[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200910077314.0

[43] 公开日 2009 年 7 月 22 日

[11] 公开号 CN 101488111A

[22] 申请日 2009.2.17
[21] 申请号 200910077314.0
[71] 申请人 普天信息技术研究院有限公司
地址 100080 北京市海淀区海淀北二街 6 号
[72] 发明人 刘道斌

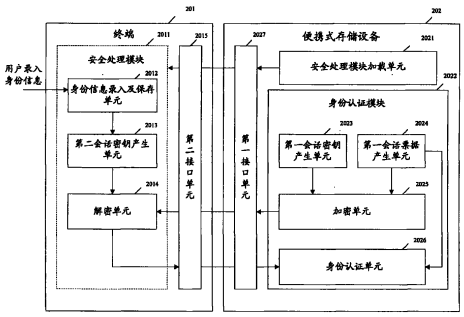
[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 王一斌 王 琦
权利要求书 3 页 说明书 9 页 附图 4 页

[54] 发明名称

一种身份认证方法和系统

[57] 摘要

本发明公开了一种身份认证方法，先由便携式存储设备将与自身相同的会话密钥产生机制、以及与自身的加密机制对应的解密机制加载至终端；然后，便携式存储设备使用自身的会话密钥对自身产生的会话票据进行加密；终端按照与便携式存储设备相同的会话密钥产生机制产生会话密钥，并使用自身的会话密钥解密来自便携式存储设备的加密的会话票据，再将解密后得到的会话票据返回给便携式存储设备；此后，便携式存储设备即可比较接收到的会话票据与自身产生的会话票据，以实现身份认证。 同时，本发明还公开了一种身份认证系统，采用该方法和系统可提高终端与便携式存储设备之间的身份认证的安全性。



1、一种身份认证系统，该系统包括：终端、便携式存储设备，其特征在于，

所述便携式存储设备包括：身份认证模块、安全处理模块加载单元，其中，

身份认证模块使用自身的会话密钥对自身产生的会话票据进行加密；

安全处理模块加载单元在所述终端中加载安全处理模块；

安全处理模块携带与身份认证模块相同的会话密钥产生机制，并与身份认证模块按照相同的会话密钥产生机制产生各自的会话密钥；安全处理模块还携带与身份认证模块中的加密机制对应的解密机制，并使用自身的会话密钥解密来自身份认证模块的加密的会话票据，并将解密后得到的会话票据返回给身份认证模块；

且，身份认证模块还用于比较接收到的会话票据与自身产生的会话票据。

2、根据权利要求 1 所述的系统，其特征在于，所述身份认证模块包括：第一会话密钥产生单元、第一会话票据产生单元、加密单元，身份认证单元；所述安全处理模块包括：身份信息录入及保存单元、第二会话密钥产生单元、解密单元；其中，

第一会话密钥产生单元，用于以便携式存储设备自身的身份信息为密钥种子产生第一会话密钥；

第一会话票据产生单元，用于产生第一会话票据并将第一会话票据发送给加密单元和身份认证单元；

加密单元，用于使用第一会话密钥加密第一会话票据，将加密的第一会话票据发送给解密单元；

身份信息录入及保存单元，用于用户录入身份信息及保存用户录入的身份信息；

第二会话密钥产生单元，用于以用户录入的身份信息为密钥种子按照第

一会话密钥的产生机制产生第二会话密钥;

解密单元,用于使用第二会话密钥按照与加密机制对应的解密机制解密来自加密单元的加密的第一会话票据,并将解密后得到的第二会话票据发送给身份认证单元;

身份认证单元,用于比较来自解密单元的第二会话票据和来自第一会话票据产生单元的第一会话票据是否一致,如果一致则对终端的身份认证通过;否则,身份认证失败。

3、根据权利要求 1 或 2 所述的系统,其特征在于,

所述终端为 PC 机、或手机、或自动柜员机 ATM;

所述便携式存储设备为智能卡、或存储卡、或 USBKey。

4、根据权利要求 2 所述的系统,其特征在于,所述终端和所述便携式存储设备之间采用 ISO7816 接口协议、或通用存储卡接口协议、或 USB 接口协议、或无线接口协议。

5、根据权利要求 2 所述的系统,其特征在于,所述身份信息为个人识别号码 PIN、或生物特征信息。

6、根据权利要求 2 所述的系统,其特征在于,所述身份信息录入及保存单元包括软键盘。

7、根据权利要求 2 所述的系统,其特征在于,所述第一会话票据和第二会话票据依据当前会话时间产生。

8、一种身份认证方法,其特征在于,该方法包括以下步骤:

便携式存储设备将与自身相同的会话密钥产生机制、以及与自身的加密机制对应的解密机制加载至终端;

便携式存储设备使用自身的会话密钥对自身产生的会话票据进行加密;

终端按照与便携式存储设备相同的会话密钥产生机制产生会话密钥,并使用自身的会话密钥解密来自便携式存储设备的加密的会话票据,然后将解密后得到的会话票据返回给便携式存储设备;

便携式存储设备比较接收到的会话票据与自身产生的会话票据。

9、根据权利要求 8 所述的方法，其特征在于，

所述终端与便携式存储设备按照相同的会话密钥产生机制产生各自的会话密钥的方法为：便携式存储设备以自身的身份信息为密钥种子产生第一会话密钥，终端以用户录入的身份信息为密钥种子按照第一会话密钥的产生机制产生第二会话密钥；

所述便携式存储设备使用自身的会话密钥对自身产生的会话票据进行加密的方法为：便携式存储设备产生第一会话票据，并使用第一会话密钥加密第一会话票据；

所述终端使用自身的会话密钥解密来自便携式存储设备的加密的会话票据的方法为：终端使用第二会话密钥按照与加密机制对应的解密机制解密来自便携式存储设备的加密的第一会话票据；

所述便携式存储设备比较接收到的会话票据和自身产生的会话票据的方法为：便携式存储设备比较来自终端的第二会话票据和自身产生的第一会话票据是否一致，如果一致则对终端的身份认证通过；否则，身份认证失败。

10、根据权利要求 8 或 9 所述的方法，其特征在于，所述终端为 PC 机、或手机、或自动柜员机 ATM；

所述便携式存储设备为智能卡、或存储卡、或 USBKey。

11、根据权利要求 9 所述的方法，其特征在于，所述终端和便携式存储设备通过 ISO7816 接口、或通用存储卡接口、或 USB 接口、或无线接口连接。

12、根据权利要求 9 所述的方法，其特征在于，所述身份信息为个人识别号码 PIN、或生物特征信息。

13、根据权利要求 9 所述的方法，其特征在于，所述用户录入身份信息的方法为：用户使用软键盘录入身份信息。

14、根据权利要求 9 所述的方法，其特征在于，所述第一会话票据和第二会话票据依据当前会话时间产生。

一种身份认证方法和系统

技术领域

本发明涉及信息安全领域，特别涉及一种身份认证方法和系统。

背景技术

当终端（如PC机、手机等）对便携式存储设备（如智能卡、存储卡等）进行访问时，便携式存储设备需要对访问的终端进行身份认证，图1为现有技术中身份认证方法的流程图。如图1所示，现有技术中身份认证的方法包括以下步骤：

步骤101，当终端探测到便携式存储设备时，给便携式存储设备上电，便携式存储设备向请求访问的终端发送身份认证请求。

步骤102，终端收到便携式存储设备发送的身份认证请求后，通过人机交互界面提示用户输入个人识别号码（PIN），用户根据人机交互界面的提示输入PIN。

步骤103，终端向便携式存储设备返回身份认证请求响应，该身份认证请求响应以明文方式携带用户输入的PIN。

步骤104，便携式存储设备收到用户输入的PIN后，对比用户输入的PIN、以及自身预先存储的PIN，如果二者一致，则身份认证通过；否则，身份认证失败。

步骤105，便携式存储设备向终端返回身份认证结果，如果身份认证通过，则该终端可对该便携式存储设备进行访问；否则，终端无法访问。

在现有的身份认证方法中，由于终端将用户输入的PIN以明文方式发送给便携式存储设备以进行身份认证，终端发送的PIN很容易被非法用户窃取或截获，导致非法用户也有可能获得访问该便携式存储设备的权限，因此

现有的身份认证方法的安全性不高。

发明内容

有鉴于此，本发明的主要目的在于提供一种身份认证方法，以提高终端与便携式存储设备之间的身份认证的安全性。

本发明的另一目的在于提供一种身份认证系统，以提高终端与便携式存储设备之间的身份认证的安全性。

为达到上述目的，本发明的技术方案具体是这样实现的：

一种身份认证系统，该系统包括：终端、便携式存储设备，

所述便携式存储设备包括：身份认证模块、安全处理模块加载单元，其中，

身份认证模块使用自身的会话密钥对自身产生的会话票据进行加密；

安全处理模块加载单元在所述终端中加载安全处理模块；

安全处理模块携带与身份认证模块相同的会话密钥产生机制，并与身份认证模块按照相同的会话密钥产生机制产生各自的会话密钥；安全处理模块还携带与身份认证模块中的加密机制对应的解密机制，并使用自身的会话密钥解密来自身份认证模块的加密的会话票据，并将解密后得到的会话票据返回给身份认证模块；

且，身份认证模块还用于比较接收到的会话票据与自身产生的会话票据。

所述身份认证模块包括：第一会话密钥产生单元、第一会话票据产生单元、加密单元，身份认证单元；所述安全处理模块包括：身份信息录入及保存单元、第二会话密钥产生单元、解密单元；其中，

第一会话密钥产生单元，用于以便携式存储设备自身的身份信息为密钥种子产生第一会话密钥；

第一会话票据产生单元，用于产生第一会话票据并将第一会话票据发送给加密单元和身份认证单元；

加密单元，用于使用第一会话密钥加密第一会话票据，将加密的第一会话票据发送给解密单元；

身份信息录入及保存单元，用于用户录入身份信息及保存用户录入的身份信息；

第二会话密钥产生单元，用于以用户录入的身份信息为密钥种子按照第一会话密钥的产生机制产生第二会话密钥；

解密单元，用于使用第二会话密钥按照与加密机制对应的解密机制解密来自加密单元的加密的第一会话票据，并将解密后得到的第二会话票据发送给身份认证单元；

身份认证单元，用于比较来自解密单元的第二会话票据和来自第一会话票据产生单元的第一会话票据是否一致，如果一致则对终端的身份认证通过；否则，身份认证失败。

所述终端为 PC 机、或手机、或自动柜员机 ATM；

所述便携式存储设备为智能卡、或存储卡、或 USBKey。

所述终端和所述便携式存储设备之间采用 ISO7816 接口协议、或通用存储卡接口协议、或 USB 接口协议、或无线接口协议。

所述身份信息为个人识别号码 PIN、或生物特征信息。

所述身份信息录入及保存单元包括软键盘。

所述第一会话票据和第二会话票据依据当前会话时间产生。

一种身份认证方法，该方法包括以下步骤：

便携式存储设备将与自身相同的会话密钥产生机制、以及与自身的加密机制对应的解密机制加载至终端；

便携式存储设备使用自身的会话密钥对自身产生的会话票据进行加密；

终端按照与便携式存储设备相同的会话密钥产生机制产生会话密钥，并使用自身的会话密钥解密来自便携式存储设备的加密的会话票据，然后将解密后得到的会话票据返回给便携式存储设备；

便携式存储设备比较接收到的会话票据与自身产生的会话票据。

所述终端与便携式存储设备按照相同的会话密钥产生机制产生各自的会话密钥的方法为：便携式存储设备以自身的身份信息为密钥种子产生第一会话密钥，终端以用户录入的身份信息为密钥种子按照第一会话密钥的产生机制产生第二会话密钥；

所述便携式存储设备使用自身的会话密钥对自身产生的会话票据进行加密的方法为：便携式存储设备产生第一会话票据，并使用第一会话密钥加密第一会话票据；

所述终端使用自身的会话密钥解密来自便携式存储设备的加密的会话票据的方法为：终端使用第二会话密钥按照与加密机制对应的解密机制解密来自便携式存储设备的加密的第一会话票据；

所述便携式存储设备比较接收到的会话票据和自身产生的会话票据的方法为：便携式存储设备比较来自终端的第二会话票据和自身产生的第一会话票据是否一致，如果一致则对终端的身份认证通过；否则，身份认证失败。

所述终端为 PC 机、或手机、或自动柜员机 ATM；

所述便携式存储设备为智能卡、或存储卡、或 USBKey。

所述终端和便携式存储设备通过 ISO7816 接口、或通用存储卡接口、或 USB 接口、或无线接口连接。

所述身份信息为个人识别号码 PIN、或生物特征信息。

所述用户录入身份信息的方法为：用户使用软键盘录入身份信息。

所述第一会话票据和第二会话票据依据当前会话时间产生。

由上述的技术方案可见，本发明先由便携式存储设备将与自身相同的会话密钥产生机制、以及与自身的加密机制对应的解密机制加载至终端；然后，便携式存储设备使用自身的会话密钥对自身产生的会话票据进行加密；相应地，终端按照与便携式存储设备相同的会话密钥产生机制产生会话密钥，并使用自身的会话密钥解密来自便携式存储设备的加密的会话票据，再将解密后得到的会话票据返回给便携式存储设备；此后，便携式存储设备即可比较接收到的会话票据与自身产生的会话票据，以实现身份认证。这样，由于终

端和便携式存储设备之间不直接传送用户输入的 PIN，避免了例如 PIN 等身份信息被非法用户窃取，因此提高了终端与便携式存储设备之间的身份认证的安全性。

附图说明

图 1 为现有技术中身份认证方法的流程图；

图 2 为本发明所提供的一种身份认证系统的结构图；

图 3 为本发明所提供的一种身份认证方法的流程图；

图 4 为本发明所提供的一种身份认证方法的实施例的流程图。

具体实施方式

为使本发明的目的、技术方案及优点更加清楚明白，以下参照附图并举实施例，对本发明进一步详细说明。

图 2 为本发明所提供的一种身份认证系统的结构图，如图 2 所示，该身份认证系统包括：终端 201、便携式存储设备 202。

终端 201 至少包括：安全处理模块 2011 和第二接口单元 2015；便携式存储设备 202 至少包括：安全处理模块加载单元 2021、身份认证模块 2022、第一接口单元 2027。

安全处理模块加载单元 2021 通过第一接口单元 2027 和第二接口单元 2015 将安全处理模块 2011 加载至终端 201，安全处理模块 2011 携带与身份认证模块 2022 相同的会话密钥产生机制、以及与身份认证模块中的加密机制对应的解密机制；安全处理模块 2011 与身份认证模块 2022 按照相同的会话密钥产生机制产生各自的会话密钥；身份认证模块 2022 使用自身的会话密钥对自身产生的会话票据进行加密，安全处理模块 2011 使用自身的会话密钥解密来自身份认证模块 2022 的加密的会话票据，并将解密后得到的会话票据通过第一接口单元 2027 和第二接口单元 2015 返回给身份认证模块 2022；身份认证模块 2022 比较接收到的会话票据和自身产生的会话票据。

安全处理模块 2011 至少包括：身份信息录入及保存单元 2012、第二会话密钥产生单元 2013、解密单元 2014；身份认证模块 2022 至少包括：第一会话密钥产生单元 2023、第一会话票据产生单元 2024、加密单元 2025，身份认证单元 2026。

其中，第一会话密钥产生单元 2023，用于以便携式存储设备 202 自身的身份信息为密钥种子产生第一会话密钥；第一会话票据产生单元 2024，用于产生第一会话票据并将第一会话票据发送给加密单元 2025 和身份认证单元 2026；加密单元 2025，用于使用第一会话密钥加密第一会话票据，将加密的第一会话票据通过第一接口单元 2027 和第二接口单元 2015 发送给解密单元 2014；身份信息录入及保存单元 2012，用于用户录入身份信息并保存用户录入的身份信息；第二会话密钥产生单元 2013，用于以用户录入的身份信息为密钥种子按照第一会话密钥的产生机制产生第二会话密钥；解密单元 2014，用于使用第二会话密钥按照与加密机制对应的解密机制解密来自加密单元 2025 的第一会话票据，并将解密后得到的第二会话票据通过第一接口单元 2027 和第二接口单元 2015 发送给身份认证单元 2026；身份认证单元 2026，用于比较来自解密单元 2014 的第二会话票据和来自第一会话票据产生单元 2024 的第一会话票据是否一致，如果一致则对终端 201 的身份认证通过；否则，身份认证失败。

另外，需要说明的是，当身份认证结束后，用于本次身份认证的安全处理模块 2011 将会自动从终端 201 中删除，当进行下次身份认证时，会有新的安全处理模块被加载至终端 201。

在实际应用中，终端 201 可为 PC 机、手机、自动柜员机 ATM 等，相应地，连接终端 201 和便携式存储设备 202 的第一接口单元 2027 和第二接口单元 2015 可采用 ISO7816 接口协议、通用存储卡接口协议、USB 接口协议，若终端 201 和便携式存储设备 202 中被置入无线通信模块（图未示出），连接终端 201 和便携式存储设备 202 的第一接口单元 2027 和第二接口单元 2015 可采用无线接口协议。

在实际应用中，用于身份认证的身份信息可为 PIN，也可为生物特征信息，例如指纹信息、虹膜信息等。当身份信息为 PIN 时，身份认证录入及保存单元 2012 可包括软键盘，用于用户输入 PIN。

基于上述身份认证系统，图 3 为本发明所提供的一种身份认证方法的流程图，如图 3 所示，该身份认证方法包括以下步骤：

步骤 301，便携式存储设备将与自身相同的会话密钥产生机制、以及与自身的加密机制对应的解密机制加载至终端。

步骤 302，终端和便携式存储设备按照相同的会话密钥产生机制产生各自的会话密钥，具体为，便携式存储设备以自身的身份信息为密钥种子产生第一会话密钥，终端以用户录入的身份信息为密钥种子按照第一会话密钥的产生机制产生第二会话密钥。

步骤 303，便携式存储设备使用自身的会话密钥对自身产生的会话票据进行加密，终端使用自身的会话密钥解密来自便携式存储设备的加密的会话票据，并将解密后得到的会话票据返回给便携式存储设备，具体为，便携式存储设备产生第一会话票据，并使用第一会话密钥加密第一会话票据，将加密的第一会话票据发送给终端，终端使用第二会话密钥按照与加密机制对应的解密机制解密来自便携式存储设备的加密的第一会话票据。

步骤 304，便携式存储设备比较接收到的会话票据与自身产生的会话票据，具体为，便携式存储设备比较来自终端的第二会话票据和自身产生的第一会话票据是否一致，如果一致则对终端的身份认证通过；否则，身份认证失败。

下面通过一个实施例详述本发明所提供的一种身份认证方法。

图 4 为本发明所提供的一种身份认证方法的实施例的流程图，如图 4 所示，该身份认证方法包括以下步骤：

步骤 401，便携式存储设备将与自身相同的会话密钥产生机制、以及与自身的加密机制对应的解密机制加载至终端。

当终端探测到便携式存储设备时，给便携式存储设备上电，此方法可按

照现有技术的方法，然后便携式存储设备立即将与自身相同的会话密钥产生机制、以及与自身的加密机制对应的解密机制加载至终端。

步骤 402，用户输入 PIN，终端保存用户输入的 PIN。

较佳地，在本实施例中，用户使用软键盘录入 PIN。使用软键盘的益处为：当用户每次录入 PIN 时，软键盘中各个字符的位置是不相同的，若终端中存在木马程序，木马程序无法通过记录用户敲击字符的顺序来窃取 PIN。

步骤 403，终端向便携式存储设备发送身份认证请求。

步骤 404，便携式存储设备产生第一会话票据 T 并以便携式存储设备自身的 PIN 为密钥种子产生第一会话密钥 K。

在现有技术中，会话票据的形式通常是一串随机数，较佳地，在本实施例中，可依据当前的会话时间产生第一会话票据 T，同时，产生第一会话密钥 K 的方法与现有技术中产生密钥的方法相同，例如采用哈希运算、异或运算等。

步骤 405，便携式存储设备使用第一会话密钥 K 加密第一会话票据 T，得到加密的第一会话票据 E（T）。

加密的方法通常采用现有技术中的加密方法。

步骤 406，便携式存储设备向终端发送身份认证请求响应，身份认证请求响应携带步骤 405 中得到的加密的第一会话票据 E（T）。

步骤 407，终端中的安全认证模块以步骤 402 中用户输入的 PIN 为密钥种子，按照第一会话密钥的产生机制产生第二会话密钥 K'。

步骤 408，终端使用步骤 406 中产生的第二会话密钥 K'按照与加密机制对应的解密机制解密接收到的加密的第一会话票据 E（T），得到第二会话票据 T'。

步骤 409，终端将第二会话票据 T'发送给便携式存储设备。

步骤 410，便携式存储设备验证接收到的第二会话票据 T'和步骤 404 中产生的第一会话票据 T 是否一致，如果一致则对终端的身份认证通过。

步骤 411，便携式存储设备向终端返回身份认证结果，如果身份认证通

过，则允许终端对便携式存储设备进行访问；否则，进入下一周期的认证流程或拒绝终端对便携式存储设备的访问。

至此，本流程结束。

综上所述，以上仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

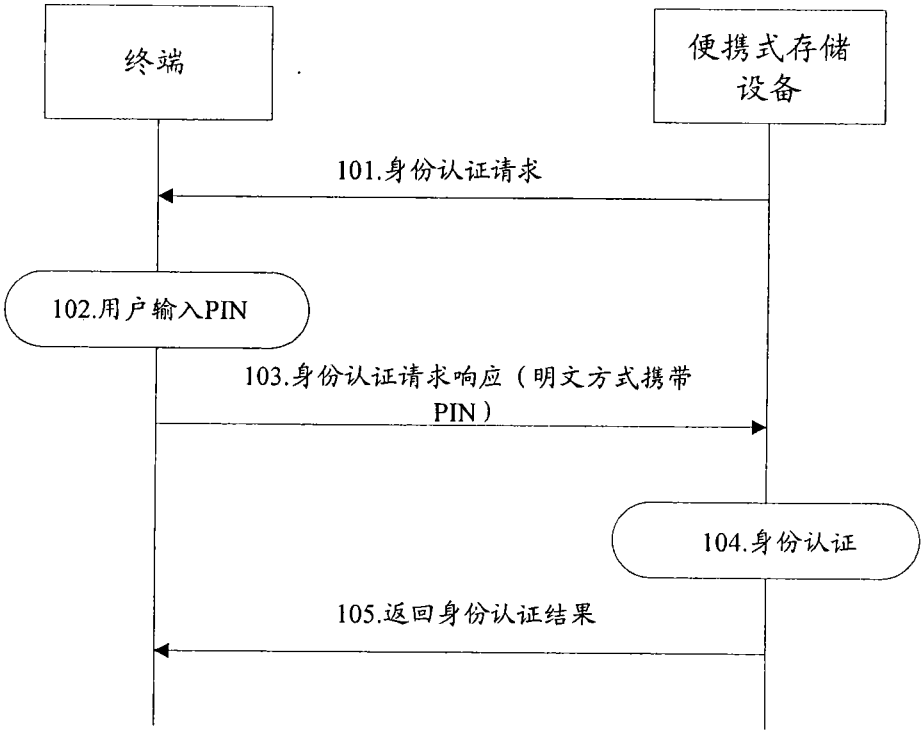

终端
便携式存储设备
101.身份认证请求
102.用户输入PIN
103.身份认证请求响应（明文方式携带PIN）
104.身份认证
105.返回身份认证结果

图 1

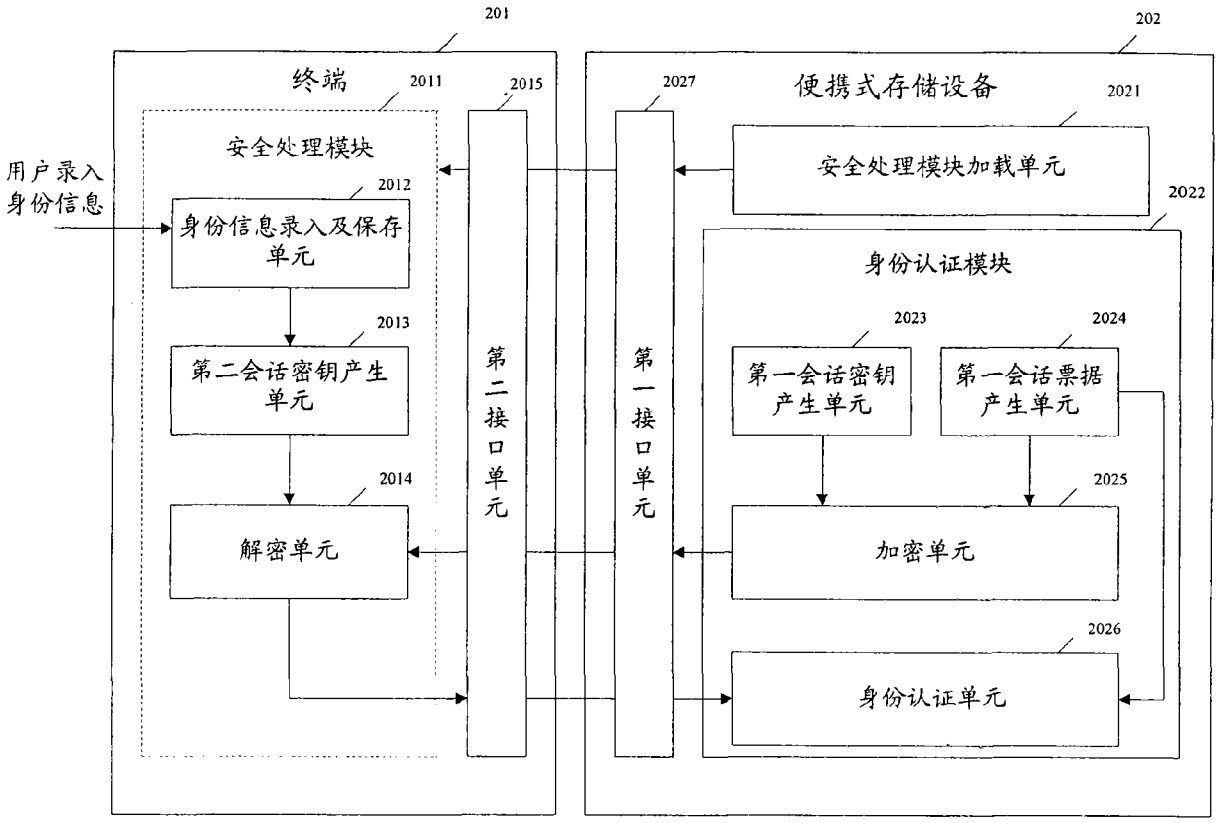

201
终端
2011
2015
安全处理模块
用户录入
身份信息
2012
身份信息录入及保存
单元
2013
第二会话密钥产生
单元
2014
解密单元
第二接口单元
202
便携式存储设备
2027
2021
安全处理模块加载单元
2022
身份认证模块
2023
2024
第一会话密钥
产生单元
第一会话票据
产生单元
2025
加密单元
2026
身份认证单元
第一接口单元

图 2

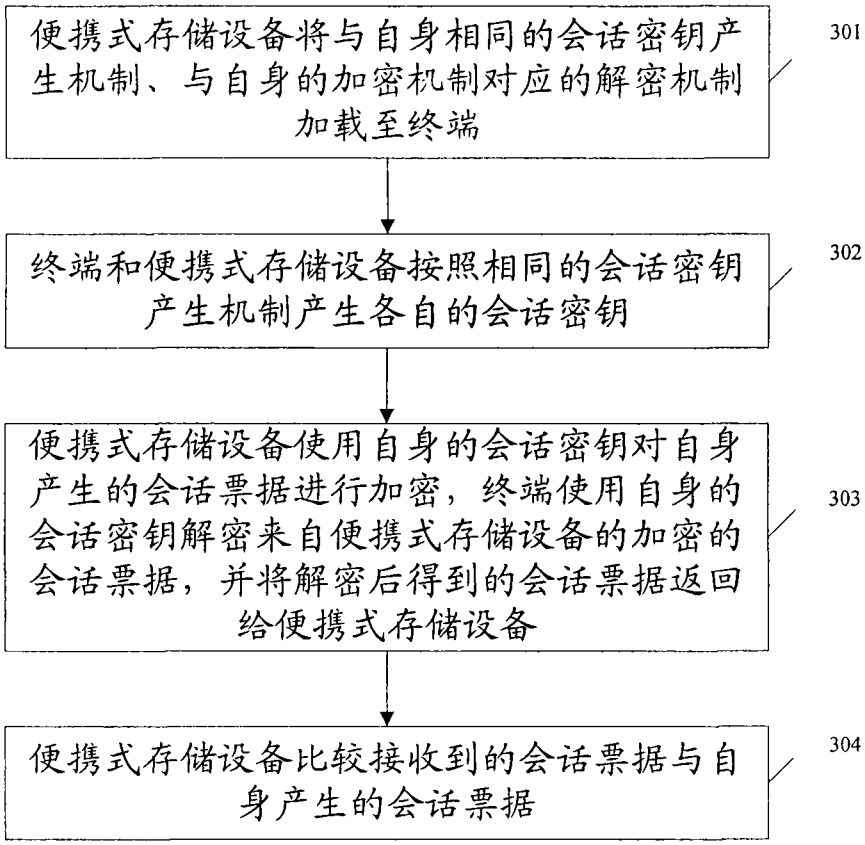

便携式存储设备将与自身相同的会话密钥产生机制、与自身的加密机制对应的解密机制加载至终端
301
终端和便携式存储设备按照相同的会话密钥产生机制产生各自的会话密钥
302
便携式存储设备使用自身的会话密钥对自身产生的会话票据进行加密，终端使用自身的会话密钥解密来自便携式存储设备的加密的会话票据，并将解密后得到的会话票据返回给便携式存储设备
303
便携式存储设备比较接收到的会话票据与自身产生的会话票据
304

图 3

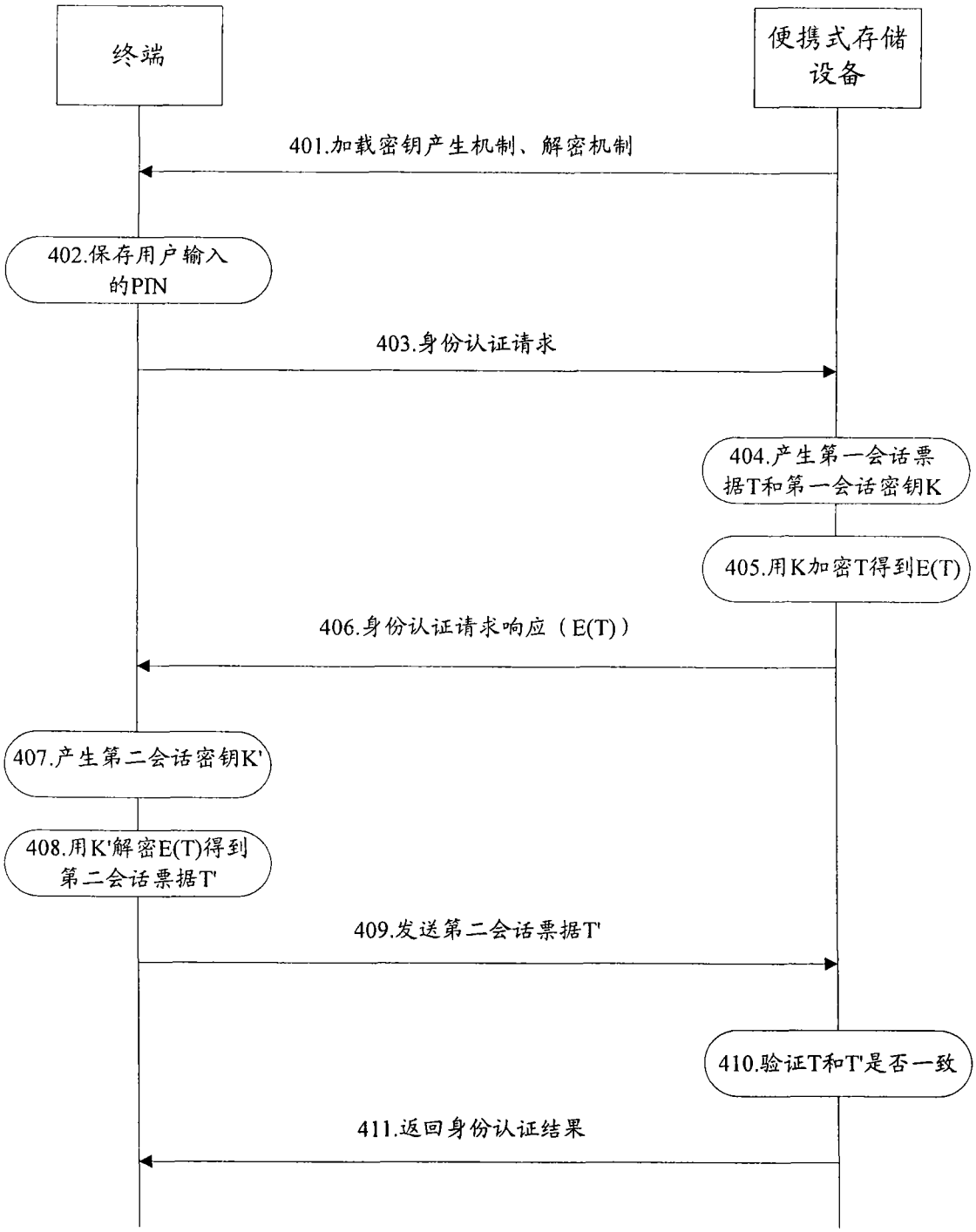

终端
便携式存储设备
401.加载密钥产生机制、解密机制
402.保存用户输入的PIN
403.身份认证请求
404.产生第一会话票据T和第一会话密钥K
405.用K加密T得到E(T)
406.身份认证请求响应（E(T)）
407.产生第二会话密钥K'
408.用K'解密E(T)得到第二会话票据T'
409.发送第二会话票据T'
410.验证T和T'是否一致
411.返回身份认证结果

图 4