(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 103888243 A
(43)申请公布日 2014.06.25

(21)申请号 201410149134.X

(22)申请日 2014.04.15

(71)申请人 飞天诚信科技股份有限公司
地址 100085 北京市海淀区学清路9号汇智大厦B楼17层

(72)发明人 陆舟 于华章

(51)Int.Cl.
H04L 9/00(2006.01)
H04L 29/06(2006.01)

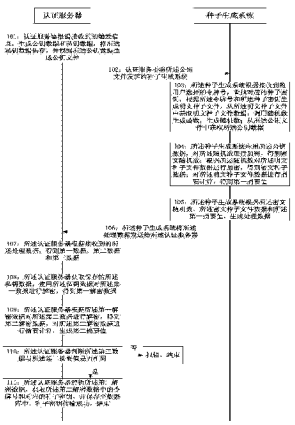
权利要求书2页 说明书11页 附图5页

(54)发明名称

一种种子密钥安全传输的方法

(57)摘要

本发明公开了一种种子密钥安全传输的方法，属于信息安全领域。所述方法包括：认证服务器根据触发信息生成公私钥数据，将私钥数据保存，将公钥数据生成公钥文件并发送给种子生成系统，种子生成系统根据接收到的令牌号查找种子密钥，生成明文种子文件数据，生成随机数，根据公钥数据、明文种子文件数据和随机数生成处理数据，并发送给认证服务器，认证服务器根据处理数据得到第一数据、第二数据和第三数据，获取私钥数据，根据第一数据、第二数据计算得到第二摘要值，当第二摘要值与第三数据相同时，获取并保存第二解密数据的令牌号和种子密钥至数据库中，种子密钥传输成功。采用本发明的方案，保证了种子密钥在传输过程中的安全性。



CN 103888243 A

1. 一种种子密钥安全传输的方法，其特征在于，应用于种子生成系统和认证服务器组成的系统中，包括以下步骤：

步骤 A1：认证服务器根据接收到的触发信息，生成公钥数据和私钥数据，将所述私钥数据保存，并根据所述公钥数据生成公钥文件，并将所述公钥文件发送给种子生成系统；

步骤 A2：所述种子生成系统根据接收到的用户选择的令牌号，查找对应的种子密钥，根据所述令牌号和所述种子密钥生成明文种子文件，从所述明文种子文件中获取明文种子文件数据；调用随机数生成函数，生成随机数；从所述公钥文件中获取所述公钥数据；

步骤 A3：所述种子生成系统应用所述公钥数据，对所述随机数进行加密，得到密文随机数；根据所述随机数对所述明文种子文件数据进行加密，得到密文种子数据；对所述明文种子文件数据进行摘要计算，得到第一摘要值；

步骤 A4：所述种子生成系统根据所述密文随机数、所述密文种子文件数据和所述第一摘要值，生成处理数据，并将所述处理数据发送给所述认证服务器；

步骤 A5：所述认证服务器根据接收到的所述处理数据，得到第一数据、第二数据和第三数据；

步骤 A6：所述认证服务器获取保存的所述私钥数据，使用所述私钥数据对所述第一数据进行解密，得到第一解密数据；

步骤 A7：所述认证服务器根据所述第一解密数据对所述第二数据进行解密，得到第二解密数据，对所述第二解密数据进行摘要计算，生成第二摘要值；

步骤 A8：所述认证服务器判断所述第三数据与所述第二摘要值是否相同，如果是，则执行步骤 A9，否则报错，结束；

步骤 A9：所述认证服务器解析所述第二解密数据，获取所述第二解密数据中的令牌号和对应的种子密钥，并保存至数据库中，种子密钥传输成功，结束。

2. 根据权利要求 1 所述的方法，其特征在于，所述步骤 A1 中，所述根据接收到的触发信息，生成公钥数据和私钥数据，具体包括：认证服务器等待接收用户选择种子生成系统标识，当接收到用户选择的种子生成系统标识后，从预先保存的多条种子生成系统记录中获取对应的种子生成系统信息，根据所述种子生成系统信息，生成公钥数据和私钥数据。

3. 根据权利要求 2 所述的方法，其特征在于，所述根据所述种子生成系统信息，生成公钥数据和私钥数据，具体为：

步骤 a1：所述认证服务器根据所述种子生成系统信息中的种子生成系统标识，生成密码；

步骤 a2：所述认证服务器根据所述种子生成系统信息和密码，生成公私钥数据存储文件；

步骤 a3：所述认证服务器从公私钥数据存储文件中获取私钥对象，对所述私钥对象进行编码生成私钥数据；

步骤 a4：所述认证服务器解析所述公私钥数据存储文件中获取公钥数据。

4. 根据权利要求 3 所述的方法，其特征在于，所述步骤 a1，具体为：所述认证服务器将所述种子生成系统信息中的种子生成系统标识作为加密因子，应用预设加密算法对所述加密因子进行加密，生成密码。

5. 根据权利要求 3 所述的方法，其特征在于，所述步骤 a2，具体为：所述认证服务器调

用 cmd 命令，将所述种子生成系统信息中的种子生成系统标识和种子生成系统名称、过期时间、域名和密码写入公私钥数据存储文件中，生成公私钥数据存储文件。

6. 根据权利要求 1 所述的方法，其特征在于，所述步骤 A1 中，所述根据所述公钥数据生成公钥文件，具体为：将所述公钥数据按照预设格式写入公钥文件中。

7. 根据权利要求 1 所述的方法，其特征在于，所述步骤 A2 中，所述根据接收到的用户选择的令牌号，查找对应的种子密钥，具体为：所述种子生成系统预先生成多条包括令牌号和对应种子密钥的令牌数据，根据需要选择的令牌号，从所述令牌数据中获取与所述令牌号对应的种子密钥。

8. 根据权利要求 1 所述的方法，其特征在于，所述步骤 A2 中，所述从所述公钥文件中获取公钥数据，具体包括：所述种子生成系统从所述公钥文件中获取公钥数据，判断是否能够获取到所述公钥数据，如果是，则执行步骤 A3，否则报错，结束。

9. 根据权利要求 1 所述的方法，其特征在于，

所述步骤 A3 中，所述对所述随机数进行加密，得到密文随机数，具体为：对所述随机数进行加密，得到第二预设长度的密文随机数；

所述步骤 A3 中，所述对所述明文种子文件数据进行摘要计算，得到第一摘要值，具体为：对所述明文种子文件数据进行摘要计算，得到第三预设长度的第一摘要值；

对应的，所述步骤 A4 中，所述根据所述密文随机数、所述密文种子文件数据和所述第一摘要值，生成所述处理数据，具体为：将第二预设长度的所述密文随机数、所述密文种子文件数据和第三预设长度的所述第一摘要值进行顺序拼接，得到所述处理数据；

对应的，所述步骤 A5 中，所述根据接收到的所述处理数据，得到第一数据、第二数据和第三数据，具体为：将所述处理数据的前第二预设长度的数据作为第一数据，将所述处理数据的后第三预设长度的数据作为第三数据，将所述处理数据中除第一数据和第三数据外的数据作为第二数据。

10. 根据权利要求 9 所述的方法，其特征在于，所述步骤 A5 之前还包括：所述认证服务器判断接收到的所述处理数据的长度是否不为空且大于第二预设长度与第三预设长度之和，如果是，则执行步骤 A5，否则报错，结束。

11. 根据权利要求 1 所述的方法，其特征在于，所述步骤 A4 中，所述将所述处理数据发送给所述认证服务器，具体为：所述种子生成系统将所述处理数据提供给使用所述认证服务器的用户，当用户接收到所述处理数据后，通过访问所述认证服务器页面，将所述处理数据上传导入到所述认证服务器中。

12. 根据权利要求 1 所述的方法，其特征在于，所述步骤 A2 中，所述调用随机数生成函数，生成随机数，具体为：调用随机数生成函数，生成第一预设长度的随机数；

对应的，所述步骤 A3，还包括：所述认证服务器判断所述第一解密数据的长度是否为所述第一预设长度，如果是，则执行步骤 A4，否则报错，结束。

一种种子密钥安全传输的方法

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种种子密钥安全传输的方法。

背景技术

[0002] 动态令牌是用来生成动态口令的终端，动态口令是根据专门算法对内置的种子密钥等进行计算，生成的一个不可预测的随机数组合，采用动态口令的认证方式就是每次在用户登录时除了输入常规的静态口令外，还需要输入一个每次都会变化的动态口令，保证了用户登录的安全性。

[0003] 种子密钥是动态令牌的核心，是由种子生成系统生成后，传输并导入认证服务器中，现有技术无法保证种子密钥在传输过程中的安全性，因此种子密钥传输的安全性是亟待解决的问题。

发明内容

[0004] 本发明为解决现有技术中存在的问题，提供了一种种子密钥安全传输的方法。

[0005] 本发明采用的技术方案是：一种种子密钥安全传输的方法，应用于种子生成系统和认证服务器组成的系统中，包括以下步骤：

[0006] 步骤 A1：认证服务器根据接收到的触发信息，生成公钥数据和私钥数据，将所述私钥数据保存，并根据所述公钥数据生成公钥文件，并将所述公钥文件发送给种子生成系统；

[0007] 步骤 A2：所述种子生成系统根据接收到的用户选择的令牌号，查找对应的种子密钥，根据所述令牌号和所述种子密钥生成明文种子文件，从所述明文种子文件中获取明文种子文件数据；调用随机数生成函数，生成随机数；从所述公钥文件中获取所述公钥数据；

[0008] 步骤 A3：所述种子生成系统应用所述公钥数据，对所述随机数进行加密，得到密文随机数；根据所述随机数对所述明文种子文件数据进行加密，得到密文种子数据；对所述明文种子文件数据进行摘要计算，得到第一摘要值；

[0009] 步骤 A4：所述种子生成系统根据所述密文随机数、所述密文种子文件数据和所述第一摘要值，生成处理数据，并将所述处理数据发送给所述认证服务器；

[0010] 步骤 A5：所述认证服务器根据接收到的所述处理数据，得到第一数据、第二数据和第三数据；

[0011] 步骤 A6：所述认证服务器获取保存的所述私钥数据，使用所述私钥数据对所述第一数据进行解密，得到第一解密数据；

[0012] 步骤 A7：所述认证服务器根据所述第一解密数据对所述第二数据进行解密，得到第二解密数据，对所述第二解密数据进行摘要计算，生成第二摘要值；

[0013] 步骤 A8：所述认证服务器判断所述第三数据与所述第二摘要值是否相同，如果是，则执行步骤 A9，否则报错，结束；

[0014] 步骤 A9：所述认证服务器解析所述第二解密数据，获取所述第二解密数据中的令

牌号和对应的种子密钥，并保存至数据库中，种子密钥传输成功，结束。

[0015] 所述步骤 A1 中，所述根据接收到的触发信息，生成公钥数据和私钥数据，具体包括：认证服务器等待接收用户选择种子生成系统标识，当接收到用户选择的种子生成系统标识后，从预先保存的多条种子生成系统记录中获取对应的种子生成系统信息，根据所述种子生成系统信息，生成公钥数据和私钥数据。

[0016] 所述根据所述种子生成系统信息，生成公钥数据和私钥数据，具体为：

[0017] 步骤 a1：所述认证服务器根据所述种子生成系统信息中的种子生成系统标识，生成密码；

[0018] 步骤 a2：所述认证服务器根据所述种子生成系统信息和密码，生成公私钥数据存储文件；

[0019] 步骤 a3：所述认证服务器从公私钥数据存储文件中获取私钥对象，对所述私钥对象进行编码生成私钥数据；

[0020] 步骤 a4：所述认证服务器解析所述公私钥数据存储文件中获取公钥数据。

[0021] 所述步骤 a1，具体为：所述认证服务器将所述种子生成系统信息中的种子生成系统标识作为加密因子，应用预设加密算法对所述加密因子进行加密，生成密码。

[0022] 所述步骤 a2，具体为：所述认证服务器调用 cmd 命令，将所述种子生成系统信息中的种子生成系统标识和种子生成系统名称、过期时间、域名和密码写入公私钥数据存储文件中，生成公私钥数据存储文件。

[0023] 所述步骤 A1 中，所述根据所述公钥数据生成公钥文件，具体为：将所述公钥数据按照预设格式写入公钥文件中。

[0024] 所述步骤 A2 中，所述根据接收到的用户选择的令牌号，查找对应的种子密钥，具体为：所述种子生成系统预先生成多条包括令牌号和对应种子密钥的令牌数据，根据需要选择的令牌号，从所述令牌数据中获取与所述令牌号对应的种子密钥。

[0025] 所述步骤 A2 中，所述从所述公钥文件中获取公钥数据，具体包括：所述种子生成系统从所述公钥文件中获取公钥数据，判断是否能够获取到所述公钥数据，如果是，则执行步骤 A3，否则报错，结束。

[0026] 所述步骤 A3 中，所述对所述随机数进行加密，得到密文随机数，具体为：对所述随机数进行加密，得到第二预设长度的密文随机数；

[0027] 所述步骤 A3 中，所述对所述明文种子文件数据进行摘要计算，得到第一摘要值，具体为：对所述明文种子文件数据进行摘要计算，得到第三预设长度的第一摘要值；

[0028] 对应的，所述步骤 A4 中，所述根据所述密文随机数、所述密文种子文件数据和所述第一摘要值，生成所述处理数据，具体为：将第二预设长度的所述密文随机数、所述密文种子文件数据和第三预设长度的所述第一摘要值进行顺序拼接，得到所述处理数据；

[0029] 对应的，所述步骤 A5 中，所述根据接收到的所述处理数据，得到第一数据、第二数据和第三数据，具体为：将所述处理数据的前第二预设长度的数据作为第一数据，将所述处理数据的后第三预设长度的数据作为第三数据，将所述处理数据中除第一数据和第三数据外的数据作为第二数据。

[0030] 所述步骤 A5 之前还包括：所述认证服务器判断接收到的所述处理数据的长度是否不为空且大于第二预设长度与第三预设长度之和，如果是，则执行步骤 A5，否则报错，结

束。

[0031] 所述步骤 A4 中，所述将所述处理数据发送给所述认证服务器，具体为：所述种子生成系统将所述处理数据提供给使用所述认证服务器的用户，当用户接收到所述处理数据后，通过访问所述认证服务器页面，将所述处理数据上传导入到所述认证服务器中。

[0032] 所述步骤 A2 中，所述调用随机数生成函数，生成随机数，具体为：调用随机数生成函数，生成第一预设长度的随机数；

[0033] 对应的，所述步骤 A3，还包括：所述认证服务器判断所述第一解密数据的长度是否为所述第一预设长度，如果是，则执行步骤 A4，否则报错，结束。

[0034] 本发明取得的有益效果是：采用本发明的技术方案，保证了种子密钥在传输过程中的安全性。

附图说明

[0035] 为了更清楚的说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单的介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0036] 图 1 是本发明实施例 1 提供的一种种子密钥安全传输的方法流程图；

[0037] 图 2 和图 3 是本发明实施例 2 提供的一种种子密钥安全传输的方法流程图；

[0038] 图 4 是本发明实施例 3 提供的一种种子密钥安全传输的系统中认证服务器的工作流程图；

[0039] 图 5 是本发明实施例 4 提供的一种种子密钥安全传输的系统中种子生成系统的工作流程图。

具体实施方式

[0040] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0041] 实施例 1

[0042] 本发明实施例 1 提供了一种种子密钥安全传输的方法，如图 1 所示，包括：该方法应用于令牌认证服务器(以下简称认证服务器)和种子生成系统组成的系统中；

[0043] 步骤 101：认证服务器根据接收到的触发信息，生成公钥数据和私钥数据，将所述私钥数据保存，并根据所述公钥数据生成公钥文件；

[0044] 步骤 102：认证服务器将所述公钥文件发送给种子生成系统；

[0045] 步骤 103：所述种子生成系统根据接收到的用户选择的令牌号，查找对应的种子密钥，根据所述令牌号和所述种子密钥生成明文种子文件，从所述明文种子文件中获取明文种子文件数据；调用随机数生成函数，生成随机数；从所述公钥文件中获取所述公钥数据；

[0046] 步骤 104：所述种子生成系统应用所述公钥数据，对所述随机数进行加密，得到密

文随机数；根据所述随机数对所述明文种子文件数据进行加密，得到密文种子数据；对所述明文种子文件数据进行摘要计算，得到第一摘要值；

[0047] 步骤 105：所述种子生成系统根据所述密文随机数、所述密文种子文件数据和所述第一摘要值，生成处理数据；

[0048] 步骤 106：所述种子生成系统将所述处理数据发送给所述认证服务器；

[0049] 步骤 107：所述认证服务器根据接收到的所述处理数据，得到第一数据、第二数据和第三数据；

[0050] 步骤 108：所述认证服务器获取保存的所述私钥数据，使用所述私钥数据对所述第一数据进行解密，得到第一解密数据；

[0051] 步骤 109：所述认证服务器根据所述第一解密数据对所述第二数据进行解密，得到第二解密数据，对所述第二解密数据进行摘要计算，生成第二摘要值；

[0052] 步骤 110：所述认证服务器判断所述第三数据与所述第二摘要值是否相同，如果是，则执行步骤 111，否则报错，结束；

[0053] 步骤 111：所述认证服务器解析所述第二解密数据，获取所述第二解密数据中的令牌号和对应的种子密钥，并保存至数据库中，种子密钥传输成功，结束。

[0054] 实施例 2

[0055] 本发明实施例 2 提供了一种种子密钥安全传输的方法，如图 2 和图 3 所示，包括：该方法应用于令牌认证服务器（以下简称认证服务器）和种子生成系统组成的系统中；

[0056] 步骤 201：认证服务器根据接收到的触发信息，生成公钥数据和私钥数据，将私钥数据保存在预设存储区中；

[0057] 本实施例中，所述根据接收到的触发信息，生成公钥数据和私钥数据，具体为：认证服务器等待接收用户对种子生成系统标识的选择，当接收到用户选择的种子生成系统标识后，从预先保存的多条种子生成系统记录中获取对应的种子生成系统信息，根据所述种子生成系统信息，生成公钥数据和私钥数据；

[0058] 其中，所述预先保存的多条种子系统记录，具体包括：种子生成系统标识和种子生成系统名称；例如，种子生成系统的信息包括：种子生成系统标识（1001）和种子生成系统的名称（ABCD）；

[0059] 进一步的，所述根据所述种子生成系统信息，生成公钥数据和私钥数据，具体为：

[0060] 步骤 a1：认证服务器根据种子生成系统的信息中的种子生成系统标识，生成密码；

[0061] 具体为：认证服务器将种子生成系统标识作为加密因子，应用预设加密算法对加密因子进行加密，生成密码，优选的，预设加密算法 RC4 算法；

[0062] 例如，认证服务器应用预设加密算法对加密因子，即种子生成系统标识 1001 进行加密，生成的密码为 A77E71CD；

[0063] 步骤 a2：认证服务器根据种子生成系统的信息和密码，生成公私钥数据存储文件；

[0064] 具体为：认证服务器调用 cmd 命令 Runtime rt=Runtime.getRuntime();Process process=rt.exec(keytool-genkey-validity3650-alias1001-keyalg RSA-keystore D:/1001.keystore-keysize1024-dname"CN=ABCD,OU=ABCD,O=ABCD,L=BJ,ST=BJ,C=CN"

-storepass A77E71CD-keypass A77E71CD);process.destroy();将种子生成系统标识(1001)、种子生成系统名称(ABCD)、过期时间(默认 3650 天)、域名(CN=ABCD,OU=ABCD,O=ABCD,L=BJ,ST=BJ,C=CN)和密码(A77E71CD)写入公私钥数据存储文件中,即生成公私钥数据存储文件;

[0065] 步骤 a3:认证服务器从公私钥数据存储文件中获取私钥对象,对所述私钥对象进行编码生成私钥数据;

[0066] 优选的,认证服务器对所述私钥对象采用 BASE64 编码方式进行编码,生成私钥数据;

[0067] 例如,本实施例中,生成的私钥数据为:MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBALD29cy/aBEI4B71MXmyMxSHlvWcJwP2R3oF6BEG/59trHlOS7YoxD2OOLNi……HuplAbYmA+f+vS1zC9LM1ycLHwp8VYNOT f80BVfbYA1LoGlrIYLHQ==;

[0068] 步骤 a4:认证服务器解析公私钥数据存储文件,从公私钥存储文件中获取公钥数据;

[0069] 例如,本实施例中,生成的公钥数据为:MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBALD29cy/aBEI4B71MXmyMxSHlvWcJwP2R3oF6BEG/59trHlOS7YoxD2OOLNi……HuplAbYmA+f+vS1zC9LM1ycLHwp8VYNOT f80BVfbYA1LoGlrIYLHQ==;

[0070] 步骤 202:认证服务器将公钥数据按照预设格式写入到公钥文件中;

[0071] 例如,本实施例中,公钥文件为:

[0072] ---BEGIN CERTIFICATE-----

[0073] MIICdgIBADANBgkqhkiG9w0BAQ

[0074] EFAASCAmAwggJcAgEAAoGBALD29cy/aBEI4B71MXmyMxSHlvWcJwP2R3oF6BEG/59trHlOS7YoxD2OOLNi……HuplAbYmA+f+vS1zC9LM1ycLHwp8VYNOT f80BVfbYA1LoGlrIYLHQ==

[0075] -----END CERTIFICATE-----

[0076] 步骤 203:认证服务器将公钥文件发送给种子生成系统;

[0077] 其中,本实施例中,认证服务器将公钥文件通过邮件或刻盘等的形式发送给种子生成系统;

[0078] 步骤 204:种子生成系统根据接收到的用户选择的令牌号,查找对应的种子密钥,根据令牌号和种子密钥生成明文种子文件,从明文种子文件中获取明文种子文件数据;

[0079] 其中,种子生成系统预先生成多条令牌数据,包括令牌号和对应的种子密钥,当访问种子生成系统时,根据需要选择的令牌号,从令牌数据中查找与令牌号对应的种子密钥,根据种子密钥生成明文种子文件,当种子生成系统接收到用户点击导出种子文件按钮时,将明文种子文件导出;

[0080] 例如,导出的明文种子文件数据为:

[0081] <?xml version="1.0"encoding="UTF-8"?>

[0082] <TokenXml>

[0083] <TokenHeader>

[0084] <Version>5.0</Version>

[0085] <Origin>FT</Origin>

[0086] <TokenType>0</TokenType>

[0087] <FirstToken>3000000003197</FirstToken>

[0088] <LastToken>3000000003198</LastToken>

[0089] <TokenNum>2</TokenNum>

[0090] <TokenBirth>2014-02-2115:54:53</TokenBirth>

[0091] <TokenDeath>2019-02-2115:54:01</TokenDeath>

[0092] <MacKey>1622D3388D13B3FE40DC34B22728E89BBEDEE125</MacKey>

[0093] </TokenHeader>

[0094] <TokenList>

[0095] <Token>

[0096] <SN>3000000003197</SN><Seed>gQANMzAwMDAwMDAwMzE5NyDYnLmKdPHSrcqQH23QcoI6Vw wB/k6TmHr/akhcYGonf8SyAkZUAA0GQgAAAAAAPAAAAAAAAAAAAAABTBwZNXG5ZGf///////wEBAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADEgAAA AoAAAAEk9UUC1TTTMtNjpRTjA2LVQxTRJPVFAtU00zLTY6UU42NC1UMU0OT1RQLVNNMy02OlFOM DYAAAAAAAAAAAAAAAAKvc=</Seed><MacKey>E72EFAC244EB6CA62E4B19D9421E1150FD2EE361</MacKey>

[0097] </Token>

[0098] <Token>

[0099] <SN>3000000003198</SN><Seed>gQANMzAwMDAwMDAwMzE5OCCsG6HMN8RjqGSgY+WP+7Y9O4+I8qJ/dIT9PbM8RPGD111vAkZUAA0GQgAAAAAAPAAAAAAAAAAAAAABTBwZNXG5ZGf///////wEBA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADEgAA AAoAAAAEk9UUC1TTTMtNjpRTjA2LVQxTRJPVFAtU00zLTY6UU42NC1UMU0OT1RQLVNNMy02OlFOMDYAAAAAAAAAAAAAAA0e4=</Seed><MacKey>CE88684EBFE2688417B281A9E07C9F5A0322B06C</MacKey>

[0100] </Token>

[0101] </TokenList>

[0102] <TokenXmlMac><MacKey>9A7F714405AEDB62D1B87D59B99C2492C1E97C25</MacKey>

[0103] </TokenXmlMac>

[0104] </TokenXml>

[0105] 步骤 205 :种子生成系统调用随机数生成函数,生成第一预设长度的随机数 ;

[0106] 优选的,第一预设长度为 16 字节 ;

[0107] 例如,随机生成的第一预设长度的随机数为 :-13,41,53,76,7,-114,-80,-104,-80,-10,0,-85,58,-10,37,-127 ;

[0108] 步骤 206 :种子生成系统从所述公钥文件中获取公钥数据,判断是否能够获取到公钥数据,如果是,则执行步骤 207,否则报错,结束 ;

[0109] 例如,本实施例中,从所述公钥文件中获取到的公钥数据为 :48,-127,-97,48,13,6,9,42,-122,72,-122,-9,13,1,1,1,5,0,3,-127,-115,0,48,-127,-119,2,-127,-127,0,-80,-10,-11,-52,-65,104,17,8,-32,30,-11,49,121,-78,51,20,-121,-106,-11,-100,39,3,-10,71,122,5,-24,17,6,-1,-97,109,-84,121,78,75,-74,40,-60,61,-76,56,-77,9

8,82,113,74,-79,119,17,-113,91,-84,7,-81,-49,98,-37,39,89,-89,40,-21,-91,-38,-94,-110,98,-70,-94,-57,-27,-62,-85,53,-109,-111,24,-100,-62,10,-96,-79,-49,-28,67,47,-10,90,-13,38,-58,63,-102,61,-31,111,-83,45,1,24,56,42,-30,-109,-21,-22,118,79,-98,114,-39,72,18,89,-108,-24,76,23,32,55,-27,-39,101,-12,83,-80,105,2,3,1,0,1 ;

[0110] 本实施例中,步骤 204、205 和 206 执行顺序可以互相调换 ;

[0111] 步骤 207 :种子生成系统使用公钥数据,对随机数进行加密,得到第二预设长度的密文随机数 ;

[0112] 优选的,种子生成系统使用公钥数据,采用 RSA_PKCS1_PADDING 填充方式,对随机数进行加密,得到第二预设长度的密文随机数,其中,第二预设长度优选为 128 字节 ;

[0113] 例如,生成的预设长度的密文随机数为 :109,-49,-122,1,110,2,103,85,56,-14,123,74,64,19,-115,10,11,83,5,29,28,-10,56,-7,39,61,50,-117,-33,-121,-13,-86,127,-8,-51,-94,125,-91,102,20,56,-89,112,111,41,-34,116,-48,-92,12,-105,74,-122,-10,97,-94,-88,-120,123,63,-82,48,-30,26,81,-59,53,-60,88,80,96,64,101,-109,87,-126,-99,68,-54,0,62,-100,-107,-116,-123,-81,-99,-92,-52,-76,20,42,-60,-9,66,-79,-29,22,121,-78,-51,70,26,95,-116,63,-124,74,-48,71,-84,-71,-74,82,92,-123,123,107,115,110,-76,125,-42,31,-62,77,-28,88 ;

[0114] 步骤 208 :种子生成系统使用随机数和预设加密算法,对明文种子文件数据进行加密,得到密文种子文件数据 ;

[0115] 优选的,种子生成系统采用对称加密算法 aes128-cbc,应用 PKCS5Padding 填充方式对明文种子文件数据进行加密 ;

[0116] 本实施例中,得到的密文种子文件数据为 :80,5,21,-35,-69,30,45,84,-4,-61,-79,100,-45,-39,41,-111,-40,-124,45,-37,124,82,80,68,31,66,42,79,87,-13,17,-26,32,103,-25,19,-50,21,67,54,49,-30,76,-126,-102,-120,49,-80,95,56,-95,-14,87,-73,-94,-61,1,-94,-94,41,-71,-76,-125,111,11,44,-17,-80,-88,-102,-9,-52,-50,21,83,-81,33,-124,-93,-1,42,14,96,103,47,……-2,123,-95,-99,18,90,-90,-39,11,45,-19,-115,-9,115,77,-38,-14,52,-12,-73,0,-22,54,-11,95,107,-9,74,68,32,-56,-28,93,15,30,46,69,-51,-98,10,-74,30,50,88,29,-79,-41,-94,-66,-29,-116,4,-36,-3,65,124,-12,94,-61,-120,-117,27,-107,-126,108,60,-34,-20,86,-117,100,-14,-99,95,-97,43,40,62,12,46,-95,-62,122,67,-4,-103,85,121,4,105,32,-29,4,73,49,-69,-11,7,24,33,-79,124,108,-81,99,36,-59,-64,-88,-62,49,4,87,70,20,-73,8,74,-18,109,49,106,-127,-40,-17,-75,121,-60,120,-126 ;

[0117] 步骤 209 :种子生成系统使用预设摘要算法对明文种子文件数据进行摘要计算,得到第三预设长度的第一摘要值 ;

[0118] 优选的,预设摘要算法为 SHA1 算法,除此之外,还可以为 SHA256、MD5 算法等,其中,第三预设长度优选为 20 字节 ;

[0119] 本实施例中,得到的第一摘要值为 :64,-91,-99,-1,45,-19,89,-99,90,-50,120,-126,97,-109,63,37,85,26,-56,-17 ;

[0120] 本实施例中,步骤 107、108 和 109 顺序可以互换 ;

[0121] 步骤 210 :种子生成系统根据第二预设长度的密文随机数、密文种子文件数据和第三预设长度的第一摘要值,生成处理数据 ;

[0122] 优选的,种子生成系统将密文随机数、密文种子文件数据和第一摘要值进行顺序拼接,得到处理数据 ;除此之外,还可以将密文随机数、密文种子文件数据和第一摘要值进行预设运算,将得到的值作为处理数据 ;

[0123] 本实施例中,生成的处理数据为 :109,-49,-122,1,110,2,103,85,56,-14,123,74,64,19,-115,10,11,83,5,29,28,-10,56,-7,39,61,50,-117,-33,-121,-13,-86,127,-8,-51,-94,125,-91,102,20,56,-89,112,111,41,-34,116,-48,-92,12,-105,74,-122,-10,97,-94,-88,-120,123,63,-82,48,-30,26,81,-59,53,-60,88,80,96,64,101,-109,87,-126,-99,68,-54,0,62,-100,-107,-116,-123,-81,-99,……-62,122,67,-4,-103,85,121,4,105,32,-29,4,73,49,-69,-11,7,24,33,-79,124,108,-81,99,36,-59,-64,-88,-62,49,4,87,70,20,-73,8,74,-18,109,49,106,-127,-40,-17,-75,121,-60,120,-126,64,-91,-99,-1,45,-19,89,-99,90,-50,120,-126,97,-109,63,37,85,26,-56,-17 ;

[0124] 步骤 211 :种子生成系统将处理数据发送给认证服务器 ;

[0125] 本实施例中,所述将处理数据发送给认证服务器,具体为 :种子生成系统将处理数据提供给使用认证服务器的用户,用户接收到该处理数据后,访问认证服务器页面,将该处理数据上传导入到认证服务器中 ;

[0126] 步骤 212 :认证服务器根据接收到的处理数据,判断所述处理数据是否不为空且长度是否大于第四预设长度,如果是,则执行步骤 213,否则报错,结束 ;

[0127] 优选的,第四预设长度为第二预设长度与第三预设长度之和,本实施例优选为 128 字节 +20 字节 =148 字节 ;

[0128] 步骤 213 :认证服务器根据所述处理数据,得到第一数据、第二数据和第三数据 ;

[0129] 本实施例中,如果接收到的处理数据未被截取或篡改等,则从处理数据中获取到的第一数据为密文随机数、第二数据为密文种子文件数据、第三数据为第一摘要值 ;

[0130] 优选的,认证服务器对接收到的处理数据进行拆分,将前第二预设长度即 128 字节的数据作为第一数据,将后第三预设长度即 20 字节的数据作为第三数据,将中间数据作为第二数据 ;

[0131] 其中,如果传输过程没有错误,则拆分得到的第一数据为 109,-49,-122,1,110,2,103,85,56,-14,123,74,64,19,-115,10,11,83,5,29,……-71,-74,82,92,-123,123,107,115,110,-76,125,-42,31,-62,77,-28,88 ;

[0132] 第二数据为 :80,5,21,-35,-69,30,45,84,-4,-61,-79,100,-45,-39,41,-111,-40,-124,45,-37,124,82,80,68,31,66,42,79,87,-13,17,-26,32,103,-25,19,-50,21,……121,4,105,32,-29,4,73,49,-69,-11,7,24,33,-79,124,108,-81,99,36,-59,-64,-88,-62,49,4,87,70,20,-73,8,74,-18,109,49,106,-127,-40,-17,-75,121,-60,120,-126 ;

[0133] 第三数据为 :64,-91,-99,-1,45,-19,89,-99,90,-50,120,-126,97,-109,63,37,85,26,-56,-17 ;

[0134] 步骤 214 :认证服务器从预设存储区中获取私钥数据,使用私钥数据,对第一数据进行解密,得到第一解密数据 ;

[0135] 优选的,认证服务器使用私钥数据,采用 RSA_PKCS1_PADDING 填充方式,去掉填充

数据，得到第一解密数据，如果过程无误，则生成的第一解密数据即为随机数；

[0136] 进一步的，还包括：认证服务器判断所述第一解密数据的长度是否为第一预设长度，如果是，则执行步骤 215，否则显示错误信息，结束；

[0137] 本实施例中，解密得到的第一解密数据为 -13,41,53,76,7,-114,-80,-104,-80,-10,0,-85,58,-10,37,-127；

[0138] 步骤 215：认证服务器使用第一解密数据和预设解密算法，对第二数据进行解密，得到第二解密数据；

[0139] 优选的，认证服务器应用对称解密算法 aes128-cbc，采用 PKCS5Padding 填充方式，对第二数据进行解密；

[0140] 本实施例中，得到的第二解密数据为：60,63,120,109,108,32,118,101,114,115,105,111,110,61,34,49,46,48,34,32,101,110,99,111,100,105,110,103,61,34,85,84,70,45,56,34,63,……84,111,107,101,110,88,109,108,77,97,99,62,10,60,47,84,111,107,101,110,88,109,108,62,10；

[0141] 步骤 216：认证服务器使用预设摘要算法对第二解密数据进行摘要计算，得到第二摘要值；

[0142] 优选的，预设摘要算法为 SHA1 算法，除此之外，还可以为 SHA256、MD5 算法等；

[0143] 本实施例中，得到的第二摘要值为：64,-91,-99,-1,45,-19,89,-99,90,-50,120,-126,97,-109,63,37,85,26,-56,-17；

[0144] 步骤 217：认证服务器判断第三数据与第二摘要值是否相同，如果是，则执行步骤 218，否则种子密钥传输失败，报错结束；

[0145] 步骤 218：认证服务器解析所述第二解密数据，判断是否能够解析成功，如果是，则从第二解密数据中获取令牌号和对应的种子密钥，并保存至数据库中，种子密钥传输成功，结束，否则报错，结束；

[0146] 本实施例中，如果解析成功，得到的第二解密数据即为明文种子文件数据，对所述明文种子文件数据进行解析，得到令牌号和对应的种子密钥；

[0147] 本实施例中，解析所述明文种子文件数据中 <SN></SN> 和 <Seed></Seed> 节点间的信息，即为令牌号和对应的种子密钥；

[0148] 例如，记录到数据库中的信息为：

[0149] <SN>3000000003197</SN><Seed>gQANMzAwMDAwMDAwMzE5NyDYnLmKdPHSrcqQH23QcoI6Vw wB/k6TmHr/akhcYGonf8SyAkZUAA0GQgAAAAAAPAAAAAAAAAAAAAABTBwZNXG5ZGf///////wEBAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADEgAAA AoAAAAEk9UUC1TTTMtNjpRTjA2LVQxTRJPVFAtU00zLTY6UU42NC1UMU00T1RQLVNNMy020lFOMDYAAAAAAAAAAAAAAAAAKvc=</Seed>

[0150] <SN>3000000003198</SN><Seed>gQANMzAwMDAwMDAwMzE5OCCsG6HMN8RjqGSgY+WP+7Y9O4+I8qJ/dIT9PbM8RPGD111vAkZUAA0GQgAAAAAAPAAAAAAAAAAAAAABTBwZNXG5ZGf/////wEBA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADEgAA AAoAAAAEk9UUC1TTTMtNjpRTjA2LVQxTRJPVFAtU00zLTY6UU42NC1UMU00T1RQLVNNMy020lFOMDYAAAAAAAAAAAAAAAAA0e4=</Seed>。

[0151] 实施例 3

[0152] 参见图 4，本发明实施例 3 提供了一种种子密钥安全传输的系统中认证服务器的工作流程，具体操作如下：

[0153] 步骤 301：认证服务器等待接收生成公私钥数据触发；

[0154] 步骤 302：当认证服务器接收到生成公私钥数据触发时，生成公钥数据和私钥数据，将私钥数据保存在预设存储区中；

[0155] 步骤 303：认证服务器将公钥数据按照预设格式写入到公钥文件中，并将所述公钥文件发送给种子生成系统；

[0156] 步骤 304：认证服务器等待接收种子生成系统返回的处理数据，当接收到处理数据后，判断所述处理数据是否不为空且长度大于第二预设长度与第三预设长度之和，如果是，则执行步骤 305，否则报错，结束；

[0157] 步骤 305：认证服务器根据所述处理数据，得到第一数据、第二数据和第三数据；

[0158] 具体为：认证服务器对所述处理数据进行拆分，将前第二预设长度的数据作为第一数据，将所述处理数据的后第三预设长度的数据作为第三数据，将第一数据和第三数据之间的数据作为第二数据；

[0159] 步骤 306：认证服务器从所述预设存储区中获取私钥数据，使用所述私钥数据对所述第一数据进行解密，得到第一解密数据，判断第一解密数据的长度是否为第一预设长度，如果是，则执行步骤 307，否则报错，结束；

[0160] 步骤 307：认证服务器应用所述第一解密数据和预设解密算法，对所述第二数据进行解密，得到第二解密数据；

[0161] 步骤 308：认证服务器使用预设摘要算法对所述第二解密数据进行摘要计算，得到第二摘要值；

[0162] 步骤 309：认证服务器判断第三数据与第二摘要值是否相同，如果是，则执行步骤 310，否则种子密钥传输失败，报错结束；

[0163] 步骤 310：认证服务器解析所述第二解密数据，判断是否能够解析成功，如果是，则执行步骤 311，否则报错，结束；

[0164] 步骤 311：认证服务器从第二解密数据中获取令牌号和对应的种子密钥，并保存至数据库中，种子密钥传输成功，返回步骤 304。

[0165] 实施例 4

[0166] 参见图 5，本发明实施例 4 提供了一种种子密钥安全传输的系统中种子生成系统的工作流程，具体操作如下：

[0167] 步骤 401：种子生成系统等待接收用户选择的令牌号；

[0168] 步骤 402：当种子生成系统接收到用户选择的令牌号时，根据所述令牌号获取对应的种子密钥，根据所述令牌号和所述种子密钥生成明文种子文件，从所述明文种子文件中获取明文种子文件数据；

[0169] 步骤 403：种子生成系统调用随机数生成函数，生成第一预设长度的随机数；

[0170] 步骤 404：种子生成系统判断是否能够获取到公钥文件，如果是，则执行步骤 405，否则报错，结束；

[0171] 步骤 405：种子生成系统从所述公钥文件中获取公钥数据，判断是否能够获取到公钥数据，如果是，则执行步骤 406，否则报错，结束；

[0172] 步骤 406 :种子生成系统使用所述公钥数据,对所述随机数进行加密,得到第二预设长度的密文随机数 ;

[0173] 步骤 407 :种子生成系统使用随机数和预设加密算法,对明文种子文件数据进行加密,得到密文种子文件数据 ;

[0174] 步骤 408 :种子生成系统使用预设摘要算法对所述明文种子文件数据进行摘要计算,生成第三预设长度的第一摘要值 ;

[0175] 步骤 409 :种子生成系统根据所述第二预设长度的密文随机数、密文种子文件数据和所述第三预设长度的第一摘要值,生成处理数据 ;

[0176] 步骤 410 :种子生成系统将所述处理数据发送给认证服务器,返回执行步骤 401 ;

[0177] 以上所述,仅为本发明较佳的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明公开的技术范围内,可轻易想到的变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应该以权利要求的保护范围为准。

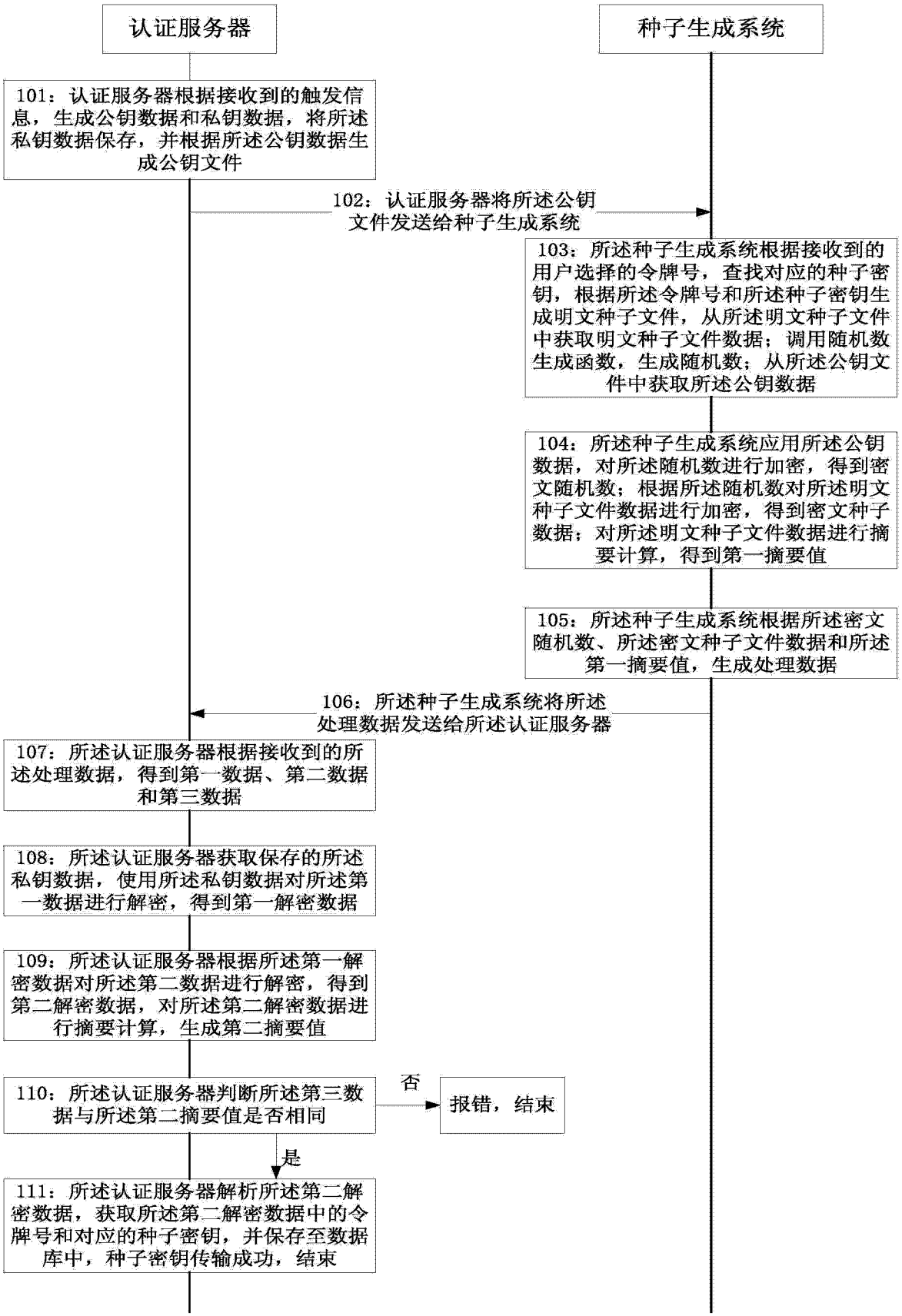

认证服务器
种子生成系统
101：认证服务器根据接收到的触发信息，生成公钥数据和私钥数据，将所述私钥数据保存，并根据所述公钥数据生成公钥文件
102：认证服务器将所述公钥文件发送给种子生成系统
103：所述种子生成系统根据接收到的用户选择的令牌号，查找对应的种子密钥，根据所述令牌号和所述种子密钥生成明文种子文件，从所述明文种子文件中获取明文种子文件数据；调用随机数生成函数，生成随机数；从所述公钥文件中获取所述公钥数据
104：所述种子生成系统应用所述公钥数据，对所述随机数进行加密，得到密文随机数；根据所述随机数对所述明文种子文件数据进行加密，得到密文种子数据；对所述明文种子文件数据进行摘要计算，得到第一摘要值
105：所述种子生成系统根据所述密文随机数、所述密文种子文件数据和所述第一摘要值，生成处理数据
106：所述种子生成系统将所述处理数据发送给所述认证服务器
107：所述认证服务器根据接收到的所述处理数据，得到第一数据、第二数据和第三数据
108：所述认证服务器获取保存的所述私钥数据，使用所述私钥数据对所述第一数据进行解密，得到第一解密数据
109：所述认证服务器根据所述第一解密数据对所述第二数据进行解密，得到第二解密数据，对所述第二解密数据进行摘要计算，生成第二摘要值
110：所述认证服务器判断所述第三数据与所述第二摘要值是否相同
否
报错，结束
是
111：所述认证服务器解析所述第二解密数据，获取所述第二解密数据中的令牌号和对应的种子密钥，并保存至数据库中，种子密钥传输成功，结束

图 1

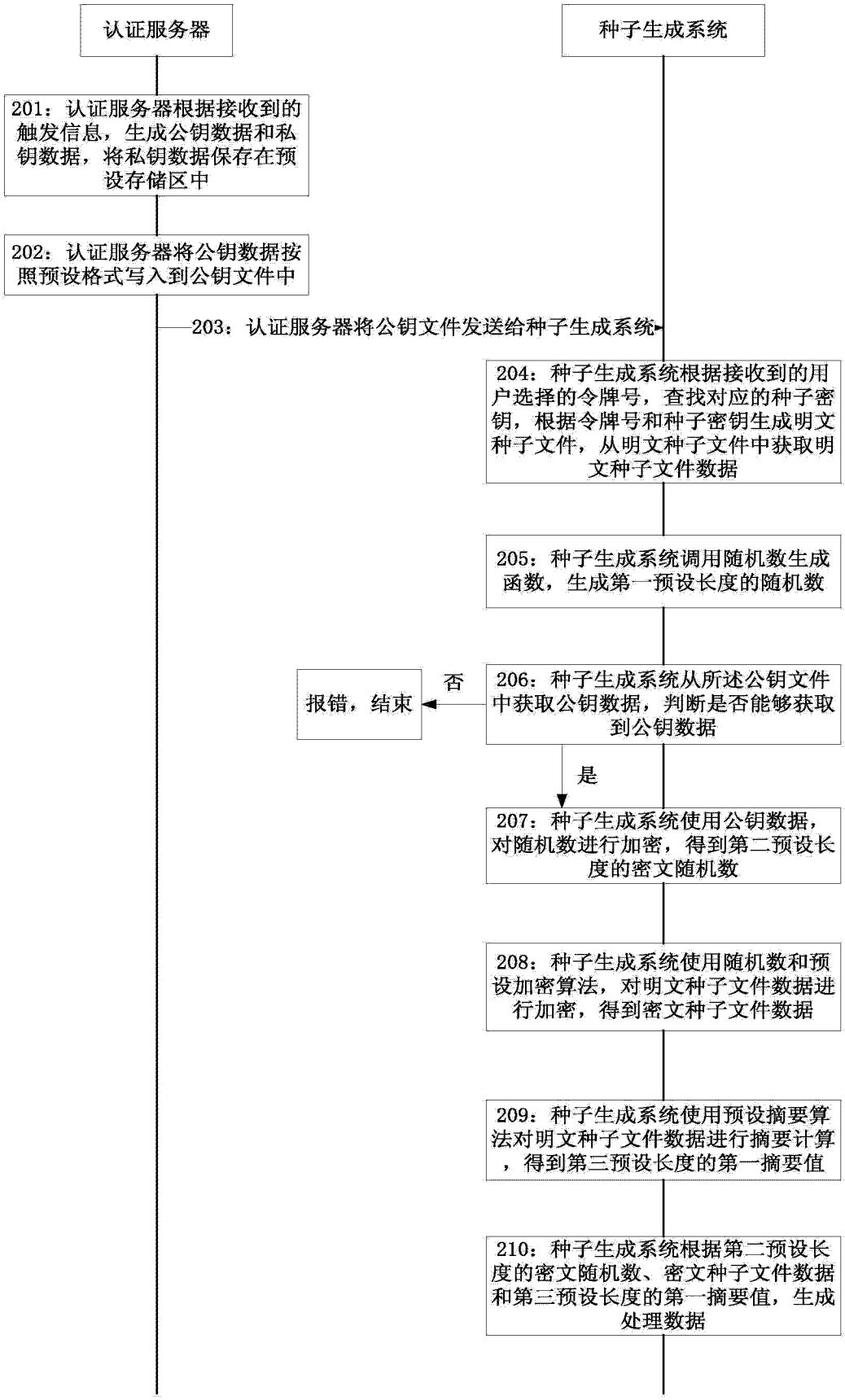

认证服务器
种子生成系统
201：认证服务器根据接收到的触发信息，生成公钥数据和私钥数据，将私钥数据保存在预设存储区中
202：认证服务器将公钥数据按照预设格式写入到公钥文件中
203：认证服务器将公钥文件发送给种子生成系统
204：种子生成系统根据接收到的用户选择的令牌号，查找对应的种子密钥，根据令牌号和种子密钥生成明文种子文件，从明文种子文件中获取明文种子文件数据
205：种子生成系统调用随机数生成函数，生成第一预设长度的随机数
206：种子生成系统从所述公钥文件中获取公钥数据，判断是否能够获取到公钥数据
否
报错，结束
是
207：种子生成系统使用公钥数据，对随机数进行加密，得到第二预设长度的密文随机数
208：种子生成系统使用随机数和预设加密算法，对明文种子文件数据进行加密，得到密文种子文件数据
209：种子生成系统使用预设摘要算法对明文种子文件数据进行摘要计算，得到第三预设长度的第一摘要值
210：种子生成系统根据第二预设长度的密文随机数、密文种子文件数据和第三预设长度的第一摘要值，生成处理数据

图 2

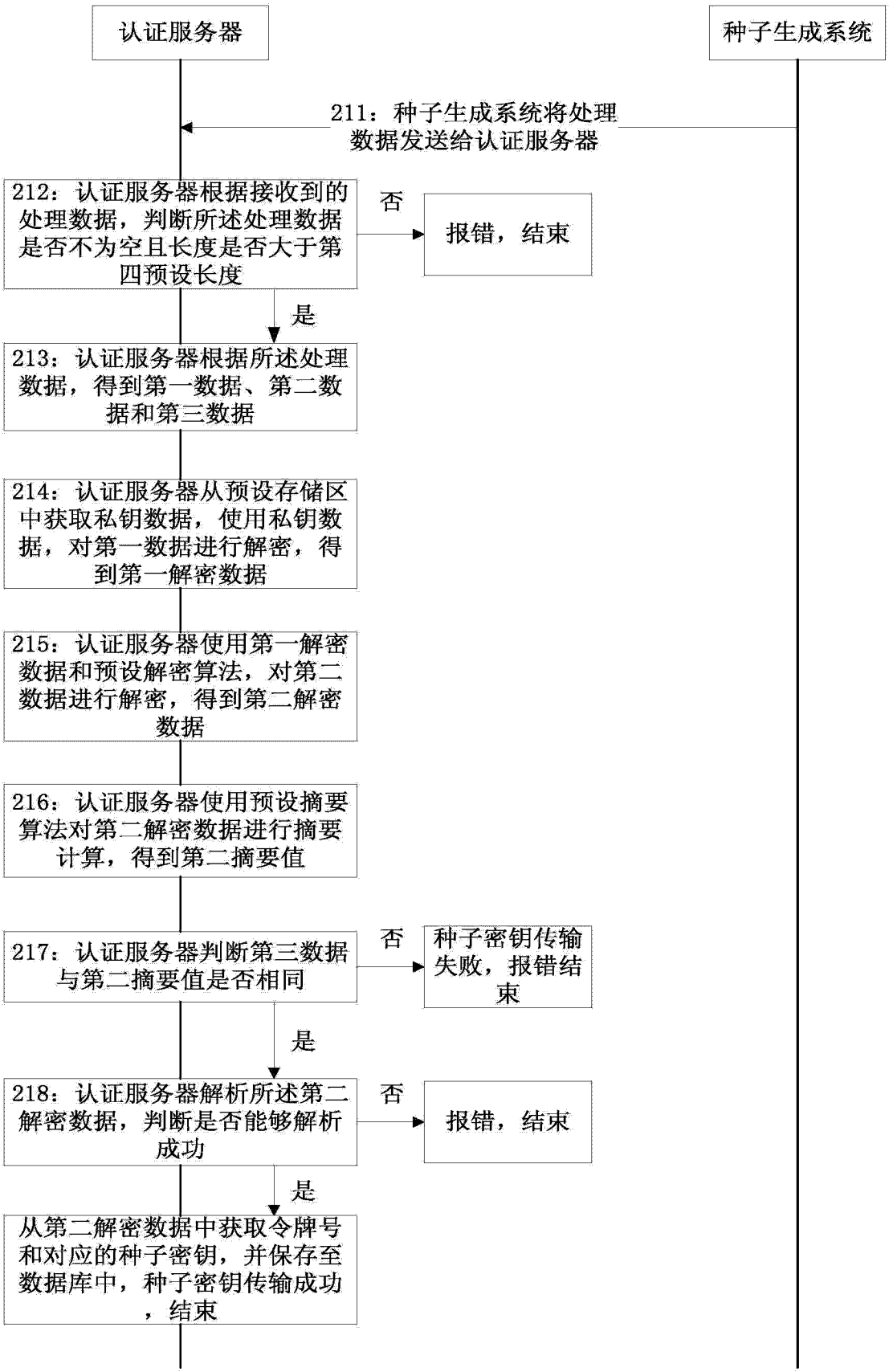

认证服务器
种子生成系统
211：种子生成系统将处理数据发送给认证服务器
212：认证服务器根据接收到的处理数据，判断所述处理数据是否不为空且长度是否大于第四预设长度
否
报错，结束
是
213：认证服务器根据所述处理数据，得到第一数据、第二数据和第三数据
214：认证服务器从预设存储区中获取私钥数据，使用私钥数据，对第一数据进行解密，得到第一解密数据
215：认证服务器使用第一解密数据和预设解密算法，对第二数据进行解密，得到第二解密数据
216：认证服务器使用预设摘要算法对第二解密数据进行摘要计算，得到第二摘要值
217：认证服务器判断第三数据与第二摘要值是否相同
否
种子密钥传输失败，报错结束
是
218：认证服务器解析所述第二解密数据，判断是否能够解析成功
否
报错，结束
是
从第二解密数据中获取令牌号和对应的种子密钥，并保存至数据库中，种子密钥传输成功，结束

图 3

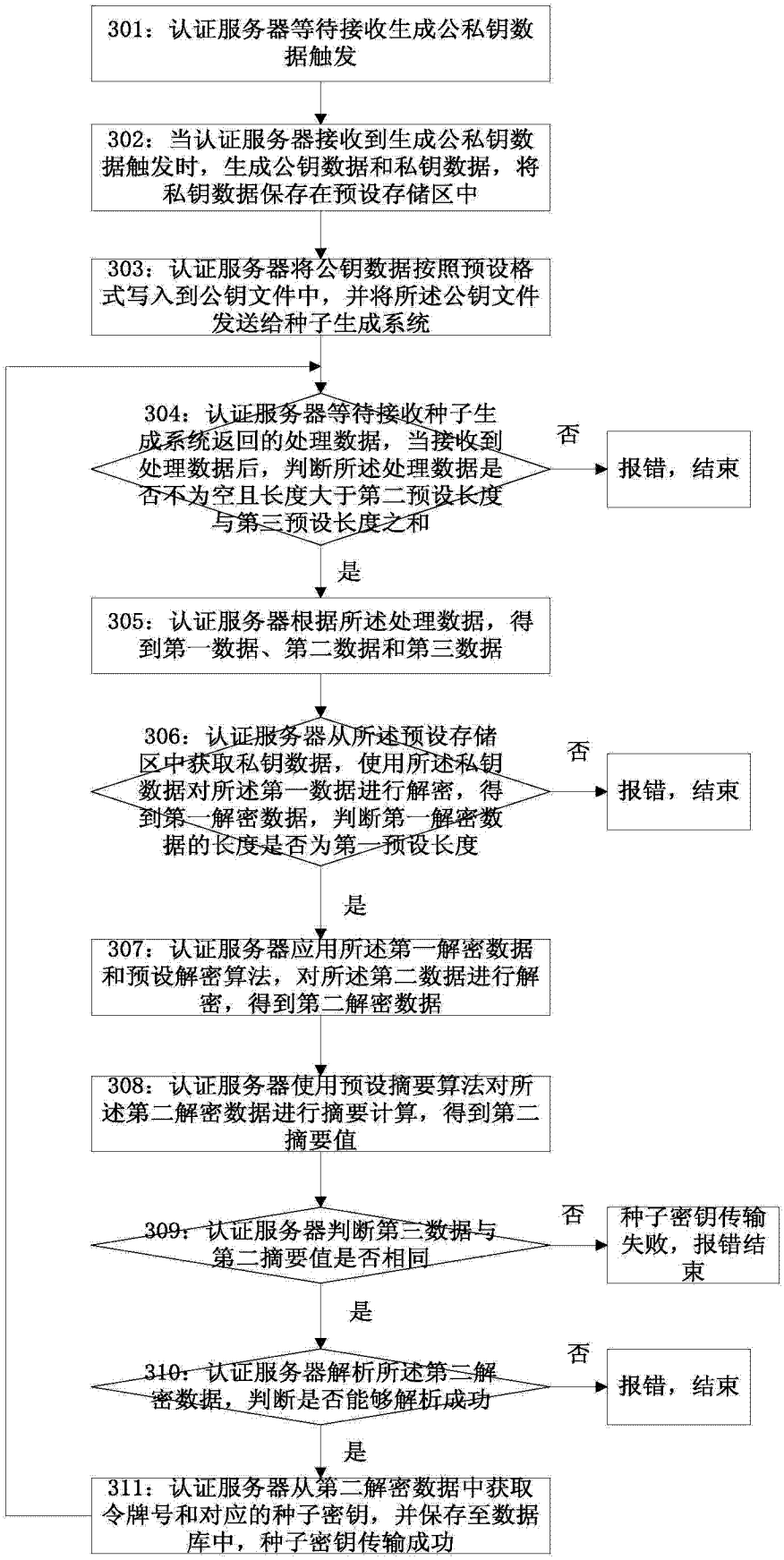

301：认证服务器等待接收生成公私钥数据触发
302：当认证服务器接收到生成公私钥数据触发时，生成公钥数据和私钥数据，将私钥数据保存在预设存储区中
303：认证服务器将公钥数据按照预设格式写入到公钥文件中，并将所述公钥文件发送给种子生成系统
304：认证服务器等待接收种子生成系统返回的处理数据，当接收到处理数据后，判断所述处理数据是否不为空且长度大于第二预设长度与第三预设长度之和
否
报错，结束
是
305：认证服务器根据所述处理数据，得到第一数据、第二数据和第三数据
306：认证服务器从所述预设存储区中获取私钥数据，使用所述私钥数据对所述第一数据进行解密，得到第一解密数据，判断第一解密数据的长度是否为第一预设长度
否
报错，结束
是
307：认证服务器应用所述第一解密数据和预设解密算法，对所述第二数据进行解密，得到第二解密数据
308：认证服务器使用预设摘要算法对所述第二解密数据进行摘要计算，得到第二摘要值
309：认证服务器判断第三数据与第二摘要值是否相同
否
种子密钥传输失败，报错结束
是
310：认证服务器解析所述第三解密数据，判断是否能够解析成功
否
报错，结束
是
311：认证服务器从第二解密数据中获取令牌号和对应的种子密钥，并保存至数据库中，种子密钥传输成功

图 4

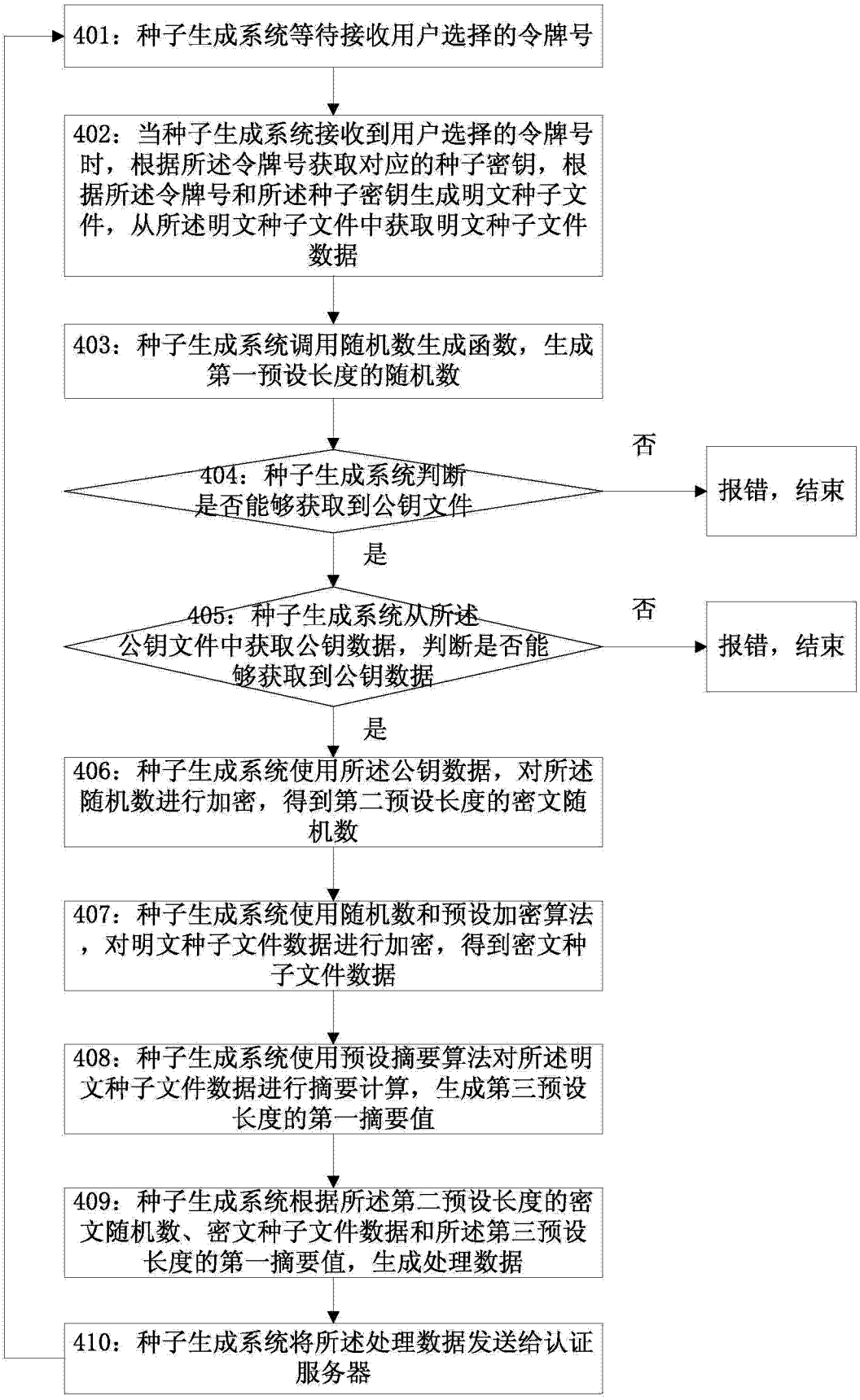

401：种子生成系统等待接收用户选择的令牌号
402：当种子生成系统接收到用户选择的令牌号时，根据所述令牌号获取对应的种子密钥，根据所述令牌号和所述种子密钥生成明文种子文件，从所述明文种子文件中获取明文种子文件数据
403：种子生成系统调用随机数生成函数，生成第一预设长度的随机数
404：种子生成系统判断是否能够获取到公钥文件
否
报错，结束
是
405：种子生成系统从所述公钥文件中获取公钥数据，判断是否能够获取到公钥数据
否
报错，结束
是
406：种子生成系统使用所述公钥数据，对所述随机数进行加密，得到第二预设长度的密文随机数
407：种子生成系统使用随机数和预设加密算法，对明文种子文件数据进行加密，得到密文种子文件数据
408：种子生成系统使用预设摘要算法对所述明文种子文件数据进行摘要计算，生成第三预设长度的第一摘要值
409：种子生成系统根据所述第二预设长度的密文随机数、密文种子文件数据和所述第三预设长度的第一摘要值，生成处理数据
410：种子生成系统将所述处理数据发送给认证服务器

图 5