(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 104065652 B
(45)授权公告日 2015.10.14

(21)申请号 201410253630.X

(22)申请日 2014.06.09

(73)专利权人 北京石盾科技有限公司
地址 100086 北京市海淀区北三环西路43号青云当代大厦1008室

(72)发明人 韩晟 王盈

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 黄志华

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

(56)对比文件
CN 101202631 A,2008.06.18,
CN 101442407 A,2009.05.27,
CN 103684796 A,2014.03.26,
CN 103714458 A,2014.04.09,

审查员 刘俭

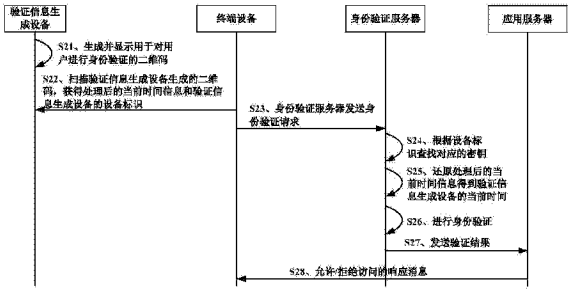
权利要求书4页 说明书11页 附图2页

(54)发明名称

一种身份验证方法、装置、系统及相关设备

(57)摘要

本发明公开了一种身份验证方法、装置、系统及相关设备，用以提高身份验证的安全性和通用性。身份验证系统包括：验证信息生成设备，用于在需要进行身份验证时生成用户身份验证信息，用户身份验证信息至少包括利用存储的密钥对种子信息进行处理得到的处理后的种子信息；身份验证服务器，用于接收终端设备发送的身份验证请求，所述身份验证请求中携带有处理后的种子信息，其中所述处理后的种子信息为所述终端设备从所述验证信息生成设备获取的用户身份验证信息中获得的；从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥；利用查找到的密钥还原和/或验证处理后的种子信息；根据还原结果或者验证结果确定身份验证是否通过。



CN 104065652 B

1. 一种身份验证系统，其特征在于，包括：

验证信息生成设备，用于在需要进行身份验证时生成用户身份验证信息，所述用户身份验证信息至少包括利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息；其中所述身份验证信息为图形码；该验证信息生成设备为单独的硬件设备，包括

安全存储模块，存储该验证信息生成设备的密钥；

运算模块，利用安全存储模块预先存储的密钥对种子信息进行处理得到处理后的种子信息，并利用处理后的种子信息生成图形码；

显示器，显示生成的图形码；

终端设备，扫描所述验证信息生成设备显示的所述图形码，获得身份验证信息，并将获得的身份验证信息发送该身份验证服务器；该终端设备获取用户当前正在访问的互联网应用的应用服务器的应用标识以及该互联网应用在全局范围内的唯一标识，并将应用标识以及该该互联网应用在全局范围内的唯一标识随着身份验证请求一起发送给身份验证服务器；

身份验证服务器，用于接收终端设备发送的身份验证请求，所述身份验证请求中携带有处理后的种子信息，其中所述处理后的种子信息为所述终端设备从所述验证信息生成设备获取的用户身份验证信息中获得的；从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥；利用查找到的密钥还原和/或验证处理后的种子信息；根据还原结果或者验证结果确定身份验证是否通过；

所述身份验证信息中还包括所述验证信息生成设备的设备标识；所述身份验证请求中还携带有所述设备标识；

所述身份验证服务器，具体用于按照以下方法确定所述验证信息生成设备中存储的密钥对应的密钥：根据所述设备标识从自身存储的设备标识与密钥的对应关系中查找所述设备标识对应的密钥，将查找到的密钥确定为所述验证信息生成设备中存储的密钥所对应的密钥，利用查找到的密钥对加密的种子信息进行解密得到所述种子信息，并进行身份验证；根据身份验证请求中携带的应用标识，向与该应用标识对应的应用服务器提供验证结果，并在发送的验证结果中携带用户当前访问的互联网应用在全局范围内的唯一标识；

应用服务器，提供各种互联网应用，根据身份验证服务器发送的验证结果向终端设备发送允许/拒绝访问的响应消息；

身份验证服务器维护每个应用的应用标识与其对应的验证信息生成设备的设备标识以及密钥之间的对应关系，以对不同的应用提供身份验证。

2. 如权利要求 1 所述的系统，其特征在于，所述种子信息为验证信息生成设备的当前时间；以及

所述身份验证服务器，具体用于在确定还原出的验证信息生成设备的当前时间与自身的当前时间之间的间隔在预设时间间隔范围之内时，确定身份验证通过；或者确定对所述验证信息生成设备的当前时间的验证通过时，确定身份验证通过。

3. 如权利要求 1 所述的系统，其特征在于，所述图形码包括一维码或者二维码。

4. 如权利要求 1 所述的系统，其特征在于，

所述验证信息生成设备，具体用于按照以下方法利用存储的密钥对种子信息进行处

理：利用存储的密钥对种子信息进行加密、签名或者哈希运算；

所述身份验证服务器，具体用于按照以下方法利用查找到的密钥还原和/或验证处理后的种子信息：利用查找到的密钥对加密的种子信息进行解密得到所述种子信息；或者利用查找到的密钥对已签名的种子信息进行验证；或者利用查找到的密钥对所述种子信息进行哈希运算后得到的哈希值进行验证。

5. 如权利要求1～4任一权利要求所述的系统，其特征在于，所述系统采用非对称密钥加密体系，其中，所述验证信息生成设备存储私钥，所述验证服务器存储所述私钥对应的公钥。

6. 一种身份验证方法，其特征在于，包括：

接收终端设备发送的身份验证请求，所述身份验证请求中携带有所述终端设备从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息；其中所述身份验证信息为图形码；该验证信息生成设备为单独的硬件设备，包括

安全存储模块，存储该验证信息生成设备的密钥；

运算模块，利用安全存储模块预先存储的密钥对种子信息进行处理得到处理后的种子信息，并利用处理后的种子信息生成图形码；

显示器，显示生成的图形码；

终端设备通过扫描所述验证信息生成设备显示的所述图形码，获得身份验证信息，并将获得的身份验证信息发送该身份验证服务器；该终端设备获取用户当前正在访问的互联网应用的应用服务器的应用标识以及该互联网应用在全局范围内的唯一标识，并将应用标识以及该该互联网应用在全局范围内的唯一标识随着身份验证请求一起发送给身份验证服务器；

身份验证服务器从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥；利用查找到的密钥还原和/或验证处理后的种子信息；根据还原结果或者验证结果确定身份验证是否通过；

所述身份验证信息中还包括所述验证信息生成设备的设备标识；所述身份验证请求中还携带有所述设备标识；以及

从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥，具体包括：

根据所述设备标识，从自身存储的设备标识与密钥的对应关系中查找所述设备标识对应的密钥；

将所述设备标识对应的密钥作为所述验证信息生成设备中存储的密钥对应的密钥；利用查找到的密钥对加密的种子信息进行解密得到所述种子信息，并进行身份验证；根据身份验证请求中携带的应用标识，向与该应用标识对应的应用服务器提供验证结果，并在发送的验证结果中携带用户当前访问的互联网应用在全局范围内的唯一标识；

应用服务器根据身份验证服务器发送的验证结果向终端设备发送允许/拒绝访问的响应消息。

7. 如权利要求6所述的方法，其特征在于，所述种子信息为验证信息生成设备的当前

时间；以及

按照以下方法确定身份验证通过：

在确定还原出的验证信息生成设备的当前时间与当前时间之间的间隔在预设时间间隔范围之内时，确定身份验证通过；或者

确定对所述验证信息生成设备的当前时间的验证通过时，确定身份验证通过。

8. 如权利要求 6 所述的方法，其特征在于，所述处理后的种子信息为所述验证信息生成设备利用存储的密钥对所述种子信息进行加密、签名或者哈希运算得到的；以及

利用查找到的密钥还原和 / 或验证处理后的种子信息，具体包括：

利用查找到的密钥对加密的种子信息进行解密得到所述种子信息；或者

利用查找到的密钥对已签名的种子信息进行验证；或者

利用查找到的密钥对所述种子信息进行哈希运算后得到的哈希值进行验证。

9. 一种身份验证装置，其特征在于，包括：

接收单元，用于接收终端设备发送的身份验证请求，所述身份验证请求中携带有所述终端设备从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息；其中所述身份验证信息为图形码；该验证信息生成设备为单独的硬件设备；所述身份验证信息中还包括所用户当前正在访问的互联网应用的应用服务器的应用标识以及该互联网应用在全局范围内的唯一标识；

查找单元，用于从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥；

处理单元，用于利用所述查找单元查找到的密钥还原和 / 或验证处理后的种子信息；

身份验证单元，用于根据还原结果或者验证结果确定身份验证是否通过；并根据身份验证请求中携带的应用标识，向与该应用标识对应的应用服务器提供验证结果，并在发送的验证结果中携带用户当前访问的互联网应用在全局范围内的唯一标识；

所述身份验证信息中还包括所述验证信息生成设备的设备标识；所述身份验证请求中还携带有所述设备标识；以及

所述查找单元，具体用于根据所述设备标识，从自身存储的设备标识与密钥的对应关系中查找所述设备标识对应的密钥；将所述设备标识对应的密钥作为所述验证信息生成设备中存储的密钥对应的密钥。

10. 如权利要求 9 所述的装置，其特征在于，所述种子信息为验证信息生成设备的当前时间；以及

所述身份验证单元，具体用于在确定还原出的验证信息生成设备的当前时间与当前时间之间的间隔在预设时间间隔范围之内时，确定身份验证通过；或者确定对所述验证信息生成设备的当前时间的验证通过时，确定身份验证通过。

11. 如权利要求 9 所述的装置，其特征在于，所述处理后的种子信息为所述验证信息生成设备利用存储的密钥对所述种子信息进行加密、签名或者哈希运算得到的；以及

所述处理单元，具体用于利用所述查找单元查找到的密钥对加密的种子信息进行解密得到所述种子信息；或者利用所述查找单元查找到的密钥对已签名的种子信息进行验证；或者利用所述查找单元查找到的密钥对所述种子信息进行哈希运算后得到的哈希值进行

验证。

12. 一种身份验证服务器，其特征在于，包括权利要求 9 ～ 11 任一权利要求所述的身份验证装置。

13. 一种身份验证方法，其特征在于，包括 ：

在访问互联网应用需要进行身份验证时，向网络侧的身份验证服务器发送身份验证请求，所述身份验证请求中携带有从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息 ；该验证信息生成设备为单独的硬件设备 ；所述身份验证信息中还包括所用户当前正在访问的互联网应用的应用服务器的应用标识以及该互联网应用在全局范围内的唯一标识 ；

接收所述互联网应用对应的应用服务器返回的允许 / 拒绝访问的响应消息，所述响应消息为所述应用服务器根据所述身份验证服务器返回的身份验证结果发送的 ；

所述身份验证信息为图形码 ；以及

按照以下方法从所述验证信息生成设备获取所述用户身份验证信息 ：

扫描所述验证信息生成设备显示的所述图形码。

14. 一种身份验证装置，其特征在于，包括 ：

发送单元，用于在访问互联网应用需要进行身份验证时，向网络侧的身份验证服务器发送身份验证请求，所述身份验证请求中携带有从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息 ；该验证信息生成设备为单独的硬件设备 ；所述身份验证信息中还包括所用户当前正在访问的互联网应用的应用服务器的应用标识以及该互联网应用在全局范围内的唯一标识 ；

接收单元，用于接收所述互联网应用对应的应用服务器返回的允许 / 拒绝访问的响应消息，所述响应消息为所述应用服务器根据所述身份验证服务器返回的身份验证结果发送的 ；

所述身份验证信息为图形码 ；以及

所述装置，还包括 ：

摄像单元，用于扫描所述验证信息生成设备显示的所述图形码。

一种身份验证方法、装置、系统及相关设备

技术领域

[0001] 本发明涉及信息安全技术领域，尤其涉及一种身份验证方法、装置、系统及相关设备。

背景技术

[0002] 随着互联网技术尤其是移动互联网技术的飞速发展，通过互联网提供的互联网应用越来越多。用户在访问这些互联网应用时，如访问电子邮件、访问即时通信应用、访问网站等，为了保证用户访问的安全性，各互联网应用的提供方通常需要在用户登录时对用户身份进行验证。

[0003] 当前，最常见的身份验证方法为通过用户注册时提供的用户名和密码，用户名和密码通常由大小写字母、数字和可输入的符号组成，若输入的用户名和密码匹配即可通过验证。在对安全性要求更高的互联网应用中，如网上银行、在线支付应用等，通常还会使用其他辅助的身份验证手段，常见的有手机验证码、RSA SecurID 双因素验证令牌和智能卡等。

[0004] 上述各种身份验证方法中，通过用户名和密码是最常用的身份验证方法，但是由于用户名和密码长度都有一定的限制，密码设置太短、太简单的话，容易被破解，太长太复杂又不便于记忆。而且，用户名和密码在通过键盘输入时，容易被终端设备中的恶意代码窃取，从而降低了身份验证的安全性。

[0005] 如果手机验证码作为辅助的身份验证手段，由于智能手机很容易被植入恶意代码，其可以拦截网络侧下发的手机验证码，从而也无法保证身份验证的安全性。而智能卡由于硬件限制，难以普及且通用性不强。至于 RSA SecurID 双因素验证令牌，其广泛应用于世界各地的重要信息系统中，但由于其是采用 6 位数字进行验证，只适合作为验证码使用，而不能作为验证身份的用户名和主要密码。且该方法只能在独立的信息系统中使用，无法通用，用户通常需要持有多个不同的 SecurID 令牌。

[0006] 由此可见，如何提高身份验证的安全性和通用性成为现有技术中亟待解决的技术问题之一。

发明内容

[0007] 本发明实施例提供一种身份验证方法、装置、系统及相关设备，用以提高身份验证的安全性和通用性。

[0008] 本发明实施例提供一种身份验证系统，包括：

[0009] 验证信息生成设备，用于在需要进行身份验证时生成用户身份验证信息，所述用户身份验证信息至少包括利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息；

[0010] 身份验证服务器，用于接收终端设备发送的身份验证请求，所述身份验证请求中携带有处理后的种子信息，其中所述处理后的种子信息为所述终端设备从所述验证信息生

成设备获取的用户身份验证信息中获得的；从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥；利用查找到的密钥还原和／或验证处理后的种子信息；根据还原结果或者验证结果确定身份验证是否通过。

[0011] 本发明实施例提供一种网络侧实施的身份验证方法，包括：

[0012] 接收终端设备发送的身份验证请求，所述身份验证请求中携带有所述终端设备从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息；

[0013] 从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥；

[0014] 利用查找到的密钥还原和／或验证处理后的种子信息；

[0015] 根据还原结果或者验证结果确定身份验证是否通过。

[0016] 本发明实施例提供一种网络侧实施的身份验证装置，包括：

[0017] 接收单元，用于接收终端设备发送的身份验证请求，所述身份验证请求中携带有所述终端设备从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息；

[0018] 查找单元，用于从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥；

[0019] 处理单元，用于利用所述查找单元查找到的密钥还原和／或验证处理后的种子信息；

[0020] 身份验证单元，用于根据还原结果或者验证结果确定身份验证是否通过。

[0021] 本发明实施例提供一种身份验证服务器，包括上述网络侧实施的身份验证装置。

[0022] 本发明实施例提供一种终端侧实施的身份验证方法，包括：

[0023] 在访问互联网应用需要进行身份验证时，向网络侧的身份验证服务器发送身份验证请求，所述身份验证请求中携带有从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息；

[0024] 接收所述互联网应用对应的应用服务器返回的允许／拒绝访问的响应消息，所述响应消息为所述应用服务器根据所述身份验证服务器返回的身份验证结果发送的。

[0025] 本发明实施例提供一种终端设备侧实施的身份验证装置，包括：

[0026] 发送单元，用于在访问互联网应用需要进行身份验证时，向网络侧的身份验证服务器发送身份验证请求，所述身份验证请求中携带有从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息；

[0027] 接收单元，用于接收所述互联网应用对应的应用服务器返回的允许／拒绝访问的响应消息，所述响应消息为所述应用服务器根据所述身份验证服务器返回的身份验证结果发送的。

[0028] 本发明实施例提供一种终端设备，包括上述终端侧实施的身份验证装置。

[0029] 本发明实施例提供的身份验证方法、装置、系统及相关设备，在需要进行身份验证

时，通过终端设备获取验证信息生成设备生成的用户身份验证信息，从而得到用户身份验证信息中包含的被处理后的种子信息。其中，验证信息生成设备利用自身存储的密钥对种子信息进行处理，终端设备将得到的被处理后的种子信息发送给网络侧的身份验证服务器，身份验证服务器查找自身存储的该验证信息生成设备中存储的密钥所对应的密钥，并利用查找到的密钥还原和 / 或验证处理后的种子信息，并根据还原结果或者验证结果确定身份验证是否通过。由于上述过程中，一方面，无需用户记忆用户名和密码，直接通过终端获取身份验证信息即可进行验证，简化了用户操作，另一方面，身份验证信息为根据处理后的种子信息生成的，其复杂程度高于人类可以记忆的密码，且其是唯一的且不可重复的，因此，即使中途被监听也无法再次使用和伪造，从而提高了身份验证的安全性。另外，本发明实施例提供的身份验证方法，适用于需要对身份进行验证的场景，因此，其提高了身份验证方法的通用性。

[0030] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0031] 此处所说明的附图用来提供对本发明的进一步理解，构成本发明的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0032] 图 1 为本发明实施例中，身份验证系统的结构示意图；

[0033] 图 2 为本发明实施例中，身份验证系统中信息交互流程示意图；

[0034] 图 3 为本发明实施例中，网络侧实施的身份验证方法的实施流程示意图；

[0035] 图 4 为本发明实施例中，网络侧实施的身份验证装置的结构示意图；

[0036] 图 5 为本发明实施例中，终端侧实施的身份验证方法的实施流程示意图；

[0037] 图 6 为本发明实施例中，终端侧实施的身份验证装置的结构示意图。

具体实施方式

[0038] 为了提高身份验证系统的安全性和通用性，本发明实施例提供了一种身份验证方法、装置、系统及相关设备。

[0039] 以下结合说明书附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明，并且在不冲突的情况下，本发明中的实施例及实施例中的特征可以相互组合。

[0040] 实施例一

[0041] 如图 1 所示，为本发明实施例提供的身份验证系统的结构示意图，包括验证信息生成设备和身份验证服务器，其中：

[0042] 验证信息生成设备 11，用于在需要进行身份验证时生成用户身份验证信息，其中，用户身份验证信息至少包括利用存储的密钥对种子信息进行处理得到的处理后的种子信息；

[0043] 身份验证服务器 12，用于接收终端设备发送的身份验证请求，身份验证请求中携带有处理后的种子信息，其中处理后的种子信息为终端设备从验证信息生成设备 11 获取

的用户身份验证信息中获得的；从自身存储的密钥中，查找验证信息生成设备中存储的密钥对应的密钥；利用查找到的密钥还原和/或验证处理后的种子信息；根据还原结果或者验证结果确定身份验证是否通过。

[0044] 较佳的，具体实施时，种子信息可以为计算机系统可处理的任一信息，如已知的固定信息（比如名字、固定的数字等等）、随机数、时间、累加计数器等等，只要是能够使用密钥进行处理的信息均可，本发明对此不做限定。

[0045] 为了便于说明，以种子信息为验证信息生成设备 11 的当前时间为例。这样，身份验证服务器 12 可以用于在确定还原出的验证信息生成设备 11 的当前时间与自身的当前时间之间的间隔在预设时间间隔范围之内时，确定身份验证通过；还可以用于确定对验证信息生成设备 11 的当前时间的验证通过时，确定身份验证通过。

[0046] 较佳的，验证信息生成设备 11 生成的身份验证信息可以但不限于为图形码，该图形码可以为一维码（条形码）和二维码，其中，二维码包括标准二维码和非标准二维码（即一些变形的二维码，如圆形二维码、彩色二维码等等），本发明对此不做限定。具体实施时，验证信息生成设备 11 可以由安全存储模块、运算模块和可显示图形码的电子显示器组成，其中，安全存储模块中存储有该验证信息生成设备 11 的密钥。基于此，在需要进行身份验证时，验证信息生成设备 11 可以按照以下方法生成该图形码：

[0047] 运算模块利用安全存储模块预先存储的密钥对种子信息进行处理得到处理后的种子信息。具体实施时，运算模块可以利用安全存储模块存储的密钥对种子信息进行加密得到该种子信息对应的密文信息；或者运算模块也可以利用安全存储模块存储的密钥对种子信息进行签名得到签名后的种子信息，还可以对种子信息进行哈希运算得到对应的哈希值。

[0048] 运算模块利用处理后的种子信息（上述得到的密文信息或者已签名的种子信息或者哈希值）生成一个图形码，显示在验证信息生成设备 11 的显示器上。这样，终端设备可以通过扫描验证信息生成设备 11 显示的图形码从而得到该图形码中包含的处理后的种子信息。终端设备将得到的处理后的种子信息携带在身份验证请求中发送给网络侧的身份验证服务器 12，身份验证服务器 12 从自身存储的密钥中查找该验证信息生成设备 11 存储的密钥所对应的密钥并使用查找到的密钥还原和/或验证处理后的种子信息，根据还原结果或者验证结果确定身份验证是否通过。

[0049] 较佳的，具体实施时，本发明实施例提供的身份验证系统可以采用对称密钥加密体系，也可以采用非对称密钥加密体系。如果采用对称密钥加密体系，安全存储模块存储的密钥和身份验证服务器 12 存储的密钥相同。如果采用非对称密钥加密体系，可以为每一个验证信息生成设备随机生成一组公钥和私钥，验证信息生成设备 11 的安全存储模块存储私钥，身份验证服务器 12 存储公钥。相比于对称密钥加密机制，非对称密钥加密机制能够进一步提高身份验证系统的安全性，这种情况下，即使身份验证服务器 12 被入侵，攻击者也无法伪造用户登录。

[0050] 具体的，在使用非对称密钥加密技术时，如果验证信息生成设备 11 使用私钥对种子信息进行签名，则身份验证服务器 12 存储的公钥可以用于对已签名的种子信息进行验证；如果验证信息生成设备 11 使用私钥对种子信息进行加密，则身份验证服务器 12 存储的公钥可以用于对加密的种子信息进行解密，得到种子信息。若使用对称密钥加密技术，如果

验证信息生成设备 11 使用存储的密钥对种子信息进行签名，则身份验证服务器 12 存储的密钥可以用于对已签名的种子信息进行验证；如果验证信息生成设备 11 使用存储的密钥对种子信息进行加密，则身份验证服务器 12 存储的密钥既可以用于对加密的种子信息进行解密得到种子信息后再验证，也可以不还原直接验证密文；如果验证信息生成设备 11 使用哈希算法对种子信息进行哈希运算得到哈希值，则身份验证服务器 12 可以用于对得到的哈希值进行验证。

[0051] 以种子信息为验证信息生成设备 11 的当前时间为例，如果还原得到的验证信息生成设备 11 的当前时间与身份验证服务器 12 的当前时间之间的时间间隔在预设时间间隔范围之内（如可以设置为极短的时间间隔），确定身份验证通过，否则，确定身份验证不通过；或者确定对验证信息生成设备 11 的当前时间的验证通过时，确定身份验证通过，否则确定身份验证不通过。

[0052] 上述方法中，身份验证服务器 12 在接收到终端设备的身份验证请求之后，需要从自身存储的所有密钥中查找验证信息生成设备 11 中存储的密钥对应的密钥还原和 / 或验证处理后的种子信息。具体的，身份验证服务器 12 可以依次尝试自身存储的每一密钥，直至其能够还原和 / 或验证处理后的种子信息为止。

[0053] 较佳的，为了提高身份验证服务器 12 还原和 / 或验证处理后的种子信息的效率，本发明实施例中，验证信息生成设备 11 生成的身份验证信息中还可以包含该验证信息生成设备 11 的设备标识，这样，终端设备可以从身份验证信息中获取该设备标识，并和处理后的种子信息一起携带在身份验证请求中一并发送给身份验证服务器 12，身份验证服务器 12 可以根据设备标识从预先存储的设备标识与密钥的对应关系中直接查找该设备标识对应的密钥，将其作为验证信息生成设备 11 中存储的密钥对应的密钥。

[0054] 实施例二

[0055] 为了更好的理解本发明实施例，以下结合身份验证时的信息交互流程对本发明实施例的具体实施过程进行说明，为了便于说明，本发明实施例以用户访问网上银行为例进行说明，用户登录网上银行的流程如图 2 所示，可以包括以下步骤：

[0056] S21、验证信息生成设备生成并显示用于对用户进行身份验证的二维码。

[0057] 具体实施时，用户可能通过以下两种方式访问网上银行：

[0058] 方式一、

[0059] 用户使用获取用户身份验证信息的终端设备访问网上银行，例如，用户使用手机访问网上银行，同时使用该手机获取验证信息生成设备生成的用户身份验证信息。这种情况下，用户所访问的网上银行的登录页面需要提供使用本发明实施例提供的身份验证方法封装的应用程序接口，在用户需要登录网上银行时通过调用该应用程序接口触发对用户的身份验证。

[0060] 方式二、

[0061] 用户使用获取用户身份验证信息的终端设备以外的其他终端设备访问网上银行，例如用户使用电脑访问网上银行，使用自己的手机获取验证信息生成设备生成的用户身份验证信息。这种情况下，网上银行登录页面需要嵌入本发明实施例提供的身份验证方法封装的验证程序，并在登录页面以图形码（可以但不限于为二维码）的形式显示，当用户需要登录网上银行时，直接扫描该二维码便可以触发对用户的身份验证。

[0062] 在触发对用户的身份验证之后，用户通过触发自己拥有的验证信息生成设备（该设备可以为用户注册银行账户时由银行提供给用户）生成用户身份验证信息，具体方法可以参见上述实施例一中的描述，这里不再赘述。

[0063] 较佳的，为了避免用户丢失验证信息生成设备带来的风险，本发明实施例中，验证信息生成设备还可以在生成用户身份验证信息之前对用户身份进行识别，例如，可以通过指纹进行识别，也可以通过用户预先设置的密码对用户进行识别，这里不做限定，相应的，验证信息生成设备还可以包括数字按键或者指纹采集装置。

[0064] S22、终端设备扫描验证信息生成设备生成的二维码，获得处理后的当前时间信息和验证信息生成设备的设备标识。

[0065] 具体实施时，对于方式一，其可以直接调用根据本发明实施例提供的身份验证方法实现的身份验证应用程序对验证信息生成设备生成的用户身份验证信息进行扫描。对于方式二，用户自行启动终端设备中安装的根据本发明实施例提供的身份验证方法实现的身份验证应用程序，对验证信息生成设备生成的用户身份验证信息进行扫描。

[0066] S23、终端设备向网络侧的身份验证服务器发送身份验证请求。

[0067] 其中，身份验证请求中携带有得到的处理后的种子信息和验证信息生成设备的设备标识。另外，终端设备还需要在身份验证请求中携带用户访问的互联网应用的应用标识或者应用名称和该互联网应用在全局范围内的唯一标识，该唯一标识是一个全局唯一的编码，在不同的互联网应用、不同的终端设备、不同时间上都不重复。较佳的，该唯一标识可以但不限于为UUID(Universally Unique Identifier，通用唯一识别码)或者GUID(Globally Unique Identifier，全局唯一标识符)，当然也可以是采用类似技术实现的全局范围内的一个标识，为了便于描述以下以UUID为例进行说明。

[0068] 如果用户通过上述第一种方式访问互联网应用，则终端设备可以直接获取用户当前正在访问的互联网应用的应用标识或者应用名称及其对应的UUID一并发送给身份验证服务器；如果用户通过上述第二种方式访问互联网应用，则在生成登录页面显示的图形码中包括互联网应用的应用标识或者应用名称和该互联网应用对应的UUID，这样，终端设备通过扫描该图形码便可以获取应用标识或者应用名称和该互联网应用对应的UUID，与从验证信息生成设备生成的二维码中获取的处理后的种子信息和验证信息生成设备的设备标识一并发送给身份验证服务器。

[0069] 具体实施时，终端设备可以通过有线网络、无线网络和移动通信网络等向网络侧的身份验证服务器发送身份验证请求。

[0070] S24、身份验证服务器根据身份验证请求中携带的设备标识查找对应的密钥。

[0071] S25、身份验证服务器利用查找到的密钥还原和/或验证处理后的当前时间信息。

[0072] S26、身份验证服务器进行身份验证。

[0073] 具体实施时，以验证信息生成设备对当前时间加密为例，身份验证服务器比较还原出的验证信息生成设备的当前时间和自身的当前时间，如果时间间隔不超过预设的时间间隔则确定验证通过，否则，确定验证不通过。

[0074] S27、身份验证服务器向提供互联网应用的应用服务器发送验证结果。

[0075] 具体实施时，身份验证服务器根据身份验证请求中携带的应用标识或者应用名称向该应用标识或者应用名称对应的应用服务器提供验证结果，并在发送的验证结果中携带

用户当前访问的互联网应用的UUID。

[0076] S28、应用服务器向终端设备发送允许/拒绝访问的响应消息。

[0077] 具体实施时，应用服务器根据UUID确定用户访问互联网应用的终端设备及应用程序，并根据验证结果向该终端设备发送允许/拒绝访问的响应消息。

[0078] 具体实施时，本发明实施例提供的身份验证系统可以针对不同的互联网应用提供一个验证信息生成设备，也可以针对安全要求高的互联网应用如网上银行、在线支付等提供单独的验证信息生成设备，此时，身份验证服务器需要维护互联网应用的应用标识与其对应的验证信息生成设备的设备标识以及密钥之间的对应关系，以对不同的互联网应用提供身份验证。

[0079] 需要说明的是，本发明实施例中涉及的终端设备可以为手机、平板电脑、PDA（个人数字助理）、智能手表等移动终端设备，也可以是PC（个人电脑）等设备，只要是安装有摄像装置或扫描装置，能够扫描获取验证信息生成设备生成的图形码的终端设备均可。

[0080] 另外，本发明实施例中涉及的互联网应用包括能够通过互联网/移动互联网进行访问的网站、应用程序客户端等。

[0081] 由于现有的采用加密机制的安全系统中，非对称密钥加密技术的安全性已得到充分理论证明，并广泛使用。但其最主要的缺点是密钥太长，人类无法直接记忆和输入，用户通常需要将密钥存储在电脑文件或硬件设备中，使用时进行导入，这样，便存在密钥泄露的风险，且使用极为不便。而本发明实施例中，由于图形码作为一种方便的机器自动识别技术，可以用来表示密文信息，且容易被识别和传输进而解密。这解决了现有的非对称密钥加密机制中密钥太长，不便于直接使用的问题。此外，本发明实施例中，使用独立硬件生成图形码，可以避免私钥被窃取、复制和篡改，与用户使用的互联网应用物理隔离，从根本上避免了遭受黑客入侵的可能性，具有极高的安全性。同时，本发明实施例中使用非对称密钥加密机制时，私钥存储在验证信息生成设备的安全存储模块中，公钥存储在身份验证服务器中，即使身份验证服务器遭受黑客入侵，公钥全部泄露，攻击者也无法伪造任何用户的身份进行验证，从而不构成任何威胁。最后，由于密钥的长度和强度足够，因此可以直接使用验证信息生成设备的设备标识（可以为其唯一的编号）作为用户名，每次对种子信息加密生成的密文信息或已签名的信息作为密码进行身份验证，实现一次一密，且密码复杂度远远高于普通人类设置的密码，安全性和便利性均大大提高。

[0082] 因此，相对于传统的身份验证方法，本发明实施例提供的身份验证方法安全性更高，实现了高度复杂的密码和一次一密，避免了密码被窃取的风险。且本发明实施例提供的身份验证方法，更方便快捷，用户无需记忆和输入各种不同的用户名和密码，直接扫描图形码即可快速完成身份验证过程。

[0083] 由于本发明实施例提供的身份验证方法中的密码长度和强度比普通用户设置的密码及现有的RSA SecurID双因素认证令牌使用的6位纯数字高很多，因此，可以直接作为主密码进行身份验证。

[0084] 另外，本发明实施例提供的身份验证系统还可以用于企业门禁系统，即企业只需要安装图形码扫描装置（例如可以为摄像头），并为每一员工配备一个验证信息生成设备，在进入时可以通过扫描验证信息生成设备生成的用户身份验证信息对其进行验证，通过则允许进入，同时，还可以记录门开启时间等信息。

[0085] 基于同一发明构思，本发明实施例中还分别提供了一种网络侧和终端侧实施的身份验证方法、装置和相关设备，由于上述方法、装置及设备解决问题的原理与身份验证系统相似，因此上述方法、装置及设备的实施可以参见方法的实施，重复之处不再赘述。

[0086] 实施例三

[0087] 如图 3 所示，为本发明实施例提供的网络侧实施的身份验证方法的实施流程示意图，包括：

[0088] S31、身份验证服务器接收终端设备发送的身份验证请求。

[0089] 其中，所述身份验证请求中携带有所述终端设备从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息。

[0090] S32、身份验证服务器从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥；

[0091] S33、身份验证服务器利用查找到的密钥还原和 / 或验证处理后的种子信息；

[0092] S34、身份验证服务器根据还原结果或者验证结果确定身份验证是否通过。

[0093] 具体实施时，所述身份验证信息中还包括所述验证信息生成设备的设备标识；所述身份验证请求中还携带有所述设备标识；以及

[0094] 从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥，具体包括：

[0095] 根据所述设备标识，从自身存储的设备标识与密钥的对应关系中查找所述设备标识对应的密钥；

[0096] 将所述设备标识对应的密钥作为所述验证信息生成设备中存储的密钥对应的密钥。

[0097] 具体实施时，所述种子信息可以是任何计算机系统可处理的信息，较佳的，种子信息可以但不限于为验证信息生成设备的当前时间；以及

[0098] 所述身份验证服务器可以按照以下方法确定身份验证通过：

[0099] 在确定还原出的验证信息生成设备的当前时间与当前时间之间的间隔在预设时间间隔范围之内时，确定身份验证通过；或者确定对所述验证信息生成设备的当前时间的验证通过时，确定身份验证通过。

[0100] 具体实施时，所述处理后的种子信息为所述验证信息生成设备利用存储的密钥对所述种子信息进行加密、签名或者哈希运算得到的；以及

[0101] 利用查找到的密钥还原和 / 或验证处理后的种子信息，具体包括：

[0102] 利用查找到的密钥对加密的种子信息进行解密得到所述种子信息；或者

[0103] 利用查找到的密钥对已签名的种子信息进行验证；或者

[0104] 利用查找到的密钥对所述种子信息进行哈希运算后得到的哈希值进行验证。

[0105] 实施例四、

[0106] 如图 4 所示，为本发明提供的网络侧实施的身份验证装置，包括：

[0107] 接收单元 41，用于接收终端设备发送的身份验证请求，所述身份验证请求中携带有所述终端设备从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少

包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息；

[0108] 查找单元 42，用于从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥；

[0109] 处理单元 43，用于利用所述查找单元 42 查找到的密钥还原和 / 或验证处理后的种子信息；

[0110] 身份验证单元 44，用于根据还原结果或者验证结果确定身份验证是否通过。

[0111] 具体实施时，所述身份验证信息中还包括所述验证信息生成设备的设备标识；所述身份验证请求中还携带有所述设备标识；以及

[0112] 查找单元 42，可以用于根据所述设备标识，从自身存储的设备标识与密钥的对应关系中查找所述设备标识对应的密钥；将所述设备标识对应的密钥作为所述验证信息生成设备中存储的密钥对应的密钥。

[0113] 其中，种子信息可以是任何计算机系统可处理的信息，较佳的，种子信息可以但不限于为验证信息生成设备的当前时间；以及

[0114] 身份验证单元 44，可以用于在确定还原出的验证信息生成设备的当前时间与当前时间之间的间隔在预设时间间隔范围之内时，确定身份验证通过；或者确定对所述验证信息生成设备的当前时间的验证通过时，确定身份验证通过。

[0115] 具体实施时，处理后的种子信息为所述验证信息生成设备利用存储的密钥对所述种子信息进行加密、签名或者哈希运算得到的；以及

[0116] 处理单元 43，可以用于利用查找单元 42 查找到的密钥对加密的种子信息进行解密得到所述种子信息；或者利用查找单元 42 查找到的密钥对已签名的种子信息进行验证；或者利用查找单元 42 查找到的密钥对所述种子信息进行哈希运算后得到的哈希值进行验证。

[0117] 为了描述的方便，以上各部分按照功能划分为各模块（或单元）分别描述。当然，在实施本发明时可以把各模块（或单元）的功能在同一个或多个软件或硬件中实现，例如上述实施例四提供的身份验证装置可以设置在身份验证服务器中。

[0118] 实施例五、

[0119] 如图 5 所示，为本发明实施例提供的终端侧实施的身份验证方法的实施流程示意图，可以包括：

[0120] S51、在访问互联网应用需要进行身份验证时，向网络侧的身份验证服务器发送身份验证请求；

[0121] 在所述身份验证请求中携带有从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息；

[0122] S52、接收所述互联网应用对应的应用服务器返回的允许 / 拒绝访问的响应消息；

[0123] 所述响应消息为所述应用服务器根据所述身份验证服务器返回的身份验证结果发送的。

[0124] 较佳的，所述身份验证信息可以为图形码，基于此，本发明实施例中，可以按照以下方法从所述验证信息生成设备获取所述用户身份验证信息：

[0125] 扫描所述验证信息生成设备显示的所述图形码。

[0126] 实施例六、

[0127] 如图 6 所示，为本发明实施例提供的身份验证装置的结构示意图，可以包括：

[0128] 发送单元 61，用于在访问互联网应用需要进行身份验证时，向网络侧的身份验证服务器发送身份验证请求，所述身份验证请求中携带有从验证信息生成设备获取的用户身份验证信息，所述身份验证信息中至少包括所述验证信息生成设备利用存储的密钥对种子信息进行处理得到的处理后的种子信息，所述种子信息为计算机系统能够处理的任一信息；

[0129] 接收单元 62，用于接收所述互联网应用对应的应用服务器返回的允许 / 拒绝访问的响应消息，所述响应消息为所述应用服务器根据所述身份验证服务器返回的身份验证结果发送的。

[0130] 较佳的，所述身份验证信息为图形码。则本发明实施例提供的终端侧的身份验证装置，还可以包括：摄像单元，用于扫描所述所述验证信息生成设备显示的所述图形码。

[0131] 为了描述的方便，以上各部分按照功能划分为各模块（或单元）分别描述。当然，在实施本发明时可以把各模块（或单元）的功能在同一个或多个软件或硬件中实现，例如上述实施例六提供的身份验证装置可以设置在终端设备中。

[0132] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序信息的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[0133] 本发明是参照根据本发明实施例的方法、设备（系统）和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

[0134] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

[0135] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

[0136] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0137] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

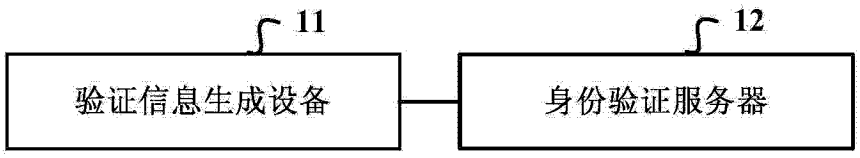

11
12
验证信息生成设备
身份验证服务器

图 1

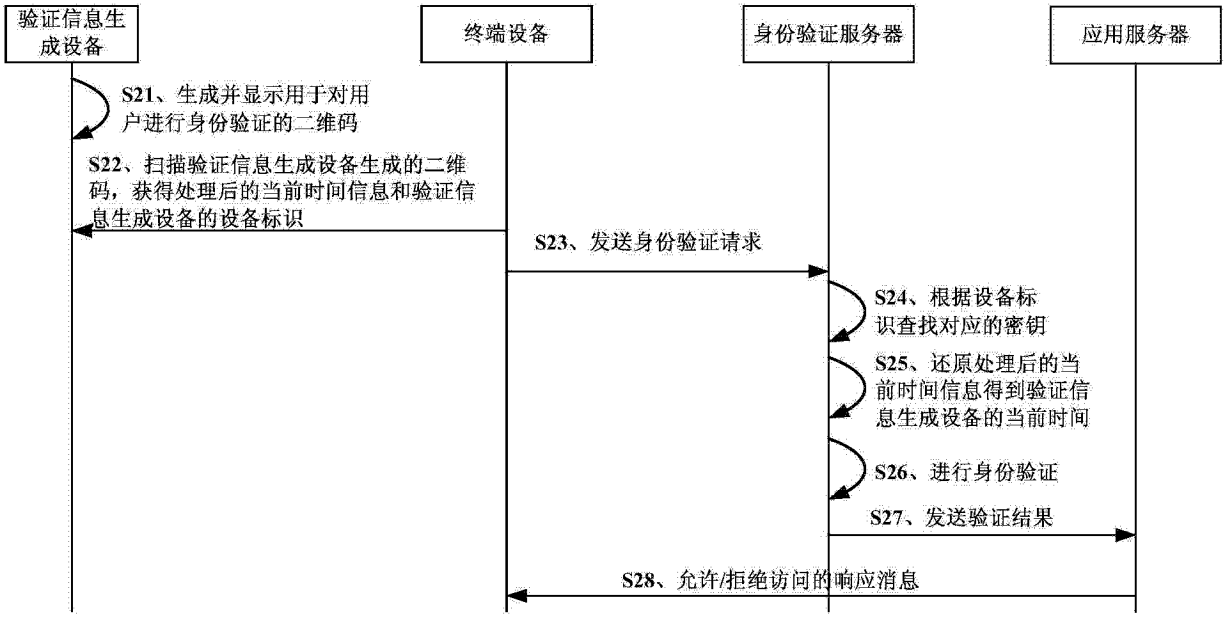

验证信息生成设备
终端设备
身份验证服务器
应用服务器
S21、生成并显示用于对用户进行身份验证的二维码
S22、扫描验证信息生成设备生成的二维码，获得处理后的当前时间信息和验证信息生成设备的设备标识
S23、发送身份验证请求
S24、根据设备标识查找对应的密钥
S25、还原处理后的当前时间信息得到验证信息生成设备的当前时间
S26、进行身份验证
S27、发送验证结果
S28、允许/拒绝访问的响应消息

图 2

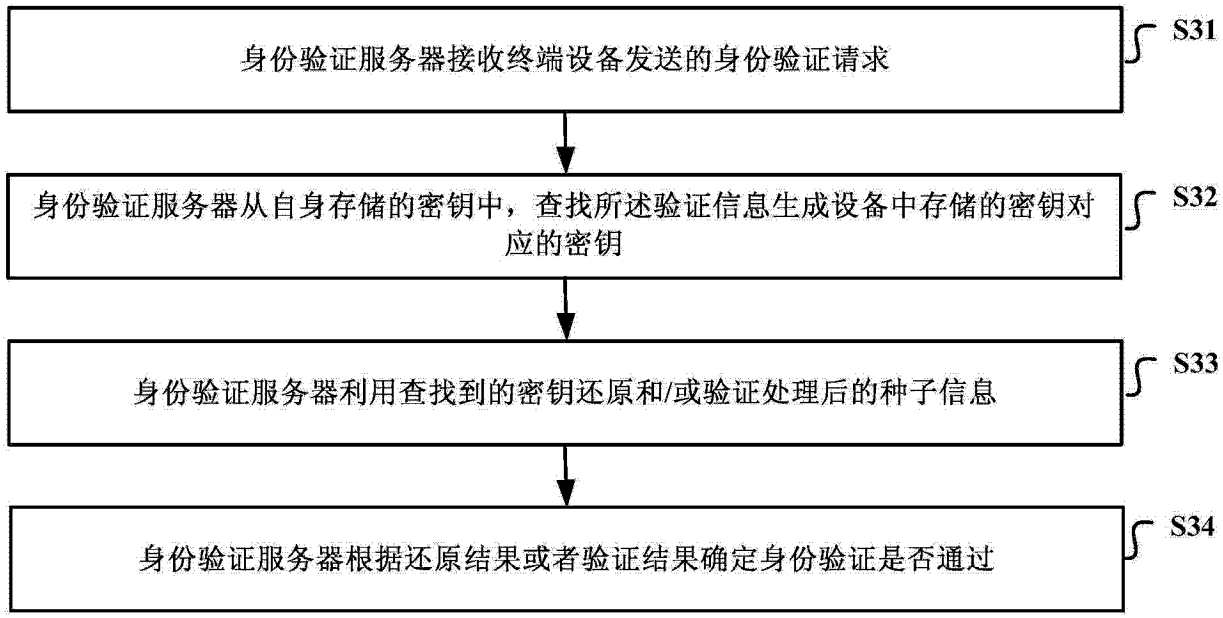

身份验证服务器接收终端设备发送的身份验证请求
S31
身份验证服务器从自身存储的密钥中，查找所述验证信息生成设备中存储的密钥对应的密钥
S32
身份验证服务器利用查找到的密钥还原和/或验证处理后的种子信息
S33
身份验证服务器根据还原结果或者验证结果确定身份验证是否通过
S34

图 3

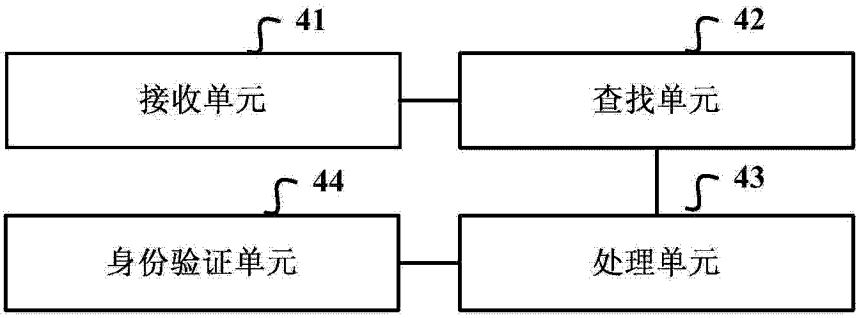

41
42
接收单元
查找单元
44
43
身份验证单元
处理单元

图 4

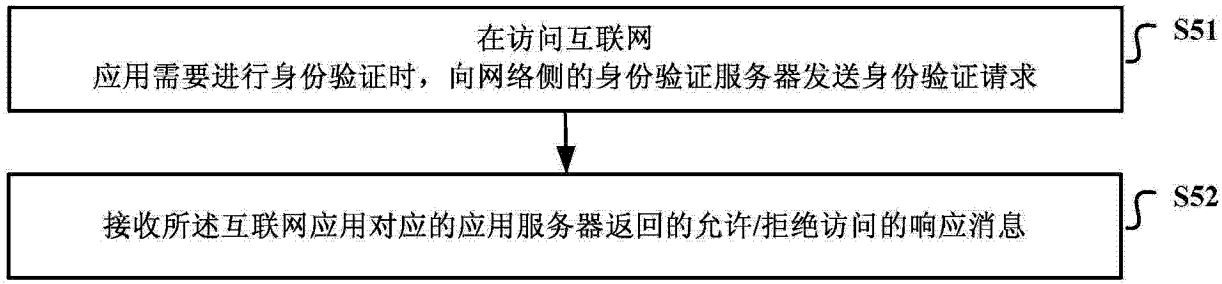

在访问互联网
应用需要进行身份验证时，向网络侧的身份验证服务器发送身份验证请求
S51
接收所述互联网应用对应的应用服务器返回的允许/拒绝访问的响应消息
S52

图 5

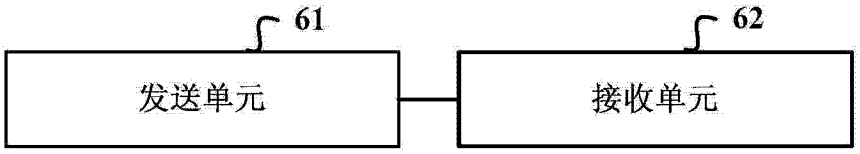

61
62
发送单元
接收单元

图 6