国 际 电 信 联 盟

ITU-T X.1253

(09/2011)

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

网络空间安全 – 身份管理

身份管理系统的安全指南

ITU-T X.1253 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
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

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1253 建议书

身份管理系统的安全指南

摘要

ITU-T X.1253建议书为身份管理（IdM）系统提出了安全指南。安全指南介绍了应如何部署IdM系统并在NGN（下一代网络）或网络空间安全中用于安全身份识别业务。安全指南侧重于提供有关如何利用各种安全机制保护通用IdM系统的建议，同时提供在两个IdM系统互操作时所需要的安全程序。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1253	2011-09-02	17

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.1253 建议书

身份管理系统的安全指南

1 范围

本建议书的范围如下：

- 通用IdM系统模型和服务
- 有关IdM系统的安全威胁和风险
- 部署IdM系统的安全指南
- 运行IdM系统的安全指南
- IdM系统中的隐私考虑

本建议书的范围主要侧重于多域身份管理业务。然而，该指南亦适用于集中身份管理系统。

注 – 上述指南的实施和使用须符合所有现行国家和区域法律、规定和政策。一些具体的指南和法规可能需要实施保护个人可识别信息的机制。

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和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。

[ITU-T X.1205] ITU-T X.1205建议书，网络安全概述。

[ITU-T X.1252] TU-T X.1252建议书，基线身份管理术语和定义。

3 术语和定义

3.1 其它地方定义的术语

本建议书使用以下其它地方定义的术语：

3.1.1 接入控制[ITU-T X.1252]：用来确定一实体是否应按照预先确定的规则和请求方的具体权利或相关授权被授予获得资源、设施、服务或信息的程序。

3.1.2 属性[ITU-T X.1252]：针对一实体并说明该实体特性的信息。

3.1.3 （实体）认证[ITU-T X.1252]：对实体与所介绍身份之间关联性实现充足信任的过程。

3.1.4 证书[ITU-T X.1252]：作为被声称的身份和/或权利的证明的一组数据。

3.1.5 身份[ITU-T X.1252]：以一个或多个信息元素表示一实体，使实体足以在语境内得到区分。在IdM中，术语身份被理解为语境下的身份（属性子集）即，属性的多样性受限于实体存在和互动的边界条件（语境）框架。

注 – 各实体通过一个综合身份表示，它包括所有描述这类实体（属性）的可能信息元素。然而，这种综合身份是一个理论问题，不包括任何描述和实用情况，因为可能的属性数量是无限的。

3.1.6 身份管理[ITU-T X.1252]：一系列功能和能力（如管理、管理和维护、发现、通信交换、关联和绑定，政策执行、认证和维护等），用于：

- 保证身份信息（如标识符、证书、属性）
- 保证实体（如，用户/订户、人群、用户设备、组织、网络和服务提供方、网络元素和对象及虚拟对象）
- 支持商业和安全应用。

3.1.7 用户[ITU-T X.1252]：使用如系统、设备、终端、流程、应用或公司网络等资源的实体。

3.1.8 以用户为中心[ITU-T X.1252]：身份管理（IdM）系统提供用户控制和执行各种不同隐私和安全政策能力，这些政策管理诸如用户个人可识别信息（PII）的实体间身份信息交换。

3.2 本建议书定义的术语

本建议书定义了以下术语：

3.2.1 实体：单独和独立存在的任何事物，可在语境内识别。

注 – 实体可以为真人、动物、法定人、组织、主动或被动之物、设备、软件应用、服务等或上述个体的组合。在电信中，实体的例子包括接入点、订户、用户、网源、网络、软件应用、服务和设备、接口等。

3.2.2 IdM客户机：与IdM服务器互动以检索身份信息的客户程序。

3.2.3 IdM服务器：管理用户身份生命周期的服务器。

3.2.4 移动IdM客户机：安装并用于移动设备的IdM客户机。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

DB 数据库

DoS 服务拒绝

FDDI 光纤分布数据接口

IdM 身份管理

IdP 身份提供方

IDS 入侵检测系统

IPS 入侵防范系统

LAN 局域网

NGN 下一代网络

OS 操作系统

PII 个人可识别信息

PIN 个人识别号码

PKI 公共密钥

SP 服务提供商

SSL 安全套接层

TTP 可信赖第三方

VPN 虚拟专用网

5 惯例

无。

6 背景

在过去十年间，IdM（身份管理）系统已从一个独立的系统发展成为联合式或以用户为中心的IdM系统。目前开发的多数IdM系统侧重于如何高效便捷地提供与身份相关的服务。很多最近开发的IdM系统为提供安全和隐私保护做出了一些努力。

早些时候，IdM系统是在企业范围内作为一个独立模型开发的。在此情况下，每个IdM系统与其它系统无关，因此无法共享用户的身份信息以便在不同域中提供有益服务。此外，一个用户的身份可在不同的IdM系统中加以复制。这使系统管理难以安全和有效地管理用户的身份。

下一步是收集一个IdM系统中的所有用户身份并在需要时予以分发。这种方法被称为集中化模型。在此模型中，有关一个用户的过多信息集中在一个服务器上。这种方法有很多不利之处，因为IdP不仅会成为单一故障点，同时会失去各方信任。

下一种方式是使每个IdP管理自己的身份并将责任分散到用户可选择的多个IdP中。这种方法被称为联合式模型。在此模型中，用户可信赖的IdP不止一个，这些IdP在必要时可以管理用户的部分身份信息。每个IdP中有关用户的身份信息可通过使用所谓联合身份的假名加以共享。这种模型避免了单点故障问题。

随着用户隐私变得越来越重要，IdM技术侧重于用户对其身份信息的全面掌控。这种方式称为以用户为中心的模型。在此模型中，身份信息在两个IdP共享用户身份信息时，必须在一个用户向另一个用户提供应用此隐私政策的情况下才能传送身份信息。这种模型已被多个产品采用并利用了其它现有IdM技术。

这些IdM系统的融合面临的一项挑战就是，如何保证融合系统的安全性并在提供最佳性能的情况下平衡安全与隐私。此外，目前提供的多数安全指南往往侧重于身份提供方和依赖方。随着用户安全和隐私称为强制性要求，有必要考虑IdM系统安全中的以用户为中心内容，从而反映出人们对用户隐私的日益关注。

7 身份管理系统概况

7.1 IdM系统的一般性模型

7.1.1 以应用为中心的IdM系统

在大型IdM系统中，以应用为中心的IdM系统意味着，身份服务和政策旨在满足身份提供方和依赖方的要求并为达到应用要求而得到优化，举例而言，提供用户账户信息。在此以应用为中心的IdM系统中存在一个身份提供方和一个依赖方。当为用户提供身份服务时，身份交换往往在两个实体间进行。从传统而言，身份和接入管理技术主要侧重于认真采用联合方式接入应用和服务的最终用户。因此，安全要求局限于应用域的外围。

7.1.2 以用户为中心的IdM系统

以用户为中心的IdM主要侧重于最终用户并为满足最终用户的要求而得到优化。这意味着，IdM系统的主要目标是为用户提供方便而全面的身份服务。其主要功能是使用户对其身份进行全面掌控。当用户身份信息得到传播时，必须通过用户明确给予另一用户加强个人政策的机会。在以用户为中心的IdM系统中，用户计算环境中必须安装客户端程序。因此，指导用户安全安装并部署任何相关软件需要简便易行的全面安全指南。该软件必须管理用户有关安全的信息。

以用户为中心的系统与其它IdM模型不同，它强调的是，必须由用户，而不是一些管理机构掌握用户身份属性创建、分发、更新和中止的控制。这意味着，用户对其身份的整个生命周期具有全面掌控。控制的水平由用户隐私要求确定。

7.2 身份服务

7.2.1 身份生命周期管理

该服务管理已创建、颁发、更新和中止的身份。与该服务相关的数据存储在服务器或本地机器的数据库中。因此，对该数据库的接入仅限于授权用户。

7.2.2 认证

认证服务旨在确认要求接入系统或资源的合法使用者或实体。认证是IdM系统为依赖方提供的一项关键业务。应不惜一切代价防止密码破译和伪装攻击。

7.2.3 授权

授权服务旨在处理有关用户接入权的决定，同时按照用户获得的特权加强授权决定。此项服务是保护身份系统免于非授权接入和使用必须具备的。

7.2.4 属性交换

此项服务提供属性交换和同步。这是最重要的安全服务之一，因为属性是通过通信网交换的。随着通信媒体从有线到无线的变化，需要不同水平的安全机制。

7.2.5 安全令牌

安全令牌服务是实体之间分享安全或身份信息必不可少的。安全令牌通常得到安全和加密机制的保护，因为它永远包含高度保密性信息，不得泄露。

8 IdM系统中的安全风险

网络空间中出现的多数安全风险亦可能出现在IdM系统中，因为这些系统运行在网络空间。网络空间的一般安全威胁见[ITU-T X.1205]中的描述。

在IdM系统中，很多安全威胁会使系统变得不堪一击或使安全水平下降，从而致使组织置于重大危险之中。

8.1 系统安全

一般来说，系统安全涉及对用户硬件和数据的保护。保护的目的是确保仅有授权用户和为了所有者希望的目的才能接入硬件。此外，该系统应具有其它用途。攻击者应不能剥夺资源合法用户的权利。

8.1.1 非授权接入和使用

非授权用户不得接入和使用多数系统。IdM系统应严格防止此类安全漏洞，因为任何对IdM系统身份的非授权接入都可导致安全威胁，如身份盗窃和伪装攻击。

8.1.2 不适当的使用

不适当的使用意味着，用户可利用IdM系统处理或完成不同于本意的某项工作。授权用户在没有适当特权的情况下使用IdM系统应具有一定的局限性。一些服务仅限于授权用户，一些限于专门用户，而其它一些服务则禁止除网管外其他用户使用。

8.1.3 服务拒绝

一般情况下，IdM系统是用户访问并使用应用服务的第一入口。因此，IdM系统很容易成为停止服务提供的首要攻击目标。使IdM系统拒绝服务的攻击多种多样。拒绝服务攻击通常容易操作但难以停止。很多这类攻击旨在消耗大量计算资源，从而难以或无法为合法用户提供服务。

8.2 被动安全威胁

在被动安全威胁中，攻击者将数据包读出网络，但不写入。实施这种攻击最简单的方法是与受害者处在相同的局域网中。在包括以太网、802.3和FDDI等通用局域网配置中，所有在线机器均可在相同局域网上读到针对任何其它机器的流量。

无线电通信信道值得特别关注。随着无线局域网（如使用802.11的局域网）的普及，这一点尤其重要。由于数据是在众所周知的无线频率上广播的，攻击者只需接收这些发射就可发动攻击。这些信道尤其容易受到被动攻击。尽管很多这种信道增加了加密保护，通常这些加密技术在使用时没有适当配置。

8.2.1 保密性违规

保密性攻击就是对通信线路中私密转换或通信的破坏。在互联网中，很多情况下，保密信息是以透明形式传送的。任何通过该攻击获得的证书可重复使用于未来的攻击。

8.2.2 密码截取

密码截取是对网络中传送的用户密码的收集以便获得对资源的非授权使用。可读到这些流量的攻击者因此捕获了密码并重新使用密码。换言之，攻击者可启动与IdM系统的连接，从而盗窃用户的身份信息。

8.3 主动安全威胁

当攻击涉及向网络或系统写数据时，我们将这种攻击称为主动攻击。主动攻击是对计算机网络的入侵，从而删除或修改存储于作为该网络一部分的IdM系统中的数据。这是最严重的攻击形式之一，因为很多公司的运行主要依赖于数据。

8.3.1 重复攻击

在此攻击中，攻击者在脱机状态下记录了消息序列并对最早接收这些消息的相应一方加以回放。请注意，攻击者不需要了解这些消息，而只需要捕获并重新发送这些消息。

8.3.2 中间人攻击

攻击者扭转通信流方向，从而将发送者变为接收者，而接收者变为发送者。这种攻击非常严重，因为它对发送者和接收者均进行了伪装。因此，很多提供通信流完整性的技术都无法防止中间人攻击。当协议缺少对等实体认证时，就可能出现中间人攻击。

8.4 与IdM系统相关的安全威胁

这些威胁特别涉及IdM系统。以下列出的威胁是任何IdM系统均应提供保护措施加以应对的主要安全漏洞。

8.4.1 有关密码的威胁

有关密码的威胁之一源于无力密码的使用。如用户选择一个无力密码 – 可猜到的密码 – 用于认证，该密码则可能受到词汇攻击。当用户使用相同的无力密码在不同网站登录时可能引发另一问题。在此情况下，安全力度较差的网站可能受到攻击，从而显示用户密码，攻击者只需使用盗窃的密码就可登录其它网站。

另一个威胁是通过计算机中的间谍软件截取密码。计算机可能会被截获用户或网管密码的间谍软件所感染。

8.4.2 非授权接入

非授权接入可指多种不同攻击。攻击的最终目标是争取非法接入一些资源[ITU-T X.1205]。

提供认证和身份服务的IdM系统必须提供给所有需要使用用户身份提供应用服务的各方。因此，为保护系统免受非授权接入需要细微的接入控制机制。

8.4.3 窃听

窃听是一种难以发现的威胁。实施此类攻击的目的在于听取企业局域网的信息，并最准确地记录其原始数据。攻击者采用市场上销售的现成“混杂模式”以太网适配器展开攻击。通过该模式，攻击者可以在网络上获取每一个数据包。如今攻击者可以通过诸多免费的网络嗅探程序来实施窃听[ITU-T X.1205]。

IdM系统通常与用户和其它实体沟通以便使用有线或无线网络分享通常保密的证书和身份信息。因此，通过窃听获取的任何信息均可导致身份盗窃。

8.4.4 钓鱼

这是第三方通过模仿或假冒具体而通常知名的品牌从个人、小组或组织中收集秘密信息从而获得经济收益的做法。攻击者企图欺骗用户披露个人数据，如信用卡号码、在线银行证书和其它敏感信息，攻击者之后可使用这些信息从事不法行为。钓鱼网站旨在模仿一组织的合法网站。该组织的品牌被冒充。在IdM系统中，钓鱼是一个严重的威胁，因为， 攻击者获得的受害者的认证信息或其它个人可识别信息可用于身份盗窃或其它欺诈行为。

8.4.5 身份盗窃

对于存储和管理大量个人身份信息的组织而言面临一项高风险安全问题。安全漏洞不仅可以导致个人数据的丢失，从而降低客户和机构信息，同时还能对组织的声誉造成严重伤害。数据损坏也能给各组织带来经济代价。

9 IdM系统的安全指南

安全指南第9.1和9.2节规定了如何在部署和操作一般性IdM系统时管理安全。这些指南为在各种计算环境下安全部署和操作IdM系统提供了基本安全要求。第9.3、9.4和9.5节涉及包括IdM服务器、客户机和移动客户机在内的IdM系统实体。第9.6节描述了IdM系统的隐私考虑。

9.1 部署IdM系统的安全指南

该条款提供了IdM系统安装和部署的安全指南。在多数情况下，为信任和密钥管理做好准备是一个重要的问题。

9.1.1 信任管理

使用IdM系统做出的每项授权取决于对实体及其属性真实性和正确性的信任。因此，身份只有在授权时才发挥作用。授权是以信任为基础提供的。信任管理计划是成功部署和操作IdM系统的第一步。

PKI（公共密钥）是身份管理系统的基本信任机制。PKI的主要目的是提供可用来认证并做为安全通道的公共密钥证明。在大型IdM系统中，我们大力提倡使用PKI建立TTP（信任第三方）。由PKI颁发的这一证书可用来证明IdM系统的用户并为SSL中的通信信道提供加密。数字签名是该证书的另一项关键应用。

9.1.2 网络安全

使用各种手段确保网络安全是一项必不可少的要求。首先，网络外围应使用防火墙确保安全。任何IdM系统必须安放在防火墙以内。此外，诸如VPN和IDS/IPS等更复杂的网络安全机制也可用来提供更安全的网络环境。

9.1.3 安全托管环境

托管环境是安装和操作IdM系统的地方。在安装IdM系统组件的服务器或工作站中，需要在IdM系统安装前首先安装防病毒程序和键盘保护程序。必须保证托管环境在IdM系统安装和部署前不会受到任何安全攻击的破坏。

9.1.4 安全存储

很多重要和敏感的数据存储在数据库或目录服务器等存储器中。在设置时，存储服务器应安装在安全的计算机上，同时按照适当的安装指南建立管理员账户，以避免任何可用来破坏系统的不良账户的建立。

9.2 运行IdM系统的安全指南

该条款为运行IdM系统提供安全指南。认证和接入控制是需要处理的主要问题之一。

9.2.1 数字签名

数字签名是可确保所签署的消息的真实性和完整性的安全机制。在IdM系统中，用户经常需要表明其意愿或对某些数字交易的认同。在此情况下，数字签名可用做证明这一真实性的证据。

9.2.2 加密

IdM系统需要在各个操作层面加密。首先，在具有保密性要求的情况下，实体之间交换的信息需要加密。根据IdM操作政策的不同，为确保保密性和防止非授权接入，需要对存储在数据库中的一些数据加密。加密可以为IdM系统提供最大保密性，最终确保用户的隐私及其安全信息的安全。

9.2.3 认证

认证是防止非法用户在非授权的情况下进入系统的一个门户功能。在互联网中，广泛使用身份id/密码认证，但这种做法从安全角度而言存在很多不足。因此，建议在确保系统用户保持高度信心的情况下，使用强有力的认证。如使用相互认证就可缓解钓鱼和嫁接攻击。

9.2.4 安全通信

多数用户和IdM系统之间的信息交换涉及隐私并具有保密性质。此外，实体之间的协议信息可能承载需要在通信线路上加密的敏感和保密信息。使用现有的诸如SSL和VPN等技术就可以实现安全通信。

9.2.5 接入控制

网管和用户等各种实体可以接入IdM系统以便获得某种服务和日常维护。为防止系统不受第三方恶意侵入，需要适当的接入控制机制。在多数情况下，简便易行的接入控制（即接入控制清单）模型就足以解决问题。然而，由于基于角色的接入控制模型可以提供更加严密和细微的控制，在需要更加安全和灵活的接入控制模型的情况下，可以使用这种模型。

9.3 有关IdM服务器的安全指南

该条款为大型工作站和服务器中安装和操作的IdM服务器提供了安全指南。

9.3.1 安全保证和操作系统

多数普遍使用的IdM服务器在通用OS（操作系统）上工作。如IdM服务器使用的操作系统得到适当配置，可以避免多数安全问题。由于IdM服务器安装在现有操作系统上，其安全在多数情况下取决于操作系统。保障不同操作系统安全的技术多种多样，因此，该条款包涵确保多数操作系统安全的通用程序。更加具体的操作系统的安全管理见[ITU-T X.1205]和[b-NIST SP 800-123]中。

为确保IdM服务器的安全，有必要采取以下基本措施以确保操作系统安全：

- 为操作系统提供补丁和更新；
- 硬化并配制操作系统以充分解决安全问题；
- 必要时安装并配置更多的安全控制；
- 检测操作系统的安全性以确保上述措施彻底解决所有安全问题。

9.3.2 配置用户认证

对于IdM服务器，可配置服务器的授权用户应局限于少量指定服务器网管人员。在有必要执行政策限制时，服务器网管应对服务器加以配置，从而通过要求用户得到这种接入授权的证明对用户给予认证。对于需要提供高度保密性和信任度的IdM服务器，各组织可使用防破坏认证硬件，如硬盘或一次性密码装置。在此情况下，重复使用认证信息（如密码）并通过不受信赖网络传送文本的认证机制是不可行的，因为，有关信息可能被伪装成授权用户的攻击者截获和使用。

操作系统的默认配置通常包含使用或不使用密码的客户账户。网管应取消或停止不用的客户账户，以防止攻击者的使用。

9.3.3 配置接入控制

多数IdM服务器提供确定有关证书各项接入权利、身份信息和能力。接入IdM服务器的用户不得获取其他用户的身份信息。对接入控制的适当设定有助于防止并非针对公众传播的敏感或限制性身份信息的披露。此外，接入控制可用来在出现针对服务器的DOS（服务拒绝）时限制资源使用。

9.3.4 登录

登录是良好的安全措施的必要组成部分。登录日志必须获得正确的数据，之后受到密切监测。网络和系统登录均很重要，在加密通信中系统登录尤其重要，在此情况下，网络监测不太有效。

审议登录日志是发现可疑行为的强制有效手段。在多数情况下，登录文件只作为可疑行为的记录。建立登录信息的适当机制可以使登录日志检测成功和未遂入侵尝试，并在需要进一步调查时启动报警机制。处理和分析日志文件并审议告警通知需要制定程序和工具。

必须保证，接入控制能够加强责任分工，确保服务器日志不被服务器网管修改并确保服务器程序仅用于登录文件。

9.4 有关IdM客户机的安全指南

在操作IdM客户机程序时，该条款可提供安全指南。当网络浏览器作为IdM客户机时，安全强度取决于浏览器本身。然而，仍可通过遵循该指南确保客户机环境的安全性。

9.4.1 客户机程序的安全分布

目前，依赖于浏览器的插件多数是从万维网上下载的。如果客户无意间下载了可能破坏用户系统的IdM客户程序，任何有利的安全机制都无法防止客户受到该恶意活动的影响。因此，IdM客户程序的提供方必须确保所发布的客户程序得到整体保护并为认证其完整性提供安全的方式。

9.4.2 客户程序的完整性

为提供客户程序的完整性，数字签名是一项关键的解决方案。如果客户程序得到提供方的签名，而且为认证提供了签名证书，用户可安全地下载并认证程序代码的完整性。另一种方法是使用哈希算法确保代码的完整性。客户代码是哈希算法产生输出值的输入，即客户代码的压缩，如，哈希值以安全的方式公布在万维网上，用户可以通过计算已下载的客户程序的哈希值确认其客户程序。然而，前者比后者更加安全。

9.4.3 客户DB文件

客户DB（数据库）文件应得到安全存储。对DB的接入应严格局限于认证用户。在多数情况下，IdM客户机管理包括密码和安全令牌在内的证书信息。这些信息应在加密的形式下得到保管。此外，DB文件本身应受到保护，免受非法更改和替换。当DB文件从系统中取消时，硬盘中应不存任何可以用来日后恢复的痕迹。

9.4.4 安全密码

多数安全机制最终取决于接入系统的认证密码。如用户使用可被强有力的攻击击破的无力密码，没有其它安全机制可以防止系统受到恶意用户的攻击。因此，IdM服务提供方最重要的任务就是确保用户登录时使用有力的密码。

9.4.5 卸载客户程序

当卸载用户系统中的客户程序时，所有密码、证书和身份信息均应永久消除，同时还应删除个人对客户程序的配置。

9.5 有关移动IdM客户机的安全指南

该条款为移动IdM客户机提供安全指南。移动IdM客户机安装并运行于移动设备中。移动设备具有便携性和移动性等专有特点。然而，这些特点在遇到攻击时将成为安全隐患。

9.5.1 设备丢失或被盗

由于移动设备具有便携性，因此很可能丢失或被盗。进入移动设备提取用于身份盗窃的个人信息的方式多种多样。因此，移动设备中移动客户机应为可能造成非授权使用或身份盗窃的各种安全攻击做好准备。当该设备被盗或丢失时，应将事件报告给移动通信提供方。运营商可根据情况远程锁住设备，以防止对设备的任何接入。当设备丢失在家里或工作场所等熟悉环境时，这种方法是适当的。在其它情况下，如设备所有者认为该设备将永久丢失或不可能找回该设备的情况下，运营商应能删除设备中存储的个人信息和身份记录。

9.5.2 设备认证

如移动设备的输入显示器很小，用户很难每次使用由字母数字组成的密码登录，PIN（个人身份号码）被用于密码，但在很多情况下的使用并非为了方便。为解决这种问题，IdM的移动客户机应提供适用于移动设备的方便用户且确保安全的认证机制。移动客户机必须在该设备不使用任何用户登录认证机制的情况下执行密码的认证。

9.5.3 数据库备份

多数身份信息在很多业务中是在移动设备中收集处理的。然而，很多这些身份信息是敏感的个人隐私信息，因此，有必要保护其完整性和保密性。如上所述，移动设备容易丢失或被盗。因此，IdM的移动客户机应提供备份身份信息数据库的方式。可行的做法有两种。第一种方法是在二级存储如（安全数字存储卡）中备份数据库。第二种方法是使用外部备份服务器为客户机提供数据库备份服务。在此情况中，用户数据库即使在设备丢失或被盗的情况下，也可永远得到存储。

9.5.4 移动通信安全性

在多数情况下，移动设备使用移动通信与其它设备沟通。然而，人们认识到，移动通信非常容易受到主动和被动攻击。IdM移动客户机通常通过移动链路传送敏感个人信息。因此，任何使用移动链路的移动客户机通信都需要为保障完整性和保密性得到传输层安全性能的保护。

9.6 IdM系统的隐私考虑

隐私是IdM安全中的一个重要问题，然而，在隐私保护指南的实施上，各国的规定五花八门。此条款探讨并提供了一些有关IdM系统的隐私问题。

9.6.1 用户的认可

在收集用户身份并于IDP或SP时，应明确得到用户认可，最好能够通过数字签名得到用户认可。在出现问题时，该签名可得到确认。

9.6.2 身份选择

IdM系统为个人是否选择允许收集、使用、传送、存储、存档或处理身份提供了明确方式。用户隐私由此得到进一步保护，因为用户可以管理身份和隐私政策。这种以用户为中心的方式应在IdM系统设计阶段得到考虑。

9.6.3 身份的目的

IdM系统应以可理解的方式在收集身份前将收集和使用个人信息的所有目的告之用户。此外，系统应为按照上述目的使用身份而做出适当的努力。

9.6.4 身份限制和压缩

收集身份的IdM系统应只为满足有关目的收集身份信息，个人认同或法律允许或要求的身份信息除外。

收集身份的IdM系统应认真考虑并记载明确指出需要哪些身份信息以及如何确保所有身份信息处理仅涉及最少必要的身份信息的程序。

9.6.5 身份的清理

IdM系统应在实现所述目标以及法律和规则无需更长久保留身份的情况下清理身份。在清理身份时，IdM系统应确保所有存储在相关系统（如备份和存档系统）中的身份亦被删除。

9.6.6 隐私政策的设立

在IdM系统运行之前，必须建立个人喜好和个人授权等隐私政策。该政策涉及用户提交给系统的身份信息的使用。

9.6.7 匿名性

匿名性是实现增强型隐私保护的IdM系统的最终目标，然而，以合理的成本提供这项功能是非常困难和复杂的。因此，在多数情况下，可为满足IdM系统的隐私保护要求提供伪匿名性。

参考资料

[b-NIST SP 800-123] Scarfone, K.A., Jansen, W., and Miles, T. (2008), *Guide to General Server Security*, NIST Special Publication SP-800-123.

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	电缆和外部设备其它组件的结构、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、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2012年，日内瓦