(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 102197399 B
(45)授权公告日 2014.10.22

(21)申请号 200980142630.X
(22)申请日 2009.10.16
(30)优先权数据
61/107,953 2008.10.23 US
12/410,680 2009.03.25 US
(85)PCT国际申请进入国家阶段日
2011.04.22
(86)PCT国际申请的申请数据
PCT/US2009/060966 2009.10.16
(87)PCT国际申请的公布数据
WO2010/048046 EN 2010.04.29
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 K·W·肖特 K·卡梅隆
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 胡利鸣
(51)Int.Cl.
G06F 21/33(2013.01)
G06F 21/45(2013.01)
G06F 21/62(2013.01)
(56)对比文件
US 2003/0163733 A1,2003.08.28,
CN 101004718 A,2007.07.25,
US 2008/0016195 A1,2008.01.17,
WO 2005/032041 A1,2005.04.07,
US 2006/0080730 A1,2006.04.13,
审查员 边臻

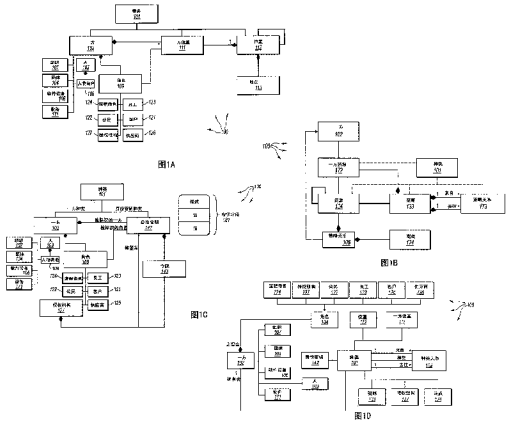
权利要求书2页 说明书13页 附图9页

(54)发明名称

对计算机存储系统内的一方身份进行建模

(57)摘要

本发明涉及用于对计算机存储系统内的一方身份进行建模的方法、系统和计算机程序产品。联合身份结构根据统一模式对计算机存储系统内的身份数据以及身份数据各部分之间的关系进行建模。联合身份结构可联合来自各种不同计算环境内的计算存储系统的分布身份以及身份关系数据。在计算环境处与联合身份结构相关联的代码和元数据可互操作以便于对联合身份结构内的身份以及身份关系数据进行统一的存储、访问、修改、删除和保护。本发明的各实施例包括利用身份密钥表格条目来定位一方身份信息并且执行不同类型的身份密钥之间的密钥转换。



CN 102197399 B

1. 在包括一个或多个处理器和系统存储器的计算机系统 (202) 上，一种用于利用联合身份结构 (207) 来定位身份相关数据的方法，所述计算机系统连接到所述联合身份结构 (207)，所述联合身份结构对计算机存储系统内的身份相关信息进行建模，所述联合身份结构跨多个不同的应用、多个不同的计算机系统 (201、203、213、214)、多个不同的上下文以及多个不同的网络提供对身份信息的一致的视图和访问，所述方法包括 ：

在一数据结构内创建第一数据对象 (212P) 的动作，所述第一数据对象表示一方，所述第一数据对象包括唯一地标识所述方的一方标识符，所述第一数据对象还包括各自标识所述方扮演的角色的多个角色类型，所述角色类型中的每一个具有相关联的角色标识符 ；

将所述第一数据对象 (212P) 插入所述联合身份结构 (207) 中的动作 ；

创建第二数据对象 (212K) 的动作，所述第二数据对象包括在所述联合身份结构内所述方使用的第一标识符，所述第二数据对象还包括所述方在与所述第一数据对象相关联的第一标识符的上下文中扮演的角色 ；

创建第三数据对象的动作，所述第三数据对象包括在所述联合身份结构内所述方使用的第二标识符，所述第三数据对象还包括所述方在与所述第二数据对象相关联的第二标识符的上下文中扮演的角色 ；

将所述第二和第三数据对象 (212K) 插入所述联合身份结构 (207) 中的动作 ；

将所述一方标识符包括在所述第二和第三数据对象中，以将所述第二和第三数据对象与所述第一数据对象相关 (233)，使得所述一方标识符与所述第一和第二标识符相关的动作 ；

接收包括所述第一标识符的请求的动作，所述请求在所述一方的角色之一的上下文中对与所述一方相关联的标识符进行请求 ；

在之后将所述第二数据对象中的第一标识符用作用于定位所述第二数据对象的模板的动作 ；

使用所述第二数据对象 (212K) 中的所述一方标识符来在使用所述第一标识符 (233) 定位所述第二数据对象 (212K) 之后定位所述第一数据对象 (212P) 的动作 ；

从所述第一数据对象 (212P) 中检索所述方的身份相关数据的动作，包括标识用于表示所述方的所述第三数据对象存在且所述第三数据对象表示所述请求中标识的所述方的角色 ；

使用所述一方标识符来定位所述第三数据对象的动作 ；以及

检索并返回所述第三数据对象中包括的所述第二标识符以满足所述请求的动作。

2. 如权利要求 1 所述的方法，其特征在于，从所述第一数据对象中检索所述方的身份相关数据的动作包括利用所述第一数据对象来检索以下的任意组合的动作 ：

对任何种类的各方通用的信息 ；

使用用于已被定位的特定种类的一方的模式存储的信息 ；

关于该一方具有的对任何其它类型的任意其他方的关系的信息 ；以及

关于与相同一方有关的替换标识符的信息。

3. 如权利要求 2 所述的方法，其特征在于，所述明确标识符的类型对应于分类数据结构内的分类条目。

4. 如权利要求 3 所述的方法，其特征在于，分类数据结构内的各个条目是相同的，而不

管它们存储在身份系统的哪个实例中。

5. 如权利要求 1 所述的方法，其特征在于，额外存在具有能够表示任意类型的任意两个实体之间的任意关系的单个模式的单个数据结构。

6. 如权利要求 5 所述的方法，其特征在于，特定的关系实例具有表示关系类型的类型。

7. 如权利要求 1 所述的方法，其特征在于，在数据结构内创建第一数据对象、所述第一数据对象表示一方的动作包括创建表示选自以下的一方的第一数据对象：组织、人、团体、服务和设备。

8. 如权利要求 1 所述的方法，其特征在于，所述方是人，并且其中所述角色选自以下各项：客户、基本公民、员工、流程角色、以及私人。

9. 一种从联合身份结构 (207) 中检索一方的身份相关数据的方法，所述联合身份结构 (207) 包括一个或多个计算机系统 (201、202、213、214)，每个计算机系统包括一个或多个处理器和系统存储器，所述联合身份结构 (207) 跨多个不同的应用、多个不同的计算机系统、多个不同的上下文以及多个不同的网络提供对身份信息的一致的视图和访问，所述方法包括以下：

所述联合身份结构接收针对一方的身份相关数据的请求 (221)，所述请求包括：

根据单个模式内的身份密钥分类定义的身份密钥类型 (231)，所述单个模式能表示能被明确标识的任何实体的存在；

指示所述身份密钥类型 (231) 的值的身份密钥值 (232)，身份密钥类型 (231) 和身份密钥值 (232) 的组合表示密钥标识表格信息 (261) 内的条目 (211K)；以及

数据值请求 (251)，所述数据值请求 (251) 表示针对来自可通过使用身份密钥类型 (231) 和身份密钥值 (232) 的组合以及对一方标识表格信息的关系来标识的一方表格条目 (212P) 中的一方相关身份数据的一部分的请求；

所述联合身份结构在所述密钥标识表格信息中定位与身份密钥类型 (231) 和身份密钥值 (232) 的组合相对应的密钥标识表格条目 (211K)；

所述联合身份结构访问来自所述密钥标识表格条目 (211K) 的一方标识符值 (233)，所述一方标识符值 (233) 与和所述身份密钥相关联的一方相对应；

所述联合身份结构基于所访问的一方标识符 (233) 和对所述一方身份表格信息的关系来参考一方身份表格信息 (262) 内的一方身份条目 (212P)；

所述联合身份结构响应于所述数据值请求 (251) 通过确定包括所请求的一方标识数据的第二密钥标识表格条目存在并从所述第二密钥标识表格中检索所述一方身份数据来从所述一方身份条目 (212P) 检索一方身份数据 (249)；以及

所述联合身份结构响应于 (222) 接收到的请求返回一方身份数据 (249)。

10. 如权利要求 9 所述的方法，其特征在于，所述联合身份结构检索一方身份数据包括所述联合身份结构检索从以下选择的一方的一方身份数据：组织、人、团体、服务和设备。

11. 如权利要求 9 所述的方法，其特征在于，所述联合身份结构检索一方身份数据包括所述联合身份结构检索具有从以下选择的角色的人的一方身份数据：客户、基本公民、员工、流程角色、以及私人。

对计算机存储系统内的一方身份进行建模

背景技术

[0001] 1. 背景和相关技术

[0002] 计算机系统和相关技术影响社会的许多方面。的确，计算机系统处理信息的能力已转变了人们生活和工作的方式。计算机系统现在通常执行在计算机系统出现以前手动执行的许多任务（例如，文字处理、日程安排和会计等）。最近，计算机系统彼此耦合并耦合到其他电子设备以形成计算机系统和其他电子设备可以在其上传输电子数据的有线和无线计算机网络。因此，许多计算任务的执行分布在多个不同的计算机系统和 / 或多个不同的计算环境上。

[0003] 存储的数据能在多个不同的范围内并在多个不同的站点处存储。例如，在公共网络（例如，基于因特网的万维网）和私有网络（例如，特定公司的内部局域网）内的计算机系统对关于个人、公司以及其他组织（政府和私有）的信息的访问越来越多。这种信息可在这些网络上的单个位置内或在多个位置内保存。此外，许多软件系统越来越多地在联网计算机和它们的人类用户之间共享或联合信息。个人以及组织之类所考虑的是，跨各种上下文、设备以及规模共享足够的信息以提供对有用数据的一致访问，但同时防止对私密信息的偶然或恶意的暴露。

[0004] 存在用于使用各种机制来检查个人和组织的真实性以及用于在传送信息之前在各种基于计算机的存储内编码或加密信息的技术。然而，这些技术依赖以下方式 :个人或组织所存储的表示可能与已知出于某些目的唯一地标识该个人或组织的字符序列相关联。这样的字符串的示例包括公司的万维网域名（诸如 www.microsoft.com），以及由 hotmail.com 向个人签发的电子邮件地址（例如 JohnDoe@hotmail.com）。这样的字符序列已知是明确的标识符，其中多个明确的标识符可标识一单个实体。然而，通常，这些明确标识符与给定实体的非标识属性没有区分地建模（例如，员工的电子邮件地址将通常是员工记录内的属性或是电子邮件表格内的元组）。

[0005] 不管选择了什么数据结构，由于单个类型的明确标识符必须被用来标识不同数据结构内的实体的事实，将明确标识符表示为任一数据结构内的属性证实是不充分的。如果明确标识符被表示为多个数据结构内的属性，那么先前不可能知道什么数据结构可能包括给定的明确标识符，从而导致系统用作大规模的查找机制是困难的、昂贵的或不可行的。

[0006] 当确定将明确标识符存储在基于计算机的存储内的方式时将产生多个问题。例如，确定表示组织和个人的适当方式通常是困难的。这可包括确定应该在基于计算机的存储内使用什么数据结构。

[0007] 此外，各个明确标识符必须通常与签发机构相关联。然而，个人或组织可具有多个明确标识符，其中各个明确标识符被用在不同的上下文中。由此，没有单个明确标识符可用作数据存储唯一标识符。例如，如果 Jane Smith 具有由 hotmail.com 签发的电子邮件地址 JaneSmith@hotmail.com 以及来自 www.gmail.com 的 JaneSmith@gmail.com，这两个标识符虽然明确但是没有一个是计算机系统内针对个人 Jane 的唯一标识符。

[0008] 此外，各个明确标识符可与一组特定的许可相关联，许可指定什么信息可通过该

明确标识符获得以及可如何使用该信息。例如，Jane 希望将她的与她当前雇主有关的身份的各方面与她的关于体现在 www.Facebook.com 或 www.hotmail.com 上的社交上下文的身份的各方面分开。她可同意授予对使用她的雇员身份创建的资源和事件的完全访问许可，但将对她在 spaces.msn.com 上的照片的访问权限制给她指定的朋友，并保持所有在 www.hotmail.com 上的她的邮件私密。

[0009] 此外，个人之间的关系、组织之间的关系、以及组织和个人之间的关系可影响身份信息如何被共享和使用。然而，至少部分地因为可被用来存储这些实体之间的关系的各种不同的数据格式，在一计算存储内—或以不同规模和在不同上下文中存在的一组计算机存储内—表示这些实体之间的关系可以是困难的。由于可被用来标识这样的关系的成员的多个明确标识符，关系也可以是难以表示的。

[0010] 某些身份信息是根据位置而置于适当的上下文中。位置可包括诸如邮寄地址等常规位置信息以及诸如动态或静态纬度和经度坐标等地理存在。与关系类似，至少部分地因为可被用来存储上下文信息的各种不同的数据格式，表示这样的上下文信息可以是困难的。

[0011] 此外，身份数据通常与使用该身份数据的应用分开。例如，身份可在为指定的应用上下文定制的不同规模的不同计算机存储内维护。由此，身份数据也通常与应用使用的应用数据分开存储。例如，X.500 可将身份数据存储在没有很好地与由访问 X.500 目录的应用所使用的应用数据集成的单独身份目录中。因此，身份数据的分类、身份数据各部分之间的关系、以及应用数据和身份数据各部分之间的关系通常在这些数据结构中很难反映。

[0012] 简要概述

[0013] 本发明涉及用于对计算机存储系统内的一方身份进行建模的方法、系统和计算机程序产品。联合身份结构对计算机存储系统内的身份数据以及身份数据各部分之间的关系进行建模。根据逻辑统一模式对身份以及身份关系数据进行建模。逻辑统一模式可表示可被明确地标识的任何实体的存在。例如，由于身份数据是根据逻辑统一模式建模的，一计算环境内的应用可容易地对由另一计算环境提供的身份以及身份关系数据进行存储、访问、修改、删除和保护。

[0014] 由此，联合身份结构可联合来自各种不同计算环境内的计算存储系统的分布身份以及身份关系数据。在计算环境处与联合身份结构相关联的代码和元数据可互操作以便于对联合身份结构内的身份以及身份关系数据进行统一的存储、访问、修改、删除和保护。例如，由于身份数据是根据逻辑统一模式建模的，一计算环境内的应用可容易地对由另一计算环境提供的身份数据进行存储、访问、修改、删除和保护。

[0015] 在某些实施例中，联合身份结构被用来定位身份相关数据。第一数据对象是在数据结构内创建的。第一数据对象在数据结构内表示来自物理或数字世界的实体。数据结构能够通过逻辑统一模式表示能被明确地标识的任何实体的存在。

[0016] 第一数据对象被存储到联合身份结构内。创建第二数据对象。第二数据对象表示在联合身份结构内使用的明确标识符。第二对象被插入到联合身份结构中。第二数据对象与第一数据对象相关。因此，该第二数据对象可在之后被用来定位第一数据对象。

[0017] 明确标识符之后被用作用于定位第二数据对象的模板。在使用明确标识符定位第二数据对象之后，第一数据对象和第二数据对象之间的关系然后被用来定位第一数据对

象。从第一数据对象检索实体的身份相关数据。

[0018] 本发明的各实施例可对身份模型内的各方、角色、人、组织、团体、位置、服务、设备、权限、分类和身份密钥进行建模。在身份模型内表示的这些对象的定义以及这些对象之间的关系可被用来导出计算机存储系统内有效的存储机制。身份模型提供一种集成并一致地维持这些对象的机制。

[0019] 因此，在某些实施例中，身份密钥（例如，第二数据对象）被用来访问一方的身份相关数据（例如，第一数据对象）。在其他实施例中，一身份密钥（例如，第二数据对象）被用来访问来自另一身份密钥的身份相关数据（例如，第三数据对象）。

[0020] 提供本发明内容是为了以简化的形式介绍将在以下具体实施方式中进一步描述的一些概念。本发明内容并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。

[0021] 本发明的附加特征和优点将在以下描述中叙述，且其一部分根据本说明书将是显而易见的，或可通过对本发明的实践来获知。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。

[0022] 附图简述

[0023] 为了描述可获得本发明的上述和其它优点和特征的方式，将通过参考附图中示出的本发明的具体实施例来呈现以上简要描述的本发明的更具体描述。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：

[0024] 图 1A-1D 示出了可被用来对身份数据进行建模以供存储在计算机存储系统内的示例模式。

[0025] 图 2A 示出了便于对计算机存储系统内的身份信息进行建模的示例计算机架构。

[0026] 图 2B 示出了图 2A 的计算机架构中用于访问来自密钥标识符的一方身份数据的一部分。

[0027] 图 2C 示出了图 2A 的计算机架构中用于转换密钥标识符的一部分。

[0028] 图 3 示出了用于对来自计算机存储系统的身份数据进行建模并访问建模身份数据的示例方法的流程图。

[0029] 图 4 示出了用于访问来自计算机存储系统的建模身份数据的示例方法的流程图。

[0030] 详细描述

[0031] 本发明涉及用于对计算机存储系统内的一方身份进行建模的方法、系统和计算机程序产品。联合身份结构对计算机存储系统内的身份数据以及身份数据各部分之间的关系进行建模。根据逻辑统一模式对身份以及身份关系数据进行建模。逻辑统一模式可表示可被明确地标识的任何实体的存在。例如，由于身份数据是根据逻辑统一模式建模的，一计算环境内的应用可容易地对由另一计算环境提供的身份以及身份关系数据进行存储、访问、修改、删除和保护。

[0032] 由此，联合身份结构可联合来自各种不同计算环境内的计算存储系统的分布身份以及身份关系数据。在计算环境处与联合身份结构相关联的代码和元数据可互操作以便于对联合身份结构内的身份以及身份关系数据进行统一的存储、访问、修改、删除和保护。例

如，由于身份数据是根据逻辑统一模式建模的，一计算环境内的应用可容易地对由另一计算环境提供的身份数据进行存储、访问、修改、删除和保护。

[0033] 在某些实施例中，联合身份结构被用来定位身份相关数据。第一数据对象是在数据结构内创建的。第一数据对象在数据结构内表示来自物理或数字世界的实体。数据结构能够通过统一模式表示能被明确地标识的任何实体的存在。

[0034] 第一数据对象被存储到联合身份结构内。创建第二数据对象。第二数据对象表示在联合身份结构内使用的明确标识符。第二对象被插入到联合身份结构中。第二数据对象与第一数据对象相关。因此，该第二数据对象可在之后被用来定位第一数据对象。

[0035] 明确标识符之后被用作用于定位第二数据对象的模板。在使用明确标识符定位第二数据对象之后，第一数据对象和第二数据对象之间的关系然后被用来定位第一数据对象。从第一数据对象中检索实体的身份相关数据。

[0036] 本发明的各实施例可对身份模型内的各方、角色、人、组织、团体、位置、服务、设备、权限、分类和身份密钥进行建模。在身份模型内表示的这些对象的定义以及这些对象之间的关系可被用来导出计算机存储系统内有效的存储机制，诸如举例而言数据服务器（例如，SQL 服务器数据库）、存储器中数据结构等等。身份模型提供一种集成并一致地维持这些对象的机制。

[0037] 因此，在某些实施例中，身份密钥（例如，第二数据对象）被用来访问一方的身份相关数据（例如，第一数据对象）。在其他实施例中，一身份密钥（例如，第二数据对象）被用来访问来自另一身份密钥的身份相关数据（例如，第三数据对象）。即，给定第一对象“A”，第二对象可被视作“A”的身份。第三对象可以是“A”的另一身份密钥。

[0038] 本发明的各实施例可以包括或利用诸如，一个或多个处理器和系统存储器等包括计算机硬件的专用或通用计算机，这将在以下做出进一步讨论。本发明范围内的各实施例还包括用于承载或存储计算机可执行指令和 / 或数据结构的物理和其他计算机可读介质。这样的计算机可读介质可以是可由通用或专用计算机系统访问的任何可用介质。存储计算机可执行指令的计算机可读介质是计算机存储介质。承载计算机可执行指令的计算机可读介质是传输介质。由此，作为示例而非限制，本发明的各实施例可包括至少两种完全不同的计算机可读介质 ：计算机存储介质和传输介质。

[0039] 计算机存储介质包括 RAM、ROM、EEPROM、CD-ROM 或其他光盘存储、磁盘存储或其他磁存储设备、或可用于存储计算机可执行指令或数据结构形式的所需程序代码装置且可由通用或专用计算机访问的任何其他介质。

[0040] “网络”被定义为允许在计算机系统和 / 或模块和 / 或其他电子设备之间传输电子数据的一个或多个数据链路。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，该计算机将该连接适当地视为传输介质。传输介质可包括可用于携带计算机可执行指令或数据结构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网络和 / 或数据链路。上述的组合也应被包括在计算机可读介质的范围内。

[0041] 此外，在到达各种计算机系统组件之后，计算机可执行指令或数据结构形式的程序代码装置可从传输介质自动转移到计算机存储介质（或者相反）。例如，通过网络或数据链路接收到的计算机可执行指令或数据结构可被缓存在网络接口模块（例如，“NIC”）内

的 RAM 中，然后最终被传送到计算机系统 RAM 和 / 或计算机系统处的较不易失性的物理存储介质。由此，应当理解，计算机存储介质可被包括在同样（或甚至主要）利用传输介质的计算机系统组件中。

[0042] 计算机可执行指令例如包括，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。计算机可执行指令可以是例如二进制代码、诸如汇编语言等中间格式指令、或甚至源代码。尽管用结构特征和 / 或方法动作专用的语言描述了本主题，但可以理解的是，所附权利要求书中定义的主题不必限于上述特征或动作。相反，上述特征和动作是作为实现权利要求的示例形式而公开的。

[0043] 本领域的技术人员将理解，本发明可以在具有许多类型的计算机系统配置的网络计算环境中实践，这些计算机系统配置包括个人计算机、台式计算机、膝上型计算机、消息处理器、手持式设备、多处理器系统、基于微处理器的或可编程消费电子设备、网络 PC、小型计算机、大型计算机、移动电话、PDA、寻呼机、路由器、交换机等等。本发明也可以在其中通过网络链接（或者通过硬连线数据链路、无线数据链路，或者通过硬连线和无线数据链路的组合）的本地和远程计算机系统两者都执行任务的分布式系统环境中实践。在分布式系统环境中，程序模块可以位于本地和远程存储器存储设备中。

[0044] 相应地，本发明的诸实施例包括多个计算机系统，该多个计算机系统通过诸如例如局域网（“LAN”）、广域网（“WAN”）或甚至因特网等网络（或作为网络的一部分）彼此连接。多个计算机系统中的至少某些计算机系统的应用可根据统一身份模型模式维持身份以及身份关系数据。由此，身份以及身份关系数据能跨各种不同的计算环境分布（例如，以下的一个或多个：不同的应用、不同的计算机系统、不同的上下文、不同的网络等等）。

[0045] 计算机系统也可以各自创建消息相关数据并通过计算机网络交换消息相关数据（例如，网际协议（“IP”）数据报和利用 IP 数据报的其他更高层协议，诸如传输控制协议（“TCP”）、超文本传输协议（“HTTP”）、简单对象访问协议（“SOAP”）等）。通过使用网络（或甚至系统总线）来传送消息，维持身份以及身份关系数据的应用可联合以产生联合身份结构。由于各个对身份以及身份关系数据建模的应用根据统一身份模型模式这么做，因此也根据统一身份模型模式对联合身份结构内的共同身份以及身份关系数据进行建模。因此，身份以及身份关系数据能通过联合身份结构跨应用进行交换。

[0046] 由此，联合身份结构可联合跨各种不同计算环境内的计算存储系统分布的身份以及身份关系数据。在计算环境处与联合身份结构相关联的计算机可执行指令和元数据可互操作以便于对联合身份结构内的身份以及身份关系数据进行统一存储、访问、修改、删除和保护。

[0047] 图 1A-1D 示出了可被用来对身份数据进行建模以供存储在计算机存储系统内的示例模式 100。模式表示关于具有关系的数字主题和资源的信息。模式 100 是可具有各种实现的逻辑统一模式。即，各种模式实现中的任一种能被用来实现示例模式 100 内的关系。数字主题的不同种类 101 可共享相同特性中的多个—尽管是不同的。模式通过称作 Party（一方）的实体来表示所有数字主题的通用方面。Party（一方）可接着被如在图 1A 中描绘地那样具体化。例如，图 1A 描绘了具有名称、描述、时间、跨度、以及 PrimaryKind（主种类）（例如，人、组织、团体、软件服务、或设备）的 Party（一方）条目。各方也可具有 SecondaryKind（次种类）。例如，组织可具有公司或政府的次种类。

[0048] 可通过组织 107、人 103、团体 104、服务 106、以及设备 171 之一来定义一方类型 102。

[0049] 图 1A 描绘了用于对一方进行建模的模式 100 的一部分。如在图 1A 中描绘的，一方类型 102 被定义为一其的具体化（如组织、人、设备、软件服务、或团体）、一个或多个一方位置、以及与其他方的一个或多个关系。

[0050] 各方可具有它们之间的关系。可通过一方对一方关系来定义各个方对方关系。

[0051] 通过一方位置 111 来定义各个方位置，从而表示一方可位于的位置。通过从一个或多个父位置细化的位置 112 来定义各个一方位置 111。通过各个地点 113 来定义各个位置 112。由此，各方可位于多于一个的位置处。对于一方所位于的各个位置，存在必须被记录的诸如表示一方与该位置相关联的持续时间的开始日期和结束日期的信息。在模型中，这些事实被记录为类型一方位置 (Party Location) 的实例，其表示关注一方相关于一位置的事实。位置可进一步由一组地理坐标定义，诸如纬度和经度值。

[0052] 可通过人物角色 108 的混合来定义一人。由此，人 (Persons) 是人物角色 (Personas) 的混合。人物角色的实例包括个人信息，诸如举例而言个人姓名、性别、和照片、以及对于人物角色所涉及的一方的引用。这允许通过跟随从人物角色到一方的引用，多个人物角色（潜在地也具有不同的种类）是相同“一人”方（被标记为默认的人物角色中的一个）的各方面。因此，个人的概念是跨这些人物角色中的一个或多个的特性的共同聚合值。例如，一个人 Jane Smith 可具有她在登录到不同网站时使用的多个人物角色，当她在不同购物网站上时她所维护的多个客户 (Customer) 角色，以及表示她受雇于 Microsoft（微软）的员工 (Employee) 角色。Jane Smith，该真实的人是一方 (Party) 的人 (Person) 类型的实例，但是希望知晓 Jane Smith 的不同方面的任何人必须获准检查描述该个人的那些不同方面的人物角色的所有类型的实例。各方可作用或被施加作用。在某些实施例中，对一方施加作用能够至少在提供其身份所必需的程度上作用。

[0053] 模式 100 调用称为角色 (Roles) 的 PartyToPartyRelationships（一方对一方关系）的具体化。角色提供一种定义并添加关于专用于给定关系的一方的各方面的信息的方式。图 1A 描绘了一方能扮演的角色 109 的示例：员工 (Employee)123、客户 (Customer)121、市民 (Citizen)122、供应商 (Vendor)126、授权机构 (Authority)127 以及流程角色 (ProcessRole)124。鉴于一方的具体化可以是互斥的，角色是混合的。由此，一方可以并经常具有多个不同的角色。

[0054] 角色除了具有已知为涉及角色针对其所扮演的一方的 ContextParty（上下文方）的引用之外，角色还具有对于“扮演”角色的一方的引用。角色可具有 StartDate（开始日期），EndDate（结束日期）以及 Kind（种类）。由此，例如，一人在给定组织的整个工作历史可被建模为在相同的人和上下文方之间的一组员工角色，从而保留各个职位何时开始以及何时结束的完整知识。相同的模式可对由人在多个组织的所有工作进行建模、或对在单一组织的单个工作进行建模、或甚至对随着时间的流逝具有某些工作的所有人进行建模。

[0055] 可通过不同上下文中的不同人物角色，例如，“家庭”人物角色和“工作”人物角色，来表示相同的人。当结合相关角色（例如，公民—可能是一个以上国家的公民；员工信息等）时，可表示关于人的多个方面的信息。

[0056] 所描绘的一方类型和角色类型是可在与联合身份结构相关联的应用之间交换的

不同类型的各方和角色的某些示例。然而，也可定义其他类型的各方和角色。例如，一组织可以是另一组织的客户。类似地，一人可以是一组织的“成员”。

[0057] 由此，更一般地，一方具有称为组织、人、团体、软件服务和设备的具体细化。一方表示其具体细化的通用属性，其中各个具体细化具有进一步表征特定概念的专用属性。例如，软件服务表示是软件代理和计算机程序的各方。

[0058] 图 1B 描绘了用于对策略和资源进行建模的模式 100 的一部分。身份模式的一种能力是要提供用于分布策略存储的基础。策略 134 被用来促进并控制各方对资源的动作。一般而言，提供对于资源 134 的访问的服务使用策略 133 来确定一方 102 是否能访问该资源以及如何访问该资源。

[0059] 资源（由资源 134 定义）可由多方拥有，每一方可控制一个或多个资源。PartyResource（一方资源）172 通过指定对特定资源以及特定一方（由一方 102 定义）的引用来表示一方 102 和资源 134 之间的关系的实例。通过 PartyResource（一方资源）172 的实例来引用管控对特定资源的访问的策略集。

[0060] 在访问控制期间，可做出至少两个策略评估。第一个策略评估是为确保访问符合与资源相关联的策略。第二个策略评估是为确保访问符合在 PartyResource（一方资源）关系中指定的策略一换言之，可应用于访问给定资源的主题方。

[0061] 例如，与销售报告相关联的策略可指出组织的具有读取许可的各个成员可访问该销售报告。在销售团体方和销售报告资源之间的 PartyResource（一方资源）关系可指定“当企业内部时有写许可”的额外策略。访问可由这些策略的组合控制。模式 100 允许这些策略中的各个策略由通过 PolicyRelationships（策略关系）173 指定的其他策略组成以允许策略组件的重用。

[0062] 软件服务 106 和端点 174 指出资源 134 可被定义为软件服务端点。

[0063] 图 1C 描绘了用于对身份密钥进行建模的模式 100 的一部分。一般地，身份密钥可以与一组令牌相关联，该组令牌中的每一个令牌支持零个或多个声明。各个声明可以是令牌的持有人获准对特定资源执行特定动作的断言的编码。

[0064] 如在图 1C 中描绘的，不同类型（人 103、团体 104、软件服务 106、组织 107 以及设备 171）的各方（由一方 102 定义）中的每一方可具有一个或多个身份密钥。身份密钥可由 IdentityKey（身份密钥）142 定义，并由授权机构（由授权机构 127 定义）分配且包括一个或多个令牌。令牌可由令牌 143 定义，并可包括一个或多个安全声明。可在密钥字段 181 内表示该数据的各个部分，诸如举例而言描述、值、以及时间窗口。

[0065] 图 1D 描绘了用于对分类进行建模的模式 100 的一部分。一般地，分类条目是可被用来描述概念是什么事物类型的类别。例如，存在不同种类的各方 102、不同种类的角色 109、不同种类的一方对一方关系、不同种类的身份密钥 142 以及不同种类的位置 112。在模式 100 中，分类条目被称为种类 101。例如，一种身份密钥可以是电子邮件别名。另一种身份密钥可以是联邦社会保险号。各个身份密钥的类别可由身份密钥实例和种类实例之间的关联来记录。

[0066] 如在图 1D 中描绘的，可为不同类型（人 103、团体 104、软件服务 106、组织 107 以及设备 171）的各方（由一方 102 定义）中的每一方制订种类，该每一方可具有由身份密钥定义的一个或多个身份。也可为策略 133、授权机构 127、以及身份密钥 142 制订种类。种

类之间的关系由种类关系 162 定义。

[0067] 由此，种类通常形成多头（即，每一种类可具有也有多个种类的多个父类别）。然而，分层安排的种类也是可能的（即，每一种类具有也有一种类的一个父类别）。诸如“父”的关联被表示为种类关系。种类关系本身可以是分类的，并因此也可与表示种类之间关系的种类的一种类相关联。

[0068] 例如，地址（一种类）可以称为位置的类型。相比于地址的概念而言，邮寄地址和账单地址（各自是一种类）可被视为地址的更为细化的定义。通过种类关系 162 的两个实例—一个从邮寄地址到地址、另一个从账单地址到地址，地址可被记录为邮寄地址和账单地址的父。分类关系的这些实例可通过引用其内容是 RefinementOf（之细分）的种类（其自己可由另一种类关系实例相关联，该另一种类关系实例将 RefinementOf（之细分）分类为其本身是一种类的 StructuralRelationship（结构关系）的类型）被分类为 ParentOf（之父）。

[0069] 因此，本发明的各实施例利用一方的概念以及其更具体的细分—人、组织、团体、服务、设备以及服务—可在使用对各方的引用的情况下使用。各方可表示来自物理世界或数字世界的对象，并且既可表示消费者也可表示包括由授权机构提供的数字服务的服务的供应者。

[0070] 通过可由一方扮演的角色的概念来加深各方的表示。每一个这样的角色引用扮演该角色的一方。角色也可引用某些它们应用于其的上下文，例如，某些其他方。例如，“员工”是可由一方（例如，一人）相对于另一方（例如，一组织）扮演的角色。在一实施例中，一人本身仅仅是人们可扮演的单个角色—例如，公民、客户、员工、流程角色、以及私人—的混合。

[0071] 单个方可扮演多种类型的角色。例如，一人可以是员工以及公民（不同类型的角色）。一方也可以具有多于一个的相同类型的角色。例如，一人可扮演两个员工角色，每个员工角色针对不同的组织。一方可在不同的（可能重叠的）时间跨度具有相同类型的角色并在相同的上下文中。各方通常支持不同类型的一方对一方关系（诸如，“谁的朋友”，下属、主管等等）。

[0072] 各方中的每一方以及一方扮演的单独角色可通过多种不同的方式来唯一地标识—例如，通过使用电子邮件地址、联合标识符、员工编号等等。本发明的各实施例包括使用身份密钥数据类型来表示唯一标识符。身份密钥数据类型指示各个方的安全身份（安全特征是可变化的），例如，由已知授权机构（其本身是由某一方扮演的角色）签发的。

[0073] 身份密钥可通过给定类型的唯一值来区别并可引用相关方。一个益处是任何给定类型的身份密钥可通过任何其他身份密钥的呈现被有效地定位，并且对相关方的引用以及相关联的角色可被有效地获得。由此，身份密钥的使用许可数字经验的定制—例如，对于访问各个数据的许可。

[0074] 本发明的各实施例还利用位置类型来支持各方可被定位的不同类型的物理和虚拟地点。可使用文本字段（如使用地址）或使用地理坐标来描述位置。由于各方、位置以及身份密钥可具有大量以及非常不同的种类，先前描述为种类的分类机制可被用来定义并记录各个种类变化的类型。如先前描述的，种类可以是多头或分层的，并且其本身可以是分类的（即，可存在种类的种类）。

[0075] 不同类型的各方和位置的使用配合不同类型的身份密钥和不同类型的一方对一方关系提供了益处，该益处关于将涉及在例如世界规模上表示信息所需的跨多个机器边界的极大量各方的信息划分。这些益处便于在相对大的（以及可能巨大的）对象空间内的定位，并且最重要的，促进跨这些空间的通过引用的关系的表示。以上定义的数据结构和机制可在多个不同种类的包括盘上和存储器内的数据库的计算机存储中有效地实现。计算机存储可被用来表示逻辑集中式储存库。当身份数据跨多个不同的计算环境分布时，联合身份结构可表示逻辑集中式储存库。不同的计算环境内的计算机系统可包括用于组成联合身份结构的计算机可执行指令和元数据。由此，在计算机系统处的计算机可执行指令和元数据可互操作以组成联合身份结构并将集中式存储库反射回计算机系统。

[0076] 集中式存储库可根据模式 100 的各种数据模型存储数据结构和机制（例如，应用和服务）。由此，构建在和 / 或集成到集中式存储库中的应用和服务可被配置成根据各种数据模型处理数据。结果，应用和服务可相互共享以对象为中心的数据，诸如举例而言身份相关数据。

[0077] 本发明的各实施例还从各种不同角度跨变化的上下文、设备、以及规模提供对信息的一致访问。例如，一个人可在印度旅游时使用蜂窝电话通过无线因特网连接、或该人可使用美国办公室内的台式计算机系统通过企业 LAN 连接来一致地访问他的或她的信息。处理这样的通信的服务和应用可具有用于处理根据模式 100 的各种数据模型来定义的身份相关数据的嵌入计算机可执行指令和元数据。因此，用于跨多个规模、设备以及上下文导航的功能可被包括为联合（例如，逻辑统一的身份结构内的组件。

[0078] 本发明的各实施例通过采用用来主管数据的相同数据结构和便于复制的元数据对该数据进行复制和高速缓存，来提供对信息的访问。复制和高速缓存提供对实时采用电信系统访问存储在包括因特网的网络中别处的信息的有效替换。例如，关于 Jane Doe 的各方的身份信息，包括一方对一方关系、身份密钥、位置信息等等，可按在别处使用的相同逻辑结构被复制到她的蜂窝电话上。由此，即使与中央位置的通信是困难或昂贵的，在她的蜂窝电话上的应用也可有效地处理身份数据。此外，相对于在其他数据存储中呈现的信息对象的协同定位，她所携带的信息的混合可表示不同的信息对象的协同定位（即，不同的设备和设备集可包括共享信息对象的不同编组）。

[0079] 图 2A 示出了便于对计算机存储系统内的身份信息进行建模的示例计算机架构 200。如在计算机架构 200 内描绘的，计算机系统 201、202、213 和 214 连接到联合身份结构 207。各个计算机系统 201、202、213 和 214 可包括具有用于组成并关联联合身份结构 207 的计算机可执行指令和元数据的应用。例如，各个计算机系统 201、202、213 和 214 可包括具有用于向分别在各个计算机系统 201、202、213 和 214 上的其他应用将联合身份结构 107 呈现为身份数据的集中式存储库的计算机可执行指令和元数据的应用。各个计算机系统 201、202、213 和 214 也可包括具有与联合身份结构 207 进行互操作以便于对联合身份结构 207 内的身份以及身份关系数据进行统一存储、访问、修改、删除和保护的计算机可执行指令和元数据的应用。

[0080] 例如，计算机系统 201 可本地地将密钥标识表格 201K 以及一方标识表格 210P 维护在诸如例如盘上或系统存储器内。密钥标识表格 201K 可包括根据图 1C 中的模型定义的一个或多个密钥标识条目。例如，条目 211K 包括密钥类型 231（例如，电子邮件别名）、密

钥 ID 值（例如，jdoe@test.com）、一方 ID 233（与具有 jdoe@test.com 的电子邮件别名的人对应的 ID）、以及可任选的角色 ID 234（与由一方 ID233 标识的人的角色对应的 ID 针对该电子邮件别名选用）。

[0081] 一方标识表格 201P 可包括根据图 1A 中的模型定义的一个或多个一方标识条目。例如，条目 211P 包括一方类型 235（从组织、人、团体、服务和设备中选择的一方的类型）、一方 ID 值 236（一方类型的 ID 值）、角色类型 237（来自那些为一方类型定义的角色的类型，诸如举例而言客户、基本公民、员工、流程角色、私人、授权机构等等）以及角色 ID 值（角色类型的 ID 值）。条目 211P 在适当时还可包括一个或多个位置以及一方对一方关系。条目 211P 还可包括身份数据值 239。身份数据值 239 表示一方的数据，诸如例如，显示名称。身份数据值 239 可包括与一方相关联的任何数据并用或不用该方的身份密钥表示。例如，一方的电话号码可被用在身份密钥内，但也可被包括在身份数据值 239 内。

[0082] 计算机系统 201 处的应用还可将密钥标识表格 201K 和一方标识表格 201P 缝合到联合身份结构 207 中。

[0083] 计算机系统 202 处类似的应用可将密钥标识表格 202K 和一方标识表格 202P 缝合到联合身份结构 207 中。如所描绘地，密钥标识表格 202K 包括条目 212K，该条目 212K 包括密钥类型 241、密钥 ID 值 242、一方 ID 值 233 和可任选的角色 ID234。由于条目 212K 包括一方 ID 233 和可能的角色 ID 234，条目 212K 可指示与和密钥类型 231 相关联的相同方对应的不同类型的密钥（即，一方 ID 值 233 和 / 或角色 ID 234 链接条目 211K 和 212K）。

[0084] 也如所描绘的，一方标识表格 202P 包括条目 212P，该条目 212P 包括一方类型 245、一方 ID 值 233、角色类型 246、角色 ID 234、其他字段以及标识数据值 249。由于条目 212P 包括一方 ID 233 以及可能的角色 ID 234，与一方 ID 值 233 和 / 或角色 234 相关联的密钥条目可被用来定位身份数据值 249。

[0085] 在其他计算机系统（例如，潜在的计算机系统 213 和 214）处的类似应用可将密钥标识表格 203K 和 204K 以及一方标识表格 206P 缝合到联合身份结构 207 中。

[0086] 计算机系统 201 处的应用还可向计算机系统 201 处的其他应用（例如，应用 208）将联合身份结构 207 呈现为中央存储库。由此，计算机系统 201 处的应用可将密钥标识表格 201K、202K、203K、和 204K 共同地视为密钥标识表格信息 261。类似地，计算机系统 201 处的应用可将一方标识表格 211P、212P 和 206P 共同地视为一方标识表格信息 262。计算机系统 202、213 和 214 可具有提供类似功能的应用。因此，在计算机系统 201、202、213 和 214 中任一计算机系统处的应用可安全地访问、修改并删除联合身份结构 207 内根据模式 100 内的定义的身份以及身份关系数据。

[0087] 图 3 示出了用于对来自计算机存储系统的身份数据进行建模并访问建模身份数据的示例方法的流程图。将关于附图 2A 中的组件和数据以及模式 100 内的定义来描述方法 300。

[0088] 方法 300 包括在数据结构内创建第一数据对象的动作，该第一数据对象在数据结构内表示来自物理或数字世界的实体，该数据结构能够通过逻辑统一模式表示可被明确标识的任何实体的存在（动作 301）. 例如，计算机系统 202 可在一方标识表格 202P 内创建条目 212P。条目 212P 可根据图 1A 内的数据模型来表示组织。方法 300 包括将第一数据对象插入联合身份结构中的动作（动作 302）。例如，计算机系统 202 可将条目 212P 缝合到联合

身份结构 207 中。

[0089] 方法 300 包括创建第二数据对象的动作，该第二数据对象包括在联合身份结构中使用的明确标识符的表示（动作 303）。例如，计算机系统 202 可以创建条目 212K。条目 212K 的各种特征，诸如举例而言字段值的组合，可被用来在联合身份结构 207 内表示条目 212K 的明确标识符。方法 200 包括将第二数据对象插入联合身份结构中的动作（动作 304）。例如，计算机系统 202 可将条目 212K 缝合到联合身份结构 207 中。

[0090] 方法 300 包括将第二数据对象和第一数据对象相关使得第二数据对象能在之后被用来定位第一数据对象的动作（动作 305）。将相同的值包括到两个不同的条目中可被用来将条目互相相关。例如，对条目 212K 和条目 212P 中的一方 ID 值 233 的引用将条目 212K 和 212P 互相相关。由此，条目 212K 可被用来定位条目 212P（并且可能反之亦然）。

[0091] 方法 300 包括用于通过关系来访问来自第一对象的身份相关数据的以功能结果为导向的步骤（步骤 309）。步骤 309 可包括实质上任意对应动作来实现通过关系访问来自第一对象的身份相关数据的结果。然而，在方法 300，步骤 309 包括在之后将明确标识符用作用于定位第二数据对象的模板的对应动作（动作 306）。例如，应用 208 可将查询 221 发送到联合身份结构 207。查询 221 可包括条目 212K 的明确标识符。联合身份结构 207 可接收来自应用 208 的查询 221。联合身份结构 207 可使用明确标识符来定位条目 212K。

[0092] 在方法 300 中，步骤 309 还包括使用第一数据对象和第二数据对象之间的关系来在使用明确标识符定位第二数据对象之后定位第一数据对象的动作（动作 307）。例如，联合身份结构 207 可使用来自条目 212K 的字段值（例如，一方 ID 值 233）来在使用明确标识符定位条目 212K 之后定位条目 212P。

[0093] 在方法 300 中，步骤 309 还包括从第一数据对象中检索实体的身份相关数据的动作（动作 308）。例如，联合身份结构 207 可从条目 212P 中检索身份相关数据。身份相关数据可包括对任何种类的各方通用的信息、使用用于已经定位的特定种类的一方的模式所存储的信息、关于一方具有的对任何类型的任意其他方的关系的信息、或关于与相同方有关的替换明确标识符的信息。

[0094] 图 4 中描绘了可被用来实现通过关系来访问来自第一对象的身份相关数据的结果（即，步骤 309）的对应动作的另一实例。图 4 示出了用于访问来自计算机存储系统的建模身份数据的示例方法 400 的流程图。图 2B 示出了图 2A 的计算机架构中用于访问来自密钥标识符的一方身份数据的一部分。方法 400 将关于图 2A 和 2B 中的组件和数据来描述。

[0095] 方法 400 包括接收一方对身份相关数据的请求的动作（动作 401）。例如，参考图 2B，联合身份结构 207 可接收查询 221。请求可包括根据单个模式内的身份密钥分类定义的身份密钥类型。单个模式能够表示可被明确地标识的任何实体的存在。请求还可包括指示身份密钥类型的值的身份密钥值。身份密钥类型和身份密钥值的组合（明确地）表示密钥标识表格信息内的条目。例如，如图 2B 中描绘的，查询 221 包括密钥类型 231 和密钥 ID 值 232。简要地再参考图 2A，密钥类型 231 和密钥 ID 值 232 的组合明确地表示密钥标识表格信息 261 内的条目 211K（或是条目 211K 的明确标识符）。

[0096] 请求也可包括数据请求。该数据请求通过使用身份密钥类型和身份密钥值的组合以及对其他标识表格信息的关系表示对身份相关数据的一部分的请求。在某些实施例中，请求是数据值请求。该数据值请求表示针对来自可通过使用身份密钥类型和身份密钥值的

组合以及对一方标识表格信息的关系来标识的一方表格条目中的一方相关身份数据的一部分的请求。

[0097] 例如，如在图 2B 中描绘地，查询 221 包括数据值请求 241。该数据值请求 251 表示针对来自可通过使用身份密钥类型 231 和身份密钥值 232 的组合以及对一方标识表格信息 262 的关系来标识的一方表格条目中的一方相关身份数据的一部分的请求。

[0098] 方法 400 包括在密钥标识表格信息中定位与身份密钥类型和身份密钥值的组合相对应的密钥标识表格条目的动作（动作 402）。例如，联合身份结构 207 可在密钥标识表格信息 262 中定位与密钥类型 231 和密钥 ID 值 232 的组合相对应的条目 221K。方法 400 包括访问来自密钥标识表格条目的一方标识符值的动作，该一方标识符值对应于与身份密钥相关联的一方（动作 403）。例如，联合身份结构 207 可访问来自条目 211K 的一方 ID 值 233。

[0099] 方法 400 包括基于所访问的一方标识符以及对该一方标识符的关系来引用其他表格信息内的条目的动作 (404)。例如，联合身份结构 207 可基于既被包括在条目 211K 中又被包括在条目 212P 中的一方 ID 值 233 来引用条目 212P（在一方标识表格 202P 中）。

[0100] 方法 400 包括响应于数据请求，从其他表格内的条目中检索身份数据的动作（动作 405）。例如，联合身份结构 405 可从条目 212P 中检索身份数据值 249（例如，显示名称）。身份数据值 249 可响应于数据值请求 251。方法 400 包括响应于接收到的请求返回身份数据的动作（动作 406）。例如，联合身份结构 207 可响应于查询 221 返回包括数据值 249 的结果 222（例如，返回到应用 208）。

[0101] 或者，数据请求是密钥类型请求。本发明的各实施例包括实现针对密钥类型请求的方法 400。密钥类型请求表示针对与一方相关联的第二身份密钥类型的对应密钥值的请求。也可根据单个模式内的身份密钥分类来定义第二身份密钥类型。例如，现在参考图 2C，密钥类型 231 可以是电子邮件别名的密钥类型，而密钥 ID 值 232 可以是 jdoe@test.org。此外，查询 221 包括密钥类型请求 271。密钥类型请求 271 表示针对密钥标识表格信息 261 内密钥类型 241 的密钥标识条目的请求。也可根据模式 100 来定义密钥类型 241。密钥类型 241 可以是电话号码的密钥类型。因此，查询 221 可以是针对具有电子邮件别名 jdoe@test.org 的一方的电话号码的请求。

[0102] 联合身份结构 207 然后可在密钥标识表格信息 262 中定位与密钥类型 231 和密钥 ID 值 232 的组合相对应的条目 221K。即，联合身份结构 207 可定位具有 jdoe@test.org 的值的电子邮件别名的密钥条目。联合身份结构 207 然后可访问来自条目 211K 的一方 ID 值 233。一方 ID 值 233 表示具有电子邮件别名 jdoe@test.org 的一方的 ID 值。

[0103] 联合身份结构 207 然后可参考密钥标识表格信息 261 来定位条目 212K。条目 212K 具有密钥类型 241 并包括一方标识符 233。即，条目 212K 是具有电子邮件别名 jdoe@test.org 的一方的电话号码的身份密钥。联合身份结构 207 然后可从条目 212K 中检索密钥 ID 值 242（例如，电话号码）。联合身份结构 207 可响应于查询 221 返回包括密钥 ID 值 242 的结果 222（例如，返回到应用 108）。

[0104] 因此，本发明的各实施例包括利用身份密钥表格条目来定位一方身份数据（例如，如在图 2B 中描绘的）以及执行不同类型的身份密钥之间的转换（例如，如图 2C 中描绘的）。更一般地，一个数据对象（例如，第二数据对象）可以是重定向到或间接来自另一数

据对象（例如，第一数据对象）的统一配置点。即，一数据对象可被配置为提供另一数据对象的明确标识（例如，通过该一个对象和另一对象之间的关系来配置）。由此，现有的不可被明确标识的对象依然可通过使用是可被明确标识的另一相关对象来明确地标识。

[0105] 本发明可具体化为其它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。从而，本发明的范围由所附权利要求书而非前述描述指示。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。

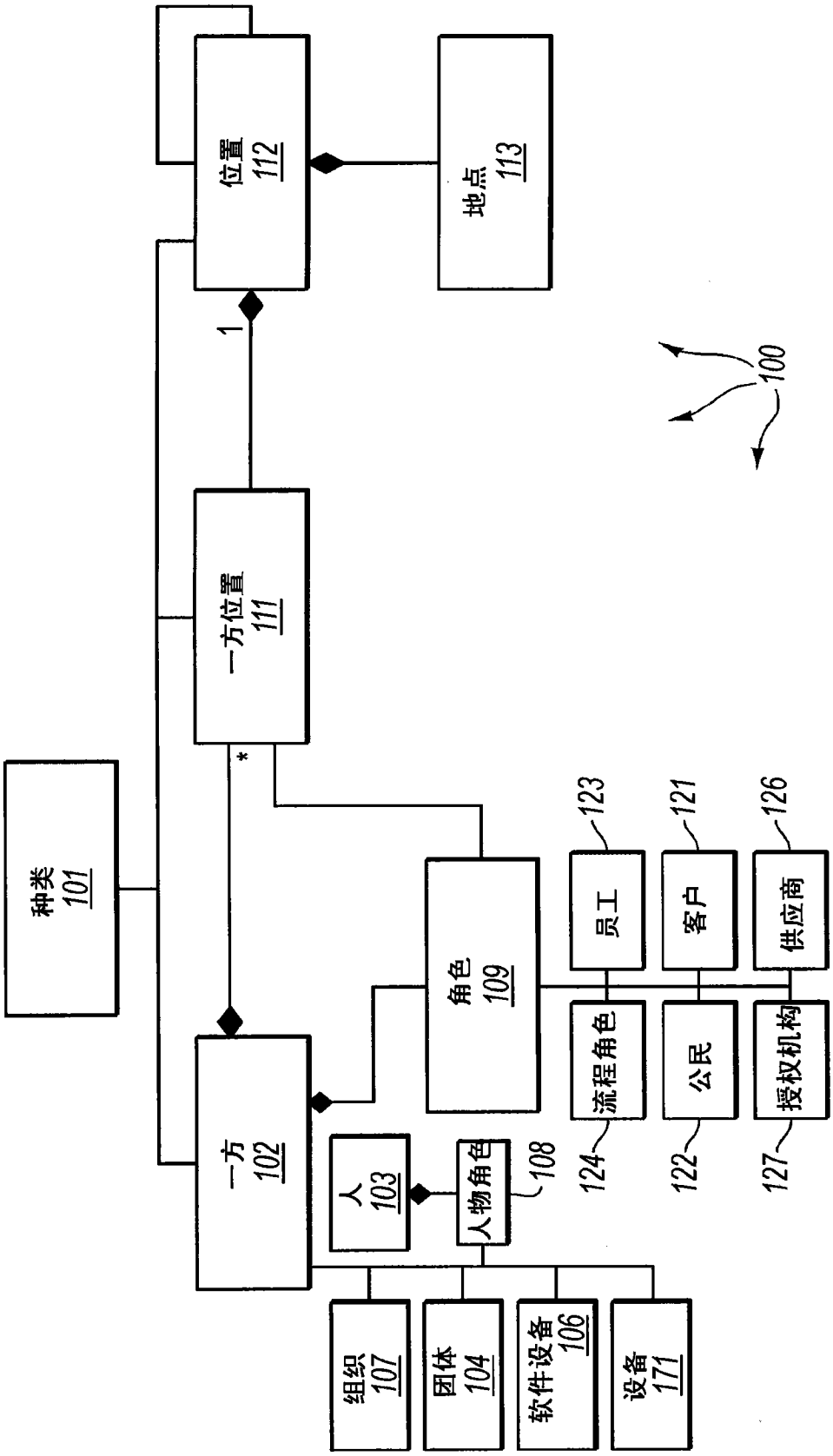

位置 112
地点 113
1
100
一方位置 111
*
种类 101
角色 109
123
员工
121
客户
126
供应商
流程角色
公民
授权机构
124
122
127
一方 102
人 103
人物角色
108
组织 107
团体 104
软件设备 106
设备 171

图 1A

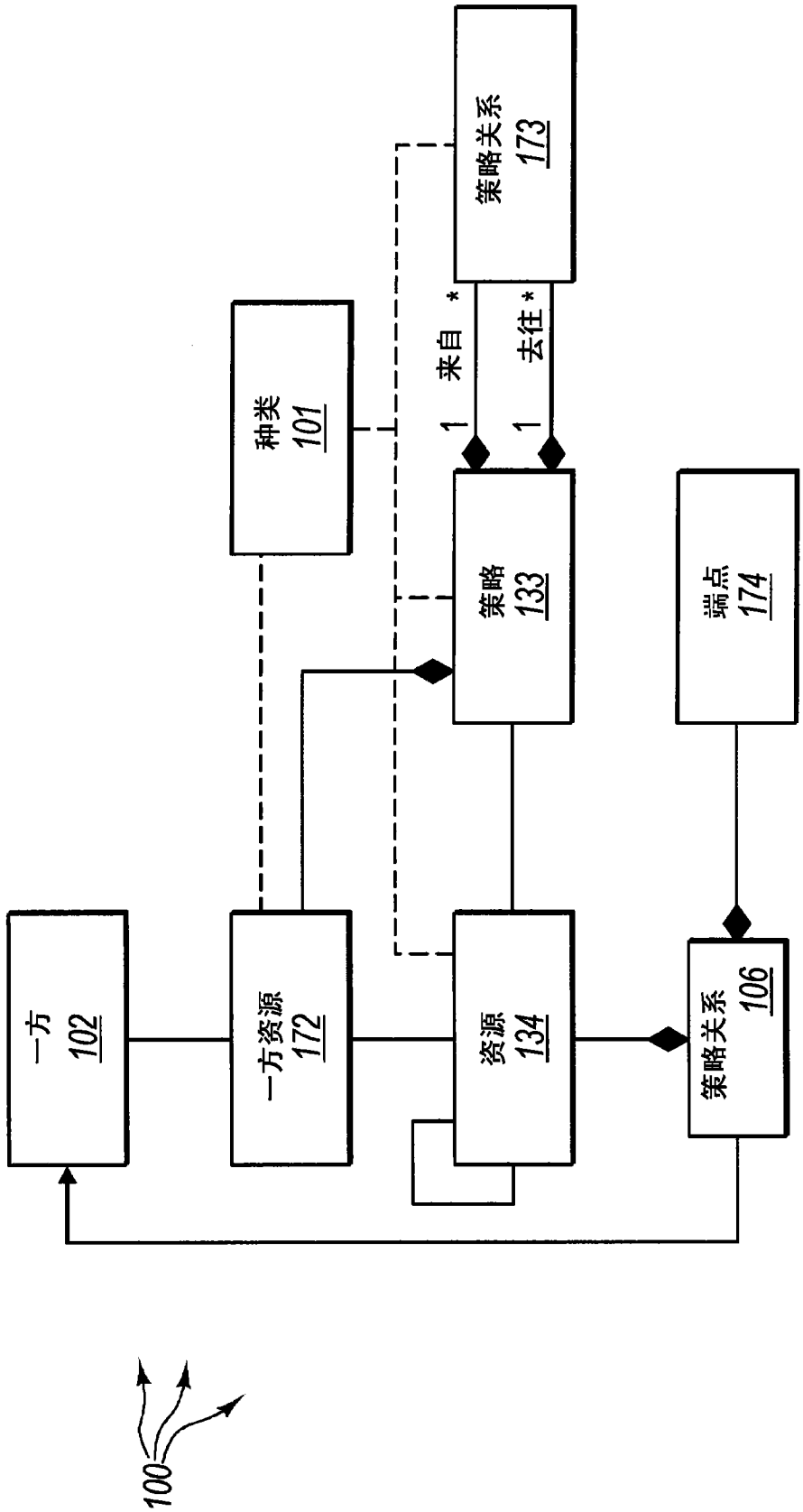

策略关系
173
种类
101
1 来自 *
1 去往 *
策略
133
端点
174
一方
102
一方资源
172
资源
134
策略关系
106
100

图 1B

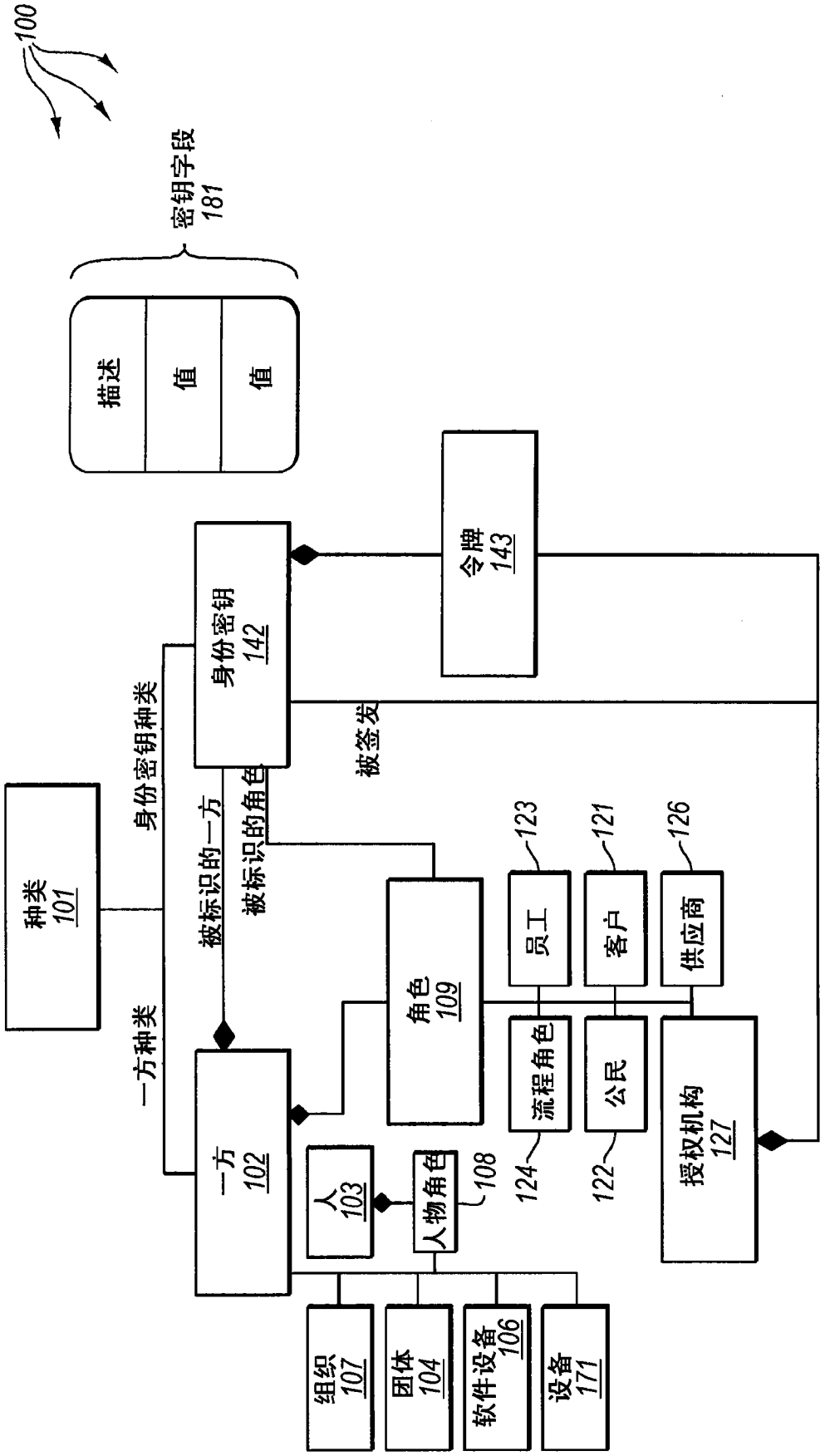

100
密钥字段
181
描述
值
值
令牌
143
身份密钥
142
被签发
身份密钥种类
被标识的一方
被标识的角色
种类
101
一方种类
一方
102
角色
109
员工
123
客户
121
供应商
126
流程角色
124
公民
122
授权机构
127
人
103
人物角色
108
组织
107
团体
104
软件设备
106
设备
171

图 1C

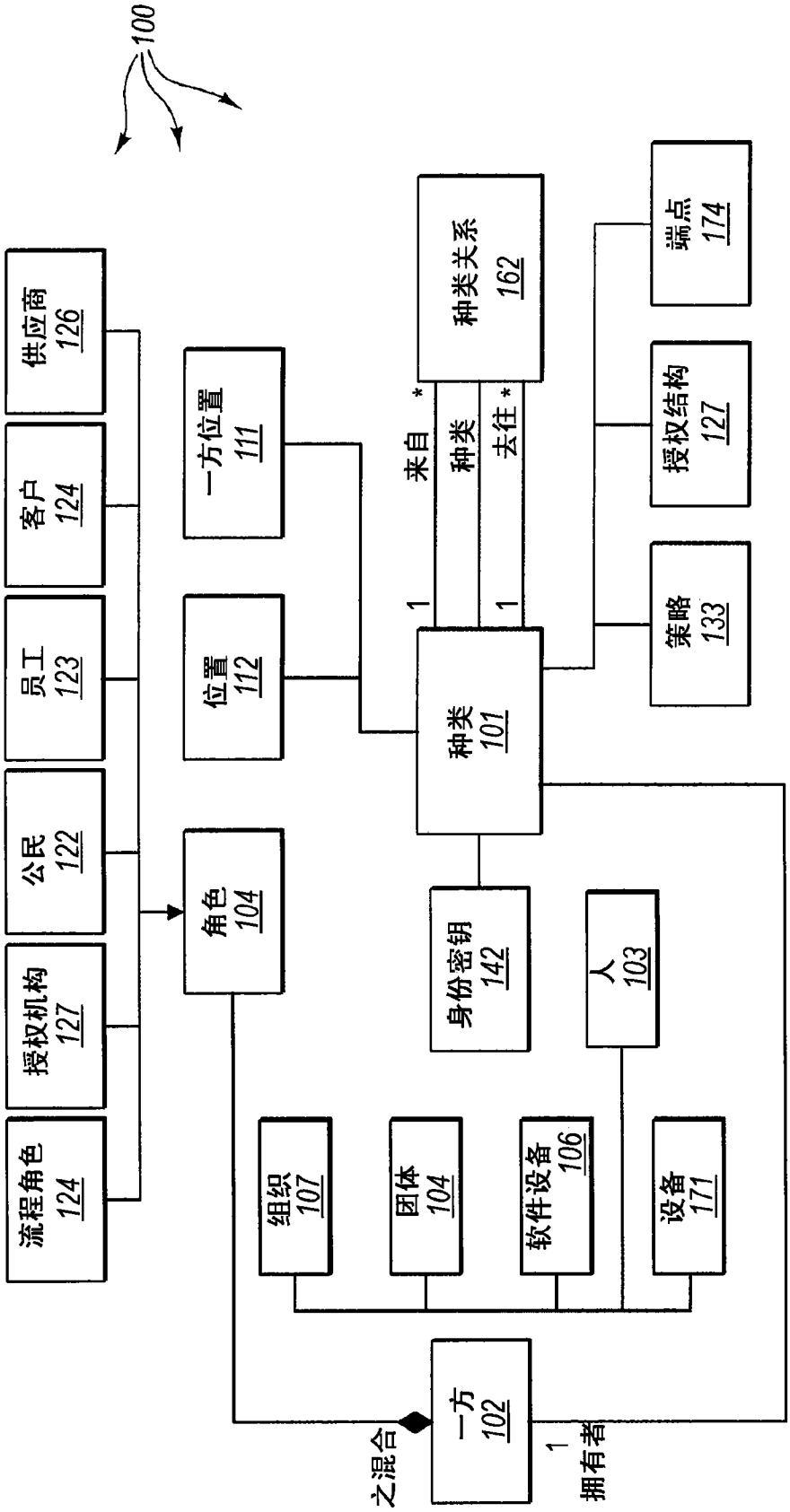

100
供应商 126
客户 124
员工 123
公民 122
授权机构 127
流程角色 124
一方位置 111
位置 112
角色 104
种类关系 162
来自 *
种类
去往 *
1
1
种类 101
端点 174
授权结构 127
策略 133
身份密钥 142
人 103
组织 107
团体 104
软件设备 106
设备 171
一方 102
之混合
1
拥有者

图 1D

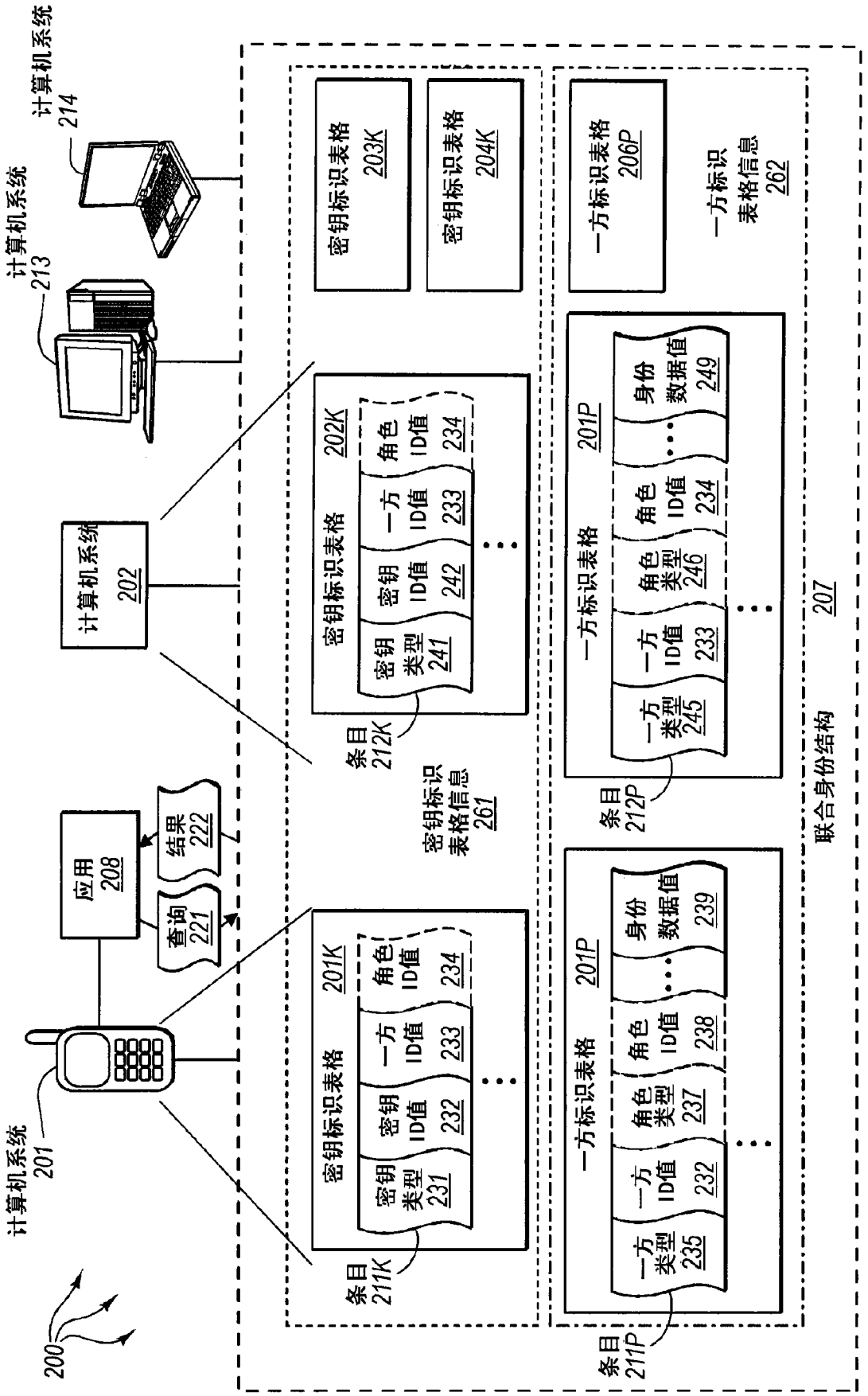

计算机系统 214
计算机系统 213
计算机系统 201
计算机系统 202
应用 208
查询 221
结果 222
200
密钥标识表格 203K
密钥标识表格 204K
一方标识表格 206P
一方标识表格信息 262
密钥标识表格 202K
密钥类型 241
密钥ID值 242
一方ID值 233
角色ID值 234
条目 212K
密钥标识表格信息 261
一方标识表格 201P
一方类型 245
一方ID值 233
角色类型 246
角色ID值 234
身份数据值 249
条目 212P
密钥标识表格 201K
密钥类型 231
密钥ID值 232
一方ID值 233
角色ID值 234
条目 211K
一方标识表格 201P
一方类型 235
一方ID值 232
角色类型 237
角色ID值 238
身份数据值 239
条目 211P
联合身份结构 207

图 2A

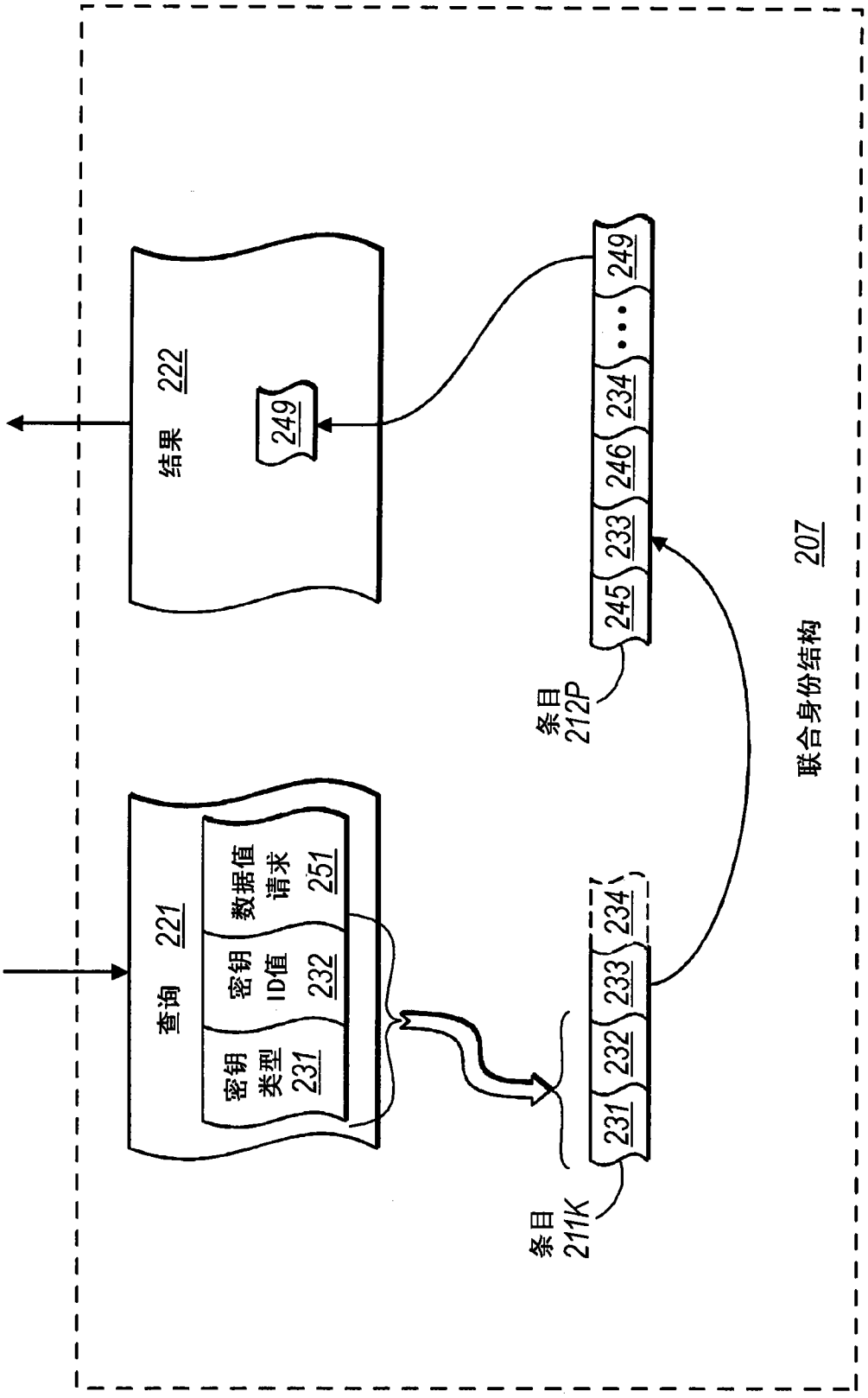

结果 222
249
查询 221
密钥类型 231
密钥ID值 232
数据值请求 251
条目 212P
245 233 246 234 ... 249
条目 211K
231 232 233 234'
联合身份结构 207

图 2B

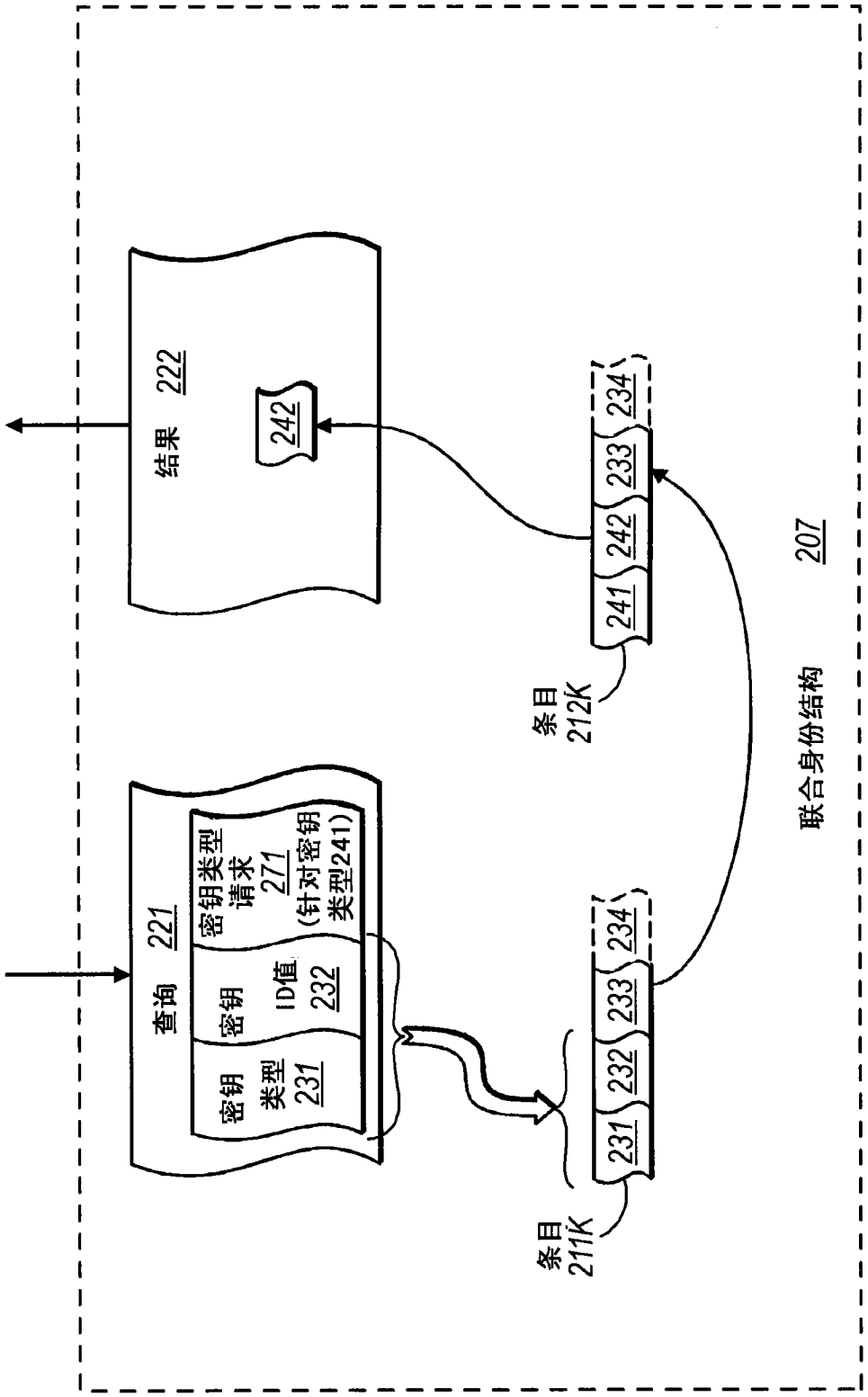

查询 221
密钥类型 231
密钥 ID值 232
密钥类型请求 271 (针对密钥类型241)
结果 222
242
联合身份结构 207
条目 211K
231 232 233 234
条目 212K
241 242 233 234

图 2C

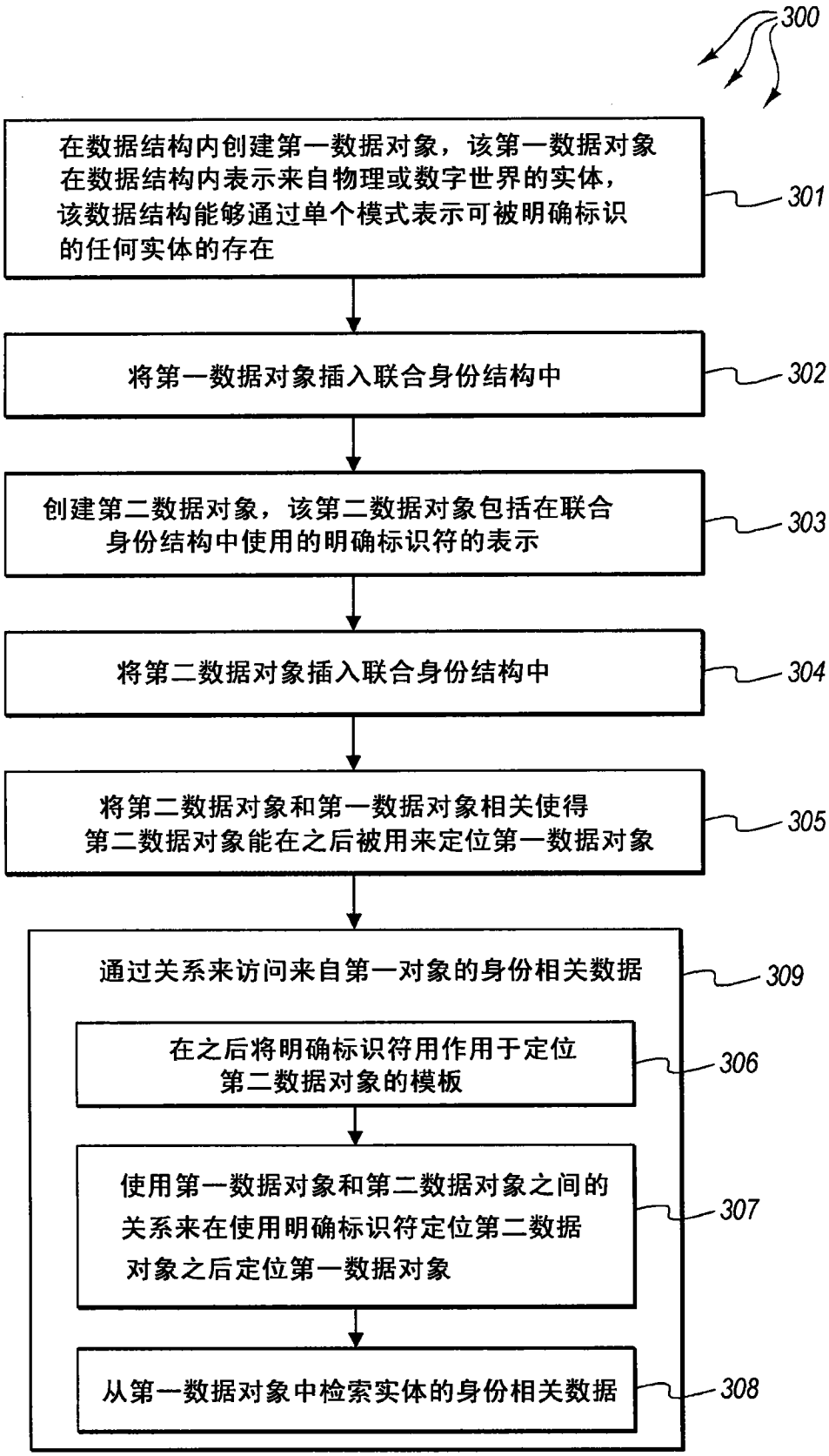

300
在数据结构内创建第一数据对象，该第一数据对象在数据结构内表示来自物理或数字世界的实体，该数据结构能够通过单个模式表示可被明确标识的任何实体的存在
301
将第一数据对象插入联合身份结构中
302
创建第二数据对象，该第二数据对象包括在联合身份结构中使用的明确标识符的表示
303
将第二数据对象插入联合身份结构中
304
将第二数据对象和第一数据对象相关使得第二数据对象能在之后被用来定位第一数据对象
305
通过关系来访问来自第一对象的身份相关数据
309
在之后将明确标识符用作用于定位第二数据对象的模板
306
使用第一数据对象和第二数据对象之间的关系来在使用明确标识符定位第二数据对象之后定位第一数据对象
307
从第一数据对象中检索实体的身份相关数据
308

图 3

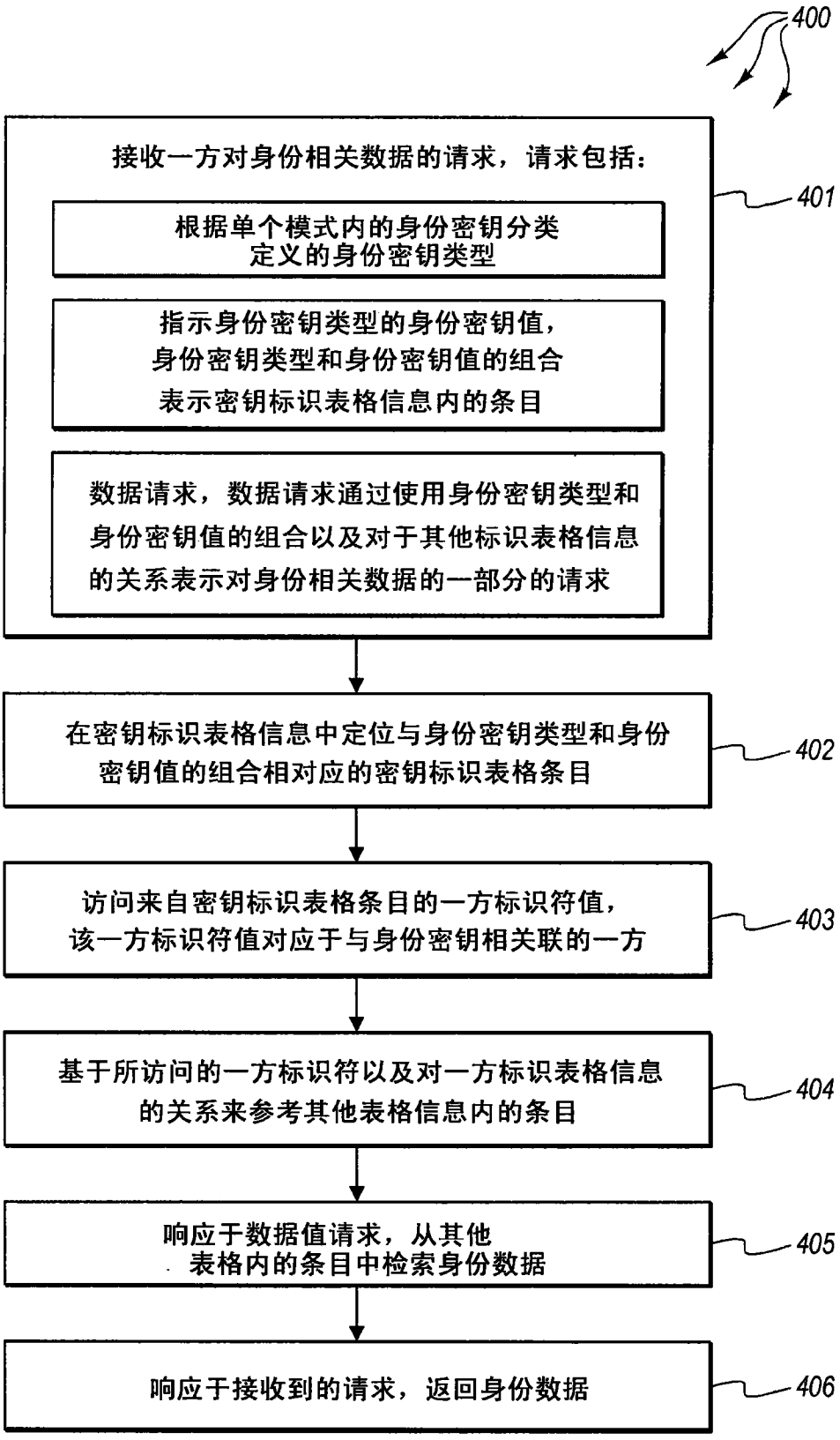

400
接收一方对身份相关数据的请求，请求包括：
根据单个模式内的身份密钥分类定义的身份密钥类型
指示身份密钥类型的身份密钥值，身份密钥类型和身份密钥值的组合表示密钥标识表格信息内的条目
数据请求，数据请求通过使用身份密钥类型和身份密钥值的组合以及对于其他标识表格信息的关系表示对身份相关数据的一部分的请求
401
在密钥标识表格信息中定位与身份密钥类型和身份密钥值的组合相对应的密钥标识表格条目
402
访问来自密钥标识表格条目的一方标识符值，该一方标识符值对应于与身份密钥相关联的一方
403
基于所访问的一方标识符以及对一方标识表格信息的关系来参考其他表格信息内的条目
404
响应于数据值请求，从其他表格内的条目中检索身份数据
405
响应于接收到的请求，返回身份数据
406

图 4