

国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1251

(09/2009)

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

数字身份的用户控制框架

ITU-T X.1251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
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

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T X.1251建议书

数字身份的用户控制框架

摘要

ITU-T X.1251建议书规定了增强用户控制和交换数字身份相关信息的框架。本建议书也规定了数字身份信息交换的用户和功能要求。其工作包括向用户提供控制发布个人可识别信息的能力。

来源

ITU-T 第17研究组（2009-2012）按照WTSA第1号决议规定的程序，于2009年9月25日批准了ITU-T X.1251建议书。

关键词

数字合同、数字身份、数字身份客户机、身份、身份互换、身份管理、身份服务器。

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，国际电联已经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/>。

© 国际电联 2010

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

	页码
1 范围	1
2 参考文献	1
3 术语和定义	1
3.1 其他文献规定的术语	1
3.2 本建议书规定的术语	2
4 缩写词和首字母缩略语	3
5 惯例	3
6 总体能力	4
6.1 用户能力	4
6.2 功能能力	4
6.3 安全指南	5
7 增强数字身份互换的用户控制	5
7.1 引言	5
7.2 安全威胁	6
7.3 用于数字身份互换的概念模型	6
7.4 数字合同	8
7.5 用于身份互换的三个层	9
8 数字身份互换框架	10
8.1 设计原则	10
8.2 框架构成	11
I.1 引言	14
I.2 背景	14
I.3 DIIF能力	15
参考资料	18

数字身份的用户控制框架

1 范围

本建议书规定了增强用户控制和交换数字身份相关信息的框架。

本建议书也规定了数字身份信息交换的能力。其工作包括向用户提供控制发布个人可识别信息的能力。

注 – 在本建议书中，使用与IdM相关的术语“身份”不表明它的绝对含义，尤其是不构成任何对个人的肯定验证。

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考文献的最新版本。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。

[ITU-T X.1205] ITU-T X.1205建议书（2008年），《网络安全综述》。

[ITU-T X.1250] ITU-T X.1250建议书（2009年），《增强的全球身份管理和互操作性的基本能力》。

3 术语和定义

3.1 其他文献规定的术语

本建议书使用其他文献规定的下列术语。

3.1.1 credential 证书[b-ITU-T X.1252]: 提供声明身份和/或权利证明的一组数据。

3.1.2 entity 实体[b-ITU-T X.1252]: 是单独明确地存在且能在环境中被识别的任何事物。

注 – 一个实体可能是一个物理的个体、动物、法人、组织、有源或无源的事物、设备、软件应用、服务等或是这些个体的组合。在电信环境中，实体的例子包括接入点、订户、用户、网络单元、网络、软件应用、服务和设备、接口等。

3.1.3 federation 联邦[b-ITU-T X.1252]: 由用户、服务提供商和身份服务提供商构成的联合体。

3.1.4 identifier 标识符[b-ITU-T X.1252]: 在某个环境内，用于识别某个实体的一种或多种属性。

¹ 根据某些国家本国的法律，本建议书可能不适用。

3.1.5 identity 身份 [b-ITU-T X.1252]: 以一个或多个信元的形式表示一个实体，使其在某一环境下被充分区分开来。出于IdM的目的，把术语“身份”理解成环境身份（属性子集），即属性的种类受某个框架的限制，该框架对于实体存在和交互条件有规定的边界条件（环境）。

注 – 每一个实体由一个整体身份代表，包括表示该实体特性的所有可能信元（属性）。然而，由于所有可能的属性种类是不确定的，因此该整体身份只是一个理论问题，而不包括任何具体描述和实际应用。

3.1.6 identity management 身份管理 [b-ITU-T Y.2720]: 是用于以下目的的一系列功能和能力（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）：

- 保证身份信息（如标识符、证书、属性）；
- 保证实体（如用户/订户、组、用户设备、机构、网络和服务提供商、网络单元和物件、虚拟物）身份；以及
- 实现业务和安全应用。

3.1.7 identity service provider (IdSP) 身份服务提供商 [b-ITU-T X.1252]: 验证、维护和管理，并可以创建和指配其他实体的身份信息的一个实体。

3.1.8 personally identifiable information (PII) 个人可识别信息 [b-ITU-T Y.2720]: 与活着的个人相关、可能用于识别该个体的信息（包括这样的信息，即使它不能单独明确地识别某个人，但与其他信息结合起来就能够识别的情况）。

3.1.9 relying party 依赖方 [b-ITU-T Y.2720]: 在某些请求的环境中，依赖于请求/断言实体提供身份特征或声称的实体。

3.1.10 user 用户 [b-ITU-T X.1252]: 任何使用了某种资源的实体，例如系统、设备、终端、程序、应用或企业网。

3.1.11 user-centric 以用户为中心 [b-ITU-T X.1252]: 在对实体间身份信息（包括PII）交换进行管理时，为(IdM)用户控制和执行各类隐私和安全政策提供能力的一个IdM系统。

3.2 本建议书规定的术语

本建议书规定下列术语：

3.2.1 circle of trust 信任圈: 为加入一个协会内组织而建立的一套标准，该协会的目的是为能可靠地使用相互的资源。请注意，信任圈也是加入一个联盟内组织的最终结果。

3.2.2 digital contract 数字合同: 以数字形式订立的协议，并由获得协议的双方实体签署。

3.2.3 digital identity 数字身份: 有关特定个人、团体或组织的信息的数字表现形式。

3.2.4 digital identity client 数字身份客户机: 是为用户提供认证和证书管理、身份互换和隐私保护服务的一个客户机程序。

3.2.5 identity fraud 身份欺诈: 冒名顶替者获得个人可识别信息（PII）的关键部分，例如社会安全号码和驾驶执照号码，并使用这些信息用于牟取自己个人的利益的一种犯罪行为。

3.2.6 identity information 身份信息: 识别一个用户（包括可信的（网络产生的）和/或不可信（用户产生的）地址）的信息。

3.2.7 identity interchange 身份互换: 身份服务提供商与依赖方之间通过数字身份客户机传送用户身份信息的过程。

3.2.8 identity selector 身份选择器: 通过用户控制并分发他/她的数字身份, 用户可使用的数字身份客户机中的软件组件。

3.2.9 identity server 身份服务器: 管理用户证书和身份信息并把该信息提供给数字身份客户机的服务器。

3.2.10 identity synchronization 身份同步: 当身份服务提供商中身份信息来源改变时对传递给依赖方的用户身份信息进行更新的过程。

3.2.11 identity termination 身份终止: 当存储的用户身份信息有效期满时将其删除的过程。

3.2.12 identity token 身份认证令牌: 数字身份的数据模型, 其中可包含用户PII和证书信息。

3.2.13 phishing 网络钓鱼: 在电子通信中, 通过伪装成一个可信任的实体, 试图获得例如用户名、密码和信用卡细节等敏感信息的犯罪欺诈过程。

3.2.14 privacy policy 隐私政策: 规定个人隐私信息获取和传播保护规则的政策声明。

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:

CoT	信任圈
DIC	数字身份客户机
DIIF	数字身份互换框架
IdM	身份管理
IdS	身份服务器
IdSP	身份服务提供商
PII	个人可识别信息
PKI	公共密钥基础设施
RP	依赖方
SP	服务提供商
XML	可扩展标记语言

5 惯例

无。

6 总体能力

本建议书规定了以下一些能力。除非标明为可选的能力，否则以下这些用户部分和功能部分规定的要求均为强制性的。

6.1 用户能力

要求该框架满足以下用户能力：

- 1) 支持相互认证机制。
- 2) 提供给用户与数字身份客户机（IDC）一致的认证接口以支持不同的认证机制。
- 3) 提供给用户身份选择器，以允许用户选择认证要使用的证书。对用于认证的证书的选择可能也受到一些网站要求的限制。为方便起见，对认证方法和相关证书的选择也可委托给身份服务提供商（用户仅选择身份服务提供商而非该身份服务提供商认证所使用的特定证书的可能性）。
- 4) 提供给用户直观一致的接口以最安全地管理其证书信息。
- 5) 支持网站的自动填写登记或订阅，以使用户与网站的互动最小，包括用户对这样机制的激活和去激活的完全控制。这是可选的。
- 6) 在用户需要的任何时候提供身份信息的共享，并允许用户在适当的隐私保护机制下完全控制身份互换。
- 7) 当在用户的完全控制下改变了原始资料时，要提供给用户共享身份信息的自动更新。
- 8) 提供给用户能力，使其能完全控制安全政策和隐私政策的建立过程，以及在共享身份信息之前如何控制身份互换的实施，以使用户可以直接影响到政策的控制和执行。
- 9) 提供给用户能力，使其能查看与各实体共享的身份信息的详情。
- 10) 支持认证会话管理能力，以避免用户为登录网站而通过一个身份服务提供商进行系统性地重新认证。

6.2 功能能力

用于数字身份互换框架的功能能力规定如下。要求这些功能能力提供数字身份互换框架所需的最小功能。

- 1) 支持综合证书管理，能够管理用户的认证证书信息。
- 2) 支持身份互换链路管理，给用户提供全方位的角度，查看用户身份互换时和哪些实体联系。
- 3) 支持多种认证机制，可能包括密码认证、PKI认证和生物测定认证。
- 4) 支持能提供双向链路的身份互换机制，以使用DIC在实体之间共享用户的身份信息。
- 5) 支持数字合同机制，为身份互换建立一个协议，执行发布PII的安全和隐私政策。

- 6) 支持身份信息同步以便在传播的身份信息来源改变时，相应地更新发布的和共享的身份信息。需保持同步的身份信息仅限于用户直接修改的PII。
- 7) 建议要支持普遍令牌转换，使该框架可与现有的身份管理系统共同使用。
- 8) 尽可能确保该框架对于认证过程的不确定性，以避免DIC和身份服务提供商支持的认证机制之间的相关性（或至少使该框架易于支持所有认证机制，特别是电信运营商的特定机制）。
- 9) 所支持的机制使身份服务提供商能在认证过程中与用户进行互动，并可能提供自己的认证界面（图形用户界面（GUI））。
- 10) 支持在各种媒体（USB接收器、SIM卡、网络存储服务等）以明确界定的存储层存储可供DIC使用的身份令牌。

6.3 安全指南

为了开发安全可靠的DIIF，建议的安全指南如下所示：

- DIIF通信安全取决于基本信任模型，一般是基于关键管理基础设施上（例如，PKI或密钥）。
- 建议使用传输层安全协议的有些形式，当通过网络传输消息时，这些形式应当用于提供数据完整性和保密性（例如，加密技术）。
- 各方应当数字签署数字合同以达成一致；如果必要，可以加密作为一个选项。
- 存储在DIC中的包括身份信息的数据在进行存储时，应当进行数字签署和加密。
- 鉴于允许用户将其身份令牌由一台设备移至另一台设备，因此制定一项政策以保证数据在传输过程中的安全性。

7 增强数字身份互换的用户控制

7.1 引言

引入身份联合[b-LA-FF]来连接身份服务提供商（IdSP）和服务提供商（SP）之间发布的身份信息。如果SP要确保来自IdSP的认证信息可靠，要求在双方之间建立一个信任关系。这样的信任领域成为信任圈（CoT），可能包括一个或多个IdSP和几个SP。在一个CoT内，如用户已在一个IdSP得到认证，则无需再次认证便可获取CoT内SP的服务。这样，用户在一个CoT内只需认证一次。

但随着CoT数量的急剧增长，用户必须通过的认证次数也不断增加。在这种情况下，用户在每次访问时均需通过CoT认证。这意味着用户须管理一个CoT中IdSP提供的证书信息。这往往导致用户忘记密码或将它记录下来，未经授权而披露的风险增加了。CoT内的联盟为交换用户的身份信息提供了方便。但在CoT之间共享身份信息需要事先签署商业协议，因为涉及到法律程序，通常需花费很长的时间完成。如果身份管理的领域限于企业环境内部，则联盟将是一种高效有效的可行方案。但如果身份管理（IdM）系统的领域扩展到了互联网，就很难在所有协会的企业之间达成商业协议。

在大规模身份管理系统中，侧重于应用的IdM系统指身份服务和政策的目的是满足对IdSP和SP的要求，并通过优化满足各应用（如提供用户账户信息）的要求。向用户提供身份服务时，身份交换通常在IdSP和SP之间直接进行。在这种情况下，用户对其身份信息传播的控制是有限的。

由于身份信息在企业实体之间交换时没有用户干涉，则隐私和隐私保护可能被忽略。产生这样的问题是由于两个实体试图共享属于某个用户的用户身份信息。由于两个实体都涉及用户身份，因此他们需要事先签订商业和隐私政策协议。如果一个实体只需要与原始的所有者共享用户身份，则每个实体只需要与该所有者签订使用其身份信息的协议，并制定一项安全和隐私政策（或与管理其身份的实体）。

为了解决这个问题，本建议书规定了与用户数字身份相关信息交换时增强用户控制的框架。

7.2 安全威胁

除非注明，许多网络空间中出现的的安全威胁极有可能存在于IdM系统中。网络空间中的一般安全威胁在[ITU-T X.1205]中描述。

在IdM系统中，有各种不同的安全威胁，使系统易受攻击或导致一种安全妥协，而使组织处于非常危险的境地。在这些安全威胁中，身份欺诈是最常见的IdM环境的安全威胁类型之一。

身份欺诈是个严重的安全问题，对于存储和管理大量个人可识别信息的组织来说尤为如此。不仅会造成个人数据的损失，破坏消费者和机构的信心，导致对某个组织名誉的严重毁坏，而且数据的破坏也可能给组织带来财务上的昂贵代价。目前网络钓鱼可导致身份盗用。

网络钓鱼是第三方试图通过模拟或欺骗一个具体的、通常很知名的品牌，从某个人、团体或组织获得机密信息，通常是为了获得金钱上的收益。网上钓鱼网站是设计用于模仿被盗用品牌合法网站的网站。该机构的品牌被模仿攻击者试图欺骗用户泄露个人数据，例如信用卡号码、网上银行证书以及其他的敏感信息，以便其使用这些信息进行欺骗行为。因为受害者的认证信息或其他个人可识别信息 – 当被攻击者捕获时 – 可以被用做盗用身份或其他欺骗行为，因此在IdM系统里，网上钓鱼是严重的威胁。

7.3 用于数字身份互换的概念模型

在该概念模型中，数字身份互换框架（DIIF）使用了数字身份客户机（DIC）的概念，能够控制数字身份信息的交换。由用户控制身份信息的发布可大大减轻安全威胁一节中所述的安全威胁（见第7.2节）。

图1示出了用于数字身份互换的概念模型。

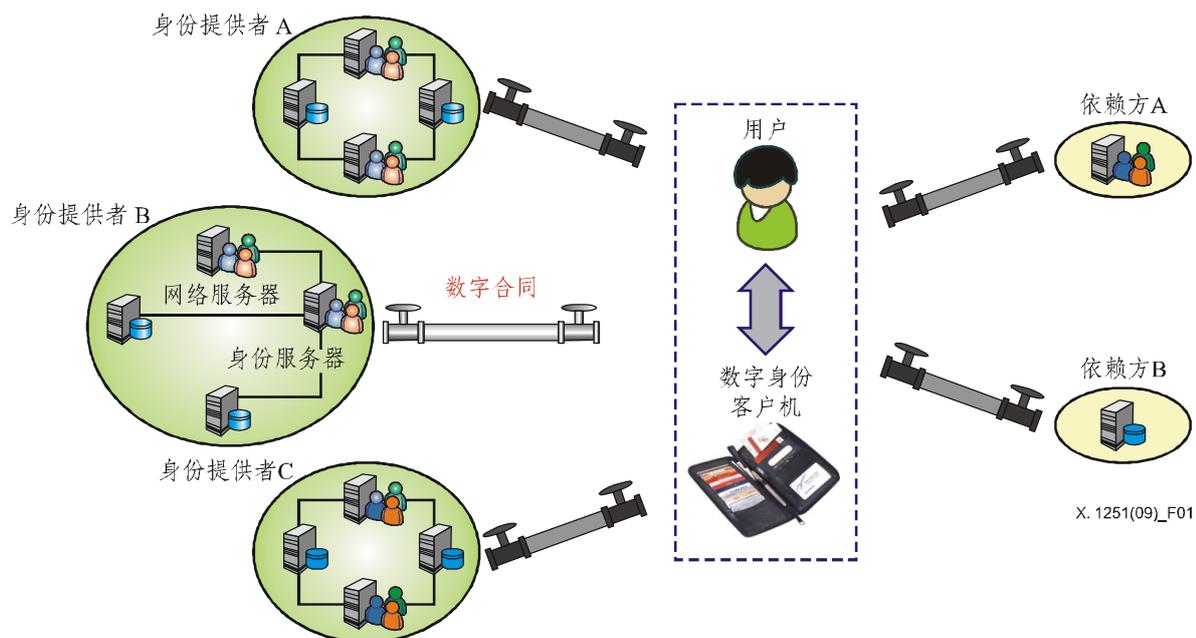


图1 – 用于数字身份互换的概念模型

7.3.1 身份服务器

身份服务器 (IdS) 是把用户身份信息提供给请求实体，或请求身份信息到一个用于网络服务DIC的主服务器。如果IdS提供身份信息，则它可能是一个身份服务提供商；如果IdS使用用户提供的身份信息，则它可能是一个依赖方 (RP)。IdS的角色可以是身份服务提供商，也可以是依赖方。网络服务器可以要求IdS提供用户身份信息以便提供网络服务。

7.3.2 数字身份客户机

数字身份客户机是给用户提供一个认证、证书和会话管理、身份互换和隐私保护服务的程序。如果需要与IdSP或RP共享身份信息，则DIC在一个域中与IdS建立一个链接。DIC可以与IdS签订一个协议来描述身份互换服务的术语和条件，这样可以增强交换的身份信息的隐私和安全。每个用户的身份信息均通过DIC，这样所述用户能控制其身份信息的共享。特别是取决于用户和实体之间认可的政策，用户完全控制交换哪些数据、用于什么目的、交换的对象和所用时间。由于所有要求推和拉身份信息的链接信息客户机都有，因此发现用户身份信息不是必需的。

7.3.3 身份服务提供商

身份服务提供商 (IdSP) 是管理用户身份信息、提供认证和授权服务并为网络服务器提供身份互换服务的实体。IdSP是一个概念角色模型，可以把它指派给管理用户身份的实体，并在DIC请求信息时提供这样的信息。IdSP管理由用户提交或自身产生的身份信息。

7.3.4 依赖方

依赖方（RP）是另一个概念角色模型，可以把它指配给向DIC请求用户身份并使用接收到的身份信息提供服务的实体。依赖方不依靠IdSP进行认证。用户在RP使用将得到认证的DIC。

7.3.5 用户

用户已在第3节中进行定义。在概念模型中用户通常指以用户为中心的IdM环境中的一个人或订户。用户是拥有并运行DIC的最终用户。

7.4 数字合同

在以用户为中心的身份管理环境中，身份服务提供商和依赖方之间流过的个人可识别信息（PII）必须经过数字身份客户机。这就给用户提供一个控制其PII使用的机会。数字合同仅在用户和IdSP或用户和依赖方之间签定。不允许实行多方合同，因为这会给用户带来复杂的管理问题。数字合同是使用户能有理有据地控制其PII流的核心组件。图2示出了数字合同的结构。



图2 - 数字合同结构

由数字合同规定的控制类型可以规定包括任何要求调解身份互换关系的政策。基于规则或其他政策要求，不会在每一次身份互换时都要求数字合同。只有需要控制共享PII流或高速缓冲时，才需要数字合同。这种协议和现实世界里的合同一样有灵活性和延展性（例如，要保密的协议）。而且，由于数字合同可能是XML文件本身，因此他们能管理对自己的修订、修改和删除（即现实世界的合同）。合同的要素包括：

- 1) 通用术语：描述版本、协议日期和生效期以及其他任何给用户的注意事项。这是一个必需的单元。
- 2) 目的：使用用户PII的意图。这是一个必需的单元。
- 3) 属性引用：表明协议中所指的一个实体的属性。这是一个必需的单元。

- 4) 安全政策：要求该单元包括认证和信息安全政策，指明两个实体如何能被认证以及如何能确保信息安全。这是一个必需的单元。
- 5) 隐私政策：该单元可以包括任何种类的隐私政策表述。已传播的用户PII的同步和终止也可以在此规定。必须根据适用的区域/国家隐私立法提供隐私保护。因此，这是一个可选单元。
- 6) 访问控制政策：可在该单元中描述访问控制政策或授权政策。这是一个可选单元。
- 7) 政策引用：可在该单元中详细说明对外面规定政策的参考。这是一个可选单元。
- 8) 签名：协议可以由在数字合同内容上达成一致的两个实体签署。然而，该合同最多能有两个数字签名，代表同意该合同的两个实体。然而，根据本节第一段中阐述的理由，签名不能超过两个。为确保有效性和完整性，协议必须由两个实体签名。当用户签署了协议，表示用户同意。签名的范围包括图2中的通用术语到政策引用。这是一个必需的单元。

7.5 用于身份互换的三个层

本节规定了三个层：应用层、身份互换层和通信层。

7.5.1 应用层

应用层可能是在互联网或移动通信环境下运行的典型的网络应用。例如，用户使用网络浏览器在网络服务器上请求网络服务。当应用中的实体需要请求身份服务或认证时，则调用身份互换层提供的服务。逻辑上来说，DIC位于应用层和身份互换层上，连接两个层给用户提供与身份相关的无缝式服务。每次用户试图登录一个网站时，会调用身份选择器，这是客户机内用户接口管理器的组件之一，用来选择代表身份的令牌进行网站认证。当网络应用需要共享用户身份信息以处理用户服务请求时，可以调用身份互换层提供的身份互换服务中的一个。身份互换层的服务描述位置供网络应用管理员使用。

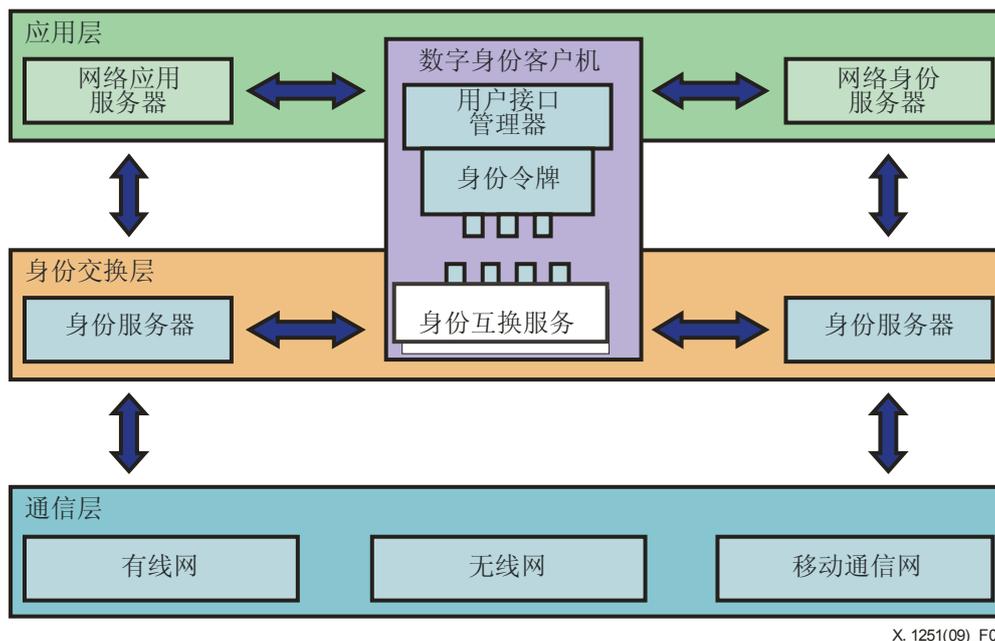


图3 – 身份互换层

7.5.2 身份互换层

身份互换层提供透明的身份互换链路层，以便于实体间的身份互换，并让用户完全控制其安全和隐私政策。

由于某个应用不需要知道身份互换的具体操作，则通过引入该层，可在任何应用之外独立开发和部署不同实体之间身份信息的共享。而且，身份互换层能提供给现有的没有身份互换能力的IdM解决方案，与身份互换相关的各种功能。数字合同一节详细描述了身份互换层是如何加强安全和隐私政策合规性的（见第7.4节）。

7.5.3 通信层

通信层是一个独立的层，负责把数据从一个设备传输到另一个设备。通信层可以是有线网、无线网或移动通信网。

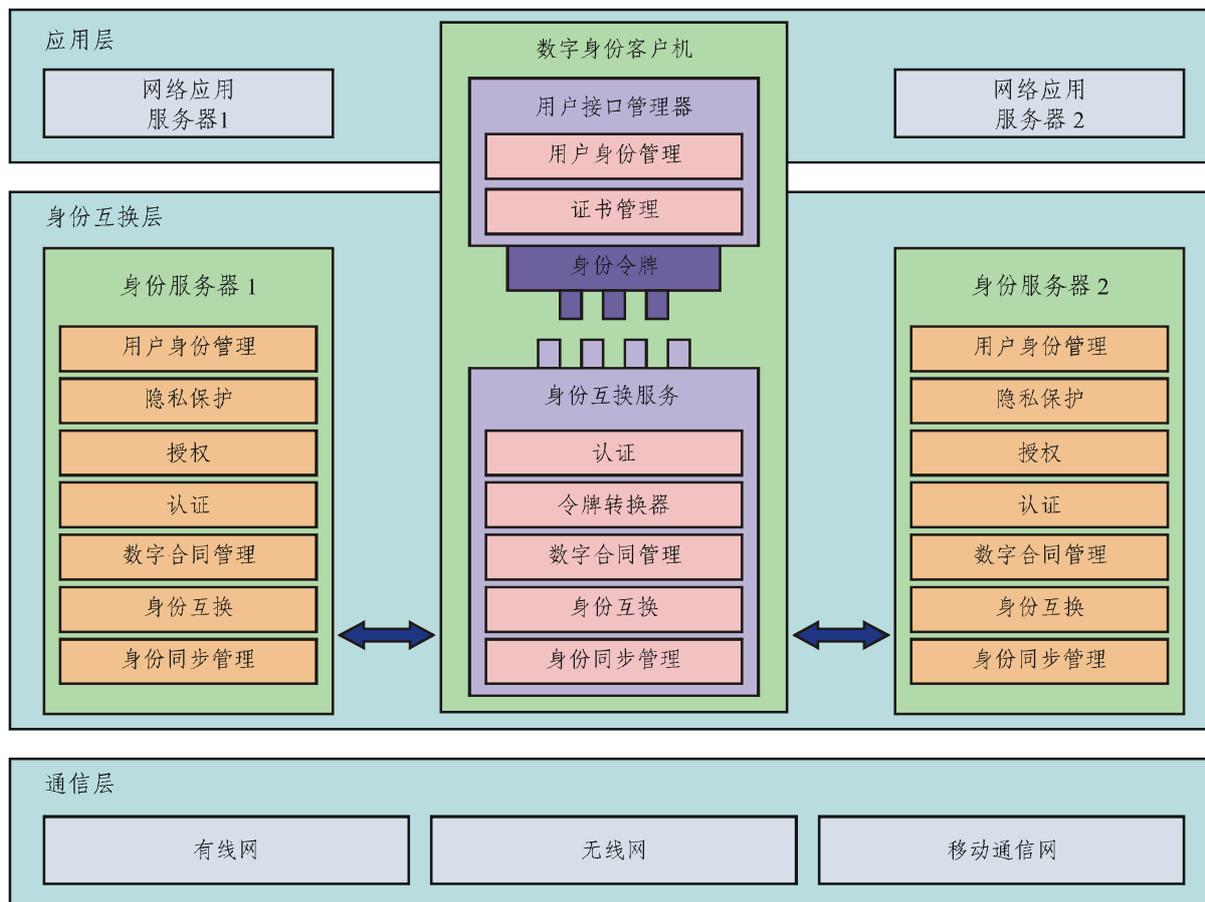
8 数字身份互换框架

8.1 设计原则

该框架有如下设计原则，在计算环境下，包括移动计算和普遍存在的计算，在实体之间提供无缝式的身份互换。

- **独立的** – 该框架不附加在任何具体的应用或网络环境上。如果必要，该框架本身应该适用于任何环境。
- **可插入的** – 在移动或普遍存在的计算环境里，用户可以为了工作或为了娱乐，在几台机器上操作。在这种情况下，用户需要的是能够建立其身份的基本身份信息。该信息的设计应适合任何一台机器，这样用户只要将其身份信息插入到机器中就可以使用了。

- **灵活的** – 该框架的设计应足够灵活适合任何一台机器，从工作站到小的普遍存在的计算设备。该框架还应有足够的延展性，为适应不同的计算环境还可进行结构配置。
- **可升级的** – 该框架本身必须可从一个简单的域到一个域间都可进行操作，而不会给现有系统带来通信或计算管理费用。



X.1251(09)_F04

图4 – 数字身份互换框架

8.2 框架构成

DIC是该框架内的核心组件，便于身份链路连接所有用户身份服务提供商和依赖方。每次需要时，用户能够使用预先建立的链路来检索和更新其身份信息。

DIC包括三个部分：用户接口管理器、身份互换服务和身份令牌。

图4表示功能的框架构成。

8.2.1 用户身份管理

用户身份管理是管理将被不同实体共享的用户身份信息的组件。在IdS中，身份管理主要集中在存储上。另一方面，DIC的身份管理设法集中在代表用户身份信息的图形用户界面上。

8.2.2 隐私保护

隐私保护是对保护用户身份信息的与隐私相关功能进行管理的组件。它跟踪与用户身份的使用和用途相关的审核信息。不管是有意使用用户身份还是无意使用，该功能都可以执行数字合同中描述的隐私限制。必须根据适用的区域/国家隐私立法提供隐私保护。

8.2.3 授权

关于用户访问权和根据用户权限执行授权决定，通过规定授权服务来处理这些决定。授权是一项选用服务；它只在基于用户权利需要控制访问资源时提供。

8.2.4 认证

认证是为支持各种不同的认证机制而提供一个一般认证框架的组件。该认证服务包括客户机和服务器的相互认证。

8.2.5 数字合同管理器

数字合同管理器是管理在用户和身份服务提供商之间为认证、访问控制和隐私保护而签定的数字合同清单的组件。该管理器管理数字签名签署的数字合同的生命周期。

8.2.6 身份互换

这是提供身份互换服务的核心组件。身份互换分为两种服务：检索和更新。如果身份信息存储在一个实体中，则DIC能够从实体中检索到其身份，反之亦然。如果存储在实体中的身份信息发生改变，则该实体能够更新或把改变后的身份信息推给DIC，反之亦然。对该组件的详细描述不在本建议书的范围内。

8.2.7 身份同步管理器

身份同步管理器是管理在DIC中的身份同步过程的组件。当存储在IdSP中的身份信息发生改变时，IdSP把改变后的身份更新到DIC。在DIC中，该组件为每一位与DIC共享用户身份的依赖方(RP)，执行身份互换功能中的身份更新操作。注意，只有DIC已把其身份推送一次的依赖方，才有资格接收更新后的身份信息。

8.2.8 用户接口管理器

用户接口管理器是代表用户身份和证书信息的图形用户接口的组件。一般来说，当用户需要使用认证或共享其身份信息登录某些服务时，该组件与网络应用服务器有紧密的联系。

8.2.9 证书管理

证书管理是管理由实体产生或由站点产生的认证证书信息的组件。用户能有各种不同的证书，例如密码、X.509证书和生物识别。为给用户一致的信息，规定了证书信息的通常图形表示。

8.2.10 身份令牌

身份令牌是数字身份的数据模型。可以把身份令牌插入数字身份客户机，把用户接口管理器连接到身份互换服务，使DIC能够发挥作用。当接上用户接口管理器时，可以实现令牌的逻辑表示。例如，当用户转变其工作环境，从一台个人计算机到一个移动电话，用户只需要携带令牌并把它插入到移动电话中。包含令牌的硬件可以是一个智能卡、一个USB令牌等。

8.2.11 身份互换服务

这是负责身份互换和同步的服务部分。根据所使用的网络或通信平台，要求调整该部分以适应环境。例如，个人计算机的身份互换服务模块完全不同于移动电话的身份互换服务模块。

8.2.12 令牌转换器

令牌转换器是把另一个IdM系统发出的令牌，转换到能够在DIIF中识别和处理令牌的组件。这是用于不同令牌交换（例如，身份、安全）时与其他现有IdM系统互通的网关组件。这是一个选用组件。

附录一

使用网络服务信任和信息卡技术的数字身份的用户控制框架参考实施指南

(本附录不是本建议书的组成部分)

注 – 本附录提供按照本建议书要求的网络服务信任 [b-WS-TRUST]和信息卡[b-IS-INTEROP]映射能力示例。

1.1 引言

本附录描述在本建议书中规定的要求如何被网络服务信任和信息卡[b-CARDSPACE]技术所满足。

1.2 背景

1.2.1 数字身份客户机

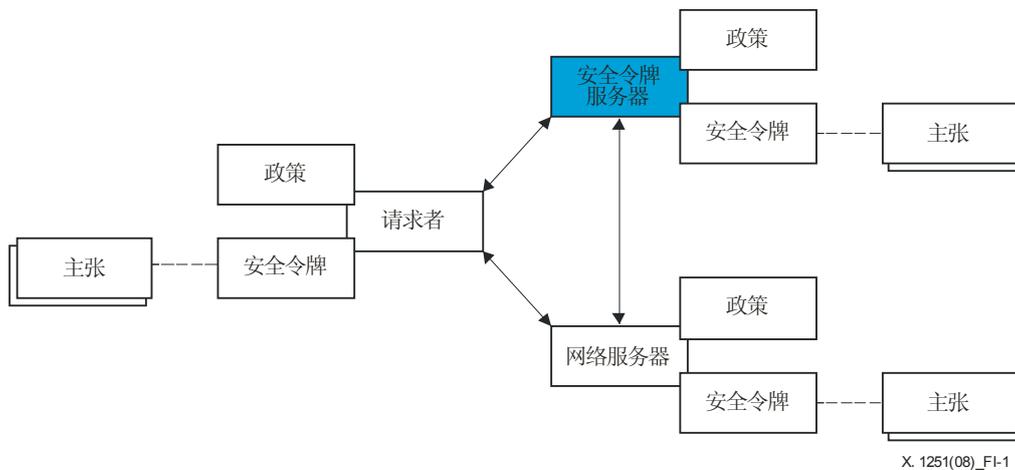
第 7.3.2 节描述了“能够控制数字身份相互交换的数字身份客户机的概念”。

1.2.2 身份互换层

第 7.5.2 节描述了“便于在实体之间进行身份互换以及完全控制实体实施其安全和隐私政策的身份互换层。”

1.2.3 网络服务信任 (WS-Trust)

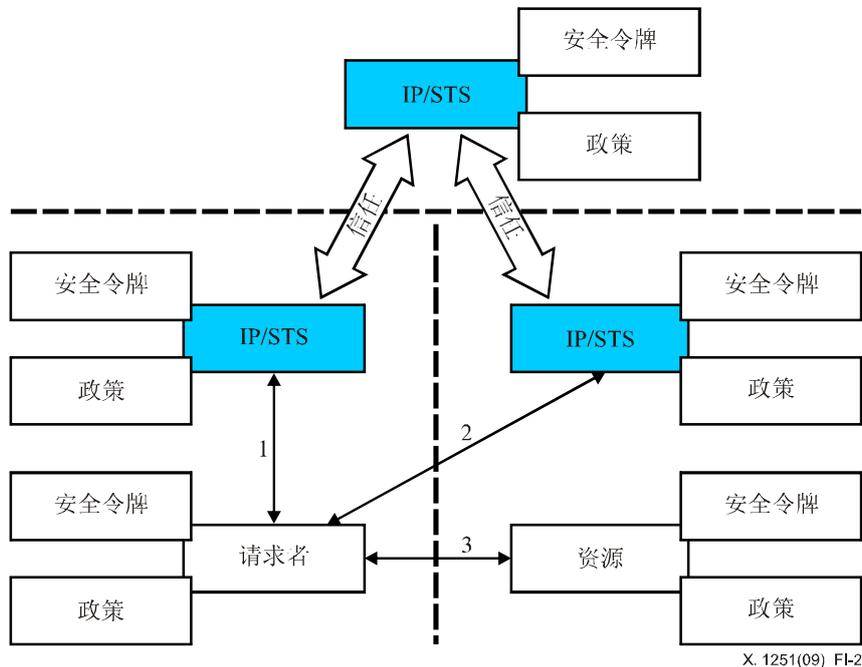
网络服务信任规范定义了建立在网络服务安全上的扩展，为请求和发布安全令牌提供框架并提供中间信任关系。一个代表实体的请求方通常发送一个 RequestSecurityToken (RST) 消息给一个安全令牌服务 (STS)，并收回一个通常包含安全令牌的安全令牌。然后可以把包括一套声明的安全令牌，发送给网络服务器作为请求方身份的证明。或者，可以发送给安全令牌服务一个带有请求的 RST，以确认或取消先前发布的安全令牌。这些相互作用如图 I-1 中所示。



X. 1251(08)_FI-1

图I-1 – 网络服务信任的直接信任模型

可以使用网络服务信任来实施多种模型而不只是单一的直接信任模型。在某些情况下，IP/STS(身份服务提供商/安全令牌服务)为了满足原来的 RST 而给另一个 STS 发送一个 RST 时，可以使用间接模型，如图 I-2 所示。



图I-2：网络服务信任的间接信任模型

1.2.4 信息卡

在身份选择器互操作轮廓[b-IS-INTEROP]中描述信息卡技术。有了信息卡技术，身份选择器和相关身份系统组件允许实体来管理不同身份服务提供商的数字身份，并在不同的环境下使用这些身份接入到在线服务。

当实体与 IdSP 建立关系时，实体收到信息卡。这些信息卡包括描述了能够通过网络服务信任来请求可能的安全令牌的元数据，以及用来保护和认证消息交换的安全机制的元数据。信息卡的典型安装是，实体把信息卡安装到身份选择器可以访问的卡存储器内。通过网络服务安全政策[b-WS-SECURITY]来规定依赖方安全政策，并可通过多种方式检索，包括嵌入在网页中。对于在网络服务安全中规定的用于认证和消息保护的机制，在该安全政策中也有代表性地予以规定。身份选择器评价了依赖方政策和在用户卡存储器中安装的信息卡集，并允许实体从信息卡集中选择匹配的信息卡（能够得到符合政策的安全令牌）。然后必要时，该身份选择器指定实体用于认证信息，并发送一个 RST 给所选信息卡中规定的 STS。然后，来自结果 RSTR 的安全令牌可以附加到要发送给依赖方的消息上。当网站是依赖方时，可以贴上安全令牌作为对包含该政策[b-IS-GUIDE]的形式的响应。

1.3 DIIF能力

本节重申了 DIIF 能力并描述了如何使用网络服务信任和/或信息卡技术来满足这些能力。

I.3.1 总体能力

I.3.1.1 用户能力

DIIF 应完成以下目标：

- 1) 给用户提供一个身份选择器以允许用户选择要使用哪个证书来进行认证。

信息卡中描述的身份选择器提供了一个安全、直观和一致的实体体验，允许实体选择信息卡，这些信息卡代表由多种认证机制下不同 IdSP 提供的多种实体。

- 2) 给用户提供一个直观和一致的接口以最大安全地管理其证书信息。

信息卡中描述的身份选择器提供了一个安全、直观和一致的实体体验。

- 3) 支持网站自动填表登记或签字以使用户与网站的互动最小化，包括由用户完全控制激活和去激活这样的机制。

该主张值包含在安全令牌中，与信息卡中描述的身份选择器一起使用，能够在登记时提供由实体输入的代表信息。

- 4) 在任何时候提供用户希望的身份信息共享，并允许用户在适当的隐私保护机制下完全控制身份互换。

假定信息卡技术是 IdSP 只是为了响应实体的请求而提供身份信息。在选择信息卡过程中，可以在安全身份选择器用户接口内获得依赖方和 IdSP 的隐私政策。

- 5) 当原始资料改变时给用户共享身份信息的自动更新，过程完全由用户控制。

该主张值包含在安全令牌中，与信息卡中描述的身份选择器一起使用，能够在登记时提供由实体输入的代表信息。由于每次访问时依赖方请求的安全令牌主张值可能相同，因此这些值的改变很容易获知。

- 6) 使用户能完全控制安全和隐私政策的建立以及在共享身份信息之前如何执行政策以控制身份互换。

在选择信息卡过程中，可以在安全身份选择器用户接口内获得依赖方和 IdSP 的安全政策，在信息卡中描述。

I.3.1.2 功能能力

- 1) 支持综合证书管理，能够管理用于认证的用户证书信息。

信息卡技术包括身份选择器和卡管理用户接口。

- 2) 支持身份互换链路管理，给用户全方位的角度，查看用户身份互换时和哪些实体联系。

在代表会话的一个安全令牌从 IdSP 返回的情况下，IdSP 能够提供一个接口，允许实体查看已建立的会话集。

3) 支持多重认证机制，包括密码认证、PKI认证和生物测定认证。

网络服务信任和网络服务安全提供一个支持多种认证机制的一致直观的协议。实施信息卡技术提供了直观的 API 以启动认证过程。

4) 支持身份互换机制，能够提供双向链路以使用DIC在实体之间共享用户身份信息。

有了信息卡技术，身份选择器和卡存储可执行与 DIC 相关的功能。

5) 支持数字合同机制，为用户进行身份互换制定合同并在发布PII时用于执行安全和隐私政策。

在选择信息卡过程中，可以在安全身份选择器用户接口内获得依赖方和 IdSP 的安全政策，在信息卡中描述。

6) 支持身份信息同步，当传播身份信息的来源发生改变时相应地更新已发布和共享的身份信息。需要同步的身份信息限于用户直接改变的PII。

该主张值包含在安全令牌中，与信息卡中描述的身份选择器一起使用，能够在登记时提供由实体输入的代表信息。由于每次访问时依赖方请求的安全令牌主张值可能相同，因此这些值的改变很容易获知。

7) 支持普遍令牌转换，使框架与现有身份管理系统可以互操作。

网络服务信任提供了一个令牌交换机制。RST 消息可以包括一个或多个安全令牌还有依赖方的身份指示。RSTR 可以包括适用于依赖方的安全令牌。

1.3.2 附加能力

DIIF 应该为身份选择器和相关协议提供可延展性机制，以允许支持多种认证机制的登录和传输并确保相关信息。

这包括（但不限于）对智能卡用户和生物识别输入设备以及与之相关的数据格式的支持，例如在[b-NIST]中描述的那样。

参考资料

- [b-ITU-T X.1252] ITU-T X.1252建议书 (2010年), 《基线身份管理的术语和定义》。
- [b-ITU-T Y.2091] ITU-T Y.2091建议书 (2008年), 《下一代网络的术语和定义》。
- [b-ITU-T Y.2701] ITU-T Y.2701建议书 (2007年), 《下一代网络 (NGN) 第一阶段的安全性要求》。
- [b-ITU-T Y.2720] ITU-T Y.2720建议书 (2009年), 《NGN身份管理框架》。
- [b-CARDSPACE] Microsoft (2006), *Introducing Windows CardSpace*.
- [b-ETSI 133 980] ETSI TR 133 980 V8.0.0 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Liberty Alliance and 3GPP security interworking*.
- [b-IS-INTEROP] Microsoft (2007), *Identity Selector Interoperability Profile V1.0*.
- [b-IS-GUIDE] Microsoft (2007), *A Guide to Using the Identity Selector Interoperability Profile V1.0 within Web Applications and Browsers*.
- [b-LA-FF] Liberty Alliance, *Liberty ID-FF Protocols and Schema Specification (ver 1.2)*.
- [b-NIST] National Institute of Standards and Technology (2006), *FIPS PUB 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors*.
- [b-WS-SECURITY] OASIS (2007), *WS-SecurityPolicy 1.2*.
- [b-WS-TRUST] OASIS (2007), *WS-Trust 1.3*.

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	终端和主观与客观评估方法
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、互联网的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