网络运营商的

物联网安全指南

物联网服务生态系统的物联网安全指南

版本 2.0

2017 年 10 月 31 日

本文档是 GSMA 无约束力永久参考文档

安全密级：非机密

对本文档的获取和分发限于安全密级允许的人员。本文档是协会机密信息，受到版权保护。本文档仅用于所述目的，未经协会事先书面批准，不得向安全密级允许人员以外的其他人员披露文档信息或以任何方式令其获取，无论是整个文档还是文档部分内容。

版权声明

免责声明

GSM 协会（以下简称“协会”）不做与本文档信息相关的任何陈述、保证或承诺，不接受相应的责任，对本文档信息的准确性或完整性或及时性概不负责。可能变更本文档中包含的信息，恕不另行通知。

反垄断通知

本文档中包含的信息完全遵守 GSM 协会之反垄断合规政策。

目录

1 简介

1.1 概述

本文档为旨在向物联网服务供应商提供服务的网络运营商提供顶级安全指南，以确保系统安全和数据隐私。本文给出的建议基于目前现成可用的系统和部署的技术。

1.2 文档结构

本文档面向网络运营商和物联网服务供应商。本文档的读者可能也会有兴趣阅读 GSMA 物联网安全指南文档集［11］中的下列其他文档。

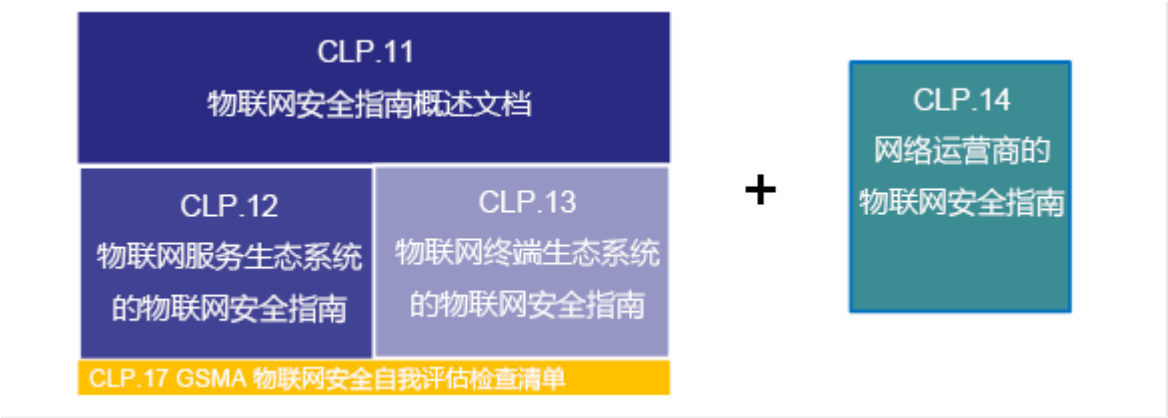


图 1 - GSMA 物联网安全指南文档集的结构

1.3 文档目的和范围

本文档应作为物联网服务供应商与其网络运营商合作伙伴签订供应商协议时的检查表。

本文档的范围仅限于：

- 与物联网服务相关的安全指南。
- 网络运营商提供的安全服务相关建议。
- 蜂窝网络技术。

本文档并非意在建立新物联网规格或标准，但会涉及现行解决方案、标准和最佳实践。

亦非有意加速淘汰当前的物联网服务生态。如果网络运营商现有的物联网服务足够安全，应保持对这些服务的向后兼容性。

物联网服务平台（或物联网连接管理平台）上实施了一些接口和 API，以便物联网服务平台与最终用户（例如通过智能手机或 PC 应用程序与最终用户共享数据）或生态系统中的其他实体共享数据。本文档并不涉及与此类接口和 API 相关的安全问题。应按照互联网安全技术和协议“最佳实践”对此类接口与 API 进行保护。

请注意，必要时，特定地区的国家法律法规可能要高于本文档中所述的指导原则。

1.4 目标受众

本文档的主要受众包括：

- 首先是为物联网服务供应商提供服务的网络运营商。
- 其次是要利用固定线路蜂窝网络开发创新互联产品和服务（即所谓“物联网”）的企业或组织。在本文档中，我们将这些企业称为“物联网服务供应商”。

1.5 定义

术语	描述
设备主机识别报告	终端设备向网络运营商报告主机信息的功能。请参见 GSMA 连接效率指南 [17]
Diameter	Diameter 是一种用于计算机网络的认证、授权和计费协议。请参见 IETF RFC 6733 [18]
终端	物联网终端是一种物理计算设备，作为连接至互联网的产品或服务的一部分执行功能或任务。有关物联网设备的三种常见类别和每个终端类别的示例，请参考 CLP.13 [29] 第 3 节。
网关	网关是一种复杂的终端设备，通常用于桥接轻型终端设备（通过本地网络连接）和广域网。有关详细信息，请参考 CLP.13 [29]。
物联网	物联网是指不同机器、设备和家用电器都可以通过不同网络连接到互联网。这些设备包括日常用品，包括平板电脑和电子消费产品、以及其他机器，如具有发送和接收数据的通信功能的汽车、监视器和传感器。
物联网连接管理平台	通常是由网络运营商托管的系统，以便物联网服务供应商对物联网订阅和价格计划进行自我管理。
物联网服务	利用物联网设备数据执行服务的任何计算机程序。
物联网服务平台	该服务平台由物联网服务供应商托管，与终端进行通信以提供物联网服务。
物联网服务供应商	致力于开发创新互联的新物联网产品和服务的企业或组织。供应商可以是网络运营商。
轻型终端	通常是通过网关设备连接至物联网服务的受限设备（如传感器或致动器）。
网络运营商	将物联网终端设备连接至物联网服务平台的通信网络运营商。
UICC	ETSI TS 102 221 规定的安全元素平台，可支持以密码区分的安全域中多个标准网络或服务验证应用程序。可体现为 ETSI TS 102 671 标准中指定的嵌入式设计规格。
广域网	覆盖地理距离较远的电信网络。

1.6 缩略语

术语	描述
3GPP	第 3 代项目合作伙伴
AKA	验证和密钥协议

术语	描述
APDU	应用程序协议数据单元
API	应用程序编程接口
APN	接入点名称
BGP	边界网关协议
CEIR	中央设备身份寄存器
CERT	计算机应急响应小组
DNS	域名系统
DoS	拒绝服务
DPA	数据处理协议
EAB	扩展接入限制
EAP	可拓展验证协议
EID	eUICC 身份
ETSI	欧洲电信标准协会
EU	欧盟
eUICC	嵌入式 UICC
FASG	反欺诈安全小组
GCF	全球认证论坛
GGSN	网关 GPRS 支持节点
GPRS	通用分组无线服务
GRX	GPRS 漫游交换
GSM	全球移动通信系统
GSMA	GSM 协会
GTP	GPRS 隧道协议
HLR	归属位置寄存器
HSS	归属用户服务器
ICCID	集成电路卡识别码
IMEI	国际移动设备识别码
IMSI	国际移动用户识别码
IoT	物联网
IP	互联网协议
IPSec	互联网协议安全
L2TP	第二层隧道协议
LBO	本地突破
LPWAN	低功率广域网

术语	描述
LTE	长期演进
M2M	机器对机器
MAP	移动应用部分
MME	移动管理实体
OMA	开放移动联盟
OSS	运营支持系统
OTA	远程
PTCRB	伪首字母缩略词，原指 PCS 类型认证审查委员会，但已不再适用。
RAN	无线接入网络
SAS	安全认证计划
SGSN	服务 GPRS 支持节点
SIM	用户识别模块
SMS	短消息服务
SoR	漫游引导
SS7	七号信令系统
UMTS	通用移动通信服务
USSD	非结构化补充服务数据
VLR	访客位置寄存器
VPN	虚拟专用网络
VoLTE	LTE 语音
WAN	广域网

1.7 参考文献

参考文献	文件编号	标题
[1]	ETSI TS 102 225	Secured packet structure for UICC based applications www.etsi.org
[2]	ETSI TS 102 226	Remote APDU structure for UICC based applications www.etsi.org
[3]	3GPP TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application www.3gpp.org
[4]	不适用	Open Mobile API specification www.simalliance.org

参考文献	文件编号	标题
[5]	OMA DM	OMA Device Management www.openmobilealliance.org
[6]	OMA FUMO	OMA Firmware Update Management Object www.openmobilealliance.org
[7]	GSMA SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification www.gsma.com
[8]	ETSI TS 102 310	Extensible Authentication Protocol support in the UICC www.etsi.org
[9]	3GPP TS 23.122	Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode www.3gpp.org
[10]	NISTIR 7298	Glossary of Key Information Security Terms www.nist.gov
[11]	GSMA CLP.11	IoT Security Guidelines Overview Document https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[12]	不适用	Introducing Mobile Connect - the new standard in digital authentication https://www.gsma.com/identity/mobile-connect
[13]	3GPP TS 34.xxx	3GPP 34 series specifications www.3gpp.org/DynaReport/34-series.htm
[14]	3GPP TS 37.xxx	3GPP 37 series specifications www.3gpp.org/DynaReport/37-series.htm
[15]	3GPP TS 31.xxx	3GPP 31 series specifications www.3gpp.org/DynaReport/31-series.htm
[16]	GSMA FS.04	Security Accreditation Scheme for UICC Production http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
[17]	GSMA CLP.03	IoT Device Connection Efficiency Guidelines https://www.gsma.com/iot/iot-device-connection-efficiency-guidelines/
[18]	IETF RFC 6733	Diameter Base Protocol www.ietf.org

参考文献	文件编号	标题
[19]	ETSI TS 102 690	Machine-to-Machine communications (M2M); Functional architecture www.etsi.org
[20]	TR-069	CPE WAN Management Protocol www.broadband-forum.org
[21]	不适用	OpenID Connect openid.net/connect/
[22]	不适用	FIDO (Fast IDentity Online) Alliance fidoalliance.org/
[23]	ETSI TS 102 204	Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface www.etsi.ord
[24]	不适用	National Institute of Standards and Technology (NIST) www.nist.gov
[25]	不适用	European Network of Excellence in Cryptology (ECRYPT) www.ecrypt.eu.org
[26]	GSMA CLP.12	IoT Security Guidelines for IoT Service Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[27]	IETF RFC 5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) tools.ietf.org/html/rfc5448
[28]	IETF RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) tools.ietf.org/html/rfc4186
[29]	GSMA CLP.13	IoT Security Guidelines for IoT Endpoint Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[30]	不适用	Wireless Security in LTE Networks www.gsma.com/membership/wp-content/uploads/2012/11/SenzaFili_WirelessSecurity_121029_FINAL.pdf
[31]	不适用	oneM2M Specifications www.oneM2M.org
[32]	GSMA CLP.17	IoT Security Assessment Checklist https://www.gsma.com/iot/iot-security-assessment/

参考文献	文件编号	标题
[33]	不适用	LPWA Technology Security Comparison. A White Paper from Franklin Heath Ltd https://goo.gl/JIOlr6
[34]	CLP.28	NB-IoT Deployment Guide www.gsma.com/iot
[35]	CLP.29	LTE-M Deployment Guide www.gsma.com/iot
[36]	3GPP TS33.163	Battery efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST) www.3GPP.org

2 网络运营商可以保护的物联网服务资产

为了充分保护物联网服务资产而实施的安全功能具体要取决于各个服务。因此，物联网服务供应商有责任采取适当的风险和隐私影响评估流程，以得出特定的安全需求。网络运营商和物联网服务供应商对于保护资产的安全需求通常是类似的，因此他们可以采用共同的安全解决方案，而不是实施重复（并且可能冗余）的安全基础设施。另外在许多情况下，网络运营商同时也是物联网服务供应商。

在保护用于提供物联网服务的资产时，网络运营商提供的安全服务可以起到关键作用。其中包括：

- 在物联网终端设备和物联网服务平台之间发送的物联网服务数据 – 包括主要的隐私敏感性数据（例如最终用户相关数据）和可能对隐私有一定影响的可商用数据（例如致动器控制数据）。
- 终端设备（包括网关设备）中使用的安全资产（IMSI、密钥集等）和网络配置设置（APN、计时器值等）。
- 物联网服务供应商的业务敏感信息，包括品牌信誉、公司负责的客户/用户数据、战略信息、财务数据及健康记录等。
- 物联网服务供应商的业务基础设施、服务平台、企业网络和其他专用网络元素。
- 网络运营商提供给物联网服务使用的公共（即共享）数据中心基础设施。其中可能包括公共服务、托管功能、虚拟化基础设施、云基础设施等。
- 通信网络基础设施，包括无线接入网络、核心网络、骨干网络、基本服务功能（DNS、BGP 等）、固定和蜂窝网络的接入与聚合等。

3 网络安全原则

网络运营商必须在其网络中实施正确可靠的安全机制。

本节介绍网络如何在物联网生态系统中提供价值。

通信网络提供的最基本安全机制包括：

- 物联网服务相关实体（如网关、终端设备、家庭网络、漫游网络、服务平台）的识别和验证。
- 建立物联网服务需要连接的不同实体的访问控制。
- 保证网络所承载物联网服务信息的安全性（保密性、完整性、可用性、真实性）与隐私所需的数据保护。
- 确保网络资源可用并防止其受到攻击的流程与机制（例如部署适当的防火墙，入侵防御和数据过滤技术）。

3.1 用户、应用程序、终端设备、网络和服务平台的安全识别。

识别包括为物联网服务中的实体提供唯一标识，并将这些电子身份与真实世界中具有法律约束力的身份相关联。

在蜂窝连接的物联网服务中，使用 IMSI 和/或 IMEI 来识别终端设备（EID 也可以用于识别带有 eUICC 的设备）。网络使用网络代码和国家代码进行识别。每种提供身份的方法所对应的安全保障级别都不同。

身份在验证过程中起着至关重要的作用，因为安全验证只能在安全身份的基础上实现。因此，必须保护物联网服务中发放和使用的身份（如 IMSI、IMEI 或 ICCID），防止未经授权的修改、冒充或盗窃。

物联网服务供应商可能面临的一个实际问题是，物联网服务可能需要与许多物联网服务平台进行通信，其中每个平台可能都需要单独的唯一标识。因此，物联网服务需要安全地提供、存储和管理每个用于与各物联网服务平台建立通信链路的身份。

在适用于物联网服务的情况下，网络运营商建议使用基于 UICC 的机制来安全地识别终端设备。网络运营商还可能将 UICC 提供的安全存储功能扩展至物联网服务供应商，使其能够在 UICC 上存储其他物联网服务相关的身份。这项技术同时适用于蜂窝和非蜂窝终端设备（如 EAP-AKA [27]）。

网络运营商还可能提供“单点登录”服务，允许终端设备建立和证明其身份一次，然后无需更多麻烦即可连接至多个物联网服务平台。必须考虑跨多个平台使用这种服务的安全权衡和风险。

3.2 用户、应用程序、终端设备、网络和服务平台的安全验证。

根据 NIST [10] 的定义，“验证”是指“验证用户、过程或终端设备的身份，通常是允许访问信息系统中资源的必要条件”。

网络运营商可以提供服务以确保与物联网服务相关的用户、应用程序、终端设备、网络和服务平台得到安全验证。

验证有一个相关属性，即不可否认性。根据 NIST [10]，不可否认性的定义是：“保证向信息发送者提供送达证明，并且向接收者提供发送者的身份证明，这样双方此后都无法否认曾处理过该信息”。不可否认性取决于在识别该交易或消息来源时认定未违反真实性。

3.3 提供安全的通信信道

网络运营商为广域蜂窝和固定网络提供通信安全机制，以保证“业界最高”的通信完整性、保密性和真实性。在适当情况下，网络运营商可以使用虚拟专用网络 (VPN) 和加密的互联网连接提供并管理与企业网络之间的安全连接。

安全通信信道的目的在于确保在未经数据主体知情和同意的情况下，不处理、使用或传输通过信道发送的数据。加密技术可以确保机密性、完整性和真实性，从而在安全数据传输中起着至关重要的作用。加密技术必须适合所设计和部署的系统，同时考虑到轻型终端设备、网络方面（例如卫星回程限制）以及提供的服务。

网络运营商可以为物联网服务供应商提供数据加密服务，以确保通信完整性和网络恢复能力。

传统上，网络运营商会提供公共电信基础设施或是公共或私有网络基础设施的混合。许多网络运营商可以确保经过其公共网络基础设施的客户/用户数据在进入公共网络基础设施到离开网络之间的某个点进行加密。在需要时，网络运营商还可以协助物联网服务供应商部署或派生自己的加密凭证，以确保物联网数据通过网络运营商基础设施传输期间的保密性。

网络运营商可以为其客户提供专用网络，在其中为单个客户提供专用通信信道，以确保没有数据穿过互联网等公共网络。这种专用网络可通过以下方式创建：

1. 使用第二层隧道协议 (L2TP) 等隧道协议，并通过互联网协议安全 (IPsec) 等协议进行保护，或
2. 使用 BEST [36] 等为客户提供 UE 和应用服务器之间的端到端安全性，或
3. 部署一个带有共享无线网络的单独核心网络实例，为物联网服务创建一个专用网络，如下例所示。

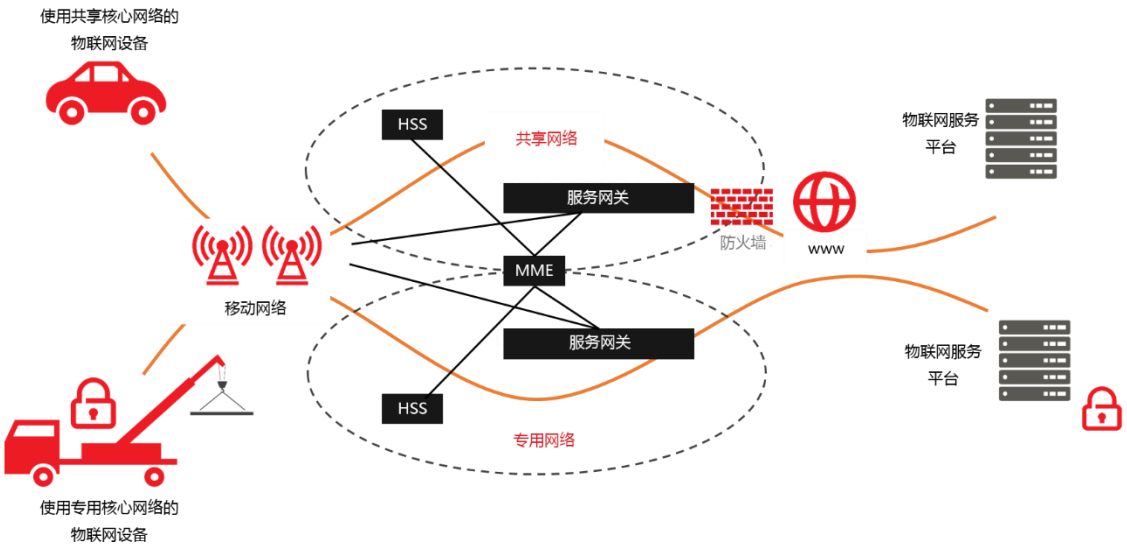


图 2 - 专用网络配置示例

3.4 确保通信信道的可用性

根据 NIST [10]，“可用性”是指经过授权的实体可以根据需要访问和使用的属性。

网络运营商可以为物联网服务供应商提供可用网络。网络运营商提供网络可用性的最基本机制如下：

3.4.1 使用许可频谱

GSMA 网络运营商成员将根据其所在国家监管机构颁发的许可条款，使用专用许可频谱运营网络。使用许可频谱可确保将其他无线电技术的干扰控制在最低限度，因为任何未经授权使用此频谱的行为都会受到惩治。网络运营商和国家监管机构会搜寻任何未经授权的干扰源，以确保网络可用性不受影响。

使用许可频谱可为网络运营商提供用于运营网络的专用无线电频段，确保网络运营商能够进行细致的网络覆盖和容量规划，以确保客户获得最大程度的网络可用性。

3.4.2 实施标准化和成熟的网络技术

GSMA 的网络运营商成员实施 3GPP 等标准机构规定的 GSM、UMTS 和 LTE 等标准化网络技术。使用标准化技术不仅可以确保网络运营商之间的互操作性，还可以确保标准在制定期间经过最大限度的审查，以确保技术的稳健性。

3.4.3 实施经过测试和认证的网络技术

网络运营商网络的许多部分会根据国际测试标准进行测试和认证。复杂终端设备及其包含的通信模块需要遵循 3GPP 测试规范 [13]，通过 GCF、PTCRB 和网络运营商验收测试。无线接入网络 (RAN) 需要遵循 3GPP 测试规范 [14]，通过网络运营商验收测试。UICC 需要遵循 3GPP 测试规范 [15]，通过网络运营商验收测试，此外可能还需要通过 GSMA SAS 认证 [16]。

3.4.4 弹性网络拓扑和配置

网络运营商在必要的地理冗余度和隔离度下实施并构建弹性网络，以最大限度地确保可用性，缩短停机时间。所有网络元素都经过仔细配置并受到监控，以确保达到严格的服务质量和服务级别协议要求。

3.4.5 网络资源的实时监控和管理

网络运营商部署最先进的网络运营中心，全天候实时监控其网络性能，以管理网络流量，响应网络需求并修复故障。有关详细信息，请参见第 4.10 节

3.4.6 威胁管理和信息共享

GSMA 反欺诈安全小组 (FASG) 为所有网络运营商提供一个开放、包容和可信的环境，以及时且负责的方式共享欺诈和安全情报以及事件详细信息。该小组会评估全球欺诈和安全威胁形势，分析网络运营商及其客户的相关风险，确定相应的缓解措施及其优先级。

3.4.7 漫游服务

由于使用标准化的网络和终端设备技术以及互连服务，网络运营商可以提供网络漫游服务，进一步为客户提高网络覆盖和可用性。

3.4.8 终端设备性能监控和管理

网络运营商可以测量与其网络连接的终端设备性能，以隔离可能产生过量无线电干扰（例如不符合国家规定）或网络信令流量（例如不符合 GSMA 连接效率指南 [17]），从而降低整个网络性能的终端设备。因此在检测到异常行为时，可以监控和断开终端设备或者更新其固件。

4 隐私注意事项

为了抓住物联网提供的机遇，消费者必须信任提供物联网服务并收集消费者数据的物联网服务供应商。GSMA 及其成员认为，只有让用户感到自己的隐私得到适当的尊重和保护，才能完全获得消费者的信任与信心。

世界各地已经制定了完善的数据保护和隐私法，并得到网络运营商的实施和遵守。运营商相信，应用现有的数据保护法规和原则可以满足物联网服务与技术环境中的隐私需求。

但是，物联网服务通常需要运营商与物联网服务供应商进行合作。物联网服务需要明确的监管和确定的法律，所有物联网服务供应商无论采用何种服务和技术，始终都需要遵守隐私和数据保护法规。

网络运营商应该了解，只要以任何方式处理数据，就需要与物联网服务供应商签署数据处理协议 (DPA)。针对特定物联网服务制定的数据保护和安全实践，应当反映出个人隐私的整体风险以及收集、分发和使用个人数据的具体状况。监管干预应仅限于已经发现风险且现有措施不足以解决风险的领域。例如，oneM2M（通过 TS-0003 [31]）允许运营商扮演服务供应商隐私管家的角色。

网络运营商可以利用其在解决隐私和安全问题方面的丰富经验，与物联网服务供应商进行合作，以保证物联网技术和整体消费体验的隐私与安全。通过这种协作，能够确保物联网服务供应商在所提供服务的环境中识别和缓解相关的消费者隐私风险。

欲了解更多信息，请查看 GSMA 移动隐私原则：http://www.gsma.com/publicpolicy/mobile-and-privacy/mobile-privacy-principles

5 网络运营商提供的服务

网络运营商可以为物联网服务供应商提供安全的蜂窝和固定广域网 (WAN)。

本节提供了将物联网服务连接至广域网的最佳实践建议。如果适用，这些建议将与所用的技术无关，但同时也会采用蜂窝以及其他网络类型的最佳实践。

5.1 安全订阅管理程序

本节提供了关于网络运营商应如何管理物联网服务供应商订阅的建议：

- 网络运营商或物联网服务供应商应对现在和将来提供物联网服务（语音、数据、SMS 等）所需的网络服务进行评估。
- 网络运营商应当根据此类评估结果，在操作中遵循“最小权限原则”，只为物联网服务供应商的订阅提供特定物联网服务所需的服务。比如：
    - 仅使用数据承载的物联网服务不应提供语音和 SMS 服务。
    - 如果终端设备仅连接至一个已知的物联网服务平台，则设备相关订阅只可允许其连接至一个已知的 IP 地址（或域）白名单。
    - 如果物联网服务使用语音或 SMS，应考虑使用预配置的固定拨号列表。

- 对于与实现关键物联网服务相关的物联网订阅（例如与关键医疗保健服务相关的订阅），网络运营商应当实施安全订阅管理流程。这些服务不可随意断开。
- 网络运营商应区分用于物联网服务的 UICC 和提供传统服务的传统 UICC，并根据物联网服务供应商的要求对这些 UICC 进行适当隔离。
    - 如果将用于物联网服务的 UICC 和用于传统“手机”的 UICC 进行隔离，就可为网络运营商更加安全高效地管理相关订阅提供基础。例如，网络运营商可能考虑对使用寿命较长且配置较好的终端设备采用单独的 HLR/HSS，以便为这些 UICC 提供长期（持续数年）支持。

5.1.1 UICC 供应和管理

5.1.1.1 UICC 的远程管理（空中下载，OTA）

在一些情况下，物联网终端并不能实际接触到。为了对 UICC 进行远程更改，网络运营商应当支持 UICC OTA 管理。UICC OTA 安全机制应遵循最新的 ETSI [1] [2] 和 3GPP [3] 规范，采用最适合物联网服务的安全级别。

物联网终端设备应支持 UICC 识别的必要 APDU 指令，以确保 UICC OTA 指令顺利执行。

5.1.1.2 不可拆卸 UICC

如果物联网服务的威胁模型表明物联网终端设备可能容易遭受物理篡改，则网络运营商应为其提供不可拆卸 UICC（即机器外形因素）。应采取额外的安全措施，以便发现此类威胁并作出响应。

5.1.1.3 嵌入式 UICC（eUICC）的远程管理

如果物联网服务需要将终端设备置于远程或难以到达的位置，网络运营商应提供不可拆卸 UICC（即 eUICC）的安全远程管理。

例如，对于需要管理大量嵌入终端设备中的 eUICC，但自身并不是这些设备的所有者，也无法方便地接触这些设备（如汽车）的物联网服务供应商。

运营商通常使用物联网连接管理平台监测和控制 (e)UICC 为物联网设备提供的通信服务。

网络运营商应支持 GSMA 嵌入式 UICC 远程提供架构技术规范 [7]。

5.1.1.4 基于 UICC 的服务

网络运营商可能为物联网服务供应商提供基于 UICC 的服务。这样，物联网服务供应商就可将 UICC 作为其物联网服务的安全防篡改平台。此类基于 UICC 的服务通常使用 JavaCard™ 开发，可以在所有兼容 JavaCard™ 的 UICC 卡之间进行互操作。这种物联网终端设备应用的一个示例是网络质量监控和报告。对于攻击者能够实际接触到的物联网终端设备，UICC 平台提供的防篡改功能极具价值。将 UICC 作为所有利益相关者的通用安全元素，可以最大程度提高安全物联网设备的成本效益。

UICC 还可用于物联网服务中敏感数据的防篡改存储，包括物联网服务供应商控制的安全密钥。ETSI TS 102 225 [1] 利用 GlobalPlatform 卡片规范中的机密卡内容管理功能，让物联网服务供应商能够彼此独立地管理各自在 UICC 上的安全域。

物联网服务供应商或网络运营商可以要求 UICC 供应商在 UICC 内部创建此类安全域。UICC 的发行者应确保 UICC 受到适当安全密钥的保护，且物联网终端设备可以执行必要的 ADPU 指令以进行访问。

此外，UICC 还可用于加密（使用其安全存储的密钥）和发送物联网服务的敏感内容，或者通过开放移动 API [4] 或 oneM2M TS-0003 [31] 等服务为基于终端设备的应用程序提供安全服务。

5.1.1.5 UICC 的安全制造和提供

网络运营商应向制造和提供过程通过 GSMA 安全认证计划 (SAS) [16] 认证的制造商采购 UICC。

5.2 网络验证和加密算法

本节针对不同广域网提供网络验证和链路加密的建议与最佳实践。

网络运营商应实施符合物联网服务供应商终端设备预期使用寿命的网络验证和算法。

网络运营商提供多种可供物联网服务使用的通信服务，例如 USSD、SMS 和 IP 数据连接。本文档仅讨论 IP 数据连接，因为它是物联网服务最常用的通信服务形式。

许多现有物联网服务使用 USSD 和 SMS，因此需要强调，与 IP 数据连接相比，USSD 和 SMS 的安全支持功能较为有限。一般而言，USSD 和 SMS 流量并非默认由网络运营商和加密保护机制进行“端对端”加密保护以确保 SMS 消息没有的保密性和完整性。使用 USSD 或 SMS 进行通信的物联网服务供应商需要了解与 USSD 和 SMS 相关的漏洞，并在可能的情况下对服务层实施其他加密措施。

5.2.1 GSM/GPRS (2G) 系统安全

提供 GSM/GPRS 网络的网络运营商应当：

- 使用至少 128 位的 A5/3 流密码以保护物联网终端设备和基站之间的链路。网络运营商应尽可能避免使用 A5/1 和 A5/2 或未加密链路。
- 使用 MILENAGE 验证算法。网络运营商应避免使用 COMP128-1 和 COMP128-2。网络运营商应考虑支持 TUAK 验证算法
- 采用适当措施应对和缓解虚假基站攻击。

在 GSM/GPRS 系统中，终端设备不会验证网络，只有网络会验证终端设备。因此，在使用 GSM/GPRS 系统时，建议采用服务层端对端加密。在作为物联网服务提供的解决方案中，必须考虑到实际处理、终端设备限制和网络带宽限制。

在 GSM/GPRS 系统中，GRX 网络上创建的 SGSN 和 GGSN 之间的 GTP 隧道并未加密。网络运营商应将 GRX 网络作为专用网络进行管理，以确保该链路的安全。

5.2.2 UMTS（3G）系统安全

UMTS 网络允许相互验证，不仅网络会验证终端设备，设备也会验证网络。

提供 UMTS 网络的网络运营商应当支持 MILENAGE 验证和密钥生成算法。网络运营商应支持 Kasumi 保密性和完整性加密算法。

网络运营商应考虑支持 TUAK 验证算法

5.2.3 LTE（4G）系统安全

提供 LTE 网络的网络运营商应当支持 MILENAGE 验证算法。网络运营商应支持 LTE EEA1、EEA2 或 EEA3 加密算法。

网络运营商应考虑支持 TUAK 验证算法。

建议网络运营商参考 GSMA 白皮书“LTE 网络中的无线安全”[30]。

5.2.4 低功率广域网安全

不同网络运营商部署了几种低功率广域（LPWA）网络技术。如需获取完整的最新 LPWA 网络部署列表，请访问 GSMA 网站：www.gsma.com/iot

可参阅 GSMA 网站上的 NB-IoT [34] 和 LTE-M [35] 部署指南，从网络和设备角度确保这些技术得到一致部署。

2017 年 5 月，信息安全分析师 Franklin Heath 发布了题为《LPWA Technology Security Comparison》[33] 的独立报告，针对智能农业、智能路灯、烟雾探测器、水表和智能仪表等几种典型的物联网用例，就五种不同低功率宽带（LPWA）网络技术的安全功能予以对照和比较。报告评估了在许可频谱 LTE-M、NB-IoT 和 EC-GSM-IoT 以及非许可频谱技术 LoRaWAN 和 Sigfox 中采用的三种 3GPP 标准化移动物联网技术的安全功能。可通过此链接下载该报告：https://goo.gl/JI0lr6 [33]。

报告认为，在考虑 LPWA 解决方案时，除了成本、电池寿命和网络覆盖率之外，组织还须确定其所需的安全级别。报告指出，物联网安全需求在很大程度上受到隐私和安全问题的驱动，任何采用 LPWA 技术的部署都应借助 GSMA 物联网安全评估 [32] 等工具进行安全风险评估。

报告中强调的一些重要的网络安全因素也应视为此类评估的组成部分，包括：

- 带宽（包含最大下行和上行数据速率） - 可能会限制由 LPWA 网络支持或在应用层实现的安全功能。
- 每日下行和上行吞吐量 - LPWA 设备通常不会传输或接收可能影响安全功能的数据，比如远程安全更新。
- 验证（设备、用户和网络） - 安全的网络连接需要有关各方彼此进行身份验证，例如设备、用户和网络供应商，所用相应技术必须能够防范恶意代理商对各方的“欺骗”。
- 数据机密性 - 通常采用加密来保护数据安全，使其免受攻击者拦截。还可通过在应用层建立端到端安全性来增加信任度。

- 密钥配置 – 用于验证、机密性和完整性的密码技术均依赖各方之间安全共享的密钥。
- 认证设备 – 在众多市场中，根据相关法律规定，具备无线传输功能的设备须取得批准或认证方可销售。可借此机会验证安全功能。
- IP 网络 – IP 的使用可能成为从互联网对设备发动攻击的切入点，因此必须考虑 IP 安全功能。

报告总结认为，LPWA 技术的几项潜在的重要安全功能在一定程度上属于可选功能，可由网络运营商直接启用，也可能与网络运营商做出的其他选择相关。网络运营商必须确保了解其在网络配置中所做出选择的安全后果，并确保将这些选择的状态明确地传达给客户。如何选择还受设备制造商控制（例如是否包括不可拆卸的 eUICC 等固定安全元素），他们同样也有义务将这类安全隐患告知相应客户。

采用 LPWA 技术时在安全性方面的具体注意事项包括：

对于所有 LPWA 网络技术：

- IP 网络层是否通过链路层实现。
- 是否存在安全元素，如果是，是否为可拆卸。
- 数据完整性在多大程度上得到保证。
- 该技术支持的算法或密钥长度是否列入黑名单或不宜使用（例如用于 GPRS 的 64 位密钥）。

对于 3GPP LPWA 网络技术（即 NB-IoT 和 LTE-M）：

- 是否支持远程 SIM 配置 (RSP)。
- 哪些完整性算法 (EIAx/GIAx) 和机密性算法 (EEAx/GEAx) 已实现并获准。

对于 LoRaWAN：

- 是否实现 ABP（个性化激活）或 OTAA（空中下载激活），以及 OTAA 是否可在设备之间共享 AppKey。

对于 SigFox：

- 使用 SigFox 网络时，必须考虑有效负载加密属于可用的可选功能。因此须使用 Sigfox 认证的密码芯片来启用 AES 128 加密，并对无线传输数据保密。

对于所有 LPWA 设备：

- 已采取何种安全认证形式（如果有）。

5.3 固定网络安全

对于网络运营商或物联网服务供应商控制的 Wi-Fi 网络，其默认配置的建议包括 EAP-SIM [28] 或 EAP-AKA [27] 验证，并可能依赖于 ETSI TS 102 310 的 UICC EAP 框架 [8]。

5.4 流量优先级

网络运营商可根据所提供的物联网服务提供相应的服务质量级别。

5.5 回程安全

指定 GSM、UMTS 和 LTE 的 3GPP 标准没有强制使用加密回程链路。此外，不同网络运营商之间的 RAN 和回程共享可能会引入其他安全漏洞。

网络运营商应为最终用户数据和信令平面数据流量实施 GSM、UMTS 和 LTE 网络的回程加密。

5.6 漫游

网络运营商可使用漫游服务，为物联网服务供应商提供国际移动布局。

连接归属网络和漫游网络的 SS7/Diameter 互通功能相对较为开放，因此漫游网络可能容易出现安全漏洞。这与物联网服务特别相关，因为驻留在漫游网络上的物联网终端设备比例可能较高。漫游终端设备比例较高有以下几个原因。首先，许多终端设备在同一个地点制造，但分布在全球各地。因此在许多情况下，对于嵌入式 UICC 而言，更换 UICC 并不现实或者不可能。其次，在许多情况下，由于可能存在多个漫游网络的多重覆盖，漫游状态的优先级高于本地连接。在本地法律允许的前提下，全球 UICC 联盟的成立和专用物联网漫游协议的制定促进了永久漫游状态的采用。

网络运营商应考虑如何保护其 HLR 和 VLR，防御拒绝服务攻击（包括非故意 DoS 攻击）、未授权来源的请求以及对“漫游定向”服务的利用。

漫游由主核心移动网络实体之间交换的网络间运营商信令协议促成：

1. 漫游（被访问）网络的 VLR 或 SGSN 与归属网络的 HLR 之间 - MAP（移动应用部分）协议（对于 CDMA 网络，IS41 与 MAP 类似）。
2. LTE 漫游网络的 MME 与归属 LTE 网络的 HSS 之间 - Diameter（存在某些变体，如 S6a）协议。
3. 被访问网络的 SGSN/S-GW 与归属网络的 GGSN/P-GW 之间 - 漫游数据传输使用 GTP（GPRS 隧道协议）。

本节将集中讨论与物联网服务相关的漫游安全问题。常规漫游安全问题由 GSMA FASG（反欺诈安全小组）及其下辖小组负责。因此，本文档不涉及漫游中来自两个位于不同国家的不同 VLR 的双重登记（典型的漫游欺诈情况）等问题。

5.6.1 漫游信令风暴/攻击

由于终端设备的性质不同，且服务的重要程度可能较高，因此物联网对移动网络有一些额外的安全要求。为大量终端设备提供服务时，移动网络会处于信令风暴的风险之中。故意的恶意拒绝服务攻击只是信令风暴的一种成因。在许多国家，服务移动网络的某个区域发生电源故障、自然灾害或覆盖故障可能是常有之事，这些故障也会引发此类问题。位于该区域的所有漫游智能仪表和其他终端设备会同时尝试漫游至另一个漫游网络。这种情况会引发信令风暴，使归属 HLR/HSS 面临严重风险。为了应对这种情况，3GPP TS 23.122 [9] 定义了扩展接入限制 (EAB) 服务：除通用和特定于域的访问控制机制外，网络运营商还可限制对为 EAB 所配置终

端设备的网络访问。EAB 配置可以在 UICC 或终端设备中进行。网络安全网关应配置为“容纳”故意拒绝服务攻击。

归属网络运营商还可能需要（与物联网服务供应商一同）区分低优先级终端设备和关键终端设备。例如，医疗设备可能需要在发生信令风暴和服务拒绝攻击时继续维持服务。网络可能需要在发生信令风暴时拒绝“低优先级”漫游终端设备登记，但允许“高优先级”终端设备登记。拒绝机制可以与回退定时器一起实施，以在信令风暴结束后协助终端设备处理登记重新尝试。

一般建议网络运营商筛选接收来自归属网络/漫游合作伙伴的所有漫游消息。除了阻止来自未授权/假冒归属网络/漫游合作伙伴的消息之外，还需要根据终端设备优先级对消息进行过滤。发生信令风暴/拒绝服务攻击时，需要允许来自高优先级/关键终端设备的消息，或者拒绝来自非关键终端设备的消息。需要采取拒绝方法，以便将登记尝试和其他活动推迟一段时间。

5.6.2 基于安全的漫游引导 (SoR)

出于安全目的，网络运营商可以执行的另一种安全用例是物联网终端设备漫游引导 (SoR)。如果没有回退定时器，拒绝更新位置会导致终端设备进行重试，最后尝试从另一个漫游（被访问）网络注册。SoR 的另一种方法是通过 OTA，使用 UICC 漫游优先列表和 UICC 上存储的其他参数。UICC 的 OTA 更新功能让归属网络可以更新优先漫游列表，该列表确定了漫游网络选择过程中的网络优先顺序。归属网络还可以使用新列表刷新终端设备内存，让终端设备立即搜寻新网络。

如果在特定被访问网络中检测到安全风险，归属网络可以决定使用 SoR 机制将其出站漫游终端设备转移至另一个被访问网络。这种终端设备的主动转移可以在终端设备下一次尝试登记时进行，也可以临时使用 SIM OTA 服务进行。如果在特定被访问网络上漫游的较多终端设备报告了问题，或者其他输入接收到了信息，就可以检测出该网络的相关安全风险。

5.6.3 数据漫游拒绝服务

拒绝服务攻击并不仅限于移动信令空间，数据漫游领域也可能发生信令风暴。目前大多数漫游数据是从被访问网络 SGSN（LTE 为 S-GW）路由至归属网络 GGSN（LTE 为 P-GW），很少会实施将数据从被访问网络直接路由至互联网的 LBO（本地突破）用例。由于相关法规的影响，未来的情况可能有所改变，例如欧盟法规从 2014 年 7 月起启用 LBO 服务、LTE 特别是 VoLTE（LTE 语音），漫游网络中进行的语音呼叫可由国内 P-GW 处理（例如现在被访问网络中进行的常规电路交换语音呼叫）。

当归属 GGSN/P-GW 的新数据会话请求泛滥时，可能会发生信令风暴。GPRS 协议在终端设备和 GGSN 之间创建了一条安全隧道，发出新会话请求（创建 PDP 上下文）会建立一条隧道，并为终端设备分配一个 IP 地址。如果物联网终端设备没有按照个性化方式运行，可能会产生之前所述的新数据会话请求爆发。少量终端设备可能产生拒绝服务攻击，并行创建多个新数据会话请求。GGSN/P-GW 服务器的容量有限，应避免其受到这种风暴的攻击。

为了防止信令风暴，网络运营商可以基于安全策略，通过更改受影响设备的通信配置文件或在网络数据包核心中执行安全策略，防止某些设备连接到其网络。

在发生拒绝服务攻击的情况下，需要让关键终端设备接收到服务，而将低优先级终端设备的请求推迟一定时间。

5.7 终端和网关设备管理

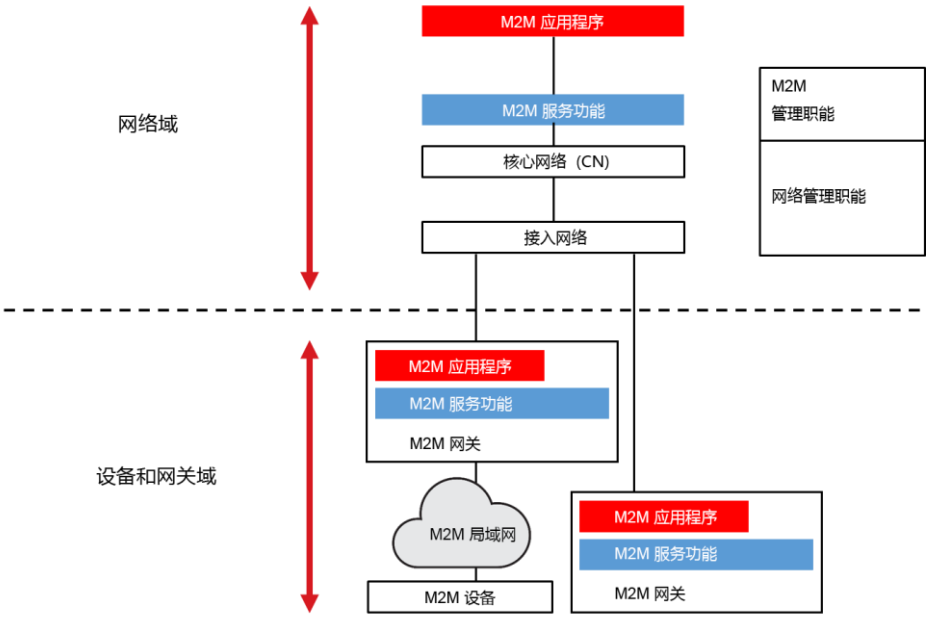
需要注意的是，本文档不涉及硬件和软件安全措施，包括终端设备和网关设备的本地配置管理控制台。本节介绍的是与网络有关的方面。关于终端设备相关的安全指南，请参考 GSMA 文档“CLP.11 物联网安全指南概述”[11]。

5.7.1 终端设备管理

网络运营商可以为物联网服务供应商提供基础功能，采用一些为“传统”移动设备管理开发的原则和技术，安全地配置和管理终端设备与订阅。可以利用现有的连接管理平台、设备管理平台和 UICC 管理平台，对使用 UICC 登记和连接蜂窝网络的物联网终端设备进行管理。

除了这种基本的终端设备管理功能，物联网服务平台还可以提供更为复杂和具体的终端设备管理功能。

下图所示是一个典型终端设备管理架构的示例，来自 ETSI M2M 通信原理 [19]。



a) - 用于 M2M 设备管理的 ETSI 高级架构

蓝框表示通常由网络运营商现有的设备管理平台管理，红框表示由物联网服务平台管理的服务组件。

网络运营商可以应物联网服务供应商要求，承担一些红框内的设备管理功能。

5.7.2 网关设备管理

使用网关设备可能会令物联网服务供应商的设备管理复杂程度增加一个级别。一些情况下，物联网网关设备可以是连接蜂窝网络的基于 UICC 的设备，有些情况下则使用固定线路。

网关应当是一个受控对象，以便根据需要对其进行监控或使用新的固件或软件进行更新。采用的协议应当能够提供安全的固件和软件更新以及安全的软件和系统集成机制，从而保障网关与骨干网络的互连。

网络运营商可以代表物联网服务供应商提供和管理安全网关，让终端设备通过与网络运营商广域网安全机制整合程度最高的方式安全连接。

可以使用宽带论坛 TR-069 客户端设备 (CPE) 广域网 (WAN) 管理协议 [20]，对使用固定网络连接的网关进行远程管理。

可以使用 OMA 设备管理 (DM) 和固件更新管理对象 (FUMO) 协议 [5] [6]，对使用蜂窝网络连接的网关进行远程管理。

5.7.3 物联网终端设备黑名单

网络运营商应当实施物联网终端设备黑名单，并连接至 GSMA 中央设备身份寄存器 (CEIR) 数据库。CEIR 是由 GSMA 管理的一个中央数据库，包含与丢失和被盗终端设备以及应禁止接入网络的设备相关的 IMEI。IMEI 进入 CEIR 之后，所有取得该数据并通过设备身份寄存器实施本地黑名单的网络运营商都会将含有该 IMEI 的设备列入黑名单。

网络运营商还可以实施本地化设备“灰名单”，允许临时挂起“可疑”设备，在列入黑名单之前对此类设备的性质进行调查。需要注意的是，对于医疗等关键服务，封锁 IMEI 可能并不适当或者不可能。网络运营商必须清楚了解已连接终端设备的详细信息，以便识别终端设备的真实应用（或主机）。如果终端设备使用发放给通信模块供应商的 IMEI，则应支持设备主机识别报告功能，这样终端设备就能向网络运营商报告主机信息。GSMA 连接效率指南 [17] 中介绍了设备主机识别报告。

5.8 其他安全相关服务

5.8.1 云服务/数据管理

网络运营商可以为客户提供托管的云物联网服务平台，用于实施物联网服务，还可以提供服务来存储和管理此类服务产生的数据。

网络运营商可以根据物联网服务供应商要求，提供私有云或共享云基础设施。

5.8.2 基于分析的安全

网络运营商可以提供数据分析与深度包检测服务，以识别物联网服务所产生的数据是否存在威胁和异常。例如，网络运营商可以定期对社会安全号码和 GPS 坐标等可能未受到正确保护的特定字符串进行深度包检测，并提醒对其负责的物联网服务供应商信息可能泄漏。

这对于物联网而言是一个优势，因为轻型终端设备和服务本身并不能提供这项功能。网络运营商可以为物联网服务供应商提供安全状态、识别的威胁和攻击等信息，以及整体安全情况检查。这些内部检测服务至关重要，可确保威胁不会进入内部，特别是在数据服务加密的情况下。提供的服务包括：

- 使用异常检测和机器学习发现问题。

- 在实时终端设备诊断中建立入侵防护系统。
- 提供仪表板，以便显示和识别异常情况。
- 提供自动标记和阻止可疑连接的方法。
- 提供云服务的威胁分析。

5.8.3 安全网络管理

网络运营商可以提供能够安全管理和维护的网络。

- 在物理或逻辑链路发生故障时提供备用信道
- 识别链路故障，作为潜在安全漏洞的证据
- 实施影响安全性和完整性的漫游策略
- UICC/SIM 管理
- 安全信息管理
- CERT 成员并参与威胁信息共享，以缓解和预防未来的攻击。
- 防御拒绝服务攻击
- 进行定期安全扫描/漏洞评估
- 管理和处理网络安全相关监管要求
- 将通信选项严格限制为特定物联网服务所需的最低限度。

5.8.4 安全物联网连接管理平台

网络运营商正越来越多地利用专用核心网络和 OSS 基础架构，以高效灵活地管理物联网订阅和价格计划。运营商的业务客户（即物联网服务供应商）经常可以访问此类基础架构，以便管理自己的订阅（包括单独或批量激活服务、暂停等）。

CLP 12“物联网服务生态系统的物联网安全指南”[26] 中的服务平台指南提供了有价值的指导，对于支持物联网连接管理平台的网络运营商会有助益。这些指南包含以下建议：

- 网络运营商应确保按照 NIST [24]和 ECRYPT2 [25] 等组织最新发布的行业指南，对其物联网连接管理平台门户网站（可能由网络运营商或云托管）的访问采用“业界最佳”的加密技术。
- 网络运营商应确保对其物联网连接管理平台门户网站的访问使用标准的“最佳实践”程序进行密码创建、更新和重置。

5.8.5 证书管理

网络运营商可以提供 X.509 证书管理服务。

5.8.6 多因素身份验证

多因素身份验证服务通常需要用户在用户名和密码之外，还要使用电子凭证来验证自己的身份。因此，多因素身份验证可以针对未授权用户对物联网服务的访问提供额外的防护。

GSMA 移动连接计划 [12] 与 OpenID Connect [21]、FIDO [22] 和 ETSI MSS [23] 都是推动多因素身份验证的规范，让物联网服务供应商可以从终端用户得到额外的验证和信息。在这种

情况下，最终用户是可以向物联网服务平台提供信息以提供不同级别保证的人，例如输入 PIN 和提供生物特征签名。

虽然目前大部分多因素身份验证解决方案都用于实现传统的“智能手机”服务，但此类技术也可用于需要保证某些任务（如执行网络连接操作、软件更新或硬复位）人员授权的物联网服务。

例如，如果使用多因素身份验证，在车联网中除网关设备外，还可以使用移动身份。在此用例中，多因素身份验证基础设施可以作为乘客访问车内信息娱乐和支付服务时的附加授权层。

附录 A 文档管理

A.1 文档历史

版本	日期	更改简介	授权批准	编辑/公司
1.0	2016 年 2 月 8 日	新版 PRD CLP.14	PSMC	Ian Smith GSMA
1.1	2016 年 11 月 17 日	新增 GSMA 物联网安全评估计划参考资料。 小幅编辑更正。	PSMC	Ian Smith GSMA
2.0	2017 年 9 月 30 日	进行大幅修订，新增 LPWA 参考资料	物联网安全团队	Rob Childs GSMA

A.2 其他信息

类型	描述
文件所有者	GSMA 物联网项目
联系人	Rob Childs - GSMA

为您提供卓越的产品是我们不懈的追求。如果您发现任何错误或遗漏，请告诉我们。您可发送邮件至 prd@gsma.com

欢迎您随时向我们提出建议和问题。