国际电信联盟
电信标准化部门

建议书

ITU-T X.1454 (09/2023)

X系列：数据网、开放系统通信和安全性

安全应用和服务 (2) – 应用安全(2)

支持位置的智能办公服务的安全措施

ITU-T X系列建议书

数据网、开放系统通信和安全性

公众数据网络	X.1-X.199
开放系统互连	X.200-X.299
网络间的互通	X.300-X.399
消息处理系统	X.400-X.499
目录	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
开放式分布式处理	X.900-X.999
信息和网络安全	X.1000-X.1099
安全应用和服务 （1）	X.1100-X.1199
网络空间安全	X.1200-X.1299
安全的应用程序和服务 （2）	X.1300-X.1499
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
经认证的邮件	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
分布式账本技术（DLT）安全	X.1400-X.1429
应用安全(2)	**X.1450-X.1459**
网络安全(2)	X.1470-X.1489
网络安全信息交换	X.1500-X.1599
云计算安全	X.1600-X.1699
量子通信	X.1700-X.1729
数据安全	X.1750-X.1799
IMT-2020安全性	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.1454建议书

支持位置的智能办公服务的安全措施

摘要

结合多种智能应用的智能办公服务旨在提高办公业务的质量和加强效率管理。由于信息通信技术（ICT）是智能办公服务的技术基础，电信运营商在智能办公服务的利益攸关方中扮演着重要的角色。

典型的智能办公服务包括智慧停车、智能驾驶、智能零售店、智能办公室、智能会议室管理、智慧水务和智能能耗管理。在这些典型的智能办公服务中，运营商提供的位置数据是大多数智能办公服务实施的关键要素之一。

为了确保支持位置的智能办公服务的安全性，需要分析特定于支持位置的服务的安全威胁和相关安全性要求，并制定整体的安全措施。

ITU-T X.1454建议书分析了支持位置的智能办公服务的典型应用场景，明确了其安全威胁和要求，并为智能办公场所的运营商和关键利益攸关方制定了安全措施，以保护支持位置的服务。

历史沿革 *

版本	建议书	批准时间	研究组	唯一ID
1.0	ITU-T X.1454	2023-09-08	17	11.1002/1000/15111

关键词

位置、安全措施、智能办公服务。

* 欲查阅建议书，请在网络浏览器地址域键入URL https://handle.itu.int/ ，随后输入建议书的唯一识别码。

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”等其他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他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，国际电联未收到实施本建议书可能需要的受专利/软件版权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ITU-T网站查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1454建议书

支持位置的智能办公服务的安全措施

1 范围

本建议书分析了支持位置的智能办公服务的典型应用场景，明确了特定于支持位置的服务的安全威胁和要求，从而为智能办公场所的运营商和关键利益攸关方制定了安全措施，以保护支持位置的服务。

2 参引

下列ITU-T建议书和其他参引的条款，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。所有建议书和其他参引均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参引的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

无。

3 定义

3.1 他处定义的术语

无。

3.2 本建议书定义的术语

本建议书定义下列术语：

3.2.1 智能办公服务：一种集多种智能应用（如，智慧停车、智慧水务、智能零售店）于一体的服务，旨在服务和支持办公业务，提高办公质量、管理效率，并为人们创造适宜的办公环境。

4 缩写词和首字母缩略语

本建议书采用下列缩写词和首字母缩略语：

DDoS 分布式拒绝服务

GNSS 全球卫星导航系统

ICT 信息通信技术

RNSS 卫星无线电导航系统

SEM 智慧环境监测

UWB 超宽带

WiFi 无线保真

5 惯例

关键词“须”（**is required to**）指必须严格遵守某项要求，如果宣称符合本文件，则不得出现任何偏差。

6 支持位置的智能办公服务概览

根据利用信息通信技术（ICT）和其他手段来提高生活质量、城市运营和服务效率以及竞争力的可持续智慧城市愿景，智能办公服务成为可持续智慧城市的一项典型应用。

结合了多种智能应用（如，智慧停车、智慧水务、智能零售店）的智能办公服务旨在提高办公企业产品的质量及其管理效率。

由于智能办公服务结合了多种智能应用，因此其关键利益攸关方呈多样化。由于ICT是智能办公服务的技术基础，在典型的智能办公服务中，运营商提供的位置数据是实施大多数这些服务的关键要素之一。

支持位置的智能办公系统的关键利益攸关方主要包括：

– 智能办公服务提供商；

– 数据和计算提供商；

– 传感和基础设施提供商；

– 用户。

注 – 这些关键利益攸关方，即支持位置的智能办公系统中的智能办公服务提供商、数据和计算提供商以及传感和基础设施提供商，可以是多家独立的提供商，也可以是一家集成服务提供商。

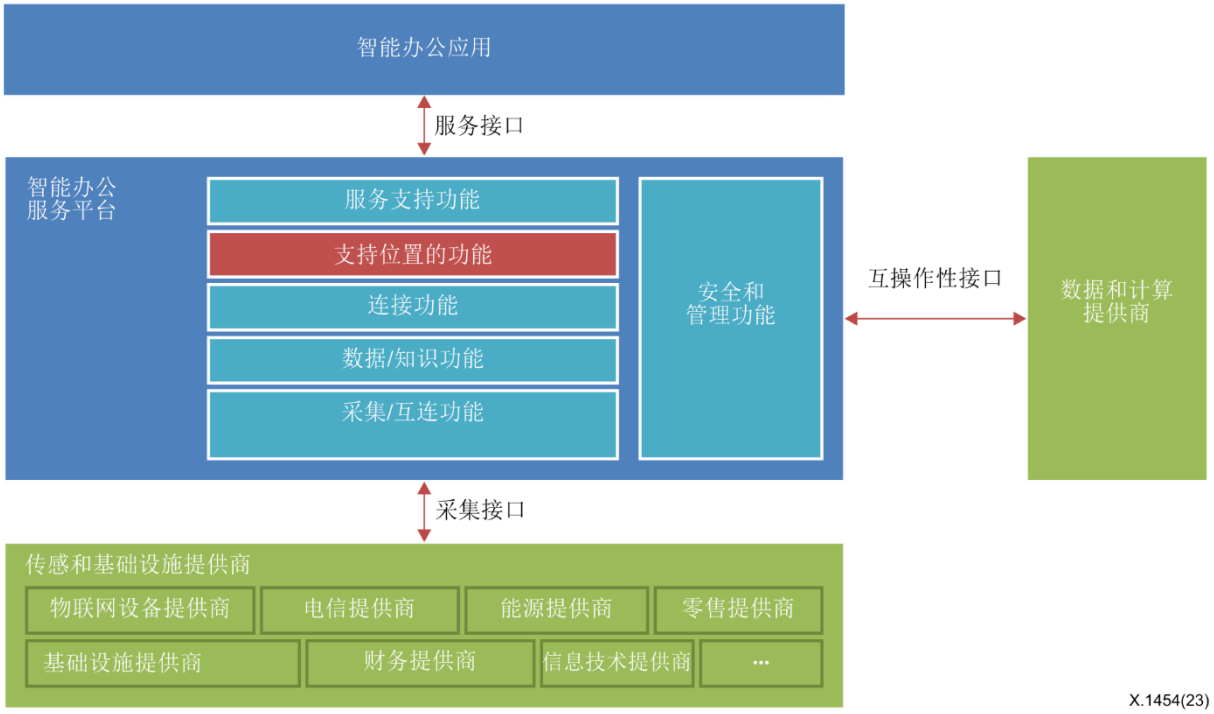

图1 – 支持位置的智能办公系统概览

支持位置的智能办公系统提供下列功能：

– **采集/互连功能：**提供从不同数据收集系统来源采集数据的机制。
– **数据/知识功能：**支持数据处理、增值和将信息转化为知识。
– **连接功能：**实现访问不同级别的信息。
– **支持位置的功能：**提供来自运营商系统的位置数据。
– **服务支持功能：**协调每项行动中可能涉及的所有服务，为互操作性功能提供支持。
– **安全和管理功能：**提供审计、监控和安全等横向功能。

接口实现了各功能之间的通信：

– **采集接口：**该接口实现了从外部元素收集信息。
– **互操作性接口：**该接口实现了与外部数据提供商和第三方计算系统的通信。
– **服务接口：**该接口实现了应用程序对应用程序的访问，以支持智能办公服务平台提供的功能。

7 支持位置的智能办公服务的典型应用场景

7.1 智慧停车

智慧停车将停车资源高效整合到办公场所的停车场，并与其他系统（如，外部支付系统、WEB/app停车系统）协调停车设施。

智慧停车可包括停车引导、预订停车位、反向寻车、车辆自动进入控制和自助缴费等典型功能。支持位置的智慧停车功能如下：

– **停车引导：**空闲停车位的位置信息支持发布停车引导信息。
– **预订停车位：**位置信息可以帮助搜索关于可用停车位的信息并提前预订停车位。
– **反向寻车：**如果车主忘记把车停在了哪里，位置信息可以帮助他们识别他们的停车位置。

7.2 智慧环境监测

作为一种自我监测和自我保护的环境监测应用，智慧环境监测（SEM）可以感知当前的环境状态。

SEM可包括SEM平台、SEM设备和网络等功能实体。支持位置的智慧环境监测功能如下：

– **测量设置管理：**设备的位置以及环境因素是测量设置的必要信息。
– **数据展示：**（一台或多台SEM设备在）每个给定位置的原始数据是用于展示环境质量的可选信息。

7.3 智能递送

智能递送利用了智能办公场景中的无人驾驶车辆和机器人应用，可以自动递送包裹、文件、办公用品等。

支持位置的智能递送功能如下：

– 通过提供厘米级精度的定位能力来辅助自动驾驶。
– 通过将递送订单与设备位置对照起来，提高车辆/机器人的配送效率。

– 通过跟踪车辆/机器人的实时位置和轨迹，优化递送路线并监控递送过程。

8 支持位置的智能办公服务面临的安全威胁

8.1 数据安全威胁

8.1.1 窃取位置数据

智能办公服务中的位置数据可能基于开放的无线网络，攻击者可通过监控无线信道来窃取位置数据。

8.1.2 篡改位置数据

攻击者可以捕获网络传输的位置数据中的数据包，并恶意修改/伪造位置数据以发起进一步攻击。在某些情况下，被修改/伪造的位置数据可导致安全问题，如智慧停车、智能驾驶和紧急救援。

8.1.3 拦截位置数据报告

攻击者可通过拒绝向网络或智能办公服务平台报告物联网设备的位置数据来捕获或篡改物联网设备。

8.1.4 未经授权调用位置数据

如果应用程序和智能办公服务平台之间没有身份验证机制，位置数据可被攻击者未经授权地调用。

8.1.5 数据不可用

数据格式不统一可导致智能办公室中的应用不可用，例如，室内位置数据格式不统一（包括与楼层、房间、座位相关的数据）可令机器人在向收件人递送包裹时感到迷惑。

8.1.6 泄露行为信息

这种威胁可能发生在智能办公平台被篡改或攻击者假冒法人实体，趁机获取用户的行为信息（如路线规划偏好）用于恶意目的，例如倒卖以获利。

8.1.7 未经用户同意的定位

当位置功能实体在未经用户同意的情况下收集用户的位置数据，并对相关数据进行分析时，包括在范围、意图、方法、结果和使用方面，就会发生这种威胁。

8.2 设备安全威胁

8.2.1 软硬件漏洞

在开发定位设备的过程中有可能引入安全漏洞和威胁。例如，用于调试的端口可能未得到适当保护，可能使用了弱加密算法，无法应用硬件和软件更新，以及缺乏及时的完整性检查。

8.2.2 操纵定位设备

攻击者可通过篡改传感和基础设施系统来操纵定位设备，这可能导致定位结果不准确。

8.3 接口安全威胁

8.3.1 采集接口

传感和基础设施提供商与智能办公服务平台之间的接口容易受到以下威胁：

– **嗅探数据：**如果智能办公服务平台与传感和基础设施提供商之间没有身份验证和授权机制，攻击者可冒充智能办公服务平台来收集传感和基础设施数据。

– **拒绝服务：**攻击者可通过修改数据收集策略（例如，在非常短的时间内频繁收集传感和基础设施数据）来发起分布式拒绝服务（DDoS）攻击。

– **信息泄露：**移动设备通过采集接口向智能办公服务平台定期发送服务数据，尤其是位置数据，如果攻击者能够嗅探到服务和位置数据，他们会注意到用户的日常生活。

8.3.2 互操作性接口

智能办公服务平台和数据/计算提供商之间的接口容易受到以下威胁：

– **未经授权的数据访问：**如果智能办公服务平台和数据/计算提供商之间没有身份验证和授权机制，互操作性接口可被攻击者篡改以访问服务数据、位置数据和配置文件数据。

– **伪造数据：**如果智能办公服务平台和数据/计算提供商之间没有身份验证和授权机制，互操作性接口可被攻击者篡改以伪造服务数据、位置数据和配置文件数据，这种威胁可能导致信息泄漏、不正确的平台运行以及不正确的数据/计算提供商计费。

8.3.3 服务接口

智能办公服务平台和智能办公应用程序之间的接口容易受到以下威胁：

– **未经授权的数据访问：**如果智能办公服务平台和智能办公应用程序之间没有身份验证和授权机制，服务接口可被攻击者篡改以访问服务数据、位置数据和配置文件数据。

– **伪造数据：**如果智能办公服务平台和智能办公应用程序之间没有身份验证和授权机制，服务接口可被攻击者篡改，以伪造服务数据、位置数据和配置文件数据，这种威胁可能会导致对客户的计费不正确。

8.4 平台安全威胁

8.4.1 混合定位技术的脆弱性

定位功能作为平台层的基本功能实体之一，可能需要聚合基于多种无线系统的混合定位技术，如GNSS、RNSS、蓝牙、Wi-Fi、蜂窝网络、超宽带（UWB）。这些混合定位技术的实现涉及信息提取、定位计算和过滤，聚合过程和算法的脆弱性可能产生不准确的定位结果。

8.4.2 能力暴露

智能办公平台将位置和其他服务能力暴露给智能应用程序，未经授权的实体可插入、改变或删除能力使用特权。未经授权的实体可以是人、程序或设备。当攻击者使用劫持连接或恶意发送配置数据的服务能力向现有连接添加数据时，就会发生这些攻击。这可能导致拒绝服务攻击，并允许访问服务数据。

8.5 智能应用安全威胁

8.5.1 未经授权的使用

当未经授权的智能应用程序通过伪装成经授权的实体来获取智能办公平台提供的服务能力时，就会出现这种威胁。

8.5.2 特洛伊木马和病毒注入

当攻击者假冒合法的智能应用程序并向智能应用程序中注入特洛伊木马或病毒时，就会发生这种情况，这将对智能办公平台造成危害，甚至发动进一步的攻击。

8.6 安全威胁与关键利益攸关方的关系

安全威胁和支持位置的智能办公服务的关键利益攸关方之间的关系如表1所示。

在表1中，各单元格中的字母“Y”（Yes（是））表明该关键利益攸关方与某一特定的安全威胁有关。

表1 – 安全威胁与实体的关系

关键利益攸关方 / 威胁	智能办公服务提供商	数据和计算提供商	传感和基础设施提供商	用户
窃取位置数据	Y		Y	Y
篡改位置数据	Y		Y	Y
拦截位置数据报告	Y		Y	Y
未经授权调用位置数据	Y		Y	Y
数据不可用	Y	Y		
泄露行为信息	Y	Y	Y	Y
未经用户同意的定位	Y		Y	Y
嗅探数据	Y		Y	Y
拒绝服务	Y		Y	
信息泄露	Y		Y	Y
未经授权的数据访问	Y	Y	Y	Y
伪造数据	Y	Y	Y	Y
混合定位技术的脆弱性			Y	
能力暴露	Y			
软硬件漏洞			Y	
操纵定位设备			Y	
未经授权的使用	Y			
特洛伊木马和病毒注入	Y			

9 支持位置的智能办公服务的安全性要求

9.1 数据的安全性要求

– R-01：要求智能办公服务提供商、数据和计算提供商以及传感和基础设施提供商提供确保数据（尤其是位置数据）保密性的功能。

– R-02：要求智能办公服务提供商、数据和计算提供商以及传感和基础设施提供商提供确保数据（尤其是位置数据）完整性的功能。

– R-03：要求智能办公服务提供商、数据和计算提供商以及传感和基础设施提供商确保只允许经授权的用户或设备访问数据，特别是位置数据。

– R-04：要求智能办公服务提供商、数据和计算提供商以及传感和基础设施提供商确认实体的身份，防止攻击者试图伪装成经授权的实体。

– R-05：要求智能办公服务提供商提供一种功能，确保只有经过授权的设备或应用程序才能访问办公环境。

– R-06：要求智能办公服务提供商、数据和计算提供商以及传感和基础设施提供商建立合作机制，统一数据格式。

– R-07：要求智能办公服务提供商、数据和计算提供商、传感和基础设施提供商在收集用户的个人数据，特别是位置数据时，必须获得用户的同意授权。用户的同意包括同意提醒、显示和向用户简要说明用户个人数据的收集情况。

对于支持位置的智能办公服务的数据，相应的安全威胁所产生的安全要求如表2所示。

表2 – 与安全威胁相对应的数据安全性要求

安全威胁	安全性要求
位置数据窃听	R-01、R-02、R-03、R-04
位置数据篡改	R-03、R-04
截取位置数据报告	R-03、R-04
未经授权的位置数据调用	R-03、R-04、R-05
不可用数据	R-06
行为信息的披露	R-01、R-03、R-04
未经用户同意的定位	R-07

9.2 设备的安全性要求

– R-08：要求智能办公服务提供商、数据和计算提供商以及遥感和基础设施提供商提供事件响应程序，以发现恶意软件、预先部署安全机制，以便及时响应和处理攻击。

– R-09：要求传感和基础设施提供商确保即使硬件被捕获，攻击者也无法访问数据，包括通过以下方式：

- 使用加密生成的数字签名来验证设备软件的真实性和完整性 [b-ISO/IEC 9796-3]；
- 通过防火墙、入侵检测和入侵防护来控制最终一定会到达设备的流量。

– R-10：要求智能办公服务提供商、数据和计算提供商以及传感和基础设施提供商使用适当的加密算法，以确保数据的保密性，尤其是位置数据的保密性。

– R-11：要求传感和基础设施提供商提供确认实体身份的功能，防止任何攻击者试图伪装成经授权的实体。

对于支持位置的智能办公服务的设备，相应安全威胁所产生的安全性要求如表3所示。

表3 – 与安全威胁相对应的设备安全性要求

安全威胁	安全性要求
硬件和软件的脆弱性	R-08、R-09、R-10
定位设备操作	R-09、R-11,

9.3 接口的安全性要求

– R-12：要求智能办公服务提供商和传感与基础设施提供商提供一种功能，确保只有经授权的用户或设备才能通过接口访问传感与基础设施数据。

– R-13：要求智能办公服务提供商以及传感和基础设施提供商提供一种功能，以确认实体的身份，防止任何攻击者试图伪装成经授权的实体。

– R-14：要求智能办公服务提供商和传感与基础设施提供商提供确保数据（尤其是位置数据）保密的功能。

– R-15：要求智能办公服务提供商和数据与计算提供商提供一项功能，确保只有经授权的用户才能访问服务数据、位置数据和个人资料数据。

– R-16：要求智能办公服务提供商和数据与计算提供商提供一个功能提供商，以确认实体的身份，防止任何攻击者试图伪装成经授权的实体。

– R-17：要求智能办公服务提供商和数据与计算提供商提供确保服务数据、位置数据和配置文件数据完整性的功能。

对于支持位置的智能办公服务的接口，相应安全威胁所产生的安全性要求如表4所示。

表4 – 与安全威胁相对应的接口安全性要求

安全威胁	安全性要求
嗅探数据	R-12、R-13
拒绝服务	R-13
信息泄露	R-13、R-14
未经授权的数据访问	R-15、R-16
伪造数据	R-17

9.4 平台的安全性要求

– R-18：要求传感和基础设施提供商提供检查混合定位算法准确性和完整性的功能。

– R-19：要求智能办公服务提供商提供一种功能，确保只允许经授权的设备或应用程序访问支持位置的智能办公服务。

– R-20：要求智能办公服务提供商提供确认实体身份的功能，防止任何攻击者试图伪装成经授权的实体。

对于支持位置的智能办公服务平台，相应的安全威胁所产生的安全性要求如表5所示。

表5 – 与安全威胁相对应的平台安全性要求

安全威胁	安全性要求
混合定位技术的脆弱性	R-18
能力暴露	R-19、R-20

9.5 智慧应用的安全性要求

– R-21：要求智能办公服务提供商提供一种功能，确保只有经授权的用户或设备才能访问数据，特别是位置数据。

– R-22：要求智能办公服务提供商提供一种功能，确保只有经过授权的设备或应用程序才能访问智能办公服务。

– R-23：要求智能办公服务提供商提供一种功能，确保只有经授权的用户或设备才能访问支持位置的智能办公服务。

– R-24：要求智能办公服务提供商提供一种功能，以提供恶意软件检测的事件响应流程，预先部署安全机制，以便及时应对和处理攻击。

对于支持位置的智能办公服务的智慧应用，相应安全威胁所产生的安全性要求如表6所示。

表6 – 与安全威胁相对应的智慧应用程序的安全性要求

安全威胁	安全性要求
未经授权的使用	R-21、R-22
特洛伊木马和病毒注入	R-23、R-24

10 安全功能

为了满足支持位置的智能办公服务的安全性要求，有若干安全功能，包括但不限于以下内容：

– 数据加密和密钥管理；

– 身份管理和访问控制；

– 完整性验证；

– 安全监控和安全事件响应；

– 用户提醒。

10.1 数据加密和密钥管理

加密和密钥管理是智能办公服务中保护数据机密性的关键机制。加密提供了一种资源保护方法，而密钥管理提供了加密密钥控制。

加密须遵循相关行业标准和政府标准。包括但不限于下列要素：

– 服务流程中动态数据的加密；

– 数据库中静态数据的加密；

– 备份文件中的数据的加密。

密钥管理包括加密密钥的生成、分发、共享、密钥更新和撤销，以实现数据机密性和身份验证。这种管理构成了服务安全性的基础，包括但不限于以下内容：

– **密钥信息保护：**密钥信息须作为敏感数据进行保护，其安全级别应高于其他信息。

– **备份和恢复：**由于潜在事件可导致特定密钥的丢失和服务的停止，因此设置密钥的备份和恢复解决方案是至关重要的。

10.2 身份管理和访问控制

应为智能办公服务的实体提供身份管理，它可为访问控制、授权和审计提供原始数据。

– 它支持身份的全生命周期管理，如注册、角色和权限分配、权限修改和删除。此外，身份注册和修改应该有一个管理员批准程序。

– 它支持实体密码管理，包括基于客户端安全策略的一组实体密码策略，如加密算法、密码长度、密码复杂度和密码更新周期。它能够支持各种类型的密码，如图形密码、基于声音验证的密码等。此外，它还支持密码同步和密码重置功能。

– 身份管理应包括身份账户命名策略和身份账户应用策略。

应提供访问控制来管理实体访问智能办公服务，该服务利用已验证的实体身份或实体能力来确定和实施实体访问特权。访问控制可以拒绝未经授权或不当的访问尝试，并报告它们以生成警报或执行安全审计跟踪。

– 作为实体访问授权的证据的身份验证数据，如密码、占有和后续展示；

– 根据办公场所安全策略制作的安全标签；

– 尝试访问的时间；

– 尝试访问的路由；

– 访问的持续时间；

– 尝试访问的物理位置。

10.3 完整性验证

数据完整性验证有两个级别：

– **单个数据单元或字段级别：**单个数据单元级别的验证涉及两个过程：一个在发送实体端，一个在接收实体端。发送实体给数据添加一个数量，该数量是数据本身的一个函数。接收实体生成一个相应的数量，并与收到的数量进行比较，以确定数据在传输过程中是否被修改了。

– **数据单元流或字段流级别：**数据单元流级别的验证要求增加某种形式的显式排序，例如序列号、时间戳或密码链。

使用预部署机制验证数据格式，并使用加密生成的数字签名机制验证未经篡改的数据，从而进行数据完整性验证。

10.4 使用加密生成的数字签名机制来验证软件和算法完整性 – 监控和安全事件响应

可以向服务管理员提供安全监控，用于检查服务故障和性能。监控包括但不限于以下内容：

– **健康状态监控：**包括收集和显示安全事件日志、漏洞信息、安全设备配置的变更、服务的性能和操作状态。它有助于管理员了解整体的服务健康状态。

– **异常行为检测：**包括非法登录、非法访问和违规访问特定服务，以及对物理设备的异常修改。
– **物理安全监控：**包括温度和湿度观察、闭路电视（CCTV）、门禁、消防系统、空调、供电系统和监视。

安全事件响应处理来自诸如事件处理和管理功能等机制的请求和恢复，并采取恢复行动作为应用一组规则取得的结果。

10.5 用户提醒

用户提醒提供了一种机制，以保证从传感设备收集到的数据将被使用，并已获得支持位置的智能办公服务用户的授权。

关键在于，对于某项需要收集用户数据的支持位置的智能办公服务，服务方要向用户发送提醒信息，显示提醒信息并向用户简要说明。可以提醒用户是否计划收集数据，将收集哪些数据。还将告知用户如何处理和处置这些数据。

10.6 安全功能与安全性要求的关系

表7提供的安全功能可以满足支持位置的智能服务的相应安全性要求。

表7 – 智慧应用程序的安全性要求与安全威胁的对应关系

安全功能	安全性要求	
数据加密和密钥管理	对于数据：R-01	
	设备的安全性要求	R-09、R-10、R-11
	接口的安全性要求	R-14
身份管理和访问控制	数据的安全性要求	R-03、R-04、R-05
	接口的安全性要求	R-12、R-13、R-15、R-16
	平台的安全性要求	R-19、R-20
	智慧应用的安全性要求	R-21、R-22、R-23
完整性验证	数据的安全性要求	R-02、R-06
	接口的安全性要求	R-17
	平台的安全性要求	R-18
安全监控和 安全事件响应	设备的安全性要求	R-08、R-09
	智慧应用的安全性要求	R-24
用户提醒	数据的安全性要求	R-07

参考文献

[b-ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

[b-ISO/IEC 9796-3] ISO/IEC 9796-3:2006, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms.*

ITU-T 建议书系列

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，以及相关联的测量和测试
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
2024年，日内瓦