国 际 电 信 联 盟

ITU-T X.1258

（09/2016）

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

网络空间安全 – 身份管理

基于聚合属性的增强型实体认证

ITU-T X.1258 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
远程生物特征测定	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	
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.1258 建议书

基于聚合属性的增强型实体认证

摘要

可能确有必要利用多属性机构提供的聚合属性，提升依赖方对其它方身份的信任度。聚合可视作必须处理一系列适用于全局的唯一标识符，这在所有属性机构之间十分常见。实践过程中，各实体并无全局统一的标识符，而是拥有不同的实体标识符和其它各种身份服务提供方（IdSP）分配的属性。

为解决此方案中的属性聚合问题，本文使用了身份联盟的概念。例如，若某网上书店计划向老年人出售产品，则该商店必须由两个IdSP分配一套聚合属性（信用卡和年龄段），但各IdSP之间相互并不了解对方的参与情况。在标准的联盟身份管理中，某实体只能提供来自一个身份的属性，但此交易要求两个身份均提供属性。目前存在多种身份联盟方法，例如安全断言标识语言（SAML）、Shibboleth、开放（OpenID）和公开鉴权（OAuth）等。

ITU-T X.1258建议书引入了属性聚合概念，使实体能够聚合来自多个IdSP的属性。属性聚合是一种收集某实体从多个IdSP那里检索到的属性的机制。属性聚合可用于按需动态汇聚各种属性。当某实体希望获得服务时，IdSP可实现聚合请求。此外，以实体为中心的属性聚合机制亦可用于缓解隐私泄露的鉴权。

沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1258	2016-09-07	17	11.1002/1000/12850

关键词

属性聚合，联盟身份管理。

* 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.1258 建议书

基于聚合属性的增强型实体认证

1 范围

本建议书介绍了基于各域实体属性聚合的增强型认证，包括以下内容：

– 多身份服务提供方（IdSP）属性的聚合方法；和

– 基于聚合属性的增强型认证。

2 参考文献

无。

3 定义

3.1 他处定义的术语

本建议书采用了下列其它资料定义的术语：

3.1.1 属性[b-ITU-T X.1252]：针对实体并说明该实体特性的信息。

3.1.2 （实体）认证[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。

注 – 在身份管理（IdM）语境中，使用术语认证是指实体认证。

3.1.3 信任圈[b-ITU-T X.1251]：为加入一个联盟内组织而建立的一套标准，目的是为能可信地使用相互的资源。请注意，信任圈也是加入一个联盟内组织的最终结果。

3.1.4 联盟[b-ITU-T X.1252]：用户、服务提供方和身份服务提供方的联合会。

3.1.5 身份[b-ITU-TX.1252]：以一个或多个属性表示实体，使实体足以在语境内得到区分。至于身份管理（IdM）的目的，术语身份可以被理解为语境下的身份（属性的子集）即，属性的多样性受限于实体存在和互动的边界条件（语境）的框架。

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，可能的属性数量是无限的。

3.1.6 身份服务提供方（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。

3.2 本建议书定义的术语

本建议书定义下列术语：

3.2.1 属性聚合：一种从多个身份服务提供方（IdSP）那里收集属性的机制。

注 – 属性一旦被收集后即需要被聚合和断言，用于认证和授权。

3.2.2 域：单个身份服务提供方的管理覆盖范围。

3.2.3 服务提供方（SP）：向客户或其他服务提供方提供服务的实体。

4 缩写词和首字母缩略语

本建议书使用了下述缩写词和首字母缩略语：

CoT 信任圈

DB 数据库

ID 身份

IdM 身份管理

IdSP 身份服务提供方

LS 关联服务

OAuth 开放认证

OpenID 开放身份

PKI 公开密钥基础设施

SAML 安全断言标识语言

SP 服务提供方

SSO 单点登录

VC 虚拟协作

5 惯例

无。

6 概述

总的来说，电子身份管理（IdM）涵盖了对任何数字身份形式的管理。IdM可能起源于号码簿的开发，如[b-ITU-T X.500]所支持的那些。[b-ITU-T X.509]定义了包含身份属性的证书。[b-ITU-T X.509]的证书和公开密钥基础设施（PKI）系统用于证明对象的在线“身份”。因此，IdM可以被认为是对信息的管理。

一个实体的身份可能包含该实体在不同语境下的各类属性。根据语境和情况的不同，可能需要不同的身份。IdM为数字世界中此类身份的管理提供了工具。IdM包含一整套的功能和能力，如身份的创建/删除、信息的发现和交换。在真实世界中，人们会根据信息的语境和敏感性来选择哪些信息可以透露给他人。同理，在数字世界中，这一任务是由IdM来完成系统的。

基于IdM的各类技术和标准，IdM系统方法可以分为传统、集中和联盟三大类。传统方法的特点是由服务提供商（SP）负责身份的处理并与身份服务提供方（IdSP）相配合。实体会为其想要获取服务的每一个SP创建一个数字身份（ID）。通常情况下，实体ID不会在各SP之间共享，这种方式对于实体和SP来说成本都更加高昂。每一个SP可能会多次要求有自己的一套属性，以构成实体的数字身份。

集中式方法主要用于解决传统方法的不灵活性，身份可以在各SP之间共享，它基于单一认证、单点登录（SSO）概念。这种方法试图避免传统方法所带来的不一致和冗余，使实体有能力在无需冗余认证的情况下与各SP交互。

与IdSP结成信任关系的每一个SP均会完全依赖于该IdSP所提供的实体认证。IdSP负责对实体进行认证，并在可以代表公司、大学等的域内向SP提供实体属性信息，由实体、多SP和单一IdSP组成。单一认证（SSO）为实体提供了极大的便利，因为仅需认证一次即可。之后，实体可以将所获得的证书用于其希望接入的所有SP。然而，集中式方法的缺点是IdSP拥有对其实体信息的绝对控制权，可以任意使用其信息。这也是为什么集中式方法没有被广泛采用的主要原因。

为解决集中式方法所带来的问题，在多IdSP认证任务分配的基础上引入了联盟身份方法。此类IdSP属于不同的域。联盟身份的概念依赖于IdSP和对应域之间的信任关系。要想在一个IdSP和一个SP之间实现分配身份信息的互联，需要在这两方之间存在信任关系。这种信任关系被称为信任圈（CoT），可以包括一个或多个IdSP和SP。在CoT中，若用户已在一个IdSP处得到认证，则无需进一步认证即可接入CoT内的各SP。因此，用户仅需在CoT中认证一次即可[b-ITU-T X.1251]。

联盟IdM可以解决单一IdSP所带来的风险，减少在认证过程中与IdSP的信息交换。不同IdSP之间的此类协议可以确保一个域所发布的身份可以被其他域的SP所认可，且即使涉及不同的域，也可以实现SSO。

对于SP来说，联盟身份的好处是可以处理更少量的实体信息。Kantara倡议[b-Kantara]、Shibboleth [b-Shibboleth]和Higgins [b-Higgins]运用的就是联盟IdM方法。在联盟身份方法中，身份被分配到不同的IdSP，联盟的其他任何第三方（IdSP）均可使用实体信息。

7 属性聚合方法的架构和流程

早期有关多属性机构属性合并的研究认为，实体拥有一个全局的唯一标识符，这在所有属性机构之间十分常见。现实情况下，各实体并无全局统一的标识符，而是拥有不同的实体标识符和其它各种IdSP分配的属性。

Kantara倡议[b-Kantara]的前身自由联盟（Liberty Alliance）[b-Liberty]是第一个通过其身份联盟概念[b-Chadwick]来应对属性聚合问题的机构。然而，还有一个问题未得到解决，那就是多个机构所断言的缺乏一个标准的实体属性聚合方法，从而使SP用于其接入控制决策。

有几个用例可能有助于解释为什么需要属性聚合：

– 若某网上书店计划向老年人出售产品，则该商店必须由多个IdSP分配一套聚合属性（信用卡细节和老年证明）。在这种情况下，就需要实体提供来自两个身份的属性。

– 假设有一个研究员想要用联盟银行账户从一家能给教育业打折的网店购买计算机，那么他就必须要能够证明自己是教育机构的成员，而且在他的银行有一个专门的账户。需要收集存储在多个不同身份中的属性，收集的结果应传送给SP，这一过程即被称为属性聚合[b-Klingenstein]。

在动态、多机构社区内共享和协调使用资源是扩大计算机应用范围的基础，从科学协作到医疗。此类共享需要高度可控。资源提供方和消费者需清晰和谨慎定义共享的对象是什么、允许进行共享的主体是谁以及共享的条件如何。由此类共享规则所定义的一系列个人和/或机构构成了所谓的虚拟协作（VC）。为使VC能够便捷地创建和管理其所在团体的会员和角色及其资源的接入控制而进行的自我管理是一个挑战，特别是在那些共享资源位于多个机构的情况下。在VC场景下，联盟IdSP通常无法提供与参与SP有关的所有属性。此类与VC有关的属性，如VC名称、会员状态、会员邮箱清单等，需要从其他地方聚合。需要有几个不同的属性机构参与用户属性的管理[b-Hulsebosch]。

有几种身份联盟的方法：安全断言标识语言（SAML）、Shibboleth [b-Shibboleth]、Web服务联盟[b-WS-Federation]、Kantara倡议[b-Kantara]、开放身份（OpenID）[b-OpenID]、开放认证[b-OAuth]、CardSpace[b-CardSpace]和Higgins项目[b-Higgins]等。根据整个流程媒介机构的不同，属性聚合方法可分为三大类：IdSP媒介方法、SP媒介方法和实体媒介方法。

7.1 身份服务提供方媒介方法

7.1.1 身份关联

由自由联盟框架所引入的这一方法是通过身份联盟概念来应对属性聚合问题的第一批方法之一，见图1，[b-Liberty]。在图1中，IdSP允许实体在两个IdSP之间创建一个成对的关联（CoT3）。当实体在服务周围活动时，第一个IdSP（图1中的IdSP 1）就会询问该实体是否愿意将此IdSP（IdSP 1）与其他IdSP（IdSP 2）进行联盟。这时，两个IdSP就会发生交互来创建一个关联指标。在从SP处接入服务的过程中，一个IdSP会将关联指标连同包含属性的断言一起提供给SP。SP可以利用该指标从其他IdSP处收回另一个包含属性的断言。通过两个IdSP属性的结合，SP就可以确定实体是否能够接入服务。

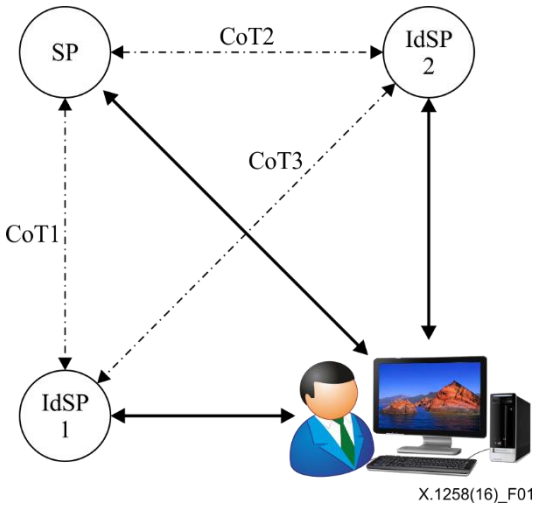
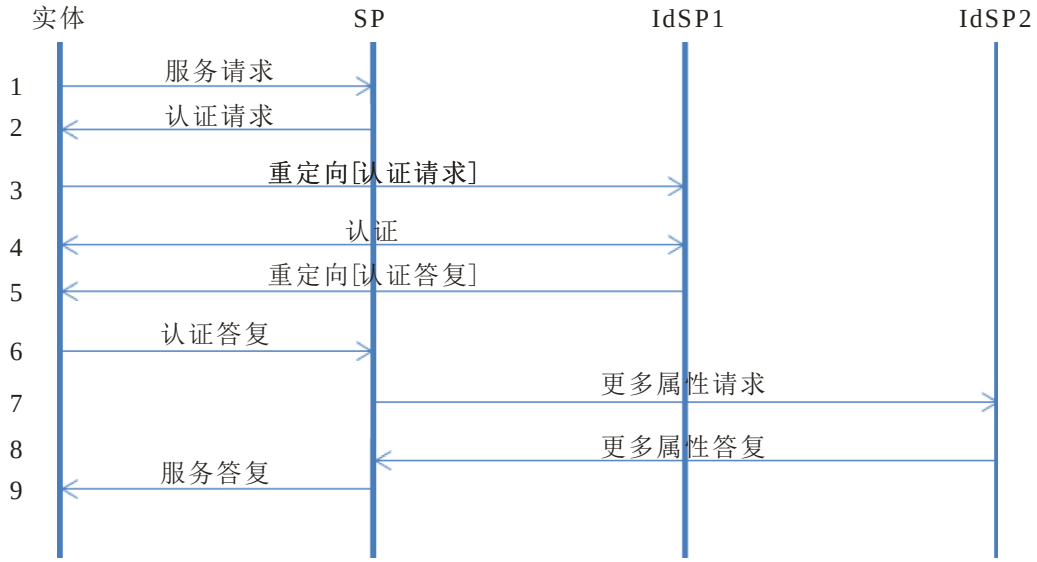


图1 – 身份关联方法架构

图2展示了身份关联方法下属性聚合的概念性控制流程：

1) 实体向SP发送服务请求。
2) 当SP需要实体服务许可时，SP会发送一个认证和认证断言请求。
3) 实体被重定向至IdSP 1进行认证。
4) IdSP 1对实体进行认证并请求更多的属性。
5) IdSP 1返回认证断言。
6) 实体向SP提交认证断言。
7) SP向IdSP 2请求更多与实体有关的属性。
8) IdSP 2提供额外的属性。
9) SP对断言进行核验，许可实体接入服务。



X.1258(16)_F02

图2 – 身份关联方法下的属性聚合流程

7.1.2 身份代理

有一个代理IdSP，且SP与其完全信任的代理IdSP之间相连；其他的IdSP不为SP所知，仅与代理IdSP（IdSP1）有信任关系，见图3 [b-Klingenstein]。若实体想要从多个IdSP处聚合属性，则实体将会首先被重定向至代理IdSP（图3中的IdSP1），然后代理IdSP会将实体重定向至其他多个IdSP。在每一个IdSP对实体进行单独认证之后，实体会把断言返回至代理IdSP。之后，代理IdSP会对每一个断言进行核验，从IdSP处收回属性，并将所有这些属性聚合。代理IdSP可以用自己的实体属性来对聚合进行补充，并重新断言。然后，代理IdSP会将所有重新断言的属性断言发送至SP。接着，SP会决定实体是否能够在聚合属性基础上接入服务。由于SP并不知道其他IdSP的存在，仅与代理IdSP结成了关系，因此它会认为所有的属性均是由代理IdSP所发出的。

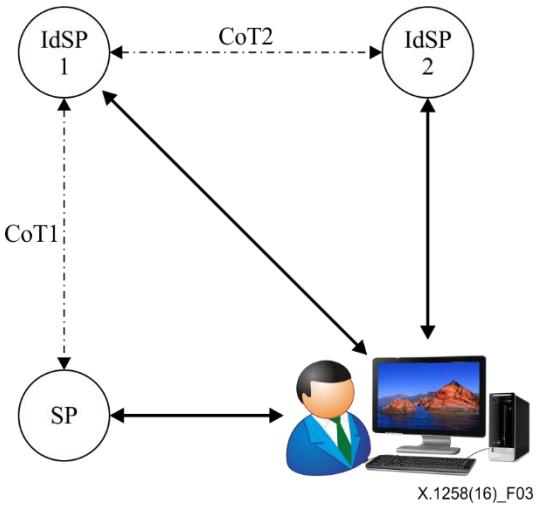
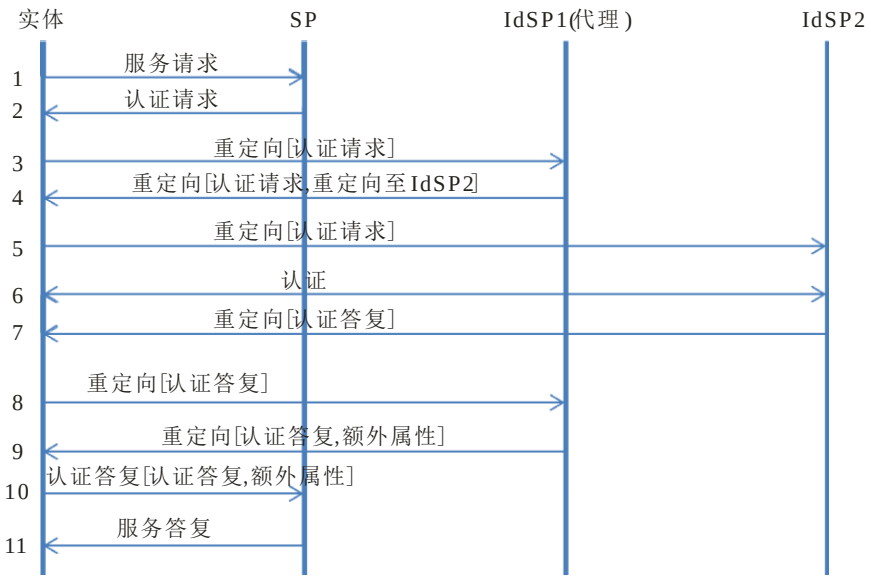


图3 – 身份代理方法架构

图4展示了身份代理方法下属性聚合的概念性控制流程：

1) 实体向SP发送服务请求。
2) 当SP需要实体服务许可时，SP会发送一个认证和认证断言请求。
3) 实体被重定向至（作为代理的）IdSP 1进行认证。
4) IdSP 1将实体重定向至IdSP 2。
5) IdSP 2收到认证和属性请求。
6) IdSP 2对实体进行认证。
7) IdSP 2返回认证结果和属性断言。
8) 实体将认证结果和属性断言转发至IdSP 1。
9) IdSP 1补充额外的属性，签署断言，并将其返回至实体。
10) 实体向SP提交断言。
11) SP对断言进行核验，许可实体接入服务。



X.1258(16)_F04

图4 – 身份代理方法下的属性聚合流程

7.1.3 身份中继

身份中继方法与代理方法类似，无需在SP和代理IdSP之间建立强信任关系。然而，代理方法需要SP对可信的IdSP完全信任；但在现实情况下，可能无法在代理IdSP和SP之间实现绝对的信任。在身份中继方法中，中间IdSP（或中继IdSP；图5中的IdSP 1）可以作为代理IdSP。之后的流程则与代理方法的流程类似，实体首先被重定向至中继IdSP，之后中继IdSP将实体重定向至其他多个IdSP。在每一个IdSP对实体进行单独认证之后，实体会把断言返回至中继IdSP。然后，中继IdSP会将所有的断言整合成一个单一的断言，并转发至SP。代理和中级模式之间的区别在于对属性断言的签署。中继IdSP不签署属性断言，但只是将原始IdSP所签署的断言进行中继。接着，SP会收到IdSP和中继IdSP的加密属性断言，决定实体是否能够在聚合属性基础上接入服务。此方法需要在IdSP和SP之间建立信任关系。

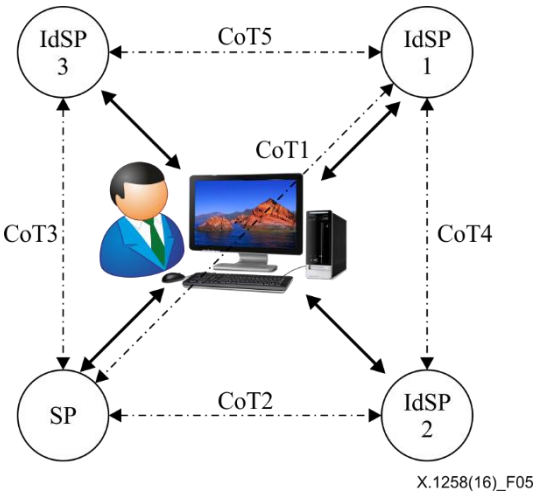


图5 – 身份中继方法架构

图6展示了身份中继方法下属性聚合的概念性控制流程：

1) 实体向SP发送服务请求。
2) 当SP需要实体服务许可时，SP会发送一个认证和认证断言请求。
3) 实体被重定向至（作为中继的）IdSP 1进行认证。
4) IdSP 1将实体重定向至IdSP 2。
5) IdSP 2收到认证和属性请求。
6) IdSP 2对实体进行认证。
7) IdSP 2返回认证结果和属性断言。
8) 实体将认证结果和属性断言转发至IdSP 1。
9) IdSP 1补充额外的属性，签署断言，并将其返回至实体。
10) 实体向SP提交断言。
11) SP对断言进行核验，许可实体接入服务。

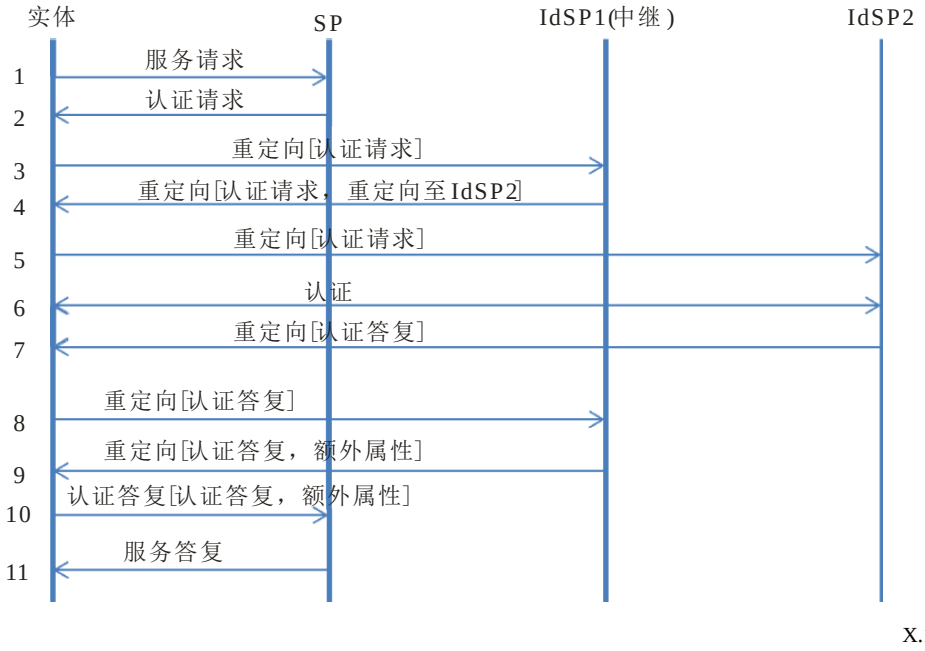


图6 – 身份中继方法下的属性聚合流程

7.2 服务提供方媒介方法

7.2.1 应用数据库

应用数据库（DB）方法是各属性聚合方法中最简单的一种，见图7 [b-Hulsebosch]。除IdSP所提供的属性外，SP会保存额外的实体属性、昵称、实体对某种服务的偏好、团体会员等。SP负责管理额外的应用属性。此外，数据库中的此类属性之后还可以由SP再取回，以决定实体是否能够接入某种服务。

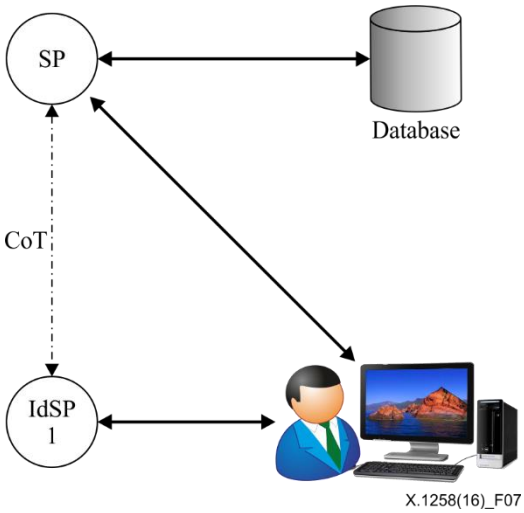


图7 – 应用数据库方法架构

图8展示了应用DB方法下属性聚合的概念性控制流程：

1) 实体向SP发送服务请求。
2) 当SP需要实体服务许可时，SP会发送一个认证和认证断言请求。
3) 实体被重定向至IdSP 1进行认证。
4) IdSP 1对实体进行认证。

5) 认证成功后，IdSP 1返回认证结果和断言。

6) 实体向SP提交认证断言。

7) 必要时，SP会从数据库中收回额外的实体属性。

8) SP对断言进行核验，许可实体接入服务。

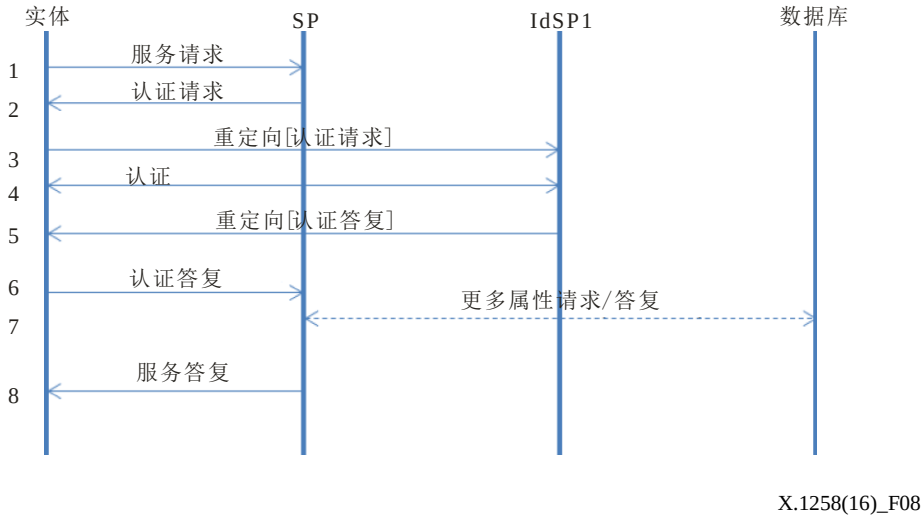


图8 – 应用数据库方法下的属性聚合流程

7.2.2 服务提供方

SP方法允许实体在一个单一会话中从多个IdSP处聚合属性，见图9 [b- Hulsebosch]。实体会被一个接一个地重定向至不同的IdSP，进行分别验证，然后将属性断言返回至SP。SP从IdSP处聚合属性断言，决定实体是否能够接入某种服务。

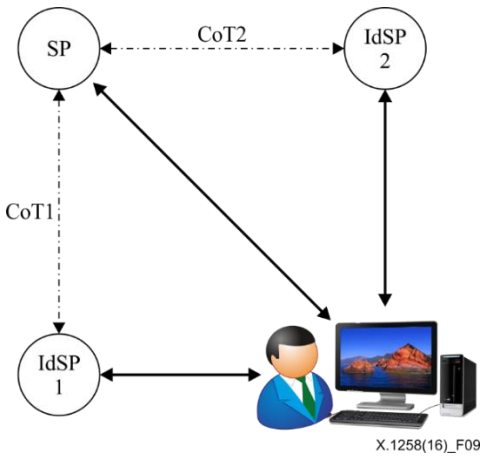


图9 – 服务提供方方法架构

图10展示了SP方法下属性聚合的概念性控制流程：

1) 实体向SP发送服务请求。

2) 当SP需要实体服务许可时，SP会发送一个认证和认证断言请求。

3) 实体被重定向至IdSP 1进行认证。

4) IdSP 1对实体进行认证。

5) IdSP 1返回认证结果和断言。

6) 实体向SP提交认证断言。

7) SP向实体索要更多与实体有关的属性。

8) 实体向IdSP 2发送更多的属性请求。

9) IdSP 2对实体进行认证。

10) IdSP 2提供额外的属性。

11) 实体向SP提交认证断言。

12) SP对断言进行核验，许可实体接入服务。

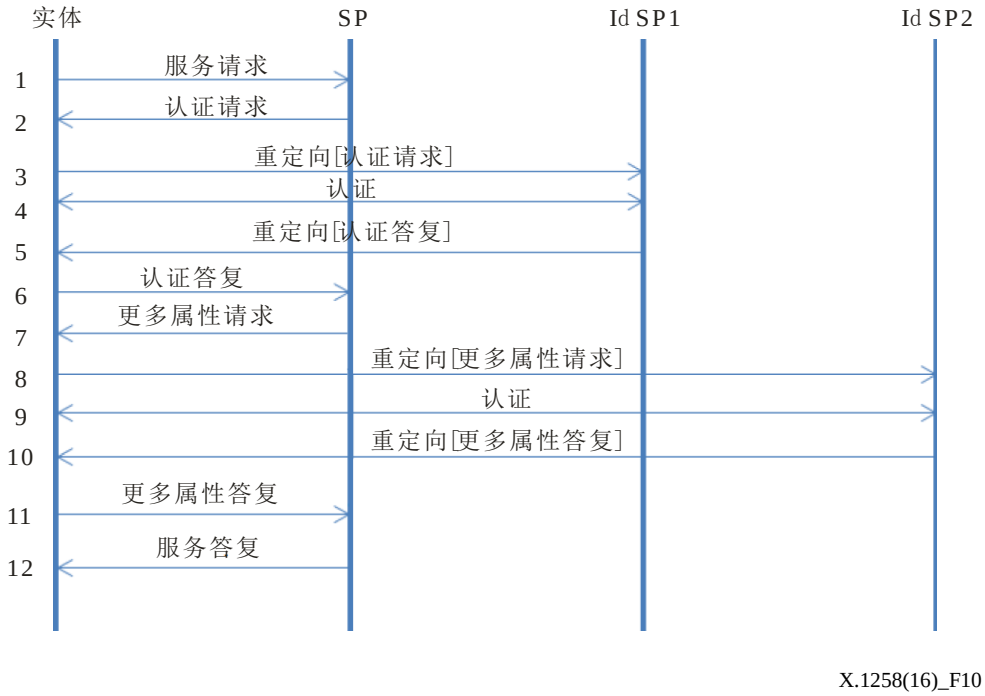


图10 – 服务提供方方法下的属性聚合流程

7.2.3 关联服务

关联服务（LS）方法是关联和身份中继方法的结合。LS是一种特殊的SP，见图11，所适用的实体使用的是由LS所提供的标识符[b-Chadwick]，[b-Hulsebosch]。由LS所提供的标识符用于关联不同的IdSP，此类IdSP使用的是关联表中由IdSP所提供的专门针对LS的持续性标识符。若实体想要接入服务，则可以访问SP，并首先被重定向至IdSP（图11中的IdSP 1）。IdSP 1对实体进行认证，之后是包含实体属性的断言，LS标识符会通过实体返回至SP。SP将标识符转发至LS，以获取更多的属性。这时，有两种选择：第一种是LS可以通过关联表收回持续性标识符的关联IdSP清单，并从各处收回属性，之后这些属性会在LS被合并起来，然后返回至SP；第二种是LS可以将关联IdSP清单发回至SP。之后，SP从每一个IdSP处收回属性。最后，SP会决定实体是否能够在聚合属性基础上接入服务。

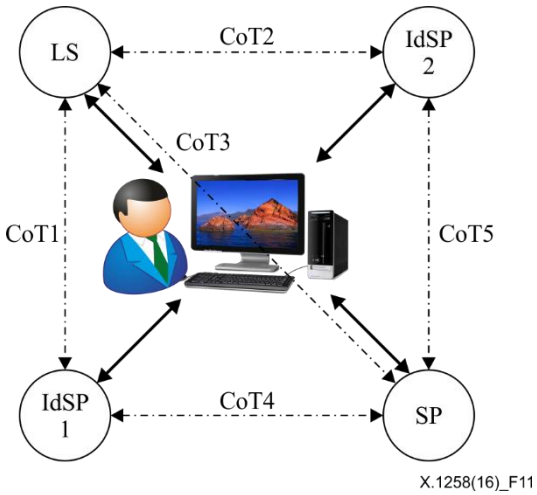


图11 – 关联服务方法架构

图12展示了LS方法下属性聚合的概念性控制流程：

1) 实体向SP发送服务请求。
2) 当SP需要实体服务许可时，SP会发送一个认证和认证断言请求。
3) 实体被重定向至IdSP 1。
4) IdSP 1对实体进行认证。
5) IdSP 1返回认证断言和LS标识符。
6) 实体向SP提交断言、LS标识符。
7) SP向实体发送更多的属性请求。
8) 实体被重定向至关联服务。
9) 关联服务向IdSP 2索要属性。
10) IdSP 2提供属性。
11) 属性返回至实体。
12) 实体向SP提交认证断言。
13) SP对断言进行核验，许可实体接入服务。

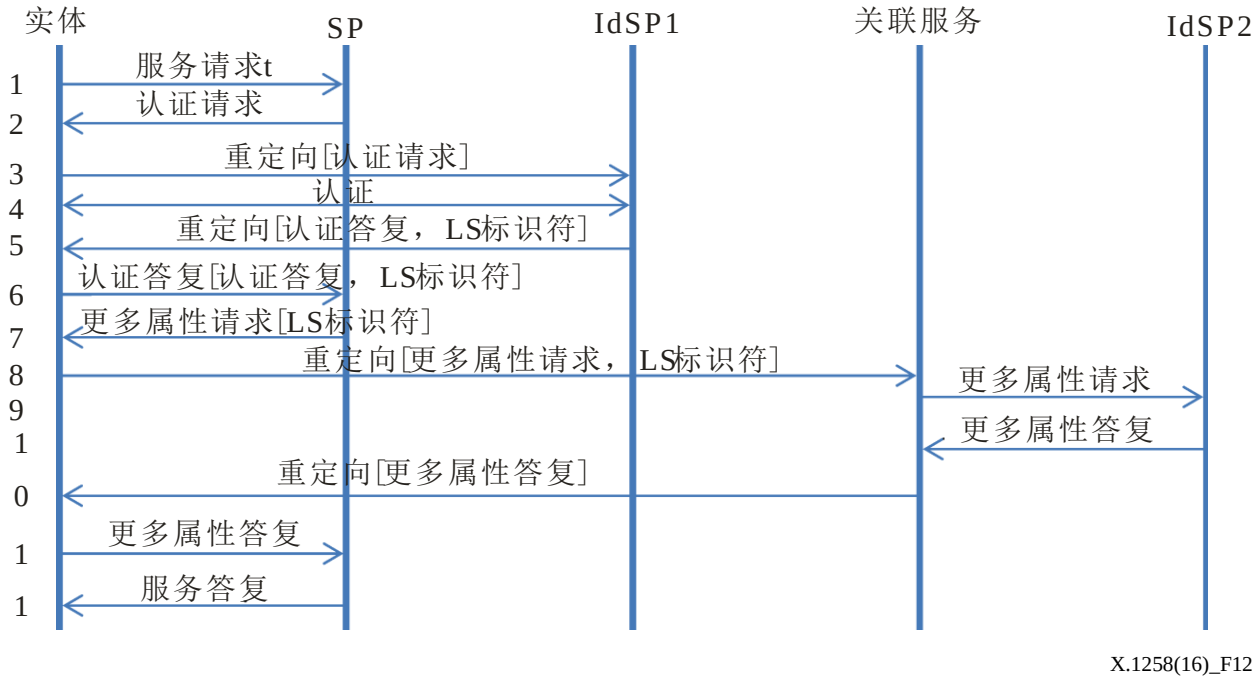


图12 – 关联服务方法下的属性聚合流程

7.3 实体媒介方法

实体媒介方法利用了有能力从不同IdSP处聚合属性的客户端（实体代理或应用），见图13 [b-Klingenstein]和[b-Hulsebosch]。SP将可信的IdSP清单告知客户端。客户端将实体重定向至每一个此类IdSP。在每一个IdSP进行相应的认证之后，客户端从所有IdSP处收到断言，并将整合后的断言交给SP。SP对每一个断言进行核验，收回所有的属性，之后决定实体是否能够接入服务。

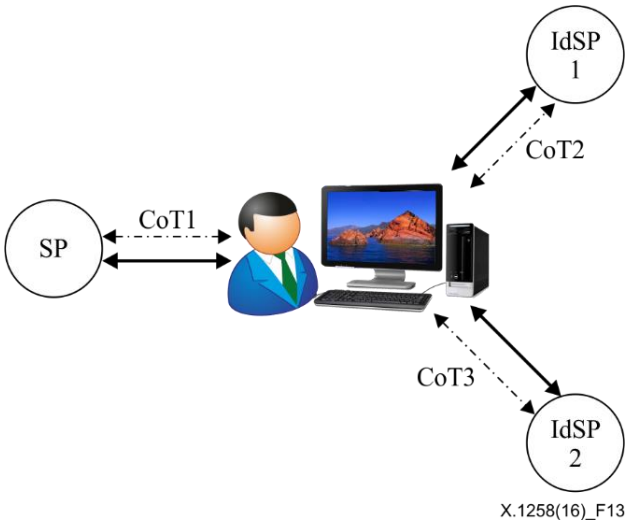


图13 – 客户端方法架构

图14展示了客户端方法下属性聚合的概念性控制流程：

1) 实体向SP发送服务请求。
2) 当SP需要实体服务许可时，SP会发送一个认证和认证断言请求。
3) IdSP 1对实体进行认证。

4) IdSP 1返回认证断言。

5) 实体被重定向至IdSP 2，以获取更多的属性断言。

6) IdSP 2对实体进行认证。

7) IdSP 2返回属性断言。

8) 实体向SP提交认证断言。

9) SP对断言进行核验，许可实体接入服务。

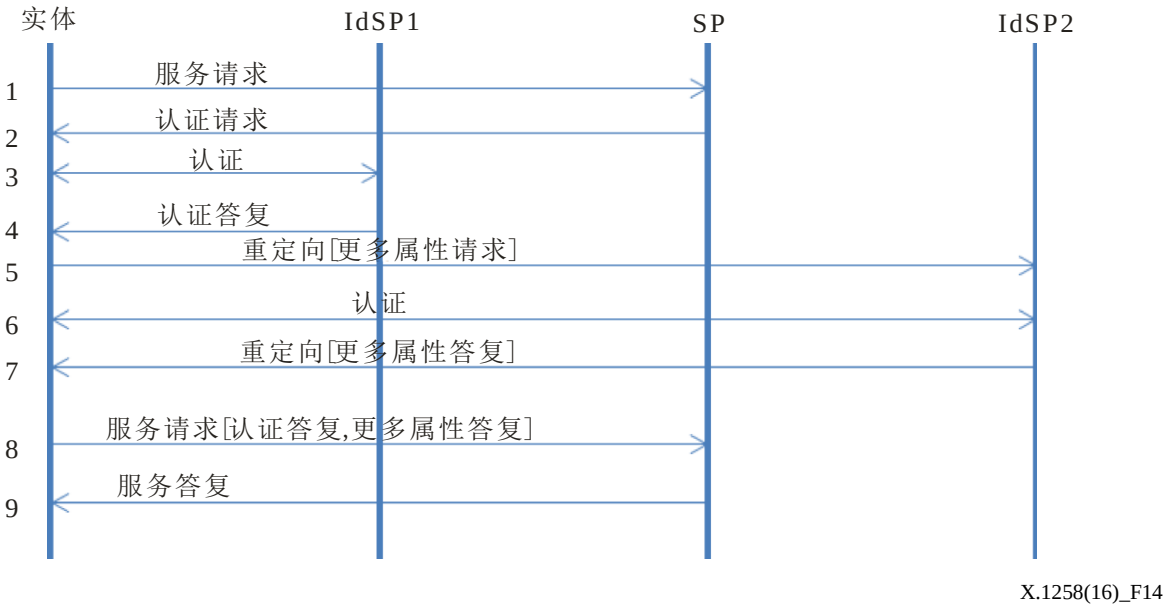


图14 – 客户端方法下的属性聚合流程

8 各聚合认证方法比较

与传统的联盟IdM系统相比，第7条中的七种方法均为新方法，且每一种都有额外的实体或交互。在此修改基础之上，可从各个要素对这七种方法进行分析和比较，以选出一种合适的聚合方法。设计人员和开发人员应考虑的问题包括：由谁来媒介/聚合/核验属性、实施难度或新元素的增加等。

条款7中提出了基于SAML的几种属性聚合方法。此类方法根据其在SAML中的表达方式可实现互操作。

从聚合媒介、聚合执行和额外元素几个方面对聚合方法进行了分析。各聚合方法比较结果如表1所示。

在表1中，格中的“✓”表示这一行的聚合方法具备这一列的能力。更准确的来说，标记的能力应通过标记方法的实施来获得支持。

表1 – 各聚合方法比较

聚合方法	能力						
	IdSP媒介	SP媒介	客户端媒介	IdSP聚合	SP聚合	客户端聚合	额外元素
身份关联	✓				✓		
身份代理	✓			✓			
身份中继	✓			✓			
应用数据库		✓			✓		DB
服务提供商		✓			✓		
关联服务		✓			✓		LS
客户端			✓			✓	客户端

对于身份关联方法来说，聚合由IdSP作为媒介，SP执行。也就是说，属性聚合协议应在IdSP和SP实施。但在其他情况下，聚合媒介与执行可以在同一个提供方实施。对于提供方来说，属性聚合比身份关联方法可能更为简单。对于属性聚合的额外元素来说，应用DB方法需要其自己的DB；作为一种特殊类型的SP，关联服务方法需要一种LS（关联服务）；实体媒介方法需要一个客户端作为代理。基于以上标准，在各IdSP媒介方法中，建议采用身份代理方法和身份中继方法，而在各SP媒介方法中，建议采用SP方法。

参考资料

[b-ITU-T X.500] ITU-T X.500建议书（2016年）| ISO/IEC 9594-1:2017，信息技术 – 开放系统互连 – 号码簿：概念、模型和服务概述

[b-ITU-T X.509] ITU-T X.509建议书（2016年）| ISO/IEC 9594-8:2017，信息技术 – 开放系统互连 – 号码簿：公开密钥和属性证书框架

[b-ITU-T X.1251] ITU-T X.1251建议书（2009年），数字身份的用户控制框架

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

[b-CardSpace] *Introducing windows cardspace*. MSDN technical articles, Microsoft Corporation.
Available (viewed 2016-12-19) at: http://msdn.microsoft.com/en-us/library/aa480189.aspx.

[b-Chadwick] Chadwick, D.W., Inman, G. (2009). Attribute aggregation in federated identity management. *IEEE Computer*, **42**(5), pp. 33–40.
<http://doi.ieeecomputersociety.org/10.1109/MC.2009.143>

[b-Higgins] Higgins, *Project.*
Available (viewed 2016-12-05) at: <http://www.eclipse.org/higgins/>

[b-Hulsebosch] Hulsebosch, B., Wegdam, M., Zoetekouw, B., van Dijk, N,, Poortinga-van Wijnen, R. (2012), Virtual collaboration attribute management. 41 pp. Available (viewed 2016-12-05) at:
<https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/EDS+11-06+Attribute+Management+v1.0.pdf >

[b-Kantara] Kantara, *Initiative*
Available (viewed 2016-12-19) at: https://kantarainitiative.org/reports-recommendations/

[b-Klingenstein] Klingenstein, N. (2007). Attribute aggregation and federated identity. In: *Proceedings of the 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07)*, p. 26–29.

[b-Liberty] Liberty Alliance, *ID-FF 1.2 Specifications*, Available (viewed 2016-12-05) at:
<http://www.projectliberty.org/liberty/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications

[b-OAuth] OAuth.
Available (viewed 2016-12-19) at: http://oauth.net/documentation/getting-started/

[b-OpenID] OpenID authentication 2.0.
Available (viewed 2016-12-19) at: http://openid.net/specs/openid-authentication-2_0.html

[b-Shibboleth] Shibboleth Consortium, *Open Source Project*.
Available (viewed 2016-12-05) at: <https://shibboleth.net/>

[b-WS-Federation] Web Services Federation Language (WS-Federation) Version 1.2.
Available (viewed 2016-12-19) at: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html

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他组件的建设、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