国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1606

(09/2020)

X系列：数据网、开放系统通信和安全性

云计算安全 – 云计算安全设计

通信即服务应用环境的安全要求

ITU-T X.1606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
网页安全	X.1140–X.1149
安全协议（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.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
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
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
5G 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.1606建议书

通信即服务应用环境的安全要求

摘要

ITU-T X.1606建议书可用于识别安全威胁，并针对通信即服务（CaaS）的应用环境提出了有关安全要求的建议。本建议书阐述了包含多种通信能力的CaaS场景和特征。接下来，建议书确定了由独特CaaS特性引发的特定威胁，并就CaaS安全要求提出了适当的建议。

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.1606	2020-09-03	17	11.1002/1000/14265

关键词

CaaS、云计算、风险、安全性要求。

* 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.1606建议书

通信即服务应用环境的安全要求

1 范围

本建议书侧重于通信即服务（CaaS）应用环境的安全要求，这与[ITU-T X.1602]软件即服务（SaaS）的安全要求不同。电信组织的CaaS融合了电信和互联网的通信能力。这种融合催生出一些受到特定风险影响的独特CaaS特性。本建议书确定了这些风险，并提出了适当的安全要求建议。

这些要求措施已将CaaS所在成员国的国家法律和监管义务考虑在内。本建议书的案文是基于[ITU-T X.1601]第10节规定的方法。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书或其他参考文献最新版本的可能性。当前有效的ITU-T建议书清单定期出版。本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

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

[ITU-T X.1602] ITU-T X.1602建议书（2016年），*软件即服务应用环境的安全要求*。

[ITU-T Y.3501] ITU-T Y.3501建议书（2016），*云计算 – 框架和高层要求*。

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 认证（authentication）[ITU-T X.1601]：核实用户、程序或装置的身份，这常常是允许获取信息系统资源的前提条件。

3.1.2 能力（capability）[b-ISO 15531-1]：有能力从事特定活动的品质。

3.1.3 云计算 cloud computing[b-ITU-T Y.3500]：有助于网络以按需自助方式调配和管理获取一系列可伸缩和富有弹性的、可共享的物理或虚拟资源的范式。

注 – 资源的例子包括服务器、操作系统、网络、软件、应用和存储设备。

3.1.4 云服务（cloud service）[b-ITU-T Y.3500]：通过使用定义的接口启动的云计算实现的一种或多种功能。

3.1.5 云服务客户（cloud service customer）[b-ITU-T Y.3500]：为使用云服务而具有业务关系的一方。

注 – 业务关系不必隐含财务协议。

3.1.6 云服务合作伙伴（cloud service partner）[b-ITU-T Y.3500]：支持或辅助云服务提供商或云服务客户活动或双方活动的一方。

3.1.7 云服务提供商（cloud service provider）[b-ITU-T Y.3500]：提供云服务的一方。

3.1.8 云服务用户（cloud service user）[b-ITU-T Y.3500]：与使用云服务的云服务客户相关联的自然人或其代表实体。

注 – 这类实体的例子包括设备和应用。

3.1.9 通信即服务（communications as a service）（CaaS）[b-ITU-T Y.3500]：云服务的类别，其中为云服务客户（3.1.5）提供的能力是实时通信和协作。

注 – CaaS既可提供平台能力类型，也可提供应用能力类型。

3.1.10 多租户（multi-tenancy）[b-ITU-T Y.3500]：物理和虚拟资源的分配方法能够使多租户及其计算和数据相互隔离并无法实现互访。

3.1.11 编排（orchestration） [b-ITU-T Y.3100]：IMT-2020背景下，旨在通过优化标准，对物理和虚拟基础设施的网络功能和资源进行自动安排、协调、实例化和使用的过程。

3.1.12 软件即服务（software as a service）[b-IUT-T Y.3500]：一种类别云服务，其中向云服务客户提供的云能力类型为应用能力类型。

3.2 本建议书定义的术语

无

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：

CaaS 作为服务的通信

CSC 云服务客户

CSN 云服务伙伴

CSP 云服务提供商

CSU 云服务用户

DDoS 分布式拒绝服务

GSM 全球移动系统

IAM 身份和接入管理

IaaS 基础设施即服务

ID 标识符

MMS 多媒体消息服务

NaaS 作为服务的网络

OS 操作系统

PaaS 作为服务的平台

PC 个人计算机

QR 快速响应

SaaS 作为服务的软件

SDK 软件开发包

SIM 用户身份模块

SMS 短消息

URL 统一资源定位符

(U)SIM （通用）用户识别模块

VoLTE 长期演进语音承载

VPN 虚拟专用网

5 惯例

在本建议书中，服务器和虚拟服务器没有区别。

6 CaaS概述

CaaS的定义见第3.1.9节。推荐将通信能力的开放性、通信软件支持和统一通信作为CaaS的一般要求（见[ITU-T Y.3501第11节）。

根据行业实践，这些功能通常通过CaaS实现或得到其支持：

– 电信服务和互联网服务的结合；
– 实时通信；
– 多设备同步；
– 通信资源隔离；
– 用户状态更新；
– 群聊或会议；
– 由其他SaaS嵌入；
– 用户选择加入或退出；
– 服务流程定制；
– 数据或文件共享；
– 身份和访问管理（IAM）。

图6-1描述了一个通用的CaaS服务模型。在图6-1中标注了四层：用户层；访问层；服务层和资源层。

– 用户层包含云服务用户（CSU）终端，这些终端可以运行一些CaaS客户端，并可以访问互联网甚至是电信网络。
– 接入层提供各种类型的隧道，通常允许终端接入其目标CaaS服务。
– 云服务提供商（CSP）拥有服务层，即CaaS层，且该提供商需依赖必要的内部和外部资源完成服务操作。服务层为云服务客户（CSC）定制服务流程并分配资源，为CSC与CSU维护（虚拟）动态服务网络，并为所有CSC隔离计算资源和通信网络。
– 资源层提供与数据处理和通信相关的底层基础设施资源，其中有些部分可以采用基础设施即服务（IaaS）、平台即服务（PaaS）和网络即服务（NaaS）。

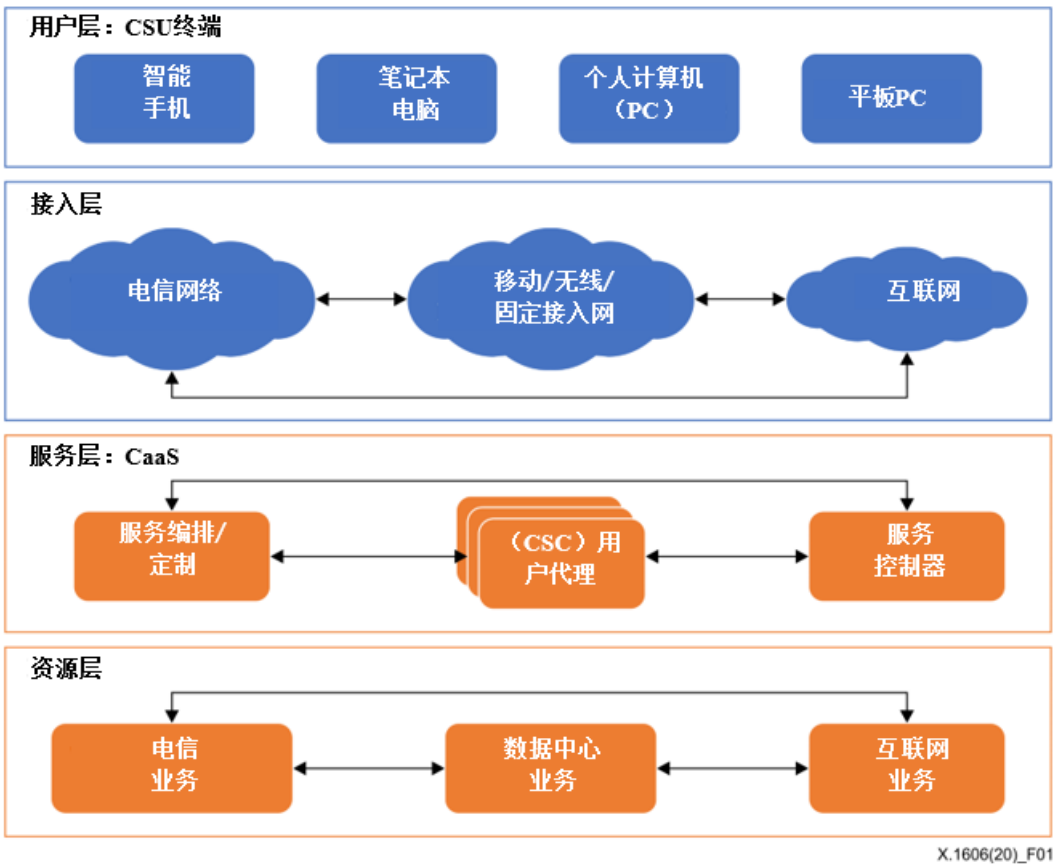

图 1 – 通用CaaS服务模型

本建议书的其它章节：

– 第7节分析了CaaS的安全威胁，其针对的是四层中一层或多层。

– 第8节就负责处理三层威胁的CaaS的安全要求提出了建议：

- CSU终端层；
- CaaS层；
- 业务资源层。

这里未涵盖接入层，因为其安全功能不受CaaS控制，尽管接入层的安全级别可以由CaaS和CSU评估或监控。

7 对CaaS的安全威胁

[ITU-T X.1601]确定的云计算安全威胁和挑战（亦在附录一中列出）适用于各种CaaS场景。此外，第7.1至7.8节确定了CaaS面临的一些具体威胁。

7.1 身份威胁

CaaS的核心是统一的通信能力，这与SaaS略有不同。CaaS利用云计算集成并增强终端之间的通信能力。CaaS支持大多数主流类型的终端或操作系统（OS），如智能手机或个人计算机。

因此在多点到多点的通信模式下，如果发生身份滥用现象，CaaS可能遭遇一些特殊威胁。

7.1.1 身份凭证盗窃

为了方便CSU，许多CaaS采用了一种认证解决方案，这种方案支持移动号码（即，移动标识符（ID））认证或用户名和密码认证，或同时支持两者。在这种情况下，解决方案中的默认用户名可以像移动标识一样配置。此外，一些CaaS支持使用一个标识的CSU通过多个终端同时接入某业务，或者支持同步多终端之间的历史通信信息。

移动号码认证的安全性在很大程度上有赖于认证的可信度、移动网络运营商的加密水平以及持有凭证的（通用）用户身份模块（U）SIM卡。移动网络，尤其是在全球移动通信联盟（GSMA）的网络中，存在一些漏洞（已得到实际认证）。这些漏洞会降低信任度，并可能导致身份凭证（暂时）失窃。例如，某些类型的用户识别模块（SIM）卡可以物理复制；在全球移动通信系统（GSM）网络中，一些通过短消息业务（SMS）传输的动态认证码会被截获。遭截获的临时加密密钥亦可悄悄临时用于盗窃用户身份。

此外，用户名和密码认证可以为滥用者提供与其他合格终端一起，使用这种认证类型监控CSU（同时） 的机会。例如，如果滥用者可以使用（U）SIM卡或软SIM凭证来处理CSU移动终端，则滥用者可以在缓存中获得用户名，并使用重置机制设置新密码，然后将密码缓存于终端。那么CSU有可能意识不到密码已经被重置，且正在进行的通信内容甚至它通信史都可能遭到滥用者的秘密监控。

7.1.2 伪造身份

一旦CSU的身份凭证遭盗用或被滥用者获得，该身份就可能被用来访问与CSU相关联的CSC服务。同时，滥用者还可得到拥有CSU身份凭证的社会实体，甚至伪造其他社会实体或创建新的社会实体，并首先通过存在（presence）功能显示。

存在是CaaS的一个常见特性，通常用小尺寸的图片和有限的文本实现一个CSU的自画像。通过存在特性，与同一CSC相关联的CSU可以从一个CSU获得快速确认。然而，滥用身份的存在可能被伪造，滥用于欺诈活动。例如，滥用者可以伪造成董事会成员，从会计师那里窃取机密的公司财务数据。

实时视频聊天可以是一种标准CaaS配置。此外亦可伪造遭滥用身份通过视频流显示的场景，以增强社会实体和欺诈活动的真实性。

7.2 账户生命周期面临的管理威胁

CSU、CSC或CSP可能都有权要求删除其管理的账户。在整个账户生命周期中，当账户要退出时，应事先商定CSP应如何通过整个CaaS服务进行内容和账户信息通信，CSC是否可以将这些数据保留在其逻辑空间中，或者CSU是否可以将这些数据保留在其终端内。

对终端的处置或终端失窃也可能意味着任何缓存的账户信息均应删除，且任何相关数据亦应删除。

7.3 编排造成的威胁

利用编排（见[b-ITU-T Y.3100]）功能，CSC可以自行或通过CSP定制其服务流程和服务能力。例如，CSC可以调整管理聊天组成员资格的流程和权限，还可以降低或提高CSU搜索联系人的限制范围。

就客户需求而言，CSP可以允许两个以上的CSC共享其联系人，甚至可以直接相互通信，还可将一个以上的CSC合并成一个更大的CSC。

此外，为了实现新的服务功能，CSP可以提高或降低CSU可访问网络的安全性前提。

任何没有充分考虑安全性的编排，都会给信息和服务的隔离造成负面影响。例如，如果通过编排让CSC的CaaS集成GSM网络的话音和消息服务，那么几乎不可能实现端到端的隔离特征，因为GSM网络实体采用的是早期技术，不支持任何类型的隔离特征。如果编排允许使用不安全的网络类型为更灵活服务功能提供支持，那么它会比某些CSC更容易增加CaaS的风险级别。例如，如果为确保CaaS的视频聊天质量，将作为隔离手段的虚拟专用网（VPN）接入要求从强制改为可选，则窃听风险将会增加。

7.4 终端环境的威胁

CaaS终端的安全环境可能不确定，尤其当终端为智能手机或便携式设备时。如果这些终端是个人财产，则背景可能会更复杂。CSU的亲属或访客亦可使用这些终端。终端的屏幕可以投影至另一屏幕或与另一屏幕共享，从而使通过未知屏幕录制成为可能。在不安全的网络中，终端的漏洞可能会更直接地暴露给攻击者。通过CaaS的通信内容可以进行解密并存储在终端中。所有这些情况都有可能导致数据泄漏。

如果攻击者能够控制一个终端（远程或本地），则可通过该终端利用CaaS甚至其CSU的漏洞。假设许多终端被同时控制并成为僵尸网络的一部分，攻击者也可能触发分布式拒绝服务（DDoS）攻击。

7.5 垃圾邮件威胁和恶意软件分发

CSU可能会受到来自其他CSU的骚扰或者甚至是通过CaaS发起的垃圾邮件钓鱼攻击。事实上，在大多数情况下，CSU很难合理地确定是信任短统一资源定位符（URL）还是快速响应码（QR）的信息，而这可能会导致CSU访问网络钓鱼网站或下载恶意软件。

7.6 插件威胁

对于CaaS而言，在基本服务之上提供一些插件功能是很自然的事情，例如文件共享、内置网络浏览器、内容管理系统甚至是电子商务。在大多数情况下，这些插件绝对属于轻量级。

插件的漏洞会给CaaS本身带来严重威胁。例如，点击一个不安全的短URL就可以调用网络浏览器扩展，但这种扩展缺乏应对危险网址的能力，从而大大增加了CSU甚至CaaS安全性遭破坏的可能。

有些插件可以引导CSU离开其当前的CaaS，并切换到某种无赖服务。如果CSU没意识到这种切换，就无法及时、适当地调整其信任度，从而造成大范围的损害（更多的漏洞被利用、勒索、恶意软件等）。

7.7 软件开发工具包威胁

CaaS可以提供一个软件开发工具包（SDK）以鼓励其他应用程序或SaaS的集成。集成意味着CaaS与其SDK用户之间存在一定程度的信任。因此，SDK用户的漏洞会增加攻击或滥用对CaaS的威胁。

由于一个终端可能有多个不同CSC的身份证书，因此CaaS SDK用户可以滥用这些证书，在未获允许的情况下非法访问其他CSC。

7.8 电信网络漏洞的威胁

如果除互联网接入外，CaaS还纳入了短信、长期演进语音（VoLTE）、电路呼叫、多媒体消息服务（MMS）和定位等电信网络运营商的其他功能，那么电信网络的安全性就会对CaaS产生直接影响。

任何成功滥用电信网络漏洞的行为都可能导致CaaS数据泄漏。同样，对电信网络的任何成功攻击，特别是对与CaaS服务器相连的节点发起攻击，都可能扩大CaaS的暴露面。

此外，由于现代商用终端可以根据预定义的策略，在不同的提供商之间主动切换接入网和虚拟专用网，而不会考虑接入网络可信性和真实性，因此CSU可能无法意识到是否在使用非安全网络环境，从而可能导致机密信息的泄漏。

8 CaaS的安全要求

[ITU-T X.1602]确定的SaaS安全要求适用于CaaS的场景。此外，为应对第7节阐述的威胁，本节又进一步确立了一些安全要求。

8.1 身份和访问管理

8.1.1 身份管理

CaaS应设置共享相同身份凭证的并行终端的上限。CaaS可将拥有必要硬件和服务标识的终端作为主控制器，通过它按需授权其他终端访问。

CaaS可以用相同的身份证书监控并行终端，使所有终端（或至少是主控制器）了解其他并行终端的最新状态。CSU可以使用主控制器或通过更安全的身份验证（如绕过身份验证）强制特定终端退出，禁止此终端将来的任何访问，甚至是删除其该终端内剩余的信息。

CaaS可以考虑指导CSU对不同CSC使用不同凭证（至少是不同的密码），这可以降低盗窃人使用被盗凭证访问多个CSC的风险。

8.1.2 接入控制

如果拥有一个身份证书的终端的并行功能属于CaaS的共同能力，那么允许CaaS获取并更新终端的地理位置，以使CaaS能够发现任何终端接入异常是有意义的。由于一个终端可以同时访问多个网络，所以CaaS可以考虑是否可以使用多维信息互查位置的真实性。

如果网络安全得不到保证，那么虚拟专网可能是增强基础设施安全性的上上之选。CaaS应考虑要求CSU 或CSC使用强制性虚拟专网服务，并禁止CSU或CSC采用任何其他虚拟专用网络服务作为接入强制VPN服务的跳接或中继。可选或不可信的虚拟专用网络可能会模糊终端的位置，还可能增加中间人攻击的风险。

此外，如果CSC不能接受被截获GSM SMS的风险，则CaaS应考虑监控所有CSU接入的网络类型。如果CSU属于GSM网络，则拒绝使用将SMS作为认证方法。另一种方法是，CaaS可以仅排除针对CSC的GSM SMS资源。

8.1.3 身份认证

由于CSU可以使用模糊的、不准确的、甚至是伪造的信息制作自画像，因此CaaS应提醒所有CSU考虑其联系人的社会身份是否已得到某可信第三方的验证。第三方可以是CSC、CaaS或任何其他独立机构。验证既可以是强制要求也可以是可选功能，如果是可选功能，则有必要提醒CSU，CSP或CSC不能对CSC中的社会身份真实性负责。

由于已成为CaaS客户的CSC的社会或商业身份可能与公开使用的完全不同，因此建议认证机构考虑将公开宣称的CSC身份与现有信息进行比较，以防止潜在的公众或商业欺诈。例如，恶意CSC可以伪装成一个慈善组织，通过伪造捐赠物品滥用CSU。

8.1.4 账户管理

由于一个CSU在CSC下至少可以有一个账户，一个CSC亦可在CaaS下至少拥有一个账户，因此CSC应根据数据的所有权向CSU或CSC提供账户的全部数据访问权。此外，由于需要取消或删除账户，所以CaaS应该提供可靠的能力，根据数据所有者的合法授权条款，在终端侧、服务侧和网络侧物理销毁账户数据。

8.2 终端安全

8.2.1 内部安全

CaaS应提供技术措施，如嵌入到CSU终端的安全工具或安全模块，进行循环安检或按需安检。安全检查可以在访问CaaS前评估CSU终端的背景是否满足强制性安全的要求。如果CSU终端未能通过安全检查，CaaS可以考虑（部分）拒绝提供服务。与此同时，CaaS应指导CSU解决发现的安全风险，或在CSU授权下直接修复漏洞。

8.2.2 外部安全

CSU终端使用的软件应由CaaS提供。CaaS还应提供一个安全的、官方或授权软件发布平台或来源。CaaS还应该公布验证机制，以便CSU终端可以在更新前使用此机制验证数据的真实性和完整性。如果更新失败，CSU终端中的操作系统或软件本身应该具有回滚功能。

大多数情况下，终端软件的安全更新是可选的。然而，如果某个漏洞会对CaaS、CSC或者甚至是另一CSU造成重大损害，且终端软件的安全更新会修复该漏洞，则CaaS可以考虑在根据用户协议成功实施更新前，暂时拒绝CSU终端的服务访问。

在大多数情况下，CaaS的终端软件分发是公开的。尽管如此，但在某些情况下CSC可能需要使用定制的终端软件，并要求仅在有限范围分发软件，例如仅向CSC员工分发。分发应该是有针对性的。在软件下载或更新完成之前，CSU与CaaS之间需要双向认证。

8.3 服务安全

8.3.1 编排的安全性

在部署或配置编排变更之前，有必要评估该变更是否会影响安全边界、降低安全级别或混淆信任关系。如果可能出现一些负面影响，那么应该重新协商CaaS的安全要求或协议，并由CSP、CSC甚至是CSU重新磋商并同意。

8.3.2 抵制垃圾邮件

CaaS应考虑支持将打击垃圾邮件的功能，作为CSC的一项可选能力。CSP也可以考虑允许CSC将第三方的打击垃圾邮件功能集成到自己的CaaS中。CSP、CSC和CSU之间的不同服务和用户协议可能会对是否以及如何使用打击垃圾邮件功能设置不同的限制。

例如，如果所有CSU都是某CSC的雇员，并且相应的CaaS专门用于为CSC服务，那么CSP与CSC之间的协议可能就足以使用打击垃圾邮件功能。

否则，如果有些CSU是CSC的客户，那么这些CSU有必要授权CSC （与CSP一起）助其对付垃圾邮件。

一般而言，打击垃圾邮件功能应安装于终端侧或云端或两者兼有。关于该功能使用的替代技术，请参见[b-ITU-T X.1244]和[b-ITU-T X.1246]。

8.4 安全协调

8.4.1 插件和SDK安全

CaaS应只允许使用已通过其服务所载安全检查的插件。终端软件应该有助于CaaS监测和分析任何插件异常。白名单将有助于CaaS限制插件访问外部链接或域名的能力。

如果插件需要访问客户数据才能提供服务，则先决条件是CSU的明确授权。插件访问客户数据的清晰记录，对以后的审计工作意义重大。

CaaS的软件开发工具包应能监控和分析应用程序异常或集成了软件开发工具包的SaaS。SDK应加密并隔离身份凭证，以避免任何潜在的滥用。例如，应用程序A和应用程序B都集成了相同的SDK并且存在于同一终端内，但是它们都不能访问对方的身份凭证。

8.4.2 基础设施安全

鉴于基础设施整合了短信和话音呼叫等电信网络的服务能力，因此CaaS应意识到来自基础设施的威胁。CaaS应考虑在自身和电信网络之间设置一个网关，以监控、反击或过滤可能在电信业务中传播的垃圾邮件和身份欺诈。CaaS能就CSU正在使用的通信渠道或服务类型发出提醒，是有意义的。

附录I

ITU-T X.1601所列安全威胁和挑战的快速指南

（此附录并非本建议书不可分割的组成部分。）

如第7节所述，[ITU-T X.1601]确定的云计算安全威胁和挑战适用于各种CaaS场景。本附录列出了[ITU-T X.1601]中的所有安全威胁和挑战，供快速查阅。如果需要更多的细节，请见[ITU-T X.1601]。

– 云计算的安全威胁

a) 云计算客户（CSC）的安全威胁

1) 数据丢失和泄露

2) 不安全的服务获取

3) 内部威胁

b) 云服务提供商（CSP）的安全威胁

1) 未经授权的管理获取

2) 内部威胁

– 云计算的安全挑战

a) 云服务客户（CSC）的安全挑战

1) 职责分工不明确

2) 丧失信任

3) 丧失管理

4) 丧失隐私

5) 服务的不可用性

6) 锁定云服务提供商

7) 盗用知识产权

8) 丧失软件完整性

b) 云服务提供商（CSP）的安全挑战

1) 职责分工不明确

2) 共享环境

3) 保护机制之间的相互矛盾和冲突

4) 管辖冲突

5) 演进风险

6) 不良的过渡和集成

7) 业务中断

8) 云服务伙伴（CSN）的锁定

9) 供应链漏洞

10) 软件依赖

c) 云服务伙伴（CSN）的安全挑战

1) 职责分工不明确

2) 盗用知识产权

3) 丧失软件完整性

附录II

安全威胁和安全要求的映射

（此附录并非本建议书不可分割的组成部分。）

本附录在第7节阐述的威胁与第8节的要求之间建立了关联（见表I.1）。

表 I.1 – 本建议书中的安全威胁与安全挑战的对应关系

第7节阐述的威胁	第8节提出的对应要求
7.1 身份威胁	8.1 身份和访问管理
7.1.1 身份凭证盗窃	8.1.1 身份管理 8.1.2 接入控制 8.1.4 账户管理
7.1.2 伪造身份	8.1.3 身份认证 8.1.4 账户管理
7.2 账户生命周期的管理威胁	8.1.4 账户管理
7.3 编排造成的威胁	8.3.1 编排的安全性
7.4 终端环境的威胁	8.2 终端安全
7.5 垃圾邮件威胁和恶意软件分发	8.2 终端安全 8.3.2 抵制垃圾邮件
7.6 插件威胁	8.4.1 插件和SDK安全
7.7 软件开发工具包威胁	8.4.1 插件和SDK安全
7.8 电信网络漏洞的威胁	8.4.2 基础设施安全

参考资料

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-ITU-T X.1246] Recommendation ITU-T X.1246 (2015), *Technologies involved in countering voice spam in telecommunication organizations*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network.*

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ISO 15531-1] ISO 15531-1:2004, *Industrial automation systems and integration – Industrial manufacturing management data – Part 1: General overview*.

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
2021年，日内瓦