(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 101681254 B
(45)授权公告日 2012.07.18

(21)申请号 200880017117.3

(22)申请日 2008.04.01

(30)优先权数据
11/752,818 2007.05.23 US

(85)PCT申请进入国家阶段日
2009.11.23

(86)PCT申请的申请数据
PCT/US2008/058994 2008.04.01

(87)PCT申请的公布数据
WO2008/147593 EN 2008.12.04

(73)专利权人 美国索尼电脑娱乐公司
地址 美国加利福尼亚州

(72)发明人 S·沃纳 E·惠尔普利

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 张晓冬 李家麟

(51)Int.Cl.
G06F 7/04(2006.01)

(56)对比文件
CN 1906576 A,2007.01.31, 全文.
US 2001036865 A1,2001.11.01, 摘要、说明书第0081段、第0084段、第0090段、第0101段、第0158段.
US 2002086734 A1,2002.07.04, 全文.
US 2004162787 A1,2004.08.19, 参见0007段、0009段、0025-0039段、0056段、0102段、0145段.

审查员 王洵

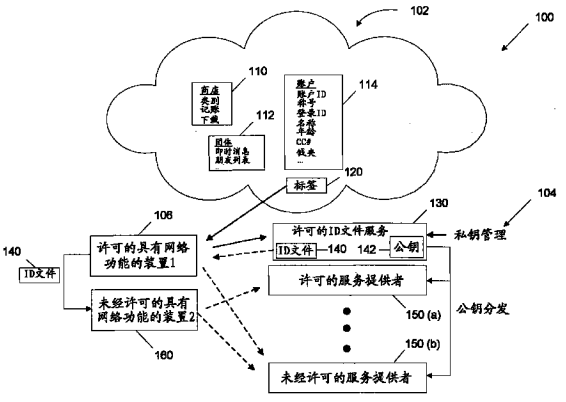
权利要求书 3 页 说明书 12 页 附图 9 页

(54)发明名称

用于认证网络中的用户的方法和设备

(57)摘要

描述了一种用于认证网络用户的方法、设备和技术。一旦用户已经在第一网络上被认证,那么用户就可以使用来自第一网络的认证信息来使用相同的或不同的具有网络功能的装置或控制台在其它网络上获得对该用户的帐户的访问。



CN 101681254 B

1. 一种用于认证网络用户的方法，所述方法包括：

使用第一具有网络功能的装置从第一网络接收认证标签，所述认证标签包括与网络用户相关联的唯一标识器；

向第二网络内的 ID 文件服务提供所述认证标签以生成与所述第二网络兼容的加密的用户 ID 文件；

从所述 ID 文件服务接收所述加密的用户 ID 文件，所述加密的用户 ID 文件基于所述认证标签中的信息；以及

向访问所述第二网络内的服务提供者的第二具有网络功能的装置提供所述加密的用户 ID 文件，其中网络用户由所述服务提供者根据所述 ID 文件和网络用户提供的密码来认证。

2. 如权利要求 1 所述的方法，其中所述第一具有网络功能的装置包括游戏控制台。

3. 如权利要求 1 所述的方法，其中所述第二具有网络功能的装置包括第二游戏控制台。

4. 如权利要求 1 所述的方法，其中所述第二具有网络功能的装置包括个人计算机。

5. 如权利要求 1 所述的方法，其中所述第二具有网络功能的装置包括蜂窝电话。

6. 如权利要求 1 所述的方法，其中使用私钥加密所述 ID 文件。

7. 如权利要求 6 所述的方法，还包括所述服务提供者使用公钥来解密所述 ID 文件。

8. 如权利要求 1 所述的方法，还包括巡览所述服务提供者并且购买服务以供所述用户在所述第一网络上使用。

9. 如权利要求 1 所述的方法，还包括响应于所述第二网络上的活动而将文件与所述 ID 文件相关联。

10. 如权利要求 1 所述的方法，其中所述用户 ID 文件包括触发将在出现预定事件时激活的数据。

11. 一种用于认证网络用户的方法，所述方法包括：

使用第一具有网络功能的装置来访问第一网络中的服务器；

从所述第一网络接收认证标签，所述认证标签包括与网络用户相关联的唯一标识器；

向第二网络内的 ID 文件服务提供所述认证标签以生成与所述第二网络兼容的加密的用户 ID 文件；

接收基于所述认证标签中的信息的所述加密的用户 ID 文件；并且

向所述第二具有网络功能的装置提供所述加密的用户 ID 文件，其中所述第二具有网络功能的装置使用所述加密的 ID 文件来访问所述第二网络内的服务提供者，其中网络用户由所述服务提供者根据所述 ID 文件和网络用户提供的密码来认证。

12. 如权利要求 11 所述的方法，其中所述第一具有网络功能的装置包括游戏控制台。

13. 如权利要求 11 所述的方法，其中所述第二具有网络功能的装置包括第二游戏控制台。

14. 如权利要求 11 所述的方法，其中所述第二具有网络功能的装置包括个人计算机。

15. 如权利要求 11 所述的方法，其中所述第二具有网络功能的装置包括蜂窝电话。

16. 如权利要求 11 所述的方法，还包括响应于所述第二网络上的活动而将文件与所述 ID 文件相关联。

17. 如权利要求 16 所述的方法，还包括向所述第一具有网络功能的装置提供相关联的文件和所述 ID 文件。

18. 如权利要求 11 所述的方法，其中所述用户 ID 文件包括触发将在出现预定事件时激活的数据。

19. 一种系统，包括：

第一具有网络功能的装置，用于访问第一网络中的服务器，所述第一网络把访问限制为授权用户集，所述服务器包括认证模块，用于认证所述用户是所述授权用户集的成员并且向所述用户提供认证标签，

其中所述装置向第二网络内的 ID 文件服务提供所述认证标签并针对用户生成与所述第二网络兼容的 ID 文件；和

由所述用户使用的第二具有网络功能的装置，其中所述 ID 文件被用于访问所述第二网络内的服务提供者，

其中由所述服务提供者进行的认证基于所述 ID 文件和所述用户提供的密码。

20. 如权利要求 19 所述的系统，其中所述第一具有网络功能的装置包括游戏控制台。

21. 如权利要求 19 所述的系统，其中所述第二具有网络功能的装置包括游戏控制台。

22. 如权利要求 19 所述的系统，其中所述第二具有网络功能的装置包括个人计算机。

23. 如权利要求 19 所述的系统，其中所述第二具有网络功能的装置包括蜂窝电话。

24. 如权利要求 19 所述的系统，其中所述 ID 文件服务使用私钥加密所述 ID 文件。

25. 如权利要求 24 所述的系统，其中所述服务提供者使用公钥解密所述 ID 文件。

26. 如权利要求 20 所述的方法，其中所述用户巡览所述第二网络中的所述服务提供者并且购买服务以供在所述第一网络上使用。

27. 如权利要求 20 所述的方法，还包括响应于所述第二网络上的活动而将文件与所述 ID 文件相关联。

28. 如权利要求 20 所述的方法，还包括使用相关联的文件和所述 ID 文件来访问所述第一网络。

29. 如权利要求 20 所述的方法，其中所述 ID 文件包括触发数据，其将在出现预定事件时激活。

30. 一种用于认证网络用户的方法，所述方法包括：

使用第一具有网络功能的装置同步到第一网络；

根据所述第一网络中的服务器所提供的认证信息创建与第二网络兼容的用户 ID 文件；

向所述第二具有网络功能的装置传输所述用户 ID 文件；

使用第二具有网络功能的装置和所述用户 ID 文件同步到第二网络；

根据所述第二网络上的活动更新所述用户 ID 文件，以由此创建更新的 ID 文件；

向所述第一具有网络功能的装置传输所述更新的用户 ID 文件；以及

将文件与所述用户 ID 文件相关联并且响应于相关联的文件中的信息而修改所述网络用户在所述第一网络上的账户。

31. 如权利要求 30 所述的方法，其中所述第一具有网络功能的装置包括游戏控制台。

32. 如权利要求 30 所述的方法，其中所述第二具有网络功能的装置包括第二游戏控制

台。

33. 如权利要求 30 所述的方法，其中所述第二具有网络功能的装置包括个人计算机。

34. 如权利要求 30 所述的方法，其中所述第二具有网络功能的装置包括蜂窝电话。

35. 如权利要求 30 所述的方法，还包括使用私钥加密所述 ID 文件。

用于认证网络中的用户的方法和设备

发明背景

技术领域

[0001] 本发明涉及一种通信网络，并且尤其涉及在这样的通信网络中对用户进行认证。

背景技术

[0002] 在典型的通信网络应用中，诸如在线游戏，玩家可以在在线体验期间与伙伴和虚拟世界交互和通信。体验的效果对玩家来说可能是重要的，所述玩家可以具有对在线游戏及其它活动的多种选择。体验的效果对在线游戏提供者在保留玩家参与到由该提供者所提供的游戏中这方面也是重要的。

[0003] 在线游戏的玩家一般在各种服务或游戏提供者上建立帐户。所述帐户例如被用来维护用户的简档、游戏统计、伙伴列表等。为了维护用户帐户的完整性，用户一般需要使用密码来认证它们自己和获得访问他们的帐户。在各种服务提供者处使用密码要求玩家记住针对每个服务提供者的帐户和密码信息。随着玩家使用越来越多的服务提供者，维护许多密码对玩家来说可能是负担。

[0004] 为了保持游戏质量，游戏提供者可能希望把访问限定为认证玩家，例如具有特定游戏控制台的玩家。通过把访问限制为特定游戏控制台，游戏提供者有信心使玩家与游戏的交互在跨过多个玩家和多个标题都是一致的。例如，游戏提供者可能不想让玩家使用个人计算机 (PC) 来玩针对具有特定游戏控制台的玩家而设计的游戏。虽然依照这种方式限制玩家访问可能保持所想要的质量等级，但是对用户来说依照这种方式限制对他们的账户的访问可能也是麻烦的。例如，如果玩家只想检查来自他伙伴的消息，那么他们或许不能，这是因为他们在那时不能访问所要求的控制台。

[0005] 从而，需要改进对访问通信网络的用户的认证。

发明内容

[0006] 本发明的实施例提供了一种用于认证网络用户的方法、系统、设备和程序。在一个实施例中，第一封闭或安全的网络把对网络的访问限制为认证用户。一旦用户已经在安全网络上被认证，那么所述用户可以使用从所述安全网络接收的认证信息来访问在第二开放网络中的服务提供者网络。换句话说，服务提供者使用来自封闭网络的认证信息来确定是否应当允许该用户访问所述服务提供者。

[0007] 在另一实施例中，认证信息可以被用户传输给另一具有网络功能的装置，所述装置被用来访问服务提供者网络或安全网络。依照这种方式，可以在不同的具有网络功能的装置上把用户与相同的认证信息相关联。

[0008] 在一个实施例中，一种用于访问网络的方法包括由用户访问第一网络以及对该用户进行认证。然后生成与所述用户相关联的标签 (ticket)。根据标签中的信息和用户密码来生成与该用户相关联的加密的 ID 文件。然后用户使用所述 ID 文件来访问在第二网络内

的服务提供者。

[0009] 在另一实施例中，一种用于生成与用户相关联的 ID 文件的方法包括从安全网络接收关于所述用户的认证信息。然后提供用户数据，所述用户数据包括 ID 文件服务的用户密码和该认证信息。ID 文件服务把所想要的用户数据和密码汇编 (assemble) 到中间文件中，然后把所述中间文件加密到签名的 ID 文件中。然后把该签名的 ID 文件提供给用户并且所述用户可以使用所述签名的 ID 文件来访问各种网络。

[0010] 在实施例中，ID 文件包括对用户来说是唯一的信息。依照这种方式，一旦服务提供者已经认证用户，那么所述服务提供者就可以由此向用户提供对他们账户的访问。

[0011] 另外，ID 文件可以包括触发数据，其将在出现预定事件时激活。还可以更新 ID 文件。例如，可以利用关于网络上活动的信息来更新 ID 文件。然后，当用户进入不同的网络或者重新进入先前已经进入的网络时，可以使用更新的 ID 文件来进行访问。在用户已经被认证之后，可以响应于另一网络上的活动而使用更新的信息来修改或调整用户在该网络上的帐户。

[0012] 可以由用户使用以访问各种网络和服务提供者的具有网络功能的装置的例子包括可以访问网络的任何设备，诸如游戏控制台、个人计算机 (PC)、个人数字助理 (PDA)、蜂窝电话、机顶盒等。

[0013] 在查阅以下详细描述和附图之后，本发明的其它特征和优点对那些本领域普通技术人员来说将变得更容易理解。

附图说明

[0014] 图 1 是图示依照本发明的实施例的认证系统的框图。

[0015] 图 2 是图示用于创建 ID 文件的实施例的框图。

[0016] 图 3 是使用在不同的具有网络功能的装置上所生成的 ID 文件来访问服务提供者的框图。

[0017] 图 4 是图示访问网络的实施例的流程图。

[0018] 图 5 是图示创建 ID 文件的实施例的流程图。

[0019] 图 6 是图示访问网络的实施例的流程图。

[0020] 图 7 是图示访问网络的实施例的流程图。

[0021] 图 8 是在两个具有网络功能的装置之间传输信息的实施例的流程图。

[0022] 图 9 是图示可以结合所描述的各种实施例使用的示例具有网络功能的装置的框图。

具体实施方式

[0023] 在阅读以下描述之后，一个本领域技术人员会变得清楚怎样在各种候选实施例和候选应用中实现本发明。然而，尽管这里将描述本发明的各种实施例，不过应当理解这些实施例只作为例子给出而并非意味着限制。同样地，对各种实施例的详细描述不应当被解释为限制本发明的范围或幅度。

[0024] 这里所描述的方法、设备、技术、程序和系统的各种实施例提供对网络用户进行认证。例如，在一个实施例中，第一封闭或安全的网络把对网络的访问限制为认证用户。一

旦用户已经在该安全网络上被认证，那么所述用户可以使用从该安全网络接收的认证信息来访问在第二网络中许可或未经许可的服务提供者网络。换句话说，第二网络中的服务提供者使用来自封闭网络的认证信息来确定是否应当允许该用户访问所述服务提供者。在另一实施例中，认证信息可以被用户传输到另一未经许可的具有网络功能的装置，所述装置被该用户用来访问经许可的服务提供者网络。在另一实施例中，认证信息可以被传输到另一许可的或未经许可的具有网络功能的装置，并且由所述用户用来访问未经许可的服务提供者网络。依照这种方式，可以在不同的具有网络功能的装置上以及许可和未经许可的服务提供者这两者上把用户与相同的认证信息相关联。可以由用户使用的具有网络功能的装置的例子包括可以访问网络的任何设备，诸如游戏控制台、个人计算机 (PC)、个人数字助理 (PDA)、蜂窝电话、机顶盒等。

[0025] 图 1 是图示依照本发明实施例的认证系统的框图。如图 1 的例子中所示，认证系统 100 包括第一网络 102 和第二网络 104。第一用户具有网络功能的装置 106 可以用来访问第一网络 102 和第二网络 104。在一个实施例中，第一网络可以是封闭或安全的网络并且第二网络可以是开放服务提供者网络。

[0026] 在一个实施例中，对封闭网络 102 的访问可以限于授权用户集，诸如正使用特定的具有网络功能的装置或特定类别的具有网络功能的装置的用户。例如，对封闭网络 102 的访问可以限于正使用特定的许可游戏控制台的用户。在一个实施例中，封闭网络 102 发出认证令牌以便保持封闭网络的完整性。一旦用户已经被认证，则可以向他们提供认证令牌，其允许用户巡览该网络。

[0027] 例如，封闭网络 102 可以通过验证用于访问封闭网络 102 的具有网络功能的装置具有其它形式标识的序列号来认证用户，所述序列号把具有网络功能的装置标识为特定的类别。一旦确定具有网络功能的装置被授权，那么网络可以向具有网络功能的装置提供令牌或标签，以允许所述具有网络功能的装置巡览网络。在一个实施例中，通过把对封闭网络 102 的访问限制为特定类型的游戏控制器，可以保持在游戏中以及跨不同的游戏标题玩的一致性。另外，可以跨过多个标题跟踪用户的网络身份。封闭网络 102 还可以包括商品或商店模块 110，在那里用户可以购买商品。另外，封闭网络 102 可以包括服务模块 112，其容许用户建立各种网络团体，例如即时消息发送团体和朋友列表等。

[0028] 在一个实施例中，对封闭网络 102 的访问由请求访问的、许可用户的具有网络功能的装置 106 来实现。封闭网络 102 中的服务器或网络控制器对用户进行认证。当用户被认证时，准许用户访问他们的用户帐户模块 114。用户帐户模块 114 维护关于用户的信息，诸如用户的称号 (handle)、登录名、信用卡号，以及该用户在封闭网络 102 中的先前会话中提供的其它信息。如果用户没有已存在的帐户，那么可以运行服务器上的应用来收集用户信息并且建立帐户。另外，用户可以修改他们帐户中的信息。

[0029] 封闭网络 102 中的服务器可以向许可用户的具有网络功能的装置 106 发出认证 120 的文件，其被称为标签或令牌。认证 120 的标签可以包括来自用户的帐户的信息中一些信息。例如，标签可以包括唯一的网络标识器、网络登录 ID、用户的称号等。标签还可以包括与帐户特权级别、权利和帐户偏好相关的信息。典型情况下，标签通常将不包括敏感的个人信息，诸如信用卡信息。

[0030] 在一个实施例中，用户具有网络功能的装置 106 可以使用在封闭网络 102 上所生

成的标签 120 来访问第二服务提供者网络 104。依照这种方式，服务提供者知道所述用户已经被封闭网络 102 认证。服务提供者还根据标签中的信息知道用户的身份。例如，用户具有网络功能的装置 106 可以向服务提供者网络 104 中的许可的 ID 文件服务器 130 传送标签 120。ID 文件服务器 130 证实该标签 120。标签证实过程要求使用与封闭网络 102 兼容的技术验证源签名和正确地解密标签。

[0031] 在一个实施例中，在标签 120 已经被许可的 ID 文件服务 130 证实之后，ID 文件服务 130 汇编、加密并签名 ID 文件。在一个实施例中，使用那些本领域技术人员已知并且被认为是公钥 / 私钥技术的技术来签名 ID 文件。

[0032] 签名的 ID 文件 140 被从许可的 ID 文件服务 130 传送到用户具有网络功能的装置 106。ID 文件服务 130 还向网络 104 中的许可和未经许可的服务提供者 150(a，b) 传送公钥 142 的拷贝。当用户想要访问未经许可的服务提供者 150(b) 时，用户具有网络功能的装置 106 向未经许可的服务提供者 150(b) 传送签名的 ID 文件 140 和由用户所提供的密码。未经许可的服务提供者 150(b) 使用从 ID 文件服务 130 接收的公钥的拷贝来解密 ID 文件 140。未经许可的服务提供者 150(b) 然后验证来自 ID 文件 140 的密码与用户所提供的密码匹配。在另一实施例中，用户具有网络功能的装置 106 可以向未经许可的服务提供者 150(b) 传送 ID 文件 140 并且未经许可的服务提供者 150(b) 然后可以请求用户密码。

[0033] 如果来自 ID 文件 140 的密码与由用户所提供的密码匹配，那么允许用户具有网络功能的装置 106 访问未经许可的服务提供者 150(b)。依照这种方式，用户可以使用相同的密码和帐户信息来访问多个许可和未经许可的服务提供者 150，由此消除了用于为不同的服务提供者 150 维护多个帐户和密码的需要。

[0034] 在一个实施例中，可以在许可的服务提供者 150 内包括经许可的 ID 服务 130。在其它实施例中，可以在其它位置中包括经许可的 ID 服务提供者，例如它可以是独立的服务，或者它可以包括在封闭网络 102 中或者在用户具有网络功能的装置 106 中。

[0035] 在实施例中，多个服务提供者可以被分组并且相同的公钥 / 私钥组合被用于签名他们各自的 ID 文件。在另一实施例中，对于每个单独的服务提供者可以使用不同的私钥 / 公钥。

[0036] 继续参照图 1，许可用户的具有网络功能的装置 106 可以向第二未经许可的具有网络功能的装置 160 输出或以其它方式传送 ID 文件 140。在一个实施例中，许可用户的具有网络功能的装置 106 和第二未经许可的具有网络功能的装置 160 可以都是相同类别或类型的具有网络功能的装置。在其它实施例中，第二未经许可的具有网络功能的装置 160 可以是不同于许可用户的具有网络功能的装置 106 的其它类别的具有网络功能的装置。

[0037] 例如，许可用户的具有网络功能的装置 106 可以是特定类别的游戏控制台，诸如由特定制造商或制造商组制造的系列游戏控制台的成员。游戏控制台可以访问封闭网络 102，这是因为封闭网络与游戏控制台制造商相关联并且对封闭网络 102 的访问限定于只允许制造商所标识的授权游戏控制台来访问。在此例子中，一旦被授权，游戏控制台就可以接收来自封闭网络的标签。游戏控制台然后可以向许可的 ID 文件服务 130 传送标签并且接收签名的 ID 文件 140。然后游戏控制台可以使用 ID 文件 140 访问许可和未经许可的服务提供者 150。服务提供者知道用户已经被封闭网络 102 认证并且从 ID 文件 140 中的信息还知道关于用户的附加信息，诸如他们的身份。

[0038] 游戏控制台还可以向第二未经许可的具有网络功能的装置 160 输出或传送 ID 文件 140，并且第二具有网络功能的装置可以使用 ID 文件 140 来访问许可和未经许可的服务提供者 150。在一个实施例中，第二具有网络功能的装置 160 是另一游戏控制台。在其它实施例中，第二具有网络功能的装置 160 可以是个人计算机、来自不同制造商的游戏控制台、个人数字助理、蜂窝电话、机顶盒或其它具有网络能力的装置。

[0039] 在以上例子中，第二未经许可的具有网络功能的装置 160 使用 ID 文件 140 可以在许可和未经许可的服务提供者访问帐户或帐户信息。依照这种方式，用户可以使用不同的许可和未经许可的具有网络功能的装置来访问他们的帐户信息。例如，用户可以在第一封闭网络 102 上使用游戏控制台建立帐户，并且在第二网络 104 中的许可或未经许可的服务提供者 150 上建立相关联的帐户信息。稍后，用户可以使用不同的未经许可的具有网络功能的装置（诸如 PC）来访问他们的帐户信息。依照这种方式，用户不被限定为只能够用特定的许可的具有网络功能的装置来访问他们的帐户信息，而是能够在不同的位置从不同的具有网络功能的装置访问他们的帐户信息。一旦用户已经访问了他们的帐户，那么他们就可以使用该账户来执行各种功能，诸如玩游戏、给朋友发电子邮件、购买物品、检查消息等。

[0040] 图 2 是图示用于创建 ID 文件的实施例的框图，所述 ID 文件诸如图 1 的 ID 文件 140。如图 1 所示，在用户已经被认证之后，许可用户的具有网络功能的装置 106 接收来自封闭网络 102 的标签。然后用户可以占用 (engage) 帐户管理模块或程序 204 并且请求创建 ID 文件 140。例如，用户可能在最初开始服务时想要创建 ID 文件 140，或者用户可能因为所述用户已经改变了在 ID 文件中所包含的一些用户信息而想要创建 ID 文件 140。

[0041] 在一个实施例中，帐户模块 204 可以激活密码模块 206 来接收用户的密码。例如，如果用户第一次正生成 ID 文件 140 或者用户正改变他们的密码，那么密码模块 206 可以从所述用户接收密码。然后用户具有网络功能的装置 106 向图 1 中的 ID 文件服务 130 传送标签、密码和任何所需要的其它信息。

[0042] ID 文件服务 130 操作 ID 文件模块 224，所述 ID 文件模块 224 使用与封闭网络 102 兼容的许可技术从标签中提取所想要的用户数据。ID 模块 224 还获得密码和任何其它想要的信息，例如当前日期。ID 模块 224 然后把数据汇编到中间文件中，使用私钥加密该中间文件来制作签名的 ID 文件 140。签名的 ID 文件 140 被传送到用户具有网络功能的装置 106 中的 ID 文件模块 208。ID 文件 140 将很可能包括但不限于经由标签而变得可用的信息。附加信息可以包括不与封闭网络 102 相关联而只与一个或多个服务提供者 150 有关的数据。

[0043] 在一个实施例中，ID 文件模块 208 然后可以向存储装置输出或保存 ID 文件 140，使得可以把 ID 文件 140 安装在另一具有网络功能的装置上。在另一实施例中，ID 文件模块可以通过有线或无线网络与另一具有网络功能的装置通信。例如可以在处于有线或无线局域网上的两个具有网络功能的装置之间或经由诸如蓝牙接口之类的无线通信或其它通信网络来传送 ID 文件 140。

[0044] 图 3 是使用 ID 文件 140 访问网络或服务提供者的框图。如图 3 所示，具有网络功能的装置 160 使用浏览器 310 来访问或登录到服务提供者 150。如果必要的话具有网络功能的装置还可以下载浏览器插件 312。

[0045] 具有网络功能的装置 160 中的密码模块 316 从用户接收输入，诸如用户的称号。用

户的称号信息标识用户并且还可以用来标识与该称号相关联的 ID 文件 140。提供了密码模块 316，或者检索 ID 文件 140。例如，密码模块 316 可以从固定的或者可移动的存储器或存储装置检索 ID 文件 140。密码模块 316 还接收用户的密码。

[0046] 密码模块可以使用用户的称号信息在具有网络功能的装置中的存储介质内在预定位置搜索 ID 文件 140。例如，存储介质可以包括硬盘驱动器、RAM、ROM 或可移动的介质驱动器，诸如记忆棒或其它类型的存储介质。如果没有找到 ID 文件 140，则密码模块 316 可以向用户呈现浏览器模块 318 并且让用户标识所述 ID 文件的位置。

[0047] 然后通信模块 320 向服务提供者 150 传送 ID 文件 140 和密码。在服务提供者处，认证模块 340 接收 ID 文件 140 和密码。认证模块 340 对 ID 文件 140 进行解密并且把 ID 文件 140 中的密码与用户所提供的密码进行比较。如果密码不匹配，则拒绝用户访问该服务提供者 150。如果密码确实匹配，表明用户与 ID 文件 140 相关联，于是服务提供者 150 将建立 WEB 会话。例如，服务提供者 150 可以向具有网络功能的装置返回会话 cookie（少量信息）350。

[0048] 认证模块 340 任选地用服务提供者 150 所访问的数据库 342 中的已知签名来检查 ID 文件 140 签名。认证模块 340 还可以任选地检查 ID 文件 140 日期或期限以确定 ID 文件 140 是否仍然适时或者是否它已经期满。

[0049] 用于访问服务提供者的具有网络功能的装置可以是与用于创建 ID 文件 140 的装置相同的具有网络功能的装置或不同的具有网络功能的装置。例如第一具有网络功能的装置可以用来创建 ID 文件 140 以及然后该 ID 文件 140 可以被传输到第二具有网络功能的装置。依照这种方式，用户可以向多个具有网络功能的装置传输他们的 ID 文件 140 并且使用不同的具有网络功能的装置来在不同的网络上访问他们的帐户。

[0050] 图 4 是图示访问如图 1 和 3 所描述的网络的实施例的流程图。流程在块 402 中开始，其中用户使用具有网络功能的装置来访问第一受控网络。流程继续至块 404，其中用户由第一受控网络认证。然后流程继续至块 406 并且第一网络向用户传送认证标签。标签例如可以包括关于用户的信息以及确认用户已经被第一网络认证的信息。

[0051] 流程继续至块 408 并且用户访问许可的 ID 文件服务。ID 文件服务从用户接收标签和密码。在块 410 中，ID 文件服务验证用户被第一网络授权。通过受控的第一网络的说明来确定用于此的装置，并且可以要求许可的标签认证软件在 ID 文件服务他 130 上运行。然后 ID 文件服务生成针对用户的 ID 文件 140 并且向所述用户传送 ID 文件 140 的拷贝。在一个实施例中，使用公钥 / 私钥技术来签名 ID 文件 140。在块 412 中，用户使用签名的 ID 文件来访问服务提供者。

[0052] 使用所描述的技术，用户可以使用第一具有网络功能的装置来访问第一网络并被第一网络认证。用户然后可以在第二具有网络功能的装置上使用来自第一网络的认证来访问第二网络。在与第二网络中的服务提供者交互期间，用户可以参与诸如购买货物或服务之类的活动以供在第二具有网络功能的装置上使用或供在第一具有网络功能的装置上使用。例如，用户可以访问第二网络以登录到服务提供者上并且购买电影、游戏、线性程序、音乐、电影、电视节目、情景内容或其它娱乐节目以供在第二具有网络功能的装置上使用或供在第一具有网络功能的装置上使用。在一个例子中，用户可以使用 PC（第二具有网络功能的装置）来访问服务提供者并且购买电影。然后该电影可以被下载或推入 (push) 到用户

的第一具有网络功能的装置，诸如游戏控制台。在一个例子中，如果该游戏控制台处于开，那么该电影能够被立即推入到该游戏控制台，或者如果该游戏控制台处于关闭，则所述电影可以被服务提供者排队并且当该游戏控制台开时被下载或推入到该游戏控制台。

[0053] 在另一实施例中，用户可以使用第一具有网络功能的装置（诸如游戏控制台）来访问服务提供者，诸如游戏站点。用户可以使用该游戏控制器来与游戏交互或者“玩”游戏。用户然后可以使用 ID 文件用第二具有网络功能的装置（诸如 PC）登录到相同的游戏站点。该站点将识别用户并且允许用户在他们早些时候玩游戏时他们离开的点处进入相同的游戏环境。在此例子中，用户可以使用不同的具有网络功能的装置（诸如游戏控制台和 PC）玩相同的游戏。当用户登录到该站点时，他们可以使用该用户在该站点上的帐户来查询该站点以确定已经出现了什么活动。依照这种方式，用户可以确定在他们不知道的帐户上是否已经有活动。

[0054] 在又一实施例中，在第一和第二具有网络功能的装置之间传输的 ID 文件 140 可以包括关于在每个具有网络功能的装置上已经出现的活动的信息，以及要在这两个具有网络功能的装置之间传送的其它信息。例如，从第一具有网络功能的装置传输到第二具有网络功能的装置的 ID 文件 140 可以包括信息或触发数据，如果在第二具有网络功能的装置上出现预定事件，那么所述触发数据将激活。ID 文件 140 还可以包括广告、活动信息或简档数据。同样，从第二具有网络功能的装置传输到第一具有网络功能的装置的 ID 文件 140 可以包括信息或触发数据以及广告、活动信息或简档数据，如果在第一具有网络功能的装置上出现预定事件，那么所述触发数据将激活。例如，可以更新 ID 文件 140 以包括关于哪些 web 站点已经被具有网络功能的装置或其它具有网络功能的装置活动访问的信息。

[0055] 图 5 是图示创建 ID 文件的实施例的流程图，所述 ID 文件诸如图 1-3 中的 ID 文件。流程在块 502 中开始，其中用户请求创建 ID 文件。流程继续至块 504，其中提示用户输入密码。然后在块 506 中，用户从安全网络原始接收的标签被传送到 ID 文件服务。关于用户的信息可以包括关于用户的简档信息以及来自安全性网络的认证数据。

[0056] 流程继续至块 507，在那里 ID 文件和所述 ID 文件的密码被传送到 ID 文件服务。然后在块 508 中 ID 文件服务验证标签真实性，把所想要的数据项和密码汇编到中间文件中，以及然后把所述中间文件加密到签名的 ID 文件 140 中。例如可以使用公钥 / 私钥来签名 ID 文件 140。流程继续至块 510 并且把签名的 ID 文件 140 传送给用户。

[0057] 图 6 是图示访问诸如图 1-3 中所描述的网络的实施例的流程图。流程在块 604 中开始，其中用户提供他们的称号和密码。流程继续至块 606，其中在那里向服务提供者提供与用户的称号和密码相关联的 ID 文件 140。在一个实施例中，已经使用公钥 / 私钥签名了 ID 文件 140。在块 608 中服务提供者根据 ID 文件 140 和密码来认证用户。例如，如果 ID 文件 140 已经被签名，那么服务提供者使用签名该 ID 文件的 ID 文件服务所提供的公钥来解密所述 ID 文件 140。

[0058] 流程继续至块 610，在那里确定用户是否被认证。在一个实施例中，在 ID 文件 140 内包括的是密码，把它与用户所提供的密码相比较以确定密码是否匹配。如果密码匹配，则评估 ID 文件中的认证数据以确定用户是否被认证。如果用户未被认证，则流程继续至块 612 并且拒绝用户访问服务提供者。如果在块 610 中确定了用户被认证，则流程继续至块 614 并且建立在服务提供者上的会话。

[0059] 图 7 是图示访问诸如在图 1-3 中所描述的网络的实施例的流程图。流程在块 704 中开始，其中用户使用第一具有网络功能的装置同步到网络。例如，第一具有网络功能的装置可以是游戏控制台、PC、PDA、蜂窝电话或其它具有网络功能的装置。在块 706 中，生成与用户相关联的 ID 文件 140 和密码。然后在块 708 中 ID 文件 140 被传输到第二具有网络功能的装置。第二具有网络功能的装置的例子包括游戏控制台、PC、PDA、蜂窝电话或其它具有网络功能的装置。使用密码和 ID 文件，用户使用第二具有网络功能的装置来访问网络。因为第二具有网络功能的装置使用与用户相关联的 ID 文件 140 和密码获得对网络的访问，所以所述用户可以使用所述第二具有网络功能的装置在该网络上访问他们的帐户。

[0060] ID 文件 140 和密码允许用户使用不同的具有网络功能的装置在相同的不同的网络上访问他们的帐户。例如，用户可以用像游戏控制台的第一具有网络功能的装置，使用 ID 文件 140 和密码来访问第一网络。用户可以用第二具有网络功能的装置，使用 ID 文件 140 和密码来访问相同的或不同的网络。第二具有网络功能的装置可以是与第一具有网络功能的装置相同类型的具有网络功能的装置或者它可以是不同类型的具有网络功能的装置。依照这种方式，用户可以使用不同的具有网络功能的装置来访问他们的帐户。

[0061] 以上是使用 ID 文件以使得许可和未经许可的具有网络功能的装置（客户端）这两者都可以访问相同的许可的服务提供者的例子。其它例子包括 1) 使用 ID 文件以使得相同的许可的具有网络功能的装置（客户端）可以访问许可和未经许可的服务提供者这两者；和 2) 使用 ID 文件以使得未经许可的具有网络功能的装置（客户端）可以访问未经许可的服务提供者。

[0062] 图 8 是用于在诸如在图 1-3 中所描述的两个具有网络功能的装置之间传输信息的实施例的流程图。流程在块 804 中开始，其中，第一具有网络功能的装置被用来使用第一具有网络功能的装置同步到网络。然后在块 806 中，由第一网络根据认证来创建 ID 文件 140。流程继续至块 808 并且 ID 文件 140 被传输到第二具有网络功能的装置。

[0063] 在块 810 中，第二具有网络功能的装置使用 ID 文件 140 来访问网络。例如，第二具有网络功能的装置可以访问与第一具有网络功能的装置所访问的网络相同的网络，或者它也可以访问不同的网络。在块 812 中，可以把文件与 ID 文件 140 相关联并且由第二具有网络功能的装置根据该网络上的活动来更新相关联的文件。例如，可以在该相关联的文件中包括标识由第二具有网络功能的装置访问的网络站点的信息或者第二具有网络功能的装置参与的活动或者其它信息，所述活动诸如购买的物品。

[0064] 在块 814 中，ID 文件 140 和相关联的文件被传输到第一具有网络功能的装置。在块 816 中，评估相关联的文件。例如，可以评估相关联的文件以确定第二具有网络功能的装置访问什么网络站点、是否购买物品或者其它类型的网络活动。

[0065] 虽然上面例子描述了两个具有网络功能的装置，但是可以使用两个以上的具有网络功能的装置。例如，第一具有网络功能的装置可以生成生 ID 文件。然后可以在第二具有网络功能的装置上使用该 ID 文件 140。ID 文件 140 可以从第二具有网络功能的装置被传输到第三具有网络功能的装置等。换句话说，用户可以把他们相关联的 ID 文件 140 传输到多个具有网络功能的装置以便由此获得使用不同的具有网络功能的装置对他们的帐户的访问。例如，用户可以把他们的 ID 文件 140 存储在记忆棒或其它可移动存储上，并且随身携带该可移动存储，使得所述用户可以使用任何可获得的具有网络功能的装置来访问他们

的帐户。

[0066] 在一个例子中，用户可以在家里的游戏控制台上使用他们的 ID 文件 140 来访问在线游戏。当离开家时，用户可以把该 ID 文件 140 传输到可移动存储设备并且随身带着该存储设备。然后用户可以使用该 ID 文件用在诸如朋友家之类的另一地点处的 PC 来访问相同的在线游戏。因为用户使用相同的 ID 文件 140，所以游戏提供者将允许用户访问他们的帐户并且所述用户可以在他们先前结束的相同点处重新进入该游戏。当用户离开他们朋友的家时，可以更新 ID 文件 140。然后用户可以把 ID 文件 140 传输到具有在线访问的他们的蜂窝电话、PDA 或其它移动设备，并且再次在相同点处重新进入该游戏。

[0067] 同样，用户可以从这些各种具有网络功能的装置访问除游戏之外他们帐户的其它特征。例如，当在线时，他们可以用他们的蜂窝电话向他们的伙伴发送消息并且让他们知道该用户何时将回到家并且回到线上。

[0068] 图 9 是图示可以结合这里所描述的各种实施例使用的示例具有网络功能的装置 950 的框图。对那些本领域技术人员来说清楚的是，可以使用其它具有网络功能的装置，诸如其它计算机或游戏控制台和 / 或体系结构。

[0069] 具有网络功能的装置 950 优选包括一个或多个处理器，诸如处理器 952。可以提供附加处理器，诸如管理输入 / 输出的辅助处理器，执行浮点数学运算的辅助处理器，具有适于快速执行信号处理算法的体系结构的特殊目的的微处理器（例如，数字信号处理器），从属于主处理系统的从处理器（例如，后端处理器），用于双或多处理器系统的附加微处理器或控制器，或者协处理器，例如如果要实现并行处理的话。这样的辅助处理器或协处理器可以是分立的处理器或者可以与处理器 1352 集成。

[0070] 处理器 952 优选连接到通信总线 954。通信总线 954 可以包括用于便于在计算机系统 950 的存储和其它外围组件之间传输信息的数据通道。通信总线 954 还可以提供用于与处理器 952 通信的信号集，包括数据总线、地址总线和控制总线（未示出）。通信总线 954 可以包括任何标准或非标准的总线体系结构，诸如像顺从工业标准体系结构（“Industry standard architecture，ISA”）的、扩展的工业标准体系结构（“extended industry standard architecture，EISA”）的、微通道体系结构（“Micro Channel Architecture，MCA”）的、外围组件互连（“peripheralcomponent interconnect，PCI”）本地总线的或由电气与电子工程师协会（“Institute of Electrical and Electronics Engineers，IEEE”）所颁布的标准的总线体系结构，所述电气与电子工程师协会所颁布的标准包括 IEEE 488 通用接口总线（“general-purpose interface bus，GPIB”）、IEEE696/S-100 等。

[0071] 具有网络功能的装置 950 优选包括主存储器 956 并且还可以包括次级存储器 958。主存储器 956 提供对在处理器 952 上执行的程序的指令和数据的存储。主存储器 956 典型地是基于半导体的存储器，诸如动态随机存取存储器（“dynamic random access memory，DRAM”）和 / 或静态随机存取存储器（“static random access memory，SRAM”）。其它基于半导体的存储器类型例如包括同步动态随机存取存储器（“synchronous dynamic random access memory，SDRAM”）、Rambus 动态随机存取存储器（“Rambus dynamic random access memory，RDRAM”）、铁电随机存取存储器（“ferroelectric random access memory，FRAM”）等，包括只读存储器（“read only memory，ROM”）。

[0072] 次级存储器 958 任选地可以包括硬盘驱动器 960 和 / 或可移动存储设备驱动器

962，例如软盘驱动器、磁带驱动器、压缩光盘（“CD”）驱动器、数字通用盘片（“DVD”）驱动器、记忆棒等。可移动存储驱动器 962 已公知的方式从可移动存储介质 964 读取和 / 或向其写入。可移动存储介质 964 例如可以是 CD、DVD、闪速驱动器、记忆棒等。

[0073] 可移动存储介质 964 优选是其上已经存储计算机可执行代码（即，软件）和 / 或数据的计算机可读介质。在可移动存储介质 964 上所存储的计算机软件或数据作为电通信信号 978 被读入到计算机系统 950 中。

[0074] 在可替换实施例中，次级存储器 958 可以包括用于允许计算机程序或其它数据或指令加载到计算机系统 950 中的其它类似装置。这样的装置例如可以包括外部存储介质 972 和接口 970。外部存储介质 972 的例子可以包括外部硬盘驱动器或外部光驱动器和 / 或外部磁光驱动器。

[0075] 次级存储器 958 的其它例子可以包括基于半导体的存储器，诸如可编程只读存储器（“PROM”）、可擦除可编程只读存储器（“EPROM”）、电可擦只读存储器（“EEPROM”）或闪速存储器（与 EEPROM 类似的按块存储器 (block oriented memory)）。还包括任何其它可移动存储单元 972 和接口 970，其允许软件和数据从可移动存储部件 972 传输到具有网络功能的装置 950。

[0076] 具有网络功能的装置 950 还可以包括通信接口 974。通信接口 974 允许软件和数据在具有网络功能的装置 950 和外部装置、网络或信息源之间进行传输。例如，计算机软件或可执行代码可以经由通信接口 974 从网络服务器传输到具有网络功能的装置 950。另外，通信接口 974 可以建立并保持到诸如因特网之类的外部网络的有线和无线这两者的通信。通信接口 974 的例子包括调制解调器、网络接口卡（“network interface card，NIC”）、通信端口、PCMCIA 插槽和卡、红外接口和 IEEE 1394 火线、无线 LAN、IEEE 802.11 接口、IEEE 802.16 接口、蓝牙接口、网状 (mesh) 网络接口，这里只给出几个。

[0077] 通信接口 974 优选实现工业颁布的协议标准，诸如以太网 IEEE 802 标准、光纤通道、数字用户线路（“DSL”）、异步数字用户线路（“ADSL”）、帧中继、异步传输模式（“ATM”）、集成数字服务网络（“ISDN”）、个人通信服务（“PC”）、传输控制协议 / 网际协议（“TCP/IP”）、串行线路网际协议 / 点到点协议（“SLIP/PPP”）等，不过还可以实现定制的或非标准的接口协议。

[0078] 经由通信接口 974 传输的软件和数据通常以电通信信号 978 的形式。这些信号 978 优选经由通信通道 980 被提供到通信接口 974。通信通道 980 携带信号 978 并且可以使用各种有线或无线通信装置来实现，所述有线或无线通信装置包括有线或电缆、光纤、常规的电话线、蜂窝式电话链路、无线数据通信链路、射频 (RF) 链路或红外链路，这里只给出几个。

[0079] 计算机可执行代码（即，计算机程序或软件）可以被存储在主存储器 956 和 / 或次级存储器 958 中。计算机程序还可以经由通信接口 974 接收并且被存储在主存储器 956 和 / 或次级存储器 958 中。这样的计算机程序当被执行时使得计算机系统 950 能够执行如前所述的本发明的各种功能。

[0080] 在此说明书中，术语“计算机可读介质”用来指用于存储数据和 / 或向具有网络功能的装置 9050 提供计算机可执行代码（例如，软件和计算机程序）的任何媒体。这些媒体的例子包括主存储器 956、次级存储器 958（包括硬盘驱动器 960，可移动存储介质 964 和外

部存储介质 972)，以及可通信地与通信接口 974 耦合的任何外围装置（包括网络信息服务器或其它网络装置）。这些计算机可读介质是用于向具有网络功能的装置 950 提供可执行代码、编程指令和软件或存储和 / 或记录数据的装置。

[0081] 在利用软件实现的实施例中，软件可以被存储在计算机可读介质上并且通过可移动存储驱动器 962、接口 970 或通信接口 974 加载到具有网络功能的装置 950 中。在这样的实施例中，软件以电通信信号 978 的形式被加载到具有网络功能的装置 950 中。所述软件当被处理器 952 执行时优选促使处理器 952 执行先前这里所描述的发明特征和功能。

[0082] 例如还可以使用诸如应用特定的集成电路（“ASIC”）或现场可编程门阵列（“FPGA”）之类的组件主要以硬件来实现各种实施例。实现能够执行这里所描述功能的硬件状态机对那些相关领域技术人员来说是显然的。还可以利用硬件和软件的组合来实现各种实施例。

[0083] 术语“模块”如这里所用意思是但不限于执行一定任务的软件或硬件组件，诸如 FPGA 或 ASIC。有利地，模块可以被配置为驻留在可寻址存储介质上以及被配置为在一个或多个具有网络功能的装置或处理器上执行。因此，举例来说，模块可以包括组件、过程、功能、属性、程序、子例程、程序代码的段、驱动程序、固件、微代码、电路、数据、数据库、数据结构、表、阵列、变量等。为在组件和模块中所提供的功能可以被组合到较少组件和模块中或者进一步被分到附加的组件和模块中。另外，有利地可以实现组件和模块以在一个或多个具有网络功能的装置或计算机上执行。

[0084] 此外，那些本领域技术人员应当理解，结合上述附图所描述的各种说明性逻辑块、模块、电路和方法步骤以及这里所公开的实施例常常可以作为电子硬件、计算机软件或二者的组合来实现。为了清楚地图示硬件和软件的这种互换性，上面已经按照它们的功能总体上描述了各种说明性组件、块、模块、电路和步骤。这种功能是被实现为硬件还是软件取决于在整个系统上所采取的特定应用和设计约束。技术人员对于每个特定应用可以以可变方式来实现所描述的功能，但是这样的实现决定不应当被解释为引起来对本发明的范围的脱离。另外，对在模块、块、电路或步骤内的功能进行分组是为了便于描述。在不脱离本发明的情况下，特定功能或步骤可以从一个模块、块或电路移动到另一个。

[0085] 此外，结合这里所公开的实施例描述的各种说明性逻辑块、模块和方法可以用被设计成用于执行这里所描述功能的通用处理器、数字信号处理器（“DSP”）、ASIC、FPGA 或其它可编程逻辑器件、分立的门或晶体管逻辑、分立的硬件组件或其任何组合来实现或执行。通用处理器可以是微处理器，但是作为选择，所述处理器可以是任何处理器、控制器、微控制器或状态机。处理器也可以被实现为计算装置的组合，例如 DSP 和微处理器、多个微处理器、结合 DSP 核的一个或多个微处理器的组合或任何其它这样的配置。

[0086] 另外，结合这里所公开的实施例所描述的方法或算法的步骤可以直接用硬件、由处理器执行的软件模块或这两者的组合来体现。软件模块可以驻留于 RAM 存储器、闪速存储器、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动盘、CD-ROM 或包括网络存储介质在内的任何其它形式的存储介质。示例性存储介质可以被耦合到处理器，以致所述处理器可以从该存储介质读取信息以及向该存储介质写入信息。在可替换方式中，存储介质可以集成到所述处理器。所述处理器和存储介质还可以驻留于 ASIC 中。

[0087] 虽然上面是本发明优选实施例的完整描述，但是使用各种可替换方式、修改和等

效方式是可能的。因此，应当不是参考以上描述而是作为替代应当参考所附权利要求连同他们完全的等效范围来确定本发明的范围。这里所描述的无论是否优选的任何特征都可以与这里所描述的无论是否优选的任何其它特征组合。从而，本发明并不旨在局限于这里所示出的实施例，而是应当符合与这里所公开的原理和新颖特征抑制的最宽范围。

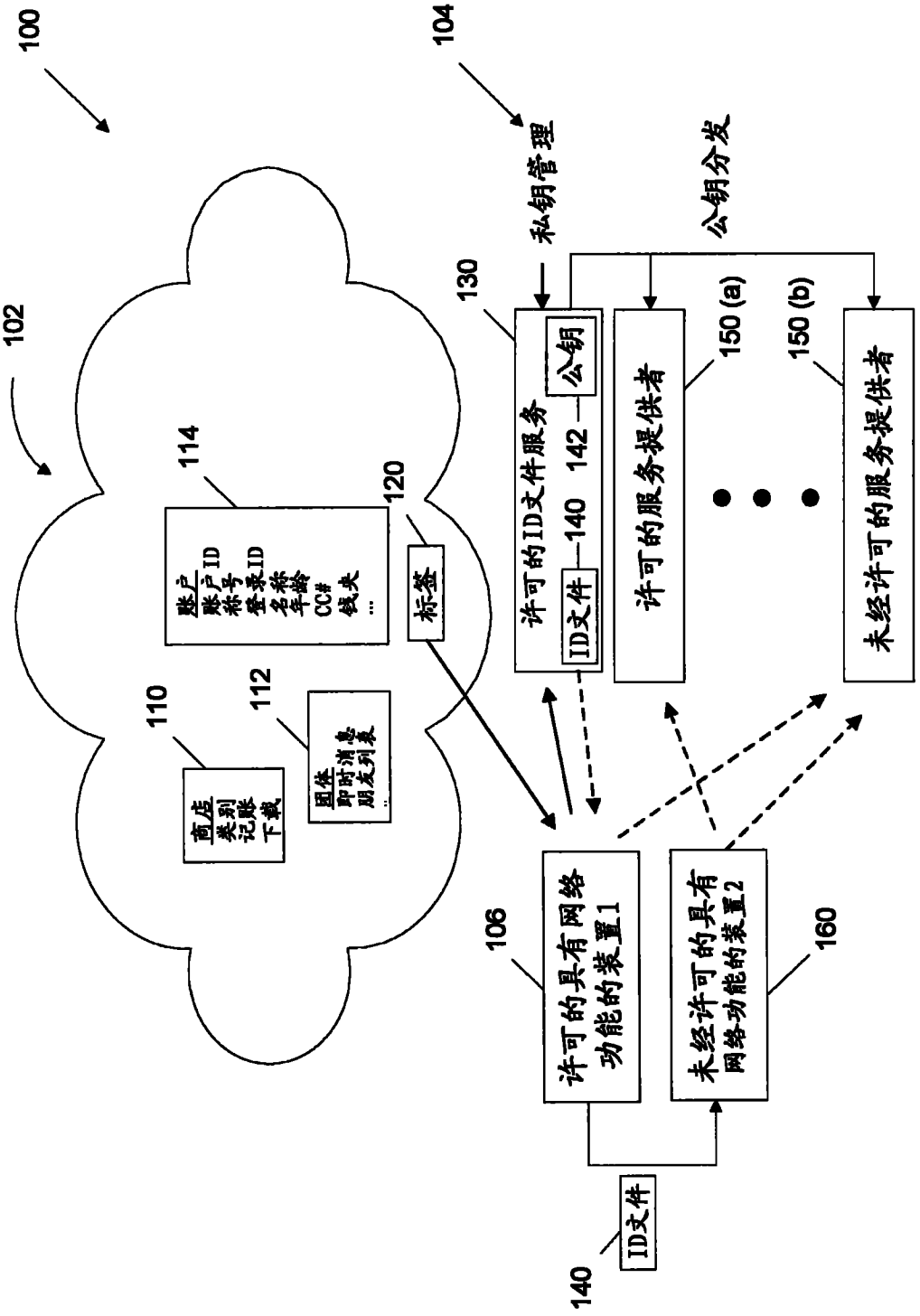

100
102
104
私钥管理
公钥分发
130
许可的ID文件服务
公钥
142
ID文件
140
150 (a)
150 (b)
许可的服务提供者
未经许可的服务提供者
114
账户
账户ID
登录ID
名称
年龄
CC#
钱夹
...
120
标签
110
商店
类到
记账
下载
112
即时消息
朋友到友
...
106
许可的具有网络
功能的装置1
160
未经许可的具有
网络功能的装置2
140
ID文件

图 1

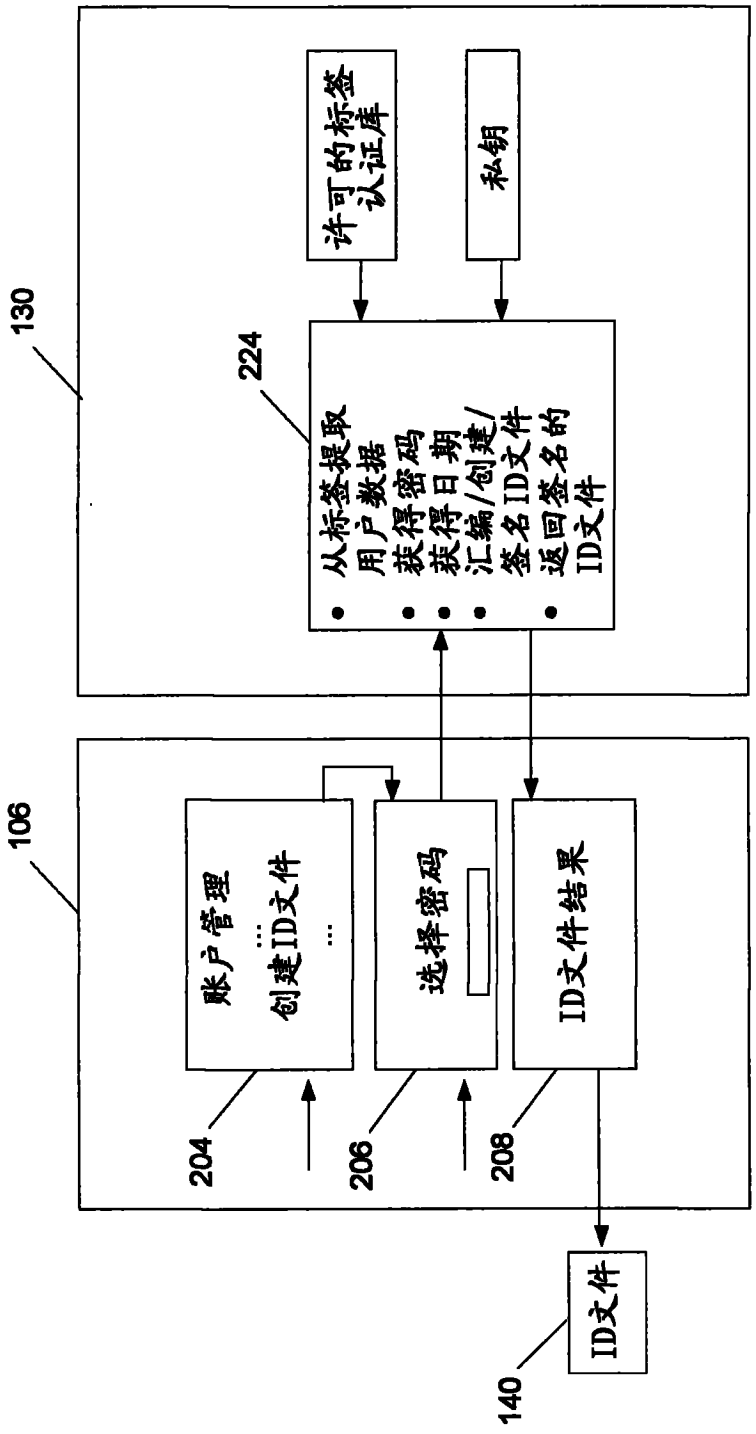

130
224
许可的标签认证库
私钥
从标签提取用户数据
获得密码
获得日期
汇编/创建/签名ID文件
返回签名的ID文件
106
账户管理
...
创建ID文件
...
选择密码
ID文件结果
204
206
208
ID文件
140

图 2

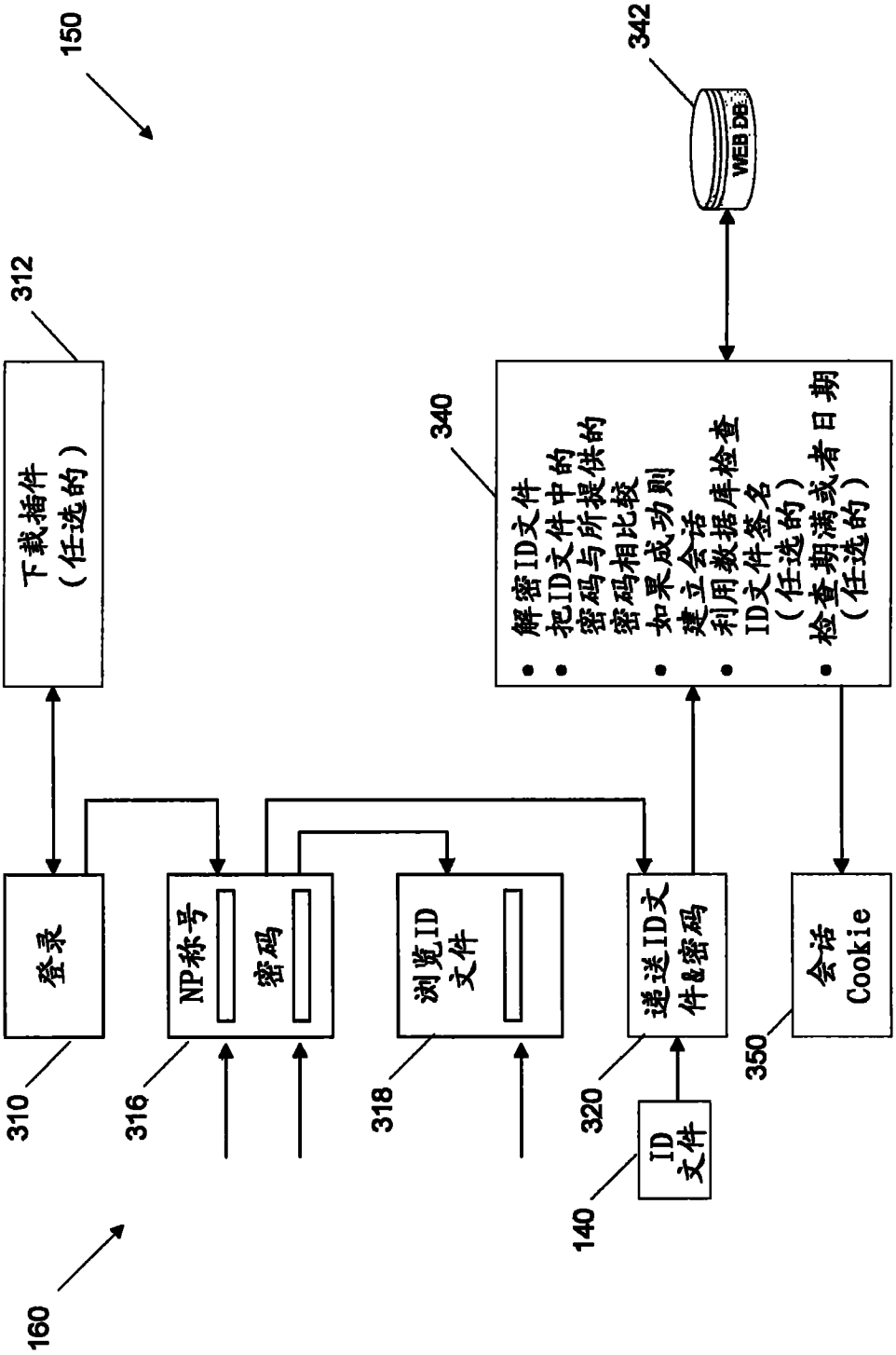

150
342
WEB DB
312
下载插件
（任选的）
340
• 解密ID文件
• 把ID文件中的
密码与所提供的
密码相比较
• 如果成功则
建立会话
• 利用数据库检查
ID文件签名
（任选的）
• 检查期满或者日期
（任选的）
登录
NP称号
密码
浏览ID
文件
递送ID文
件&密码
会话
Cookie
310
316
318
320
350
ID
文件
140
160

图 3

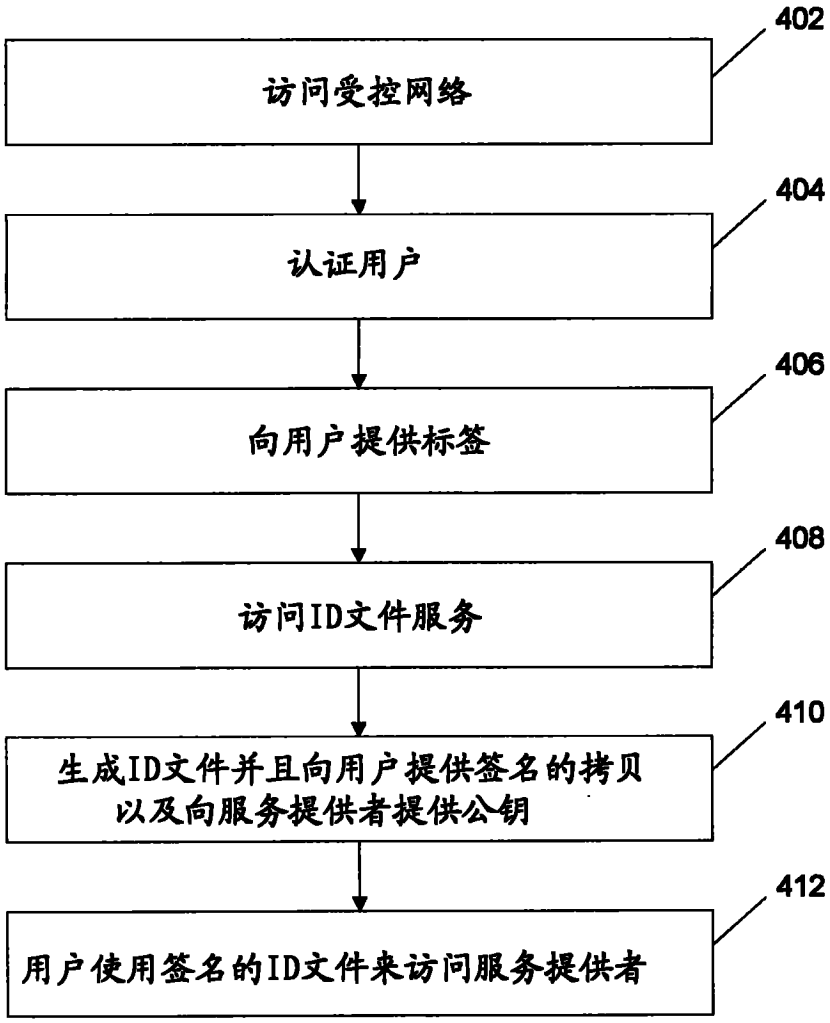

402
访问受控网络
404
认证用户
406
向用户提供标签
408
访问ID文件服务
410
生成ID文件并且向用户提供签名的拷贝
以及向服务提供者提供公钥
412
用户使用签名的ID文件来访问服务提供者

图 4

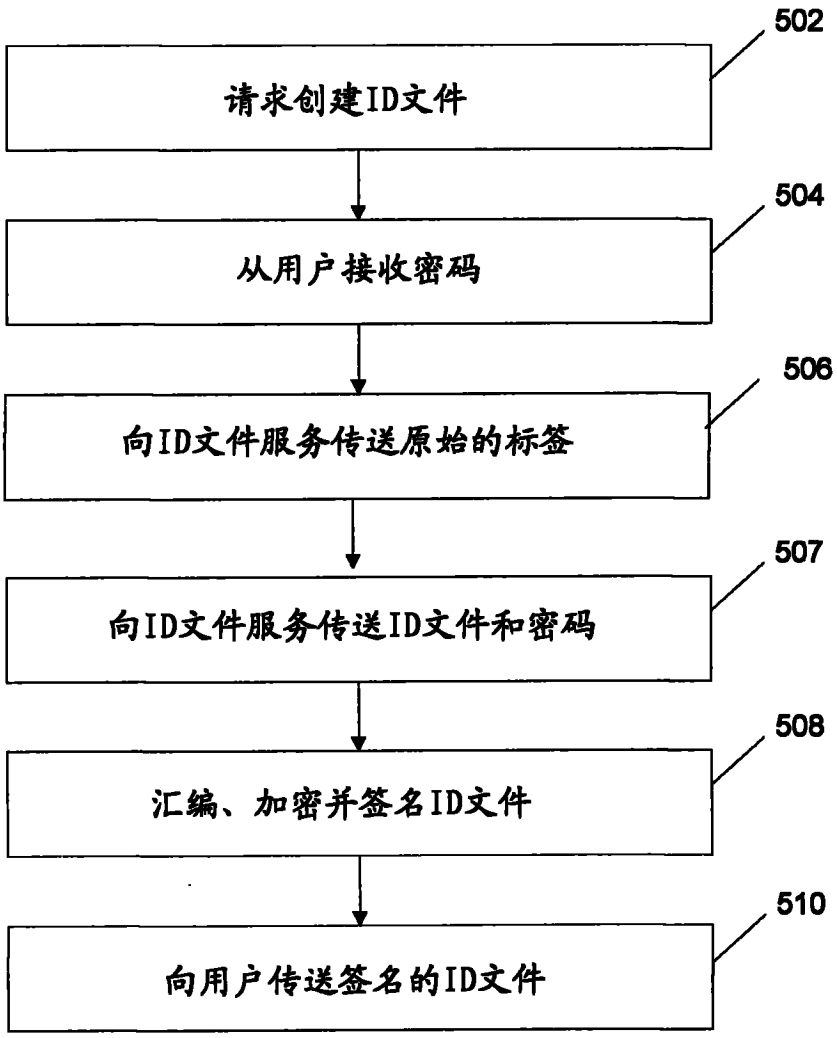

502
请求创建ID文件
504
从用户接收密码
506
向ID文件服务传送原始的标签
507
向ID文件服务传送ID文件和密码
508
汇编、加密并签名ID文件
510
向用户传送签名的ID文件

图 5

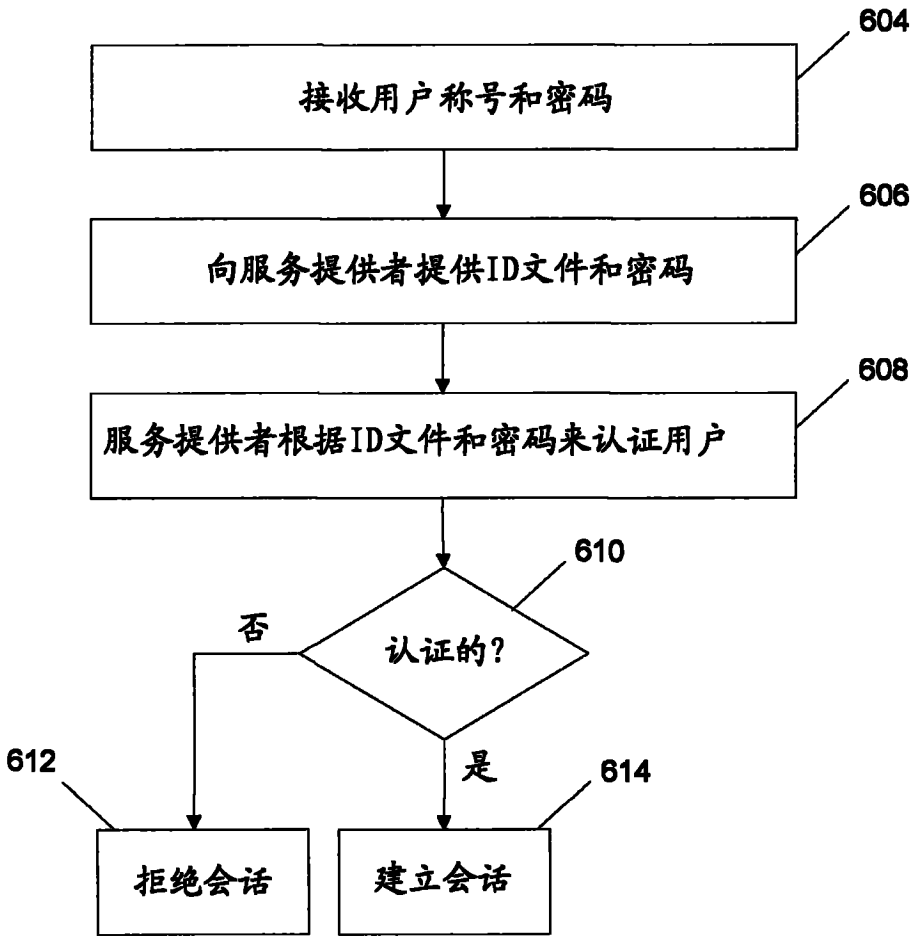

604
接收用户称号和密码
606
向服务提供者提供ID文件和密码
608
服务提供者根据ID文件和密码来认证用户
610
认证的?
否
是
612
拒绝会话
614
建立会话

图 6

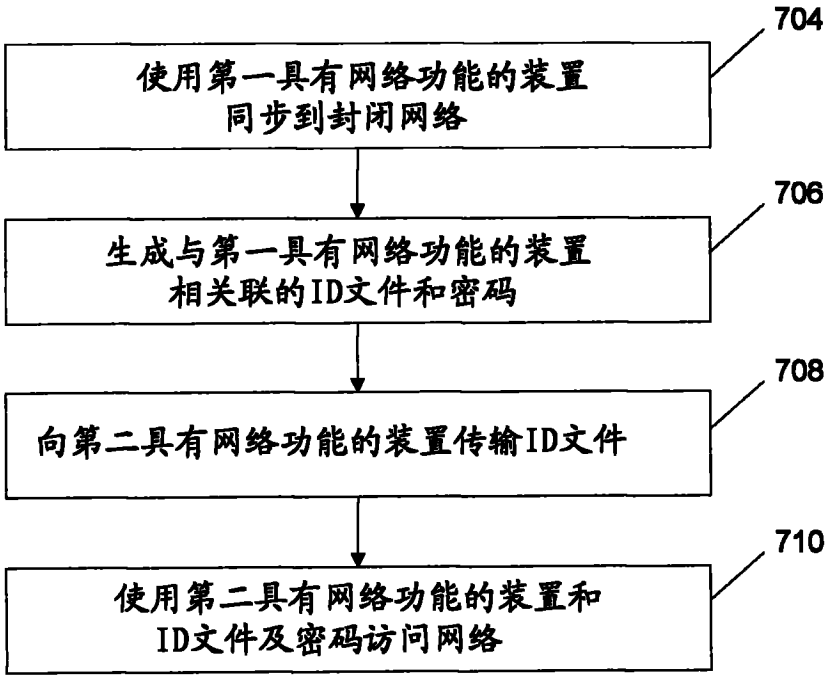

704
使用第一具有网络功能的装置
同步到封闭网络
706
生成与第一具有网络功能的装置
相关联的ID文件和密码
708
向第二具有网络功能的装置传输ID文件
710
使用第二具有网络功能的装置和
ID文件及密码访问网络

图 7

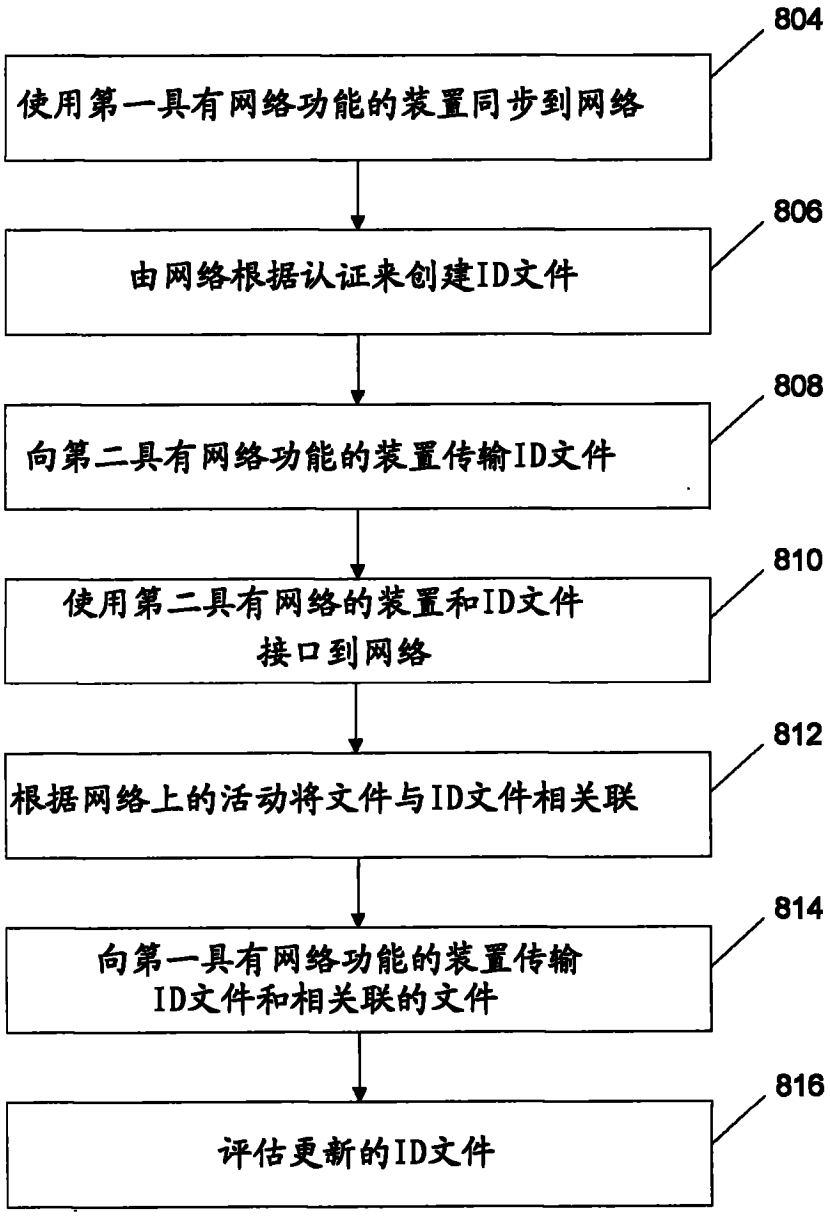

804
使用第一具有网络功能的装置同步到网络
806
由网络根据认证来创建ID文件
808
向第二具有网络功能的装置传输ID文件
810
使用第二具有网络的装置和ID文件
接口到网络
812
根据网络上的活动将文件与ID文件相关联
814
向第一具有网络功能的装置传输
ID文件和相关联的文件
816
评估更新的ID文件

图 8

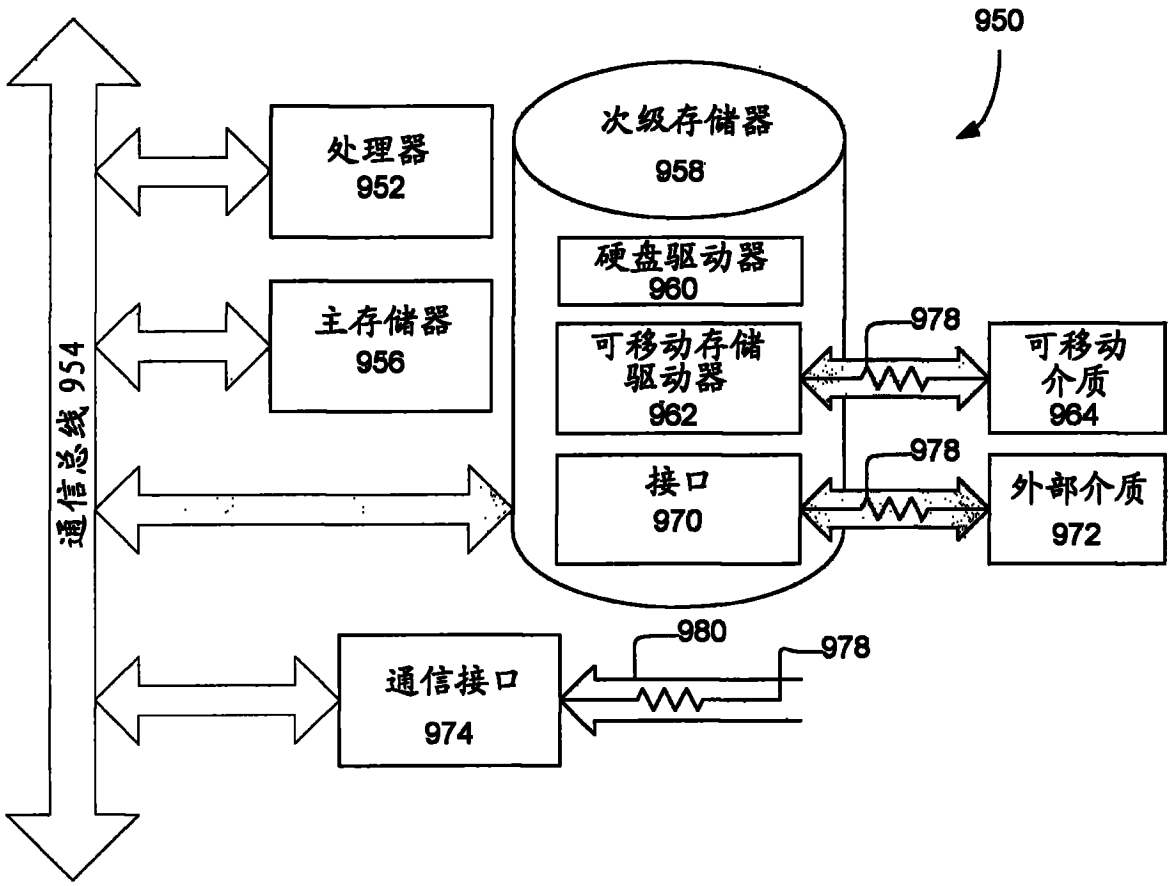

950
处理器
952
主存储器
956
通信总线 954
次级存储器
958
硬盘驱动器
960
可移动存储
驱动器
962
接口
970
978
可移动
介质
964
978
外部介质
972
980
978
通信接口
974

图 9