(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102067145 B
(45)授权公告日 2013.11.06

(21)申请号 200980123431.4

(22)申请日 2009.06.02

(30)优先权数据
12/141,515 2008.06.18 US

(85)PCT申请进入国家阶段日
2010.12.15

(86)PCT申请的申请数据
PCT/US2009/045989 2009.06.02

(87)PCT申请的公布数据
WO2009/155129 EN 2009.12.23

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 A·K·纳恩达 T·谢里夫

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 杨洁 钱静芳

(51)Int.Cl.
G06F 21/33(2013.01)
H04L 29/08(2006.01)

(56)对比文件
US 2007/0204168 A1,2007.08.30,说明书第0027,0028,0035-0058,0083-0086,0118 — 0122段,图1-4,7.
US 2005/0120219 A1,2005.06.02,全文.
US 2006/0235761 A1,2006.10.19,全文.
EP 1811421 A1,2007.07.25,全文.

审查员 李强

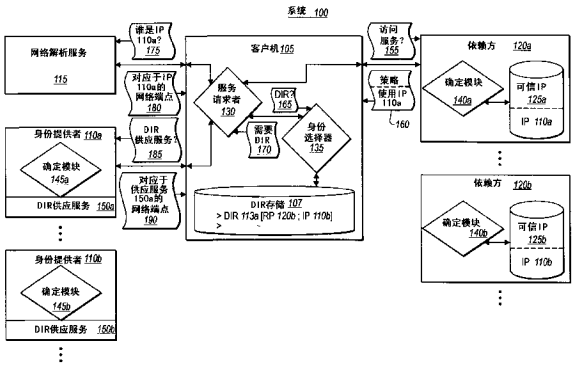
权利要求书3页 说明书9页 附图4页

(54)发明名称

通过独立端点解析来获得数字身份或令牌

(57)摘要

一种包括依赖方、身份提供者以及客户机的联合身份供应系统,该客户机从身份提供者获得令牌来访问依赖方的服务。当客户机联系新的依赖方时,该依赖方提供客户机可独立地解析和评估可信性的信息。例如,该依赖方提供通用域名地址。客户机随后可通过各种所认证的步骤来解析该域名地址以标识对应于数字身份供应服务的端点。客户机可进一步与供应服务交互并对其进行认证(例如,要求数字签名)来建立信任关系。一旦确定客户机/用户信任该供应服务,该客户机/用户可随后提供信息以获得数字身份表示。客户机可随后使用相应的身份提供者的数字身份表示来获得依赖方可确认的一个或多个令牌。



CN 102067145 B

1. 一种在联合计算机化系统（100）中的客户机计算机（105）处的方法，所述联合计算机化系统具有所述客户机、一个或多个身份提供者（110）以及一个或多个依赖方（120），所述方法是所述客户机独立地解析身份提供者的位置从而获得可由所述客户机用于访问依赖方处的一个或多个服务的安全令牌，所述方法包括以下动作：

联系（300）依赖方（120）以访问所述依赖方处的一个或多个服务；

从所述依赖方接收（310）一个或多个策略文件，其中所述一个或多个策略文件包括标识对应于一组一个或多个可信身份提供者的通用名称的信息（160）；

自动解析（320）所标识的通用名称，以获得对应于所述可信身份提供者（110）中的一个的一个或多个网络端点；

在认证了所述一个或多个网络端点之后，联系（330）所解析的那个身份提供者（110），以获得在获得一个或多个安全令牌（210）时使用的一个或多个数字身份表示（113），包括以下动作：

向所解析的身份提供者（110a）发送一个或多个请求（185）以获得有关任何可用的数字身份表示供应服务的信息；以及

接收包括有关用于所解析的身份提供者（110）的数字身份表示供应服务（150a）的信息的一个或多个消息（190）。

2. 如权利要求 1 所述的方法，其特征在于，所述通用名称包括对应于一个所述可信身份提供者（110a）的网络端点。

3. 如权利要求 1 所述的方法，其特征在于，所述通用名称包括对应于一个所述可信身份提供者（110a）的域名。

4. 如权利要求 3 所述的方法，其特征在于，所述自动解析所标识的通用名称的动作（320）进一步包括向解析服务（115）发送一个或多个请求（175）的动作。

5. 如权利要求 1 所述的方法，其特征在于，进一步包括，其中在一个或多个策略文件中的信息（160）和在一个或多个消息（190）中从身份提供者（110a）接收的信息中的一个或两者包括一个或多个元数据元素。

6. 如权利要求 1 所述的方法，其特征在于，进一步包括向解析服务（115）发送一个或多个附加消息的动作，其中，所述一个或多个附加消息请求对从所解析的身份提供者（110a）接收的一个或多个消息（190）中的信息进行解析。

7. 如权利要求 1 所述的方法，其特征在于，还包括以下动作：

标识对应于所述数字身份表示供应服务（150a）的网络端点；以及

客户机（105）将一个或多个消息（193）发送到所述数字身份表示供应服务（150a）以获得数字身份表示（113）。

8. 如权利要求 7 所述的方法，其特征在于，还包括从所述供应服务（150a）接收一个或多个数字身份表示（113b）以用于所解析的身份提供者（110a）的动作。

9. 如权利要求 8 所述的方法，其特征在于，还包括以下动作：

所述客户机（105）将包括对应于所接收的数字身份表示（113b）的信息的一个或多个附加消息（200）发送到所解析的身份提供者（110a）；以及

从所解析的身份提供者（110a）接收包括所述一个或多个安全令牌（210）的一个或多个消息。

10. 如权利要求 9 所述的方法，其特征在于，还包括以下动作 ：

所述客户机（105）将包括从所述身份提供者接收的所述一个或多个令牌（210）的一个或多个消息（220）发送到所述依赖方（120）；以及

接收来自所述依赖方（120）的指示已授予对所述一个或多个服务的访问权的一个或多个响应（230）。

11. 一种在联合计算机化系统（100）中的身份提供者（110）处的方法，所述联合计算机化系统（100）具有所述身份提供者、一个或多个客户机（105）以及一个或多个依赖方（120），所述方法将一个或多个数字身份表示和一个或多个安全令牌提供给对依赖方所提供的信息进行解析的客户机，所述方法包括以下动作 ：

在身份提供者（110）处接收来自客户机（105）的对一个或多个数字身份表示供应服务的一个或多个请求（185），所述数字身份表示供应服务用于建立一个或多个 DIR，所述一个或多个 DIR 可随后用于获得将用于向依赖方（120）验证用户的一个或多个安全令牌 ；

将标识所述身份提供者（110）所信任的至少一个数字身份供应服务（150）的信息（190）提供（410）给所述客户机（105）；

认证（420）从所述客户机（105）接收的一个或多个数字身份表示（113），其中所述身份提供者（110）确定所接收的一个或多个数字身份表示（113）是有效的 ；以及

提供（430）与所认证的一个或多个数字身份表示（113）相对应的一个或多个安全令牌（210）。

12. 如权利要求 11 所述的方法，其特征在于，所述将信息（190）提供（410）给客户机（105）的动作还包括以下动作 ：

发布包括标识所述一个或多个数字身份供应服务（150）的信息（190）的一个或多个文档 ；以及

对所述一个或多个文档进行数字签名。

13. 如权利要求 11 所述的方法，其特征在于，所述在所发布的一个或多个文档中所提供的信息（190）包括一个或多个元数据元素。

14. 如权利要求 11 所述的方法，其特征在于，所述提供给客户机（105）的信息（190）包括与所述一个或多个数字身份供应服务（150）相对应的一个或多个通用名称。

15. 如权利要求 11 所述的方法，其特征在于，在所述客户机（150）可访问数字身份供应服务（150）之前，所述一个或多个通用名称需要被解析到一个或多个网络端点。

16. 如权利要求 11 所述的方法，其特征在于，所述提供给客户机（105）的信息（190）包括与所述可信的一个或多个数字身份供应服务（150）相对应的一个或多个网络端点。

17. 如权利要求 11 所述的方法，其特征在于，所述认证（410）一个或多个数字身份表示（113）的动作进一步包括 ：

在所述身份提供者（110）处接收来自所述客户机（105）的对用于依赖方（120）的一个或多个安全令牌（210）的一个或多个新的请求（200）；以及

在所述一个或多个新的请求（200）中标识一个或多个有效的数字身份表示（113）。

18. 如权利要求 17 所述的方法，其特征在于，所述认证（410）一个或多个数字身份表示（113）的动作进一步包括，确定所接收的一个或多个数字身份表示（113）是从所述可信的数字身份供应服务（150）中的一个获得的。

19. 一种在联合计算机化系统(100)中的客户机计算机(105)处的系统,所述联合计算机化系统(100)具有所述客户机、一个或多个身份提供者(110)以及一个或多个依赖方(120),所述系统用于所述客户机独立地解析身份提供者的位置从而获得可由所述客户机用于访问依赖方处的一个或多个服务的安全令牌,所述系统包括 :

用于联系(300)依赖方(120)以访问所述依赖方处的一个或多个服务的装置 ;

用于从所述依赖方接收(310)一个或多个策略文件的装置,其中所述一个或多个策略文件包括标识对应于一组一个或多个可信身份提供者的通用名称的信息(160);

用于自动解析(320)所标识的通用名称,以获得对应于所述可信身份提供者(110)中的一个的一个或多个网络端点的装置 ;

用于在认证所述一个或多个网络端点之后,联系(330)所解析的那个身份提供者(110),以获得在获得一个或多个安全令牌(210)时使用的一个或多个数字身份表示(113)的装置,包括 :

用于向所解析的身份提供者(110a)发送一个或多个请求(185)以获得有关任何可用的数字身份表示供应服务的信息的装置 ;以及

用于接收包括有关用于所解析的身份提供者(110)的数字身份表示供应服务(150a)的信息的一个或多个消息(190)的装置。

通过独立端点解析来获得数字身份或令牌

[0001] 背景

[0002] 1. 背景和相关技术

[0003] 常规计算机系统现在通常用于各种目的，无论是出于生产力、娱乐还是其他目的。其原因之一是，计算机系统往往通过任务自动化以及使得某些类型的交易更高效来增加效率。例如，过去某些类型的交易可能会花费用户几小时或几天来完成。特别地，如果用户要进行银行存款、银行转帐、或甚至在商店中购买物品，用户可能需要物理上行进到该银行或商店位置，以便验证用户的身份并呈现用于交易的指令。在验证了用户的身份后，银行或商店可随后发起并确认所请求的交易。在该场景中，银行或商店可以被认为是“依赖方”，该“依赖方”依赖于作为“身份提供者”的用户所提供的当面身份。

[0004] 然而，最近自动化（或计算机化）机制已经将这些类型的交易简化到几秒钟或几分钟。特别地，诸如上述的交易由于允许用户从远程位置执行交易的自动化终端的出现而变得越来越高效和复杂。然而，自动化终端在提供接入服务之前允许用户满足多个质询和响应场景，而不是依赖当面身份验证。例如，用户可能需要呈现账户卡和个人识别号，该账户卡和个人识别号是先前在建立用户与依赖方之间的信任关系时从依赖方接收的。

[0005] 如同自动化终端一样，最近的基于因特网的依赖方也请求最终用户建立某种信任关系，这通常通过要求用户提供某些可验证个人信息（例如，姓名、地址、生日等）来进行。依赖方还可要求用户呈现其他第三方验证信息，诸如信用卡信息、驾驶执照信息、或社会保险卡信息。在这些类型的情况下，依赖方不仅依赖于用户的自验证信息，而且还依赖于依赖方已与其建立信任关系的其他方（例如，信用卡公司，或政府实体）的验证。由此，当用户随后访问依赖方的服务时，依赖方可要求用户呈现先前交换的部分或全部个人和第三方信息。

[0006] 由于效率增益通常是通过在线交易来提供的，因此数量愈趋增长的实体以此方式提供服务，并且用户对使用此方式的需求也在增长。然而，在线交易的增长产生了另一组问题。即，用户现在经常有大量并且数量增长的不同在线帐户需要他们跟踪和维护。特别是在用户向每个不同的依赖方提供不同的验证信息的情况下，用户可能需要记住或能够访问数量增长的不同的用户名、口令、以及潜在的其他验证信息。

[0007] 一些常规机制试图通过实现“联合”身份验证系统来缓解其中一些问题。在联合系统中，单独的身份提供者维护数据，该数据可用于为用户在各种依赖方处的许多不同帐户生成一个或多个安全令牌。一般而言，“安全令牌”是身份提供者用以向依赖方断言用户身份的手段。为了使安全令牌可在许多不同的依赖方之间移植，这种类型的身份提供者将需要与用户想访问的每个不同的依赖方建立信任关系。

[0008] 由此，当用户期望访问依赖方处的特定服务时，用户可联系身份提供者，向身份提供者验证自己，并且从身份提供者获得令牌。然后用户可向依赖方呈现来自身份提供者的令牌，该令牌包含某些有关用户和 / 或用户客户机系统的声明（以及一些有关身份提供者的信息）。由于依赖方信任身份提供者和用户，所以依赖方可使用所提供的信息来确认令牌，并且如果令牌得到确认，则依赖方向用户提供对各种所请求的服务或交易的访问权。

[0009] 由于一些依赖方可以仅信任某些身份提供者，或可以仅具有与某些身份提供者建立的信任关系，因此用户也可以具有与多个不同的身份提供者所建立的账户。在常规系统中，用户维护或存储可在每个身份提供者处使用的一个或多个身份表示以获得安全令牌。存储在用户的客户计算机系统处的身份选择服务进而可管理和标识什么身份表示应用于任何给定身份提供者。

[0010] 例如，用户可能需要对一个特定的身份提供者使用一个数字身份表示，来发放用于一个特定依赖方的令牌。用户然后可在同一（或不同）身份提供者处使用另一个数字身份表示来获得该依赖方处（或另一依赖方处）的另一些令牌。身份选择服务由此向适当的身份提供者提供适当的一个或多个数字身份表示。

[0011] 一般而言，当用户已经与所需身份提供者建立信任关系时，上述联合系统往往工作良好。然而，在一些情况下，用户可遇到接受来自用户（或客户机系统）尚未与其建立信任关系的身份提供者的令牌的依赖方。尽管用户可经历与特定的身份提供者建立关系的过程，但用户仍需要能够标识身份提供者的姓名和位置。然而，提供有关身份提供者的名称和位置的信息可涉及多个安全风险。

[0012] 例如，如果建立上述场景以便依赖方自动将客户机系统定向到特定的身份提供者，则用户会冒“网络钓鱼”攻击的风险。特别地，用户相信其为合法的恶意依赖方可自动将用户定向到恶意身份提供者。当用户试图与恶意身份提供者建立身份表示时，该身份提供者可简单地窃取该用户的身份并且利用该用户。该身份提供者甚至可提供用于访问该恶意依赖方的令牌，并且由此保持出现一段延长的时间。

[0013] 甚至对于合法的依赖方，当依赖方提供对应于数字身份表示供应服务的确切端点时，用户（和/或依赖方）也可存在一些风险。可以理解，随着越来越多的实体朝着提供安全在线交易服务发展时，这些问题往往只会增加。因此，对于联合系统，有许多可以解决的困难。

[0014] 简要概述

[0015] 本发明的实现用被配置成在获得用于依赖方的令牌之前提供数字身份表示供应服务的独立的用户/客户机验证的系统、方法和计算机程序产品解决了本领域中的一个或多个问题。在至少一个实现中，例如，响应于对依赖方处的服务的请求，客户机接收有关依赖方信任的一个或多个身份提供者的元数据。客户机随后独立地解析该元数据，以标识该身份提供者所提供的数字身份供应服务，并且确定该客户机是否可信任该供应服务。如果可信，则该客户机可随后通过该供应服务与相应的身份提供者建立数字身份表示，并且获得用于依赖方的一个或多个令牌。

[0016] 例如，从客户计算机系统的观点来看，一种获得数字身份表示和/或安全令牌的方法可涉及联系依赖方以访问依赖方处的一个或多个服务。该方法还可涉及从该依赖方接收一个或多个策略文件。在这种情况下，该一个或多个策略文件包括标识与一组一个或多个可信身份提供者相对应的通用名称的信息。另外，该方法可涉及自动解析所标识的通用名称，来获得对应于可信身份提供者中的一个的一个或多个网络端点。此外，该方法可涉及在认证该一个或多个网络端点之后，联系该所解析的身份提供者以获得在获得一个或多个安全令牌时使用的一个或多个数字身份表示。

[0017] 另外，从身份提供者的观点来看，一种向客户机提供一个或多个数字身份表示和/

或一个或多个安全令牌的方法可涉及在身份提供者处接收一个或多个来自客户机的对一个或多个数字身份表示供应服务的请求。该方法也可涉及向该客户机提供标识由该身份提供者所提供的一个或多个数字身份供应服务的信息。另外，该方法可涉及认证从该客户机接收的一个或多个数字身份表示。在这种情况下，该身份提供者确定所接收的一个或多个数字身份表示是有效的。此外，该方法可涉及提供与所认证的一个或多个数字身份表示相对应的一个或多个安全令牌。

[0018] 提供本概述以便以简化形式介绍将在以下详细描述中进一步描述的一些概念。本概述不旨在标识出所要求保护的主题的关键特征或必要特征，也不旨在用于帮助确定所要求保护的主题的范围。

[0019] 本发明的其他特征和优点将在随后的描述中阐述，并且部分地将从本说明书中显而易见，或可以通过本发明的实施来获知。本发明的特征和优点可通过在所附权利要求书中特别指出的工具和组合来实现和获得。本发明的这些和其他特征将通过以下描述和所附权利要求书变得更加显而易见，或可通过对下文中所述的本发明的实践来领会。

[0020] 附图简述

[0021] 为了描述可以获得本发明的上文所列举的及其他优点和特征的方式，将通过参考附图中所示的本发明的各具体实施例来呈现上文简要描述的本发明的更具体的描述。可以理解，这些附图只描绘了本发明的各典型实施例，并且因此不被认为是对其范围的限制，将通过使用附图并利用附加特征和细节来描述和解释本发明，在附图中：

[0022] 图 1A 示出其中客户机解析来自依赖方的一个或多个策略以标识适当的身份提供者的联合身份系统的概要示意图；

[0023] 图 1B 示出其中客户机联系身份提供者所涉及的数字身份表示供应服务，并使用该服务以获得数字身份表示的概要示意图；

[0024] 图 2 示出图 1A 和 1B 中所示的系统的示意图，其中客户机使用图 1B 中的供应服务所提供的数字身份表示以获得客户机随后用于访问依赖方处的服务的令牌；

[0025] 图 3 示出从客户机的观点来看的用于从可信端点获得数字身份表示的方法的一个或多个动作的流程图；以及

[0026] 图 4 示出从身份提供者的观点来看的用于在认证新提供的数字身份表示之后为客户机提供令牌的方法的流程图。

[0027] 详细描述

[0028] 本发明的实现涉及被配置成在获得用于依赖方的令牌之前提供数字身份表示供应服务的独立的用户 / 客户机验证的系统、方法和计算机程序产品。在至少一个实现中，例如，响应于对依赖方处的服务请求，客户机接收有关依赖方所信任的一个或多个身份提供者的元数据。客户机随后独立地解析该元数据，以标识该身份提供者所提供的数字身份供应服务，并且确定该客户机是否可信任该供应服务。如果可信任，则该客户机可随后通过该供应服务与相应的身份提供者建立数字身份表示，并且获得用于依赖方的一个或多个令牌。

[0029] 因此，并且如此处将更加全面地理解的，本发明的实现提供身份提供者可用于发布服务的位置的一个或多个机制，该服务可发放数字身份表示（即 DIR，也被称为“信息卡”）。本发明的实现还提供身份提供者可用于发布替换信息的一个或多个机制，该替换信

息允许用户在获得 DIR 之前与身份提供者建立关系。另外，本发明的实现还提供身份选择器（例如，客户机系统上的组件或应用程序）可用于查明用于特定的身份提供者的 DIR 是否可用，并且将信息呈现给用户以帮助他们获得其 DIR 的一个或多个机制。

[0030] 一般而言，本发明的这些和其他方面可在至少一个实现中使用根据 WS-FEDERATION(WS 联盟）规范来配置的元数据元素来实现。在至少一个实现中，例如，身份提供者和依赖方两者均可使用用户可用于独立地验证特定端点的各种元数据元素来将用户定向到各种端点。例如，某些元数据元素可描述发放服务的 DIR 的实际位置，用户需要去往该实际位置以获得该卡。某些元数据元素还可描述发放卡的安全要求。另外，在下载数字身份表示（即，DIR）之前需要用户与发放者 / 身份提供者的关系的情况下，万一用户没有这一关系，元数据元素可向用户指示去往哪里。这些元数据元素进而允许用户的客户机身份选择器结合此处描述的一个或多个附加组件来找出或建立用户所需要的 DIR，并且随后获得相关安全令牌。

[0031] 图 1A 示出根据本发明一实现的联合身份供应系统 100。如图所示，联合身份供应系统 100 至少包括客户机 105，以及客户机 105（即，代表用户）向其请求对特定服务的访问的一个或多个依赖方 120(a、b 等）。例如，依赖方 120 是提供各种账户或购物功能的在线银行或在线商店。图 1A 还示出每个依赖方 120(a、b 等）包括确定模块 140(a、b 等）以及可信身份提供者列表 125(a、b 等）。这些模块和列表中的每一个将在下面更全面地讨论。

[0032] 另外，图 1A 示出联合身份供应系统 100 包括一个或多个身份提供者 110(a、b 等），每一个身份提供者 110 也有其自己的确定模块 145(a、b 等）以及对应的一个或多个数字身份供应服务 150(a、b 等）。如此处更全面地理解的，该一个或多个身份提供者 110 使用一个或多个“安全令牌”（例如，210，图 2）向依赖方验证用户 / 客户机的身份。一般而言，安全令牌以依赖方 120 与可信身份提供者 110 互相达成协定的格式 / 配置来提供各种有关用户的声明。例如，银行或在线商店形式的依赖方 120 在向客户机 105 提供所请求的服务之前需要对用户 / 客户机 105 的凭证进行独立的验证；可信的身份提供者 110 进而通过一个或多个安全令牌提供此验证，该安全令牌包括用于验证用户的凭证的期望的数据。

[0033] 然而，客户机 105 不能简单地向所指示的身份提供者 110 请求安全令牌。相反，客户机 105 需要与身份提供者 110 建立信任关系。此外，客户机 105 不能简单地出于与任何特定依赖方 120 进行交互的目的来获得与任何给定的身份提供者 110 的信任关系。相反，客户机 105 需要获得与特定的身份提供者 110 的信任关系，该特定的身份提供者 110 也是客户机向其请求服务的特定依赖方 120 所信任的。即，不是每个依赖方 120 都具有与每个身份提供者 110 的信任关系，反之亦然。例如，图 1A 示出依赖方 120a 维护可信身份提供者 100 的列表 125a，在这种情况下该列表 125a 包括身份提供者 110a，但不包括身份提供者 110b。类似地，图 1A 示出依赖方 120b 维护可信身份提供者 100 的列表 125b，在这种情况下该列表 125b 包括身份提供者 110b，但不包括身份提供者 110a。

[0034] 一般而言，客户机（代表用户）与给定的身份提供者的信任关系在上述数字身份表示，即 DIR(113) 中表明。客户机进而使用特定的 DIR 113(a、b 等）以获得与特定的身份提供者 110 的安全令牌，该安全令牌最终用于信任该特定的身份提供者的一个或多个依赖方处的服务。由此，例如，图 1A 示出客户机 105 维护 DIR 存储 107，在这种情况下该 DIR 存储 107 包括身份提供者 110b 的 DIR 113a，其用于依赖方 120b 的服务，因为仅仅依赖方 120b

而非依赖方 120a 信任身份提供者 110a。因此，可以理解，任何给定 DIR 113 可用于多个不同的依赖方 120。

[0035] 另外，尽管客户机 105 可维护存储 107 中任何数量的 DIR113，但出于简明的目的，图 1A 示出客户机 105 仅仅具有单个 DIR113a。在该示例中，所示 DIR113a 允许客户机 105 从身份提供者 110b 获得安全令牌，以用于依赖方 120b。相反，图 1A 还示出客户机 105 不具有对应于身份提供者 110a，和 / 或用于依赖方 120a 处的服务的 DIR。

[0036] 因此，如图 1A 所示，当客户机 105 试图（例如，通过消息 155）访问依赖方 120a 的服务时，依赖方 120a 最终将客户机 105 定向到客户机 105 尚未与其建立关系（即，没有 DIR113）的身份提供者（即，110a）。例如，图 1A 示出响应于消息 155，依赖方 120a（例如，经由确定模块 140a）确定客户机 105 仍需要呈现安全令牌以访问服务。由此，图 1A 示出依赖方 120a 用一个或多个策略 160 来响应。

[0037] 可以理解，依赖方 120a 可以用任何数量的方式来提供一个或多个策略 160。例如，依赖方 120a 可发布包含有关适当的令牌发放者（即，身份提供者）的信息的一个或多个文档。客户机 105 随后可审阅所发布的文档来获得相关的信息。在附加或替换实现中，依赖方 120a 用关于可信身份提供者 110 的名称的特定信息来响应。

[0038] 依赖方 120a 所提供的信息 / 策略 160 进而可包括任何数量或类型的信息。如上所述，例如，策略 160 可包括关于对应于特定身份提供者 110 的网络端点的各种元数据元素（例如，根据 WS-FEDERATION 规范）。在附加或替换实现中，该一个或多个元数据元素包括或以其他方式指示一个或多个通用域名，客户机 105 需要进一步解析该通用域名以确定适当的端点。例如，一个或多个策略 160 可包括诸如“使用来自 BANK.com 的身份提供者”的信息。在这种情况下，客户机需要解析 BANK.com 以标识一个或多个身份提供者 110，并且从其中获得安全令牌。

[0039] 因此，图 1A 示出客户机 105 经由服务请求者 130 处理有关适当的身份提供者 110 的信息 160，该服务请求者 130 通过身份选择器 135 比较所接收的信息 160。具体而言，图 1A 示出服务请求者 130 将一个或多个消息 165 发送到身份选择器 135，以查询是否有对应于身份提供者 110a 的用于依赖方 120a 的 DIR（即，在存储 107 中）。在这种情况下，图 1A 示出身份选择器 135 用一个或多个消息 165 来响应，这些消息指示没有这样的 DIR，或以其他方式指示需要建立用于身份提供者 110a 的 DIR。在附加或替换实现中，身份选择器 135 进一步向用户呈现一个或多个界面，并且允许用户选择选择适当的 DIR 113 用于依赖方 120a，或如果需要，以其他方式呈现去获得新的 DIR 113 的选项。

[0040] 在所示情况中，图 1A 示出指示服务请求者 130 找出身份提供者 110a（并与身份提供者 110a 进行通信）以获得适当的 DIR 113。图 1A 还示出有关身份提供者 110a 的信息 160 需要进一步的解析，因为其没有表示出精确的网络端点。因此，图 1A 示出服务请求者 130 用一个或多个消息 175 与一个或多个域名解析服务 115 联系。在附加或替换实现中，服务请求者 130 联系一个或多个其他代理或服务，这些代理或服务进而用消息 175 联系网络解析服务 115。在任一情况下，图 1A 示出客户机 105 最终接收具有所解析的信息 180 的一个或多个消息 180，在这种情况下该信息包括对应于身份提供者 110a 的特定的网络端点。

[0041] 当然，可以理解，网络解析服务 115 可另外地或另选地用其他服务或代理的一个或多个其他域名来响应。该响应可能需要服务请求者 130 更进一步联系其他实体以在获得

对应于身份提供者 110a 的端点之前获得附加的信息 / 解析。例如，响应 180 可包括潜在地对应于身份提供者 110a 的名称的身份提供者的列表。服务请求者 130 随后可在继续的基础上联系该列表中的任何或全部所标识的身份提供者，直到标识了对应于依赖方 120a 所指示的身份提供者 110a 的适当且特定的网络端点。无论如何进行，值得注意的是，客户机 105（例如，代表用户）在没有来自依赖方 120a 的具体指示的情况下独立地确定或解析网络端点。

[0042] 在任何情况下，在经由消息 180 接收到端点之后，图 1A 示出服务请求者 130 将一个或多个消息 185 发送到身份提供者 110a（即，与其对应的所解析的端点），以获得有关其 DIR 供应服务的信息。如果客户机 105 具有先前建立的信任关系，并且已经具有适当的 DIR 113，则客户机 105 可随后使用该 DIR（例如，经由消息 200，图 2）来请求用于依赖方 120a 的适当的安全令牌 (210，图 2)。由于在这种情况下，客户机 105 没有身份提供者 110a 的 DIR，客户机 105 由此要求适当的 DIR 供应服务的位置。

[0043] 作为响应，图 1A 示出身份提供者 110a 发送一般标识数字身份表示供应服务 150a（即，“DIR 供应服务”）的一个或多个消息 190。如同策略 160 一样，该一个或多个消息 190 也可包括所发布的文档，该所发布的文档包括具有一个或多个特定网络端点的元数据元素。然而，在附加或替换实现中，消息 190 中的信息可包括可解析的域名，服务请求者 130 必须在一个或多个附加步骤中（例如，经由解析服务 115）解析该域名以标识对应于 DIR 供应服务 150 的网络端点。在任一情况下，在标识了对应于 DIR 供应服务 150（即，150a）的正确的网络端点之后，客户机 105 随后试图获得 DIR 113。

[0044] 例如，图 1B 示出服务请求者 130 将一个或多个消息 193 发送到所标识的数字身份供应服务 150a，请求用于诸如依赖方 120a 等依赖方的一个或多个 DIR113。一般而言，这不仅可包括发起 / 创建 DIR 113 的一般请求，而且可包括一系列请求和响应（即，多个不同消息）以建立和获得该 DIR 113。例如，DIR 供应服务 150a 可（通过客户机 105）请求有关用户的个人信息，并且用户经由客户机 105 可能需要提供若干对应的响应。该请求可包括与信用卡信息、驾驶执照信息、社会保险卡信息、以及可用于以某种方式个体地标识用户的其他基于质询的信息有关的信息。在确认了（由服务请求者 130 所提供的）用户的信息 / 凭证之后，DIR 供应服务 150a 可随后用适当的 DIR 113 来响应。例如，图 1B 示出 DIR 供应服务 150a 向客户机 105 发送一个或多个消息 195，该消息 195 关于与身份提供者 110a 相关的新创建的 DIR 113b，在这种情况下，客户机可将该新创建的 DIR 113b 用于依赖方 120a。

[0045] 如图 2 所示，客户机 105 将该新的 DIR 113b 存储在其 DIR 存储 107 中。另外，客户机 105 可随后使用该新的 DIR 113b 来获得一个或多个安全令牌 210，以访问依赖方 120a 的服务。如图 2 所示，例如，客户机（即，经由服务请求者 130）将一个或多个新消息 200 发送到身份提供者 110a。在这种情况下，该一个或多个消息 200 包括对应于新创建的 DIR 113b 的信息，以及对访问依赖方 120a 处的服务的一个或多个安全令牌的请求。

[0046] 作为响应，身份提供者 100a 处的确定模块 150a 随后确认所提供的 DIR113b。例如，身份提供者 110a 处的确定模块 145 确定新的 DIR 113b 对应于基于消息 190 中一个或多个元数据元素的 DIR 供应服务 150（或由其创建）。由此，由于 DIR 113b 已被认证或确认，图 2 示出身份提供者 110a 用一个或多个对应的安全令牌 210 来响应。具体而言，图 2 示出身份提供者 110a 将一个或多个安全令牌 210 直接发送给客户机 105，随之客户机 105 在一

个或多个对应的消息 220 中将该一个或多个安全令牌 210 提供给依赖方 120a。当然，可以理解，身份提供者 110a 可另外地或另选地将该一个或多个安全令牌 210 直接发送给依赖方 120a。

[0047] 另外，图 2 示出依赖方 120a 通过确定模块 140 处理在一个或多个消息 220 中所接收的安全令牌 210。例如，确定模块 140a 处理该安全令牌 210 以确定其是否符合先前所提供的信息 160（图 1）中的一个或多个数据元素。在一个实现中，这包括依赖方 120a 确定所接收的安全令牌 210 是来自可信身份提供者（例如，110a），并且该安全令牌 210 包括用于验证正请求服务的用户的期望的数据。在标识了安全令牌 210 是有效的之后，和 / 或（结合安全令牌 210）标识了由客户机 105 所提供的用户数据是经验证的之后，依赖方 120a 可随后授予对所请求的服务的访问权。例如，图 2 示出依赖方 120a 将一个或多个消息 230 发回客户机 105，这允许客户机 105 访问所请求的服务。

[0048] 因此，图 1A 至图 2 提供了用于使客户机 105 能对信息进行安全解析的一个或多个机制。具体而言，图 1A 到图 2 以及对应的文本提供用于确保客户机 105 能可靠且安全地获得与身份提供者的信任关系的多个组件和机制。在至少一个实现中，这些组件和机制涉及客户机的独立解析和动作的级别，这可避免多个安全性违背，诸如那些例如与常规网络钓鱼攻击相关联的安全性违背。

[0049] 除了上述内容之外，本发明的各实现还可以按照包括用于实现特定结果的一个或多个动作的方法来描述。例如，图 3 示出从客户机 105 的观点来看的用于解析来自依赖方的信息以从诸如身份提供者 110 等可信端点获得数字身份表示的流程图。另外，图 4 示出从身份提供者 110 的观点来看的用于认证数字身份表示以及向客户机提供对应的安全令牌的流程图。下面将结合各组件和示图 1A、1B、2 来更全面地描述图 3 和 4 的动作。

[0050] 例如，图 3 示出从客户机 105 的观点来看的方法可以包括联系依赖方 (RP) 以获得服务的动作 300。动作 300 包括联系依赖方以访问依赖方处的一个或多个服务。例如，图 1A 示出客户机 105 将一个或多个消息 155 发送到依赖方 120a，这些消息请求访问依赖方处 120a 的一个或多个服务。

[0051] 图 3 还示出从客户机 105 的观点来看的方法可包括接收有关可信身份提供者 (IP) 的信息的动作 310。动作 310 包括从依赖方接收一个或多个策略文件，其中该一个或多个策略文件包括标识对应于一组一个或多个可信身份提供者的通用名称的信息。例如，图 1A 示出由于客户机 105 不具有与依赖方 120 建立的关系，因此依赖方将一个或多个消息 160 发回客户机 105。在这一特定情况下，该一个或多个消息 160 包括指示有关可信身份提供者 110a 的通用信息的信息。如此处更全面地理解的，该信息 160 可包括对应于身份提供者 110a 的特定的网络端点。当然，该信息 160 还可以或另选地包括身份提供者 110a 的通用域名，或者可联系以标识身份提供者 110a 的网络地址的另一个服务 110a。

[0052] 另外，图 3 示出从客户机 105 的观点来看的方法可包括将身份提供者的名称解析到可信网络端点的动作 320。动作 320 包括自动解析该通用名称来获得对应于可信身份提供者中的一个的一个或多个网络端点。例如，客户机 105 处的服务请求者 130 自动将一个或多个消息 175 发送到网络解析服务 115，并且请求解析信息 160 中找出的通用名称。进而，服务请求者 130 接收一个或多个消息 180，该消息 180 将最初提供的对应于身份提供者 110a 的通用名称解析到一个或多个特定的网络端点。或者，服务请求者 130 自动联系信息

160 中找出的特定的网络端点，并且要求该网络端点处的实体提供适当的身份提供者 110 的位置。

[0053] 例如，图 3 示出从客户机 105 的观点来看的方法可包括通过可信网络端点来获得数字身份表示的动作 330。动作 330 包括在认证了该一个或多个网络端点之后联系该所解析的身份提供者，以获得在获得一个或多个安全令牌时使用的一个或多个数字身份表示。例如，图 1A 和 1B 示出身份提供者 110a 将一个或多个消息 190 发回客户机 105。该一个或多个消息 190 进而可包括指示对应于 DIR 供应服务（例如，150a）的一个或多个端点的一个或多个元数据元素（例如，根据 WS-FEDERATION 标准）。类似地，该一个或多个消息 190 可包括需要进一步被解析到对应于 DIR 供应服务（例如，150a）的一个或多个端点的一个或多个元数据元素。在任一情况下，服务请求者 130 随后使用消息 190 中的信息来最终联系适当的 DIR 供应服务（例如，150a），并且获得数字身份表示（例如，110b）。

[0054] 除上述之外，图 4 示出从身份提供者 110 的观点来看的方法可包括接收对有关 DIR 供应服务的信息的客户机请求的动作 400。动作 400 包括在身份提供者处接收来自客户机的对一个或多个 DIR 供应服务的一个或多个请求，该一个或多个 DIR 供应服务用于建立可随后用于获得可向依赖方验证用户的一个或多个安全令牌的一个或多个 DIR。如上所述，例如，图 1A 示出身份提供者 110a 接收来自客户机 105 的对 DIR 供应服务信息的一个或多个请求 185，作为最终获得一个或多个安全令牌的努力的一部分。

[0055] 图 4 还示出从身份提供者 110 的观点来看的方法可包括提供关于数字身份表示供应服务的信息的动作 410。动作 410 包括向该客户机提供标识该身份提供者所信任的的一个或多个数字身份供应服务的信息。例如，如上所述，图 1A 示出响应于请求 185，身份提供者 110a 经由一个或多个消息 190 来提供信息。在至少一个实现中，该一个或多个消息 190 包括发布的安全文档，或其中包含的信息的至少一部分。该信息可包括 DIR 供应服务 150a 的域名（可能需要经由网络解析服务 115 进行进一步的解析），或仅仅是对应于服务 150a 的特定的网络端点。

[0056] 另外，图 4 示出从身份提供者 110 的观点来看的方法包括认证客户机所提供的数字身份表示的动作 420。动作 420 包括认证从客户机接收的一个或多个数字身份表示，其中，身份提供者确定所接收的一个或多个数字身份表示是有效的。例如，如图 2 所示，身份提供者 110a（例如，经由确定模块 145a）评估消息 200 中由客户机 105 所提供的 DIR 113b。具体地，身份提供者 110a 确定 DIR 113b 是由先前在一个或多个消息 190 中所引用的 DIR 供应服务 150a 所创建并提供的。由此，身份提供者 110a 确认经由消息 200 提供 DIR 113b 的客户机 105 就是经由消息 180 请求 DIR 供应服务的相同的客户机 105。

[0057] 此外，图 4 示出从身份提供者 110 的观点来看的方法可包括将安全令牌提供给客户机的动作 430。动作 430 包括提供与所认证的一个或多个数字身份表示相对应的一个或多个安全令牌。例如，图 2 示出在确认消息 200 中的数字身份表示 113b 之后，身份提供者 110a 将一个或多个安全令牌 210 发回客户机 105。客户机 105 可随后使用所提供的安全令牌 210 来向依赖方 120a 验证请求用户的身份。

[0058] 因此，本发明的实现提供用于可靠、安全并且高效地向客户机提供对适当的安全令牌的访问权的多个不同的组件和机制。如此处所讨论的，例如，这些机制可包括客户机的身份选择器用于确定特定身份提供者的 DIR 是否可用的手段，以及如果不可用则帮助用户

获得适当的 DIR 的方式。这些机制还可以使身份提供者能够（例如，经由发布物或以其他方式）将各种元数据元素提供给用户，其中该元数据元素指示可发放适当的 DIR 的 DIR 供应服务的位置。如本文先前所提到的，该信息（例如，以元数据元素的形式）可以按使各种端点的用户能够独立解析的方式来发布，由此增强了整个联合系统的安全性。

[0059] 本发明的各实施例可以包括其中包含各种计算机硬件的专用或通用计算机，如下面更详细地讨论的。本发明的范围内的实施例也包括用于承载或其上存储有计算机可执行指令或数据结构的计算机可读介质。这样的计算机可读介质可以是可由通用或专用计算机访问的任何可用介质。

[0060] 作为示例而非限制，这样的计算机可读介质可以包括 RAM、ROM、EEPROM、CD-ROM 或其他光盘存储、磁盘存储或其他磁存储设备，或可以用来携带或存储计算机可执行指令或数据结构的形式的所需程序代码装置并可由通用或专用计算机访问的任何其他介质。当信息通过网络或另一通信连接（硬连线、无线、或硬连线或无线的组合）传输或提供给计算机时，计算机将该连接完全视为计算机可读介质。因此，任何这样的连接被适当地称为计算机可读介质。上述的组合也应被包括在计算机可读介质的范围内。

[0061] 计算机可执行指令包括，例如使通用计算机、专用计算机、或专用处理设备执行某一功能或某组功能的指令和数据。尽管用结构特征和 / 或方法动作专用的语言描述了本主题，但可以理解，所附权利要求书中定义的主题不必限于上述具体特征或动作。相反，上文所描述的具体特征和动作是作为实现权利要求的示例形式来公开的。

[0062] 本发明可被具体化为其他具体形式而不背离其精神或本质特征。所描述的实施例在所有方面都应被认为仅是说明性而非限制性的。因此，本发明的范围由所附权利要求书而不是由前面的描述指出。落入权利要求书的等效方案的含义和范围内的所有改变应被权利要求书的范围所涵盖。

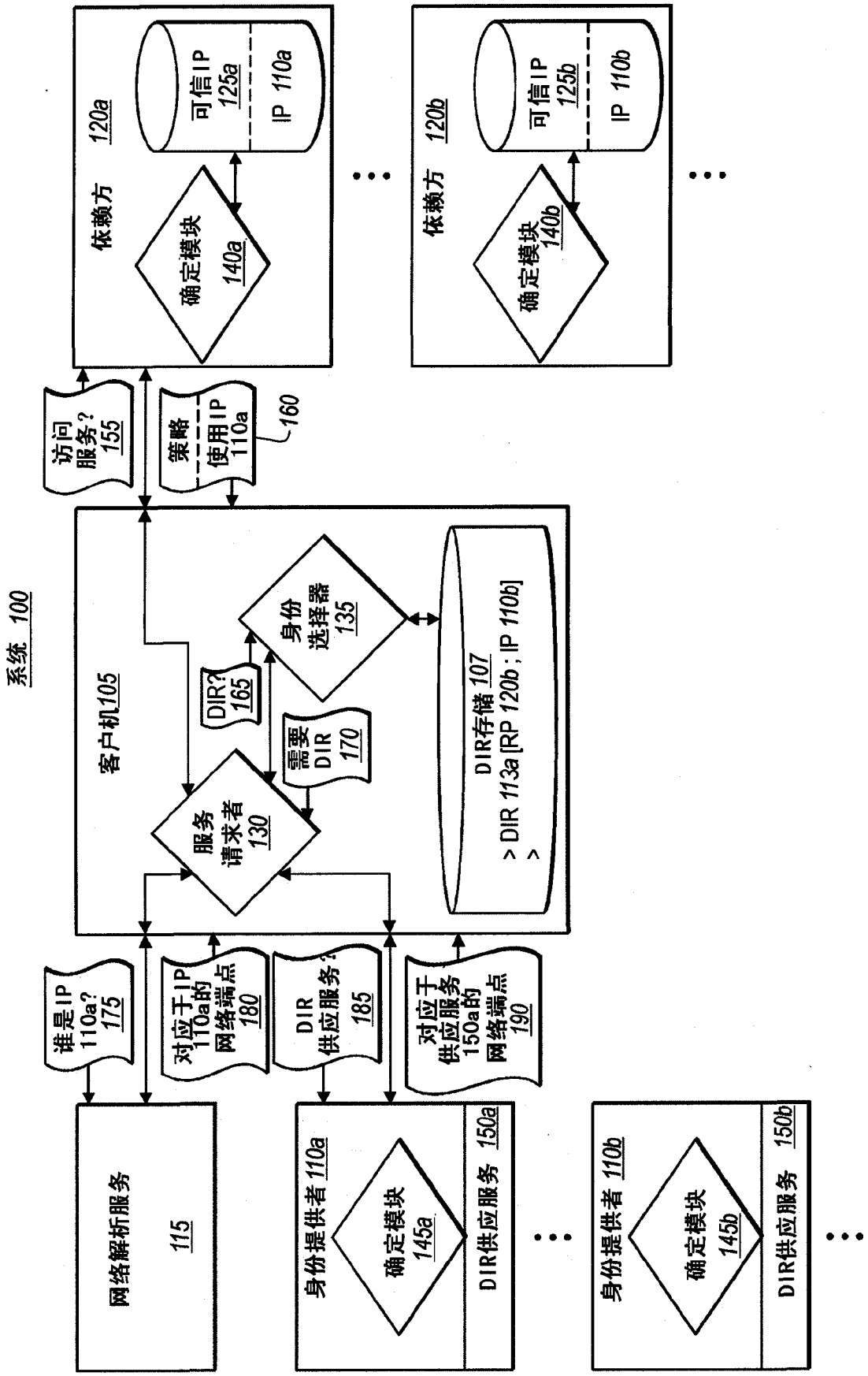

系统 100
依赖方 120a
可信IP 125a
IP 110a
确定模块 140a
依赖方 120b
可信IP 125b
IP 110b
确定模块 140b
访问服务? 155
策略 使用IP 110a
160
客户机105
身份选择器 135
DIR? 165
需要DIR 170
服务请求者 130
DIR存储 107
> DIR 113a [RP 120b ; IP 110b] >
谁是IP 110a? 175
对应于IP 110a的网络端点 180
DIR供应服务? 185
对应于供应服务150a的网络端点 190
网络解析服务 115
身份提供者 110a
确定模块 145a
DIR供应服务 150a
身份提供者 110b
确定模块 145b
DIR供应服务 150b

图 1A

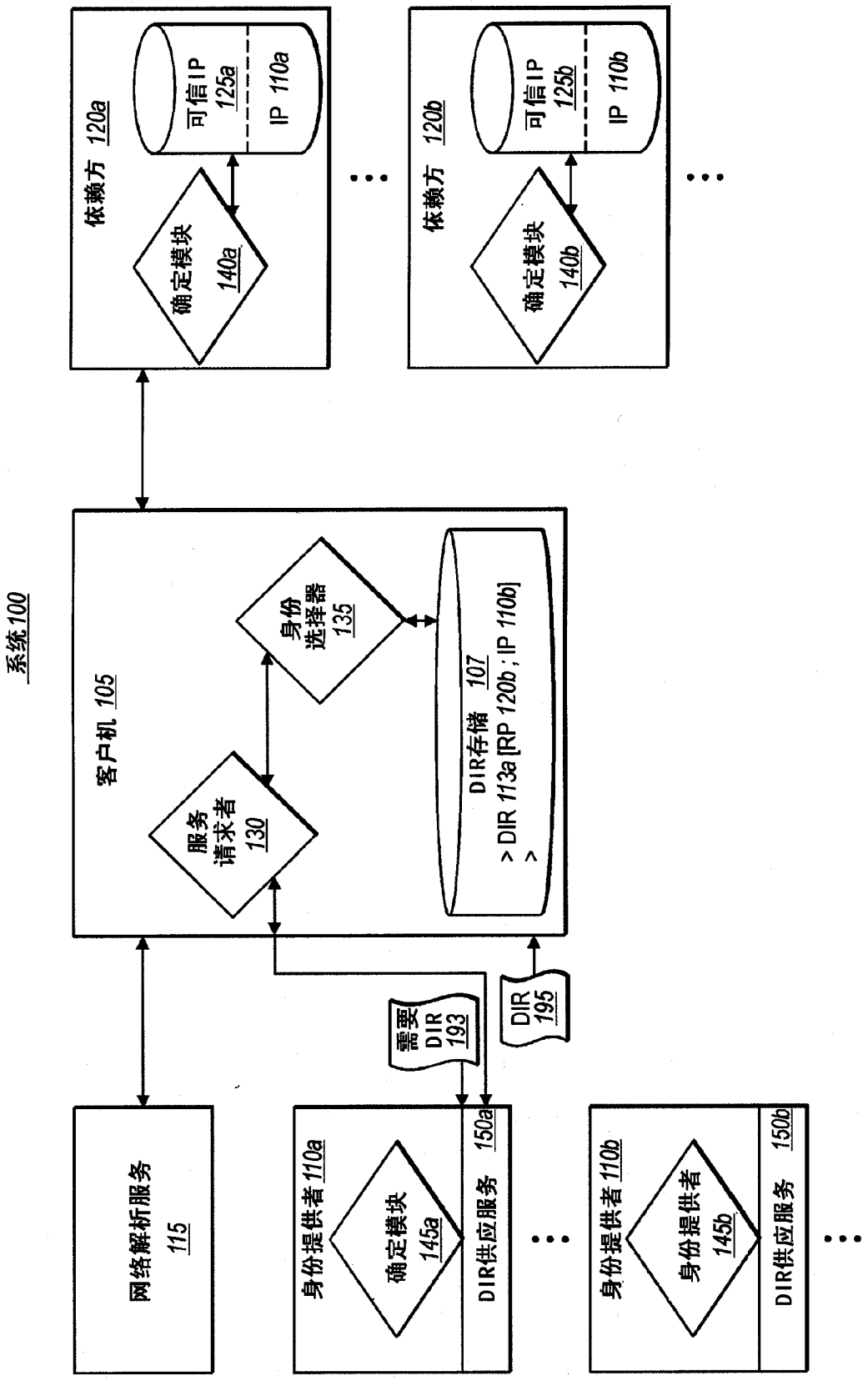

系统 100
依赖方 120a
可信IP 125a
IP 110a
确定模块 140a
依赖方 120b
可信IP 125b
IP 110b
确定模块 140b
客户机 105
身份选择器 135
服务请求者 130
DIR存储 107
> DIR 113a [RP 120b ; IP 110b]
>
需要DIR 193
DIR 195
网络解析服务 115
身份提供者 110a
确定模块 145a
DIR供应服务 150a
身份提供者 110b
身份提供者 145b
DIR供应服务 150b

图 1B

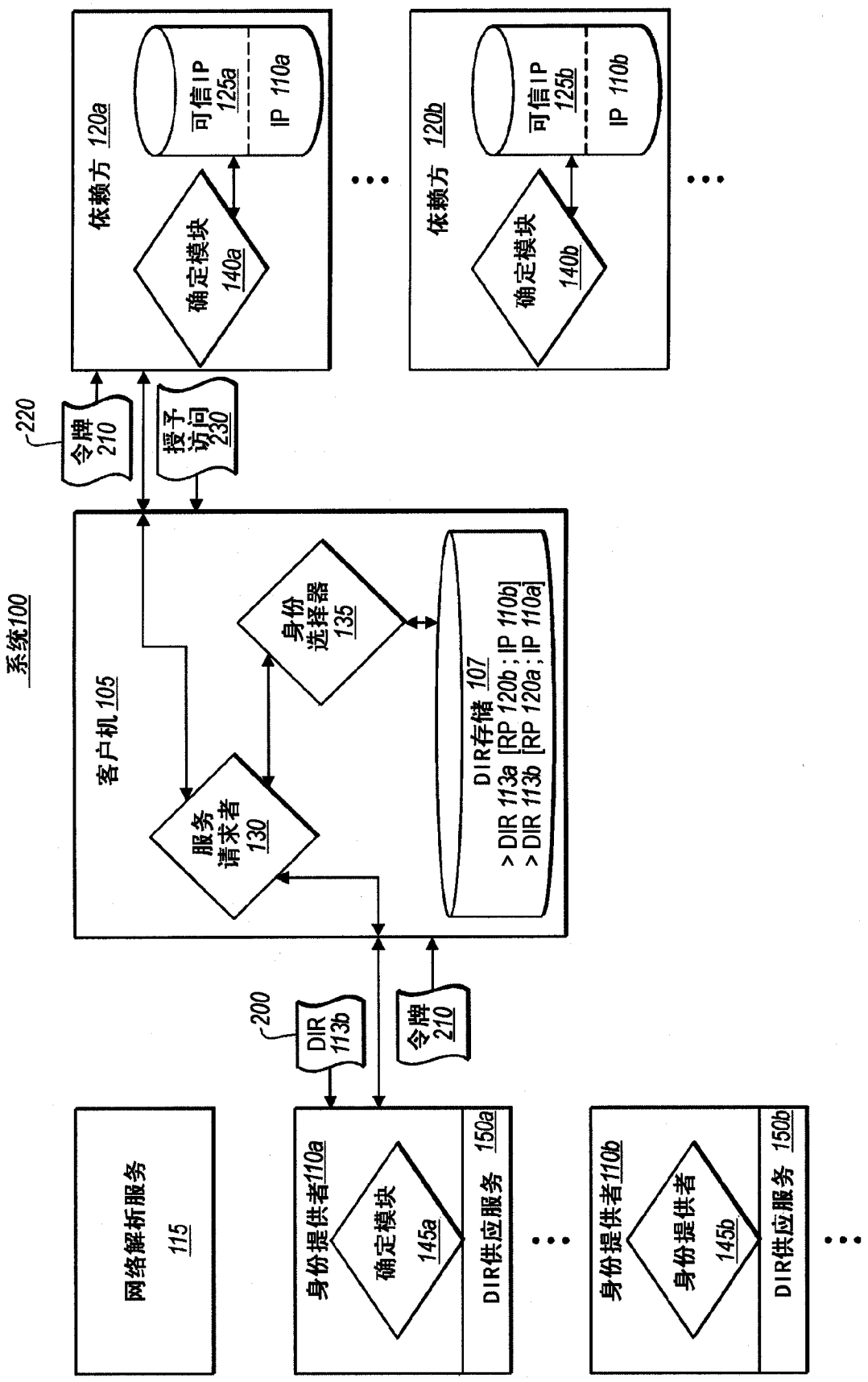

系统100
依赖方 120a
可信IP 125a
IP 110a
确定模块 140a
依赖方 120b
可信IP 125b
IP 110b
确定模块 140b
220
令牌 210
授予访问 230
客户机 105
身份选择器 135
服务请求者 130
DIR存储 107
> DIR 113a [RP 120b ; IP 110b]
> DIR 113b [RP 120a ; IP 110a]
200
DIR 113b
令牌 210
网络解析服务 115
身份提供者110a
确定模块 145a
DIR供应服务 150a
身份提供者110b
身份提供者 145b
DIR供应服务 150b

图 2

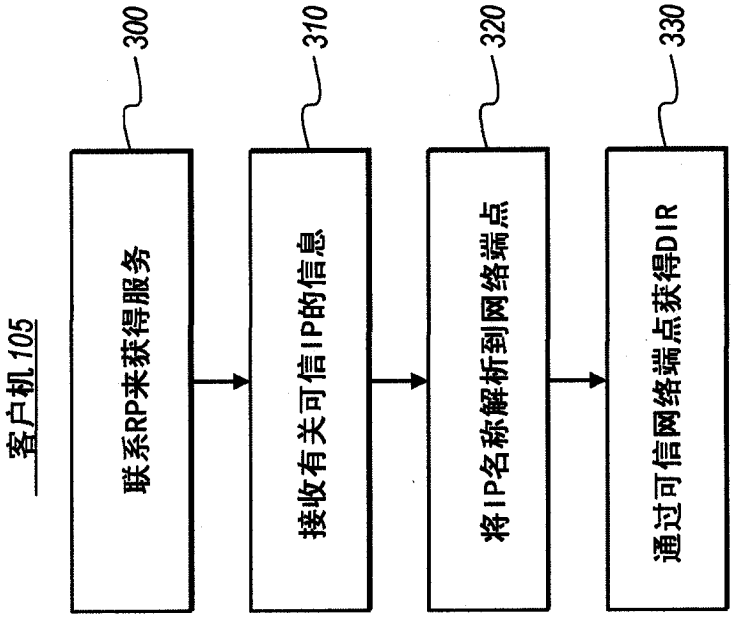

客户机 105
300
联系RP来获得服务
310
接收有关可信IP的信息
320
将IP名称解析到网络端点
330
通过可信网络端点获得DIR

图 3

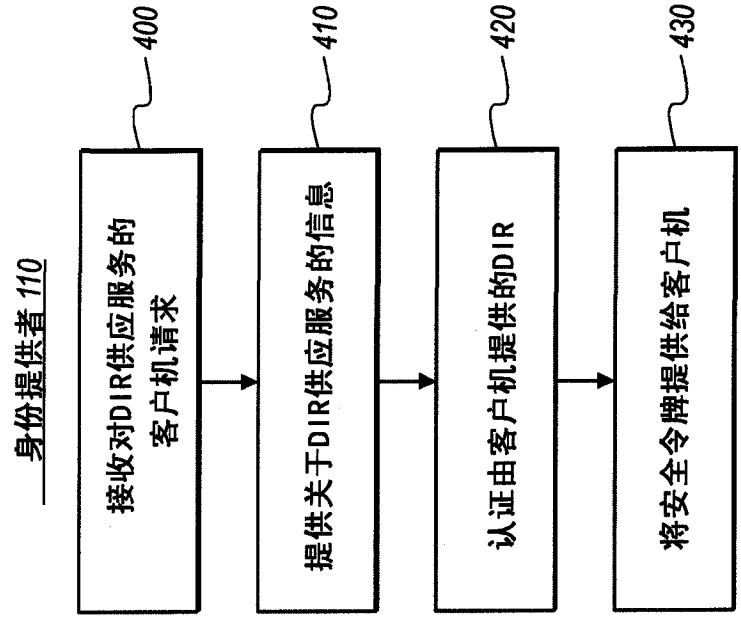

身份提供者 110
400
接收对DIR供应服务的客户机请求
410
提供关于DIR供应服务的信息
420
认证由客户机提供的DIR
430
将安全令牌提供给客户机

图 4