WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:		**PCT/CN2018/097200**
International filing date:		**26 July 2018 (26.07.2018)**
Document type:		**Certified copy of priority document**
Document details:	Country/Office:	**CN**
	Number:	**201710647845.3**
	Filing date:	**01 August 2017 (01.08.2017)**
Date of receipt at the International Bureau:		**24 August 2018 (24.08.2018)**

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-*bis*)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

证　明

本证明之附件是向本局提交的下列专利申请文件副本。

申　　请　　号：201710647845.3

申　请　类　型：发明专利

发明 创造 名称：支付数据处理方法、系统、交易装置与服务器

申　　请　　日：2017.08.01

申　　请　　人：苏州海博智能系统有限公司

发明人或设计人：刘国、张徽

局长

申长雨

2018 年 08 月 21 日

2017106478453

权　利　要　求　书

1、一种交易装置的支付数据处理方法，其特征在于，包括：

验证所输入的第一凭证通过，产生动态口令；

向服务器发送所述动态口令；

接收通讯设备生成并发送的交易报文；

显示所述交易报文的部分或全部信息；

验证所输入的第二凭证通过，向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认交易成功；其中，所述交易报文签名为根据用户的确认操作和所述交易报文产生的。

2、根据权利要求 1 所述的方法，其特征在于，所述第一凭证包括以下至少之一：

第一密码信息；

第一指纹信息；

第一指令信息。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述第二凭证包括以下至少之一：

第二密码信息；

第二指纹信息；

第二指令信息。

4、一种服务器的支付数据处理方法，其特征在于，包括：

接收交易装置发送的动态口令；所述动态口令为所述交易装置验证所输入的第一凭证通过后产生的；

验证所述动态口令通过；

接收所述交易装置发送的交易报文签名，所述交易报文签名为所述交易装置验证所输入的第二凭证通过后根据用户的确认操作和交易报文产生的；

验证所述交易报文签名通过，确认交易成功。

5、根据权利要求 4 所述的方法，其特征在于，所述第一凭证包括以下至少之一：

第一密码信息；

第一指纹信息；

第一指令信息。

6、根据权利要求 4 或 5 所述的方法，其特征在于，所述第二凭证包括以下至少之一：

第二密码信息；

第二指纹信息；

第二指令信息。

7、一种交易装置，其特征在于，包括：

所述安全模块，用于验证所输入的第一凭证通过，并反馈第一信号至所述控制器；以及：响应于所述控制器反馈的第二信号，验证所输入的第二凭证通过，并反馈第三信号至所述控制器；

所述控制器，用于接收所述第一信号产生动态口令，并向服务器发送所述动态口令；接收所述通讯设备生成并发送的交易报文，向所述安全模块发送所述第二信号，并驱动显示所述交易报文的部分或全部信息；接收所述安全模块发送的第三信号；以及：向所述服务器发送交易报文签名，其中，所述交易报文签名为根据用户的确认操作和所述交易报文产生的。

8、一种交易装置，其特征在于，包括：

第一验证模块，用于验证所输入的第一凭证通过，产生动态口令；

口令发送模块，用于向服务器发送所述动态口令；

报文接收模块，用于接收通讯设备生成并发送的交易报文；

显示模块，用于显示所述交易报文的部分或全部信息；

第二验证模块，用于验证所输入的第二凭证通过，向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认

交易成功；其中，所述交易报文签名为根据用户的确认操作和所述交易报文产生的。

9、一种服务器，其特征在于，包括：

口令接收模块，用于接收交易装置发送的动态口令；所述动态口令为所述交易装置验证所输入的第一凭证通过后产生的；

口令验证模块，用于验证所述动态口令通过；

签名接收模块，用于接收所述交易装置发送的交易报文签名，所述交易报文签名为所述交易装置验证所输入的第二凭证通过后根据用户的确认操作和交易报文产生的；

签名验证模块，用于验证所述交易报文签名通过，确认交易成功。

10、一种支付数据处理系统，其特征在于，包括：交易装置、通讯设备与服务器；

所述交易装置用于：

验证所输入的第一凭证通过，产生动态口令；

通过所述通讯设备向服务器发送所述动态口令；

接收所述通讯设备生成并发送的交易报文；

显示所述交易报文的部分或全部信息；

验证所输入的第二凭证通过，通过所述通讯设备向所述服务器发送交易报文签名；其中，所述交易报文签名为根据用户的确认操作和所述交易报文产生的；

所述服务器用于：

通过所述通讯设备接收交易装置发送的动态口令；

验证所述动态口令通过；

通过所述通讯设备接收所述交易装置发送的交易报文签名；

验证所述交易报文签名通过，确认交易成功。

2017106478453

说　　明　　书

支付数据处理方法、系统、交易装置与服务器

技术领域

本发明涉及移动支付，尤其涉及一种支付数据处理方法、系统、交易装置与服务器。

背景技术

目前，网上银行交易大部分使用的都是USBKEY，即U盾。使用U盾的交易过程如下：

1）、给U盾上电；

2）、登录网上银行，需要输入登录密码；

3）、输入U盾登录密码（可能与登录网上银行密码一致）；

4）、产生交易信息，并在U盾上确认信息的准确性；

5）、U盾产生交易签名，并传到后台，交易结束

该方式存在一定的危险性，因为个人电脑的键盘有可能被监听，这会导致密码泄露，从而产生安全风险。

为了降低风险，现有的相关技术中，可以采用例如虚拟桌面的技术，其中，电脑端输入密码时，拒绝其他进程运行，以此达到防止键盘被监听的目的。但这增加了软件的复杂程度，并不利于用户的使用体验。

发明内容

本发明提供一种支付数据处理方法、系统、交易装置与服务器，以解决以较佳的用户体验降低安全风险的问题。

根据本发明的第一方面，提供了一种交易装置的支付数据处理方法，包括：

2017106478453

验证所输入的第一凭证通过，产生动态口令；

向服务器发送所述动态口令；

接收通讯设备生成并发送的交易报文；

显示所述交易报文的部分或全部信息；

验证所输入的第二凭证通过，向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认交易成功；其中，所述交易报文签名为根据用户的确认操作和所述交易报文产生的。

可选的，所述第一凭证包括以下至少之一：

第一密码信息；

第一指纹信息；

第一指令信息。

可选的，所述第二凭证包括以下至少之一：

第二密码信息；

第二指纹信息；

第二指令信息。

根据本发明的第二方面，提供了一种服务器的支付数据处理方法，包括：

接收交易装置发送的动态口令；所述动态口令为所述交易装置验证所输入的第一凭证通过后产生的；

验证所述动态口令通过；

接收所述交易装置发送的交易报文签名，所述交易报文签名为所述交易装置验证所输入的第二凭证通过后根据用户的确认操作和交易报文产生的；

验证所述交易报文签名通过，确认交易成功。

可选的，所述第一凭证包括以下至少之一：

第一密码信息；

第一指纹信息；

第一指令信息。

可选的，所述第二凭证包括以下至少之一：

第二密码信息；

第二指纹信息；

第二指令信息。

根据本发明的第三方面，提供了一种交易装置，包括：

所述安全模块，用于验证所输入的第一凭证通过，并反馈第一信号至所述控制器；以及：响应于所述控制器反馈的第二信号，验证所输入的第二凭证通过，并反馈第三信号至所述控制器；

所述控制器，用于接收所述第一信号产生动态口令，并向服务器发送所述动态口令；接收通讯设备生成并发送的交易报文，向所述安全模块发送所述第二信号，并驱动显示所述交易报文的部分或全部信息；接收所述安全模块发送的第三信号；以及：向所述服务器发送交易报文签名，其中，所述交易报文签名为根据用户的确认操作和所述交易报文产生的。

可选的，所述的装置，还包括显示器和输入设备，所述第一凭证和第二凭证为通过所述输入设备输入得到的，所述控制器具体用于驱动所述显示器显示所述交易报文的部分或全部信息。

根据本发明的第四方面，提供了一种交易装置，包括：

第一验证模块，用于验证所输入的第一凭证通过，产生动态口令；

口令发送模块，用于向服务器发送所述动态口令；

报文接收模块，用于接收通讯设备生成并发送的交易报文；

显示模块，用于显示所述交易报文的部分或全部信息；

第二验证模块，用于验证所输入的第二凭证通过，向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认交易成功；其中，所述交易报文签名为根据用户的确认操作和所述交易报文产生的。

根据本发明第五方面，提供了一种服务器，包括：

口令接收模块，用于接收交易装置发送的动态口令；所述动态口令为所述交易装置验证所输入的第一凭证通过后产生的；

口令验证模块，用于验证所述动态口令通过；

签名接收模块，用于接收所述交易装置发送的交易报文签名，所述交易报文签名为所述交易装置验证所输入的第二凭证通过后根据用户的确认操作和交易报文产生的；

签名验证模块，用于验证所述交易报文签名通过，确认交易成功。

根据本发明的第六方面，提供了一种支付数据处理系统，包括：交易装置、通讯设备与服务器；

所述交易装置用于：

验证所输入的第一凭证通过，产生动态口令；

通过所述通讯设备向服务器发送所述动态口令；

接收所述通讯设备发送的交易报文；

显示所述交易报文的部分或全部信息；

验证所输入的第二凭证通过，通过所述通讯设备向所述服务器发送交易报文签名；其中，所述交易报文签名为根据用户的确认操作和所述交易报文产生的；

所述服务器用于：

通过所述通讯设备接收交易装置发送的动态口令；

验证所述动态口令通过；

通过所述通讯设备接收所述交易装置发送的交易报文签名；

验证所述交易报文签名通过，确认交易成功。

本发明提供的支付数据处理方法、系统、交易装置与服务器，通过交易装置验证所输入的第一凭证通过，产生动态口令；以及验证所输入的第二凭证通过，向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认交易成功，简化了电脑端的处理操作，从而增

强了安全性能。

附图说明

为了更清楚地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，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明一交易装置的支付数据处理方法的流程示意图；

图 2 是本发明一服务器的支付数据处理方法的流程示意图；

图 3 是本发明一支付数据处理系统的结构示意图。

附图标记说明：

1-支付装置；

101-控制器；

102-安全模块；

103-通信模块；

104-显示器；

105-输入装置；

2-服务器；

3-通信设备。

具体实施方式

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。

本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、

“第三”“第四”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例例如能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

下面以具体地实施例对本发明的技术方案进行详细说明。下面这几个具体的实施例可以相互结合，对于相同或相似的概念或过程可能在某些实施例不再赘述。

实施例 1

图 1 是本发明一交易装置的支付数据处理方法的流程示意图；请参考图 1，提供了一种交易装置的支付数据处理方法，包括：

S11：验证所输入的第一凭证通过，产生动态口令。

其中，第一凭证，可以理解为任意可实现验证的凭证信息，第一凭证包括以下至少之一：第一密码信息；第一指纹信息；第一指令信息。其中，第一密码信息可以理解为字符组成的密码。第一凭证可以理解为一种登录凭证。根据凭证不同，对应的输入设备可以对应的发生变化。

动态口令（OTP,One-Time Password），可以理解为一次性密码。动态口令可以理解为能够通过服务器中的口令验证服务器验证的口令。

S12：向服务器发送所述动态口令。由于动态口令为验证第一凭证后得到的，第一凭证为登录凭证，所以，发送所述动态口令，可以理解为用于实现登录的目的。

其中一种实施方式中，可以通过通讯设备向服务器发送动态口令。

S13：接收通讯设备生成并发送的交易报文。

其中，交易报文可以理解为与当下交易相关的报文，举例中，可以包括其中至少之一：比如交易金额、交易对象、交易时间等等。

其中一种实施方式中，可以通过通讯设备接收服务器发送的动态口令。

S14：显示所述交易报文的部分或全部信息；

举例中，可以显示交易金额、交易对象、交易时间等等。

S15：验证所输入的第二凭证通过，向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认交易成功；其中，所述交易报文签名为根据用户的确认操作和所述交易报文产生的。

第二凭证，可以理解为任意可实现验证的凭证信息，第二凭证可以包括以下至少之一：第二密码信息；第二指纹信息；第二指令信息。其中，第二密码信息可以理解为字符组成的密码。第二凭证可以理解为一种授权凭证。第一凭证可以与第二凭证相同，也可以不同。根据凭证不同，对应的输入设备可以对应的发生变化。

交易报文签名，可以理解为用于确认操作产生的签名，其中，还可携带有对应的交易报文的信息、用户的信息、交易装置的信息等。

其中一种实施方式中，可以通过通讯设备向服务器发送交易报文签名。

本实施例提供的支付数据处理方法，通过交易装置验证所输入的第一凭证通过，产生动态口令；以及验证所输入的第二凭证通过，向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认交易成功，简化了电脑端的处理操作，从而增强了安全性能。

实施例 2

图 2 是本发明一服务器的支付数据处理方法的流程示意图；请参考图 2，提供了一种服务器的支付数据处理方法，包括：

S21：接收交易装置发送的动态口令；所述动态口令为所述交易装置验证所输入的第一凭证通过后产生的；

S22：验证所述动态口令通过；其也可理解为登录成功。

其中一种实施方式中，可以在支付装置和服务器分别预先设置有动态口令计算逻辑，进而计算出匹配的动态口令，动态口令的验证，可以通过将支付装置通过所述计算逻辑得到的口令与服务器通过所述计算逻辑得到的口令进行比对，若一致，则认为通过。在其他可选实施方式中，也可采用其他动态口令常规的实现方式，而不限于以上举例。

S23：接收所述交易装置发送的交易报文签名，所述交易报文签名为所述交易装置验证所输入的第二凭证通过后根据用户的确认操作和所述交易报文产生的；

S24：验证所述交易报文签名通过，确认交易成功。

本实施例提供的支付数据处理方法，通过交易装置验证所输入的第一凭证通过，产生动态口令；显示所述交易报文的部分或全部信息；以及验证所输入的第二凭证通过，向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认交易成功，简化了电脑端的处理操作，从而增强了安全性能。

此外，本实施例所示的方法，与实施例 1 所示方法相对应，其实现原理、技术效果以及术语的含义类似，此处不再赘述。

实施例 3

图 3 是本发明一支付数据处理系统的结构示意图；请参考图 3，提供了一种支付数据处理系统，包括：交易装置 1、通讯设备 3 与服务器 2；

所述交易装置 1 用于：

验证所输入的第一凭证通过，产生动态口令；

通过所述通讯设备 3 向服务器 2 发送所述动态口令；

接收所述通讯设备 3 生成并发送的交易报文；

显示所述交易报文的部分或全部信息；

验证所输入的第二凭证通过，通过所述通讯设备 3 向所述服务器 2 发送交易报文签名；其中，所述交易报文签名为根据用户的确认操作和所述交易

报文产生的；

所述服务器 2 用于：

通过所述通讯设备 3 接收交易装置发送的动态口令；

验证所述动态口令通过；

通过所述通讯设备 3 接收所述交易装置 1 发送的交易报文签名；

验证所述交易报文签名通过，确认交易成功。

其中，所述交易装置 1，包括：

所述安全模块 102，用于验证所输入的第一凭证通过，并反馈第一信号至所述控制器 101；以及：响应于所述控制器 101 反馈的第二信号，验证所输入的第二凭证通过，并反馈第三信号至所述控制器 101；安全模块 102 可以理解为实现以上功能的电路。

其中，交易装置 1 可以包括输入装置 105，安全模块 102 可以直接通过输入装置 105 接收第一凭证和第二凭证。在图 3 示意的实施方式中，安全模块 102 也可以通过控制器 101 连接输入装置 105，第一凭证与第二凭证经输入装置 105 输入至控制器 101 后，通过控制器 101 发送至安全模块 102。输入装置 105 可以列举为键盘。

所述控制器 101，用于接收所述第一信号产生动态口令，并向服务器 2 发送所述动态口令；具体可以通过通信设备 3 发送；接收所述通讯装置 3 生成并发送的交易报文，向所述安全模块 102 发送所述第二信号，并驱动显示所述交易报文的部分或全部信息；以及：接收所述安全模块 102 发送的第三信号，向所述服务器 2 发送交易报文签名，其中，所述交易报文签名为根据用户的确认操作和所述交易报文产生的。

控制器 101 可以理解为交易装置的调度中心，负责对输入数据进行解释、转发以及显示等操作。控制器 101 可以分别连接显示器 104、输入装置 105、安全模块 102 和通信模块 103。

其中，交易装置 1 还可以包括显示器 104，进而通过所述显示器显示所

述交易报文的部分或全部信息。

通过显示器 104 与输入装置 105，可以为交易装置提供人机交互能力。

交易装置 1 还可包括通信模块 103，通信模块可以负责与外部中断的通信，具体可以负责与通信设备 3 的通信。其中一种实施方式中，通信模块 103 可以包括无线通讯单元，比如蓝牙单元，也可以包括优先通讯单元，比如 USB。

交易装置 1 还可以包括电池，为控制器 101 和/或安全模块 102 的实时时钟（RTC）供电，若交易装置 1 的通信模块 103 采用无线通讯单元，电池也可为通信模块 103 供电。

在具体实施过程中：

所述交易装置 1 与具有网络连接能力的通信设备 3 建立连接，具有网络连接能力的通信设备 3 与服务器 2 建立连接；在所述交易装置 1 上输入登录凭证，即第一凭证，所述交易装置 1 内部验证登录凭证，通过后，产生一次性动态口令，即 OTP；所述交易装置 1 将所述动态口令通过通信设备 3 上传给服务器 2，所述服务器 2 可以包含所述 OTP 验证服务器；所述服务器 2 验证所述动态口令，验证通过后登录所述服务器 2 成功；

所述通信设备 3 将交易报文发送到所述交易装置 1，并给出在交易装置 1 上输入授权凭证，即第二凭证的信息；交易装置 1 显示所述交易报文；进一步地，在所述交易装置 1 上确认交易报文的正确性后，接收用户在所述交易装置 1 上输入的授权凭证；所述交易装置 1 内部验证授权凭证，通过后所述交易装置 1 产生交易报文签名，并返回给所述通信设备 3；所述通信设备 3 将交易报文签名发送至所述服务器 2；所述服务器 2 验证所述交易报文签名，通过后，交易成功。

本实施例提供的支付数据处理系统与交易装置，通过交易装置验证所输入的第一凭证通过，产生动态口令；显示所述交易报文的部分或全部信息；以及验证所输入的第二凭证通过，向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认交易成功，简化了电脑

端的处理操作，从而增强了安全性能。

此外，本实施例所示的系统与交易装置，与实施例 1 和实施例 2 所示方法相对应，其实现原理、技术效果以及术语的含义类似，此处不再赘述。

实施例 4

本实施例提供了一种交易装置，包括：

第一验证模块，用于验证所输入的第一凭证通过，产生动态口令；

口令发送模块，用于向服务器发送所述动态口令；

报文接收模块，用于接收通讯设备发送的交易报文；

显示模块，用于显示所述交易报文的部分或全部信息；

签名发送模块，用于验证所输入的第二凭证通过，向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认交易成功；其中，所述交易报文签名为根据用户的确认操作和所述交易报文产生的。

本实施例提供的交易装置，通过交易装置验证所输入的第一凭证通过，产生动态口令；显示所述交易报文的部分或全部信息；以及验证所输入的第二凭证通过，向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认交易成功，简化了电脑端的处理操作，从而增强了安全性能。

此外，本实施例所示的交易装置，与实施例 1 所示方法相对应，其实现原理、技术效果以及术语的含义类似，此处不再赘述。

实施例 5

本实施例提供了一种服务器，包括：

口令接收模块，用于接收交易装置发送的动态口令；所述动态口令为所述交易装置验证所输入的第一凭证通过后产生的；

口令验证模块，用于验证所述动态口令通过；

签名接收模块，用于接收所述交易装置发送的交易报文签名，所述交易

报文签名为所述交易装置验证所输入的第二凭证通过后根据用户的确认操作产生的；

本实施例提供的服务器，通过验证所输入的第一凭证通过，产生动态口令；验证所输入的第二凭证通过，显示所述交易报文的部分或全部信息；以及向所述服务器发送交易报文签名，以使得，所述服务器能够通过验证所述交易报文签名通过确认交易成功，简化了电脑端的处理操作，从而增强了安全性能。

此外，本实施例所示的交易装置，与实施例 2 所示方法相对应，其实现原理、技术效果以及术语的含义类似，此处不再赘述。

本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

最后应说明的是：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各实施例技术方案的范围。

2017106478453

说　明　书　附　图

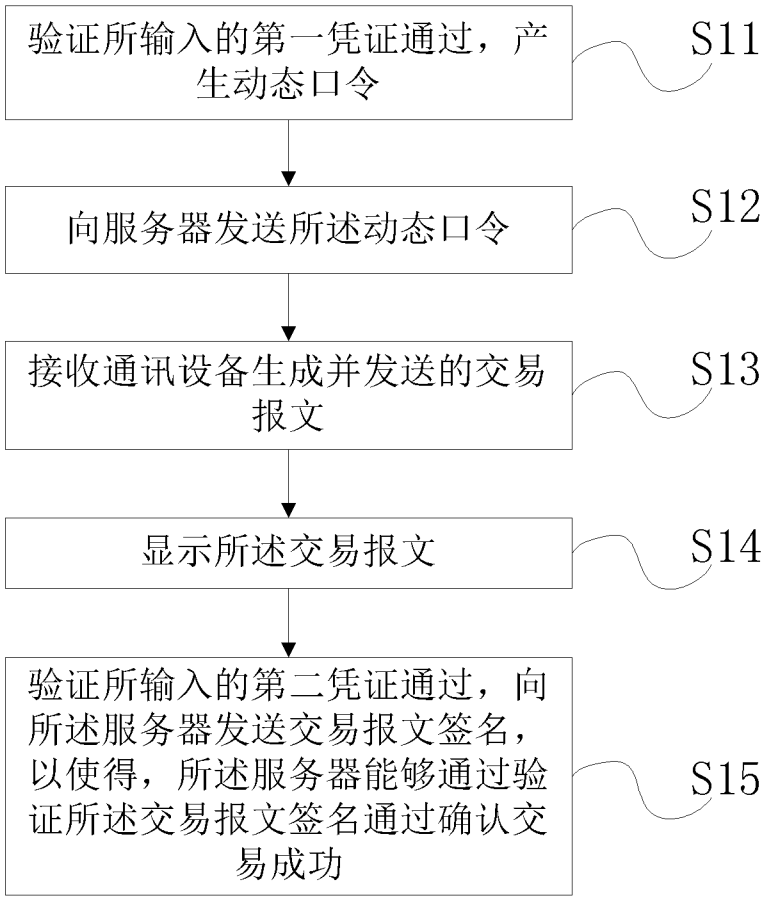

图 1

2017106478453

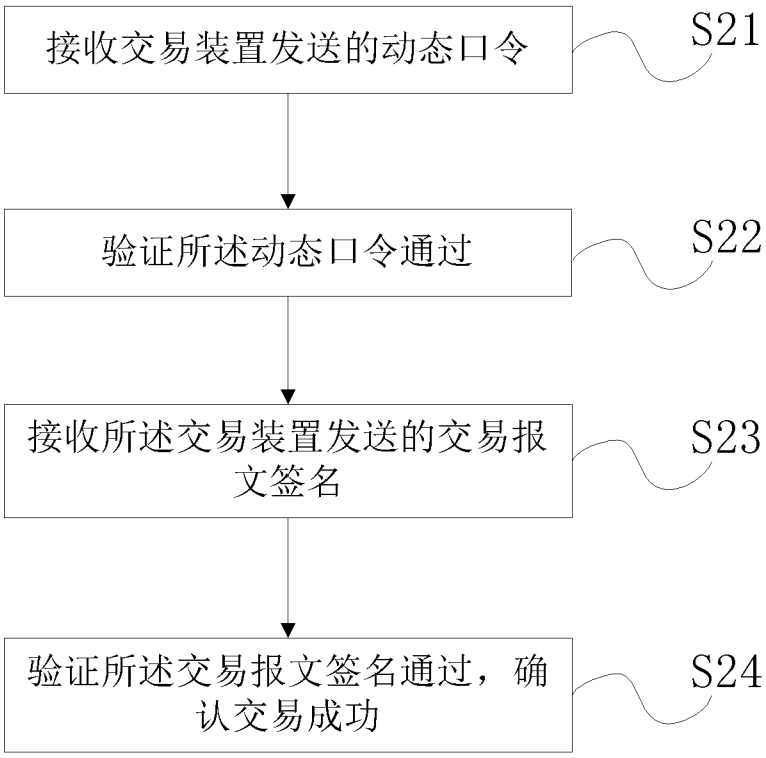

图 2

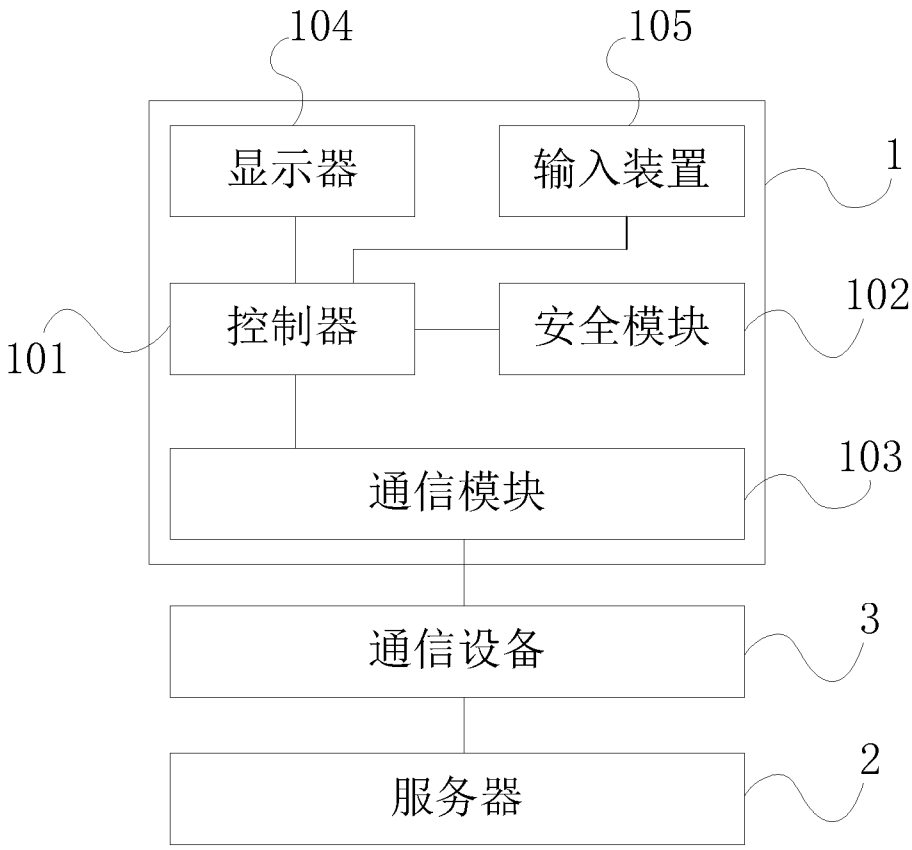

图 3