



(12) 发明专利

(10) 授权公告号 CN 1705946 B

(45) 授权公告日 2014. 06. 11

(21) 申请号 200480001261. X

(22) 申请日 2004. 07. 29

(30) 优先权数据

10/693, 175 2003. 10. 23 US

(85) PCT国际申请进入国家阶段日

2005. 05. 16

(86) PCT国际申请的申请数据

PCT/US2004/024494 2004. 07. 29

(87) PCT国际申请的公布数据

W02005/045705 EN 2005. 05. 19

(73) 专利权人 微软公司

地址 美国华盛顿州

(72) 发明人 K·卡迈龙 D·J·哈谢尔

(74) 专利代理机构 上海专利商标事务所有限公

司 31100

代理人 张政权

(51) Int. Cl.

G06F 17/30 (2006. 01)

(56) 对比文件

US 6317797 B2, 2001. 11. 13, 全文.

US 5640566 A, 1997. 06. 17, 说明书第 1 栏第 50 行到第 2 栏第 25 行, 第 3 栏第 48 到 67 行, 第 4 栏第 8 到 41 行, 第 5 栏第 45 到 67 行, 第 6 栏第 50 到 67 行, 第 7 栏第 1 到 17 行、附图 1, 7 和 8.

US 6463149 B1, 2002. 10. 08, 全文.

US 6539381 B1, 2003. 03. 25, 全文.

US 5884328 A, 1999. 03. 16, 全文.

审查员 林松岭

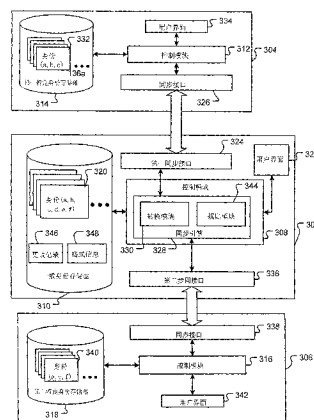
权利要求书3页 说明书12页 附图8页

(54) 发明名称

用于同步身份信息的方法和系统

(57) 摘要

身份系统和方法存储与不同当事者有关的身
份信息并将身份存储在不同或相异系统上, 使得
不同系统可使用身份。同步过程基于主要计算机
系统和相异的次级计算机系统之间的身份信息来
同步身份信息和规则。相应地, 次级计算机系统在
接收经转换信息之后具有身份信息的代表性数据
库, 其中代表性数据库代表存储在主要计算机系
统上的身份信息的主要数据库。为了同步进行了
转换。转换过程可由为次级系统设计的专有过程
来执行。或者, 使用被设计成把身份信息转换成多
种不同格式的映射表格由一般化过程来执行该转
换。



1. 一种在主要计算机系统和不同的次级计算机系统之间同步身份信息的方法,其中所述主要计算机系统和次级计算机系统以不同格式存储身份信息,且其中该方法包括:

连接所述主要计算机系统和次级计算机系统,以提供所述主要计算机系统和次级计算机系统之间的通信能力;

通过将主要计算机系统上的身份信息与次级计算机系统上的身份信息进行比较以确定新身份信息在所述主要计算机系统上存在,并确定应当执行的同步操作;

把所述新身份信息转换成不同格式,所述不同格式与所述次级计算机系统相关联;以及

把所述经转换的新身份信息传送给所述次级计算机系统;

其中,所述次级计算机系统具有基于收到的所述经转换信息的身份信息的代表性数据库,其中所述代表性数据库代表了存储在所述主要计算机系统上的身份信息的主要数据库;

其中所述次级计算机系统上的代表性数据库具有比所述主要数据库少的身份信息。

2. 如权利要求 1 所述的方法,其特征在于,所述方法由操作系统执行。

3. 如权利要求 1 所述的方法,其特征在于,所述次级计算机系统是电话系统,且所述身份信息包括联系人信息。

4. 如权利要求 1 所述的方法,其特征在于,所述次级计算机系统是手持式个人数字助理计算机系统,且所述身份信息包括联系人信息。

5. 如权利要求 1 所述的方法,其特征在于,所述次级计算机系统是电子邮件帐户系统,且所述身份信息包括联系人信息。

6. 如权利要求 1 所述的方法,其特征在于,所述新身份信息由用户输入到所述主要计算机系统。

7. 如权利要求 1 所述的方法,其特征在于,所述新身份信息由另一次级计算机系统输入到所述主要计算机系统。

8. 如权利要求 1 所述的方法,其特征在于,所述转换由为所述次级计算机系统设计的专有过程执行。

9. 如权利要求 1 所述的方法,其特征在于,所述转换由被设计成把身份信息转换成多个不同格式的一般化过程执行。

10. 如权利要求 9 所述的方法,其特征在于,还包括:

接收来自所述次级计算机系统的信息的映射表格,其中所述映射表格把主要格式的身份声明元素映射成次级格式的身份声明元素,其中所述主要格式是主要数据库的格式,而所述次级格式是代表性数据库的格式;以及

使用所述映射表格把身份信息转换成所述次级格式。

11. 一种在次级计算机系统和不同的主要计算机系统之间同步身份信息的方法,其中所述主要计算机系统和次级计算机系统以不同格式存储身份信息,且其中该方法包括:

连接所述主要计算机系统和次级计算机系统,以提供所述主要计算机系统和次级计算机系统之间的通信能力;

通过将主要计算机系统上的身份信息与次级计算机系统上的身份信息进行比较以确定新身份信息在所述次级计算机系统上存在,并确定应当执行的同步操作;

把所述新身份信息传送给所述主要计算机系统；以及

把所述新身份信息转换成不同格式，所述不同格式与所述主要计算机系统相关联；

其中，所述确定步骤包括：所述次级计算机系统具有基于收到的经转换信息的身份信息的代表性数据库，其中所述代表性数据库代表了存储在所述主要计算机系统上的身份信息的主要数据库；

所述次级计算机系统上的所述代表性数据库具有比所述主要数据库少的身份信息。

12. 如权利要求 11 所述的方法，其特征在于，所述方法由操作系统执行。

13. 如权利要求 11 所述的方法，其特征在于，所述转换由被设计成把身份信息转换成多个不同格式的一般化过程执行。

14. 如权利要求 13 所述的方法，其特征在于，还包括：

接收来自所述次级计算机系统的信息的映射表格，其中所述映射表格把主要格式的身份声明元素映射成次级格式的身份声明元素，其中所述主要格式是主要数据库的格式，而所述次级格式是代表性数据库的格式；以及

使用所述映射表格把身份信息从所述次级格式转换成所述主要格式。

15. 一种在主要计算机系统和不同的次级计算机系统之间同步身份信息的网络系统，其中所述主要计算机系统和次级计算机系统以不同格式存储身份信息，且其中该系统包括：

一同步接口，其连接所述主要计算机系统和次级计算机系统，以提供所述主要计算机系统和次级计算机系统之间的通信能力；

一控制模块，通过将主要计算机系统上的身份信息与次级计算机系统上的身份信息进行比较以确定新身份信息在所述主要计算机系统上存在，并确定应当执行的同步操作；

一转换模块，用于把所述新身份信息转换成不同格式，所述不同格式与所述次级计算机系统相关联；以及

一同步模块，其用于把所述经转换的新身份信息传送给次级计算机系统；

其中，所述次级计算机系统具有基于收到的经转换信息的身份信息的代表性数据库，其中所述代表性数据库代表了存储在所述主要计算机系统上的身份信息的主要数据库；

所述次级计算机系统上的所述代表性数据库具有比所述主要数据库少的身份信息。

16. 如权利要求 15 所述的系统，其特征在于，所述次级计算机系统是电话计算机系统。

17. 如权利要求 15 所述的系统，其特征在于，所述次级计算机系统是手持式个人数字助理计算机系统。

18. 如权利要求 15 所述的系统，其特征在于，所述次级计算机系统是电子邮件帐户系统。

19. 如权利要求 15 所述的系统，其特征在于，所述转换模块访问与所述次级计算机系统相关联的映射信息的预定表格以将所述身份信息转换成适当格式。

20. 如权利要求 19 所述的系统，其特征在于，还包括用于与另一次级计算机系统通信的第二同步接口，且其中所述转换模块把身份信息转换成对所述另一次级计算机系统的另外次级格式。

21. 如权利要求 15 所述的系统，其特征在于，所述主要计算机系统具有用户界面模块，且所述新身份信息在所述主要计算机系统上通过所述用户界面模块输入。

22. 如权利要求 15 所述的系统,其特征在于,所述新身份信息源自第三计算机系统。

23. 如权利要求 22 所述的系统,其特征在于,从所述第三计算机系统接收的所述新身份信息被转换成对所述主要计算机系统的格式并存储于主要数据库中,所述新身份信息然后被转换成对所述次级计算机系统的格式,并传送到所述次级计算机系统。

用于同步身份信息的方法和系统

技术领域

[0001] 本发明涉及标识实体,尤其涉及计算环境中当事者的标识。本发明尤其涉及在两个或多个计算机系统之间共享和同步现有身份。

背景技术

[0002] 存在很多具有许多不同专有平台的不同计算机系统。例如,诸如电话和 / 或个人数字助理 (PDA) 的手持式计算机系统已开发了它们自己的与诸如更传统的台式和膝上型计算机系统不同的专用操作系统、特征和能力。此外,诸如服务器的更大系统,通常也具有自己的与台式机、膝上型计算机、电话和 PDA 不同的操作系统平台。然而,这些不同的系统常常需要彼此通信。

[0003] 为了提供这种通信,已编写了计算机程序或应用程序以使信息能从一系统到另一系统都同步。例如,手持式计算机系统提供对台式计算机系统上已经改变或添加的信息的同步的方法。举例来说,已创建了提供台式计算机系统和手持式计算机系统之间通信的地址簿和日程表应用程序,其中对台式系统上诸如联系人的地址簿条目或者日程表条目的改变将在同步操作或过程期间被传送给手持式机器。

[0004] 然而不幸地是,为了提供这种同步,例如特定地址簿或日程表应用程序的应用程序的版本必须在双方计算机系统出现。否则,信息的格式将不可识别并不能被同步。因此,不同专有系统必须创建专用应用程序用于同步信息(如果需要这种同步)的唯一目的。因为许多不同系统都具有其自己的对信息的优选格式,这种结果不能令人满意。作为示例,电话计算机系统可能只需要特定联系人的姓名和电话号码。如果创建、存储并执行新的应用程序以与台式系统通信,然后接收、解析并存储在同步之后所接收的来自台式计算机系统的诸如联系人地址和电子邮件信息的外来信息,这样的系统将会倾覆。当特定用户可能实际上使用例如台式计算机系统、电话和 PDA 的三个或更多不同系统(都具有自己对特定联系人的表示)时,这个问题就更为复杂。

[0005] 参照这些和其它考虑作出了本发明。

发明内容

[0006] 根据本发明,以上和其它问题由在两个或多个计算机系统之间共享信息的系统解决却无需具有两种系统上应用程序版本。该系统使用每个特定系统所要求的格式或表示在两个或多个系统上存储信息。特别地,本发明涉及存储有关不同当事者的身份信息并在不同或相异系统上存储身份使得不同系统可使用这些身份。

[0007] 根据某些方面,本发明涉及在主要计算机系统和不同的次级计算机系统之间同步身份信息的系统和方法,其中主要计算机系统和次级计算机系统以不同格式存储身份信息。本发明的诸实施例首先连接主要计算机系统和次级计算机系统以提供主要计算机系统和次级计算机系统之间的通信能力,然后确定新的身份信息在主要计算机系统上存在并应当执行同步操作。然后,执行将新身份信息转换成不同格式的转换过程,该不同格式与次级

计算机系统相关联。最后,传送或同步过程将经转换信息传送给次级计算机系统。该过程可通过主要计算机系统的操作系统执行。相应地,在接收经转换信息后次级计算机系统具有身份信息的代表性数据库,其中该代表性数据库代表存储在主要计算机系统上身份信息的主要数据库。根据某些方面,次级计算机系统上的代表性数据库具有比主要数据库较少的身份信息。在某些情形中,新身份信息可源自次级计算机系统并被转换、存储在主要计算机系统上。

[0008] 在某些实施例中,次级计算机系统是电话系统而身份信息包括联系人信息。在其它实施例中,次级计算机系统可以是持式个人数字助理计算机系统、电子邮件帐户系统、和许多其它类型计算机系统。此外,可由用户将新身份信息输入到主要计算机系统中或者由另一次级计算机系统将其输入到主要计算机系统中。

[0009] 在某些实施例中,由为次级系统设计的专有过程来执行转换过程。然而,在其它实施例中,则由设计用以把身份信息转换成多种不同格式的一般化过程来执行转换。在此情形中,主要计算机系统接收来自次级计算机系统的信息的映射表格,其中映射表格将主要格式的身份声明元素(其中主要格式是主要数据库的格式)映射成次级格式的身份声明元素(其中次级格式是次级数据库的格式);且该表格由一般化过程使用以将身份信息转换成次级格式。

[0010] 根据其它方面,本发明涉及在主要计算机系统和不同次级计算机系统之间同步规则信息的系统和方法,其中主要计算机系统和次级计算机系统以不同格式存储身份信息,且其中主要计算机系统和次级计算机系统具有身份信息的代表性数据库并包括该方法。在此情形中,本发明涉及连接主要计算机系统和次级计算机系统以提供主要计算机系统和次级计算机系统之间的通信能力;确定新的规则信息存在并应当执行同步操作;以及将经转换信息从一计算机系统传送给其它计算机系统。此外,本发明还可把新的规则信息转换成不同格式,该不同格式与次级计算机系统相关联。

[0011] 本发明可实现为计算机进程、计算系统、或诸如计算机程序产品的制品。计算机程序产品可以是计算机系统可读的计算机存储介质,并编码用于执行计算机进程的指令的计算机程序。计算机程序产品还可以是计算系统可读的载体上的传播信号,并编码用于执行计算机过程的指令的计算机程序。

[0012] 参阅附图(简单归纳如下)、本发明较佳实施例的以下详述、以及所附权利要求书可获得对本发明及其改进方案的更全面理解。

附图说明

[0013] 图1示出根据本发明实施例的示例性系统。

[0014] 图2示出根据本发明特定方面可使用的计算机系统。

[0015] 图3示出根据本发明诸方面用于同步身份信息文档的软件环境表示。

[0016] 图4根据本发明特定方面示出身份信息文档的结构。

[0017] 图5是示出根据本发明特定实施例用于存储身份信息文档的一般化方式的框图。

[0018] 图6是示出根据本发明一实施例用于同步身份信息文档的过程的操作特征的流程图。

[0019] 图7是示出用于把身份信息文档更新从一次级计算机系统传送到另一次级计算

机系统的过程的操作特征的流程图。

[0020] 图 8 是示出用于把规则从一系统传送到另一系统的过程的操作特征的流程图。

具体实施方式

[0021] 此后本发明将参照附图进行更全面的描述,其中在附图中示出了本发明的诸实施例。然而,本发明可以许多不同形式来体现并不应被解释为受限于在此陈述的诸实施例;相反,提供这些实施例使得本说明书更为全面和完整,并将把本发明的范围传达给本领域技术人员。

[0022] 一般而言,本发明涉及同步信息,尤其是同步跨越多个不同计算机系统的特定身份信息 and 身份相关规则。根据本发明诸实施例,在此所述的方法可在独立的单机计算机系统中实现,但更经常地是在互相连接形成分布式计算机网络的多个计算机系统中实现。本发明所设想的用于执行同步的环境 100 在图 1 示出。环境 100 具有被视为主要计算机系统的计算机系统 102。在此使用时,“计算机系统”应当进行更广泛的解释并定义为“执行用于显示和操纵文本、图像、标记、音频、视频和 / 或数字的程序的一个或多个装置或机器”。

[0023] 主要计算机系统 102 与诸如蜂窝式电话计算机系统 104 和个人数字助理 (PDA) 计算机系统 106 的次级计算机系统通信。如果需要,主要计算机系统 102 还可与许多诸如系统 108、110 和 112 的许多其它计算机系统通信以便同步信息。尽管系统 102 可与许多诸如系统 108、110 和 112 的其它系统通信,本讨论集中在系统 102 和系统 104 和 106 之间的示例性通信。这样,仅显示如图 1 所示的系统 108、110 和 112 以表明本发明所设想的许多其它连接和通信。

[0024] 系统 102、104、106、108、110 和 112 使用无线或者直接连线链接的一个或多个众所周知的通信协议进行通信。此外,系统 102、104、106、108、110 和 112 可通过在诸如因特网 (未示出) 的网络上实现的诸如 TCP/IP 的分别协议或其它网络和 / 或通信协议进行通信。即,尽管被示为由看起来直接的箭头连接,分别系统 104、106、108、110 和 112 实际上可通过其它间接方法与系统 102 通信。事实上,在 100 中所示的连接仅表示信息可在诸系统中传递。这样,在此使用的通信的定义涉及消息、事件、或者其它信息从一系统到另一系统的传输。

[0025] 在本发明一实施例中,在发送之前,系统 102 把经同步的信息转换和 / 或过滤成诸如系统 104 和 106 的次级系统所要求的形式。因为其它计算机系统要求信息以不同格式存储,系统被视为是不同的。作为转换的结果,次级系统不需要本地地存储并执行外来应用程序。此外,本发明涉及不同计算机系统之间信息的同步,其中不同计算机系统由同一用户或同一机构所拥有和操作,从而最近的、一致的、具有意义的身份信息集合展现在分别的计算机系统中。

[0026] 根据本发明的诸方面,主要计算机系统 102 把身份信息存储在主要身份数据库 114 中。一般而言,“身份信息”包括多个分别的、独立的身份资源或文档,其中身份资源与已知当事者相关联。如在此定义,当事者是任何在计算机环境中执行某些动作的个人、个人的组合或计算机模块。示例性当事者包括操作系统、在操作系统上实现的计算机应用程序和进程、个人、以及人们的组合 (例如家庭、公司、机构等等)。

[0027] 在一实施例中,对于每个已知当事者创建一身份资源。资源在此定义为以组成电

子文档的方式安排的机器可读形式数据。因此,身份资源是当事者的电子表示或“身份”。在此这种身份资源也被称为“身份信息文档”、“当事者对象”以及“身份信息对象”。身份资源唯一地标识其对应的当事者。作为示例,系统 102 可包括与系统 102 用户已知的人们相关的许多身份资源。每个身份资源可包括其它标识元素或身份声明中这样的信息:人名、电话号码、电子邮件地址。实际上,可有许多其它身份声明,诸如个人的公钥、计算机系统的 IP 地址、组的关系、使用政策等等。对于更多的身份声明和身份资源,参见授予本专利申请受让人并与 2003 年 10 月 23 日提交的美国专利申请“Identity System for Use in a Computing Environment”(“用于在计算环境中使用的身份系统”)(律师案号为 MS306220.01/M&G40062.214-US-01),其说明书在此引入作为参考。

[0028] 系统 102 还具有控制模块 116,它用以执行创建身份资源、存储身份资源以及与存储在主要身份数据库 114 中的身份资源相关的其它管理功能。此外,使用控制模块 116 来管理系统 102 和诸如系统 104 和 106 的其它系统之间的通信。因此控制模块管理身份资源向其它系统 104 和 106 的传送,以及这些身份资源的同步。

[0029] 为了传送信息系统 104,系统 104 还具有控制模块 118。控制模块 118 进行操作以便于与系统 102 上控制模块 116 的通信。系统 104 维持存储多个身份资源的本地身份数据库 120。在一实施例中,本地身份数据库 120 对位于主要身份数据库 114 的每个身份资源具有一身份资源。即在系统 102 和 104 之间的同步之后,位于数据库 114 和 / 或 116 但不位于其它数据库上的任何身份资源,可复制或传送到其它数据库以更新该其它数据库。因此,借助数据库 114 中身份资源所代表的当事者,本地数据库 120 可视为数据库 114 的副本。

[0030] 尽管在同步之后数据库 120 对数据库 114 中每个身份资源存储了一身份资源,数据库 120 中的真实身份资源可与数据库 114 中相应的身份资源存储信息不同。存储在数据库 120 中信息的类型和数量可与数据库 114 中储存的不同。例如,由于系统 104 是蜂窝电话,存储其上的数据库 120 仅可存储数据库 114 的精简版本。在一实施例中,对于存储在数据库 114 上的每个身份资源,数据库 120 可仅存储姓名和电话号码。相应地,数据库 120 可不包括存储在数据库 114 上具有更多综合性身份资源的任意或所有给定当事者可用的所有信息。因为次级系统上的数据库 120 具有主要数据库 114 上每个当事者的条目,尽管是以不同格式并且可能具有较少(或者不同)信息,数据库 120 仍然可视为主要数据库 114 的“代表”数据库。

[0031] PDA 计算机系统 106 还具有控制模块 122 和数据库 124,分别用于与系统 102 上的控制模块 116 通信,以及用于存储身份信息。可以理解,本地数据库 124 对主要数据库 114 上每个身份资源存储一身份资源,但不会存储每个身份资源的所有信息。即,像系统 104 一样,系统 106 通常具有比系统 102 较少的计算资源,诸如存储器、计算能力、通信能力等等。因为这些限制,PDA 系统 106 仅需要在本地存储每个身份资源的精简版。然而,取决于不同系统 104 和 106 的需要和能力,存储在系统 124 上的每个身份资源的版本可比存储在数据库 120 中系统 104 上的更大或更小。

[0032] 不仅存储在本地数据库 120 和 124 上的身份资源在存储信息量、用于存储系统 104 信息的格式上不同,而且在数据库 120 中与用于存储在数据库 114 上相同信息的格式也不同。一般而言,系统 102 上控制模块 116 把数据库 114 上的数据转换成系统 104 所需的格式。因此,控制模块 118 在数据库 120 上存储数据之前不需执行这种转换。

[0033] 图2示出了本发明诸实施例可在其上实现的适当计算系统200的示例。这样,该系统200是可用来发挥分布式计算环境100中计算机系统102、104和/或106作用的代表。在其最基本的配置中,系统200包括至少一个处理单元202和存储器204。取决于计算装置的准确配置和类型,系统存储器204可以是易失性的(诸如RAM)、非易失性的(诸如ROM、闪存等等)、或两者的某些组合。该最基本配置在图2中由虚线206示出。

[0034] 除了存储器204,系统200可包括至少一种其它形式的计算机可读介质。也称为“计算机程序产品”的计算机可读介质是可由系统200访问的任何可用介质。作为示例,而非限制,计算机可读介质可包括计算机存储介质和通信介质。

[0035] 计算机存储介质可包括以任何方法或技术实现的易失性和非易失性、可移动和不可移动的介质用来存储诸如计算机可读指令、数据结构、程序模块、或其它数据的信息。系统存储器204、可移动存储208和不可移动存储210都是计算机存储介质的示例。计算机存储介质包括,但不限于RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字化多功能光盘(DVD)或其它光学存储器、磁带盒、磁带、磁盘存储器或其它磁性存储装置、或可用来存储所需信息并可由系统200访问的任何其它介质。任何这种计算机存储介质可以是系统200的一部分。

[0036] 示例性计算系统200还可包含使装置能与其它计算装置通信的通信连接212。通信连接212是通信介质的一个示例。通信介质通常包括计算机可读指令、数据结构、程序模块、或其它数据在诸如载波或其它传输机制的已调制数据的信号中,并包括任何信息传输介质。术语“已调制数据信号”意指具有以这种在信号中编码信息的方式来设置或改变的一个或多个特征的信号。作为示例,而非限制,通信介质包括诸如有线网络或直接有线连接的有线介质,以及诸如声学、RF、红外和其它无线介质的无线介质。在此使用的术语计算机可读介质包括存储介质和通信介质。

[0037] 根据一实施例,系统200包括诸如输入设备214和/或输出设备216的外围设备。示例性输入设备214包括,但不限于键盘、计算机鼠标、输入笔、语音输入装置、触摸输入装置等等。示例性输出设备216包括,但不限于显示器、扬声器、打印机等等。这些“外围设备”的每一个在本领域内众所周知,无需在此赘述。

[0038] 有了计算环境,本发明的诸实施例就可参照逻辑操作进行描述,这些逻辑操作在执行时实现体现本发明各个实施例的过程。这些逻辑操作被实现为:(1)在计算系统上运行的计算机实现步骤或程序模块序列和/或(2)计算系统中相互连接的机器逻辑电路或电路模块。实现是根据实现本发明的计算系统的性能要求,进行模块选择。相应地,在此描述的组成本发明诸实施例的逻辑操作指的是操作、结构性装置、动作或者模块。本领域技术人员可以理解,如所附权利要求书所述,这些操作、结构性装置、动作和模块可用软件、固件、专用数字逻辑以及任意组合来实现,而不背离本发明的精神和范围。

[0039] 现在参看图3,根据本发明一实施例逻辑上示出用于同步主要计算机系统302和其它计算机系统304和306之间身份信息的功能组件。一般而言,系统302是系统102(图1)的功能表示。系统304和306也是系统104和106的功能代表。因此,可以理解,控制模块308和身份存储器310与控制模块116和数据库114(图1)相对应。类似地,控制模块312和316分别与控制模块118和122相对应。而且,数据存储314和318分别与数据库120和124相对应。在一实施例中,系统302的功能组件驻留于操作系统中,并作为平台

的一部分提供存储身份信息和其它计算机系统身份信息的系统。

[0040] 如上所述,系统 302 代表主要计算机系统。主要计算机系统 302 具有存储多个身份 320 的一般身份存储器 310。多个身份 320 的每一个都与特定当事者相关,并在数据存储器 310 中作为身份信息文档或身份资源被存储。此外,存储在一般身份存储器 310 中的每个身份信息文档可具有若干信息元素或声明,在图 3 中用加在括号中的字母“a, b, c, d, e, f”表示。这些信息元素与标识特定当事者或标识身份信息文档本身的特定信息相关,诸如姓名、地址、电话号码,这在下面结合图 4 进行更详细的讨论。

[0041] 系统 302 还包括进行操作以管理一般身份存储器 310 的控制模块 308。该控制模块可接收来自用户界面模块 322 的信息。即,系统 302 的用户可输入新的身份信息文档、或对现有的信息文档作更改、甚或通过用户界面模块 322 删除现有的身份信息文档。在收到这种更改请求之后,控制模块 308 执行必要的操作以完成该请求。类似地,尽管未示出,这种更改请求(添加、编辑和/或删除)可来自其它模块(未示出),从而控制模块可由于来自许多不同模块的请求而对数据库实行各种更改。作为示例,用户可接收带有新身份信息文档的电子邮件。在此情形中,在一实施例中控制模块可不经用户交互自动把新的身份信息文档添加到数据库 310 中。然而其它实施例可要求用户手动地请求这种添加,以使控制要添加到数据库 310 的是哪些身份信息文档。作为另一示例,用户可接收带有经更新信息文档的电子邮件,并因而控制模块 308 可自动更新被存储的身份信息文档。这种更新可以要求或可以不要求用户交互。但在又一示例中控制模块可无需用户交互而自动更改数据库 310 的内容,该示例涉及所接收的来自其它系统 304 和/或 306 的更新、添加或者删除请求,如下详述。

[0042] 控制模块 308 还可与第一同步接口模块 324 通信。而该第一同步接口模块 324 又与系统 304 上的同步接口模块 326 通信。控制模块使用同步引擎 328 来执行同步步骤。一般而言,同步引擎 328 比较存储在一般身份存储器上和存储在第一特定身份存储器 314 上的身份信息文档的属性,并确定两者之间的差异。例如,同步引擎标识哪些未在一存储器上出现却在另一存储器上出现。另外,同步引擎还确定自上个同步过程起哪些作了更改而哪些已经删除。在确定差异之后,同步引擎通过同步模块 324 和 326 向系统 304 和最终向数据库 314 传送这些更改。在一实施例中,可使用更改记录 326 来快速标识在上次同步之后的更改。

[0043] 同步引擎 328 还具有转换模块 330,它用以在发送信息之前把诸如一般身份存储器 310 的一种格式的信息转换成诸如存储器 314 所要求的另一形式。在把信息发送给系统 304 之前,转换模块 330 还可过滤或剥离预定信息。转换模块 330 和因此同步引擎 328 理解,不要发送基于最终不存储在新系统 304 上的信息的更新。例如,如果特定标识信息文档中的地址字段已更改但地址字段未存储在 304 上,则对于该地址更改无需对 304 作更新。

[0044] 因而,同步引擎 328 不仅理解最终存储在 304 上的文档格式,而且理解要存储在 304 上的信息类型,使得同步引擎仅作相关更新。为了理解要存储的信息格式和类型,在一实施例中同步引擎 328 依赖于存储的格式信息资源 348,它支配存储在存储器 314 上条目的格式以及要同步条目的可用参数或字段。通常在系统 302 和 304 都向其它允许将来同步过程的系统提供相关信息的初始化阶段中,这种格式信息资源 348 被提供给同步引擎 328。格式信息资源 348 可存储在作为如图 3 所示一般身份存储器 310 一部分的文件中或者其它

位置上。在其它实施例中,每当同步过程开始时提供格式信息。在另外的其它实施例中,同步引擎发送所有更新,但接收装置 304 仅接受适当的更改。

[0045] 在一特定实施例中,格式信息资源是信息的表格。信息表格把诸如系统 304 的次级系统的身份资源格式的元素映射成诸如系统 302 的主要系统的身份资源格式的类似元素。例如,系统 304 可对应于将“工作电话”表示为对象的一属性,“家庭电话”为另一属性,以及“电子邮件地址”为第三属性的电子邮件服务器。在此情形中,表格标识这些属性对象并将其等同于或映射成身份资源的类似身份声明。因而,转换模块可仅在表格中查找属性指示以理解如何将身份资源转换成适当格式。

[0046] 使用该方法,其它转换被简化了,因为需要向系统 302 提供的仅是适当的信息表格。例如,继续上例,另一装置可不同地分析对象,(基本上)每个身份资源具有五个称为地址 1 到地址 5 的属性,其中每一个都具有类别(“家庭”、“工作”、“手机”、“电子邮件”等等)和值。其它系统还可使用类似的经分类电话号码集合,但将电子邮件地址置于单独集合中。在这些情形中,转换模块 330 能够将对象 320 上的属性映射成对象 332 和 340 上的不同属性,反之亦然,因为表格向转换模块 330 提供了映射方向。当然,如果该映射是一对一的(例如“名字”变成“教名”),该过程是直截了当的且表格可能就不必要了。然而,给定这些不同的系统(每个都有它们自己的组合和拆分值和属性的方法),上述的表格方法仅通过给予新表格就可得到可处理任何变换的一段代码,使得不必对每个外来系统编写定制代码。

[0047] 操作上,在确定应执行同步操作之后,同步模块 328 从一般身份存储器 310 检索信息。如果必要,转换模块 330 使用与系统 304 相对应的格式资源 348 把信息转换成所需格式。在转换信息之后,同步模块 328 将经更新信息传递给第一同步接口 324,而 324 又将信息传递给系统 304 上的同步接口 326。在收到经更新信息之后,控制模块 312 把新信息存储在特定身份存储器 314 中。如图所示,存储器 314 中新的经更新身份 332 具有比存储器 310 中身份 320 的所有信息要少的信息。这是因为在该示例中,系统 304 不需要元素 d, e 和 f 从而不向系统 304 传送这些元素。在把经更新身份存储到存储器 314 中之后,可使用用户界面模块 334 来向相同用户显示系统 304 上的身份。

[0048] 类似地,在确定应执行同步操作之后,同步模块 328 操作以同步系统 306 上的信息。实际上,同步模块 328 从一般身份存储器 310 检索信息,并且如果需要,转换模块 330 使用与系统 306 相对应的格式资源 348 把信息转换成所需要的格式。在转换信息之后,同步模块 328 把经更新信息传递给第二同步接口 336,而该同步接口 336 把信息传递给系统 306 上的同步接口 338。在接收到经更新信息之后,控制模块 316 把新信息存储在第二特定身份存储器 318 中。如图所示,存储器 318 中的新更新身份 340 可具有比存储器 310 中身份 320 的所有信息少的信息。在此例中,这是因为系统 306 不需要元素 b, c 和 d,从而这些元素不向系统 306 传送。而且应注意这些格式和元素能够且通常与诸如系统 304 和 306 的各别的第二系统不同。在把经更新身份存储在存储器 318 之后,可使用用户接口模块 342 以向其用户显示系统 306 上的身份。

[0049] 在本发明一实施例中,可分别使用用户接口模块 334 和 342 来添加、编辑和删除诸如文档 332 和 340 的身份文档的本地副本。然后,可将这些更改传送给主要系统 302。实际上,在同步之后,对身份文档的更改可传到回主要系统 302 以更新一般身份存储器 301。例

如,系统 304 的用户可更改身份文档 332 上的电话号码字段。在作了更改之后,可更新系统 304 上的本地更改记录(未示出)。然后,在同步之后,控制模块 312 可通过同步接口 336 和第一同步接口 324 把带有新电话号码的新更新身份传递给控制模块 308,并最终传递给同步引擎 328。同步引擎 328 确定是否必须作把更改转换成一般化形式的任一转换,如果是,则使用转换模块 330 来执行这种转换。在转换信息之后,把身份信息存储在一般身份存储器 310 中。此时,可修改更改记录以提醒同步引擎 328 更新在诸如系统 306 的所有其它次级系统中都是必需的。因此,假设系统 306 对诸如电话号码的更改感兴趣,则在后来对系统 306 的同步操作中,将把源自系统 304 的更新传送到系统 306。

[0050] 在特定实施例中,同步引擎 328 还包括规则模块 344。规则模块 344 存储有关某些身份或所有身份的规则信息。这些规则还与向次级系统 304 和 306 的用户通知的事件相关。在诸如通过用户接口 322 输入或更改规则之后,规则随后在同步操作期间被传送给诸如系统 304 和 306 的各种次级系统。在收到规则之后,如果必要次级系统 304 和 306 应用这些规则。

[0051] 例如,系统 302 的用户可能不想在的工作时间接来自朋友的电话,并通过用户界面 322 把该规则输入到系统 302 中。假设一个或多个身份 320 具有把当事者标识为朋友的相关联标记或字段,则在例如星期一到星期五上午 8:00 ~ 下午 5:00 的工作时间不应允许来自这些当事者的电话。可将该规则传送给系统 304(例如手机)。由于系统 304 具有存储在其数据库上的身份信息,通过把来电的电话号码与已存储身份的电话号码相匹配可实施该规则,并确定是否允许接该电话。在此例中,系统 304 及其控制模块 312 具备这些能力:确定来电、电话号码,将它们与已存储身份相匹配,并根据传送规则封锁不想接的电话。

[0052] 规则可特别列举某些身份,而其它则会更一般并可应用到所有身份。一般而言,从用户界面 322 输入和编辑规则,但其它实施例可使规则更改在诸如系统 304 和 306 的次级系统上输入。在同步之后,如果需要可在系统 302 上更新来自次级系统 304 和 / 或 306 的更改,并将之传送给其它系统。此外,因为规则在不同计算机系统上是不同的,例如用于接受电话的规则适于电话计算机系统但不适于电子邮件计算机系统,转换模块 330 还可在传送规则之前把规则转换成对当前正被同步的次级计算机系统合适的格式。为了完成该转换,一组预定的规则转换数据(未示出)被存储在系统 302 上以备使用。该预定规则转换数据标识适当的规则及其格式,从而转换模块能够把系统 302 上的给定规则翻译成次级系统上的适当规则。

[0053] 在图 4 示出可表示存储在一般身份存储器 310(图 3)中的身份信息文档的身份信息文档 400 的示例性格式。作为一数据结构,身份信息文档 400 是可绑定于公钥并由嵌入式使用政策进行管理的身份声明和其它属性 / 特性声明的集合。可把 XML 用作身份信息的编码语言。然而,其它格式也被视为一样适用。如果身份信息文档 400 的元素包含必须保密的信息,则还可任选地对其进行加密。

[0054] 可将身份信息文档 400 中的数据分为两个类别,包括逻辑组件组 402 和属性标记组 404。身份信息文档 400 有六个主要的逻辑组件:1) 当事者标识符 406;2) 当事者的一个或多个身份声明 408;3) 当事者的显示名及零个或多个可选择性揭示的属性 410;4) 以任何可接受形式(例如 X509v3 证书中的公钥)封装的当事者的一个或多个密钥 412;5) 表示当事者私密需求的使用政策 414;以及 6) 在身份信息更新的情形中保护数据完整性并认证

发送者的对整个身份信息内容的数字签名 416。这六个逻辑组件 402 的每一个在后面依次进行讨论。

[0055] 当事者标识符是标识在身份信息文档 400 中所包含身份声明的当事者的用户友好句柄 (handle)。如果当事者为人, 优选当事者标识符 406 是当事者的电子邮件地址。然而, 应当把当事者标识符广泛地解释为唯一标识当事者的任何类型的用户友好句柄, 并可包括但不限于, 电子邮件地址、电话号码、手机号码等等。

[0056] 身份声明 408 包括与作为身份信息文档的主题的当事者相关的其它结构化信息。身份声明应当被广泛地解释为有关当事者的描述性信息, 可包括但不限于, 通信地址、电话及传真号码、雇员信息、生日等等。“身份声明”尤其是唯一真正有关一实体 (人、机构等等) 的。因而, 在某些实例中, 电话号码可以是一个人的有效身份声明。例如, 手机号码、直拨工作电话、或家庭电话可以是对不共享手机、直拨工作电话号码或者独自居住的人的有效身份声明。在其它实例中, 电话可能不是一个单个人的有效身份声明, 诸如家人共享的家庭电话号码。在这种情形中, 家庭电话号码可以是代表家庭而不是个人的身份声明。

[0057] 机器位置 410 提供了当事者计算机系统的唯一地址, 且可包括但非限制 IP 地址或公钥。类似于具体街道地址, 机器位置必须定位、连接、或通信分布式网络内的计算机系统。

[0058] 密钥部分 412 包含一个或多个可能封装于证书格式 (例如 X509v3 证书) 中的密钥。密钥 605 可以是公钥并可包括在身份信息中作为身份信息主题的识别信息。如果使用了证书, 它可以是由证书机构自己签名或签发的。

[0059] 使用政策 414 传送有关对身份信息文档 400 的内容可允许使用的当事者指令。例如, 使用政策 414 可指示不应向其它方泄露身份信息的内容。诸如图 1 中数据库 114 的接收者的经识别身份信息数据库, 将存储用户政策以及定义当事者的其余信息。

[0060] 数字签名 416 向当事者提供签名身份信息文档中数据的能力。XML 签名有三种有关文档签名的方法: 封装、被封装、以及被剥离。根据本发明一实施例, 当签名身份信息内容时, 身份信息文档使用 XML 被封装的签名。

[0061] 身份信息文档 400 可携带与身份信息文档 400 本身相关的六个或多个属性标记 404。尽管未示出, 属性标记可包括身份信息文档 400 的 ID 值、文档 400 的版本信息和 / 或文档 400 代表的当事者类型, 例如人、计算机或机构。也可采用其它属性标记。

[0062] 在一实施例中, 身份信息文档以一般化方式被存储在主要计算机系统中, 诸如分别结合图 1 和 3 如上所述的系统 102 和 103。信息文档可用其存储的一般化方式的说明如图 5 所示。

[0063] 如图 5 所示, 可称为 “iCard” 的身份信息文档 500 可用 SAML 或者 XML (或其它诸如 XXML 的格式) 来创建或存储。如图 5 所示的样本 iCard 500 具有一些值得注意的特征。例如, 电子邮件标识符 502 与当事者的电子邮件地址相关。此外, 身份信息文档 500 具有显示名称属性 504。为了安全, 文档 500 还具有当事者的证书 506 (在此略去) 及其数字签名 508 (在此略去)。

[0064] SAML 是一种用于安全地表示包括认证的安全断言和其它断言的 XML 标准, 并较好地集成了其它诸如 “XPath” 和 “XMLDSIG” 的 XML 技术。顶层 SAML 元素是 Assertion (断言), 它包含 Subject (主题) 和一系列 Statement (语句), 其中 Statement 是断言 Subject 为特定认证属性或属性值的结构。Assertion 可能要遵从一个或多个条件。SAML 是当前本

行业所采用的优选安全断言描述语言。

[0065] Assertion 的各个组件和 / 或全部都可以加密, 并且整个 Assertion 由 Issuer 签发。SAML 格式被设计为是可扩展的, 即在此讨论的每个元素都可使用 XML 替代组来替换和 / 或使用本领域技术人员所众所周知的“任何”XML 元素来扩展。

[0066] 在此讨论的模式片断指定用于编码 iCard 各个元素的 XML 模式。在这些模式定义中使用和引用的各种 XML 名空间如表格 1 所示:

名空间	URI
xmlns:xsd	http://www.w3.org/2001/XMLSchema
xmlns:ds	http://www.w3.org/2000/09/xmldsig#
xmlns:xenc	http://www.w3.org/2001/04/xmenc#
xmlns:saml	Urn:oasis:names:tc:SAML:1.0:assertion
xmlns:ms	http://www.microsoft.com/security/2003/IS/iCard

[0067] 表格 1:XML 名空间

[0068] 另外的实施例并不以一般化方式把身份信息存储在主要数据库 310 中。在这些其它实施例中, 可执行其它转换操作以确保在把每个身份信息文档发送给另一系统之前, 文档具有适当格式。类似地, 可要求其它的转换, 即在诸如分别结合图 1 和图 3 如上所述的系统 102 和 302 的主要系统上的主要数据库中进行存储之前, 把收到的身份信息文档转换成所需格式。

[0069] 图 6 是根据本发明实施例示出用于同步身份信息文档的过程的操作特征的流程图。一般而言, 图 6 涉及一般同步系统及该系统中所涉步骤。开始, 连接操作 602 连接两个不同系统。在一实施例中, 两个不同系统与例如上述系统 302 的主要计算机系统以及例如上述系统 304 的次级计算机系统相关。真正的连接涉及提供两系统之间通信链接 (无线或物理链接) 的已知方法。在链接之后, 发生通信操作, 其中分别的系统传递有关每个系统的类型和该链接的目的的信息。用户交互可涉及或不涉及初始链接操作 602。链接操作 602 的完成涉及可执行有关或多个同步操作的两个不同系统之间的理解。

[0070] 在链接操作 602 之后, 可选传送类型信息操作 604 传送次级计算机系统所使用的有关格式和字段参数的信息。因为这种信息在以前链接期间已被传送到主要计算机系统, 传送操作 602 是可选的。

[0071] 在识别同步将要发生之后, 并且一旦适当的格式和字段参数可用, 转换操作 606 将拟传送的数据转换成适当格式。转换操作 606 主要从诸如数据库 310 (图 3) 的数据库检索新的或经更新的数据, 并将其从一般化格式转换成次级系统所需的特定格式。然后, 过滤操作 608 滤去不必要的信息。过滤操作 608 防止将不必要的更新信息传递给不想存储该信息的次级系统。例如, 如果次级系统是电话且它不需要地址信息、电子邮件信息、数字签名等等, 则过滤操作 608 从经转换文档中移除这些信息。在另外实施例中, 过滤操作在转换操作之前发生。

[0072] 在过滤数据之后, 传送操作 610 以适当格式把身份信息从第一计算机系统传送到第二计算机系统。在该传送之后, 流程 600 在结束操作 612 结束。尽管未示出, 也可在收到经更新信息之后执行把经更新的身份信息存储在次级系统上的另一操作。

[0073] 可以理解, 流程 600 涉及单个身份信息文档的传送。在本发明的诸实施例中, 对主要系统上所有经更新身份信息文档重复流程 600。另外, 当为了同步把新的次级系统连接到主要系统时, 所有的身份文档被复制、转换、过滤并传送到次级系统用于存储。

[0074] 图 7 是示出把身份信息文档更新从一次级计算机系统传送到另一次级计算机系统的过程的操作特征的流程图。流程 700 开始时在诸如结合图 3 如上所述的系统 304 的次级计算机系统上输入对身份信息文档的更改时。在一实施例中, “更改” 涉及添加身份信息文档、删除身份信息文档或者更改现有身份信息文档。另外的实施例包括对诸如保密信息或认证信息的其它条目的更改。而且, 在一实施例中, 次级计算机系统的用户通过诸如模块 334 (图 3) 的用户界面模块输入该更改, 且该更改被存储在诸如数据库 332 的本地数据库中。此外, 在作更改之后, 可更新更改记录 (未示出) 以表明在下一同步操作期间应同步的一个或多个更改。

[0075] 然后, 传送操作 704 把改变信息发送给诸如系统 302 (图 3) 的主要计算机系统。通常, 可在传送操作 704 之前执行诸如操作 602 的连接操作, 即在把信息从一系统传送到另一系统之前, 该两个系统必须可进行通信连接。还有, 在发送信息之前, 实施例发送诸如参照操作 604 上述的类型信息使接收主要计算机系统理解所接收更改的格式。在一实施例中, 收到的更改涉及接收整个身份信息文档, 而在其它实施例中, 仅向主要计算机系统提供更改。当然, 为了使主要计算机系统理解更新或更改, 某些描述要更新身份信息文档的标识信息必须与更改信息一起传送。

[0076] 在收到更改信息之后, 转换操作 706 把收到的信息转换成一般化信息, 并存储或更新诸如数据库 310 (图 3) 的一般身份数据库。然而, 如果更新涉及删除操作, 则操作 706 仅删除数据存储中适当的身份信息文档。还有, 如果该更新涉及现有身份信息文档的更改, 则操作 706 可不需转换而仅编辑位于数据库中的现有身份信息文档。在更改数据库时, 可更新诸如更改记录 346 的更改记录以表明在与其它次级计算机系统的下一同步操作期间应当同步的一个或多个更改。

[0077] 最后, 传送操作 710 把源自一次级系统的更改 (操作 702 和 704) 发送到诸如系统 306 (图 3) 的其它次级系统。该更改的传送以参照图 6 中流程 600 如上所述的方式进行。即, 其它次级计算机系统连接到主要计算机系统, 并在连接之后, 主要计算机系统确定该同步应发生, 把经更新信息之后成对相连次级计算机系统适当的格式, 如果需要过滤这种信息, 并将该新信息传送给其它次级计算机系统。

[0078] 在把新数据传送给另一次级计算机系统之后, 流程 700 在结束操作 712 上结束。当然, 在与又一次级计算机系统相连之后, 以上的更改被传送到下一次级计算机系统中。使用流程 700 中所述方法, 可将在次级计算机系统上所作对身份信息数据库的更改传送给与特定用户相关联的任意或所有次级计算机系统。例如, 如果用户具有 PDA、台式计算机系统和手机, 可使用以上方法来接收 PDA 上当事者身份信息的更改, 然后它将与台式计算机系统同步以更新台式计算机系统上的数据存储。然后, 在电话和台式计算机系统之间的同步事件期间, 开始在 PDA 上所作更改将从台式计算机系统上传送到手机, 并存储在手机上。

[0079] 图 8 是示出用于从一系统向另一系统传递规则的过程的操作特征的流程图。流程 800 是基于以上系统的,其中两个或多个计算机系统具有与两个或多个系统的用户相关联的各个身份的概念。例如,如果主要计算机系统的用户已经在其台式计算机系统中建立了已知和受信任身份的数据库,则使用以上系统和方法,用户还可在诸如手机或 PDA 的次级计算机系统上具有相同或代表性的数据库(虽然是精简的)。相应地,用户可能希望可建立有关这些身份的某些规则。更重要的是,用户可在诸如桌面计算机系统的一计算机系统上输入这些规则。实际上,流程 800 从输入操作 802 开始,其中规则被输入诸如系统 302(图 3)的系统。在其它实施例中,可把规则输入诸如系统 304 和 306 的次级计算机系统之一中。

[0080] 在输入规则之后的某些时候,翻译操作 803 可把规则翻译成与次级计算机系统一致的格式。通常,翻译过程在确定同步规则信息之后,且在向次级计算机系统发送规则信息之前发生。然而,翻译可在输入规则到主要计算系统后和向次级计算机系统发送规则信息前之间的任何时间完成。翻译过程 803 关系到把给定规则翻译成适当格式,或者换言之,翻译成次级计算机系统能够实施的规则。由于不同次级计算机系统执行不同功能,对于不同的系统规则也可以不同。例如,一系统可响应于一规则封锁电话,而另一系统则可封锁电子邮件。

[0081] 在翻译规则之后,传送操作 804 将该规则传送到一个或多个次级计算机系统。在一实施例中,传送操作 804 在两个系统之间的同步阶段进行。接收新的经更新规则的一个或多个次级计算机系统能够实施这些规则。

[0082] 因为系统 302 用一组身份声明表示当事者,指向当事者的规则可从一系统转换成另一系统。可将系统 302 上“don't let Joe Smith bother me”(“不要让 Joe Smith 打扰我”)的规则翻译成电话服务器上“don't accept calls from 555-1212”(“不要接受来自 555-1212 的电话”),和邮件服务器上的“don't accept mail fromjoe@isp.com”(“不要接受来自 joe@isp.com 的邮件”)。假设不同的次级系统具有理解谁是当事者(例如 Joe Smith)的代表性数据库,用户不需要在每个系统上重新输入类似规则。

[0083] 即使当不同计算机系统以不同格式存储了部分身份和/或存储了信息时,上述系统和方法提供了能跨越许多不同计算机系统共享一组身份的能力。这样,次级系统无需为了发送、接收和存储这种身份信息文档而存储和执行复杂的计算机应用程序。此外,上述系统涉及将此功能包括在主要计算机系统的操作系统中的和/或在程序平台上。

[0084] 尽管已经以结构特征、方法论动作和包含这些动作的计算机可读介质的专用语言对本发明进行了描述,可以理解在所附权利要求书中定义的本发明无须受限于所述特定结构、动作或介质。作为实例,可根据本发明的原理来创建和同步许多不同的身份信息文档,包括说明性信息、保密信息和认证信息。而且,根据本发明诸方面,可将许多不同计算机系统用作次级计算机系统,诸如 web 门户或因特网帐户。因此,在此揭示的特定结构、动作和介质,作为实现请求保护的本发明的优选形式。

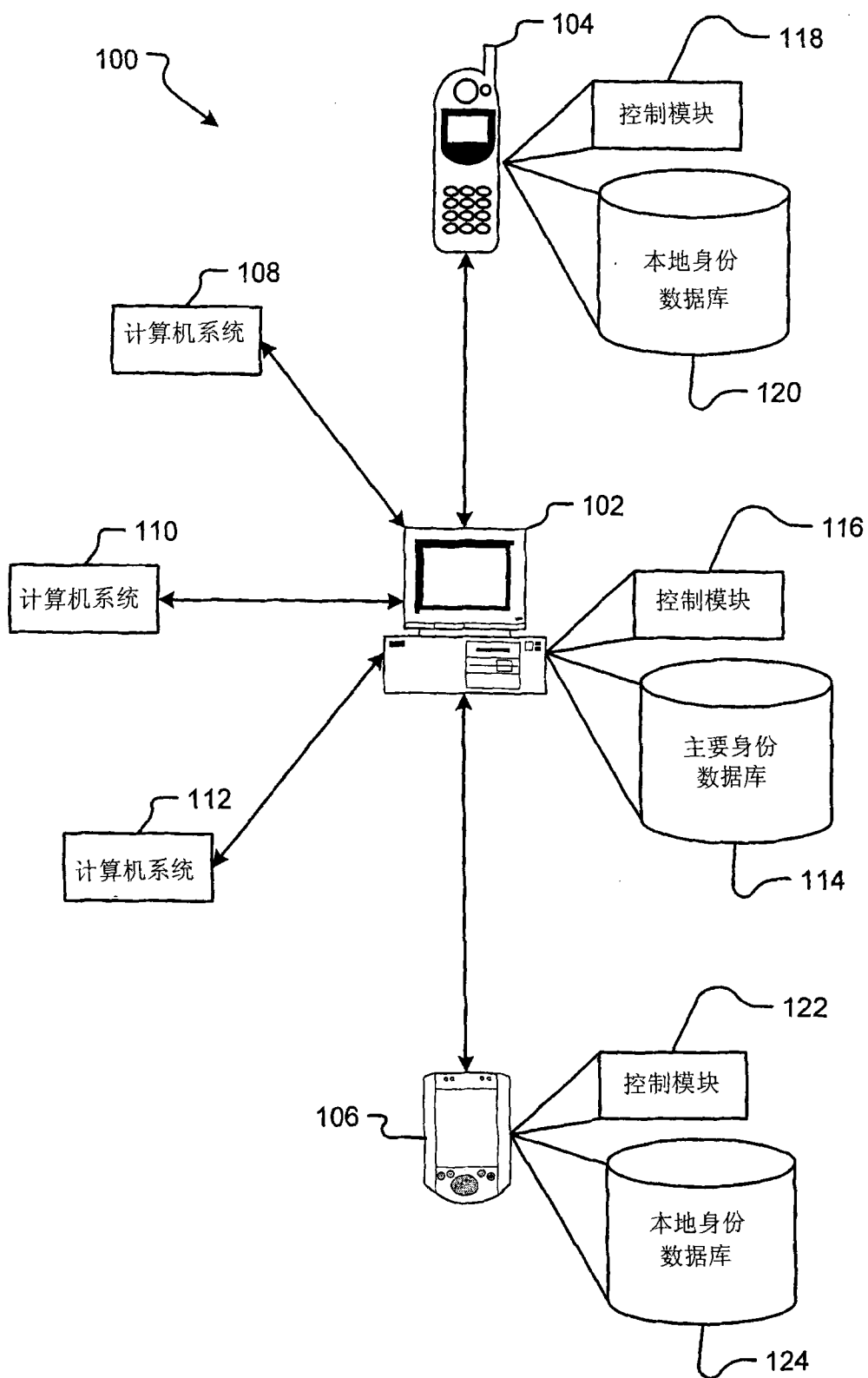


图 1

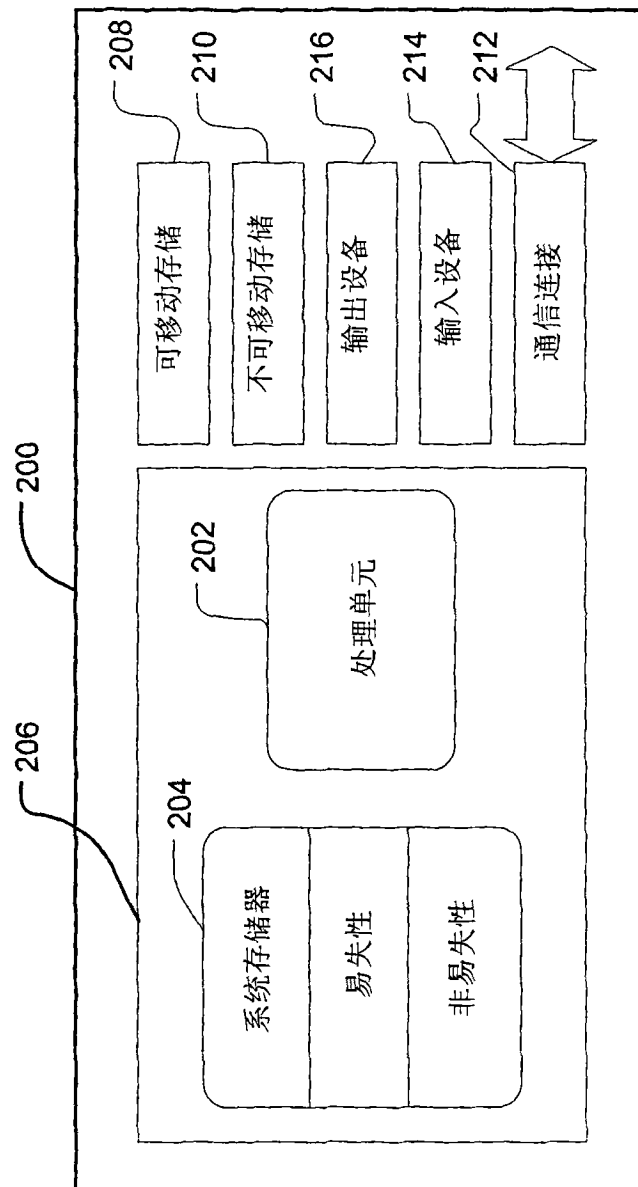


图 2

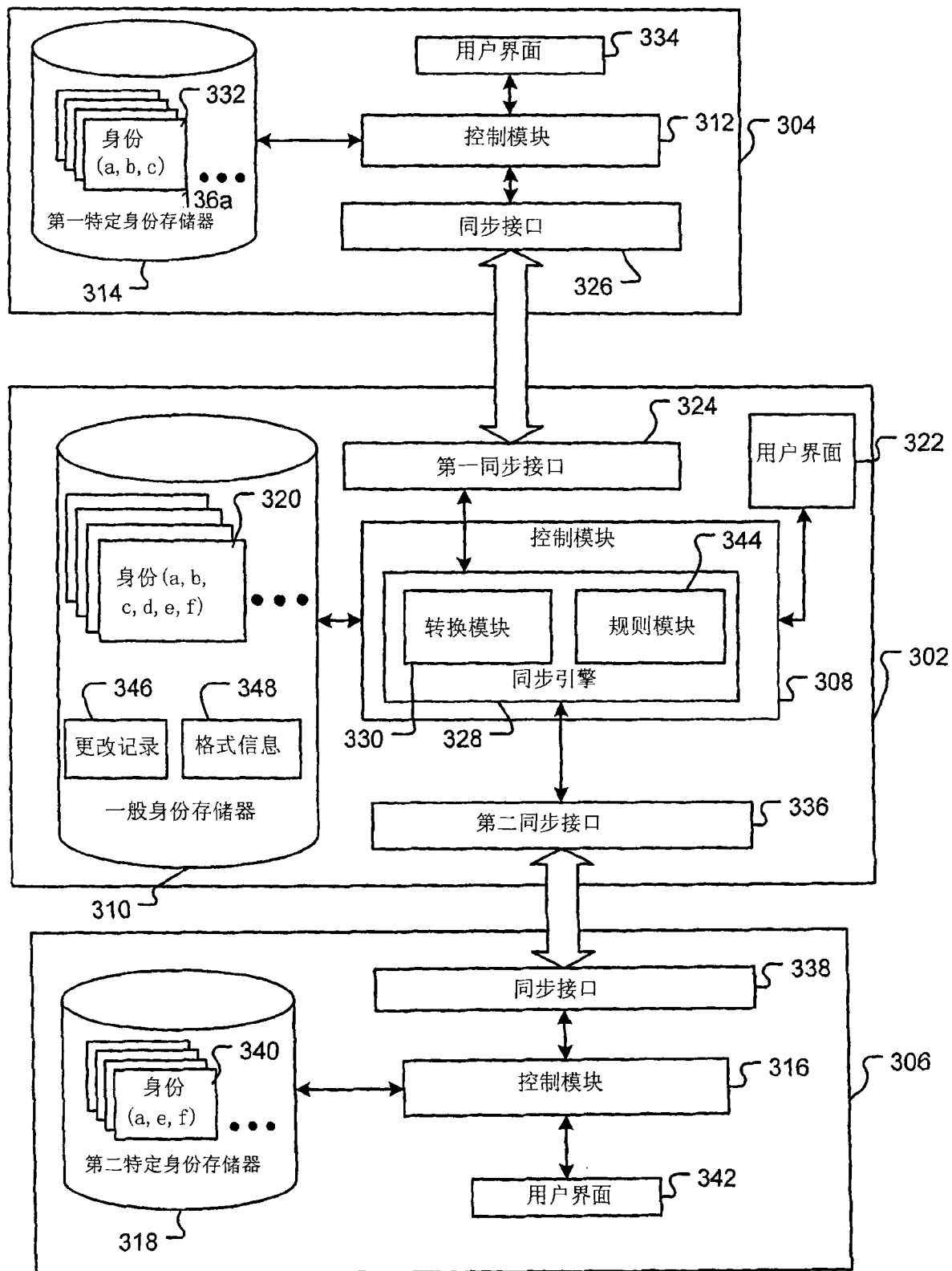


图 3

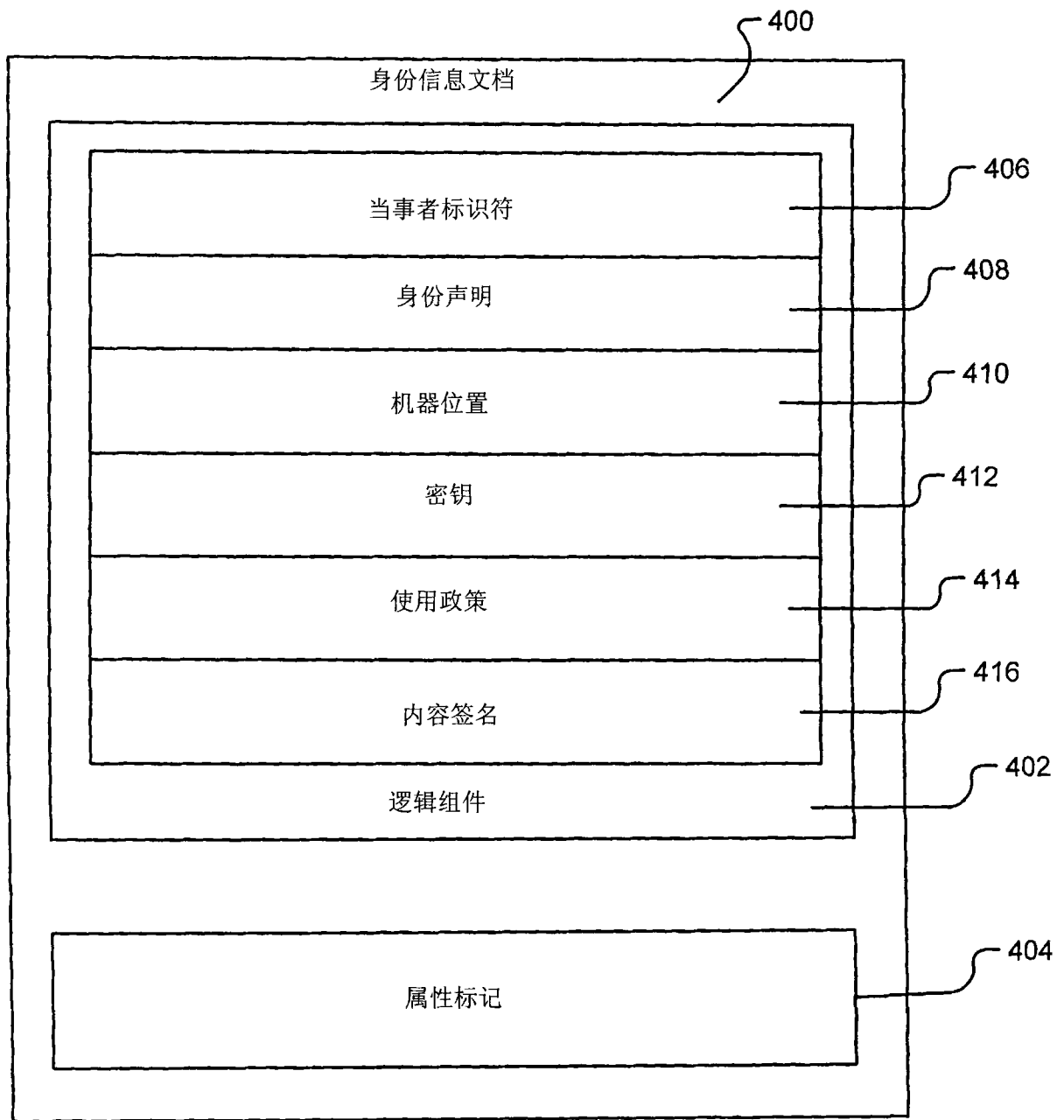


图 4

```

500 <ms:iCard IcardID="9e0d704c-20bf-495c-afe1-76ba2db6f6c3" MajorVersion="1"
      MinorVersion="0" SubjectType="Person" ICardType="New" IssueInstant="2003-08-
      21T00:02:07Z" xmlns:ms="http://www.microsoft.com/security/2003/IS/iCard">
502   <saml:AttributeStatement xmlns:saml="Urn:oasis:names:tc:SAML:1.0:assertion">
      <saml:Subject>
504       <saml:NameIdentifier Format="saml:emailAddress">
          jsmith@msn.com
          </saml:NameIdentifier>
          </saml:Subject>
          <saml:Attribute AttributeName="DisplayName"
            AttributeNamespace="http://www.microsoft.com/security/2003/IS/iCard">
            <saml:AttributeValue>
              <ms:DisplayName>John Smith</ms:DisplayName>
              </saml:AttributeValue>
              </saml:Attribute>
            </saml:AttributeStatement>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
506               <ds:X509Data>
                  <ds:X509Certificate> base-64 encoded certificate omitted </ds:X509Certificate>
                  </ds:X509Data>
                </ds:KeyInfo>
                <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
508                  XML digital signature omitted
                  </Signature>
                </ms:iCard>

```

图

5

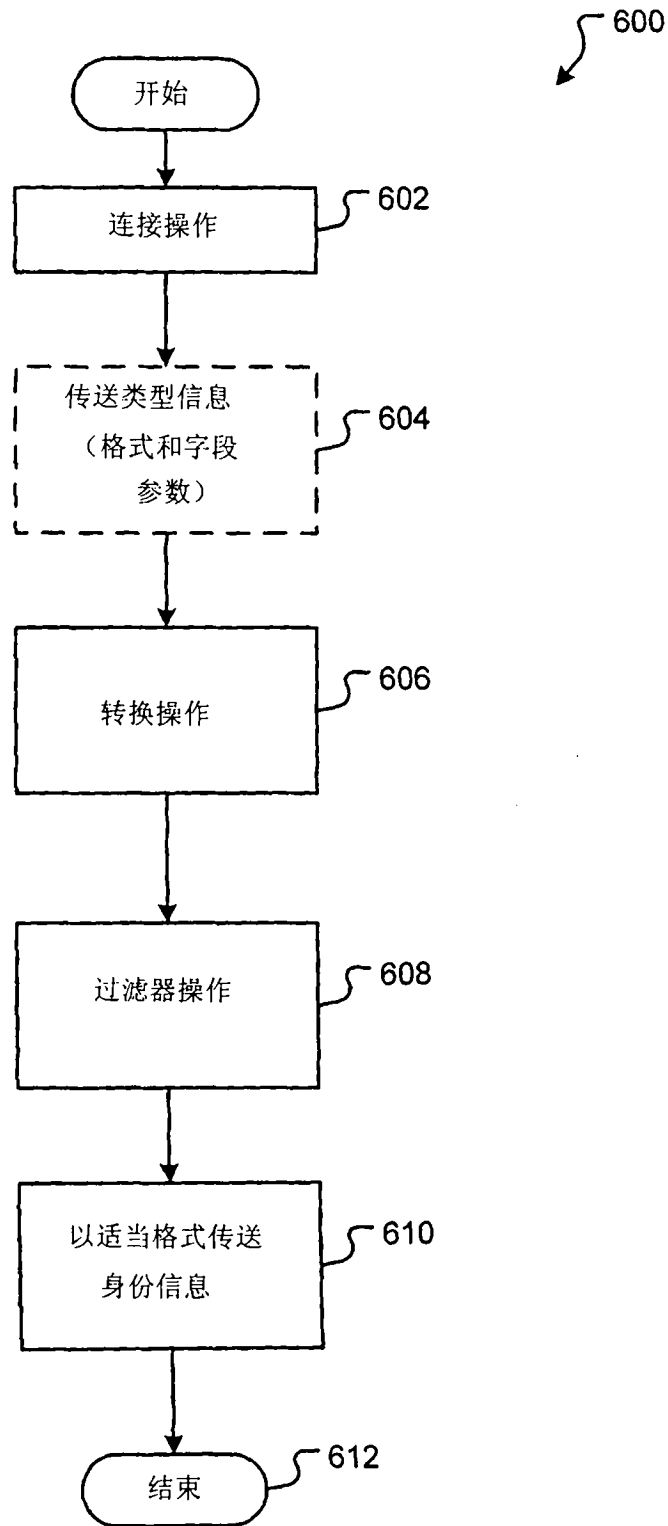


图 6

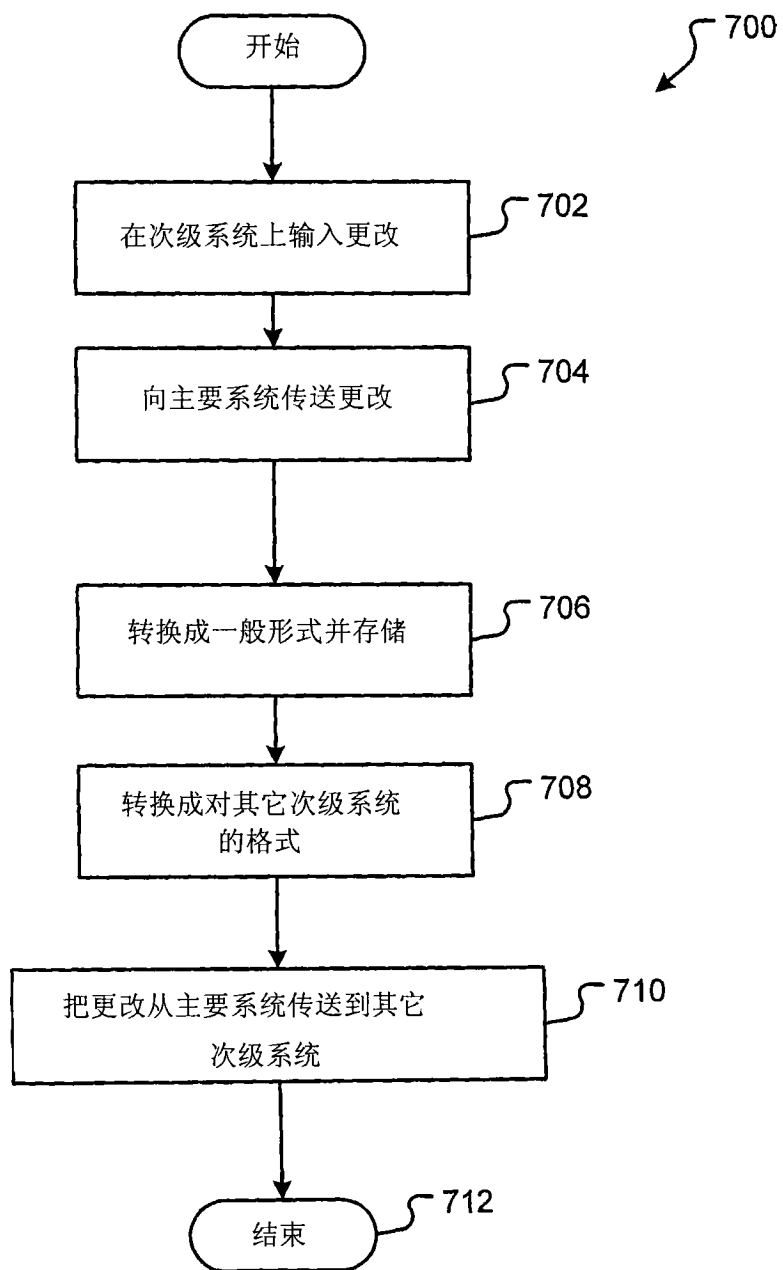


图 7

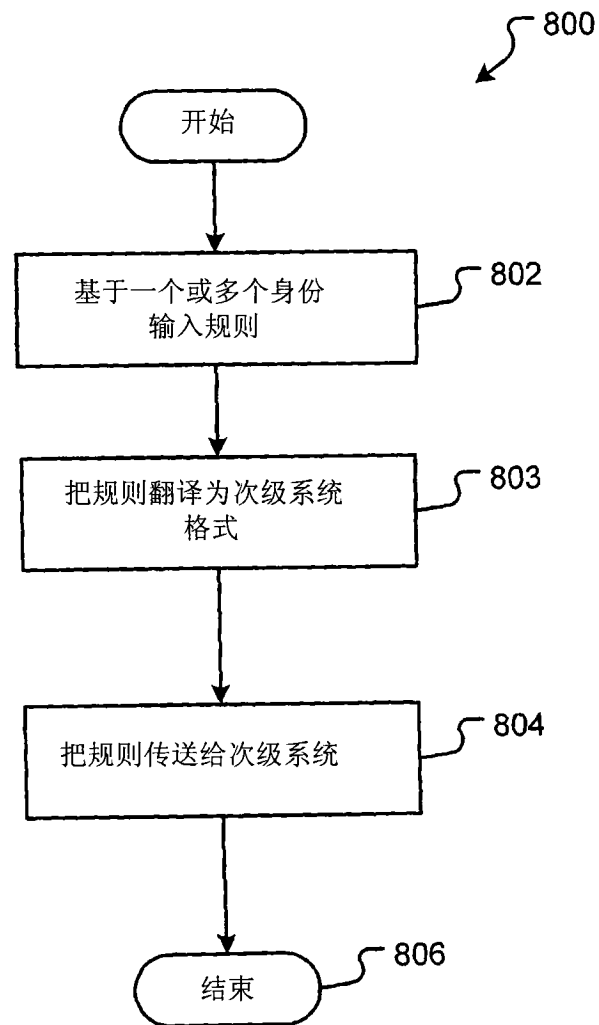


图 8