(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105743883 A
(43)申请公布日 2016.07.06

(21)申请号 201610041947.6

(22)申请日 2016.01.21

(71)申请人 兴唐通信科技有限公司
地址 100191 北京市海淀区学院路40号

(72)发明人 吴江 张知恒 王俊峰 程福兴 王萌希

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 李相雨

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

权利要求书2页 说明书11页 附图2页

(54)发明名称

一种网络应用的身份属性获取方法及装置

(57)摘要

本发明提供的一种网络应用的身份属性获取方法及装置，涉及身份属性获取领域，其中所述方法包括，接收所述网络终端反馈的身份管理参数，将所述身份管理参数转发至所述网络身份基础信息服务器，以使所述网络身份基础信息服务器查找与所述身份管理参数对应的用户身份属性信息，并反馈所述用户身份属性信息；接收所述网络身份基础信息服务器反馈的用户身份属性信息，并将所述用户身份属性信息转发至所述网络应用服务器，以使所述网络应用服务器实现用户身份属性的获取。本发明提供的网络应用身份属性获取方法通过网络身份基础信息服务器获取网络用户的现实身份属性信息，提供了权威的身份属性断言参考。

CN 105743883 A

1.一种网络应用的身份属性获取方法,其特征在于,包括:

接收所述网络终端反馈的身份管理参数,将所述身份管理参数转发至所述网络身份基础信息服务器,以使所述网络身份基础信息服务器查找与所述身份管理参数对应的用户身份属性信息,并反馈所述用户身份属性信息;

接收所述网络身份基础信息服务器反馈的用户身份属性信息,并将所述用户身份属性信息转发至所述网络应用服务器,以使所述网络应用服务器实现用户身份属性的获取。

2.根据权利要求1所述的方法,其特征在于,在所述接收所述网络终端反馈的身份管理参数步骤之前,所述方法还包括:

在接收到网络应用服务器发送的请求身份属性指令时,向网络终端发送读取指令,以使所述网络终端读取用户身份证对应的身份管理参数,并反馈所述身份管理参数。

3.根据权利要求1所述的方法,其特征在于,所述身份管理参数包括:芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个;

或者

所述身份管理参数包括:芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个经过运算处理以后的值。

4.根据权利要求2所述的方法,其特征在于,所述在接收到网络应用服务器发送的请求身份属性指令时,向网络终端发送读取指令,以使所述网络终端读取用户身份证对应的身份管理参数,并反馈所述身份管理参数,接收所述网络终端反馈的身份管理参数,具体包括:

在接收到网络应用服务器发送的请求身份属性指令时,向网络终端发送挑战码和读取指令,以使所述网络终端读取用户身份证对所述挑战码应答的挑战结果和用户身份证对应的身份管理参数,并反馈所述挑战结果和身份管理参数;

接收所述网络终端反馈的挑战结果和身份管理参数,对所述挑战结果和身份管理参数进行核验,在核验通过时,执行所述将所述身份管理参数转发至所述网络身份基础信息服务器的步骤。

5.根据权利要求1-4任一项所述的方法,其特征在于,所述在接收到网络应用服务器发送的请求身份属性指令时之前,所述方法还包括:

获取用户输入的个人识别口令,将所述个人识别口令与预设口令库进行匹配核验,在匹配值为真时,执行所述在接收到网络应用服务器发送的请求身份属性指令时的步骤;

或

所述将所述身份管理参数转发至所述网络身份基础信息服务器之前,所述方法还包括:

获取用户输入的指纹信息,将所述指纹信息与在预设指纹库中查找到和所述身份管理参数相对应的指纹信息进行匹配核验,在匹配值为真时,执行所述在接收到网络应用服务器发送的请求身份属性指令时的步骤。

6.一种网络应用的身份属性获取装置,其特征在于,包括:

接收单元,用于接收所述网络终端反馈的身份管理参数,将所述身份管理参数转发至所述网络身份基础信息服务器,以使所述网络身份基础信息服务器查找与所述身份管理参数对应的用户身份属性信息,并反馈所述用户身份属性信息;

转发单元，用于接收所述网络身份基础信息服务器反馈的用户身份属性信息，并将所述用户身份属性信息转发至所述网络应用服务器，以使所述网络应用服务器实现用户身份属性的获取。

7.根据权利要求6所述的装置，其特征在于，所述装置还包括：

发送单元，用于在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送读取指令，以使所述网络终端读取用户身份证对应的身份管理参数，并反馈所述身份管理参数。

8.根据权利要求6所述的装置，其特征在于，所述身份管理参数包括：芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个；

或者

所述身份管理参数包括：芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个经过运算处理以后的值。

9.根据权利要求7所述的装置，其特征在于，所述发送单元，具体用于在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送挑战码和读取指令，以使所述网络终端读取用户身份证对所述挑战码应答的挑战结果和用户身份证对应的身份管理参数，并反馈所述挑战结果和身份管理参数；

所述接收单元，具体用于接收所述网络终端反馈的挑战结果和身份管理参数，对所述挑战结果和身份管理参数进行核验，在核验通过时，将所述身份管理参数转发至所述网络身份基础信息服务器，以使所述网络身份基础信息服务器查找与所述身份管理参数对应的用户身份属性信息，并反馈所述用户身份属性信息。

10.根据权利要求6-9任一项所述的装置，其特征在于，所述装置还包括：

第一匹配单元，用于获取用户输入的个人识别口令，将所述个人识别口令与预设口令库进行匹配核验，在匹配值为真时，调用所述转发单元；

或

第二匹配单元，用于获取用户输入的指纹信息，将所述指纹信息与预设指纹库进行匹配核验，在匹配值为真时，调用所述转发单元。

一种网络应用的身份属性获取方法及装置

技术领域

[0001] 本发明涉及身份属性获取领域，尤其涉及一种网络应用的身份属性获取方法及装置。

背景技术

[0002] 当今社会网络已经渗入到我们生活的方方面面，我们可以在网络空间中开展社团组织、交友沟通、电子交易等活动，也能借助网络进行生产、学习、交易的互动。尽管借助网络，提高了生产率、开发了新平台、创建了商务场所，但是在快速发展中出现了由于身份隐私泄露造成的大量网络威胁，如网络账户虚拟财富被盗、交易篡改、网络欺诈、以及隐私泄露造成的其他权益受损事件不断增加。这些网络威胁难于治理的重要原因是网络空间的身份应用和隐私保护之利弊难于平衡。

[0003] 目前的网络空间用户身份信息管理依赖于网络身份供应商。网络身份供应商通常也是网络应用提供商，它负责用户网络身份标识的注册、管理、使用等。用户的身份信息安全完全由网络身份供应商保障，用户本人无法监督，政府无法监管，导致用户信息泄露、身份冒充等网络安全事故频发。

[0004] 现有的身份属性获取技术和方法多种多样，比如以“知道什么”的方式来进行身份属性获取，包括“用户账号+口令”方式、“问答式”等，也有些以“拥有什么”的方式来进行身份属性获取，包括“动态短信验证码”来验证手机号码的拥有权等方法。这些身份属性获取技术和方法在用于映射用户网络身份与现实身份时都需要在网络上传输真实的身份证号码，存在着身份隐私泄露的风险。

发明内容

[0005] 针对现有技术的缺陷，本发明提出了解决上述技术问题的一种网络应用的身份属性获取方法及装置，实现获取网络用户的现实身份属性信息的权威断言。

[0006] 第一方面，本发明提供一种网络应用的身份属性获取方法，包括：

[0007] 接收所述网络终端反馈的身份管理参数，将所述身份管理参数转发至所述网络身份基础信息服务器，以使所述网络身份基础信息服务器查找与所述身份管理参数对应的用户身份属性信息，并反馈所述用户身份属性信息；

[0008] 接收所述网络身份基础信息服务器反馈的用户身份属性信息，并将所述用户身份属性信息转发至所述网络应用服务器，以使所述网络应用服务器实现用户身份属性的获取。

[0009] 优选的，在所述接收所述网络终端反馈的身份管理参数步骤之前，所述方法还包括：

[0010] 在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送读取指令，以使所述网络终端读取用户身份证对应的身份管理参数，并反馈所述身份管理参数。

[0011] 优选的，所述身份管理参数包括：芯片厂商管理号、芯片序列号和身份证卡序列号

中的至少一个；

[0012] 或者

[0013] 所述身份管理参数包括：芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个经过运算处理以后的值。

[0014] 优选的，所述在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送读取指令，以使所述网络终端读取用户身份证对应的身份管理参数，并反馈所述身份管理参数，接收所述网络终端反馈的身份管理参数，具体包括：

[0015] 在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送挑战码和读取指令，以使所述网络终端读取用户身份证对所述挑战码应答的挑战结果和用户身份证对应的身份管理参数，并反馈所述挑战结果和身份管理参数；

[0016] 接收所述网络终端反馈的挑战结果和身份管理参数，对所述挑战结果和身份管理参数进行核验，在核验通过时，执行所述将所述身份管理参数转发至所述网络身份基础信息服务器的步骤。

[0017] 优选的，所述在接收到网络应用服务器发送的请求身份属性指令时之前，所述方法还包括：

[0018] 获取用户输入的个人识别口令，将所述个人识别口令与预设口令库进行匹配核验，在匹配值为真时，执行所述在接收到网络应用服务器发送的请求身份属性指令时的步骤；

[0019] 或

[0020] 所述将所述身份管理参数转发至所述网络身份基础信息服务器之前，所述方法还包括：

[0021] 获取用户输入的指纹信息，将所述指纹信息与在预设指纹库中查找到和所述身份管理参数相对应的指纹信息进行匹配核验，在匹配值为真时，执行所述在接收到网络应用服务器发送的请求身份属性指令时的步骤。

[0022] 第二方面，本发明提供一种网络应用的身份属性获取装置，包括：

[0023] 接收单元，用于接收所述网络终端反馈的身份管理参数，将所述身份管理参数转发至所述网络身份基础信息服务器，以使所述网络身份基础信息服务器查找与所述身份管理参数对应的用户身份属性信息，并反馈所述用户身份属性信息；

[0024] 转发单元，用于接收所述网络身份基础信息服务器反馈的用户身份属性信息，并将所述用户身份属性信息转发至所述网络应用服务器，以使所述网络应用服务器实现用户身份属性的获取。

[0025] 优选的，所述装置还包括：

[0026] 发送单元，用于在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送读取指令，以使所述网络终端读取用户身份证对应的身份管理参数，并反馈所述身份管理参数。

[0027] 优选的，所述身份管理参数包括：芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个，

[0028] 或者

[0029] 所述身份管理参数包括：芯片厂商管理号、芯片序列号和身份证卡序列号中的至

少一个经过运算处理以后的值。

[0030] 优选的，所述发送单元，具体用于在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送挑战码和读取指令，以使所述网络终端读取用户身份证对所述挑战码应答的挑战结果和用户身份证对应的身份管理参数，并反馈所述挑战结果和身份管理参数；

[0031] 所述接收单元，具体用于接收所述网络终端反馈的挑战结果和身份管理参数，对所述挑战结果和身份管理参数进行核验，在核验通过时，将所述身份管理参数转发至所述网络身份基础信息服务器，以使所述网络身份基础信息服务器查找与所述身份管理参数对应的用户身份属性信息，并反馈所述用户身份属性信息。

[0032] 优选的，其特征在于，所述装置还包括：

[0033] 第一匹配单元，用于获取用户输入的个人识别口令，将所述个人识别口令与预设口令库进行匹配核验，在匹配值为真时，调用所述转发单元；

[0034] 或

[0035] 第二匹配单元，用于获取用户输入的指纹信息，将所述指纹信息与预设指纹库进行匹配核验，在匹配值为真时，调用所述转发单元。

[0036] 由上述技术方案可知，本发明提供的一种网络应用的身份属性获取方法及装置，通过接收将网络终端反馈回来的身份管理参数发送至网络身份基础信息服务器，网络身份基础信息服务器在信息库中查找到与接收到的身份管理参数对应的用户身份属性信息，从而得出用户身份属性证明断言。本发明提供的网络应用身份属性获取方法通过网络身份基础信息服务器获取网络用户的现实身份属性信息，可提供权威、隐私安全的身份属性断言。

附图说明

[0037] 图1为本发明一实施例提供的网络应用的身份属性获取方法的流程示意图；

[0038] 图2为本发明一实施例提供的网络应用的身份属性获取装置的结构示意图；

[0039] 图3示出了本发明一实施例提供的网络应用的身份属性获取系统的结构示意图；

[0040] 图4示为本发明一实施例提供的网络应用的身份属性获取系统的工作流程图。

具体实施方式

[0041] 下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述。以下实施例用于说明本发明，但不用来限制本发明的范围。

[0042] 图1示出了本发明一实施例提供的网络应用的身份属性获取方法的流程示意图，如图1所示，本实施例的网络应用的身份属性获取方法如下所述。

[0043] 101、接收所述网络终端反馈的身份管理参数，将所述身份管理参数转发至所述网络身份基础信息服务器，以使所述网络身份基础信息服务器查找与所述身份管理参数对应的用户身份属性信息，并反馈所述用户身份属性信息。

[0044] 网络身份基础信息服务器是网络空间中的权威身份服务设施，是提供公共身份服务的基础设施。网络身份基础信息服务器包含身份证信息库和国家人口信息资源库以及其它个人身份信息权威数据库，如：逃犯信息库，个人信用信息库等，此外网络身份基础信息服务器还提供网络身份映射服务，以及提供权威的身份/属性断言。

[0045] 102、接收所述网络身份基础信息服务器反馈的用户身份属性信息，并将所述用户身份属性信息转发至所述网络应用服务器，以使所述网络应用服务器实现用户身份属性的获取。

[0046] 网络应用服务器依据该断言确定为网络用户提供相应的应用服务。网络应用服务器可通过安全网站或安全邮件等安全渠道获得最新的网络身份提供服务器名单。

[0047] 上述方法提供的网络应用身份属性获取方法通过网络身份基础信息服务器获取网络用户的现实身份属性信息，提供了权威的身份属性断言参考。

[0048] 在本发明的一个优选的实施例中，在所述接收所述网络终端反馈的身份管理参数步骤之前，所述方法还包括：

[0049] 在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送读取指令，以使所述网络终端读取用户身份证对应的身份管理参数，并反馈所述身份管理参数。

[0050] 可以理解的是，用户身份证是存储有个人身份数字信息的第二代居民身份证卡。

[0051] 网络终端是由连接于网络的终端设备和用于网络身份属性获取的网络身份证阅读设备组成。网络终端中的连接网络的终端设备包括但不局限于PC机、平板pad、智能手机、专用定制终端。

[0052] 网络应用服务器在网络空间中提供丰富业务的具体应用，每个网络应用服务器独立管理用户在应用中的账户，但不管理用户的真实身份。当用户访问网络应用时，发出请求身份属性指令；

[0053] 在接收到请求身份属性指令后，将请求身份属性指令发送给网络终端，网络终端会提示用户刷身份证；网络终端接收用户的身份证对应的身份管理参数，并反馈接收到的身份管理参数。

[0054] 上述方法将基于网络空间的身份证认证过程和身份属性获取结合起来，在获取网络应用身份属性过程中不需要传输用户身份证号，保证了用户身份信息的安全，避免了因网络应用提供商的身份属性获取可信度低，用户隐私泄露的风险，通过网络身份基础信息服务器获取网络用户的现实身份属性信息。提高了获取的网络空间身份属性的权威性。

[0055] 在本发明的一个优选的实施例中，所述参数信息包括：芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个；

[0056] 或者

[0057] 所述身份管理参数包括：芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个经过运算处理以后的值。

[0058] 居民身份证属于智能卡的一种，该智能卡存储一组可以自由读取但不可更改的、具有唯一性的号码，包括芯片厂商管理号、芯片序列号、身份证卡序列号，这组号码组合在一起可称为身份管理参数。更进一步的，身份管理参数还可以是由上述参数经过数学运算或者其他算法进行处理以后的某一个特定的值。

[0059] 上述方法通过传输芯片厂商管理号、芯片序列号和身份证卡序列号信息中的至少一个；

[0060] 或者

[0061] 所述身份管理参数包括：芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个经过运算处理以后的值，增强了用户隐私的安全性。

[0062] 在本发明的一个优选的实施例中，所述在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送读取指令，以使所述网络终端读取用户身份证对应的身份管理参数，并反馈所述身份管理参数，接收所述网络终端反馈的身份管理参数，具体包括：

[0063] 在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送挑战码和读取指令，以使所述网络终端读取用户身份证对所述挑战码应答的挑战结果和用户身份证对应的身份管理参数，并反馈所述挑战结果和身份管理参数；

[0064] 接收所述网络终端反馈的挑战结果和身份管理参数，对所述挑战结果和身份管理参数进行核验，在核验通过时，执行所述将所述身份管理参数转发至所述网络身份基础信息服务器的步骤。

[0065] 可以理解的是，由于非现场的身份属性获取过程中，数据经由网络传输，网络安全直接关系到身份属性获取结果。因此，每次身份属性获取过程中网络身份提供服务器发送的挑战码是唯一的且不可预测，采用先前截获的应答码进行重放攻击不可行。

[0066] 网络终端上用于网络身份属性获取的身份证阅读器支持在网络终端设备上安装的安全插件，在获取身份属性的交互过程中，读取身份证与身份证验证服务器之间的挑战码、挑战结果、以及读取网络用户身份管理参数。连接终端设备的身份证阅读器对读取的信息可自动进行加密保护，且在网络终端与网络身份提供服务器的身份验证服务器进行通信时也必须经安全传输通道。

[0067] 网络终端的网络身份证阅读器仅包含射频读取和信息加密模块，不包含验证身份证的专用身份证安全访问设备。

[0068] 身份证验证服务设备作为身份证安全访问设备实现身份证安全访问的最小限度功能，仅实现对身份证的真伪鉴别和产生读取身份管理参数的指令及接收外部的指令。

[0069] 上述方法基于居民身份证管理号的网络应用的身份属性获取方法具有网络通信安全的特点。每次认证中网络身份提供子系统发送的挑战码是唯一的且不可预测，采用先前截获的应答码进行重放攻击不可行。克服了互联网环境下身份证阅读终端暴露在不受控环境，服务端与终端信道可能不安全。这种身份属性获取过程不仅能提供权威的网络空间身份属性获取，还能避免身份信息在网络空间的传播从而保护用户隐私。

[0070] 在本发明的一个优选的实施例中，所述在接收到网络应用服务器发送的请求身份属性指令时之前，所述方法还包括：

[0071] 获取用户输入的个人识别口令，将所述个人识别口令与预设口令库进行匹配核验，在匹配值为真时，执行所述在接收到网络应用服务器发送的请求身份属性指令时的步骤；

[0072] 或

[0073] 所述将所述身份管理参数转发至所述网络身份基础信息服务器之前，所述方法还包括：

[0074] 获取用户输入的指纹信息，将所述指纹信息与在预设指纹库中查找到和所述身份管理参数相对应的指纹信息进行匹配核验，在匹配值为真时，执行所述在接收到网络应用服务器发送的请求身份属性指令时的步骤。

[0075] 可以理解的是，由于网络环境下的身份证验证过程受网络环境影响，对信息机密性、完整性、可用性、不可抵赖性等的网络攻击有可能破坏基于居民身份号的身份证验证的

过程。本实施例中，针对现实使用环境中存在身份证冒用、网络欺诈的安全问题提出相应的解决方法，实现以密码技术为基础的网络通信，为了保障信息机密性、可用性、完整性和不可抵赖性，为居民身份证网络应用增设口令，在网络上使用身份证时可要求口令验证。该方法需要公安机关或相关职能部门提供网络空间管理的服务，包括身份证在网络空间应用的支撑管理和服务系统。具体方法如下：

[0076] (1)网络用户持第二代居民身份证到就近派出所申请开通身份证网络空间身份证真伪验证功能；

[0077] (2)网络用户激活身份证网络空间身份证认证功能，网络用户通过身份代理软件和网络身份证阅读器提交身份信息和激活码，权威的网络身份提供服务器(一般是公安部门的网络身份提供服务器)鉴别网络用户身份后设置口令并录入预设口令库；

[0078] (3)网络用户使用身份证进行网络空间的身份证认证时，在读取身份证信息前要求用户输入个人识别口令，当用户输入的个人识别口令与预设口令库能够匹配时，返回匹配值为真，说明持有身份证的用户和该身份证所对应的用户是同一个，保证了人证的同一性。

[0079] 或者

[0080] 利用用户指纹信息对用户进行同一性验证，获取用户输入的指纹信息，将所述指纹信息与在预设指纹库中查找到和所述身份管理参数相对应的指纹信息进行匹配核验，在匹配值为真时，说明输入指纹信息的用户与预设指纹库中的用户是同一个用户。

[0081] 具体的，方法如下：

[0082] (1)连接在网络终端上的网络身份证阅读器采集网络用户指纹信息；

[0083] (2)网络终端将采集的指纹信息加密后录入预设指纹库；

[0084] (3)接收用户输入的指纹信息，通过比对接收的网络用户指纹信息和依据身份管理参数查询到的权威数据库中的指纹信息，当用户输入的指纹信息与依据身份管理参数查询到的权威数据库中的指纹信息能够匹配时，返回匹配值为真，说明持有身份证的用户和该身份证所对应的用户是同一个，保证了人证的同一性。

[0085] 上述方法解决了在进行身份证验证的过程中会遇到身份证冒用问题，实现了对人证同一性的严苛验证，解决非现场模式下的人证同一性认证难题。

[0086] 图2示出了本发明一实施例提供的网络应用的身份属性获取装置的结构示意图，如图2所示，本实施例的网络应用的身份属性获取装置包括：

[0087] 接收单元21，用于接收所述网络终端反馈的身份管理参数，将所述身份管理参数转发至所述网络身份基础信息服务器，以使所述网络身份基础信息服务器查找与所述身份管理参数对应的用户身份属性信息，并反馈所述用户身份属性信息；

[0088] 转发单元22，用于接收所述网络身份基础信息服务器反馈的用户身份属性信息，并将所述用户身份属性信息转发至所述网络应用服务器，以使所述网络应用服务器实现用户身份属性的获取。

[0089] 在本发明的一个优选的实施例中，所述装置还包括图2未示出的：

[0090] 发送单元23，用于在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送读取指令，以使所述网络终端读取用户身份证对应的身份管理参数，并反馈所述身份管理参数。

[0091] 在本发明的一个优选的实施例中，所述身份管理参数包括：芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个；

[0092] 或者

[0093] 所述身份管理参数包括：芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个经过运算处理以后的值。

[0094] 在本发明的一个优选的实施例中，所述发送单元23，具体用于在接收到网络应用服务器发送的请求身份属性指令时，向网络终端发送挑战码和读取指令，以使所述网络终端读取用户身份证对所述挑战码应答的挑战结果和用户身份证对应的身份管理参数，并反馈所述挑战结果和身份管理参数；

[0095] 所述接收单元21，具体用于接收所述网络终端反馈的挑战结果和身份管理参数，对所述挑战结果和身份管理参数进行核验，在核验通过时，将所述身份管理参数转发至所述网络身份基础信息服务器，以使所述网络身份基础信息服务器查找与所述身份管理参数对应的用户身份属性信息，并反馈所述用户身份属性信息。

[0096] 在本发明的一个优选的实施例中，所述装置还包括图2未示出的：

[0097] 第一匹配单元24，用于获取用户输入的个人识别口令，将所述个人识别口令与预设口令库进行匹配核验，在匹配值为真时，调用所述转发单元；

[0098] 或

[0099] 第二匹配单元25，用于获取用户输入的指纹信息，将所述指纹信息与预设指纹库进行匹配核验，在匹配值为真时，调用所述转发单元。在本实施例的另一个可实现的实施方式中，所述身份管理参数包括：芯片厂商管理号、芯片序列号和身份证卡序列号中的至少一个。更进一步的，身份管理参数还可以是由上述参数经过数学运算或者其他算法进行处理以后的某一个特定的值。

[0100] 上述装置克服了目前网络空间身份属性获取的权威性不足，网络应用提供商的身份属性获取可信度低，用户隐私泄露风险高，及身份证的当前机读模式不适合直接接入网络等现状，设计了一种有效的具有法律权威的、可用于网络空间多种角色系统的身份属性获取系统及方法，以支持对网络空间的包括对身份属性断言进行证明在内的多样化身份属性获取需求。同时，上述装置还实现了具有个人隐私安全保护、身份属性获取结果法律认可、身份证验证安全访问专用设备得到保护的效果。

[0101] 另外，根据本发明提供的网络空间身份属性获取装置，可以组成网络空间身份属性获取系统，图3示出了本发明一实施例提供的网络应用的身份属性获取系统的结构示意图，如图3所示，该系统包括：网络终端31、网络应用服务器32、网络身份提供服务器33和网络身份基础信息服务器34；网络身份基础信息服务器34、网络身份提供服务器33、网络应用服务器32、网络终端31、网络用户身份证等构成了相互制约和相互依存的生态系统。在需要时，网络身份提供服务器33可向网络应用服务器32出示有关非身份证记载的其他身份信息的断言，如网络用户是否在逃犯罪人员，是否有犯罪前科，以及个人信用状况等其他身份信息。

[0102] 为了保证通信的安全性，网络终端31、网络应用服务器32、网络身份提供服务器33、网络身份基础信息服务器34采用私钥签名技术实现数据的可鉴别性，防止仿冒攻击。各子系统之间传输的信息必须采用密码技术实现密文形式传输，以保护身份属性获取过程中

数据的机密、完整性、可用性等安全。传送信道采用安全的传输通道，如TLS/SSL。

[0103] 可以理解的是，本发明提供的网络空间身份属性获取装置即为系统中的网络身份提供服务器33。网络身份提供服务器33是身份和属性验证方，被网络应用服务器32信任并向网络应用服务器32提供身份属性获取服务。每个网络身份提供服务器33都包含身份证验证服务设备，身份证验证服务设备是身份证验证安全访问专用设备，主要用于通过与网络终端31的交互实现对网络用户身份证的真伪鉴别、向网络终端31发送读取身份管理参数的指令等功能。本发明的网络身份提供服务器33不经网络终端31读取身份证信息。网络身份提供服务器33的身份属性获取服务依赖于网络身份基础信息服务器34提供的断言证明。此外，网络身份提供服务器33还具有与网络应用服务器32、与网络终端31的交互接口。每个网络身份提供服务器33可同时支持多个网络应用服务器32。

[0104] 图4示出了本发明一实施例提供的网络应用的身份属性获取系统的工作流程图，具体的，如图4所示：

[0105] (1)网络用户访问网络应用服务器42；

[0106] (2)网络应用服务器42向信任的网络身份提供服务器43发送请求身份属性指令；

[0107] (3)网络身份提供服务器43向网络用户请求身份管理参数，具体的实现是由身份验证服务设备发出阅读身份管理参数指令；

[0108] (4)网络用户在网络终端41的支持射频功能的网络身份证阅读器上刷身份证；

[0109] (5)网络终端41的网络身份证阅读器读取身份管理参数发送给网络终端41设备经安全传输通道发送给网络身份提供服务器43；

[0110] (4)网络身份提供服务器43记录身份管理参数，并由身份验证服务设备向网络终端41发送挑战身份证的挑战码；

[0111] (7)网络终端41请求挑战网络用户身份证；

[0112] (8)网络用户在网络终端41的网络身份证阅读器上刷身份证；

[0113] (9)身份证接受并处理挑战码后，返回处理结果给网络终端41；

[0114] (10)网络终端41经安全传输通道向网络身份提供服务器43的身份证验证服务设备发送证件挑战结果；

[0115] (11)网络身份提供服务器43的身份证验证服务设备处理挑战结果；

[0116] (12)在网络用户身份证鉴别为真的情况下，网络身份提供服务器43向网络身份基础信息服务器44请求网络用户的身份属性；

[0117] (13)网络身份提供服务器43向网络应用服务器42发送网络应用服务器42所请求的网络用户身份属性。

[0118] 身份属性获取开始之前，网络终端41和网络身份提供服务器43预先建立安全的网络传输通道。身份属性获取过程中，经安全网络传输通道传输的身份管理参数和挑战码可被加密保护，该加密保护可在网络身份证阅读器中实现。为了验证身份证的真伪，网络身份提供服务器43向身份证发起的挑战采用的是身份证专用算法，所使用的算法、密钥承载于独立的专用密码设备中，比如身份证验证服务设备，可以是身份证验证服务器。

[0119] 上述的身份属性获取系统支持通过扩展接入网络身份基础信息服务器44提供额外的身份/属性查询，并在严格审核的前提下向特定的网络身份提供服务器43提供专门的身份/属性证明服务。这些特定的网络身份提供服务器43可以提供网络生态系统的其他身

份/属性断言。

[0120] 上述的身份属性获取系统支持通过扩展接入网络身份基础信息服务器44提供额外的身份/属性查询，并在严格审核的前提下向特定的网络身份提供服务器43提供专门的身份/属性证明服务。这些特定的网络身份提供服务器43可以提供网络生态系统的其他身份/属性断言。

[0121] 本发明的网络身份属性获取系统可以实现网络空间多个应用系统的身份统一和通用性，可为网络空间用户提供唯一身份属性获取。居民身份证的全民所有性实现了统一的、通用的网络身份，用户可以很方便的管理更少的网络账户和口令；直接利用现有的第二代居民身份证，节省了其它网络身份属性获取方式的系统研发建设费用。解决了网络身份的可信度不高的问题，居民身份证具有国家权威性，能为网络身份属性获取提供法律依据；统一了网络空间与现实社会中的身份。

[0122] 在身份属性获取过程中采用的密码技术可保障身份属性获取过程安全，基于身份证的自有密码技术对用户身份进行身份属性获取。身份属性获取过程不读取身份证信息，实现用户隐私安全。身份属性获取过程只获取用户身份管理参数，网络应用服务器42不能获得并存储用户身份信息。

[0123] 基于居民身份管理参数的网络空间身份属性获取系统支持可扩展的身份/属性身份属性获取，包括身份属性获取，身份/属性断言证明等。特定的网络身份提供服务器43可以根据网络应用的身份属性获取请求，提供扩展的身份/属性断言。

[0124] 采用身份证验证专用设备，避免了通过其它用身份证身份属性获取过程中的阅读机具中验证安全控制模块暴漏在用户端的监管风险。

[0125] 用于网络身份属性获取的数据通信具有安全保障，通信数据经由安全信道从发送端发送到接受端。发送端和接受端通过密码技术实现信任连接，安全信道采用SSL/TLS安全协议。

[0126] 基于居民身份管理参数的网络空间身份属性获取系统是由网络身份基础信息服务器44、网络身份提供服务器43、网络应用服务器42、网络终端41和网络用户身份证组成。该身份属性获取系统的角色划分考虑了未来网络空间生态系统的演进，身份属性获取由独立的身份提供子系统这一角色实现，身份提供子系统依赖于权威的身份基础服务子系统。

[0127] 本发明提出的身份属性获取既可以获取基本的身份证登记信息，也可以身份属性获取其它的身份/属性信息，如网络用户的信用度、用户犯罪与否等。本发明提出的身份属性获取系统由多样子系统构成网络生态系统，身份属性获取过程根据身份管理参数获取网络身份基础信息服务器44的身份属性/身份属性获取或断言证明。网络身份基础信息服务器44可提供身份证信息、用户信用信息、犯罪信息等身份/属性断言。本发明的身份属性获取方法其身份/属性证明具有可扩展性，可依据需要网络身份提供服务器43请求网络身份基础信息服务器44获取其它身份属性证明。

[0128] 各子系统或实体之间通过密码技术实现相互信任和身份属性获取，并满足机密性、完整性、可用性和不可抵赖性的要求。

[0129] 本发明中在网络空间使用了居民身份证进行身份属性获取，且身份属性获取过程不从用户身份证中读取身份证中的身份信息，不在用户所在的网络终端41和网络应用服务器42间传递身份信息。使用居民身份证进行身份属性获取的过程中，由网络身份提供服务

器43对身份证进行真伪验证后从网络身份基础信息服务器44中获得网络用户身份的断言。使用居民身份证实现网络空间身份属性获取统一了网络空间与现实社会的身份。

[0130] 本发明的网络身份属性获取系统中的网络身份提供服务器43部署有用于身份证验证的身份验证服务设备。其形态可以是专用的身份证验证服务器或内嵌有身份证验证服务的安全访问模块。

[0131] 本发明的基于居民身份管理参数的网络空间身份属性获取方法拥有适用于网络的人证同一性核验的方法。其方法一是采用增设用于网络空间的身份证口令方法，其方法二是采用网络用户指纹与网络身份基础信息服务器44的国家人口信息资源库进行指纹比对的方法。

[0132] 本发明中的网络身份提供服务器43与网络应用服务器42可以独立部署在不同的组织安全交互。网络身份提供服务器43也可以与应用子系统部署在一起，还可以作为网络身份基础服务的一部分部署。

[0133] 本发明的基于居民身份管理参数的网络空间身份属性获取方法具有网络通信安全的特点。每次身份属性获取中网络身份提供服务器63发送的挑战码是唯一的且不可预测，采用先前截获的应答码进行重放攻击不可行。网络中传输的信息以密文形式传输，以保护身份属性获取过程中数据的机密、完整性、可用性等安全。传送信道可采用安全的传输通道，如TLS/SSL。

[0134] 本领域技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在于该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是互相排斥之处，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0135] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0136] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0137] 最后应说明的是：本领域普通技术人员可以理解：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域

的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分或者全部技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明权利要求所限定的范围。

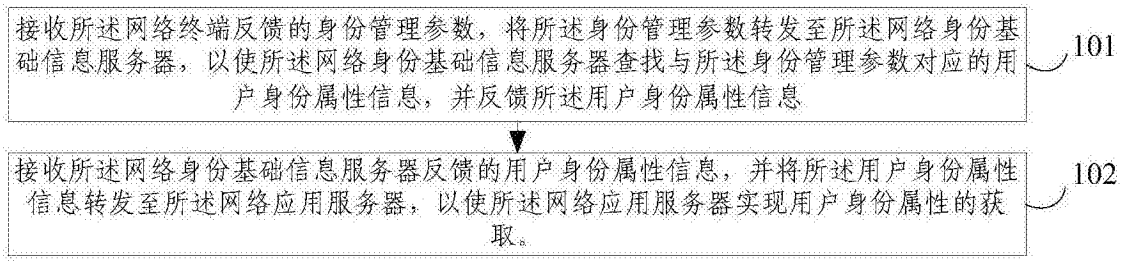
接收所述网络终端反馈的身份管理参数，将所述身份管理参数转发至所述网络身份基础信息服务器，以使所述网络身份基础信息服务器查找与所述身份管理参数对应的用户身份属性信息，并反馈所述用户身份属性信息
101
接收所述网络身份基础信息服务器反馈的用户身份属性信息，并将所述用户身份属性信息转发至所述网络应用服务器，以使所述网络应用服务器实现用户身份属性的获取。
102

图1

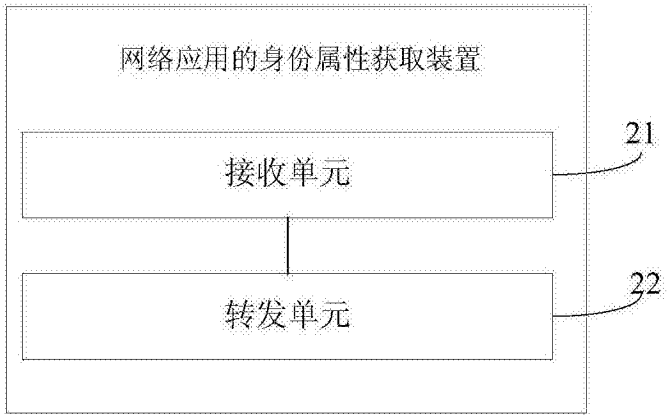
网络应用的身份属性获取装置
接收单元
21
转发单元
22

图2

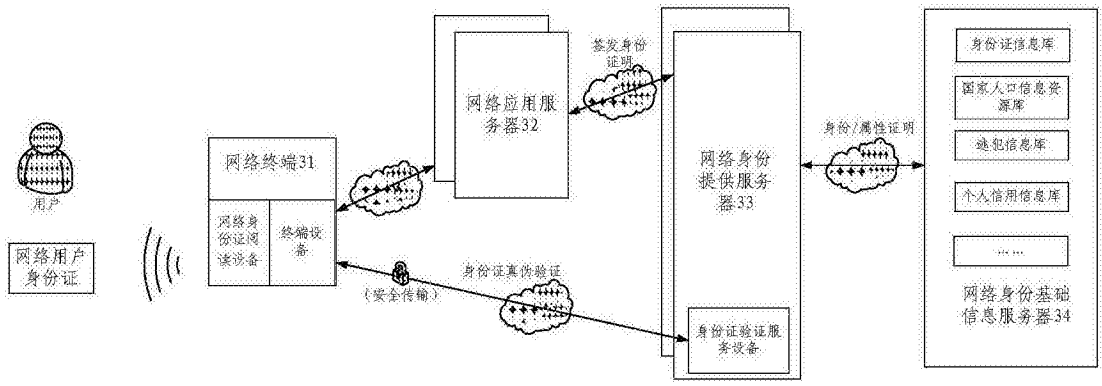
用户
网络用户身份证
网络终端31
网络身份证阅读设备
终端设备
网络应用服务器32
签发身份证明
网络身份提供服务器33
身份证验证服务设备
身份/属性证明
身份证真伪验证
（安全传输）
身份证信息库
国家人口信息资源库
逃犯信息库
个人信用信息库
……
网络身份基础信息服务器34

图3

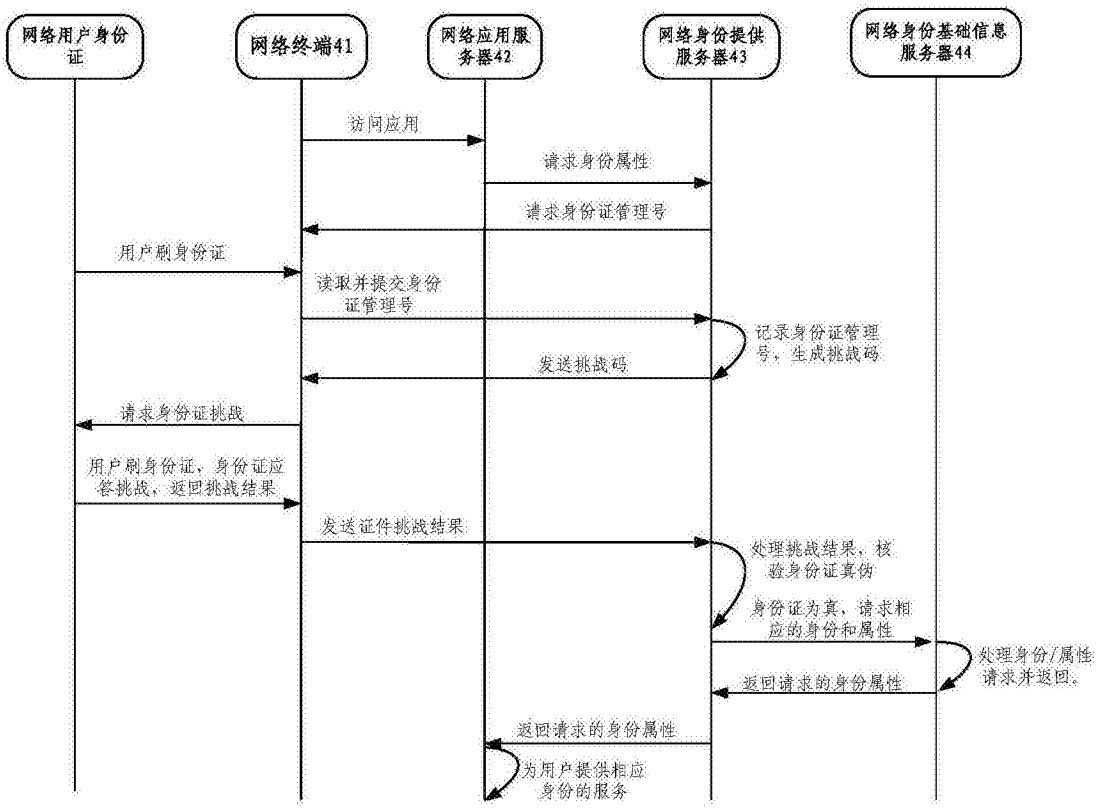
网络用户身份证
网络终端41
网络应用服务器42
网络身份提供服务器43
网络身份基础信息服务器44
访问应用
请求身份属性
请求身份证管理号
用户刷身份证
读取并提交身份证管理号
记录身份证管理号，生成挑战码
发送挑战码
请求身份证挑战
用户刷身份证，身份证应答挑战，返回挑战结果
发送证件挑战结果
处理挑战结果，核验身份证真伪
身份证为真，请求相应的身份和属性
处理身份/属性请求并返回。
返回请求的身份属性
返回请求的身份属性
为用户提供相应身份的服务

图4