级攻击。

更新机制包括设备直接从远程服务器下载更新、从移动应用程序传输更新或通过 USB 或其他物理接口传输更新。如果攻击者破坏了这一机制，则能够在设备上安装恶意软件。

规定 5.3-3 用户应能便捷地进行更新。

便捷程度取决于设备的设计和预期用途。应用简单的更新会自动应用，或使用相关服务（如移动应用程序）启动，或通过设备上的 Web 界面启动。如果更新难以应用，就会增加用户反复推迟更新设备的几率，使设备处于易受攻击的状态。

规定 5.3-4 软件更新应采用自动机制。

如果自动更新失败，在某些情况下，用户可能无法再使用设备。看门狗等检测机制以及双库闪存或恢复分区的使用可以确保设备恢复到已知的良好版本或出厂状态。

作为自动更新的一部分，可以以预防性方式为设备提供安全更新，从而在安全漏洞被利用之前将其消除。管理起来可能比较复杂，尤其是在同时有相关服务更新、设备更新和其他服务更新需要处理的情况下。因此，一个明确的管理和部署计划对制造商来说是有益的，对消费者来说，更新支持的现状也是透明的。

在许多情况下，发布软件更新很大程度上依赖于其他组织，如生产子组件的制造商；但是，这并不是拒绝更新的

理由。制造商在开发和部署安全更新时，不妨考虑整个软件供应链。

通常建议不要将安全更新与功能更新等更复杂的软件更新捆绑在一起。引入新功能的功能更新可能会触发额外的要求，并延迟向设备交付更新。

例 5： 根据欧盟产品立法，功能更新可能会改变设备的预期用途，从而使其成为新产品，需要进行新的合格评定。不过，影响有限的软件更新可视为维护更新，不需要进行新的符合性评估。有关欧盟产品立法背景下软件更新影响的更多信息，请参阅《蓝色指南》[i.13]。

规定 5.3-5 设备应在初始化后检查是否有安全更新，并定期检查。

例 6： 可通过设备初始化界面向用户显示是否存在更新。

例 7：设备每天在随机时间检查可用更新。

对于某些产品，由相关服务而非设备本身来执行此类检查可能更为合适。

规定 5.3-6 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这些功能并进行配置， 以便用户可以启用、禁用或推迟安装安全更新和/或更新通知。

从消费者权益和所有权的角度来看，用户对是否接收更新拥有控制权是非常重要的。用户选择不升级是有充分理由的，其中包括安全性。此外，如果更新部署后发现会导致问题，制造商可以要求用户不要升级软件，以免这些设备受到影响。

规定 5.3-7 设备应使用最佳实践加密技术来促进安全更新机制。

规定 5.3-8 安全更新应及时。

安全更新的“及时性”含义可能会有变化，这取决于特定的问题和修复方法，以及其他因素，如到达设备的能力或设备的限制因素。重要的是，制造商应优先处理修复关键漏洞（即可能造成大规模负面影响的漏洞）的安全更新。由于现代软件结构复杂，通信平台无处不在，安全更新可能涉及多个利益相关方。

例 8： 某软件更新涉及第三方软件库供应商、物联网设备制造商和物联网服务平台运营商。这些利益相关者之间的合作可确保软件更新的及时性。

规定 5.3-9 设备应验证软件更新的真实性和完整性。

确认更新有效的常用方法是验证其完整性和真实性。这可以在设备上完成，但受限于设备的功率，执行加密操作的成本会很高。在这种情况下，可以由另一个可信的设备进行验证。经过验证的更新将通过安全通道发送到设备。在集线器上对更新进行验证，然后再在设备上进行验证，这样可以降低泄密风险。

设备在检测到无效和潜在恶意更新时采取应对措施是一种很好的做法。除了拒绝更新外，设备还可以向适当的服务部门报告事件和/或通知用户。此外，还可以采取缓解控制措施，防止攻击者绕过或滥用更新机制。作为更新机制的一部分，尽可能少地向攻击者提供信息，可降低他们利用该机制的能力。

例 9：当设备检测到更新无法成功交付或应用（完整性或身份验证检查失败）时，设备可以通过不向更新过程的发起者提供任何有关失败的信息来减少信息泄漏。不过，设备可以生成日志条目，并通过安全通道将日志条目通知发送给受信任的一方（如设备管理员）这样就可以知道事件的发生，设备所有者或管理员就可以做出适当的响应。

规定 5.3-10 在通过网络接口传送更新时，设备应通过信任关系验证每次更新的真实性和完整性。

注 3：有效的信任关系包括：经过身份验证的通信渠道、要求设备拥有关键安全参数或口令才能加入的网络、基于数字签名的更新验证或用户确认。

注 4：信任关系的验证对于确保非授权实体（如设备管理平台或设备）无法安装恶意代码至关重要。

规定 5.3-11 制造商应以可识别和明显的方式告知用户需要进行安全更新，并提供有关该更新可减轻的风险的信息。

例 10：制造商通过用户界面上的通知或电子邮件通知用户需要更新。

规定 5.3-12 设备应在应用软件更新将中断设备基本功能时通知用户。

注 5：如果通知是由关联服务发出的，则不需要这样做。

该通知可以包含更多细节，例如设备离线的预计持续时间。

例 11：通知中包含有关停机的紧迫性和大致预计持续时间的信息。

对用户来说，设备在更新期间能否继续运行至关重要。这就是为什么上述条款建议在可能的情况下，在更新会中断功能时通知用户。特别是那些具有安全相关功能的设备，在更新时不应该完全关闭，而应该具有一些最基本的系统功能。如果考虑不周或管理不当，功能中断可能成为某些类型设备和系统的关键安全问题。

例 12：在更新期间，手表将继续显示时间，家用恒温器将继续保持合理的温度，智能锁将继续锁门和开锁。

规定 5.3-13 制造商应以对用户明确和透明的方式公布规定的支持期。

在购买产品时，消费者希望明确了解软件更新支持的期限。

规定 5.3-14 对于不能更新软件的受限设备，制造商应以对用户清晰和透明的方式公布不进行软件更新的理由、硬件更换支持的期限和方法以及规定的支持期限。

规定 5.3-15 对于无法更新软件的受限设备，产品应可隔离，硬件可更换。

在某些情况下，设备无法打补丁。对于受限制的设备，需要制定更换计划，并明确告知消费者。该计划通常会详细说明何时需要更换技术，以及在适用的情况下，何时结束对硬件和软件的支持。

规定 5.3-16 消费级物联网设备的型号标识应通过设备上的标签或物理接口清晰可辨。这通常是通过逻辑接口与设备进行通信，但也可以是用户界面的一部分。

例 13：某设备有一个 HTTP（或 HTTPS（如适用））API，可报告型号名称（用户认证后）。

要检查软件更新的规定支持期或软件更新的可用性，通常需要了解设备的具体名称。

5.4 安全存储敏感的安全参数

规定 5.4-1 持久存储中的敏感安全参数应被设备安全地存储。

安全存储机制可用于确保敏感安全参数的安全。根据 ETSI TR 121 905 [i.29], ETSI TS 102 221 [i.25] /根据 GSMA SGP.22 技术规范 v2.2.1 [i.26]的嵌入式UICC，适当的机制包括由可信执行环境 (TEE) 提供的机制、与硬件相关的加密存储、安全元件 (SE) 或专用安全组件 (DSC) 以及在 UICC 上运行的软件的处理能力。

注： 本规定适用于持久存储，但制造商也可对内存中的敏感安全参数采用类似方法。

例 1： 授权和访问许可的无线电频率（如 LTE-m 蜂窝接入）所涉及的根密钥存储在 UICC 中。

例 2： 使用可信执行环境 (TEE) 来存储和访问敏感安全参数的遥控门锁。

例 3： 无线恒温器将无线网络的凭证存储在防篡改微控制器中，而不是外部闪存中。

规定 5.4-2 如果为安全目的在设备中使用硬编码的每个设备的唯一标识，其实施方式应能抵御物理、电气或软件等手段的篡改。

例 4： 用于网络访问的主密钥对设备而言是唯一的，它存储在符合相关 ETSI 标准（例如，见 ETSI TS 102 221 [i.25]）的 UICC 中。

规定 5.4-3 设备软件源代码中不得使用硬编码的关键安全参数。

对设备和应用程序进行逆向工程，可以轻松发现软件中硬编码的用户名和口令等凭证。这些凭证也可能是允许使用远程服务中安全敏感功能的 API 密钥，或者是设备用于通信的协议安全中使用的私钥。这些凭证通常会出现在源代码中，这是众所周知的不良做法。用于隐藏或加密这些硬编码信息的简单混淆方法也会被轻易破解。

规定 5.4-4 用于软件更新完整性和真实性检查以及保护与设备软件中相关服务通信的任何关键安全参数，必须是每个设备独有的，并应通过一种机制来降低针对设备类别的自动攻击风险。

例 5： 在同一产品类别的每台设备上部署不同的对称密钥，用于生成和验证软件更新的信息验证码。

例 6： 设备使用制造商的公钥验证软件更新。这不是一个关键的安全参数，每个设备不需要是唯一的。

为设备配置独特的关键安全参数有助于保护软件更新的完整性和真实性，以及设备与相关服务的通信。如果全局关键安全参数被使用，其泄露会导致对其他物联网设备的大范围攻击，如创建僵尸网络。

5.5 安全通信

规定 5.5-1 消费级物联网设备应使用最佳实践加密技术进行安全通信。

安全控制的适当性和最佳实践加密技术的使用取决于许多因素，包括使用环境。由于安全问题日新月异，因此很难在给出有关密码学或其他安全措施的规范性建议的同时其不会很快过时。

规定 5.5-2 消费级物联网设备应使用经过审查或评估的实施方案来提供网络和安全功能，特别是在加密领域。

审查和评估可由独立的内部或外部实体进行。

例 1： 开发和测试社区内的分布式软件库、经认证的软件模块和硬件设备加密服务提供商（如安全元件和可信执行环境）都要接受审查或评估。

规定 5.5-3 密码算法和基元应可更新。

注 1：这也被称为“密码灵活性”。

对于无法更新的设备，重要的是设备的预期使用期限不能超过设备所使用的加密算法的建议使用期限（包括密钥尺寸）。

规定 5.5-4 只有在对网络接口进行身份验证后，才能通过处于初始化状态的网络接口访问设备功能。

注 2：功能可因使用情况而有很大不同，可包括访问个人数据和设备制动器等一系列内容。

例如，物联网[i.18]中就有提供公共开放数据的设备。这些设备无需身份验证即可访问，向所有人开放。

设备可通过网络服务中的漏洞被入侵。合适的身份验证机制可以防止未经授权的访问，并有助于设备的深度防御。

规定 5.5-5 允许通过网络接口更改与安全有关的配置的设备功能只能在验证后才能访问。但设备依赖的网络服务协议除外，因为制造商无法保证设备运行所需的配置。

注 3：例外协议包括 ARP、DHCP、DNS、ICMP 和 NTP。

例 2： 与安全相关的更改包括权限管理、网络密钥配置和口令更改。

规定 5.5-6 关键安全参数应在传输过程中加密，加密程度应与技术特性、风险和使用情况相适应。

规定 5.5-7 消费级物联网设备应保护通过远程访问的网络接口进行通信的关键安全参数的机密性。

有许多不同的注册和认证方法。有些认证值是通过带外认证机制提供的，如二维码，有些则是人类可读的，如口令。

如果身份验证机制在每次身份验证尝试中使用唯一值（如在挑战-响应机制中或使用一次性口令作为第二要素时），响应本身就不是身份认证值。不过，对这些值进行保密保护仍然是一种好的做法。

保密保护可通过加密通信信道或有效载荷加密来实现。通常使用的协议或算法的强度至少与传输的密钥材料相当，但也有其他缓解措施，例如需要近距离传输。

规定 5.5-8 制造商应遵守与设备有关的关键安全参数的安全管理程序。

强烈建议使用公开的、经同行评审的关键安全参数（通常称为“密钥管理”）标准 。

5.6 尽量减少暴露的攻击表面

“最小特权原则”是良好安全工程的基石，适用于物联网，也适用于任何其他应用领域。

规定 5.6-1 应禁用所有未使用的网络和逻辑接口。

例 1： 默认情况下，无法从广域网访问本应通过局域网访问的管理用户界面。

例 2： 通过蓝牙®低功耗暴露的直接固件更新 (DFU) 服务用于开发，但预计不会用于生产。它在产品成品中将被禁用。

规定 5.6-2 在初始化状态下，设备的网络接口应尽量减少未经验证的安全相关信息的泄露。

作为初始化过程的一部分，安全相关信息可能会通过网络接口泄露。当设备在建立连接时共享安全相关信息时，攻击者可利用这些信息识别易受攻击的设备。

例 3： 在整个 IP 地址空间中查找易受攻击的设备时，与安全相关的信息可能是设备配置、内核版本或软件版本的信息。

规定 5.6-3 设备硬件不应使物理接口受到不必要的攻击。

攻击者可利用物理接口入侵设备上的固件或内存。“不必要”是指制造商评估开放接口的好处，用于用户功能或调试目的。

例 4： 仅用于为设备供电的微型 USB 端口被物理配置为不允许同时进行命令或调试操作。

规定 5.6-4 如果调试接口可以物理访问，则应在软件中禁用。

例 5： 通过设备上的引导加载程序软件禁用 UART 串行接口。由于禁用，因此没有登录提示和交互式菜单。

规定 5.6-5 制造商应仅启用设备的预期用途或操作所使用或需要的软件服务。

例 6： 制造商没有为设备设置任何非预期用途所需的后台进程、内核扩展、命令、程序或工具。

规定 5.6-6 代码应尽量减少到服务/设备运行所需的功能。

例 7：删除“死”代码或未使用的代码，不视为良性代码。

规定 5.6-7 软件应以最低必要权限运行，同时考虑到安全性和功能性。

例 8： 使用“root”权限运行的最小守护进程/进程。特别是使用网络接口的进程需要非特权用户，而不是“root”用户。

例 9： 在包含多用户操作系统（如 Linux®）的设备上运行的应用程序，每个组件或服务都使用不同的用户。

可以通过堆栈金丝雀、地址空间布局随机化（ASLR）等机制来减轻对设备的软件攻击，这些攻击的目的是破坏内存。制造商可以使用可用的平台安全功能来帮助进一步降低风险。降低运行权限和减少代码也有助于降低风险。

规定 5.6-8 设备应包括存储器的硬件级访问控制机制。

软件漏洞往往利用内存缺乏访问控制来执行恶意代码。访问控制机制限制了设备内存中的数据能否被执行。合适的机制包括 MMU 或 MPU、可执行空间保护（如 NX 位）、内存标记和可信执行环境等技术。

规定 5.6-9 制造商应对设备上部署的软件遵循安全的开发流程。

安全开发流程（包括使用版本控制）或启用与安全相关的编译器选项（如堆栈保护）有助于确保软件成品更加安全。制造商可以在使用支持这些选项的工具链时使用这些选项。

5.7 确保软件的完整性

规定 5.7-1 消费级物联网设备应使用安全启动机制验证其软件。

作为安全启动机制的一部分，硬件信任根是提供强有力证明的一种方法。硬件信任根是系统中的一个组件，所有其他组件都从这个组件中获得“信任”，即系统中加密信任的来源。为了实现其功能，硬件信任根必须可靠， 并能抵御物理和逻辑篡改，因为没有任何机制可以确定该组件已经失效或被修改。通过使用硬件信任根，设备可以对加密功能（如用于安全启动的加密功能）的结果有信心。硬件信任根可以由用于安全存储凭证的机制或其他替代方案提供支持，这些替代方案可提供与特定设备所需安全级别相称的基线安全保证级别。

规定 5.7-2 如果检测到对软件进行了未经授权的更改，设备应提醒用户和/或管理员注意该问题，并且不应连接到比执行警报功能所需的网络更宽的网络。

从未经授权的更改中远程恢复的能力可依赖于已知的良好状态，如本地存储已知的良好版本，以实现设备的安全恢复和更新。这将避免拒绝服务和代价高昂的召回或维护访问，同时管理攻击者破坏更新或其他网络通信机制而接管设备的潜在风险。

如果消费级物联网设备检测到其软件有未经授权的更改，它将能够通知正确的利益相关者。在某些情况下，设备可以进入管理模式。

例：房间里的恒温器可以有用户模式；该模式可防止更改其他设置。如果检测到对软件进行了未经授权的更改，则应向管理员发出警报，因为管理员有能力对警报采取行动（而用户则没有）。

注：如果设备无法成功执行此操作，或者攻击者能够反复造成这种影响，那么迫使设备恢复到已知良好状态的攻击可能会带来 DoS 风险。

5.8 确保个人数据安全

规定 5.8-1 在设备和服务（尤其是相关服务）之间传输的个人数据的保密性应受到保护，并采用最佳的加密技术。

规定 5.8-2 设备和相关服务之间通信的敏感个人数据的保密性应受到保护，并采用与技术和使用特性相适应的加密技术。

注 1：在本条款中，“敏感个人数据”是指披露后极有可能对个人造成伤害的数据。被视为“敏感个人数据”的内容因产品和用例而异，但例子包括：家庭安全摄像头的视频流、支付信息、通信数据内容和带有时间戳的位置数据。进行安全和数据保护影响评估可以帮助制造商做出适当的选择。

注 2：此处的相关服务通常是云服务。此外，这些服务受制造商控制或影响。这些服务通常不由用户操作。

注 3：根据最佳密码学实践，保密性保护通常包括完整性保护。

规定 5.8-3 设备的所有外部传感功能必须以清晰透明的方式记录在案，且能够访问。

例：外部传感能力可以是光学或声学传感器。

本文件第 6 条包含保护个人数据的具体规定。

5.9 使系统能够抵御中断

本条款规定的目的是，随着物联网设备在消费者生活各方面应用的增加，包括与人身安全相关的功能，确保物联网服务保持正常运行。值得注意的是，与安全相关的法规也可以适用，但关键是要避免电力中断作为影响用户的原因，并设计出能提供一定程度的弹性以应对这些挑战的产品和服务。

规定 5.9-1 考虑到数据网络和电力中断的可能性，消费级物联网设备和服务应具有复原能力。

规定 5.9-2 消费品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，并应在断电结束后顺利恢复。

注：“干净利落地恢复”通常是指在相同或改进的状态下恢复连接和功能。

规定 5.9-3 消费者物联网设备应在预期、可操作和稳定的状态下有序地连接网络，同时考虑到基础设施的能力。

例 1： 智能家居在断电后失去了与互联网的连接。网络连接恢复后，家中的设备会在随机延迟后重新连接，以尽量减少网络使用。

例 2： 在提供更新后，制造商会分批通知设备，以防止所有设备同时下载更新。

物联网系统和设备在越来越重要的用例中受到消费者的依赖，这些使用案例可能与安全相关，也可能是性命攸关。在网络中断的情况下保持服务在本地运行是提高复原力的措施之一。其他措施还包括在相关服务中建立冗余，以及减轻分布式拒绝服务（DDoS）攻击或信号风暴的影响，这些攻击或风暴可能是在网络中断后大量设备重新连接造成的。预计必要的恢复能力水平应与使用情况相称并由使用情况决定，同时考虑到依赖该系统、服务或设备的其他人，因为电力中断可能会产生比预期更广泛的影响。

有序的重新连接是指采取明确的步骤，避免大量物联网设备同时发出请求，如软件更新或重新连接。这种明确的步骤可包括在尝试重新连接之前，根据增量后退机制引入随机延迟。

5.10 检查系统遥测数据

规定 5.10-1 如果从消费级物联网设备和服务收集遥测数据（如使用和测量数据），则应检查其是否存在安全异常。

例 1： 安全异常可以通过监控指标显示的设备正常行为偏差来表示，例如登录失败尝试的异常增加。

例 2： 来自多台设备的遥测数据可让制造商发现，由于软件更新真实性检查无效导致的更新失败。

检查包括日志数据在内的遥测数据对安全评估非常有用，可以及早发现并处理异常情况，最大限度地降低安全风险，并快速解决问题。

本文件第 6 条说明了在收集遥测数据时保护个人数据的具体规定。

5.11 方便用户删除用户数据

规定 5.11-1 应向用户提供以简单方式从设备中删除用户数据的功能。

注 1：此处的用户数据是指存储在物联网设备上的所有个人数据，包括个人数据、用户配置和加密材料（如用户口令或密钥）。

规定 5.11-2 应在设备上为消费者提供功能，以便以简单的方式从相关服务中删除个人数据。

此类功能适用于所有权转让、消费者希望删除个人数据、消费者希望从设备中删除服务和/或消费者希望处置设备的情况。预计此类功能符合适用的数据保护法，包括 GDPR [i.7]。

“轻松”删除个人数据是指完成该操作所需的步骤极少，每个步骤的复杂程度也极低。

这种功能有可能成为攻击载体。

规定 5.11-3 应向用户提供如何删除其个人数据的明确说明。

规定 5.11-4 应向用户提供从服务、设备和应用程序中删除个人数据的明确确认。

消费者的物联网设备经常易主，最终将被回收或处理。可以提供一些机制，让消费者能够继续控制并从服务、设备和应用程序中删除个人数据。当消费者希望完全删除其个人数据时，他们也希望能追溯删除备份副本。

从设备或服务中删除个人数据通常不是简单地将设备重置回出厂默认状态就能实现的。在许多使用案例中，消费者不是设备的所有者，但希望从设备和所有相关服务（如云服务或移动应用程序）中删除自己的个人数据。

例：用户可以在租用的公寓内临时使用消费类物联网产品。对产品进行出厂重置可删除配置设置或禁用设备，从而损害公寓所有者和未来用户的利益。出厂重置会删除物联网设备中的所有数据，但这并不是在共享使用的情况下删除单个用户个人数据的适当方式。

注 2：本文件附件 A 包含设备状态的示例模型，包括每个状态的数据存储。

5.12 轻松安装和维护设备

规定 5.12-1 消费者物联网的安装和维护应尽量最小化用户做决定的次数，并遵循可用性方面的安全最佳做法。

例：用户使用向导设置设备，在向导中会显示配置选项子集，并已指定常用默认值和默认情况下已打开的适当安全选项。

规定 5.12-2 制造商应向用户提供如何安全设置设备的指导。

不过，最理想的情况是尽量减少人工干预，自动实现安全配置。

规定 5.12-3 制造商应向用户提供如何检查设备是否安全设置的指导。

通过适当解决用户界面的复杂性和设计不当问题，可以减少甚至消除因消费者混淆或配置错误而导致的安全问题。为用户提供如何安全配置设备的明确指导，也可以减少他们面临的威胁。

在一般情况下，安全设置设备的平均成本高于检查设备是否安全设置的平均成本。从流程的角度来看，安全设置的检查大部分可由制造商通过与设备进行远程通信的自动流程来完成。这种自动程序的一部分可包括验证设备建立安全通信通道的能力。

5.13 验证输入数据

规定 5.13-1 消费级物联网设备软件应验证通过用户界面输入的数据，或通过应用编程接口 (API) 传输的数据， 或在服务和设备的网络之间传输的数据。

在不同类型的界面上传输格式不正确的数据或代码，可能会破坏系统。攻击者或测试人员可使用模糊器等自动化

工具，利用因未验证数据而出现的潜在漏洞和薄弱环节。

例 1：设备接收到的数据不属于预期类型，例如可执行代码而非用户输入的文本。设备上的软件在编写时对输入内容进行了参数化或“转义”处理，从而阻止了这些代码的运行。

例 2：温度传感器接收到超出范围的数据时，不会尝试处理该输入，而是识别出其超出了可能的范围，并将其丢弃，同时在遥测中捕获该事件。

6 消费级物联网产品数据保护规定

许多消费级物联网设备都会处理个人数据。希望制造商在消费类物联网设备中提供支持保护此类个人数据的功能。此外，还有与消费级物联网设备中的个人数据保护相关的法律法规（例如 GDPR [i.7]）。本文件旨在从严格的技术角度帮助消费级物联网设备制造商提供一些保护个人数据的功能说明。

规定 6-1 制造商应向消费者提供清晰透明的信息，说明每种设备和服务的个人数据处理内容、使用方式、使用人和目的。这也适用于可能涉及的第三方，包括广告商。

规定 6-2 在消费者同意的基础上处理个人数据时，应以有效方式获得同意。

“以有效方式”获得同意通常包括让消费者自由、明显和明确地选择是否将其个人数据用于特定目的。

规定 6-3 同意处理其个人数据的消费者可以随时撤销同意。

消费者希望能够通过适当配置物联网设备和服务功能来保护自己的隐私。

规定 6-4 如果从消费级物联网产品设备和服务中收集遥测数据，对个人数据的处理应保持在预期功能所需的最低限度。

规定 6-5 如果从消费者物联网设备和服务中收集遥测数据，应向消费者提供信息，说明收集了哪些遥测数据、如何使用、由谁使用以及用于何种目的。

附件 A（信息性）： 基本概念和模型

A.1 结构

消费级物联网设备是硬件和软件组件的集合，一般具有物理接口，也可以是网络接口。下图 A.1 显示了一个一般示例和一个具体的“智能扬声器”复杂示例。这些架构仅供参考，并不要求设备拥有图中的全部或部分组件。

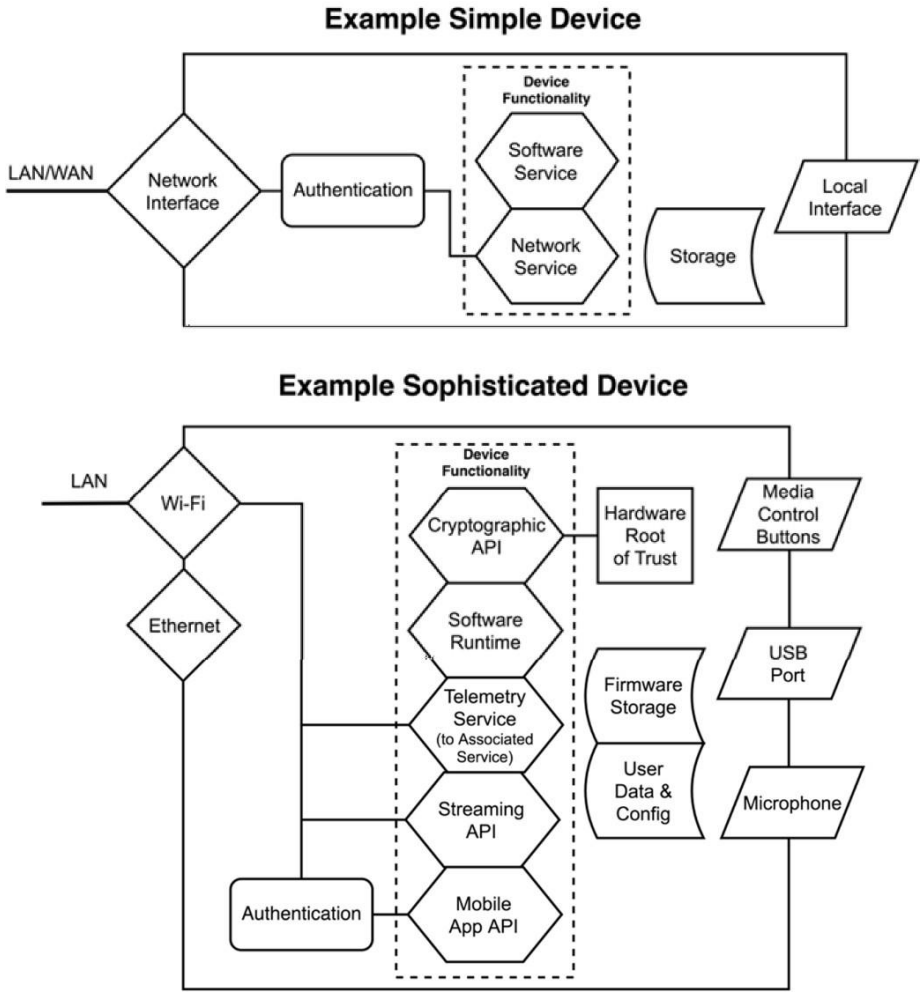

图 A.1：设备总体结构和智能扬声器结构示例

部署在家庭中的消费级物联网产品通常由各种受限和非受限设备组成，这些设备将直接通过 IP 连接（如通过以太网或 Wi-Fi® ）或通过网关或集线器间接连接到局域网。这种与局域网的间接连接通常使用非 IP 连接（例如基于 IEEE 802.15.4 [i.24]的协议）。然后，路由器将局域网连接到广域网（即互联网）。但在某些情况下，家庭中的设备可以通过其他非 IP 或 IP 连接（如 GSM 或 LoRaWAN）直接连接到广域网。

家庭中的消费级物联网设备通常会向外连接（或被连接到）在线或本地服务。在本文件中，制造商提供的服务（例如遥测或配套移动应用程序）或作为初始化的一部分而必须安装的服务被归类为关联服务--如果用户选择安装服务或访问外部内容，则这些服务将不被视为关联服务。例如，某些情况下：

- 通过设备浏览器访问的网站很可能不是关联服务，因为决定访问这些网站的是用户，而不是设备软件开发商；
- 在设备上运行的软件应用程序（如可能安装在智能电视上的“应用程序”）；如果这些程序是默认安装的，则一般被归类为关联服务。但如果是用户自行选择通过商店安装的，则不属于关联服务；
- 连接到遥测平台将是一项相关服务，因为这通常由设备制造商预先配置。

图 A.2 提供了这种部署模式的架构示例。“家庭”边界代表本文件所定义的大致范围，包括与相关服务的通信。

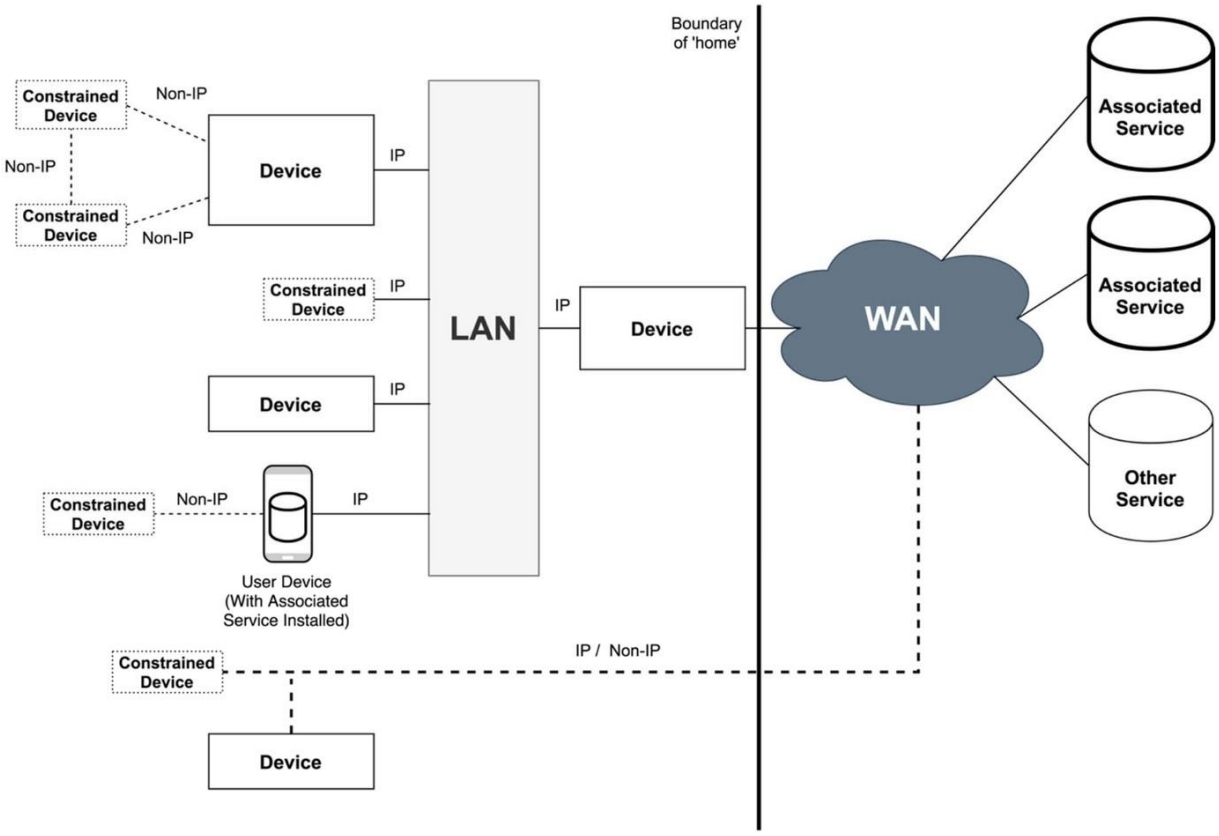

图 A.2：在家庭环境中部署消费级物联网产品的参考架构示例

图 A.3 举例说明了家庭消费级物联网产品的实际部署情况。以下用例说明了如何使用这种设置，并澄清了定义中涵盖和不涵盖的内容：

- 智能电视与两个外部服务进行通信。第一个是设备遥测服务（关联服务）；经用户许可，该服务可从电视中获取信息，如崩溃日志和使用数据，以便开发人员修复软件缺陷并优先开发新功能。智能电视还通过用户在初始化后下载的应用程序连接到视频共享服务。该视频共享服务使用户能够通过第三方应用程序观看娱乐节目，该应用程序可安装在电视使用的操作系统中。这种流媒体服务不属于关联服务。
- 网关可接入各种受限设备，包括一个 IEEE 802.15.4 [i.24] 网状网络和一个光传感器，用于监控和管理家庭。它连接到云访问服务，使用户能够远程控制智能锁并查看传感器的数据。这是一项关联服务。
- 智能冰箱安装了网络浏览器，用户可以使用冰箱浏览新闻网站的头条新闻。新闻网站不属于关联服务。
- 天气传感器供用户用来检测室外温度。由于它远离住宅本身，因此无法连接到局域网。它只能通过GSM 直接与广域网通信。天气传感器连接的服务是关联服务。

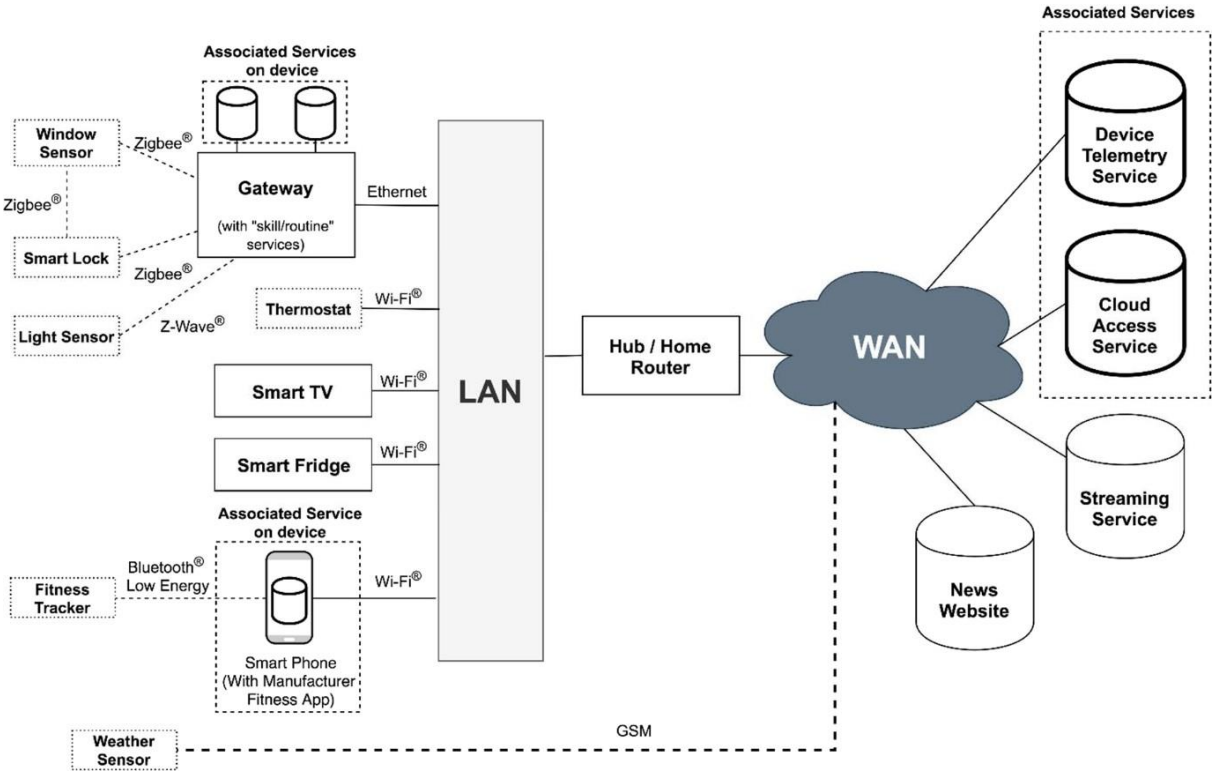

图 A.3：消费级物联网产品部署架构示例

A.2 设备状态

设备退役不属于本文件的范围。退役设备处于不存在敏感数据的状态。设备（从制造到退役）将在几种状态之间转换。图 A.4 举例说明了这些转换，以清楚说明如何在设备中使用所定义的状态。在此模型中，退役设备将处于出厂默认状态，因为出厂重置过程可能是用于删除所有用户数据和配置的过程。

例：设备退役后，可以回收、转售或销毁。

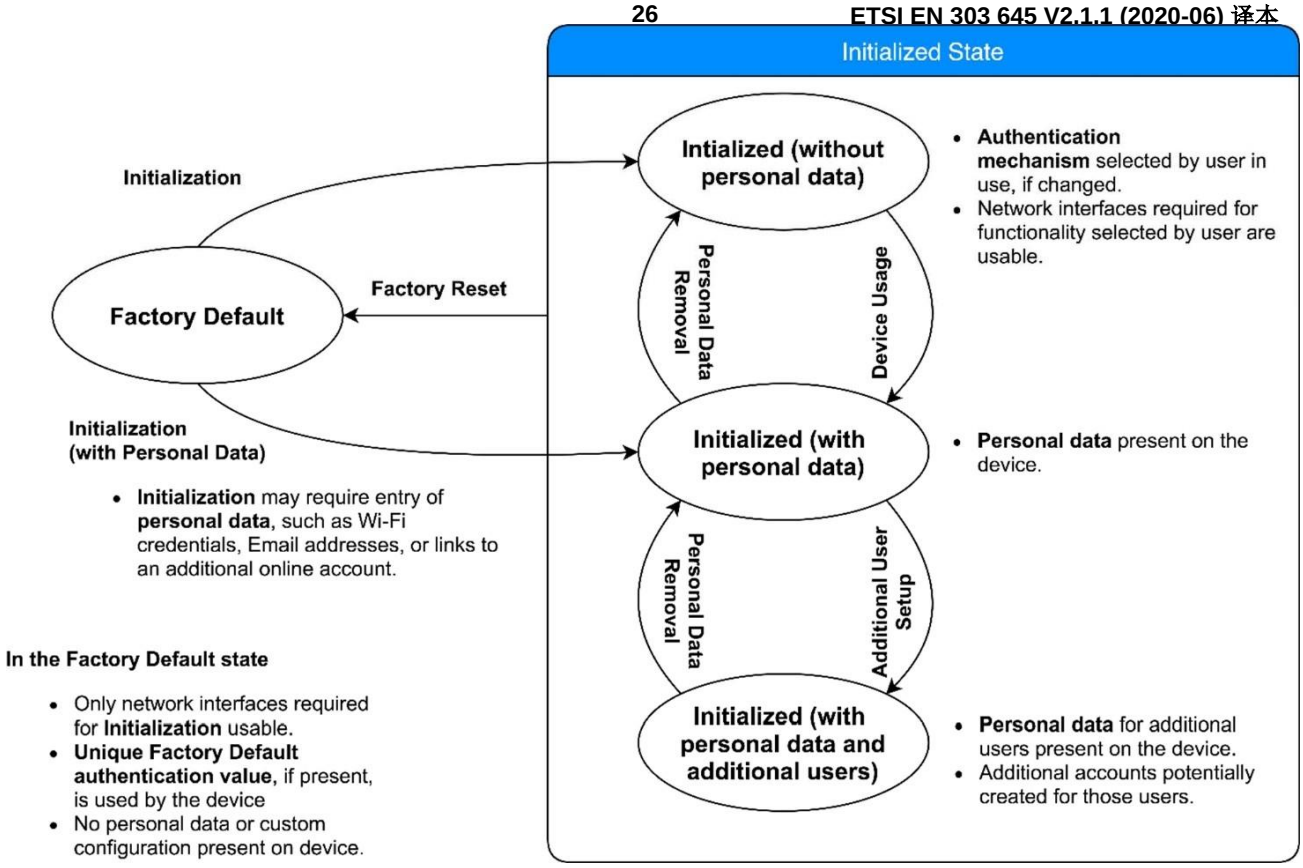

图 A.4：消费类物联网设备状态图

在这些状态下，图 A.5 显示了一个任意设备中存储数据的示例模型。但并不是每种情况都是如此。

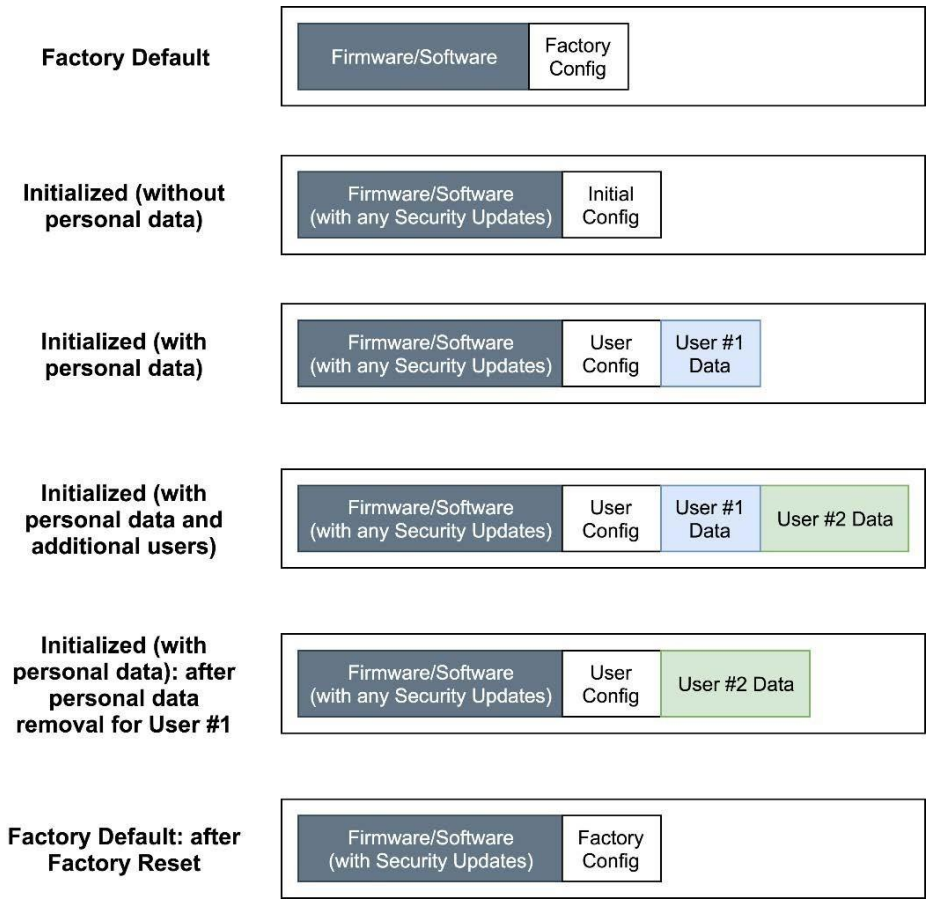

图 A.5：以状态存储设备为例的模型

附件 B（信息性）：
实施一致性声明形式

尽管有与本文件文本有关的版权条款的规定，但 ETSI 允许本文件用户自由复制本附件中的形式，以便用于其预期目的，并可进一步出版包括表 B.1 在内的完整附件。

表 B.1 可为本文件的用户（预计是参与开发或制造消费级物联网产品的实体）提供一个机制，以提供有关本文件内各项规定执行情况的信息。

参考资料一栏注明了本文件中的相关规定。

状态栏表示规定的状态。使用以下符号：

M 该规定为强制性要求

R 该条款是一项建议

MC 该条款为强制性要求，且有条件

RC 该条款为建议性要求，且有条件

注：凡使用条件符号时，均以条款文本为条件。表格底部提供了相关条件，并提供了相关条款的参考资料，以帮助理解。

本文件用户可填写辅助栏。使用以下符号：

Y 受实施支持

N 不受实施支持

N/A 该规定不适用（只有在状态栏中显示该条款是有条件的，且已确定该条件不适用于相关产品的情况下才被允许）。

详细信息栏可由本文件用户填写：

- 如果某项规定受实施支持，详细栏中的条目应包含为实现支持而采取的措施的信息。
- 如果某项规定不受实施支持，详细栏中的条目应包含不可能或不适合实施的原因。
- 如果某项规定不适用，详细栏中的条目应包含做出这一决定的理由。

表 B.1：消费者物联网安全规定的执行情况

条款编号及名称			
参考	**状态**	**支持**	**细节**
5.1 不使用通用默认口令			
5.1-1	MC (1)		
5.1-2	MC (2)		
5.1-3	M		
5.1-4	MC (8)		
5.1-5	MC (5)		
5.2 实施管理漏洞报告的方法			
5.2-1	M		
5.2-2	R		
5.2-3	R		
5.3 不断更新软件			
5.3-1	R		
5.3-2	MC (5)		
5.3-3	MC (12)		
5.3-4	RC (12)		
5.3-5	RC (12)		
5.3-6	RC (9, 12)		
5.3-7	MC (12)		
5.3-8	MC (12)		
5.3-9	RC (12)		
5.3-10	M (11, 12)		
5.3-11	RC (12)		
5.3-12	RC (12)		
5.3-13	M		
5.3-14	RC (3, 4)		
5.3-15	RC (3, 4)		
5.3-16	M		
5.4 安全存储敏感的安全参数			
5.4-1	M		
5.4-2	MC (10)		
5.4-3	M		
5.4-4	M		
5.5 安全通信			
5.5-1	M		
5.5-2	R		
5.5-3	R		
5.5-4	R		
5.5-5	M		
5.5-6	R		
5.5-7	M		
5.5-8	M		
5.6 尽量减少暴露的攻击面			
5.6-1	M		
5.6-2	M		
5.6-3	R		
5.6-4	MC (13)		
5.6-5	R		
5.6-6	R		
5.6-7	R		
5.6-8	R		
5.6-9	R		
5.7 确保软件的完整性			
5.7-1	R		
5.7-2	R		
5.8 确保个人数据安全			
5.8-1	R		
5.8-2	M		
5.8-3	M		

5.9 使系统能够抵御故障			
5.9-1	R		

5.9-2	R		
5.9-3	R		
5.10 检查系统遥测数据			
5.10-1	RC (6)		
5.11 方便用户删除用户数据			
5.11-1	M		
5.11-2	R		
5.11-3	R		
5.11-4	R		
5.12 使设备的安装和维护更加简便			
5.12-1	R		
5.12-2	R		
5.12-3	R		
5.13 验证输入数据			
5.13-1	M		
6 消费级物联网产品数据保护规定			
6.1	M		
6.2	MC (7)		
6.3	M		
6.4	RC (6)		
6.5	MC (6)		

条件

1) 使用口令；
2) 使用预装口令；
3) 软件组件不可更新；
4) 设备受到限制；
5) 设备不受限制；
6) 正在收集的遥测数据；
7) 个人数据的处理以消费者的同意为基础；
8) 允许用户验证的设备；
9) 设备支持自动更新和/或更新通知；
10) 为安全起见，每个设备都使用一个硬编码的唯一标识；
11) 更新通过网络接口传送；
12) 实施更新机制；
13) 调试接口可物理访问。

历史

文件历史		
V1.1.1	2019 年 2 月	作为 ETSI TS 103 645 出版
V2.0.0	2019 年 11 月	EN 批准程序 AP 20200224：2019-11-26 至 2020-02-24
V2.1.0	2020 年 4 月	投票 V 20200619：2020-04-20 至 2020-06-19
V2.1.1	2020 年 6 月	发布