(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 101286847 B
(45)授权公告日 2011.06.15

(21)申请号 200810082784.1

(22)申请日 2008.03.19

(30)优先权数据
11/784,835 2007.04.10 US

(73)专利权人 赛门铁克公司
地址 美国加利福尼亚州

(72)发明人 苏拉伯·撒提斯 布莱恩·贺纳基

(74)专利代理机构 北京律诚同业知识产权代理有限公司 11006
代理人 徐金国

(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
CN 1845119 A,2006.10.11,
WO 2006029054 A2,2006.03.16,
CN 1283827 A,2001.02.14,
CN 1356648 A,2002.07.03,

审查员 何琳琳

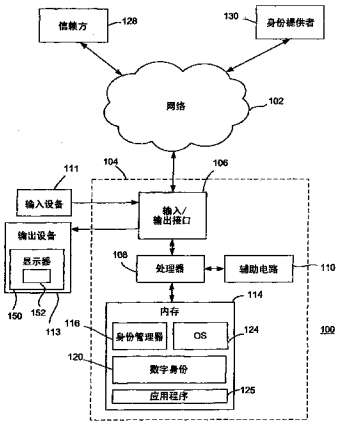
权利要求书 2 页 说明书 6 页 附图 3 页

(54)发明名称

通过单一界面管理数字身份的方法和设备

(57)摘要

本文描述了通过单一界面管理数字身份的方法和设备。本发明的一个方面涉及管理与用户有关的数字身份。获得了实体的身份政策。从数字身份中选择至少一个相关的数字身份。每个相关的数字身份包括身份政策所需的信息。从相关的数字身份中获得所选的数字身份。将符合身份政策的所选数字身份的表示法提供给实体。



CN 101286847 B

1. 一种管理与用户有关的数字身份的方法，包括：

获得实体的身份政策；

从数字身份中识别至少一个相关的数字身份，至少一个相关数字身份的每个包括身份政策所需的信息；

获得至少一个相关数字身份的所选数字身份；

提供符合实体的身份政策的所选数字身份的表示法；

将该至少一个相关数字身份提交给用户以选择所需的数字身份；

确定实体的置信水平；以及

基于置信水平，向用户提交该至少一个相关数字身份中被推荐的一个。

2. 根据权利要求 1 所述的方法，其特征在于，还包括：

除了该至少一个相关数字身份以外，使得实体使用的每个数字身份失效。

3. 根据权利要求 1 所述的方法，其特征在于，推荐的数字身份包括在置信水平高时用于用户的真实身份信息或在置信水平低时用于用户的匿名身份信息。

4. 根据权利要求 1 所述的方法，其特征在于，所选的数字身份包括第一表示法，且提供的步骤包括：

将所选数字身份的第一表示法转化为符合身份政策的表示法。

5. 根据权利要求 1 所述的方法，其特征在于，所选数字身份包括第一表示法，且其中该方法还包括：

给所选数字身份的第一表示法产生至少一个可选的表示法以产生多个表示法。

6. 根据权利要求 5 所述的方法，其特征在于，提供的步骤包括：

选择多个表示法中的一个作为符合身份政策的表示法。

7. 根据权利要求 1 所述的方法，其特征在于，每个数字身份包括至少一个表示法，其中该至少一个相关数字身份的至少一个表示法包括符合身份政策的表示法。

8. 根据权利要求 1 所述的方法，其特征在于，所选数字身份中的信息包括多个凭证，且其中该方法还包括：

选择包含在提供给实体的所选数字身份的表示法中的多个凭证的其中之一。

9. 根据权利要求 1 所述的方法，其特征在于，身份政策支持多种表示法，所选数字身份包括多种表示法，且该方法还包括：

选择多个表示法之一作为最安全的表示法；以及

指定最安全的表示法作为提供给实体的表示法。

10. 一种管理与用户有关的数字身份的设备，包括：

获得实体的身份政策的装置；

从数字身份中识别至少一个相关数字身份的装置，至少一个相关数字身份中的每一个包括身份政策所需的信息；

获得至少一个相关数字身份中的所选数字身份的装置；

为所选数字身份提供符合实体的身份政策的表示法的装置；

向用户提交至少一个相关数字身份以选择所需的数字身份的装置；

确定实体置信水平的装置；以及

基于置信水平向用户提交至少一个相关数字身份中所推荐的一个的装置。

11. 根据权利要求 10 所述的设备，其特征在于，所选数字身份包括第一表示法，且提供的装置包括：

将所选数字身份的第一表示法转化为符合身份政策的表示法的装置。

12. 根据权利要求 10 所述的设备，其特征在于，所选数字身份包括第一表示法，且该设备还包括：

为所选数字身份的第一表示法产生至少一个可选的表示法以产生多个表示法的装置。

13. 根据权利要求 12 所述的设备，其特征在于，提供的装置包括：

选择多个表示法之一作为符合身份政策的表示法的装置。

14. 根据权利要求 10 所述的设备，其特征在于，身份政策支持多种表示法，所选数字身份包括多种表示法，且该设备还包括：

选择多种表示法之一作为最安全的表示法的装置；以及

指定最安全的表示法作为提供给实体的表示法的装置。

15. 一种计算机系统，包括：

配置为存储与用户相关的数字身份的存储器；以及

配置为在网络上与实体通信的接口；以及

身份管理器，其配置为：

通过接口获得实体的身份政策；

从数字身份中识别至少一个相关数字身份，该至少一个相关数字身份中的每个包括身份政策所需的信息；

获得至少一个相关数字身份中的所选数字身份；

通过接口提供符合实体的身份政策的所选数字身份的表示法；

将该至少一个相关数字身份提交给用户以选择所需的数字身份；

确定实体的置信水平；以及

基于置信水平，向用户提交该至少一个相关数字身份中被推荐的一个。

16. 根据权利要求 15 所述的计算机系统，其特征在于，还包括：

显示器；

其中该身份管理器还配置为利用显示器上的视觉表示向用户提交该至少一个相关数字身份以供选择所选的数字身份。

17. 根据权利要求 15 所述的计算机系统，其特征在于，所选数字身份包括第一表示法，且身份管理器配置成为所选数字身份的第一表示法产生至少一个可选择的表示法以产生多种表示法。

通过单一界面管理数字身份的方法和设备

技术领域

[0001] 本发明的实施例主要涉及计算机。更具体地说，本公开涉及通过单一界面管理数字身份的方法和设备。

背景技术

[0002] 网络，如互联网，正越来越多地用于多方之间的安全通信。目前，绝大多数网络主机，如互联网网站，基于用户名和密码认证用户。通常情况下，用户最初被要求在网站提供的表格里填入各种信息，如通信地址、电子信箱地址、用户名和密码。然后用户向网站递交表格以建立帐户。此后，网站要求正确的用户名和密码以允许用户访问帐户。实际上，用于建立帐户的信息就是用户的数字身份。

[0003] 基于用户名和密码的认证已被确认为不安全。例如，用户名和密码很容易透露给未经授权的当事方，他们会利用这些信息恶意访问用户帐户。这样，正在使用其它更安全的数字身份。例如，现在的数字身份标准和系统包括公开 ID、轻量级身份协议 (LID)、安全可扩展身份协议 (SXIP)、MICROSOFT CARDSPACE 等。此外，软件包如 SYMANTEC 公司开发的 NORTON CONFIDENTIAL 提供数字身份信息的安全存储和网站表格的自动填充。

[0004] 随着跨网站的数字身份系统多样性的增加，用户需要保持以不同的格式表现并且与不同标准兼容的许多不同的数字身份。这可能导致用户避开更安全的数字身份形式而认同传统的用户名 / 密码身份。因此，本领域需要一种利用单一的界面为用户管理不同格式的数字身份的方法和设备。

发明内容

[0005] 本说明书描述了通过单一界面管理数字身份的方法和设备。本发明的一个方面涉及管理与用户相关的数字身份。获得了实体的身份政策。至少从多个数字身份中选择一个相关的数字身份。每个相关的数字身份包括身份政策所需的信息。所选的数字身份从相关的一个数字身份或多个数字身份中获得。所选的数字身份的请求书提供给符合身份政策的实体。

附图说明

[0006] 因此，参考如附图所示的实施例，可以详细理解本发明的上述特征以及上面简要概括的本发明的更独特的描述。然而应注意到，附图只阐述了本发明典型的实施例，因此不能理解为对其范围的限制，本发明可应用于其它同样有效的实施例。

[0007] 图 1 是根据本发明的一个或多个方面描述网络化的计算机系统的一个示意性实施例的方框图；

[0008] 图 2 是根据本发明的一个或多个方面描述管理与用户有关的数字身份的方法的一个示意性实施例的流程图；以及

[0009] 图 3 是根据本发明的一个或多个方面描述将用户的数字身份提供给信赖方的方

法的一个示意性实施例的流程图。

具体实施方式

[0010] 图 1 是依照本发明的一个或多个方面描述网络化的计算机系统 100 的一个示意性实施例的结构图。系统 100 包括连接到计算机 104 的网络 102。如图所示，计算机 104 包括处理器 108、存储器 114、各种辅助电路 110、和输入 / 输出接口 106。处理器 108 可包括本领域熟知的一个或多个微处理器。用于处理器 108 的辅助电路 110 包括常规的高速缓冲存储器、电源、时钟电路、数据寄存器、输入 / 输出接口等等。输入 / 输出接口 106 可直接连接或通过处理器 108 连接到存储器 114。输入 / 输出接口 106 也可配置为与输入设备 111 和 / 或输出设备 113 通信，如网络设备、各种存储设备、鼠标、键盘等等。特别地，输出设备 113 可包括显示器 150。输入 / 输出接口 106 也连接到网络 102。网络 102 包括利用电线、电缆、光纤和 / 或由各种类型的已知网络元件提供便利的无线链接，如网络集线器、交换机、路由器等等连接到计算机系统的通信系统。网络 102 可使用各种已知的协议传递信息。例如，网络 102 可为互联网的一部分。

[0011] 存储器 114 存储可由处理器 108 执行和 / 或使用的处理器可执行的指令和 / 或数据。这些处理器可执行的指令可包括硬件、固件、软件等，或其组合。存储在存储器 114 中的具有处理器可执行指令的模块可包括身份管理器 116。计算机 104 可由操作系统 124 进行编程，操作系统可包括 OS/2、Java 虚拟机、Linux、Solaris、Unix、HPUX、AIX、Windows 及其它已知平台。至少一部分操作系统 124 可设置在存储器 114 中。存储器 114 可包括一个或多个下列随机存取存储器、只读存储器、磁电阻式读 / 写存储器、光学读 / 写存储器、高速缓冲存储器、电磁读 / 写存储器等等，以及下面描述的信号轴承媒介。

[0012] 身份管理器 116 配置为管理用户的多个数字身份 120。数字身份 120 用在通过网络 102 与远程实体的沟通中。在一个典型的情况下，用户使用应用程序，如网络浏览器，发起与远程实体，此处称为信赖方 128 的通讯。信赖方 128 是一个从用户处请求数字身份并以某种方式依赖数字身份的实体。例如，信赖方 128 可用该数字身份认证用户。信赖方 128 向用户应用提交身份政策。身份政策规定信赖方 128 接受的数字身份的格式和内容。

[0013] 身份管理器 116 具有使用数字身份 120 的权限。数字身份包括与用户相关的信息。至少有些信息可用来识别和认证用户。该信息可包括，例如，用户凭证（例如，用户名、密码等）、地址数据（例如，家庭地址、账单地址、送货地址等）、账号数据（例如，信用卡帐号、银行帐号等）、个人爱好和 / 或无数其它类型数据中的任一种。数字身份信息这里称其为“内容”。

[0014] 数字身份可以一种或多种形式表现。有些格式当通过网络 102 呈现给信赖方 128 时用法不同。例如，在一种格式中，数字身份的内容存储为用户简介。信赖方 128 向用户提交一个包括使用与用户有关的信息（例如，用户名、密码、地址等）填写的域的表格。这个表格包括信赖方 128 的身份政策。用户简介用来执行表格自动填充，即，各域自动填充所要求的信息。使用这种数字身份格式的示例性商业软件是加州 Cupertino 市 Symantec 公司开发的 NORTONCONFIDENTIAL。

[0015] 另一个示意性的数字身份格式包括由用户向信赖方 128 提供的安全令牌（以下简称令牌）。信赖方 128 向用户提交请求令牌（身份政策）的表格。令牌包括一个或多个要

求，每个要求包括数字身份传达的所有信息的一部分。例如，令牌可包括对用户名、密码、信用卡帐号的声明和 / 或无数其它类型的信息。令牌可以有多种不同的格式，如 X.509 证书、Kerberos 票等。令牌也可使用标准语言生成，如安全声明标记语言 (SAML)。使用令牌的示例性软件是 MICROSOFT CARDSPACE，提供了很好理解的比喻。CARDSPACE 使用户能创建代表他们档案信息的“卡片”（即对象），而这又可以用来创建通过网络 102 提交给实体的安全令牌。

[0016] 一些基于令牌的身份格式，如 CARDSPACE，提供两种类型的数字身份 ：自我管理身份和被管理身份。为区别两种类型的身份，需要定义一个身份提供者，其为向用户提供数字身份的实体。自我管理身份是其中用户和身份提供者为同一个时的身份。例如，如果用户在在线提供商，如 AMAZON.COM 上注册一个帐号，则用户是在创建自己的身份（例如，用户名、密码、地址等）。自我管理身份可由公钥基础设施 (PKI) 备份。如本领域所知的那样，PKI 利用公钥 / 私钥对提供不对称的加密。传达自我管理身份的安全令牌使用用户私钥进行标记，且信赖方 128 利用用户公钥认证来自用户的安全令牌。这样的认证机制在本领域是公知的。

[0017] 被管理身份是一种较强形式的数字身份，其中信息由第三方备份，因此被认为是更值得信赖的。也就是说，用户外部的身份提供者 130 向用户提供数字身份。在被管理身份的情况中，数字身份的一些或所有内容都不储存在计算机 104 上。而是，一些或所有内容由身份提供者 130 存储和管理。因此，用户请求和接收来自身份提供者 130 的安全令牌，该安全令牌又可提交给可信赖方 128。

[0018] 除了表格填写和基于令牌的表示外，另一种类型的数字身份表示包括统一资源标示符 (URI) 的使用。这样的示例性身份系统包括公开 ID、轻量级身份协议 (LIP)、明显可扩展身份协议 (SXIP) 等。在基于 URI 的系统中，身份提供者 130 为用户提供能用来向信赖方 128 认证用户的 URI。用户向信赖方 128 提交 URI，信赖方 128 与身份提供者 130 沟通以确认 URI 的物主身份。

[0019] 通常，数字身份的格式简称为数字身份的“表示法”。即，给定的数字身份可以有一个或多个表示法（例如，用于表格填充的用户简介、安全令牌、基于 URI 等）。可利用一个或多个应用程序 125 创建一个或多个数字身份 120。例如，有些数字身份 120 可使用 CARDSPACE 产生。其它的数字身份 120 可使用 NORTON CONFIDENTIAL 产生。如下所述，可利用身份管理器 116 产生一个或多个数字身份 120。

[0020] 值得注意的是，在有些实施例中，身份管理器 116 配置成引入现有的数字身份 120（例如，由应用程序 125 产生的数字身份）。通常情况下，每个引入的数字身份包括单一的表示法，尽管可提供多个表示法。在任一种情况下，对于每个引入的数字身份，身份管理器 116 可产生一个或多个可供选择的表示法。对于有些数字身份（例如，自管理的），身份管理器 116 利用存储在计算机 104 上的内容产生可供选择的表示法。如果所有或部分数字身份存储在计算机外部，如在身份提供者 130 处，则身份管理器 116 可向身份提供者 130 请求内容（例如，被管理身份）。

[0021] 数字身份的可选择表示法可由身份管理器 116 自动产生或响应来自用户的命令产生。例如，给定的数字身份可包括用于表格填充的用户简介。身份管理器 116 可利用用户简介（数字身份的内容）创建自我管理的基于令牌的身份

[0022] （例如，CARDSPACE 中的自我管理卡）。身份管理器 116 也可执行逆过程。即，自我管理的基于令牌的身份中的信息可用来产生填充表格的用户简介。身份管理器 116 也可用来产生具有多个表示法的数字身份。无论如何，有些或所有的数字身份 120 可由身份管理器 116 配置具有多重表示法。

[0023] 对于与信赖方的每次沟通，身份管理器 116 配置成获得身份政策。身份管理器 116 确定身份政策需要的信息并识别一个或多个相关的数字身份。相关的数字身份包括能用来满足身份政策的内容。相关的数字身份可呈现给用户选择如显示器 150 上的视觉表示 152。身份管理器 116 可失效其数字身份与身份政策不相关的信赖方 128 的使用（例如，不具有所需内容的数字身份）。这些失效的数字身份可在显示器上对用户隐藏，或表现为指示已失效的形式（例如，通过“变灰”的视觉显示）。用户可从呈现给信赖方 128 的相关数字身份中选择一个数字身份。或者，身份管理器 116 可由用户配置或反过来自动选择一个相关的数字身份。

[0024] 在有些实施例中，身份管理器 116 确定与身份政策所需的格式无关的相关的数字身份。即，身份管理器 116 只确定数字身份是否具有身份政策要求的内容。如果所选的数字身份不是身份政策要求的格式，身份管理器 116 可产生从内容上兼容身份政策的数字身份的表示法。或者，如上所述，身份管理器 116 可具有已经为所选数字身份产生的可供选择的表示法。如果已为所选的数字身份产生身份政策要求的表示法，则此表示法由身份管理器 116 选择传送给信赖方 128。

[0025] 在有些实施例中，身份管理器 116 基于内容和格式确定相关的数字身份。例如，如上所述，身份管理器 116 已为数字身份 120 产生了可供选择的表示法。当确定相关的数字身份时，身份管理器 116 可仅仅选择那些具有所要求的内容和表示法的身份。然后，身份管理器 116 将这些相关的身份提交给用户。例如，也有这种情况，即有些数字身份不能成为可选的表示法。在这种情况下，身份管理器 116 不能“动态产生”(on the fly) 正确的表示法，如前所述。因此，身份管理器 116 不显示不能转换为用户所需格式的数字身份。

[0026] 在有些实施例中，信赖方 128 的身份政策可支持多种不同的表示法（例如，表格填充和基于令牌的机制）。当用户选择一个数字身份提交给信赖方 128 时，身份管理器 116 选择这些表示法中的某个作为最安全的表示法并指定将此表示法提交给信赖方 128。例如，信赖方 128 可接受表格填充和基于令牌的身份格式。身份管理器 116 可选择基于令牌的格式作为更安全的格式并使用所选数字身份的基于令牌的表示法。对于所选的身份，所选的最安全格式可能已经产生，或如上所述正在动态生成中。身份管理器 116 可自动实现这种格式选择。或者，身份管理器 116 可向用户提交不同的格式以供选择。身份管理器 116 可提供关于最安全表示法的建议引导用户选择。

[0027] 在有些实施例中，数字身份可包括与相同信息关联的多个用户凭证。例如，数字身份包括可与多个信赖方一起使用的地址信息（例如，通信地址和邮件地址）。然而，用户与每个信赖方建立不同的凭证（例如，不同的用户名和密码）。这样，包含地址信息（或任意其它实体的公共信息）和多重凭证的单一的数字身份就产生了。或者，用户可使用只有单一信赖方的多重凭证。无论如何，身份管理器 116 可配置成管理给定数字身份的这些凭证，包括随着时间添加和删除凭证。身份管理器 116 也可配置成选择包含在提供给信赖方 128 的数字身份的表示法中的凭证之一。例如，当相关的数字身份提交给用户时，任一数字身份

存在多重凭证的事实也可传达给用户（例如，显示器 150 上的视觉暗示）。这允许用户既选择数字身份也选择信赖方 128 使用所需的凭证。如果数字身份具有多重凭证，凭证之一可被指定为默认凭证，这样身份管理器 116 可在用户没选择时使用默认凭证。

[0028] 在有些实施例中，身份管理器 116 分析与信赖方 128 沟通的安全性以建立信赖方 128 的置信水平。置信水平可利用启发式或其它类型的分析信赖方 128 的各种属性的基于规则的引擎来建立，如信赖方 128 的名誉、交换数据的安全机制、信赖方 128 开展业务的时间长度、与该信赖方 128 沟通的用户数等。此信息可由身份管理器 116 本地确认，从第三方获得（例如，评估其它站点声誉的第三方站点），或从信赖方 128 本身获得、或从这些信息源的组合处获得。

[0029] 身份管理器 116 利用置信水平选择待提交的特定的数字身份。例如，用户可建立具有真实身份信息（“真实数字身份”）的数字身份和匿名数字身份。真实数字身份包括用户的真实身份信息。匿名数字身份可包括虚假身份信息（例如，假冒邮件地址、假名等）。身份管理器 116 可基于确认的信赖方 128 的置信水平提交真实数字身份或匿名数字身份。例如，如果确认为高置信水平，将推荐真实数字身份给用户选择。如果确认为低置信水平，将推荐匿名数字身份给用户选择。身份管理器 116 可允许用户不考虑推荐而选择数字身份。除了上述身份选择机制外（即，基于信赖方的政策和协议的身份的选择），也可执行这种基于置信水平的身份选择。

[0030] 在有些实施例中，匿名数字身份包括真实身份信息，但具有隐私屏蔽特征。例如，匿名数字身份可包括不暴露用户的真实地址、电子邮件地址和电话号码的转发地址、转发电子邮件地址、和 / 或转接电话号码。在另一个例子中，匿名数字身份包括一次性的信用卡号。在信赖方 128 使用该信用卡号之后，卡号即失效。在另一个例子中，匿名数字身份包括特定站点的电子邮件地址。即，用户建立与特定信赖方一起使用的电子邮件地址。特定站点的电子邮件地址不暴露用户的真实电子邮件地址。

[0031] 身份管理器 116 可使用各种可视的表示 152 以显示数字身份。一般来说，身份管理器 116 显示作为对象（如卡）的数字身份。在有些实施例中，给定对象可与数字身份的多重表示法链接。因此，用户不会被大量对象淹没。或者，对象可以只是数字身份的一种表示法（例如，用于表格填充数字身份的一个对象和用于相同数字身份的基于令牌的表示法的另一个对象）。

[0032] 图 2 是根据本发明的一个或多个方面描述管理与用户有关的数字身份的方法 200 的一个示意性实施例的流程图。方法 200 开始于步骤 202，其中确定了用户的一个或多个数字身份。在步骤 204，获得了每个数字身份的内容。对于有些身份，其内容可从存储该身份的计算机本地获得。对于其它的被管理的身份，其内容可从身份提供者处获得。在步骤 206 中，每个数字身份的内容用来为每个数字身份产生一个或多个可供选择的表示法。在步骤 208 中，为每个数字身份建立了一个或多个对象。这些对象可以视觉形式表现给用户。在有些实施例中，每个数字身份及其表示法与单一的对象链接。在其它的实施例中，为每个数字身份的每个表示法建立一个对象。方法 200 可由身份管理器 116 执行以引入和 / 或反过来建立数字身份 120。

[0033] 图 3 是根据本发明的一个或多个方面描述将用户的数字身份提供给信赖方的方法 300 的一个示意性实施例的流程图。方法 300 开始于步骤 302，其中获得了实体的身份

政策。如上所述，身份政策规定了所需数字身份的内容和格式。在步骤 303 中，确定实体的置信水平。在步骤 304 中，识别一个或多个相关的数字身份。每个相关的数字身份包括身份政策要求的信息。在一个实施例中，每个相关身份包括身份政策所需的内容。在另一个实施例中，每个相关身份包括身份政策要求的表示法和内容。相关的数字身份也可基于实体确定的置信水平识别。例如，如果置信水平高，相关的数字身份可仅仅包括具有真实身份信息的数字身份。另一方面，如果置信水平低，相关的数字身份可能是具有匿名信息的身份（即，虚假信息或屏蔽了隐私的真实信息）。在步骤 306 中，相关的身份可提交给用户选择。在一个实施例中，其他不相关的数字身份被信赖方禁用并提交给用户。在有些实施例中，相关的身份带有建议提交给用户。例如，如果在步骤 303 中置信水平确定为高，将推荐那些具有真实信息的身份。或者，如果置信水平为低，将推荐那些具有匿名信息的身份。在另一个例子中，如果实体接受两种数字身份，更安全的一个将被推荐给用户。

[0034] 在步骤 308 中，从相关的数字身份中获得所选的数字身份。所选的数字身份可由用户在步骤 306 中建立。或者，可从相关的数字身份中自动选择一个数字身份。在步骤 310 中，可在所选的数字身份中选择一种凭证。如上所述，数字身份可包括多重凭证。可自动选择默认凭证。或者，用户可选择凭证中的一个。在步骤 312 中，符合身份政策的所选数字身份的表示法提供给信赖方。在一个实施例中，所选数字身份包括第一表示法，该第一表示法转化为符合信赖方的身份政策的第二表示法。在另一个实施例中，所选的数字身份包括多个表示法，其中至少一个符合信赖方的身份政策。选择符合身份政策的表示法。在有些实施例中，身份政策支持多重表示法，且所选数字身份包括多重表示法，其大多兼容身份政策。提供给信赖方的表示法可为所有可能的表示法中被认为最安全的一个。方法 300 可由身份管理器 116 在与信赖方沟通时执行。

[0035] 本发明的一个方面实现为一种与计算机系统一起使用的程序产品。程序产品的程序定义了实施例的功能且可包含在多种信号承载介质中，其包括但不限于：(i) 永久存储在不可写存储介质中的信息（例如，计算机内的只读存储器如可由光盘驱动器或 DVD 驱动器读取的 CD-ROM 或 DVD-ROM 磁盘）；(ii) 存储在可写存储介质中的可变信息（例如，磁盘驱动器内的软盘或硬盘驱动器或可读写 CD 或可读写 DVD）；或 (iii) 由通信介质传达给计算机的信息，如通过计算机或电话网，包括无线通信。后面的实施例具体从英特网和其它网络上下载的信息。在执行本发明直接功能的计算机可读指令时，这样的信号承载介质体现了本发明的实施例。

[0036] 前面所述关注于本发明的实施例，在不偏离基本适用范围的情况下可设计出本发明的其它和更进一步的实施例，其范围由下面的权利要求限定。

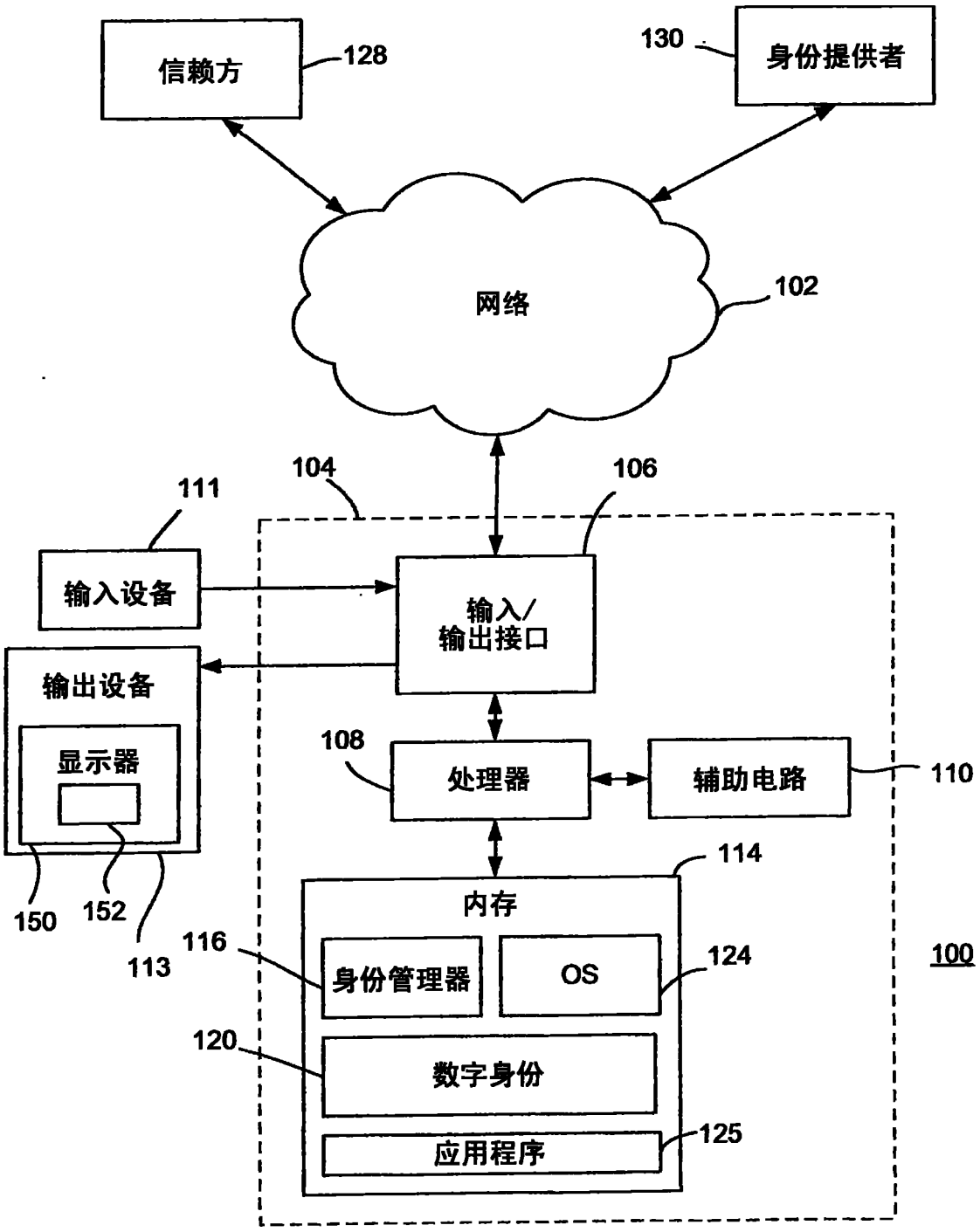

信赖方
128
130
身份提供者
网络
102
104
106
111
输入设备
输入/
输出接口
输出设备
显示器
108
处理器
辅助电路
110
114
内存
116
身份管理器
OS
124
100
120
数字身份
125
应用程序
150
152
113

图 1

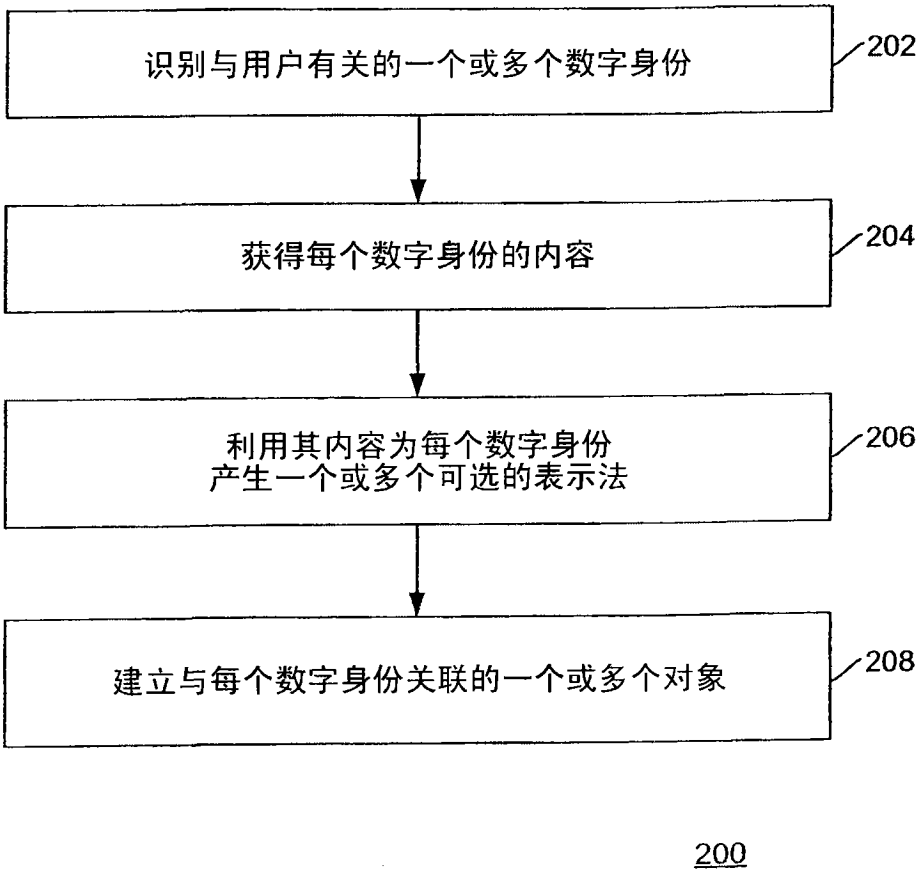

识别与用户有关的一个或多个数字身份
202
获得每个数字身份的内容
204
利用其内容为每个数字身份
产生一个或多个可选的表示法
206
建立与每个数字身份关联的一个或多个对象
208
200

图 2

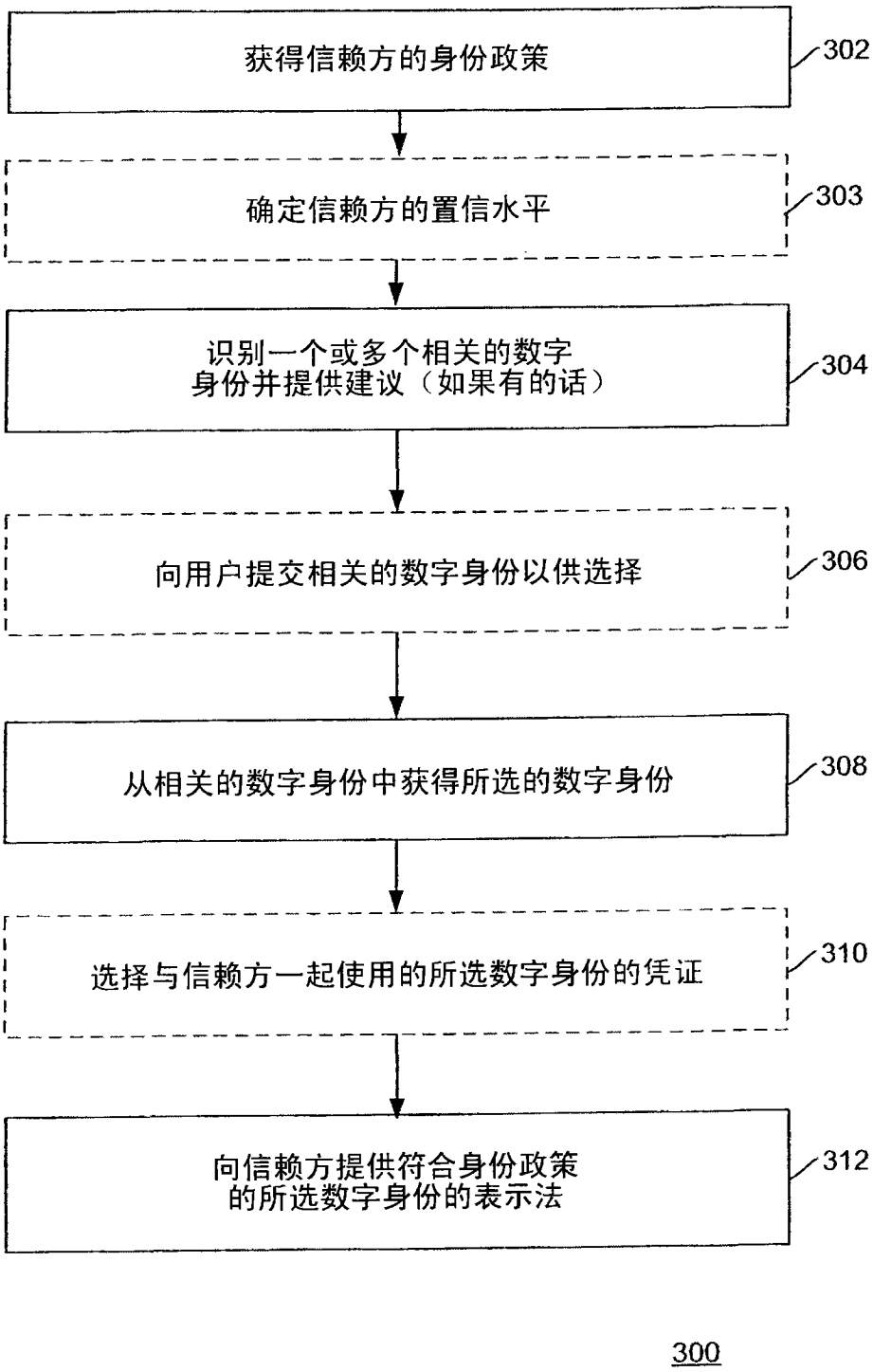

获得信赖方的身份政策
302
确定信赖方的置信水平
303
识别一个或多个相关的数字身份并提供建议（如果有的话）
304
向用户提交相关的数字身份以供选择
306
从相关的数字身份中获得所选的数字身份
308
选择与信赖方一起使用的所选数字身份的凭证
310
向信赖方提供符合身份政策的所选数字身份的表示法
312
300

图 3