国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1369

（01/2022）

X系列：数据网、开放系统通信和安全性

安全应用和服务（2）– 物联网（IoT）安全

物联网服务平台的安全要求

ITU-T X.1369建议书

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
万维网安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	**X.1350–X.1369**
智能交通系统（ITS）安全	X.1370–X.1399
分布式账簿技术（DLT）安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1369建议书

物联网服务平台的安全要求

概要

ITU-T X.1369建议书规定了物联网服务平台的安全要求。它评估了物联网业务服务平台面临的安全威胁和挑战，并描述了可以缓解安全威胁和挑战的安全措施。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1369	2022-01-07	17	11.1002/1000/14799

关键词

物联网（IoT），服务平台，安全要求，安全风险。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1369建议书

物联网服务平台的安全要求

1 范围

本建议书规定了物联网服务平台的安全要求。它评估了物联网业务服务平台面临的安全威胁和挑战，并描述了可以缓解安全威胁和挑战的安全措施。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其他参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其他参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其他参考文献的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

[ISO/IEC 30141] ISO/IEC 30141（2018年），*物联网参考架构*。

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 物联网（Internet of things（IoT））[b-ITU-T Y.4000]：指的是一种信息社会全球基础设施，它基于现有的和正在出现的、可互操作的信息通信技术，通过将（物理的和虚拟的）物体相互连接，以提供高级服务。

3.2 本建议书中定义的术语

本建议书定义了下列术语：

3.2.1 物联网服务平台（IoT Service Platform）：连接物联网设备并执行物联网应用程序的系统平台。

从功能上看，物联网服务平台提供设备管理、连接管理、应用使能和业务分析等能力。从数据管理上看，物联网服务平台为物联网应用和高级分析收集、存储和处理数据（包括用户的个人数据和机密信息）。

4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语：

API 应用程序编程接口

CSRF 跨站请求伪造

DDoS 分布式拒绝服务

DoS 拒绝服务

IMEI 国际移动设备身份

PVLAN 专用VLAN
SIM 用户身份模块
SQL 结构化查询语言
SSRF 服务器端请求伪造
VLAN 虚拟局域网
VM 虚拟机
VMM 虚拟机监视器
XSS 跨站脚本

5 惯例

在本建议书中，关键词“应/应该”（should）指明一项务必严格遵守的要求，若要宣称与本建议书一致，则不允许与该要求有任何偏离。

6 概述

[ISO/IEC 30141]定义了基于实体的物联网参考模型，如图1所示。物联网服务平台是该图中所示的应用和服务子系统的关键组件，它提供诸如设备管理、连接管理、应用启用和服务分析等能力。物联网服务平台还实现了物联网应用的数据收集、存储和分析。

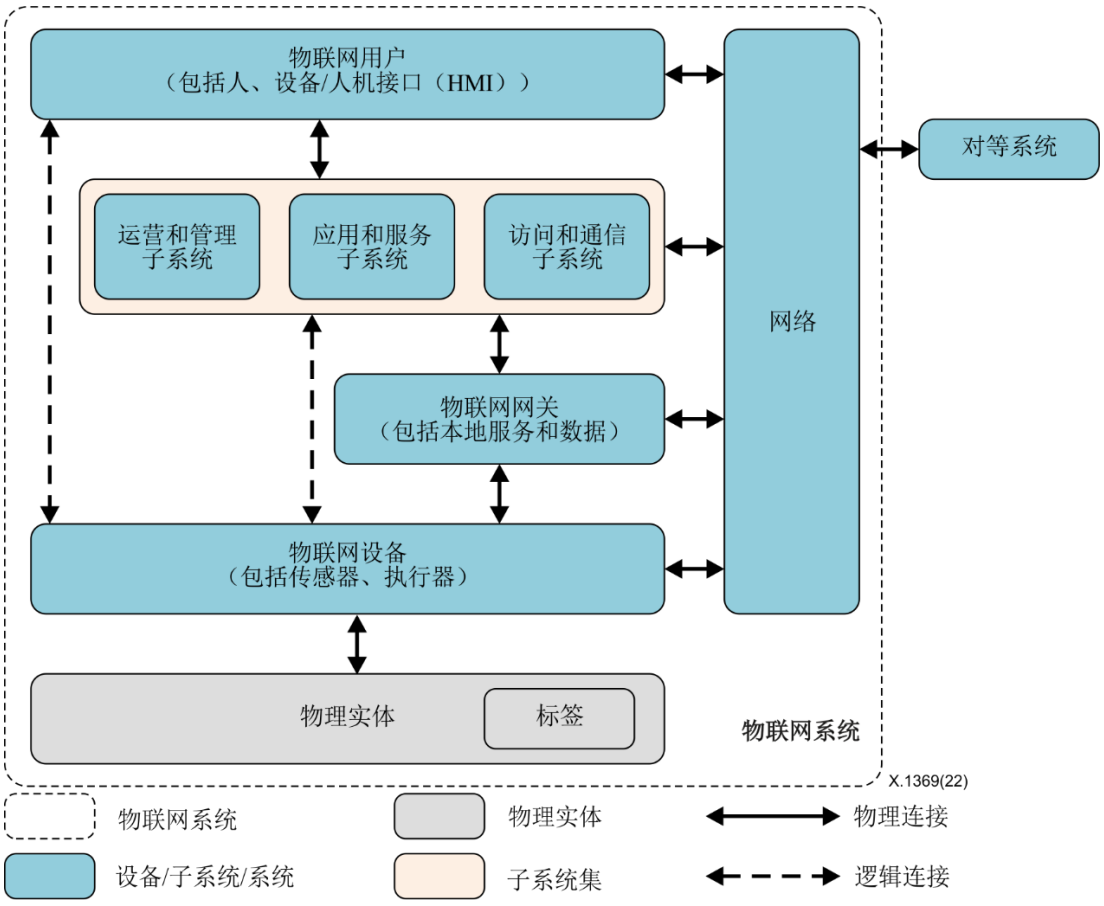

图1 – 基于实体的物联网参考模型[ISO/IEC 30141]

一般而言，物联网服务平台可分为四个部分，它们是设备管理系统、连接管理系统、应用使能系统和业务分析系统。

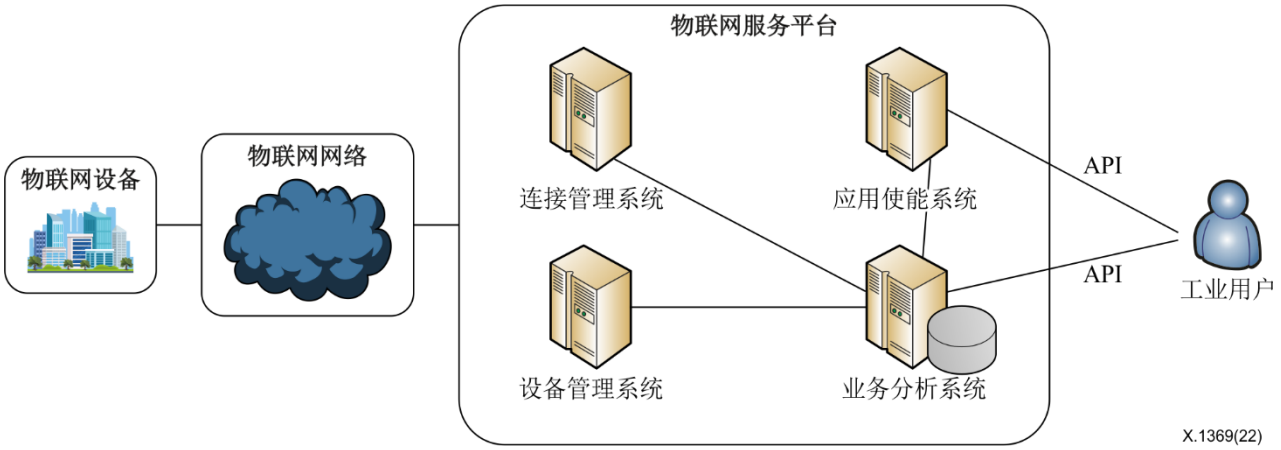

图2 – 物联网服务平台概览

- 设备管理系统

这是物联网设备的管理系统，提供远程监测、重新配置、软件升级、系统升级、故障排除、生命周期管理等功能。

- 连接管理系统

这是用户身份模块（SIM）卡的集中管理系统。它专注于蜂窝网络应用，支持用户自助服务，例如，查询数据使用和连接状态、SIM卡充值和流量管理。

- 应用使能系统

这是一个“平台即服务”平台，提供不同功能的应用程序编程接口（API）来支持实施不同的服务系统。通过该系统，电信运营商将其主要的电信能力（数据、SMS、电话、认证、计费等）开放给不同的服务系统，例如，智能交通、智慧城市、智能家居等。

- 业务分析系统

这从设备管理系统、连接管理系统和应用使能系统中收集各种各样的数据，为运营商和消费者分析并生成可视化的分析结果。

物联网服务平台的安全在整个物联网环境中扮演着重要的角色。平台的任何弱点或攻击都会影响相关设备、网络和数据的安全。物联网服务平台易受拒绝服务（DoS）、权限提升、未授权访问、暴力破解、任意代码执行等威胁，这些可能导致恶意入侵、敏感信息泄露、给设备下达恶意指令等严重后果。

本建议书分析了物联网服务平台的安全风险，提出了安全框架方法和安全措施。

物联网服务平台的安全从底层到上层涵盖基础设施安全、系统安全、数据安全、应用安全。此外，API安全和运营安全涉及四个层面。第7节至第9节分别基于这六个方面详细说明了安全风险、安全框架和安全要求。

7 物联网服务平台面临的安全威胁

7.1 应用安全威胁

应用安全威胁包括网络攻击、未授权访问、权限提升和服务漏洞。

7.1.1 网络攻击

物联网服务平台使用传统的网络技术以及通信技术、大数据、云计算等。因此，它继承了所有这些技术的主要安全风险，例如，分布式拒绝服务（DDoS）攻击、暴力破解攻击、结构化查询语言（SQL）注入、跨站点脚本（XSS）漏洞、跨站点请求伪造（CSRF）漏洞、服务器端请求伪造（SSRF）漏洞等。

7.1.2 未授权访问和权限提升

大量的物联网应用部署在中心化平台上。这使得不同的应用之间难以实现有效的安全隔离和访问控制，从而可能导致未经授权的访问、操作和权限提升。此外，容易在不同的用户和设备之间造成未经授权的访问和权限提升。

7.1.3 服务漏洞

物联网应用的服务逻辑复杂，应用协议众多，可能会在设计和实现过程中带入缺陷，导致服务漏洞和滥用。在物联网的一些应用场景中，可以通过平台来控制终端。遭破坏的平台将造成大量终端的破坏，进而影响用户的工业制造和社会生活。

7.1.4 能力暴露

作为一种应用赋能平台，物联网平台可以提供不同的功能API，来支持实现不同的业务系统。它为不同的服务带来便利，但能力的开放也可能给平台带来风险。该能力可能会被未经授权的开发者访问或被不同的服务滥用。更重要的是，开放主电信能力（数据、短信、电话、认证、计费等），如果保护不当，可能会给电信核心网带来攻击。

7.2 数据安全风险

数据的保密性、完整性和可用性形成数据安全的基线。然而，在数据的收集、传输、迁移、存储、处理和销毁过程中，存在诸多风险。

7.2.1 数据泄露

物联网应用的数据通常通过物联网终端来收集并传输到平台，而这些应用的数据通常都存储在平台上。因此，如果数据没有通过SQL注入攻击、缓冲区溢出攻击、权限提升等方式得到适当保护，那么攻击者就可获取数据。

7.2.2 数据篡改

数据在传输过程中可能会被篡改、重放或修改。在应用数据传输和存储过程中，如果数据没有得到适当保护，那么攻击者就能够篡改数据。例如，如果在传输过程中不考虑数据完整性，那么攻击者可以重放使用过的信息或伪造虚假信息并将信息发送给物联网平台。

7.3 系统安全风险

7.3.1 账号被盗

如果物联网服务平台操作系统的管理员账号不够复杂，或者如果系统一个不必要的端口被打开，那么账号可能会通过暴力破解、监测等被盗用。访问控制不当会威胁到系统安全。

7.3.2 权限滥用

平台提供的物联网服务运行在操作系统和中间件上。如果不及时对操作系统或中间件进行更新，那么存在老版本系统或中间件有漏洞的风险，这些漏洞有可能被黑客利用，并导致权限提升。

7.4 基础设施安全风险

基础设施易遭受物理安全、网络安全、虚拟化安全和设备安全等方面的威胁。

7.4.1 物理威胁

物联网平台的物理环境也会影响安全性。例如，它易遭受如地震、洪水、风暴、龙卷风等方面的自然威胁。此外，电力和冷却系统等设施，甚至安全系统本身，都可能对物联网平台构成威胁。更重要的是，还应考虑到人为因素，这可包括故意破坏、盗窃、爆炸等。

7.4.2 网络威胁

攻击者可能会扫描互联网，以寻找物联网服务平台的接入点。此外，服务平台缺乏网络隔离可能会导致跨不同服务的数据访问。

7.4.3 虚拟化的风险

服务器虚拟化技术大大提高了物联网平台的建设效率、运营灵活性和经济效益，但同时也带来了新的风险。例如，虚拟机监测（VMM）的设计缺陷使攻击者可入侵omtp虚拟主机，与同一主机的虚拟机共享一张网卡，造成安全问题很容易传播。还有其他类型的风险，例如，虚拟机（VM）跳转、拒绝服务（DoS）攻击和远程管理平台漏洞。

7.5 接口安全风险

物联网服务平台的接口包括网络接口、第三方API和厂商后端API，它面临信息泄露、跨站脚本、弱认证、弱访问控制等风险。

7.6 运营安全风险

在运维过程中，服务可能会因运维人员的错误操作行为而被中断。例如，工作人员可能会使用被恶意软件感染的U盘或者可能意外删除数据。还应考虑到异常连接、默认密码、恶意攻击和审计机制。

8 物联网服务平台的安全架构

物联网服务平台的安全架构重点关注六个方面的安全保护要求：应用安全、接口安全、数据安全、系统安全、基础设施安全和运营安全。

整体安全架构如图3所示：

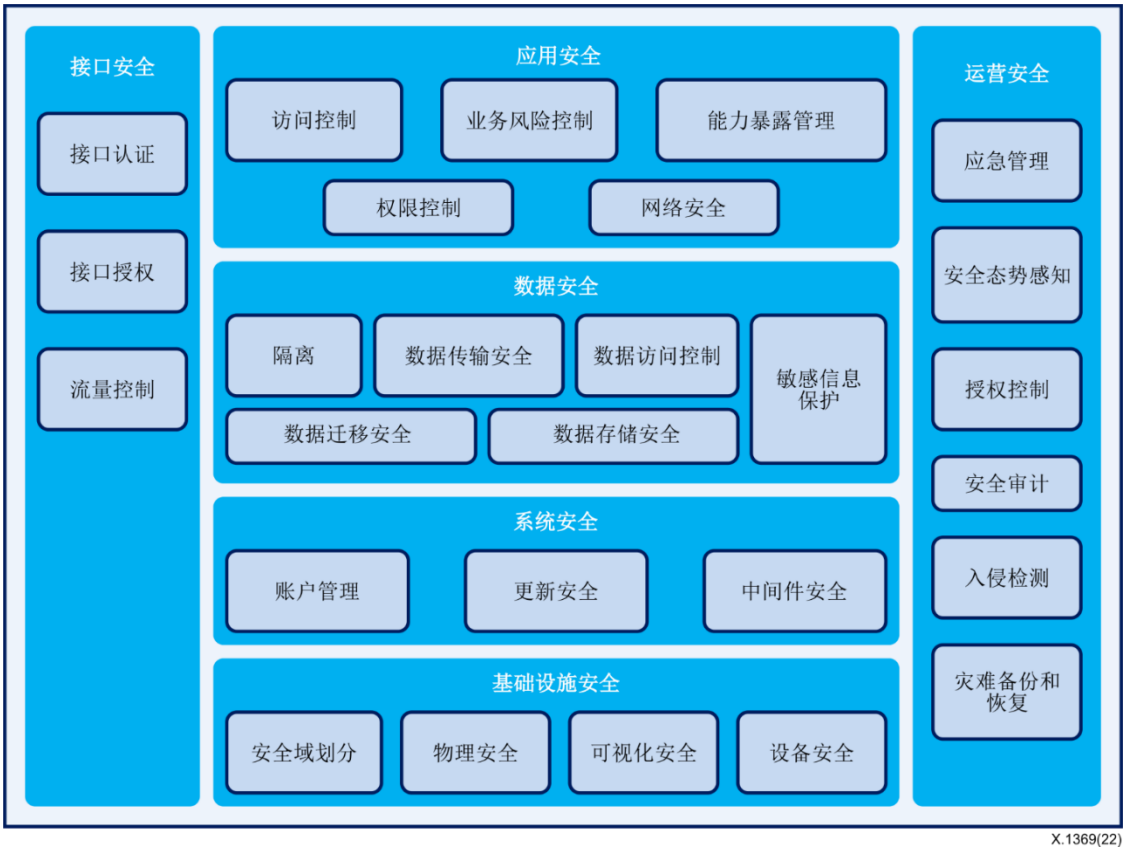

图3 – 物联网服务平台的安全架构

8.1 应用安全

应用安全包括访问控制、权限控制、业务风险控制、网络安全和能力暴露管理，这将有助于解决权限提升、未授权访问等问题。

8.2 数据安全

数据安全包括隔离、数据传输安全、访问控制和数据存储安全，这将有助于解决隐私泄露问题等数据安全问题。

8.3 系统安全

系统安全包括账户管理、软件更新安全和中间件安全，这将有助于解决已知漏洞被恶意利用问题。

8.4 基础设施安全

基础设施安全包括安全域划分、物理安全、可视化安全和设备安全，这将有助于解决已知漏洞被恶意利用问题。

8.5 接口安全

接口安全包括接口认证、接口授权和流量控制，这将有助于解决个人可识别信息泄露、SQL注入等问题。

8.6 运营安全

运营安全包括应急管理、安全态势感知、授权控制、安全审计、入侵检测、灾难备份与恢复等，这将有助于解决运营安全相关问题。

9 物联网服务平台的安全要求

9.1 应用安全

服务平台应该能够在边界上防范来自互联网的攻击，尤其是对大数据、云计算、网络应用等技术的攻击。应提供防DDoS、防篡改、防入侵、防病毒的能力，以确保服务平台的安全稳定运行。

9.1.1 访问控制

9.1.1.1 用户访问控制

1) 应构建用户识别系统，为每个用户指配一个唯一的身份标签，并且无论用户是否更改手机号码、邮箱等信息，标签都应保持不变。

2) 应定期检测弱密码。此外，密码在传输过程中应予加密。对于高安全性业务，应考虑强制定期更换密码机制。

3) 应严格处置动态短信的使用。应采取后台验证、用后即失效、限制错误登录次数、避免本地认证等安全措施。

4) 在登录场景中应使用图形认证码机制。应考虑背景噪声、非二值化、反分割、穿线、字体旋转失真等背景扰乱措施，以防机器快速识别。

5) 平台应具备风险控制和防冲突能力。它应具有确定合法访问的能力。例如，应通过对失败登录、IP地址、设备ID、锁定时间、解锁模式、同时在线等进行数字限制手段，来防止暴力破解。

6) 在密码重置和恢复过程中，应严格验证身份，以防认证旁路和身份伪造。

9.1.1.2 应用访问控制

1) 构建应用识别系统，并为每个应用指配唯一的ID。

2) 对访问平台的应用的有效性进行认证。应只有经认证的应用方可访问服务平台以做后续的服务调用。

3) 在应用认证过程中，禁止明文传输密码或对加密采用弱算法（如MD5）转换。

4) 应为不同的应用指配不同的密钥，并应支持用于密钥生成、分发、存储和更新的密钥管理功能。

5) 对接口调用应进行认证，以限制可操作的资源范围和操作权限。

9.1.1.3 设备访问控制

1) 应构建设备识别系统。为每个物联网设备分配一个唯一的ID，并将ID绑定于对应的设备信息，例如，设备制造商、设备类型、模具等。

2) 通过密钥预分配方案或密钥交换方案等手段为每个设备指配一个唯一的设备密钥。设备密钥和设备ID应绑定在一起。并应支持用于密钥生成、分发、存储和更新的密钥管理功能。

3) 在设备访问平台时进行身份认证。应只有经认证的设备方可访问服务平台以做后续的服务操作。

4) 在应用认证过程中，禁止明文传输密码或对密钥采用弱算法（如MD5）转换。

9.1.2 权限控制

1) 应支持用户分类和分组管理。应根据不同的用户分类和分组授予不同的权限。应只有经授权的用户方可访问指定的数据并执行相应的操作。

2) 应根据不同的应用分类授予不同的权限。应只有经授权的应用方可调用指定的服务能力并执行相应的操作。

3) 应根据不同的设备类型或分类授予不同的权限。应只有经授权的设备方可访问指定的数据和信息并执行相应的操作。

9.1.3 业务风险控制

9.1.3.1 物联网卡安全管理和控制

物联网卡的通信功能应根据“最小、必要、可控”的原则，针对不同的类型业务进行严格限制。例如，语音、短信功能在某些场景下应是单向的，在数据流异常时，对数据功能应做限制。

9.1.3.2 服务安全管理和控制

应具备限制数据流、短信、语音等总量和频率的能力，并能在数量超过阈值时关闭服务。

9.1.3.3 用户行为控制

应限制用户访问平台的总流量、频率和时间。当用户出现异常行为时，应立即停止访问。

9.1.3.4 设备异常监测

应对设备行为进行监测。当检测到异常设备行为（例如，非常规时间、非常规访问、异常位置区域）时，应提供告警和处理机制。

9.1.3.5 服务风险监测

对物联网终端的数据应通过总量、峰值流量等手段进行多维度分析，以便及时发现业务运行异常。在服务运营过程中，还应对服务滥用进行监测。例如，可以通过监测设备的国际移动设备身份（IMEI）号来检测设备和卡的分离。同时，利用从终端运营中收集的大数据，从全局角度提升对安全风险的检测、分析和消除能力。

9.1.4 网络安全

1) 应提供强大的抗DDOS攻击能力，应针对应用层和网络层定制抗DDOS策略（例如，流量牵引、网络流量清洗等）。

2) 平台应具备网络漏洞扫描能力，可检测和防范诸如文件上传、SQL注入、XSS漏洞、CSRF漏洞、SSRF漏洞等安全问题。

3) 平台应具备扫描主机漏洞并发现信息系统中漏洞的能力，包括安全漏洞、安全配置问题、应用系统安全漏洞、弱密码等。

4) 平台应具备限制网络应用中数据库连接和网络访问时间的能力，以避免出现不必要的资源消耗。

5) 平台应具备入侵检测能力，记录入侵的源IP、攻击类型、攻击目的和攻击时间，并在发生严重入侵时提供告警。

9.1.5 能力暴露管理

9.1.5.1 身份认证

应用使能系统应支持身份认证。开发者在请求和应用某些API功能时，应对开发者和应用程序的合法性进行认证，不得伪造合法开发者和应用程序的身份。

9.1.5.2 应用加固和保护

应用赋能系统应具备对调用API函数之应用程序进行加固和保护的功能，以防止应用程序被篡改和反编译。

9.1.5.3 数据安全保护

应用赋能系统应确保与账户、用户证书和应用程序相关之敏感信息的机密性和完整性，以防信息在存储、传输和使用过程中被盗取或篡改。例如，对在物联网应用与平台之间传输的敏感信息应予加密，并应考虑完整性保护，确保敏感信息不会暴露给未经授权的实体和进程，也不会被它们修改、破坏或重放等。

9.1.5.4 能力调用认证

应用使能系统应支持能力调用认证和授权。当应用程序调用能力时，应对开发者和应用程序可调用之能力的频率、总量和类型进行认证。只有在授权后方可调用该能力。

9.1.5.5 能力调用监测

应用使能系统应支持对有关能力调用的频率、时间和总量实施监测。当超过限制或行为异常时，应立即停止该功能并同时给出告警。

9.2 数据安全

平台应对数据进行存储、传输、使用等全生命周期保护。对关键的服务数据应定期进行备份，并应配置恢复机制，以确保数据的机密性、完整性和可用性。

9.2.1 数据隔离

对不同的数据应在隔离的环境中进行执行和保存。平台应能够在逻辑上隔离敏感信息，并严格控制不同领域之间的交互。

9.2.2 数据传输安全

1) 对服务平台与物联网设备及其他服务平台之间传输的敏感信息（包括后台管理员密码、操作系统登录密码、网络设备登录密码以及与这些密码相关的密码保护答案）应予以保密。

2) 应保护服务平台、物联网设备与其他服务平台之间敏感信息的完整性。

9.2.3 访问控制

平台应支持访问控制功能，例如，对不同虚拟化系统的数据库设置不同的访问策略，以保证用户只能在对应服务系统的数据库授权范围内进行操作，而不能访问其他未经授权的服务系统的数据。

9.2.4 数据存储安全

1) 应根据其重要性对数据进行分类，应根据数据的分类级别采用不同的机制。例如，对不太重要的数据可以以明文形式进行存储，同时应保证重要数据的机密性。

2) 平台应提供安全的密钥存储机制。例如，将密钥存储在加密机或特定代理中，以确保密钥不被泄露。

3) 应保护数据的完整性，并应对极其敏感的数据提供完整性检测机制，以便及时发现这些数据的损坏和丢失情况。极其敏感的数据包括用户名、帐号等。

4) 平台应提供完整的数据备份和恢复机制。如果数据丢失或毁坏，那么应使用备份机制来恢复数据，以保证事故发生后不会丢失数据。

5) 平台应具备对各类数据和文件进行归档的能力，并具备自动和定期清理临时数据和文件的功能。

6) 系统中文件、目录、数据库的存储空间应予以释放或重新分配，应能完全清除和不可恢复。

9.3 系统安全

平台使用的系统应考虑账户管理、软件更新安全和中间件安全，这将有助于解决已知漏洞被恶意利用的问题。

9.3.1 账户管理

1) 平台系统应自动记录系统日志，例如，用户登录信息、运营信息等。

2) 对于通过HTTP协议远程维护的系统，系统应支持HTTPS等加密协议。

3) 对于具有字符接口的系统，应支持定时账号自动退出。

4) 系统应考虑主机资源访问控制，例如，建立角色模型并设置适当的安全策略来控制不同角色用户对主机资源的访问。

9.3.2 软件更新安全

1) 应及时更新操作系统的版本/安全补丁。

2) 应只允许安装必需的组件和应用程序。

3) 系统应只开放必要的端口，并关闭不必要的端口。

9.3.3 中间件安全

1) 对中间件的版本/安全补丁应及时更新。

2) 应禁用中间件不必要的接口，以防系统信息泄露。

3) 中间件标志（软件名称/版本号标志）应受到保护，以防系统信息泄露。

9.4 基础设施安全

基础设施安全应考虑安全域划分、物理安全、可视化安全和设备安全，这将有助于解决已知漏洞被恶意利用的问题。

9.4.1 网络安全域划分

1) 对安全域应在服务平台与互联网之间、服务平台与内部支持系统之间以及平台内托管的不同服务系统之间进行划分。对安全域边界应在其他域与访问域之间、访问域与核心域之间以及核心域内进行划分。

2) 服务平台中不同的服务系统应被划分为不同的虚拟局域网（VLAN），不同的安全域应使用不同的VLAN段。每个安全域中的不同服务系统应使用不同的VLAN，默认对所有VLAN进行隔离。在同一VLAN中，应支持同一服务系统不同安全级别的VM隔离，例如，通过专用VLAN（PVLAN）技术来划分子VLAN。

3) 应设置互访策略。例如，对业务系统内不同安全域的互访、不同业务系统之间的互访进行战略配置。

4) 应支持安全域隔离功能。例如，平台网络可被划分为管理域、服务域、接口域等，不同功能的设备应分布于不同的安全域中。入侵检测和访问控制应在安全域的边界予以实施。

9.4.2 物理安全

1) 物理环境应满足位置、电源、防火、防水、防静电和温湿度控制等安全防护要求。

9.4.3 虚拟安全

1) 平台应支持管理程序保护、VM隔离、云主机系统加固、VM安全监测、恶意软件防护、应用控制等功能，以避免常见的虚拟化安全问题。

9.4.4 设备安全

1) 物理设施应满足安全防护基线配置要求和测试要求。应引入可信计算以增强设施安全性。

9.5 接口安全

接口安全包括接口认证、接口授权和流量控制，这将有助于解决个人可识别信息泄露、SQL注入等问题。

9.5.1 接口认证

1) 平台应具备验证服务系统之间合法性的能力，以便防止对平台的未经授权使用和访问。

2) 服务平台应具备记录被调用资源完整操作日志的功能。

9.5.2 接口授权

1) 服务平台应具备根据源IP地址范围进行授权的功能。除了提供静态密码外，被调用的服务平台还需要对IP地址范围进行授权。

2) 对于需要用户访问权限的接口，应具备有关拒绝/允许清单的访问机制，以便拦截非法用户访问。

9.5.3 流量控制

1) 平台应具备通过设置流量控制策略来控制流量速率的能力，并可以根据后端API服务器的性能调节来修改策略中的配置值。当并发请求数量超过限制时，拒绝超过的请求并返回错误响应。

9.6 运营安全

运营安全包括应急管理、安全态势感知、授权控制、安全审计、入侵检测、灾难备份与恢复等，这将有助于解决运营安全相关问题。

9.6.1 应急管理

1) 平台应建立应急事件响应机制，例如，网络安全事件、工作场所安全事件等。

2) 安排定期应急演练，并建立应急预案定期演练制度。

9.6.2 安全态势感知

1) 建议构建安全态势感知系统，以实现对平台安全态势的监测、评估、预警、可视化、集中响应，以便有效提升网络安全威胁监测、态势感知、应急响应、溯源等能力，并提高安全运维效率。

9.6.3 授权控制

1) 平台应对平台的不同操作进行必要的认证和授权。对于高级权限，只有受信任的系统人员方可执行高级权限操作。

2) 平台应建立角色模型，并根据安全策略来控制用户对主机资源的访问。

9.6.4 安全审计

1) 管理员的所有操作都应做记录并形成日志。

2) 当存储空间几乎耗尽时，应保证审计日志不丢失。

3) 应对审计日志做备份。

4) 审计日志应防止未经授权的访问、修改和破坏。

5) 审计日志应被导出和删除。

6) 应以安全的方式来访问日志，以确保传输过程的机密性和完整性。

7) 平台应具备基于流量分析、日志审计、沙箱等对异常连接、异常访问、异常应用等异常行为实施实时监测和定期审计的功能，并应根据发现的异常行为及时提高告警和做出处置。

9.6.5 入侵检测

1) 平台应部署入侵检测设备，以及时检测任何入侵。

9.6.6 灾难备份和恢复

1) 在发生火灾、地震等灾害时，平台应能及时切换到异地冗余备份系统，以继续其服务。

2) 平台应支持敏感数据（例如，业务数据、计费数据、系统配置数据、管理员运维记录、用户信息等）的灾难恢复，以确保在关键数据被恶意删除时，系统能够及时恢复。

参考书目

[b-ITU-T X.1361] ITU-T X.1361建议书（2018年），基于网关模型的物联网安全框架。

[b-ITU-T X.1362] ITU-T X.1362建议书（2017年），物联网（IoT）环境的简单加密程序。

[b-ITU-T X.1601] ITU-T X.1601建议书（2015年），云计算安全框架。

[b-ITU-T Y.4000] ITU-T Y.4000/Y.2060建议书（2012年），物联网概述。

[b-ITU-T Y.4100] ITU-T Y.4100/Y.2066建议书（2014年），物联网通用要求。

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2022年，日内瓦