

动态口令牌、动态口令牌数据传输方法及系统

技术领域

5 本发明涉及电子技术领域，尤其涉及一种动态口令牌、动态口令牌数据传输方法及系统。

背景技术

10 动态口令(One Time Pass-Word, OTP)作为最安全的身份认证技术之一，目前已经被越来越多的行业所应用。动态令牌根据算法、种子密钥，结合时间、事件因子或挑战信息的一种或多种，生成一个不可预测的随机数字组合（即 OTP 值），每个 OTP 值只能使用一次。由于它使用便捷，且与平台无关，被广泛应用于企业、网游、金融等领域。

在现有的动态令牌应用中，算法是预先内置在令牌中的。而每个令牌都需要不同的种子密钥，种子密钥都是在使动态口令牌生效或激活的时候，通过与后台系统服务器连接进
15 行信息交互将种子密钥注入到动态口令牌。由于 OTP 值的产生依赖于种子密钥，一旦种子密钥外泄，将极大地影响动态口令的安全性，从而危害用户的账户安全，造成用户损失。

另外，动态口令牌在使用一段时间后，当时间或者事件因子产生误差时会导致动态口令牌不能生成 OTP 值，则需要与后台系统服务器进行同步。一旦同步过程中信息外泄，导致时间或者事件因子信息被泄漏，造成用户账户不安全。

20 另外，现有的动态口令牌在使用时，在生效、激活和同步这些步骤，都需要与后台系统服务器直接相连，因此需要动态口令牌持有人当面与后台系统服务器进行操作。

发明内容

本发明旨在解决上述问题之一。

25 本发明一方面提供了一种动态口令牌数据传输方法。

本发明的另一目的在于提供一种动态口令牌。

本发明的另一目的在于提供一种动态口令牌数据传输系统。

为达到上述目的，本发明的技术方案具体是这样实现的：本发明提供一种动态口令牌数据传输方法，包括：所述动态口令牌接收开启指令，根据所述开启指令执行开启操作；
30 所述动态口令牌接收输入的操作指令；所述动态口令牌在接收到所述操作指令之后，根据所述操作指令生成请求信息，对所述请求信息进行签名得到第一数字签名，根据所述请求信息和所述第一数字签名得到请求数据包，将所述请求数据包发送至后台系统服务器；所

述后台系统服务器接收所述请求数据包，从接收到的所述请求数据包中获得所述第一数字签名和所述请求信息，并对所述第一数字签名进行验签；所述后台系统服务器在所述第一数字签名验签通过后，根据所述请求信息确定对应的反馈信息，根据所述反馈信息加密获得反馈数据包，将所述反馈数据包发送至所述动态令牌；所述动态令牌接收所述反馈数据包；所述动态令牌在接收到所述反馈数据包后，解密所述反馈数据包获得所述反馈信息；所述动态令牌在获得所述反馈信息后，保存所述反馈信息；所述动态令牌生成响应信息，对所述响应信息进行签名得到第二数字签名，根据所述响应信息和所述第二数字签名得到响应数据包，将所述响应数据包发送至所述后台系统服务器；所述后台系统服务器接收所述响应数据包，从接收到的所述响应数据包中获得所述第二数字签名和所述响应信息，并对所述第二数字签名进行验签；所述后台系统服务器对所述第二数字签名验签通过后，根据所述响应信息执行响应操作。

此外，所述操作指令为生效操作指令；所述请求信息为生效请求信息，所述生效请求信息包含生效操作码和账户信息；所述反馈信息包含至少一个种子密钥。

此外，所述反馈信息还包含事件因子信息。

此外，所述操作指令为激活操作指令；所述请求信息为激活请求信息，所述激活请求信息包含激活操作码和账户信息；所述反馈信息包含激活码；所述动态令牌在获得所述反馈信息后，保存所述反馈信息的步骤之后，该方法还包括：所述动态令牌对所述反馈信息中包含的所述激活码进行验证；所述动态令牌对所述激活码验证通过后，触发所述动态令牌生成响应信息的操作。

此外，所述动态令牌对所述反馈信息中包含的所述激活码进行验证的步骤包括：

所述动态令牌读取所述反馈信息中包含的所述激活码；所述动态令牌根据预设的激活码生成算法生成激活验证码；所述动态令牌比对所述激活码和所述激活验证码，比对一致，则触发动态令牌生成响应信息的操作；或者当所述后台系统服务器将所述反馈数据包和激活验证码一起发送至所述动态令牌时，所述动态令牌在接收到所述反馈数据包和激活验证码，从所述反馈数据包中获得所述反馈信息后，比对所述反馈信息中的激活码和所述激活验证码，比对一致，则触发动态令牌生成响应信息的操作。

此外，所述操作指令为同步操作指令；所述请求信息为同步请求信息，所述同步请求信息包含同步操作码和账户信息；所述反馈信息包含同步码。

此外，所述动态令牌在接收到所述反馈数据包后，解密所述反馈数据包获得所述反馈信息的步骤包括：所述动态令牌在接收到所述反馈数据包后，输出提示信息；所述动态令牌接收输入的对应所述提示信息的确认指令；所述动态令牌根据接收到的所述确

认指令，解密所述反馈数据包获得所述反馈信息。

本发明还提供一种动态令牌，包括第一输入模块、第二输入模块、签名模块、传输模块、加解密模块和存储模块，其中，所述第一输入模块接收开启指令并根据所述开启指令执行开启操作；所述第二输入模块接收输入的操作指令并将所述操作指令发送至所述签名模块；所述签名模块根据接收到的所述操作指令生成请求信息，根据所述请求信息进行签名得到第一数字签名，根据所述请求信息和所述第一数字签名得到请求数据包，将所述请求数据包发送至所述传输模块；所述传输模块在接收到所述签名模块发来的所述请求数据包后，将所述请求数据包向外部发送，并接收从外部发来的反馈数据包，将所述反馈数据包发送至所述加解密模块；所述加解密模块在接收到所述传输模块发来的所述反馈数据包后，解密所述反馈数据包后获得所述反馈信息，并将所述反馈信息发送至所述存储模块；所述存储模块在接收到所述加解密模块发来的所述反馈信息后，保存所述反馈信息；所述签名模块在所述存储模块保存所述反馈信息后生成响应信息，对所述响应信息进行签名得到第二数字签名，根据所述响应信息和所述第二数字签名得到响应数据包，将所述响应数据包发送至所述传输模块；所述传输模块在接收到所述签名模块发来的所述响应数据包后，将所述响应数据包向外部发送。

此外，所述动态令牌还包括动态口令生成模块，用于生成动态口令。

此外，所述动态令牌还包括生效模块；所述操作指令为生效操作指令；所述请求信息为生效请求信息，所述生效请求信息包含生效操作码和账户信息；所述反馈信息包含至少一个种子密钥；所述生效模块连接至所述存储模块，并根据所述存储模块的反馈信息完成生效操作。

此外，所述反馈信息还包含事件因子信息。

此外，所述动态令牌还包括激活模块；所述操作指令为激活操作指令；所述请求信息为激活请求信息，所述激活请求信息包含激活操作码和账户信息；所述反馈信息包含激活码；所述激活模块连接至所述存储模块；所述激活模块接收到所述反馈信息后，读取所述存储模块中的反馈信息包含的所述激活码，并根据预设的激活码生成算法生成激活验证码后，比对所述激活码和所述激活验证码，若比对一致则验证所述激活码通过；或者当所述传输模块在接收外部发来的反馈数据包的同时还接收从外部发来的激活验证码时，所述传输模块将所述反馈数据包发送至所述加解密模块的同时还将所述激活验证码发送到所述激活模块，则所述激活模块接收到所述加解密模块发来的反馈信息的同时还接收到所述传输模块发来的所述激活验证码，所述激活模块比对所述激活码和所述激活验证码，若比对一致则验证所述激活码通过。

此外，所述动态令牌还包括同步模块；所述操作指令为同步操作指令；所述请求信息为同步请求信息，所述同步请求信息包含同步操作码和账户信息；所述反馈信息包含同步码；所述同步模块连接至所述存储模块，并根据所述存储模块的反馈信息完成同步操作。

此外，所述动态令牌还包括输出模块和第三输入模块；所述输出模块在所述传输模块收到所述反馈数据包后，输出提示信息；所述第三输入模块接收输入的对应所述提示信息的确认指令，并根据所述确认指令触发所述传输模块将所述反馈数据包发送至所述加解密模块的操作。

此外，所述动态令牌数据传输系统包括后台系统服务器以及上述的动态令牌；所述后台系统服务器接收从所述动态令牌发来的请求数据包，从接收到的所述请求数据包中获得所述第一数字签名和所述请求信息，并对所述第一数字签名进行验签；所述后台系统服务器对所述第一数字签名验签通过后，根据所述请求信息生成对应的反馈信息，根据所述反馈信息加密获得反馈数据包，将所述反馈数据包发送至所述动态令牌；所述后台系统服务器接收从所述动态令牌发来的所述响应数据包，从接收到的所述响应数据包中获得所述第二数字签名和所述响应信息，并对所述第二数字签名进行验签；所述后台系统服务器对所述第二数字签名验签通过后，根据所述响应信息执行响应操作。

由上述本发明提供的技术方案可以看出，本发明提供了一种动态令牌的数据传输方法及系统，当动态令牌需要与后台系统服务器进行通信时，通过数字签名和加解密等一系列方法，以改进动态令牌与后台系统服务器的通信流程。本发明解决了现有技术中动态令牌与后台系统服务器通信的不安全问题，保证了动态令牌与后台系统服务器的能够进行可靠信息交互，在对动态令牌进行生效、激活和同步操作的过程中，保证了种子密钥等关键信息的安全传输，从而保证用户账户的安全性。同时，本发明与现有技术相比，实施方便，结构简单。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，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，对于本领域的普通技术人员来讲，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附图。

图 1 为本发明实施例 1 提供的动态令牌数据传输方法的流程示意图；

图 2 为本发明实施例 1 提供的动态令牌结构示意图；

图 3 为本发明实施例 1 提供的动态令牌数据传输系统结构示意图

图 4 为本发明实施例 2 提供的动态口令牌数据传输方法的流程示意图；

图 5 为本发明实施例 2 提供的动态口令牌结构示意图；

图 6 为本发明实施例 3 提供的动态口令牌数据传输方法的流程示意图；

图 7 为本发明实施例 3 提供的动态口令牌结构示意图；

5 图 8 为本发明实施例 4 提供的动态口令牌数据传输方法的流程示意图；

图 9 为本发明实施例 4 提供的动态口令牌结构示意图。

具体实施方式

下面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
10 明的实施例，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，都属于本发明的保护范围。

在本发明的描述中，需要理解的是，术语“中心”、“纵向”、“横向”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为
15 基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发明的限制。此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或数量或位置。

在本发明的描述中，需要说明的是，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可
20 以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通。对于本领域的普通技术人员而言，可以根据具体情况理解上述术语在本发明中的具体含义。

下面将结合附图对本发明实施例作进一步地详细描述。

25

实施例 1

如图 1 所示为动态口令牌数据传输方法的流程示意图，该动态口令牌数据传输方法包括：

步骤 S101，动态口令牌接收开启指令，根据开启指令执行开启操作。

30 具体的，用户可以通过按键的方式将动态口令牌的电源开启，或者在动态口令牌已经开启的情况下，用户通过接收外部输入的进入动态口令模式指令，根据进入动态口令模式

指令，进入动态口令模式。

步骤 S102，动态口令牌接收输入的操作指令。

具体的，该操作指令可以分别是生效指令、激活指令和同步指令，用户可以通过对动态口令牌进行按键或者通过虚拟键盘输入该操作指令，或者通过将动态口令牌连接至终端（PC、笔记本、手机等），用户从终端操作并将该操作指令发送至动态口令牌。当动态口令牌首次使用时，需要先在动态口令牌进行生效和激活操作；当动态口令牌出现不能使用或其他情况时，需要对动态口令牌进行同步操作。

步骤 S103，动态口令牌在接收到操作指令之后，根据操作指令生成请求信息，对请求信息进行签名得到第一数字签名，根据请求信息和第一数字签名得到请求数据包，将请求数据包发送至后台系统服务器。

例如，动态口令牌在根据操作指令生成请求信息后，可以使用动态口令牌中的签名模块对请求信息进行签名。

具体的，根据操作指令的不同，该请求信息可以分别是生效请求信息、激活请求信息和同步请求信息。请求信息的不同，其包含的内容也各不相同，例如生效请求信息中可以包含生效请求的操作码、该动态口令牌对应的账号信息以及其他相关信息等。

另外，在现有的动态口令牌中一般只包括动态口令生成模块，而在本发明中动态口令牌不仅包括了动态口令生成模块，还包含了签名模块，该签名模块用于对待发送至后台系统服务器的数据进行签名处理后再发送，使得后台系统在接收签名数据后先进行验证，从而确定动态口令牌的身份，防止账户被篡改或劫持，从而保证动态口令牌的账户安全。动态口令牌中可以包含一对公钥和私钥以及用于签名的数字证书等，并将该公钥分发给后台系统服务器。这样，动态口令牌可以采用私钥对数据进行签名，而后台系统服务器用公钥对数据进行验证；同时，后台系统服务器可以利用公钥对数据加密后发送至动态口令牌，而动态口令牌利用私钥对信息进行解密。

具体来说，在动态口令牌生成请求信息后，步骤 S103 所述的方法可以有以下几种实现方式：

(1) 动态口令牌在利用私钥对请求信息进行签名得到第一数字签名后，将第一数字签名和请求数据形成请求数据包，将请求数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到请求信息后，通过签名确定动态口令牌的身份。

(2) 动态口令牌在利用私钥对请求信息进行签名得到第一数字签名后，将请求信息进行加密，再将加密后的请求信息以及第一数字签名形成请求数据包，将请求数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到请求信息后，通过签名确定动态口令

30

25

20

15

10

5

令牌的身份，同时对数据加密可以保证传输的安全。

(3) 动态口令牌在利用私钥对请求信息进行签名得到第一数字签名后，将第一数字签名和请求数据加密后形成请求数据包，将请求数据包发送至后台系统服务器。这样可以使

得后台系统服务器在收到请求信息后，通过签名确定动态口令牌的身份，同时对数据加密

5 可以保证传输的安全。

本发明所用签名算法为不可逆算法（如哈希算法），以防止反悔；所用解密算法可以是

对称算法或非对称算法。

至于数字签名的具体方法的其他细节均为本领域公知，在此不再赘叙。

步骤 S104，后台系统服务器接收请求数据包，从接收到的请求数据包中获得第一数字

10 签名和请求信息，并对第一数字签名进行验证。

具体的，后台系统服务器需要对动态口令牌发送过来的数据进行验证，因此后台系统

服务器中包含了与动态口令牌签名模块相对应的验证模块，例如，后台系统服务器持有对

应于动态口令牌的私钥的公钥。具体来说，在后台系统服务器接收到请求数据包后，从请

求数据包中获得（若请求数据包为加密信息则先对其解密后获得）第一数字签名和请求信

15 息，利用对应于动态口令牌私钥的公钥对动态口令牌发送过来的第一数字签名进行验证。

有关验证的详细流程为现有技术，在此不再赘叙。

步骤 S105，后台系统服务器在第一数字签名验证通过后，根据请求信息确定对应的反

馈信息，根据反馈信息加密获得反馈数据包，将反馈数据包发送至动态口令牌。

具体的，根据请求信息（可以分别是生效请求信息、激活请求信息和同步请求信息）

20 的不同，后台系统服务器选择或者生成对应的反馈信息。例如，当请求信息是生效请求信

息时，后台系统服务器根据生效请求信息中的生效请求的操作码以及相关信息，选择对应

的种子密钥和事件因子等生成对应的反馈信息。为了传输数据的安全，后台系统服务器将

反馈数据加密传输，例如，后台系统服务器采用公钥将反馈信息进行加密得到反馈数据包。

步骤 S106，动态口令牌接收反馈数据包。

25 步骤 S107，动态口令牌在接收到反馈数据包后，解密反馈数据包获得反馈信息。

具体的，动态口令牌在收到反馈数据包后，利用私钥对反馈数据包进行解密，得到反

馈信息。

步骤 S108，动态口令牌在获得反馈信息后，保存反馈信息。

步骤 S109，动态口令牌生成响应信息，对响应信息进行签名得到第二数字签名，根据

30 响应信息和第二数字签名得到响应数据包，将响应数据包发送至后台系统服务器。

例如，动态口令牌生成响应信息后，动态口令牌中的签名模块对响应信息进行签名

得到第二数字签名。

具体的，根据操作指令（生效指令、激活指令、同步指令）的不同，则动态令牌收到的反馈数据不同，则本步骤中动态令牌生成的响应信息也可以不同或者相同，例如针对生效指令，本步骤中的响应信息中可能包含指示后台系统服务器执行生效流程的信息。

5 具体来说，在动态令牌生成响应信息后，步骤 S109 所述的方法可以有以下三种实现方式：

（1）动态令牌在利用私钥对响应信息进行签名得到第二数字签名后，将第二数字签名和响应数据形成响应数据包，将响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到响应信息后，通过签名确定动态令牌的身份。

10 （2）动态令牌在利用私钥对响应信息进行签名得到第二数字签名后，将响应信息进行加密，再将加密后的响应信息以及第二数字签名形成响应数据包，将响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到响应信息后，通过签名确定动态令牌的身份，同时对数据加密可以保证传输的安全。

15 （3）动态令牌在利用私钥对响应信息进行签名得到第二数字签名后，将第二数字签名和响应数据加密后形成响应数据包，将响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到响应信息后，通过签名确定动态令牌的身份，同时对数据加密可以保证传输的安全。

步骤 S110，后台系统服务器接收响应数据包，从接收到的响应数据包中获得第二数字签名和响应信息，并对第二数字签名进行验签。

20 步骤 S111，后台系统服务器对第二数字签名验签通过后，根据响应信息执行响应操作。

具体的，后台系统服务器根据响应信息的不同，执行不同的响应操作，例如，对于对应生效指令的响应信息，则后台系统服务器将根据响应信息执行生效流程。同时，后台系统服务器还可以将生效流程置为不可用，以防止重复生效。

优选的，步骤 S108 还可以有以下两种实现方法：

25 （1）动态令牌在接收到反馈数据包后，输出提示信息后解密反馈数据包获得反馈信息。例如，当动态令牌在接收到反馈数据包时，在屏幕上显示有数据包被接收到，即代表该动态令牌执行了某操作（例如生效、激活、同步），还可以在屏幕上显示操作的进度条，以便使得用户获知操作进度，并且当发生非用户操作时，用户能够获知，从而采取措施阻止操作，保证用户账户的安全。

30 （2）动态令牌在接收到反馈数据包后，输出提示信息；动态令牌接收输入的对应提示信息的确认指令；动态令牌根据接收到的确认指令，解密反馈数据包获得反馈信息。

例如，当动态令牌在接收到反馈数据包时（即代表该动态令牌被执行了某操作，例如生效、激活、同步），则在屏幕上显示有数据包被接收到并中断操作，等待用户的确认信息，只有在用户确认之后，动态令牌才继续后续操作，解密反馈数据包获得反馈信息。这样一来，可以使得用户获知操作进度，并且当发生非用户操作时，用户能够获知，从而采取

5 措施阻止操作，保证用户账户的安全。

如图 2 所示，本实施例还提供一种应用上述动态令牌数据传输方法的动态令牌 10，该动态令牌包括第一输入模块 101、第二输入模块 102、签名模块 103、传输模块 104、加解密模块 105 和存储模块 106，其中：

第一输入模块 101 接收开启指令并根据开启指令执行开启操作。

10 具体的，第一输入模块 101 可以是按键，用户可以通过按键的方式将动态令牌的电源开启；或者在动态令牌已经开启的情况下，用户第一输入模块 101 通过接收外部输入的进入动态令牌模式指令，根据进入动态令牌模式指令，进入动态令牌模式。

第二输入模块 102 接收输入的操作指令并将操作指令发送至签名模块 103。

具体的，该操作指令可以分别是生效指令、激活指令和同步指令，第二输入模块 102

15 可以是按键或者虚拟键盘接收操作指令，或者通过将动态令牌连接至终端（PC、笔记本、手机等），用户从终端操作并将该操作指令发送至动态令牌。

签名模块 103 根据接收到的操作指令生成请求信息，根据请求信息进行签名得到第一数字签名，根据请求信息和第一数字签名得到请求数据包，将请求数据包发送传输模块 104；签名模块 103 在存储模块 106 保存反馈信息后生成响应信息，对响应信息进行签名得到第二数字签名，根据响应信息和第二数字签名得到响应数据包，将响应数据包发送至传输模

20 块 104。

传输模块 104 在接收到签名模块 103 发来的请求数据包后，将请求数据包向外部发送；传输模块 104 在接收到签名模块发来的响应数据包后，将响应数据包向外部发送；传输模块 104 接收外部发来的反馈数据包，将反馈数据包发送至加解密模块 105。

25 具体的，传输模块 104 可以有有线和无线传输模块，例如 USB 接口传输模块、音频接口传输模块、异形口传输模块、蓝牙传输模块、红外传输模块、NFC 传输模块。

具体来说，传输模块 104 在接收到签名模块 103 发来的请求数据包或者响应数据包后，都将请求数据包向后台系统服务器发送，以便后台系统服务器对数据处理并响应。

加解密模块 105 在接收到传输模块 104 发来的反馈数据包后，解密反馈数据包后获得

30 反馈信息，并将反馈信息发送至存储模块 106。

具体的，加解密模块 105 可以包含电子签名令牌的私钥，利用私钥对反馈数据包进行

解密获得反馈信息。

存储模块 106 在接收到加解密模块 105 发来的反馈信息后，保存反馈信息。

优选的，本实施例的动态令牌中还包括输出模块 107 和第三输入模块 108；输出模块 107 在传输模块 104 收到反馈数据包后，输出提示信息；第三输入模块 108 接收输入的
5 对应提示信息的确认指令，并根据确认指令触发传输模块将反馈数据包发送至加解密模块 105 的操作。

另外，本发明的动态令牌 10 还包括动态口令生成模块 109，用于根据种子密钥、事件因子、挑战码等生成动态口令。

如图 3 所示，本发明还提供一种应用上述动态令牌数据传输方法的动态令牌数据传输系统，该动态令牌数据传输系统包括上述动态令牌 10 以及后台系统服务器 20；
10 其中动态令牌执行上述方法中的功能；

后台系统服务器 20 接收从动态令牌 10 发来的请求数据包，从接收到的请求数据包中获得第一数字签名和请求信息，并对第一数字签名进行验签；

后台系统服务器 20 对第一数字签名验签通过后，根据请求信息生成对应的反馈信息，
15 根据反馈信息加密获得反馈数据包，将反馈数据包发送至动态令牌 10；

后台系统服务器 20 接收从动态令牌 10 发来的响应数据包，从接收到的响应数据包中获得第二数字签名和响应信息，并对第二数字签名进行验签；

后台系统服务器 20 对第二数字签名验签通过后，根据响应信息执行响应操作。

由上述本发明提供的技术方案可以看出，本实施例提供了一种动态令牌、动态令牌
20 牌的数据传输方法及系统，当动态令牌需要与后台系统服务器进行通信时，通过数字签名和加解密等一系列方法，以改进动态令牌与后台系统服务器的通信流程。本发明解决了现有技术中动态令牌与后台系统服务器通信的不安全问题，保证了动态令牌与后台系统服务器的能够进行可靠信息交互，在对动态令牌进行生效、激活和同步操作的过程中，保证了种子密钥等关键信息的安全传输，从而保证用户账户的安全性。同时，本发明
25 与现有技术相比，实施方便，结构简单。

实施例 2

如图 4 所示，本实施例提供一种动态令牌的数据传输方法，具体是一种动态令牌的生效方法。

30 步骤 S201，动态令牌接收开启指令，根据开启指令执行开启操作。

具体的，用户可以通过按键的方式将动态令牌的电源开启，或者在动态令牌已经

开启的情况下，用户通过接收外部输入的进入动态口令模式指令，根据进入动态口令模式指令，进入动态口令模式。

步骤 S202，动态口令牌接收输入的生效操作指令。

具体的，用户可以通过对动态口令牌进行按键或者虚拟键盘输入该生效操作指令，或者通过将动态口令牌连接至终端（PC、笔记本、手机等），用户从终端操作并将该生效操作指令发送至动态口令牌。当动态口令牌首次使用时，需要先对动态口令牌执行生效操作，以便用户可以使用动态口令牌。

步骤 S203，动态口令牌在接收到生效操作指令之后，根据生效操作指令生成生效请求信息，对生效请求信息进行签名得到第一数字签名，根据生效请求信息和第一数字签名得到生效请求数据包，将生效请求数据包发送至后台系统服务器。

例如，动态口令牌在生成生效请求信息后，动态口令牌中的签名模块对生效请求信息进行签名得到第一数字签名。

具体的，生效请求信息中可以包含生效操作码、该动态口令牌对应的账号信息以及其他相关信息等。

另外，在现有的动态口令牌中一般只包括动态口令生成模块，而在本发明中动态口令牌不仅包括了动态口令生成模块，还包含了签名模块，该签名模块用于对待发送至后台系统服务器的数据进行签名处理后再发送，使得后台系统在接收签名数据后先进行验证，从而确定动态口令牌的身份，防止账户被篡改或劫持，从而保证动态口令牌的账户安全。动态口令牌中可以包含一对公钥和私钥以及用于签名的数字证书等，并将该公钥分发给后台系统服务器。这样，动态口令牌可以采用私钥对数据进行签名，而后台系统服务器用公钥对数据进行验签；同时，后台系统服务器可以利用公钥对数据加密后发送至动态口令牌，而动态口令牌利用私钥对信息进行解密。

具体来说，在动态口令牌生成生效请求信息后，步骤 S203 所述的方法可以有以下三种实现方式：

(1) 动态口令牌在利用私钥对生效请求信息进行签名得到第一数字签名后，将第一数字签名和生效请求信息形成生效请求数据包，将生效请求数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到生效请求信息后，通过签名确定动态口令牌的身份。

(2) 动态口令牌在利用私钥对生效请求信息进行签名得到第一数字签名后，将生效请求信息进行加密，再将加密后的生效请求信息以及第一数字签名形成生效请求数据包，将生效请求数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到生效请求信息后，通过签名确定动态口令牌的身份，同时对数据加密可以保证传输的安全。

(3) 动态令牌在利用私钥对生效请求信息进行签名得到第一数字签名后, 将第一数字签名和生效请求数据加密后形成生效请求数据包, 将生效请求数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到生效请求信息后, 通过签名确定动态令牌的身份, 同时对数据加密可以保证传输的安全。

- 5 本发明所用签名算法为不可逆算法(如哈希算法), 以防止反悔; 所用解密算法可以是对称算法或非对称算法。

至于数字签名的具体方法的其他细节均为本领域公知, 在此不再赘叙。

步骤 S204, 后台系统服务器接收生效请求数据包, 从接收到的生效请求数据包中获得第一数字签名和生效请求信息, 并对第一数字签名进行验签。

- 10 具体的, 后台系统服务器需要对动态令牌发送过来的数据进行验签, 因此后台系统服务器中包含了与动态令牌签名模块相对应的验签模块, 例如, 后台系统服务器持有对应于动态令牌的私钥的公钥。具体来说, 在后台系统服务器接收到请求数据包后, 从请求数据包中获得(若请求数据包为加密信息则先对其解密后获得)第一数字签名和请求信息, 利用对应于动态令牌私钥的公钥对动态令牌发送过来的第一数字签名进行验签。
- 15 有关验签的详细流程为现有技术, 在此不再赘叙。

步骤 S205, 后台系统服务器在第一数字签名验签通过后, 根据生效请求信息确定对应的生效反馈信息, 根据生效反馈信息加密获得生效反馈数据包, 将生效反馈数据包发送至动态令牌。

- 20 具体的, 根据生效请求信息, 后台系统服务器选择或者生成对应的生效反馈信息。例如, 后台系统服务器根据生效请求信息中的生效操作码以及相关信息, 选择对应的至少一个种子密钥和事件因子等生成对应的生效反馈信息。为了传输数据的安全, 后台系统服务器将生效反馈数据加密传输, 例如, 后台系统服务器采用公钥将生效反馈信息进行加密得到生效反馈数据包。

步骤 S206, 动态令牌接收生效反馈数据包。

- 25 步骤 S207, 动态令牌在接收到生效反馈数据包后, 解密生效反馈数据包获得生效反馈信息。

具体的, 动态令牌在收到生效反馈数据包后, 利用私钥对生效反馈数据包进行解密, 得到生效反馈信息。

步骤 S208, 动态令牌在获得生效反馈信息后, 保存生效反馈信息。

- 30 步骤 S209, 动态令牌生成生效响应信息, 对生效响应信息进行签名得到第二数字签名, 根据生效响应信息和第二数字签名得到生效响应数据包, 将生效响应数据包发送至后

台系统服务器。

例如，动态令牌生成生效响应信息后，动态令牌中的签名模块对生效响应信息进行签名得到第二数字签名。

具体的，针对生效指令，本步骤中的生效响应信息中可能包含指示后台系统服务器执行生效流程的信息。

具体来说，在动态令牌生成生效响应信息后，步骤 S209 所述的方法可以有以下三种实现方式：

(1) 动态令牌在利用私钥对生效响应信息进行签名得到第二数字签名后，将第二数字签名和生效响应数据形成生效响应数据包，将生效响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到生效响应信息后，通过签名确定动态令牌的身份。

(2) 动态令牌在利用私钥对生效响应信息进行签名得到第二数字签名后，将生效响应信息进行加密，再将加密后的生效响应信息以及第二数字签名形成生效响应数据包，将生效响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到生效响应信息后，通过签名确定动态令牌的身份，同时对数据加密可以保证传输的安全。

(3) 动态令牌在利用私钥对生效响应信息进行签名得到第二数字签名后，将第二数字签名和生效响应数据加密后形成生效响应数据包，将生效响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到生效响应信息后，通过签名确定动态令牌的身份，同时对数据加密可以保证传输的安全。

步骤 S210，后台系统服务器接收生效响应数据包，从接收到的生效响应数据包中获得第二数字签名和生效响应信息，并对第二数字签名进行验签。

步骤 S211，后台系统服务器对第二数字签名验签通过后，根据生效响应信息执行生效响应操作。

具体的，对于对应生效指令的生效响应信息，后台系统服务器将根据生效响应信息执行生效流程。同时，后台系统服务器还可以将生效流程置为不可用，以防止重复生效。

优选的，步骤 S208 还可以有以下两种实现方法：

(1) 动态令牌在接收到生效反馈数据包后，输出提示信息后解密生效反馈数据包获得生效反馈信息。例如，当动态令牌在接收到生效反馈数据包时，在屏幕上显示有数据包被接收到，即代表该动态令牌执行了某操作（例如生效、激活、同步），还可以在屏幕上显示操作的进度条，以便使得用户获知操作进度，并且当发生非用户操作时，用户能够获知，从而采取措施阻止操作，保证用户账户的安全。

(2) 动态令牌在接收到生效反馈数据包后，输出提示信息；动态令牌收输入的对

应提示信息的确认指令；动态令牌根据接收到的确认指令，解密生效反馈数据包获得生效反馈信息。例如，当动态令牌在接收到生效反馈数据包时（即代表该动态令牌被执行了某操作，例如生效、激活、同步），则在屏幕上显示有数据包被接收到并中断操作，等待用户的确认信息，只有在用户确认之后，动态令牌才继续后续操作，解密生效反馈数据包获得生效反馈信息。这样一来，可以使得用户获知操作进度，并且当发生非用户操作时，用户能够获知，从而采取措施阻止操作，保证用户账户的安全。

另外，如图 5 所示，与实施例 1 相比，本实施例 2 的动态令牌还包括生效模块 110；生效模块连接至存储模块 106，并根据存储模块 106 的反馈信息完成生效操作。

具体的，生效模块 110 根据反馈信息中包含的至少一个种子密钥和事件因子信息完成生效操作。在生效成功后，动态令牌还可以将生效模块 110 置为不可用，以防止重复生效。

由上述本发明提供的技术方案可以看出，本实施例提供了动态令牌的生效数据传输方法，当动态令牌需要与后台系统服务器进行通信时，通过数字签名和加解密等一系列方法，以改进动态令牌与后台系统服务器的通信流程。本发明解决了现有技术中动态令牌与后台系统服务器通信的不安全问题，保证了动态令牌与后台系统服务器的能够进行可靠信息交互，在对动态令牌进行生效、激活和同步操作的过程中，保证了种子密钥等关键信息的安全传输，从而保证用户账户的安全性。同时，本发明与现有技术相比，实施方便，结构简单。

实施例 3

如图 6 所示，本实施例提供一种动态令牌的数据传输方法，具体是一种动态令牌的激活数据传输方法。

步骤 S301，动态令牌接收开启指令，根据开启指令执行开启操作。

具体的，用户可以通过按键的方式将动态令牌的电源开启，或者在动态令牌已经开启的情况下，用户通过接收外部输入的进入动态令牌模式指令，根据进入动态令牌模式指令，进入动态令牌模式。

步骤 S303，动态令牌接收输入的激活操作指令。

具体的，用户可以通过对动态令牌进行按键或者虚拟键盘输入该激活操作指令，或者通过将动态令牌连接至终端（PC、笔记本、手机等），用户从终端操作并将该激活操作指令发送至动态令牌。当动态令牌首次使用时，需要先对动态令牌执行激活操作，以便用户可以使用动态令牌。

步骤 S303, 动态口令牌在接收到激活操作指令之后, 根据激活操作指令生成激活请求信息, 对激活请求信息进行签名得到第一数字签名, 根据激活请求信息和第一数字签名得到激活请求数据包, 将激活请求数据包发送至后台系统服务器。

例如, 动态口令牌生成激活请求信息后, 动态口令牌中的签名模块对激活请求信息进行签名得到第一数字签名。

具体的, 激活请求信息中可以包含激活操作码、该动态口令牌对应的账号信息以及其他相关信息等。

另外, 在现有的动态口令牌中一般只包括动态口令生成模块, 而在本发明中动态口令牌不仅包括了动态口令生成模块, 还包含了签名模块, 该签名模块用于对待发送至后台系统服务器的数据进行签名处理后再发送, 使得后台系统在接收签名数据后先进行验证, 从而确定动态口令牌的身份, 防止账户被篡改或劫持, 从而保证动态口令牌的账户安全。动态口令牌中可以包含一对公钥和私钥以及用于签名的数字证书等, 并将该公钥分发给后台系统服务器。这样, 动态口令牌可以采用私钥对数据进行签名, 而后台系统服务器用公钥对数据进行验签; 同时, 后台系统服务器可以利用公钥对数据加密后发送至动态口令牌, 而动态口令牌利用私钥对信息进行解密。

具体来说, 在动态口令牌生成激活请求信息后, 步骤 S303 所述的方法可以有以下三种实现方式:

(1) 动态口令牌在利用私钥对激活请求信息进行签名得到第一数字签名后, 将第一数字签名和激活请求信息形成激活请求数据包, 将激活请求数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到激活请求信息后, 通过签名确定动态口令牌的身份。

(2) 动态口令牌在利用私钥对激活请求信息进行签名得到第一数字签名后, 将激活请求信息进行加密, 再将加密后的激活请求信息以及第一数字签名形成激活请求数据包, 将激活请求数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到激活请求信息后, 通过签名确定动态口令牌的身份, 同时对数据加密可以保证传输的安全。

(3) 动态口令牌在利用私钥对激活请求信息进行签名得到第一数字签名后, 将第一数字签名和激活请求数据加密后形成激活请求数据包, 将激活请求数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到激活请求信息后, 通过签名确定动态口令牌的身份, 同时对数据加密可以保证传输的安全。

本发明所用签名算法为不可逆算法 (如哈希算法), 以防止反悔; 所用解密算法可以是对称算法或非对称算法。

至于数字签名的具体方法的其他细节均为本领域公知, 在此不再赘叙。

步骤 S304, 后台系统服务器接收激活请求数据包, 从接收到的激活请求数据包中获得第一数字签名和激活请求信息, 并对第一数字签名进行验签。

具体的, 后台系统服务器需要对动态令牌发送过来的数据进行验签, 因此后台系统服务器中包含了与动态令牌签名模块相对应的验签模块, 例如, 后台系统服务器持有对应于动态令牌的私钥的公钥。具体来说, 在后台系统服务器接收到请求数据包后, 从请求数据包中获得 (若请求数据包为加密信息则先对其解密后获得) 第一数字签名和请求信息, 利用对应于动态令牌私钥的公钥对动态令牌发送过来的第一数字签名进行验签。有关验签的详细流程为现有技术, 在此不再赘叙。

步骤 S305, 后台系统服务器在第一数字签名验签通过后, 根据激活请求信息确定对应的激活反馈信息, 根据激活反馈信息加密获得激活反馈数据包, 将激活反馈数据包发送至动态令牌。

具体的, 根据激活请求信息, 后台系统服务器选择或者生成对应的激活反馈信息。例如, 后台系统服务器根据激活请求信息中的激活操作码以及相关信息, 选择或者生成激活码从而确定激活反馈信息。后台系统服务器通过以下两种方式确定激活反馈信息: (1) 后台系统服务器生成激活码, 对激活码加密, 并根据加密后的激活码得到激活反馈信息; (2) 后台系统服务器生成激活码及激活验证码, 对激活码及激活验证码加密, 并根据加密后的激活码及激活验证码得到激活反馈信息。

步骤 S306, 动态令牌接收激活反馈数据包。

步骤 S307, 动态令牌在接收到激活反馈数据包后, 解密激活反馈数据包获得激活反馈信息。

具体的, 动态令牌在收到激活反馈数据包后, 利用私钥对激活反馈数据包进行解密, 得到激活反馈信息。

步骤 S308, 动态令牌在获得激活反馈信息后, 保存激活反馈信息。

步骤 S309, 动态令牌对反馈信息中包含的激活码进行验证。

具体的, 动态令牌对反馈信息中包含的激活码进行验证的步骤包括以下两种方式:

(1) 动态令牌读取反馈信息中包含的激活码; 动态令牌根据预设的激活码生成算法生成激活验证码; 动态令牌比对激活码和激活验证码, 比对一致, 则触发动态令牌生成响应信息的操作。

(2) 当后台系统服务器将反馈数据包和激活验证码一起发送至动态令牌时, 动态令牌在接收到反馈数据包和激活验证码, 从反馈数据包中获得反馈信息后, 比对反馈信息中的激活码和激活验证码, 比对一致, 则触发动态令牌生成响应信息的操作。

步骤 S310, 动态令牌对激活码验证通过后, 生成激活响应信息, 对激活响应信息进行签名得到第二数字签名, 根据激活响应信息和第二数字签名得到激活响应数据包, 将激活响应数据包发送至后台系统服务器。

例如, 动态令牌生成激活响应信息后, 动态令牌中的签名模块对激活响应信息进行签名得到第二数字签名。

具体的, 针对激活指令, 本步骤中的激活响应信息中可能包含指示后台系统服务器执行激活流程的信息。

具体来说, 在动态令牌生成激活响应信息后, 步骤 S309 所述的方法可以有以下三种实现方式:

10 (1) 动态令牌在利用私钥对激活响应信息进行签名得到第二数字签名后, 将第二数字签名和激活响应数据形成激活响应数据包, 将激活响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到激活响应信息后, 通过签名确定动态令牌的身份。

(3) 动态令牌在利用私钥对激活响应信息进行签名得到第二数字签名后, 将激活响应信息进行加密, 再将加密后的激活响应信息以及第二数字签名形成激活响应数据包, 将
15 激活响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到激活响应信息后, 通过签名确定动态令牌的身份, 同时对数据加密可以保证传输的安全。

(3) 动态令牌在利用私钥对激活响应信息进行签名得到第二数字签名后, 将第二数字签名和激活响应数据加密后形成激活响应数据包, 将激活响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到激活响应信息后, 通过签名确定动态令牌的身份, 同时对数据加密可以保证传输的安全。
20

步骤 S311, 后台系统服务器接收激活响应数据包, 从接收到的激活响应数据包中获得第二数字签名和激活响应信息, 并对第二数字签名进行验签。

步骤 S312, 后台系统服务器对第二数字签名验签通过后, 根据激活响应信息执行激活响应操作。

25 具体的, 对于对应激活指令的激活响应信息, 后台系统服务器将根据激活响应信息执行激活流程。同时, 后台系统服务器还可以将激活流程置为不可用, 以防止重复激活。

优选的, 步骤 S308 还可以有以下两种实现方法:

(1) 动态令牌在接收到激活反馈数据包后, 输出提示信息后解密激活反馈数据包获得激活反馈信息。例如, 当动态令牌在接收到激活反馈数据包时, 在屏幕上显示有数据包被接收到, 即代表该动态令牌执行了某操作 (例如激活、激活、同步), 还可以在屏幕上显示操作的进度条, 以便使得用户获知操作进度, 并且当发生非用户操作时, 用户能够
30

获知，从而采取措施阻止操作，保证用户账户的安全。

(3) 动态令牌在接收到激活反馈数据包后，输出提示信息；动态令牌收输入的对应提示信息的确认指令；动态令牌根据接收到的确认指令，解密激活反馈数据包获得激活反馈信息。例如，当动态令牌在接收到激活反馈数据包时（即代表该动态令牌被执行了某操作，例如激活、激活、同步），则在屏幕上显示有数据包被接收到并中断操作，等待用户的确认信息，只有在用户确认之后，动态令牌才继续后续操作，解密激活反馈数据包获得激活反馈信息。这样一来，可以使得用户获知操作进度，并且当发生非用户操作时，用户能够获知，从而采取措施阻止操作，保证用户账户的安全。

另外，如图 7 所示，与实施例 1 相比，本实施例 3 的动态令牌还包括激活模块 111，激活模块 111 连接至存储模块 106，所述激活模块有以下两种方式对激活码进行验证：

(1) 激活模块 111 接收到反馈信息后，读取存储模块 106 中的反馈信息包含的激活码，并根据预设的激活码生成算法生成激活验证码后，比对激活码和激活验证码，若比对一致则验证激活码通过。

(2) 当传输模块 104 在接收外部发来的反馈数据包的同时还接收从后台系统服务器发来的激活验证码时，传输模块 104 将反馈数据包发送至加解密模块 105 的同时还将激活验证码发送到激活模块 111，则激活模块 111 读取存储模块 106 中的反馈信息的同时还接收到传输模块 104 发来的激活验证码，激活模块 111 比对激活码和激活验证码，若比对一致则验证激活码通过。

由上述本发明提供的技术方案可以看出，本实施例提供了动态令牌的激活数据传输方法，当动态令牌需要与后台系统服务器进行通信时，通过数字签名和加解密等一系列方法，以改进动态令牌与后台系统服务器的通信流程。本发明解决了现有技术中动态令牌与后台系统服务器通信的不安全问题，保证了动态令牌与后台系统服务器的能够进行可靠信息交互，在对动态令牌进行生效、激活和同步操作的过程中，保证了种子密钥等关键信息的安全传输，从而保证用户账户的安全性。同时，本发明与现有技术相比，实施方便，结构简单。

实施例 4

如图 8 所示，本实施例提供一种动态令牌的数据传输方法，具体是一种动态令牌的同步数据传输方法。由于动态令牌在使用的过程中，误操作或者漏操作都有可能导致动态令牌的事件因子信息与后台系统服务器的事件因子信息不同步，由于事件因子是动态令牌生成动态口令的因素之一，因此在事件因子不同步时，会导致动态令牌产生的

动态口令与后台系统服务器不匹配，则导致该动态口令牌不能使用，此时则需要对动态口令牌进行同步操作。

步骤 S401，动态口令牌接收开启指令，根据开启指令执行开启操作。

具体的，用户可以通过按键的方式将动态口令牌的电源开启，或者在动态口令牌已经
5 开启的情况下，用户通过接收外部输入的进入动态口令模式指令，根据进入动态口令模式指令，进入动态口令模式。

步骤 S402，动态口令牌接收输入的同步操作指令。

具体的，用户可以通过对动态口令牌进行按键或者虚拟键盘输入该同步操作指令，或者通过将动态口令牌连接至终端（PC、笔记本、手机等），用户从终端操作并将该同步操
10 作指令发送至动态口令牌。当动态口令牌首次使用时，需要先对动态口令牌执行同步操作，以便用户可以使用动态口令牌。

步骤 S403，动态口令牌在接收到同步操作指令之后，根据同步操作指令生成同步请求信息，对同步请求信息进行签名得到第一数字签名，根据同步请求信息和第一数字签名得到同步请求数据包，将同步请求数据包发送至后台系统服务器。

15 例如，动态口令牌在生成同步请求信息后，动态口令牌中的签名模块对同步请求信息进行签名得到第一数字签名。

具体的，同步请求信息中可以包含同步操作码、该动态口令牌对应的账号信息以及其他相关信息等。

另外，在现有的动态口令牌中一般只包括动态口令生成模块，而在本发明中动态口令
20 牌不仅包括了动态口令生成模块，还包含了签名模块，该签名模块用于对待发送至后台系统服务器的数据进行签名处理后再发送，使得后台系统在接收签名数据后先进行验证，从而确定动态口令牌的身份，防止账户被篡改或劫持，从而保证动态口令牌的账户安全。动态口令牌中可以包含一对公钥和私钥以及用于签名的数字证书等，并将该公钥分发给后台系统服务器。这样，动态口令牌可以采用私钥对数据进行签名，而后台系统服务器用公钥
25 对数据进行验签；同时，后台系统服务器可以利用公钥对数据加密后发送至动态口令牌，而动态口令牌利用私钥对信息进行解密。

具体来说，在动态口令牌生成同步请求信息后，步骤 S403 所述的方法可以有以下三种实现方式：

（1）动态口令牌在利用私钥对同步请求信息进行签名得到第一数字签名后，将第一数字
30 签名和同步请求信息形成同步请求数据包，将同步请求数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到同步请求信息后，通过签名确定动态口令牌的身份。

(2) 动态令牌在利用私钥对同步请求信息进行签名得到第一数字签名后, 将同步请求信息进行加密, 再将加密后的同步请求信息以及第一数字签名形成同步请求数据包, 将同步请求数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到同步请求信息后, 通过签名确定动态令牌的身份, 同时对数据加密可以保证传输的安全。

5 (3) 动态令牌在利用私钥对同步请求信息进行签名得到第一数字签名后, 将第一数字签名和同步请求数据加密后形成同步请求数据包, 将同步请求数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到同步请求信息后, 通过签名确定动态令牌的身份, 同时对数据加密可以保证传输的安全。

10 本发明所用签名算法为不可逆算法(如哈希算法), 以防止反悔; 所用解密算法可以是对称算法或非对称算法。

至于数字签名的具体方法的其他细节均为本领域公知, 在此不再赘叙。

步骤 S404, 后台系统服务器接收同步请求数据包, 从接收到的同步请求数据包中获得第一数字签名和同步请求信息, 并对第一数字签名进行验签。

15 具体的, 后台系统服务器需要对动态令牌发送过来的数据进行验签, 因此后台系统服务器中包含了与动态令牌签名模块相对应的验签模块, 例如, 后台系统服务器持有对应于动态令牌的私钥的公钥。具体来说, 在后台系统服务器接收到请求数据包后, 从请求数据包中获得(若请求数据包为加密信息则先对其解密后获得)第一数字签名和请求信息, 利用对应于动态令牌私钥的公钥对动态令牌发送过来的第一数字签名进行验签。有关验签的详细流程为现有技术, 在此不再赘叙。

20 步骤 S405, 后台系统服务器在第一数字签名验签通过后, 根据同步请求信息确定对应的同步反馈信息, 根据同步反馈信息加密获得同步反馈数据包, 将同步反馈数据包发送至动态令牌。

25 具体的, 根据同步请求信息, 后台系统服务器选择或者生成对应的同步反馈信息。例如, 后台系统服务器根据同步请求信息中的同步操作码以及相关信息, 生成同步码, 同步码中包括了后台系统服务器的事件因子信息, 根据同步码确定同步反馈信息。为了传输数据的安全, 后台系统服务器将同步反馈数据加密传输, 例如, 后台系统服务器采用公钥将同步反馈信息进行加密得到同步反馈数据包。

步骤 S406, 动态令牌接收同步反馈数据包。

30 步骤 S407, 动态令牌在接收到同步反馈数据包后, 解密同步反馈数据包获得同步反馈信息。

具体的, 动态令牌在收到同步反馈数据包后, 利用私钥对同步反馈数据包进行解密,

得到同步反馈信息。

步骤 S408, 动态口令牌在获得同步反馈信息后, 保存同步反馈信息。

具体的, 动态口令牌根据同步反馈信息中获得同步码, 并用同步码中的事件因子替换原本的事件因子, 从而使动态口令牌得到同步, 从而可以使用。

- 5 步骤 S409, 动态口令牌生成同步响应信息, 对同步响应信息进行签名得到第二数字签名, 根据同步响应信息和第二数字签名得到同步响应数据包, 将同步响应数据包发送至后台系统服务器。

例如, 动态口令牌生成同步响应信息后, 动态口令牌中的签名模块对同步响应信息进行签名得到第二数字签名。

- 10 具体的, 针对同步指令, 本步骤中的同步响应信息中可能包含指示后台系统服务器执行同步流程的信息。

具体来说, 在动态口令牌生成同步响应信息后, 步骤 S409 所述的方法可以有以下三种实现方式:

- 15 (1) 动态口令牌在利用私钥对同步响应信息进行签名得到第二数字签名后, 将第二数字签名和同步响应数据形成同步响应数据包, 将同步响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到同步响应信息后, 通过签名确定动态口令牌的身份。

- 20 (4) 动态口令牌在利用私钥对同步响应信息进行签名得到第二数字签名后, 将同步响应信息进行加密, 再将加密后的同步响应信息以及第二数字签名形成同步响应数据包, 将同步响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到同步响应信息后, 通过签名确定动态口令牌的身份, 同时对数据加密可以保证传输的安全。

- 25 (3) 动态口令牌在利用私钥对同步响应信息进行签名得到第二数字签名后, 将第二数字签名和同步响应数据加密后形成同步响应数据包, 将同步响应数据包发送至后台系统服务器。这样可以使得后台系统服务器在收到同步响应信息后, 通过签名确定动态口令牌的身份, 同时对数据加密可以保证传输的安全。

- 步骤 S410, 后台系统服务器接收同步响应数据包, 从接收到的同步响应数据包中获得第二数字签名和同步响应信息, 并对第二数字签名进行验签。

步骤 S411, 后台系统服务器对第二数字签名验签通过后, 根据同步响应信息执行同步响应操作。

- 30 具体的, 对于对应同步指令的同步响应信息, 后台系统服务器将根据同步响应信息执行同步流程。

优选的, 步骤 S408 还可以有以下两种实现方法:

(1) 动态令牌在接收到同步反馈数据包后，输出提示信息后解密同步反馈数据包获得同步反馈信息。例如，当动态令牌在接收到同步反馈数据包时，在屏幕上显示有数据包被接收到，即代表该动态令牌执行了某操作（例如同步、激活、同步），还可以在屏幕上显示操作的进度条，以便使得用户获知操作进度，并且当发生非用户操作时，用户能够获知，从而采取措施阻止操作，保证用户账户的安全。

(2) 动态令牌在接收到同步反馈数据包后，输出提示信息；动态令牌收输入的对应提示信息的确认指令；动态令牌根据接收到的确认指令，解密同步反馈数据包获得同步反馈信息。例如，当动态令牌在接收到同步反馈数据包时（即代表该动态令牌被执行了某操作，例如同步、激活、同步），则在屏幕上显示有数据包被接收到并中断操作，等待用户的确认信息，只有在用户确认之后，动态令牌才继续后续操作，解密同步反馈数据包获得同步反馈信息。这样一来，可以使得用户获知操作进度，并且当发生非用户操作时，用户能够获知，从而采取措施阻止操作，保证用户账户的安全。

另外，如图 9 所示，与实施例 1 相比，本实施例 3 的动态令牌还包括同步模块 112；同步模块 112 连接至存储模块 106，并根据存储模块 106 的反馈信息完成同步操作。

由上述本发明提供的技术方案可以看出，本实施例提供了动态令牌的同步数据传输方法，当动态令牌需要与后台系统服务器进行通信时，通过数字签名和加解密等一系列方法，以改进动态令牌与后台系统服务器的通信流程。本发明解决了现有技术中动态令牌与后台系统服务器通信的不安全问题，保证了动态令牌与后台系统服务器的能够进行可靠信息交互，在对动态令牌进行生效、激活和同步操作的过程中，保证了种子密钥等关键信息的安全传输，从而保证用户账户的安全性。同时，本发明与现有技术相比，实施方便，结构简单。

流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路

的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列（PGA），现场可编程门阵列（FPGA）等。

本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，

5 该程序在执行时，包括方法实施例的步骤之一或其组合。

此外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用，也可以存储在一个计算机可读
10 取存储介质中。

上述提到的存储介质可以是只读存储器，磁盘或光盘等。

在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定
15 指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何一个或多个实施例或示例中以合适的方式结合。

尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在不脱离本发明的原理和宗旨的情况下在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。本发明的范围由所
20 附权利要求及其等同限定。

权利要求书

1、动态令牌牌数据传输方法，其特征在于，所述传输方法包括：

所述动态令牌牌接收开启指令，根据所述开启指令执行开启操作；

5 所述动态令牌牌接收输入的操作指令；

所述动态令牌牌在接收到所述操作指令之后，根据所述操作指令生成请求信息，对所述请求信息进行签名得到第一数字签名，根据所述请求信息和所述第一数字签名得到请求数据包，将所述请求数据包发送至后台系统服务器；

10 所述后台系统服务器接收所述请求数据包，从接收到的所述请求数据包中获得所述第一数字签名和所述请求信息，并对所述第一数字签名进行验签；

所述后台系统服务器在所述第一数字签名验签通过后，根据所述请求信息确定对应的反馈信息，根据所述反馈信息加密获得反馈数据包，将所述反馈数据包发送至所述动态令牌牌；

所述动态令牌牌接收所述反馈数据包；

15 所述动态令牌牌在接收到所述反馈数据包后，解密所述反馈数据包获得所述反馈信息；
所述动态令牌牌在获得所述反馈信息后，保存所述反馈信息；

所述动态令牌牌生成响应信息，对所述响应信息进行签名得到第二数字签名，根据所述响应信息和所述第二数字签名得到响应数据包，将所述响应数据包发送至所述后台系统服务器；

20 所述后台系统服务器接收所述响应数据包，从接收到的所述响应数据包中获得所述第二数字签名和所述响应信息，并对所述第二数字签名进行验签；

所述后台系统服务器对所述第二数字签名验签通过后，根据所述响应信息执行响应操作。

25 2、根据权利要求1所述的动态令牌牌数据传输方法，其特征在于，所述操作指令为生效操作指令；

所述请求信息为生效请求信息，所述生效请求信息包含生效操作码和账户信息；

所述反馈信息包含至少一个种子密钥。

3、根据权利要求2所述的动态令牌牌数据传输方法，其特征在于，所述反馈信息还包含事件因子信息。

30 4、根据权利要求1所述的动态令牌牌数据传输方法，其特征在于，所述操作指令为激

活操作指令；

所述请求信息为激活请求信息，所述激活请求信息包含激活操作码和账户信息；

所述反馈信息包含激活码；

所述动态口令牌在获得所述反馈信息后，保存所述反馈信息的步骤之后，该方法还包

5 括：

所述动态口令牌对所述反馈信息中包含的所述激活码进行验证；

所述动态口令牌对所述激活码验证通过后，触发所述动态口令牌生成响应信息的操作。

5、根据权利要求4所述的动态口令牌数据传输方法，其特征在于，所述动态口令牌对所述反馈信息中包含的所述激活码进行验证的步骤包括：

10 所述动态口令牌读取所述反馈信息中包含的所述激活码；所述动态口令牌根据预设的激活码生成算法生成激活验证码；所述动态口令牌比对所述激活码和所述激活验证码，比对一致，则触发动态口令牌生成响应信息的操作；或者

当所述后台系统服务器将所述反馈数据包和激活验证码一起发送至所述动态口令牌时，所述动态口令牌在接收到所述反馈数据包和激活验证码，从所述反馈数据包中获得所
15 述反馈信息后，比对所述反馈信息中的激活码和所述激活验证码，比对一致，则触发动态口令牌生成响应信息的操作。

6、根据权利要求1所述的动态口令牌数据传输方法，其特征在于，所述操作指令为同步操作指令；

所述请求信息为同步请求信息，所述同步请求信息包含同步操作码和账户信息；

20 所述反馈信息包含同步码。

7、根据权利要求1至6任一项所述的动态口令牌数据传输方法，其特征在于，所述动态口令牌在接收到所述反馈数据包后，解密所述反馈数据包获得所述反馈信息的步骤包括：

所述动态口令牌在接收到所述反馈数据包后，输出提示信息；

所述动态口令牌接收输入的对应所述提示信息的确认指令；

25 所述动态口令牌根据接收到的所述确认指令，解密所述反馈数据包获得所述反馈信息。

8、动态口令牌，其特征在于，所述动态口令牌包括第一输入模块、第二输入模块、签名模块、传输模块、加解密模块和存储模块，其中，

所述第一输入模块接收开启指令并根据所述开启指令执行开启操作；

所述第二输入模块接收输入的操作指令并将所述操作指令发送至所述签名模块；

30 所述签名模块根据接收到的所述操作指令生成请求信息，对所述请求信息进行签名得到第一数字签名，根据所述请求信息和所述第一数字签名得到请求数据包，将所述请求数

据包发送至所述传输模块；

所述传输模块在接收到所述签名模块发送的所述请求数据包后，将所述请求数据包向外部发送，并接收从外部发来的反馈数据包，将所述反馈数据包发送至所述加解密模块；

所述加解密模块在接收到所述传输模块发来的所述反馈数据包后，解密所述反馈数据包获得反馈信息，并将所述反馈信息发送至所述存储模块；

所述存储模块在接收到所述加解密模块发来的所述反馈信息后，保存所述反馈信息；

所述签名模块在所述存储模块保存所述反馈信息后生成响应信息，对所述响应信息进行签名得到第二数字签名，根据所述响应信息和所述第二数字签名得到响应数据包，将所述响应数据包发送至所述传输模块；

所述传输模块在接收到所述签名模块发来的所述响应数据包后，将所述响应数据包向外部发送。

9、根据权利要求8所述的动态口令牌，其特征在于，所述动态口令牌还包括动态口令生成模块，用于生成动态口令。

10、根据权利要求8或9所述的动态口令牌，其特征在于，所述动态口令牌还包括生效模块；

所述操作指令为生效操作指令；

所述请求信息为生效请求信息，所述生效请求信息包含生效操作码和账户信息；

所述反馈信息包含至少一个种子密钥；

所述生效模块连接至所述存储模块，并根据所述存储模块的反馈信息完成生效操作。

11、根据权利要求10所述的动态口令牌，其特征在于，所述反馈信息还包含事件因子信息。

12、根据权利要求8或9所述的动态口令牌，其特征在于，所述动态口令牌还包括激活模块；

所述操作指令为激活操作指令；

所述请求信息为激活请求信息，所述激活请求信息包含激活操作码和账户信息；

所述反馈信息包含激活码；

所述激活模块连接至所述存储模块；

所述激活模块接收到所述反馈信息后，读取所述存储模块中的反馈信息包含的所述激活码，并根据预设的激活码生成算法生成激活验证码后，比对所述激活码和所述激活验证码，若比对一致则验证所述激活码通过；或者

当所述传输模块在接收外部发来的反馈数据包的同时还接收从外部发来的激活验证码

时，所述传输模块将所述反馈数据包发送至所述加解密模块的同时还将所述激活验证码发送到所述激活模块，则所述激活模块接收到所述加解密模块发来的反馈信息的同时还接收到所述传输模块发来的所述激活验证码，所述激活模块比对所述激活码和所述激活验证码，若比对一致则验证所述激活码通过。

- 5 13、根据权利要求 8 或 9 所述的动态口令牌，其特征在于，所述动态口令牌还包括同步模块；

所述操作指令为同步操作指令；

所述请求信息为同步请求信息，所述同步请求信息包含同步操作码和账户信息；

所述反馈信息包含同步码；

- 10 所述同步模块连接至所述存储模块，并根据所述存储模块的反馈信息完成同步操作。

14、根据权利要求 8 至 13 任一项所述的动态口令牌，其特征在于，所述动态口令牌还包括输出模块和第三输入模块；

所述输出模块在所述传输模块收到所述反馈数据包后，输出提示信息；

- 15 所述第三输入模块接收输入的对应所述提示信息的确认指令，并根据所述确认指令触发所述传输模块将所述反馈数据包发送至所述加解密模块的操作。

15、动态口令牌数据传输系统，其特征在于，所述动态口令牌数据传输系统包括后台系统服务器以及如权利要求 8-14 中任一项所述的动态口令牌；

所述后台系统服务器接收从所述动态口令牌发来的请求数据包，从接收到的所述请求数据包中获得所述第一数字签名和所述请求信息，并对所述第一数字签名进行验签；

- 20 所述后台系统服务器对所述第一数字签名验签通过后，根据所述请求信息生成对应的反馈信息，根据所述反馈信息加密获得反馈数据包，将所述反馈数据包发送至所述动态口令牌；

所述后台系统服务器接收从所述动态口令牌发来的所述响应数据包，从接收到的所述响应数据包中获得所述第二数字签名和所述响应信息，并对所述第二数字签名进行验签；

- 25 所述后台系统服务器对所述第二数字签名验签通过后，根据所述响应信息执行响应操作。