国 际 电 信 联 盟

ITU-T X.1154

(04/2013)

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

安全应用和服务 – 安全协议

多身份服务提供者环境下的组合认证通用框架

ITU-T X.1154 建议书

ITU 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	
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.1154 建议书

多身份服务提供者环境下的组合认证通用框架

摘要

近来，由于身份（ID）盗窃的增加，很多应用服务，尤其是金融服务，要求更可靠或更全面的身份认证方法，如多因素认证。例如，一次一密认证以及其他新的身份认证方法被用于取代传统的基于口令的身份认证。

多种身份认证方法的组合使多身份服务提供者（IdSP）增强了对身份认证的保证能力。ITU-T X.1154建议书为服务提供者提供了多身份服务提供者环境下组合认证的通用框架。本建议书涉及三种组合认证方法，即：多因素认证、多方法认证和多重认证。

为了在多身份服务提供者组合的情况下维持认证保证的总体水平，本建议书中的框架描述了各模型、基本操作及对每一模型组件的安全要求以及模型组件间的各种信息。

此外，该框架对各模型、基本操作及安全要求的描述也用于支持管理多身份服务提供者组合的认证服务。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1154	2013-04-26	17

关键词

组合认证、实体认证、多因素认证

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

引言

近来，由于身份盗窃的增加，很多应用服务，尤其是金融服务，要求更可靠或更全面的身份认证方法，如多因素认证。例如，一次一密认证以及其他新的身份认证方法被用于取代传统的基于密码的身份认证。

关于安全应用服务认证的ITU-T建议书（见[b-ITU-T X.509]及[ITU-T X.1141]）是标准的认证框架。ITU-T建议书的基本出发点是一个服务提供者和/或用户同属于由一个身份服务提供者提供的安全域，即使服务提供者与用户属于不同的安全域。为了增强认证，身份服务提供者需要使用更有力的认证方法（例如[b-ITU-T X.1151]、[b-ITU-T X.1084]、[b-ITU-T X.1086]以及[b-ITU-T X.1089]中提到的方法）。

另一方面，经常出现一位用户从数个身份服务提供者那里检索到数个身份，且一个服务提供者与数个身份服务提供者建立信任关系。在这种多身份服务提供者环境下，当服务提供者使用多身份服务提供者（IdSP）认证用户时，可能存在加强认证的其他方式。

此外，即使服务提供者（SP）实施更强的身份认证，仍可以使用桥接式身份服务来组合多身份服务提供者。

然而，由于各身份服务提供者由不同的提供商运营，对多身份服务提供者进行简单的组合可能会导致整个认证级别的崩溃。

因此，要求通用框架描述出各模型组件的模型、基本操作和安全要求，以及模型组件间的各种信息，并以此在多身份服务提供者组合的情况下保持认证保证的整体水平。

另外，更强大的/更可靠的认证需求增加了认证系统运行和/或管理的复杂性。因此，管理多身份服务提供者组合认证服务被用于认证代表应用服务的用户。这一认证服务需要管理符合各应用服务认证策略需求的多身份服务提供者组合。

该框架还应描述出模型、基本操作及安全要求以支持认证服务。

ITU-T X.1154 建议书

多身份服务提供者环境中组合认证的通用框架

1 范围

本建议书为服务提供者提供了用于多身份服务提供者（IdSP）环境中组合认证的通用框架，以实现诸如多因素认证等组合认证。

为了在多身份服务提供者（IdSP）组合的情况下保持认证保证的总体水平，本建议书中的框架描述了各模型组件模型，基本操作及安全要求以及模型组件间的各种信息。

此外，该框架对模型，基本操作及安全要求的描述也用于支持管理多身份服务提供者（IdSP）组合的认证服务。

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。本建议书中引用某个文件，并非确定该文件自成一体时具备建议书的地位。

[ITU-T X.1141] ITU-T X.1141建议书 (2006)，《安全断言标记语言（SAML 2.0）》。

[ITU-T X.1254] ITU-T X.1254建议书 (2012)，《实体认证保证体系》。

3 定义

3.1 他处定义的术语

本建议书使用下列他处定义的术语：

3.1.1 断言（assertion）[b-ITU-T X.1252]：一实体在没有有效性凭证的情况下做出的声明。

3.1.2 保证水平（assurance level）[b-ITU-T X.1252]：表明对实体和所介绍的身份信息之间关联性的置信程度的量化表示。

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

3.1.4 认证保证（authentication assurance）[b-ITU-T X.1252]：是声称为或预期为沟通伙伴的实体，在认证过程中实现的信任度。

注 – 信任是基于在沟通实体和显示的身份之间绑定的信任程度。

3.1.5 最终用户（end user）[ITU-T X.1141]：以应用为目的利用资源的自然人。

3.1.6 标识符（identifier）[b-ITU-T X.1252]：用来在语境中识别实体的一个或多个属性。

3.1.7 身份（identity）[b-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。在身份管理（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。

3.1.8 身份服务桥接提供者（identity service bridge provider）[b-ITU-T X.1252]：作为其他身份服务提供者中可信赖的中介身份服务提供者。

3.1.9 身份服务提供者（identity service provider (IdSP)）[b-ITU-T X.1252]：认证、维护、管理并可能创建和分配其他实体身份信息的实体。

3.1.10 信赖方（relying party）[ITU-T X.1141]：根据来自另一个系统实体的信息决定采取动作的系统实体。例如，信任赖方依赖于从有关主体的断言方（SAML机构）接收到的断言。

3.1.11 服务提供者（service provider）[ITU-T X.1141]：系统实体所代表的角色，在服务提供者处，系统实体向责任人或其他系统实体提供服务。

3.2 本建议书定义的术语

本建议书定义下列术语：

3.2.1 认证因素（authentication factor）：一种证书，认证因素包括三种：所有权因素，知识因素以及生物识别因素。

3.2.2 生物特征识别因素（biometric factor）：一种认证因素，认证用户身份或用户所做的事。

3.2.3 组合认证（combined authentication）：一种使用多重证书的认证。

3.2.4 当前保证水平（current assurance level）：某一实体在当前时间点的认证保证水平。

3.2.5 知识因素（knowledge factor）：一种认证因素，认证用户所掌握的信息。

3.2.6 多因素认证（multifactor authentication）：一种使用三类认证因素中的两种以上的证书的认证。

3.2.7 多方法认证（multi-method authentication）：使用来自不同认证方法的多种证书的认证。

3.2.8 多重认证（multiple authentication）：使用来自同一认证方法的多种证书的认证。

3.2.9 所有权因素（ownership factor）：一种认证因素，认证用户所拥有的物品。

3.2.10 所提供保证水平（provided assurance level）：某一身份服务提供者（IdSP）认证用户时所提供的保证水平。

3.2.11 所需保证水平（required assurance level）：某一服务提供者提供其服务时所要求的保证水平。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

ID 身份

IdM 身份管理

IdSP 身份服务提供者

PKI 公开密钥基础设施

SAML 安全断言标记语言

SP 服务提供者

5 惯例

在本建议书中：

“需要”（is required to）指的是必须严格遵守的要求，要声明与本建议书一致就不得偏离这种要求。

“建议”（is recommended）指的是推荐采取但并非必须遵守的要求。因此在声明一致性时不用提及这种要求。

“禁止”（is prohibited from）指的是必须严格遵守的要求，要声明与本建议书一致就不得偏离这种要求。

“可选”（can optionally）指的是允许的任选要求，没有任何推荐的意思。该术语并不意味着供应商必须实施这一选项，是否启用这一特性由网络运营商/服务提供者任选；而是指供应商可以视情况选择提供这一特性，同时仍然声明与本建议书一致。

6 组合认证的类型

本建议书提出了如下三种组合认证方法：

– 多因素认证，使用来自三种认证因素中的两种以上因素的证书的认证。例如，（1）通过存储在智能卡中的公开密钥证书进行认证，（2）使用硬件设备通过一次性口令进行认证，以及（3）一次性口令认证与生物识别认证相组合的认证为多因素认证的实例。

– 多方法认证，使用来自不同认证方法的多重证书的认证。例如，（1）一次性口令认证与密码认证相组合，（2）指纹认证与指静脉认证相组合为多方法认证的实例。

– 多重认证，使用来自同一认证方法的多种证书的认证。例如，（1）双重密码认证，（2）使用多指纹的指纹认证为多重认证的实例。

以上三种认证方法的不同之处在于证书的组合方式。此外，“认证因素”对证书进行了分类，分别为所有权因素，知识因素以及生物识别因素三类。

– 所有权因素是根据用户所拥有的物品进行识别，例如，智能卡，安全令牌，软件权标，固网电话以及移动电话。
– 知识因素是根据用户所掌握的信息进行认证。例如，密码，口令短语以及个人识别码（PIN）。
– 生物识别因素是根据用户的身份或所做的事进行认证。例如指纹、指静脉以及虹膜。

7 多身份服务提供者（IdSP）环境中的认证模型

7.1 关于服务提供者的基本模型

如从服务提供者的角度考虑认证模型，则应在用户收到应用服务时考虑以下因素：

– IdSP所提供的认证方法是单因素认证还是组合认证。
– 模型包括的是单一IdSP还是多个IdSP。如果模型中包括多个IdSP，这些IdSP所提供的同一种认证方法还是不同的认证方法，如果IdSP提供不同的认证方法，这些方法是不同因素还是相同因素。

因此，为了实现组合认证，根据SP以及IdSP的数量，共有8种功能模型以及1种组合认证（见表1）。此外，如果多重IdSP环境中存在多用户，且一位用户不一定与所有IdSP均建立信任关系。换句话说，可将IdSP根据与其建立了信任关系的一组用户进行分组（见图1）。在这种情况下，还要考虑以下因素。

– 根据IdSP与用户建立的信任关系将IdSP划入一组或多个组。

若IdSP被划入一组中，则表1中的T-3至T-8模型适用。

若IdSP被划入两组以上的组别中，则可以考虑采用T-9至T-14模型（见表2）。

表1 – 基本认证模型（若IdSP被划为一组）

	IdSP数量	认证方法类型数量	由一位IdSP所提供的认证方法的类型	IdSP分组的数量	由组合IdSP所提供的认证方法
T-1	一个	一种	单因素	1	无
T-2			组合	1	组合（注1）
T-3	多个	一种	单因素	1	多重
T-4			组合	1	组合（注1）
T-5		多种（不同方法）	单因素	1	多重，多方法（注2）
T-6			组合（多重或多方法）	1	多重，多方法（注3）
T-7		多种（不同因素）	单因素	1	多重，多方法，多因素（注2）
T-8			组合	1	组合（注3）

表1 – 基本认证模型（若IdSP被划为一组）

	IdSP数量	认证方法类型数量	由一位IdSP所提供的认证方法的类型	IdSP分组的数量	由组合IdSP所提供的认证方法
注1 – 三种组合认证均可提供，但是所提供的认证方法要取决于IdSP所提供的认证类型。 注2 – 三种组合认证均可提供，但是所提供的认证方法要取决于IdSP的选择。 注3 – 三种组合认证均可提供，但是所提供的认证方法不仅取决于IdSP所提供的认证类型，同时也取决于IdSP的选择。					

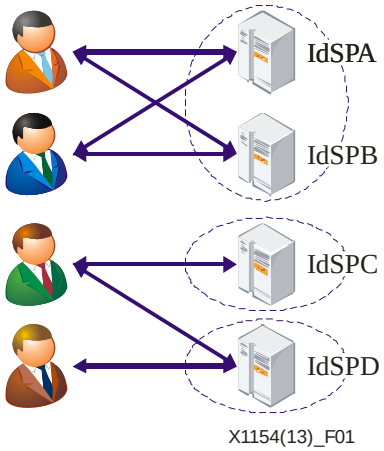


图1 – 根据与用户的信任关系对IdSP进行的多重分组

表2 – 基本认证模型（若IdSP被划分为若干组）

	IdSP数量	认证方法类型数量	由一位IdSP所提供的认证方法的类型	IdSP分组的数量	由组合IdSP所提供的认证方法
T-9	多个	一种	单因素	多个	多重
T-10			组合	多个	组合（注1）
T-11		多种（不同方法）	单因素	多个	多重，多方法（注2）
T-12			组合（多重或多方法）	1	多重，多方法（注3）
T-13		多种（不同因素）	单因素	多个	多重，多方法，多因素（注2）
T-14			组合	多个	组合（注3）

表2 – 基本认证模型（若IdSP被划分为若干组）

	IdSP数量	认证方法类型数量	由一位IdSP所提供的认证方法的类型	IdSP分组的数量	由组合IdSP所提供的认证方法
注1 – 三种组合认证均可提供，但是所提供的认证方法要取决于IdSP所提供的认证类型。 注2 – 三种组合认证均可提供，但是所提供的认证方法要取决于IdSP的选择。 注3 – 三种组合认证均可提供，但是所提供的认证方法不仅取决于IdSP所提供的认证类型，同时也取决于IdSP的选择。					

7.11 模型T-1

当一个IdSP提供一个单因素认证时，以及当一个IdSP、一个服务提供者以及一个或多个终端通过网络互相连接时，采用模型T-1。

当服务提供者从终端接收到服务请求时，服务提供者向IdSP发出请求，要求对用户进行认证。从服务提供者处接到认证要求的IdSP通过单因素认证方法对用户进行认证。若从IdSP返回的认证结果显示用户成功通过认证，则服务提供者向终端提供其服务。

这一模型不能提供组合认证，因此不在本建议书讨论范围之内。

7.12 模型T-2

当一个IdSP提供组合认证（多重、多方法或者多因素认证）时，当一个IdSP，一个服务提供者以及一个或多个终端通过网络互相连接时，采用模型T-2。

当服务提供者从终端接收到服务请求时，服务提供者向IdSP发出请求，要求对用户进行认证。从服务提供者处接到认证要求的IdSP通过组合认证方法对用户进行认证。若从IdSP返回的认证结果显示用户成功通过认证，则服务提供者向终端提供其服务。

这一模型可以依据IdSP提供的认证方法的类型提供任何类型的组合认证方法。

7.13 模型T-3

当多身份服务提供者提供相同的单因素认证方法时，当多身份服务提供者，一个服务提供者以及一个或多个终端通过网络互相连接时，采用T-3模型。在T-3模型中，所有用户和所有IdSP之间均有信任关系。

当服务提供者从终端接收到服务请求时，服务提供者选择多身份服务提供者来满足所要求的认证保证，并要求所选择的IdSP对用户分别进行认证。若从IdSP返回的所有认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

本模型可以提供多重认证方法。

需要指出的是，若由一个IdSP提供的认证方法符合所要求的认证保证，则本模型可以提供单因素认证，但是，这一模型上的单因素认证不在本建议书的讨论范围之内。

7.14 模型T-4

当多身份服务提供者提供相同的组合认证方法时，当多身份服务提供者，一个服务提供者与一个或多个终端通过网络互相连接时，采用模型T-4。在这一模型中，所有用户与所有IdSP之间均建有信任关系。

当服务提供者从终端接收到服务请求时，服务提供者选择一个或多个满足所要求的认证保证的IdSP，并要求这些IdSP对用户分别进行认证。如果所有从IdSP返回的认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

本模型提供可以依据由一个IdSP提供的组合认证的类型和/或IdSP的选择提供任何类型的组合认证。（可能执行多因素认证以及多方法认证）。

7.15 模型T-5

当多身份服务提供者提供类型不同但是用相同因素的单一认证方法时，当多身份服务提供者，一个服务提供者以及一个或多个终端通过网络互相连接时，采用模型T-5。在这一模型中，所有用户与所有IdSP之间均建有信任关系。

当服务提供者从终端接收到服务请求时，服务提供者选择满足所要求的认证保证的多身份服务提供者，并要求其对用户分别进行认证。若所有从IdSP返回的认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

本模型可以提供多重认证或多方法认证。需要指出的是，所执行的认证方法取决于组合IdSP的选择。

若由IdSP提供的认证方法符合所要求的认证保证，则本模型也可以提供单因素的认证，但是这一模型上的单因素认证不在本建议书的讨论范围内。

7.16 模型T-6

当多身份服务提供者提供类型不同但所采用因素相同的组合认证方法时（即提供多重或多方法认证方法），以及当多身份服务提供者，一个服务提供者以及一个或多个终端通过网络互相连接时，采用模型T-6。在该模型中，所有用户与所有IdSP之间均建有信任关系。

当服务提供者从终端接收到服务请求时，服务提供者选择符合所要求的认证保证的单一或多身份服务提供者并请求其对用户分别进行认证。若所有从IdSP返回的认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

此模型可以提供多重认证或者多方法认证，这取决于IdSP的选择和组合。

7.17 模型T-7

当多身份服务提供者提供采用不同因素的单一认证方法时，以及当多身份服务提供者，一个服务提供者以及一个或多个终端通过网络互相连接时，采用模型T-7。在该模型中，所有用户与所有IdSP之间均建有信任关系。

当服务提供者从终端接收到服务请求时，服务提供者选择满足所要求的认证保证的多身份服务提供者并请求其对用户分别进行认证。若所有从IdSP返回的认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

此模型可以提供任何类型的组合认证。需要指出的是，所执行的认证方法取决于IdSP的选择。

同时，若由单一IdSP提供的认证方法符合所要求的认证保证，此模型也可以提供单因素的认证，但是基于此模型的单因素认证不在本建议书的讨论范围之内。

7.18 模型T-8

当多身份服务提供者提供采用不同因素的组合认证方法时，以及当多身份服务提供者、一个服务提供者以及一个或多个终端通过网络互相连接时，采用模型T-8。在该模型中，所有用户与所有IdSP之间均建有信任关系。

当服务提供者从终端接收到服务请求时，服务提供者选择单一或多身份服务提供者来满足所要求的认证保证，并请求其对用户分别进行认证。若所有从IdSP返回的认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

本模型可以提供任何类型的组合认证方法。

7.19 模型T-9

当多身份服务提供者提供相同的单因素认证方法时，以及当多身份服务提供者、一个服务提供者以及多个终端通过网络互相连接时，采用模型T-9。在模型T-9中，一个或多个用户并不与所有IdSP建立信任关系。

注 – 在本模型中，IdSP可以同所有用户均不建立信任关系，但是包含此类IdSP的模型不在本建议书的讨论范围之内。

当服务提供者从终端接收到服务请求时，服务提供者从一组IdSP中选择与用户建有信任关系的多身份服务提供者来满足所要求的认证保证，并请求其对用户进行认证。若所有从IdSP返回的认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

本模型可以提供多重认证方法。

需要指出的是，若由IdSP提供的认证方法符合所要求的认证保证，则本模型也可以提供单因素的认证，但是这一模型上的单因素认证不在本建议书的讨论范围内。

7.1.10 模型T-10

当多身份服务提供者提供相同的组合认证方法时，以及当多身份服务提供者、一个服务提供者以及多个终端通过网络互相连接时，采用模型T-10。在模型中T-10，一个或多个用户并不与所有IdSP建立信任关系。

注 – 模型T-10中存在IdSP同所有用户之间均无信任关系的情况，但是包含此类IdSP的模型不在本建议书的讨论范围之内。

当服务提供者从终端接收到服务请求时，服务提供者选择单一或多身份服务提供者来满足所要求的认证保证，并请求其对用户分别进行认证。若所有从IdSP返回的认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

本模型提供可以依据由一个IdSP提供的组合认证的类型和/或IdSP的选择提供任何类型的组合认证。可能执行多重多因素认证以及多重多方法认证。

7.1.11 模型T-11

当多身份服务提供者提供采用相同因素但类型不同的单一认证方法时，以及当多身份服务提供者、一个服务提供者以及多个终端通过网络互相连接时，采用模型T-11。在模型T-11中，一个或多个用户并不与所有IdSP建立信任关系。

注 – 模型T-11中存在IdSP同所有用户之间均无信任关系的情况，但是包含此类IdSP的模型不在本建议书的讨论范围之内。

当服务提供者从终端接收到服务请求时，服务提供者从一组IdSP中选择与用户建有信任关系的多身份服务提供者来满足所要求的认证保证，并请求其对用户进行认证。若所有从IdSP返回的认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

本模型可以提供多重认证或多方法认证。需要指出的是，所执行的认证方法取决于IdSP组合。

若由单一IdSP提供的认证方法符合所要求的认证保证，本模型也可以提供单因素认证，但是这一模型上的单因素认证不在本建议书的讨论范围内。

7.1.12 模型T-12

当多身份服务提供者提供采用相同因素但类型不同的组合认证方法时（即提供多重或多方法认证方法），以及当多身份服务提供者、一个服务提供者以及多个终端通过网络互相连接时，采用模型T-12。在模型T-12中，一个或多个用户并不与所有IdSP建立信任关系。

注 – T-12模型中存在IdSP同所有用户之间均无信任关系的情况，但是包含此类IdSP的模型不在本建议书的讨论范围之内。

当服务提供者从终端接收到服务请求时，服务提供者从一组IdSP中选择与用户建有信任关系的单一或多身份服务提供者来满足所要求的认证保证，并请求其对用户进行认证。若所有从IdSP返回的认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

本模型可以依据IdSP的选择或组合提供多重认证或多方法认证。

7.1.13 模型T-13

当多身份服务提供者提供采用不同因素的单一认证方法时，以及当多身份服务提供者、一个服务提供者以及多个终端通过网络互相连接时，采用模型T-13。在模型T-13中，一个或多个用户并不与所有IdSP建立信任关系。

注 – T-13模型中存在IdSP同所有用户之间均无信任关系的情况，但是包含此类IdSP的模型不在本建议书的讨论范围之内。

当服务提供者从终端接收到服务请求时，服务提供者从一组IdSP中选择与用户建有信任关系的单一或多身份服务提供者来满足所要求的认证保证，并请求其对用户进行认证。若所有从IdSP返回的认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

本模型可以提供任何类型的多重认证。需要指出的是，所执行的认证方法取决于IdSP的选择。

若由单一IdSP提供的认证方法符合所要求的认证保证，本模型也可以提供单因素认证，但是这一模型上的单因素认证不在本建议书的讨论范围内。

7.1.14 模型T-14

当多身份服务提供者提供采用不同因素的组合认证方法时，以及当多身份服务提供者、一个服务提供者以及多个终端通过网络互相连接时，采用模型T-14。在模型T-14中，一个或多个用户并不与所有IdSP建立信任关系。

注 – 模型T-14中存在IdSP同所有用户之间均无信任关系的情况，但是包含此类IdSP的模型不在本建议书的讨论范围之内。

当服务提供者从终端接收到服务请求时，服务提供者从一组IdSP中选择与用户建有信任关系的单一或多身份服务提供者来满足所要求的认证保证，并请求其对用户进行认证。若所有从IdSP返回的认证结果均显示用户成功通过认证，则服务提供者向终端提供其服务。

本模型可以提供任何类型的组合认证方法。

7.2 实体认证生命周期模型

实体认证生命周期模型是[ITU-T X.1254]所定义的实体认证阶段的状态转换模型。

该模型有两种类型：用户角度的生命周期模型以及服务提供者角度的生命周期模型。

7.2.1 用户角度的生命周期模型

在用户角度的生命周期模型的认证过程中，认证状态包含四个节点：“未认证”，“已识别”，“已验证”以及“已注销”（图2）。

初始认证状态为“未认证”。

当用户发出一次认证请求并被IdSP所识别时，状态由“未认证”转为“已识别”。

用户一旦通过IdSP的认证，状态即由“已识别”转为“已验证”。

此外，如果用户发出注销请求，或者用户已被认证且状态已经为“已验证”之后又经过了一段时间，则状态由“已验证”转为“已注销”。

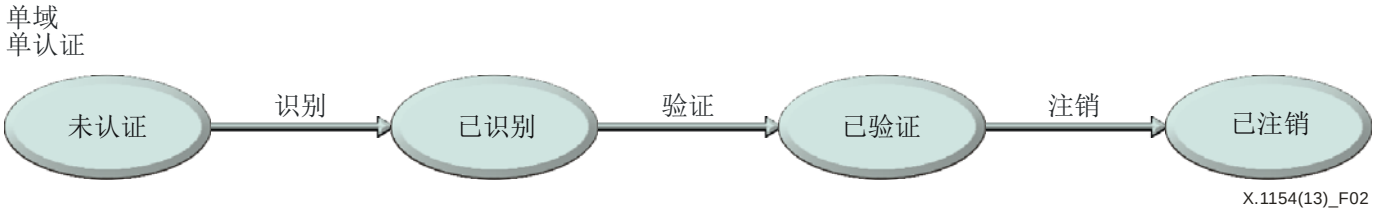


图2 – 单因素认证的状态转换

如果是组合认证，则从“已识别”至“已验证”的状态转换是不一样的（图3）。

在组合认证过程中，IdSP或者服务提供者管理用户当前的认证保证。

当用户成功通过单因素认证时，则更新当前的认证保证并评估其是否符合所要求的认证保证。

如果当前的认证保证符合要求，则状态由“已识别”转为“已验证”。

此外，如果用户发出注销请求，或者用户已被认证且状态已经为“已验证”之后又经过了一段时间，则状态由“已验证”转为“已注销”。

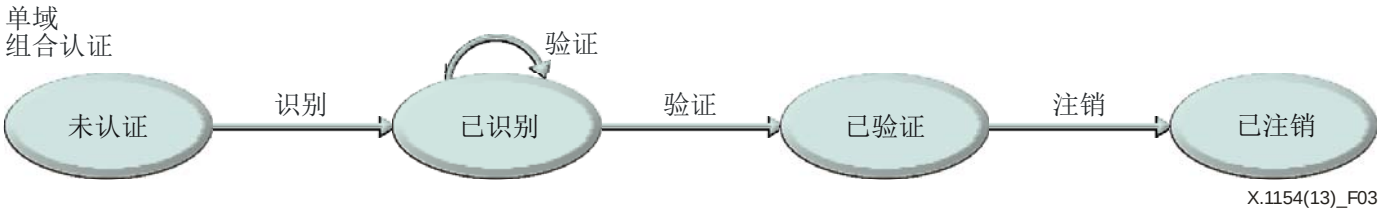


图3 – 单域中组合认证的状态转换

如果组合认证存在于包含不同认证保证要求的多域中，如模型T-4，T-6以及T-8，则状态转换如图4所示。

第一域中的状态转换与图3相同，其他域的状态转换不同。

当第一域的状态为“第一域已验证”且用户向第二域发出认证请求时，如果用户被第二域所识别，则第二域的状态变为“第二域不充分”。如果用户当前的认证保证符合第二域中所要求的认证保证，则状态由“第二域不充分”变为“第二域已验证”。

否则，用户通过IdSP（或服务提供者）的认证，并对当前认证保证进行更新并评估其是否符合所要求的认证保证。之后，如果用户向任一域发出注销请求，则所有域的状态统一由“已验证”变为“已注销”。

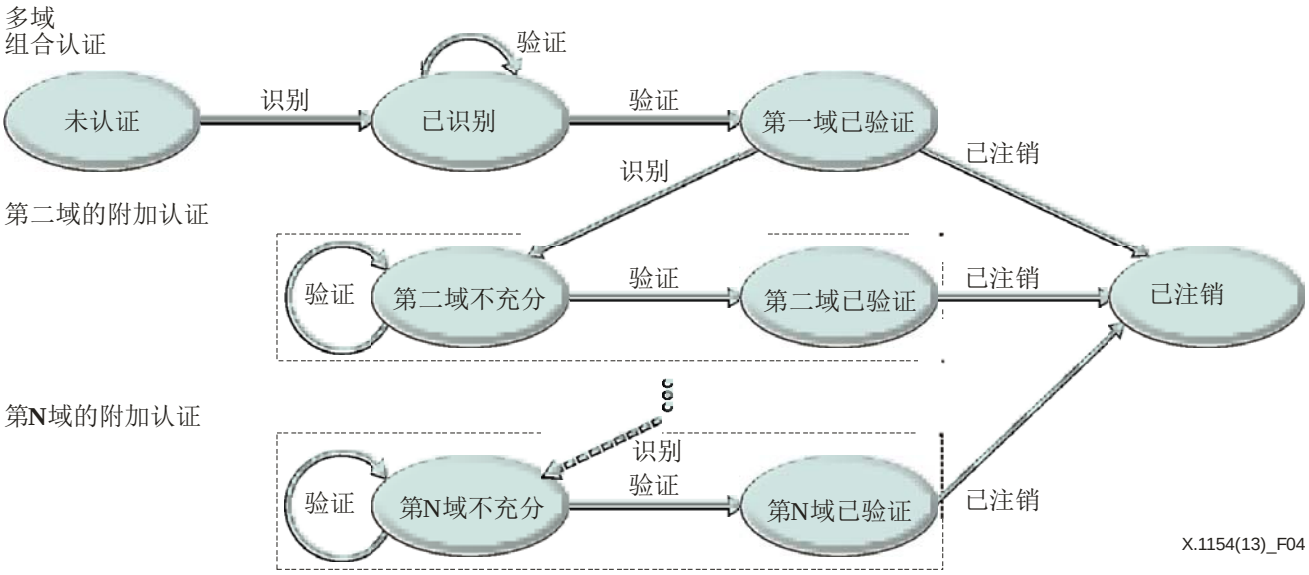


图4 – 认证保证要求不同的多域中组合认证的状态转换

多域联合情况下的组合认证状态转换关系如图5所示。这与模型T-4，T-6，T-8中具有不同认证保证要求的多域中的组合认证情况相同。

第一域中的状态转换与图3及图4相同。

当第一域中的状态为“已验证”且用户向第二域发出认证请求时，用户得到第二域的认证但是状态不发生改变。

之后，如果用户向任一域发出注销请求，则所有域的状态均由“已验证”变为“已注销”。

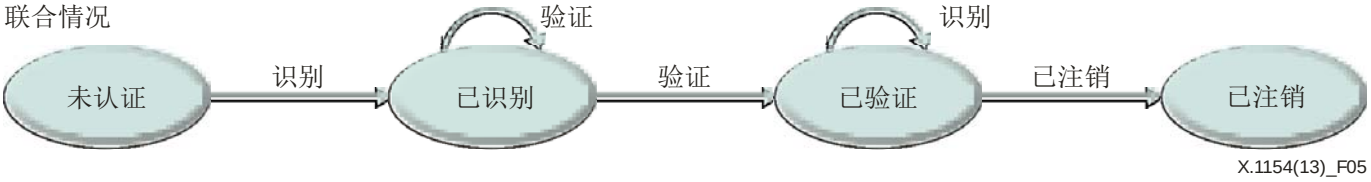


图5 – 多域联合条件下组合认证的状态转换

7.2.2 服务提供者角度的生命周期模型

在服务提供者角度的生命周期模型的认证过程中，认证状态同样包含四个节点：“未认证”，“已识别”，“已验证”以及“已注销”（图6）。

初始认证状态为“未认证”。

当服务提供者收到一次认证请求并识别出用户身份时，状态由“未认证”转为“已识别”。在此阶段之后，如果用户通过IdSP的认证，则状态由“已识别”转为“已验证”。

此外，如果SP收到退出请求，或者用户已被认证且状态已经为“已验证”之后又经过了一段时间，则状态由“已验证”转为“已注销”。

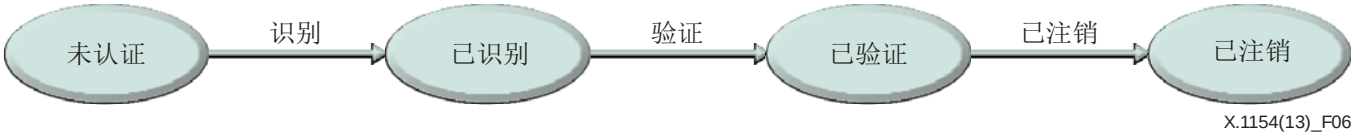


图6 – 单因素认证中的状态转换

在组合认证中，从“已识别”到“已验证”的状态转换有所不同。

在组合认证过程中，IdSP或者服务提供者管理用户当前的认证保证。

当用户成功通过IdSP的认证时，则更新当前的认证保证并评估其是否符合所要求的认证保证。

如果当前的认证保证符合要求，则状态由“已识别”转为“已验证”。

此外，如果用户发出注销请求，或者用户已被认证且状态已经为“已验证”之后又经过了一段时间，则状态由“已验证”转为“已注销”。

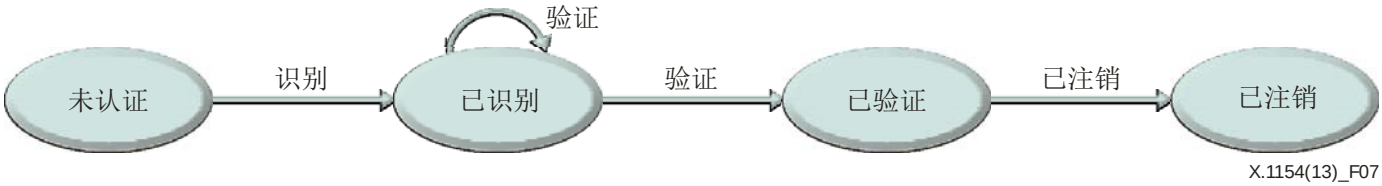


图7 – 组合认证中的状态转换

从服务提供者的角度来看，这与用户访问多域以及联合域的情况中的组合认证没有差异。

8 多重IdSP环境下的操作

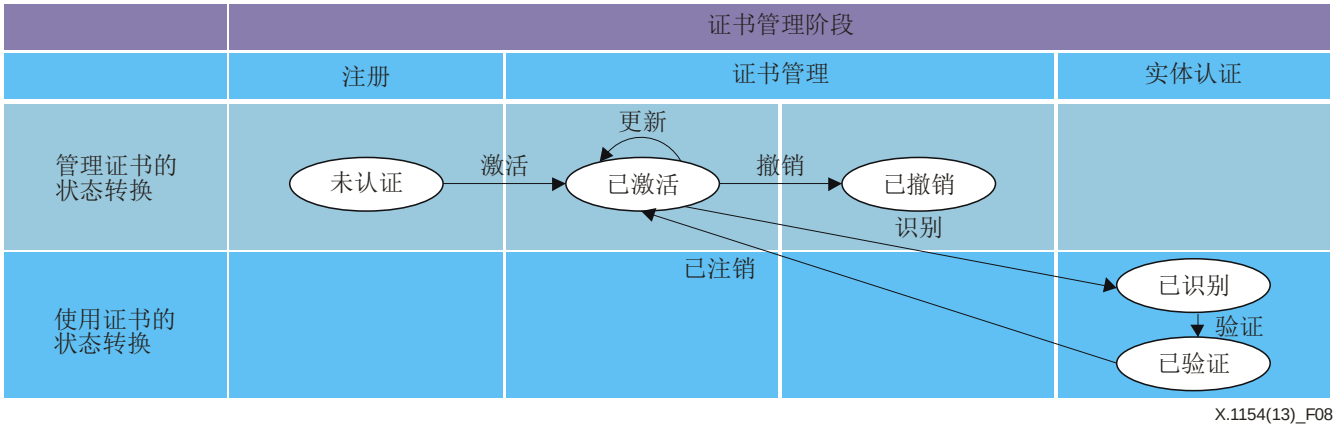


图8 – 用户的操作

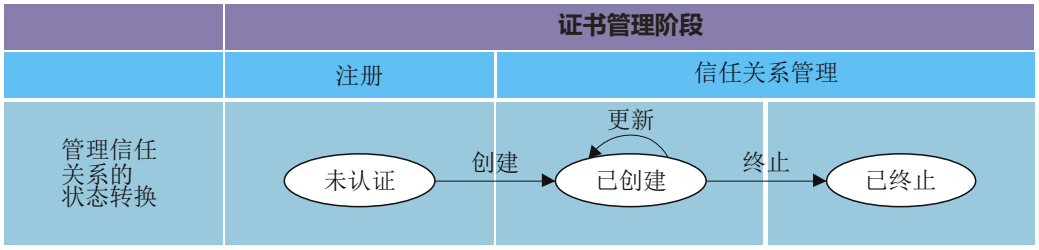


图9 – 服务提供者的操作

在第7节提到的模型中涉及了以下类型的IdSP操作：

1) 证书的管理操作（图8），

2) 证书的使用操作（图8），

3) 对与服务提供者之间的信任关系的管理操作（图9）。

8.1 证书的管理操作

证书的管理操作指用户为管理其证书的生命周期而进行的操作，具体如下：

1) 激活

激活操作执行证书的激活过程来指定用户的证书，定义于[ITU-T X.1254]。

2) 更新

更新操作执行证书的更新过程来指定用户的证书，定义于[ITU-T X.1254]。

3) 撤销

撤销操作执行证书的撤销过程来指定用户的证书，定义于[ITU-T X.1254]。

8.2 证书的使用操作

如果证书被激活，即可执行使用操作。证书的使用操作指为了进行用户识别/认证以及为用户认证终止由该操作生成的断言而进行的操作。

1) 识别

识别操作指识别用户。

本操作用于实体认证阶段。

2) 验证

认证操作指基于所呈递的证书判断通信对端是否为所宣称的用户。如通信对端通过认证，则为其生成一次断言。

本操作用于实体认证阶段。

3) 注销

退出操作之后断言过期。

本操作用于使用阶段。

8.3 对服务提供者之间的信任关系的管理操作

对服务提供者之间的信任关系的管理操作是指为了创建以及消去与服务提供者之间的信任关系，由服务提供者所执行的操作。

1) 创建

创建操作将创建与某一服务提供者之间的新的信任关系。

本操作用于信任关系注册阶段。

2) 更新

更新操作将更新已存在的与某一服务提供者之间的信任关系。

本操作用于信任关系的管理阶段。

3) 终止

终止操作将销毁与某一服务提供者之间指定的信任关系。

本操作用于信任关系的管理阶段。

9 多身份服务提供者环境下的组合认证通用框架

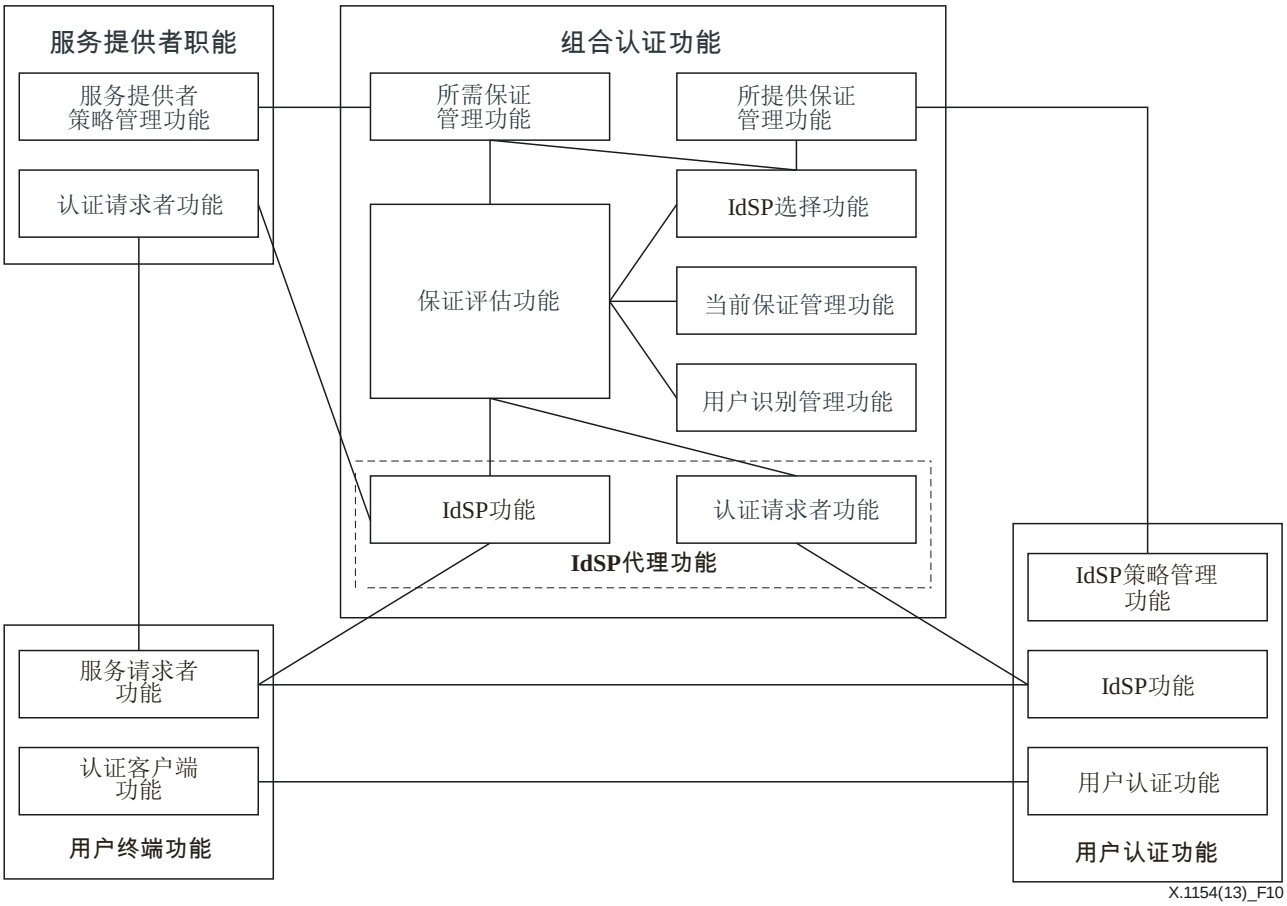


图10 – 多身份服务提供者环境下的组合认证通用框架模型

在图10中，组合认证的通用框架包含了四个逻辑模块：用户认证模块，服务提供者模块，用户终端模块，以及组合认证模块。

9.1 逻辑组件

9.1.1 用户认证功能

用户认证功能包含三个功能：用户认证功能，IdSP功能和IdSP策略管理功能。

用户认证功能指执行验证操作并认证用户的功能。

IdSP功能指从组合认证功能（的一个认证请求者功能）处收到认证请求并执行识别操作的功能。此外，IdSP功能也负责接收注销请求并执行注销操作。

IdSP策略管理功能指管理一个由用户认证模块所提供、且包含一种认证方法以及一个认证保证水平的IdSP认证策略的功能。

9.1.2 服务提供者功能

服务提供者功能包含两个功能：认证请求者功能和服务提供者策略管理功能。

认证请求者功能指将一份认证请求发送给组合认证功能块中（的IdSP功能）的功能。

服务提供者策略管理功能管理服务提供者认证策略，该策略包含一个提供服务所需的认证保证水平。

9.1.3 用户终端功能

用户终端功能包含两个功能：服务请求者功能和认证客户功能。

服务请求者功能指将一次服务请求发送到服务提供者模块（的一个认证请求者功能）。

认证客户功能指与单因素认证功能（的一个用户认证功能）进行沟通以认证用户的功能。

9.1.4 组合认证功能

组合认证功能包含八项功能：IdSP功能，认证请求者功能，所需保证管理功能，所提供保证管理职能，当前保证管理职能，用户身份管理功能，保证评估功能以及IdSP选择功能。

IdSP功能指从服务提供者功能（的一个认证请求者功能）收到一个认证请求并执行识别操作的功能。此外，IdSP功能也接受服务终止请求并执行注销操作。

认证请求者功能是将认证请求或者注销请求发送到（IdSP功能的）单因素认证功能的功能。

所需保证管理功能是通过建立/更新/终止操作来管理各服务提供者功能所需求的认证保证水平的功能。

所提供保证管理功能是通过建立/更新/终止操作来管理由各单因素认证功能提供的一种认证方法以及一个认证保证水平的功能。

当前保证管理功能是管理各用户当前认证保证水平的功能。

用户身份管理功能是通过创建/更新/撤销功能来管理每个用户身份信息的功能。

保证评估功能是验证由每个单因素认证功能的IdSP功能提供的用户认证结果、评估用户的当前保证水平并检查用户当前保证水平是否满足服务提供者所需保证水平的功能。

IdSP选择功能是为用户选择一种或多种单因素认证功能，以此来满足服务提供者所需保证水平的功能。

需要指出的是，一些现有身份管理（IdM）框架能够使用另外的功能代替IdSP功能和认证请求者功能来识别服务桥提供者功能。

9.2 行为

9.2.1 服务请求

图11给出了在多身份服务提供者环境下、在组合认证的通用框架中进行一次服务请求的基本行为。

1) 服务请求者功能将服务请求发送给服务提供者功能中的认证请求者功能。

2) 如果认证请求者功能判断用户终端功能需通过认证才能提供应用服务，服务提供者模块中的认证请求者模块收到服务请求之后，向组合认证模块中的IdSP模块发送一次认证请求。

3) IdSP功能收到服务请求之后，发送认证请求到保证评估模块。

4) 保证评估功能从当前保证管理模块中检索用户终端的当前保证水平，然后将一个IdSP选择请求和用户终端的当前保证给一个IdSP选择功能。

5) IdSP选择功能会检索服务提供者所需要的保证水平，分别给予所需保证管理功能和所提供保证管理功能中的每个IdSP一个保证水平。之后，IdSP选择功能会从一系列可用的IdSP中选择一个并把其名称发送回保证评估功能。

6) 保证评估功能会在被选择的IdSP功能里，从用户身份管理功能检索出一个用户终端中心的标识，如有必要，它会发送一个认证请求给服务请求审核功能。此外，服务请求审核功能会针对被选择的IdSP功能给IdSP中心发送一个认证请求。

7) IdSP中心会发送认证请求给认证功能，另外，认证功能会跟用户终端中心上的认证用户执行用户认证。

8) 认证功能会把认证结果通过IdSP功能群中的一个及在联合验证中心的服务请求功能，发送给保证评估功能。

9) 保证评估功能会评估并升级用户终端的保证水平。

10) 如果用户终端的保证水平不足以提供服务（比要求的水平低），那么保证评估功能就会再一次请求IdSP选择功能重新选择一个。然后，步骤（5）至步骤（9）将被重复。

11) 如果用户终端中心的目前保证水平足以提供在步骤（10）当中的服务，那么保证评估功能就会向IdSP功能发送审核结果。

12) IdSP功能会编制一个断言然后把它发送给服务提供功能的验证请求者。

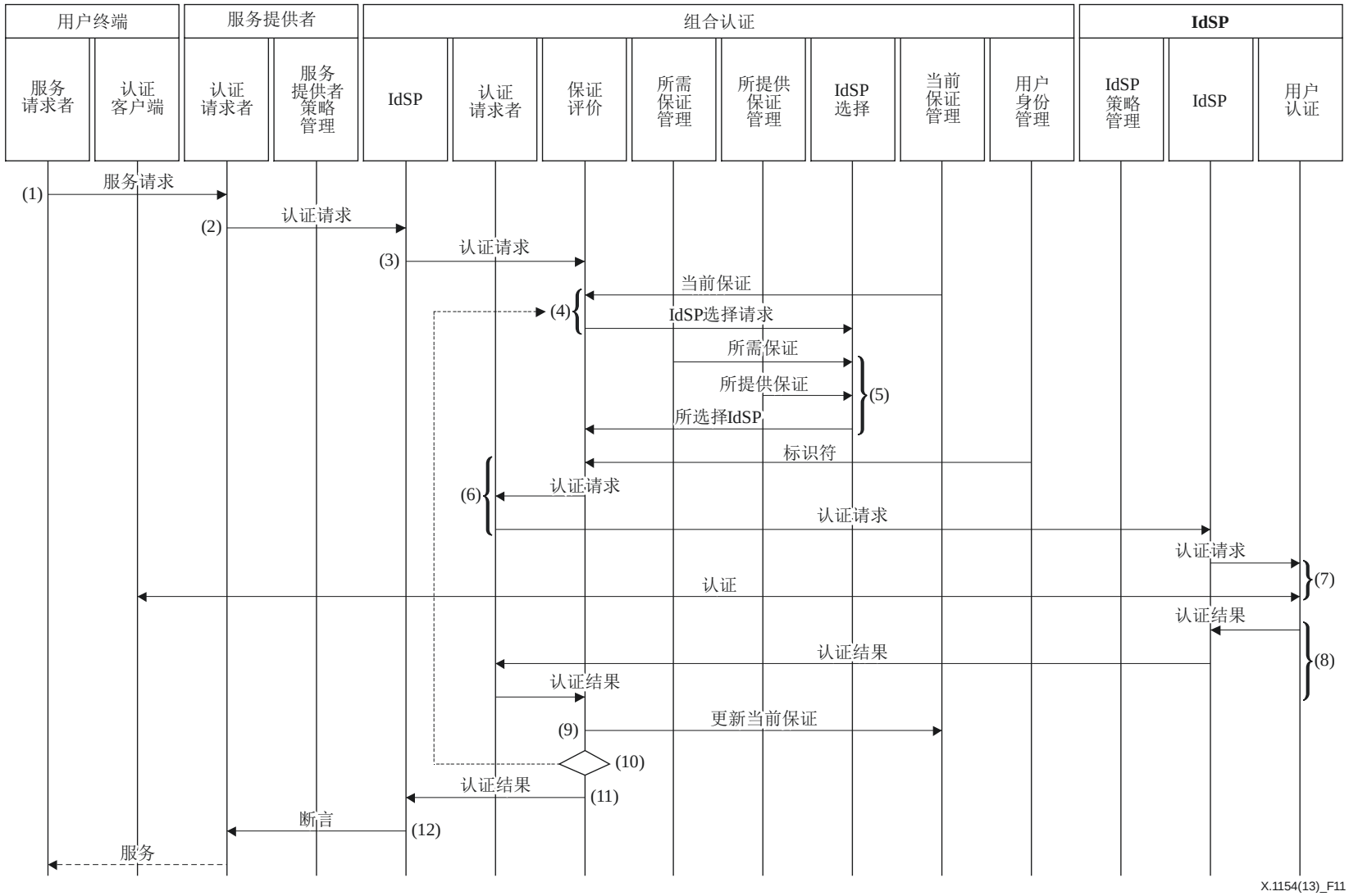


图11 – 多身份服务提供者环境下组合认证通用框架中的服务终止的基本行为表格

9.2.2 服务终止

图12给出了在提供多重身份服务的环境里，在联合身份验证中心的基本框架中进行服务终结的基本行为准则。

1) 一个服务请求者功能发送服务终结请求到服务提供者功能的认证请求功能。
2) 当服务提供者功能中的认证请求功能收到服务终止请求后，它会发送一个注销请求到合并认证中的IdSP功能。
3) 当IdSP功能收到注销请求，它会给保证评价功能发送一个终止请求。
4) 保证评价功能会检索一系列用户登陆的IdSP，并通过认证请求者功能发送注销请求给所有被列出的IdSP功能。
5) IdSP功能回复一个注销结果。
6) 当保证评价功能收到注销结果后，当前保证水平得到更新。
7) 如果保证评价功能收到所有注销结果，则它会将终止结果发还给IdSP功能。
8) IdSP功能将会把注销结果发还给身份认证请求功能。
9) 身份认证请求功能将服务终止结果发还给服务请求者。

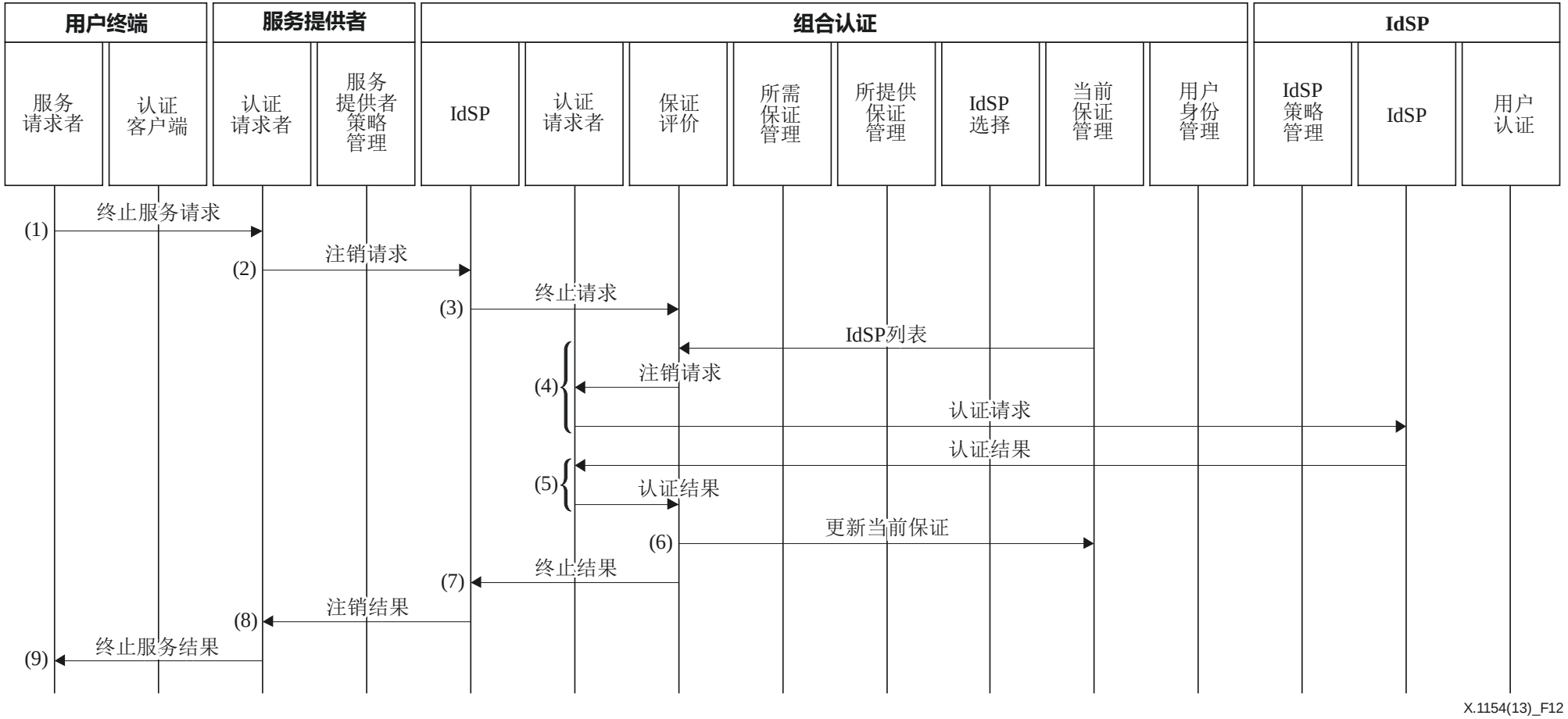


图12 – 多身份服务提供者环境下组合认证通用框架中的服务终止的基本行为

9.2.3 服务提供者功能所需的保证管理

为了对合并认证功能的服务提供者功能所需的保证进引管理，服务提供者策略管理功能通过建立/更新/终止操作，发送一个所需的保证到所需的保证管理功能。

9.2.4 IdSP功能所提供的保证管理

为了对合并认证功能的IdSP功能所提供保证进引管理，IdSP政策管理功能通过建立/更新/终止操作，发送所需的保证到所提供的保证功能。

附件A

组合认证的注意事项

（本附件是本建议书的组成部分）

A.1 达到预期的认证保证

由于组合身份认证是一种使用多种凭证的认证方式，所以需要不同的凭证的来达到预期认证保证。换句话说，如果仅使用相同的凭证，简单的多认证方式或IdSP组合相同会导致保证水平彻底失效。

为了实现预期的认证水平，需要一种验证组合认证中所使用的凭证是否相同的过程。建议在更新当前认证保证水平之前来实施这一验证过程。

在集组合认证功能和用户认证功能于一体的模型中，（例如，一个IdSP提供一种组合认证），很容易在IdSP中实现验证过程。此外，验证过程还可以在执行创建或更新操作时实施。

另一方面，在集组合认证功能和用户认证功能于一体的模型中（例如SP使用能提供单因素认证的多个IdSP），认证过程需要组合认证功能和用户认证功能之间进行其他数据交换。具体地说，用户认证功能中需要有发送数据识别凭证的功能。此外，在组合认证功能中，需要有通过比较来自用户认证功能的数据来确认使用了不同凭证的功能。

对于在公钥基础设施（PKI）的基础上使用认证方法这类情况，用户认证模块中的功能可以发送公钥作为显示证据的数据，并且在组合认证模块中的功能可以直接比较这些数据。

然而，对于身以共享秘密（如，口令）为基础的认证方法的情况，用户认证模块中的功能禁止发送共享秘密本身作为显示证据的数据。

A.2 IdSP的选择

当服务提供者受到来自终端的服务请求时，要求IdSP选择功能发现并选择合适的IdSP。

为了选择合适的IdSP，要求安全实施所需的保证管理功能和所提供的保证管理功能。

此外，要求在IdSP（一个IdSP提供一种组合认证功能的模型）或SP（SP提供组合认证功能的模型）中安全实施当前的保证管理功能。

进一步来说，要求保证评价功能应能安全地恢复当前的认证保证，所需的保证和所提供的保证。

A.3 有效身份认证保证

在某些情况下，有效身份认证保证可能会低于预期的身份认证保证，这是因为认证保证可能会因各种不同环境因素的影响而发生变化。

在这类情况下，IdSP中需要有向SP发送有效认证保证的功能。进一步说，SP中需要一个根据有效认证保证来来更新和评估用户当前认证保证的功能。

A.4 多因素认证的安全考虑

有两种多因素认证类型：一种是使用单一凭证进行验证的多因素认证方式，另一种是利用多种凭证进行验证的认证方式。

第一种认证方式是基于存储在智能卡中的公钥或基于使用硬件设备的一次性口令。

第二种认证方式是基于一次性口令和生物因素的组合。

第一种多因素认证方式需要使用防篡改硬件来存储凭证。

A.5 多方法认证的安全考虑

对于多方法认证这类情况，要求每个凭证都不能利用其他凭证加以推断（或猜出）。

A.6 多重身份认证的安全考虑

要求每个凭证都不能利用其他凭证加以推断（或猜出）。

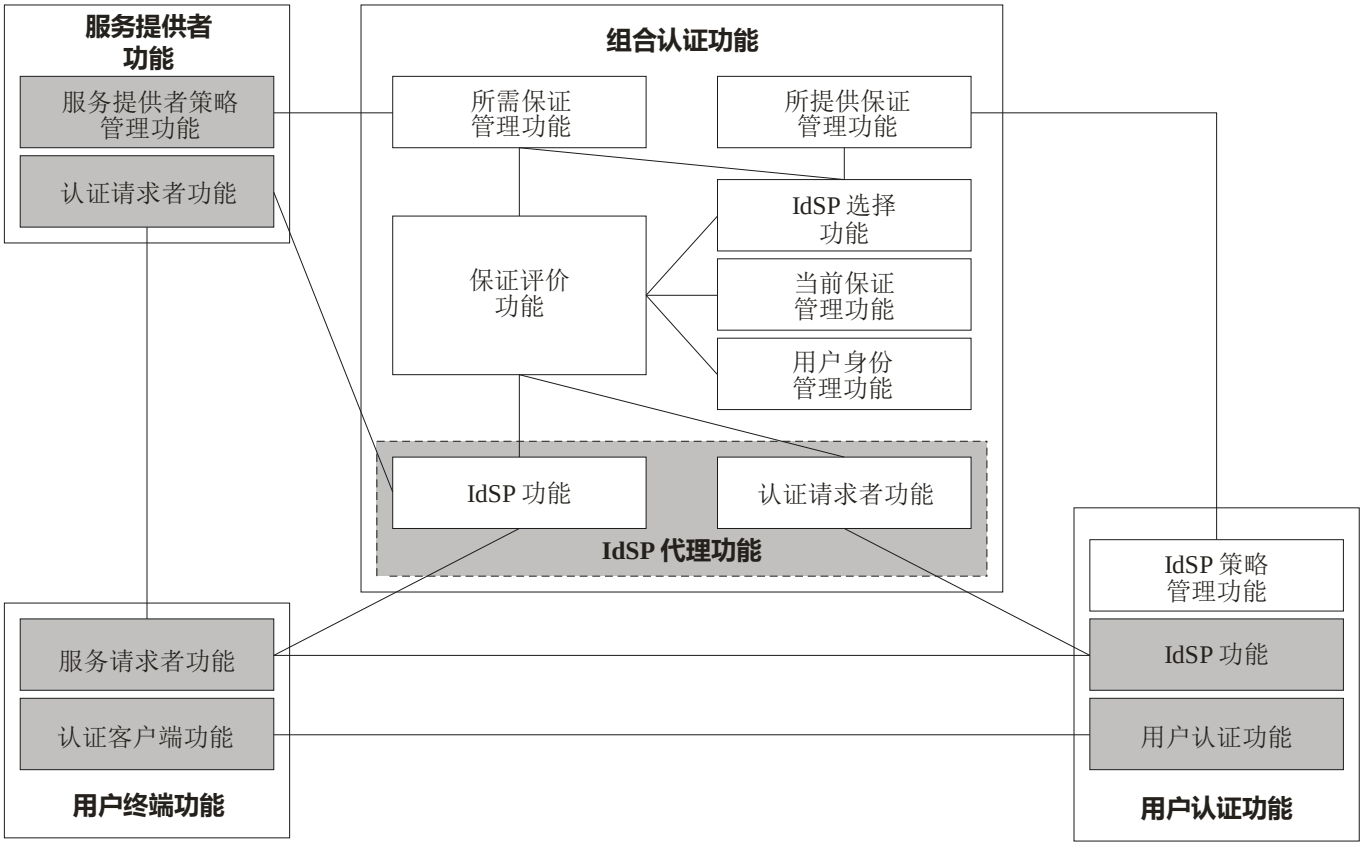
附录一

与相关标准的关系

（本附录不构成本建议书的组成部分）

I.1 与[ITU-T X.1141]的关系

图I.1给出了本建议书所介绍的模型与[ITU-T X.1141]建议书第10节和安全断言标记语言（SAML 2.0）中所介绍模型之间的关系。其中灰色框中为SAML所定义的模块。



图I.1 – 与[ITU-T X.1141]的关系

X.1154(13)_FI.1

I.2 与[ITU-T X.1254]的关系

本建议书中的框架用于提供用多重 IdSP 进行组合认证。也就是说，本建议书中的框架是[ITU-T X.1254]建议书所介绍的多重 IdSP 环境下执行认证过程的一个具体实例。

参考资料

[b-ITU-T X.509] ITU-T X.509建议书 (2008) | ISO/IEC 9594-8:2008，信息技术 – 开放系统互连 – 《号码簿：公共密钥和属性证书框架》。

[b-ITU-T X.1084] ITU-T X.1084建议书 (2008)，电信生物系统机制 – 第1部分 – 《电信系统的一般生物认证协议和系统模型轮廓》。

[b-ITU-T X.1086] ITU-T X.1086建议书 (2008)，电信生物保护程序 – 第1部分 – 《生物特征识别数据安全的技术和管理对策的指南》。

[b-ITU-T X.1089] ITU-T X.1089建议书(2008)，《电信生物特征识别认证基础设施（TAI）》。

[b-ITU-T X.1151] ITU-T X.1151建议书 (2007)，《利用密钥交换实现的基于口令的安全认证协议的指导原则》。

[b-ITU-T X.1252] ITU-T X.1252建议书 (2010)，《身份管理基准术语定义》。

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
2013年，日内瓦