国 际 电 信 联 盟

ITU-T X.1602

(03/2016)

国际电信联盟
电信标准化部门

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

软件即服务应用环境的安全要求

ITU-T X.1602 建议书

国际电信联盟

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
报文处理系统	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
生物测定安全	X.1080–X.1099
安全应用和服务	
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	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	
计算网络安全	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	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI相关建议书	X.1340–X.1349
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	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导则	X.1640–X.1659
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1602 建议书

软件即服务应用环境的安全要求

摘要

ITU-T X.1602建议书分析了软件即服务（SaaS）应用的成熟度，并为SaaS应用能有一个连贯安全的业务执行环境提出了安全要求。这些要求建议源自云服务提供商（CSP）和云服务合作伙伴（CSN），因为他们需要能满足其安全要求的SaaS应用环境。这些要求是一些通用要求，不受具体业务或情况的模型（例如，互联网业务或表述性状态转移（REST））、假设或解决方案等因素约束。

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.1602	2016-03-23	17	11.1002/1000/12615

关键词

安全要求，软件即服务（SaaS）应用环境，SaaS成熟度

* 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识别码，例如， http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）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，国际电联尚未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，因此特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.1602 建议书

软件即服务应用环境的安全要求

1 范围

本建议书主要探讨基于软件即服务（SaaS）应用成熟度级别的SaaS应用环境安全要求。本建议书的目标受众是云服务提供商（CSP）和云服务合作伙伴（CSN），如应用程序开发人员。

2 参考文献

无。

3 定义

3.1 他处定义的术语

本建议书使用的其他地方定义的术语如下：

3.1.1 **云服务**[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。

3.1.2 **云服务类别**[b-ITU-T Y.3500]：一组具有一些共同特性的云服务。

3.1.3 **云服务客户**[b-ITU-T Y.3500]：为使用云服务而具有业务关系的一方

3.1.4 **云服务合作伙伴**[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。

3.1.5 **云服务提供商**[b-ITU-T Y.3500]：提供云服务的一方。

3.1.6 **云服务用户**[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。

3.1.7 **桌面即服务** [b-ITU-T Y.3500]：提供给云服务客户的能力是远程创建、配置、管理、存储、执行和交付用户的桌面功能的能力。

3.1.8 **基础设施即服务（IaaS）**[b-ITU-T Y.3500]：一种云服务类别，其中提供给云服务客户的云功能类型是基础设施功能类型。

3.1.9 **软件即服务（SaaS）**[b-ITU-T Y.3500]：一种云服务类别，其中向云服务客户提供的云功能类型应用功能类型。

3.2 本建议书定义的术语

无。

4 缩写词及首字母缩略语

本建议书采用以下缩写词和首字母缩略语：

ASP 应用服务提供商

CaaS 通信即服务

CRM 客户关系管理

CSC 云服务客户

CSN 云服务合作伙伴

CSP 云服务提供商

DaaS 桌面即服务

IaaS 基础设施即服务

IAM 身份和接入管理

IdM 身份管理

OLAP 在线分析处理

OS 操作系统

PaaS 平台即服务

PKI 公钥基础设施

REST 表述性状态转移

SaaS 软件即服务

SAP 服务访问点

SLA 服务水平协议

5 惯例

无

6 概述

软件即服务（SaaS）应用环境是一种面向服务的多租户开发、部署和执行环境，其中软件及其相关数据集中托管，并且通常由用户利用互联网上的客户端（例如web浏览器）按需访问。

虽然本建议书主要探讨SaaS，但其中的一些概念也适用于其他云服务类别（亦包括应用功能类型，例如通信即服务（CaaS））。

图1描述了SaaS应用环境的一种概念模型。基础设施即服务（IaaS）、平台即服务（PaaS）和桌面即服务（DaaS）的基本功能将封装成服务，并利用输出的服务访问点（SAP）提供连贯的安全访问。在本建议书中，IaaS可提供计算服务、存储服务和网络服务；PaaS可提供平台服务，DaaS可为SaaS应用环境提供桌面服务。所有这些服务构成应用开发的基本构件。

这种环境还提供一些必要的服务管理功能，包括服务注册、服务配置、服务编排、服务依赖性检查、服务访问控制、服务隔离、服务监控等服务控制功能。

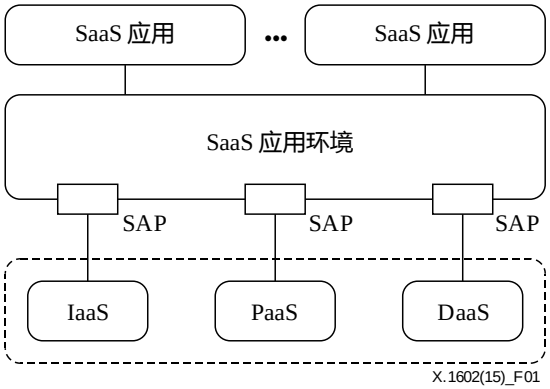
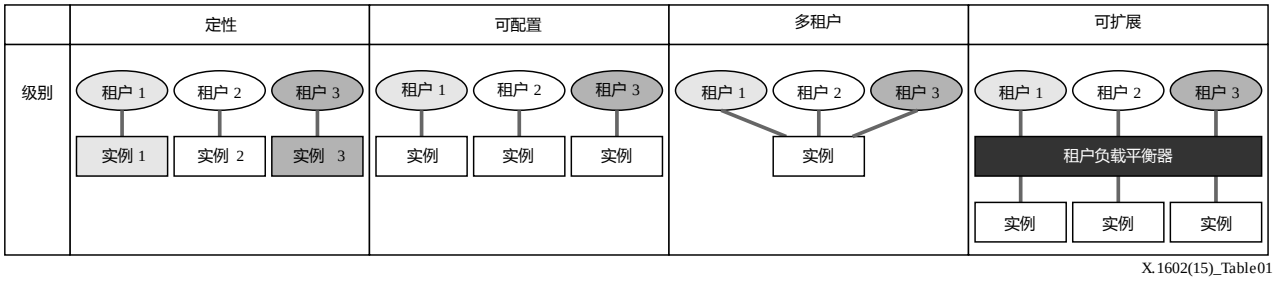


图1 – SaaS应用环境的概念模型

7 SaaS 应用的成熟度级别

业内将SaaS的成熟度分为四个级别，简单地称为定制级别、可配置级别、多租户级别和可扩展级别。每个级别覆盖前一个级别的特性，并提供扩展的特性。不同SaaS成熟度模型的特性图示见表1。

表1 – SaaS应用的成熟度图



SaaS应用的不同成熟度级别对SaaS应用环境有不同的安全要求，这些要求将在第8节从CSP和CSN角度进行说明。

7.1 第1级：定制SaaS应用

定制SaaS应用类似于传统应用服务提供商（ASP）的软件交付模式。每个客户都有属于自己的定制版SaaS应用，并在云服务器上运行单个应用实例。如图2所示，定制应用实例包含整个执行环境，包括操作系统（OS）、数据管理系统和每个租户特定的中间件，SaaS环境提供商必须维持多个实例。这个模型难以扩展，以满足客户日益增长的需求，而且运营成本很高。

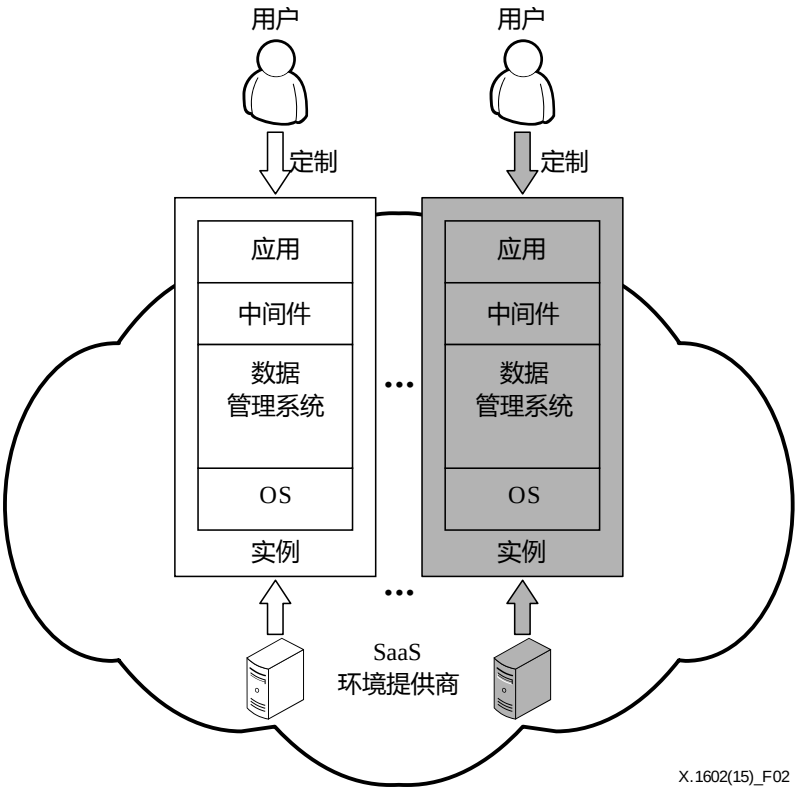


图2 – 定制SaaS应用的架构

通过将服务器移至云并进行相对较少的修改，典型的客户端-服务器应用很容易转换为定制SaaS应用。适于这种情况的应用通常按照企业或机构的特定要求开发。首要的考虑因素是系统本身的安全性，因此通常的方法是将一组物理机器集中到专用区域，部署数据管理系统（为不同类型的数据提供抽象的持久性运算和方法）并安装相关软件。该系统仅供内部使用，有严格的访问控制。所有客户的应用实例模板都相同，模板提供有限的配置能力。然而，每个客户的实例都是完全独立的。

7.2 第2级：可配置SaaS应用

对于一些非定制的常用应用，例如自助网站建设系统，SaaS应用提供商为这些应用提供通用模板，为这些应用的实例提供若干套运行环境。基于同一模板，客户能够通过配置应用的外观和行为，创建多个独立的应用实例，这些实通过单个虚拟或物理机部署和执行，以满足其定制要求。应用实例彼此隔离。这一架构见图3。

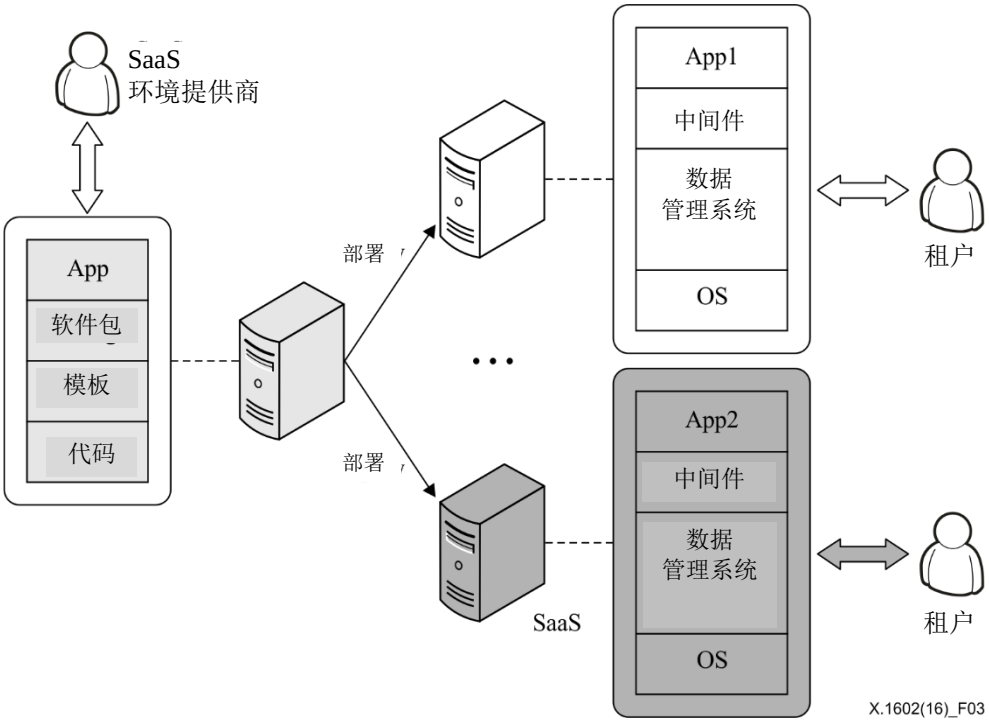


图3 – 可配置SaaS应用的架构

可配置SaaS应用具有以下特点：

1) 初始部署的应用是标准产品的副本，租户可按照自己的要求配置应用。但是产品的配置选择有限。

2) 对于SaaS应用提供商，对产品代码做出的任何改变可以马上推广给所有租户。但每个实例适合代码更新或优化很少，因为可能会发生因更新或优化而导致的向前兼容性问题。

3) 租户在各自相互隔离的虚拟机或物理机存储数据。因此，SaaS环境提供商必须提供足够的资源（如存储空间），以支撑突发的大并发压力。

随着软件技术的发展和改进，将为应用提供足够的配置选择，以满足用户的定制需求，而且配置和使用过程应更加智能和自动化。SaaS应用提供商将产品分为不同的版本，以适应不同层次租户的要求。

7.3 第3级：多租户SaaS应用

在这一级别，通过可配置化元数据，SaaS应用提供商只运行单个实例就能供应多个租户同时使用。多租户可以在不同的层（包括操作系统、数据管理系统、中间件和应用）实现。引入租户标识符，以便对不同的客户进行区分。在数据管理系统中使用数据库时，数据库架构扩展，将租户身份参数包括进来，以便将所有客户的数据存入同一组表中。数据库查询时亦需要租户身份，以便针对特定客户检索数据。图4显示了多租户SaaS应用的一般架构。

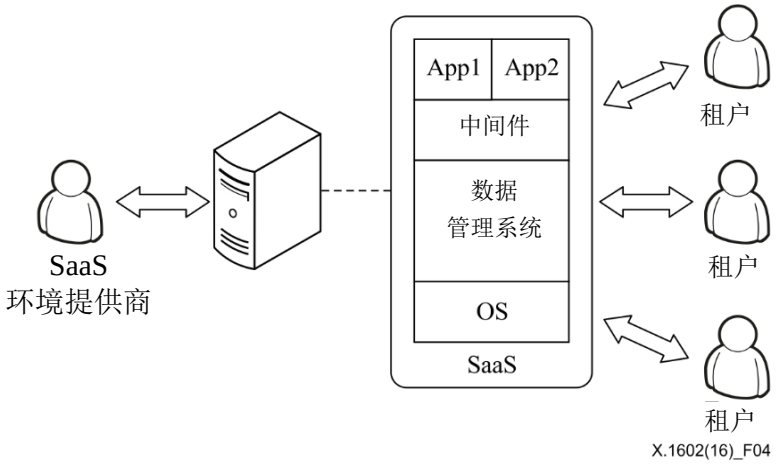


图4 – 多租户SaaS应用的架构

商业智能SaaS，例如客户关系管理（CRM），被视为这一级别的典型例子。迄今为止，更多工作放在了将数据仓储和云计算与SaaS相结合，以提供在线商业智能应用。数据仓库托管于数据中心，预先确定商业智能应用和数据模型极少与定制结合使用。对于租户，他们需要做的是选择商业智能应用所需的数据元，定义数据源到数据仓库和数据模型的数据映射。该系统将来自多个源系统的数据集成到数据仓库中，通过使用自动生成的脚本，支持在线分析处理（OLAP）应用。通常在运行时，单个商业智能应用实例利用元数据技术同时供多个租户使用。授权和安全策略保证每个客户的数据和应用访问都是相互隔离的。

此级别在计算和存储资源利用效率方面高得多，因此能够容纳更多租户。此外，利用数据分区和平行技术，也可能实现可比的性能、可扩展性和灵活性。

可配置性和多租户效率是这一级SaaS应用的显著特点。

7.4 第4级：可扩展SaaS应用

大多数公共网络服务提供商可支持任意多的客户作为多租户。因此，底层平台架构从硬件到应用的每一层须能够针对应用和服务轻松扩展，如图5所示。因此无需额外的应用系统重构，就可以增加更多的租户和每租户用户。

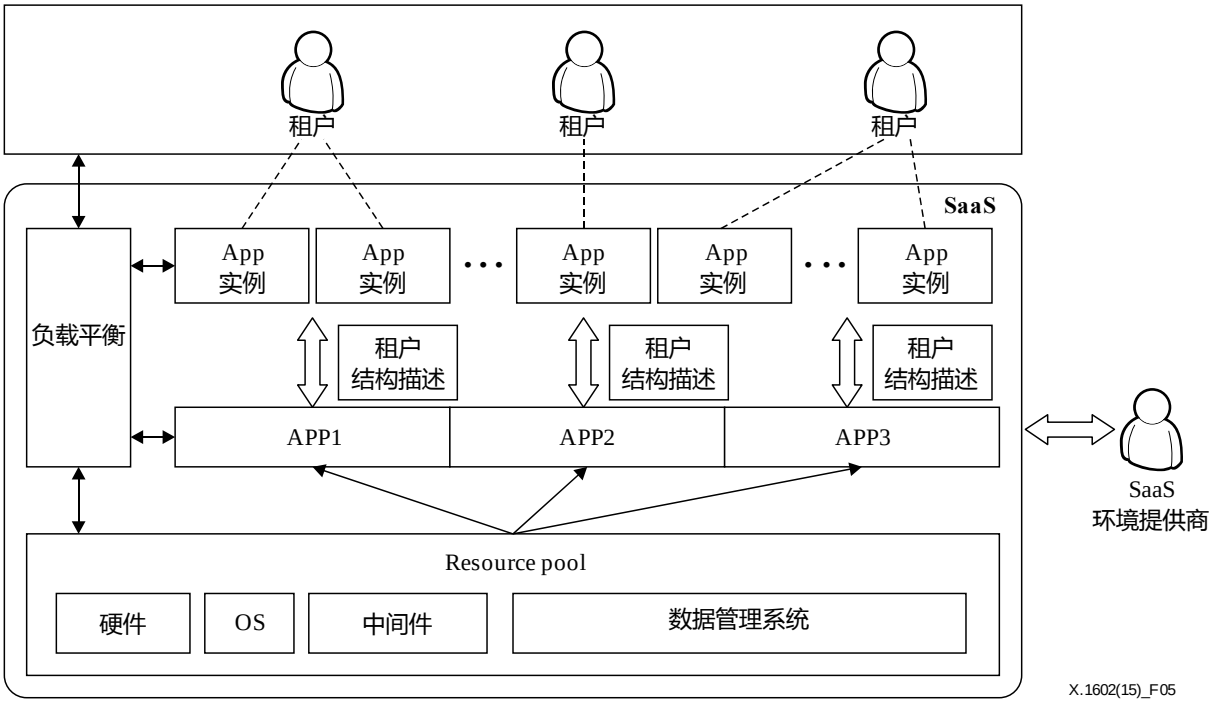


图5 – 可扩展SaaS应用的架构

对于应用层，增加新租户时，将根据具体租户的要求产生一个或以上应用实例，或根据基于负载平衡机制的要求来选择一个适当的现有实例。此类环境下所有的应用实例均须以动态的方式创建。

可扩展SaaS应用的底层资源亦支持灵活扩展。所有硬件、中间件、软件和数据在资源池进行管理。应用以动态方式从资源池获取所需资源。无需任何重组或重构，即可在必要时添加新资源。

对于动态扩展技术，有多重设计考虑，包括扩展选择、资源分配、服务水平协议（SLA）等。新租户可作为单个实例执行，也可与其他租户共享实例。运行不同类型租户的不同实例可分配到不同的资源。SaaS环境提供商在使用负载平衡和共享资源时，应针对不同租户考虑不同的SLA。

8 SaaS 应用环境的安全要求

图6显示了云服务客户（CSC）、CSP和CSN之间相对于SaaS应用环境的关系，其中CSP和CSN在执行不同功能中发挥不同的作用。CSN可作为CSP的内容提供商、软件提供商、系统集成商或审计师，而CSN和CSP可为CSC开发应用。CSP和CSN可以连接到SaaS应用环境，而CSC只能与SaaS应用环境上的应用程序进行交互。因此，本建议书主要探讨不同成熟度模型中CSP和CSN的SaaS应用环境的安全要求。SaaS应用环境的安全要求最初由CSP和CSN提出，因为他们需要能够满足其安全性需求的SaaS应用环境。

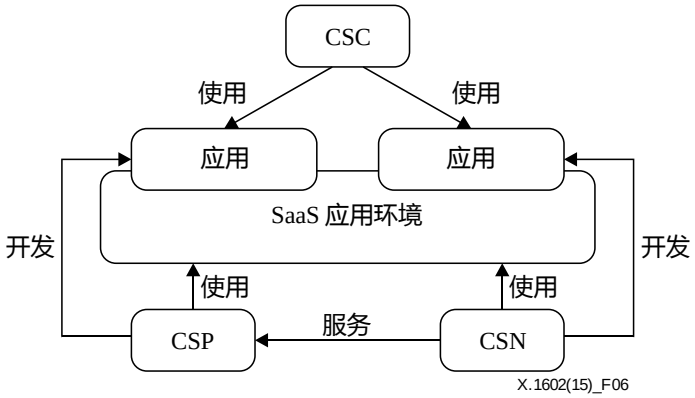


图6 – CSC、CSP和CSN之间的关系

CSP和CAN对于不同级别SaaS的环境有各自的安全要求。表2阐明了CSP和CSN对SaaS应用环境的安全性要求。同时适用于CSP和CSN的要求称为通用要求。

表2 – CSP和CSN对SaaS应用环境的安全要求

	SaaS应用环境
通用要求	身份和访问管理、数据安全、安全评估和审计、接口安全、安全强化。
CSP	可用性、服务互操作性/便携性保证、软件资产保护、合法合规、源代码的安全性验证。
CSN	审计安全、软件安全、软件的可维护性。

8.1 通用安全要求

CSP和CSN对SaaS应用环境有若干项通用安全要求。

8.1.1 身份和访问管理（IAM）

8.1.1.1 身份管理（IDM）

SaaS应用环境中涉及多个管理员和用户，SaaS应用环境可以内部访问（CSP），亦可外部访问（CSN）。出于身份保护考虑以及为了在这样一个动态和开放的SaaS应用环境中方便访问管理、认证、授权和交易审核流程，都需要IdM。

对于所有成熟度模型，IdM应能够在不同的安全域使用各种认证机制实现SaaS应用环境的单点登录和/或身份联盟。

8.1.1.2 信任模型

多租户和可扩展级别SaaS应用环境需要纳入一个总体信任模型。该信任模式便于创建可信实体的岛屿和/或联盟。从而SaaS应用环境管理系统、底层资源、管理程序、在SaaS应用环境上构建的虚拟机和应用能够对其它实体和和组件的身份和授权权限进行验证。每一个信任岛屿或联盟都将以一个或多个受信任的管理机构（如，公钥基础实施（PKI）证书管理机构）为基础。

8.1.1.3 访问管理

SaaS应用环境管理员须提供相关机制，向租户的管理员委托授权。租户的管理员针对其相应资源授予访问权限。这类SaaS应用环境的访问管理应支持多种访问控制模型，如基于身份的模型、基于策略的模型、基于角色的模型、基于任务模型等等。

对于定制和可配置级别的SaaS应用，基于角色的访问控制模型是一项基本要求。例如，支持建立CSP所提供服务的CSN可以负责的一些应用，但没有管理整个云服务体系的权限。此外，CSN只能利用被授予的访问权限访问一部分资源。但CSN可以通过向其他CSN提供应用接口共享其资源。

对于多租户和可扩展级别，需要为每个用户和每个用户组整合访问控制模型。对于基于角色的访问控制，应根据工作流中的任务组和授予这些任务组的权限使用多租户之间的共享资源。因此，在执行这些任务组时，SaaS应用环境应定义支持基于任务的访问控制机制。此机制用于确保及时授予和撤销租户对底层资源的访问权限，避免底层资源被未经授权地利用。

8.1.2 接口安全

SaaS应用环境须确保向CSP或CSN开放的接口（通过这些接口提供和开发各种云计算服务）的安全，并须确保基于这些接口的通信的安全。现有的可用来保障接口安全的机制包括但不限于：单边/相互认证、完整性校验、数字签名等。

8.1.3 数据安全性

8.1.3.1 数据隔离

数据隔离可以逻辑或物理方式实现。物理隔离应通过物理存储器的访问控制来完成，并应要求SaaS应用环境将不同租户的数据存储在不同的物理存储区，或通过访问许可、数据域或任何其他方法实现不同租户的数据访问控制。逻辑隔离意味着不同租户应避免利用虚拟化等技术手段访问其他租户的数据，即使所有数据存储在一起亦不允许。

对于定制和可配置级别的SaaS应用，在物理层面每个租户的数据都是分开储存、相互隔离的。

对于多租户和可扩展级SaaS应用，所有租户的数据都存储在云中。因此，SaaS应用环境必须足够智能，以隔离不同租户的数据，且无论是静态、处理中还是传输中，不同租户的数据之间均保持相互隔离。应确保物理层面或逻辑层面每个租户之间的界限，这取决于所要求的隔离粒度和云计算软硬件的具体部署情况。

8.1.3.2 数据机密性

在大多数情况下，租户的数据是在机房外储存和利用的，存在泄露风险。因此，SaaS应用环境须支持加密机制，以确保数据在传输、处理或流出过程中的机密性，并防止因应用中的安全漏洞导致数据泄漏。

数据加密服务对所有SaaS级别而言都是必要的。必须对关键数据进行加密，以防止泄露。

对于多租户和可扩展级别，由于租户的数据应存储在一个数据库甚至是一个大表中，SaaS应用环境须提供适当的密钥管理机制，以确保数据不被其他租户破解。

8.1.3.3 数据完整性

数据（包括系统数据和用户数据，如记录和配置数据）要求SaaS应用环境支持完整性机制，以避免数据在传输、处理和流出过程中被未经授权地篡改。

系统日志和应用日志不能修改。在这种情况下，如出现非法使用或滥用，CSP和恶意软件无法通过修改日志隐藏痕迹。

SaaS应用可能要求CSC按需进行配置。未经授权亦不得擅自修改配置数据，例如配置文件。

在SaaS应用环境中，用户数据存储在由CSP管理的云中。在这种情况下，验证数据完整性成为一项重要的安全性要求。此外，必须验证海量数据的完整性。

8.1.3.4 数据可靠性

要支持数据可靠性，SaaS应用环境须支持数据备份或冗余机制，以确保即使云的一部分存储节点失效的情况下，租户亦可访问数据。

托管的数据必须实施多站点备份；否则，该数据将完全无效。SaaS应用环境必须具备完全恢复数据和及时还原数据以及保持数据同步以确保多拷贝一致性的能力。

8.1.3.5 数据可追溯性和控制

SaaS应用环境须确保数据的物理位置遵守适用的法律和当地法规以及法律协议中的所有相关限制。SaaS应用环境须向CSC提供明确说明其数据存储位置并验证其数据被存在恰当位置的方法。

对共享和虚拟化基础设施的主要关切不仅包括用户丧失对其数据的控制，还有定位数据和控制其整个生命周期的问题。在任何特定时间，SaaS应用环境均须确切地了解系统数据和用户数据的存储和处理位置，并为CSC验证数据位置。使用期间和使用后，未经授权的第三方（包括其他CSP）均不可能跟踪数据的移动情况。

8.1.4 安全评估和审计

当底层资源发生变化、被破解或使用不当时，须触发SaaS应用环境启动安全评估程序，以评估具体的安全服务或应用的安全策略是否受到影响，如无法满足预定的条件，则建议发出指示或指令。应委托一个授权方检验SaaS应用环境是否符合适用的安全要求。安全评估或安全审计可由CSC、CSP或第三方（CSN）进行，安全认证可由得到授权的第三方（CSN）进行。

应通过独立可信的第三方来提供可靠、独立和中立的安全评估或安全审计。

8.1.5 安全强化

SaaS应用环境的主要目标是提供面向安全服务的多租户SaaS应用程序开发、部署和执行环境。在某些情况下，SaaS应用的安全功能不足或不够完备。SaaS应用环境须检索和检验SaaS应用不完善的安全功能，并根据那些不完善的安全功能提供差异化的安全强化机制来增强SaaS应用，以满足不同环境下不同租户的安全性要求。应用的安全功能包括应用处于空闲状态时的静态安全功能和应用运行时的动态安全功能。

8.2 CSP的安全性要求

除通用安全要求外，CSP对SaaS应用环境还有具体的安全性要求。

8.2.1 可用性

对于CSP，SaaS应用环境须确保CSC始终得到服务，这要求对硬件/软件故障进行处理以及拒绝服务攻击等。必须确保将CSC的停机时间降到最低。

8.2.2 服务互操作性/便携性保障

如CSC希望将其所有或部分系统迁移到另一个CSP，原CSP要求SaaS应用环境保障服务的互操作性和便携性，以便尽量减少对CSC业务的损害。此外，SaaS应用环境须保证在原CSP存储的相关数据将被永久删除，任何其它方无法恢复。

8.2.3 软件资产保护

在SaaS应用环境中，所有软件资产（如应用程序、应用程序内部数据、脚本、宏、功能代码库、软件许可等）都必须得到保护。

CSP要求SaaS应用环境保护由CSP或CSN提供的任何软件资产的保密性和完整性，这意味着这些软件资产不得被复制、盗用、篡改、泄露或以其他未授权的方式使用。

8.2.4 合法合规

虽然CSP可以使用数据备份和冗余机制来确保CSC数据的可靠性，但SaaS应用环境须确保数据副本的保留时间不超过适用的数据保护法律所允许的数据保留期。

8.2.5 源代码的安全性验证

如在SaaS应用环境中，CSN可向CSP提供应用的代码、内容或软件，SaaS应用环境须提供相关机制，协助CSP来验证代码，防范恶意代码。

8.3 CSN的安全性要求

在SaaS应用环境中，CSN可以是应用程序开发商、内容提供商、软件提供商、系统集成商和审计师。除了通用安全要求外，CSN对SaaS应用环境还有自己的安全性要求。

8.3.1 审计安全

如CSN作为审计师，SaaS应用环境须提供相关机制，协助CSN收集审计事件、记录并报告租户和应用粒度层面的信息。这些信息用来确保CSP的服务符合政府规则要求和与租户签订的法律协议。SaaS应用环境还须提供相关机制，协助CSN确保CSP系统内的审计组件收集和报告的信息是正确的，不会被篡改或操纵。

此外，SaaS应用环境须为CSN提供记录重要数据变更、在线监测数据可用性的能力，以便及时发出安全告警，从而减少损失。

8.3.2 软件安全性

如CSN作为云内容或软件开发商，SaaS应用环境须提供相关机制，协助CSN确保提供给CSP的代码或其他组件符合CSP要求的编程限制。此外，代码或组件不应包含恶意程式或侵犯CSP云服务的完整性。

8.3.3 软件的可维护性

如CSN作为云软件开发商，SaaS应用环境须支持帮助CSN为CSP系统提供源代码或其它功能的机制。源代码或功能须含有版本控制和其他适当方法，以确保在服务的整个生命周期中得以保留。这些方法包括但不限于：提供更新以修复已知的漏洞，解除对有已知漏洞的其他组件的依赖性，提高整个系统的安全性。

参考书目

[b-ITU-T X.1601] ITU-T X.1601建议书（2014年），云计算的安全框架。

[b-ITU-T Y.3500] ITU-T Y.3500建议书（2014年）| ISO/IEC 17788:2014，信息技术 – 云计算 – 概述和术语（*Information technology – Cloud computing – Overview and vocabulary*）。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其它组件的建设、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	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
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2017年，日内瓦