(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 104079562 B
(45)授权公告日 2017.07.11

(21)申请号 201410253082.0

(22)申请日 2014.06.09

(65)同一申请的已公布的文献号
申请公布号 CN 104079562 A

(43)申请公布日 2014.10.01

(73)专利权人 中国建设银行股份有限公司
地址 100032 北京市西城区金融大街25号

(72)发明人 王雨 杨杰 成亮 罗恕人
郭敏鸿 杨蔚然

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 温旭 郝传鑫

(51)Int.Cl.
H04L 29/06(2006.01)
G06Q 20/32(2012.01)
G06Q 20/40(2012.01)
H04L 9/32(2006.01)

(56)对比文件
CN 101231726 A,2008.07.30,
CN 102360480 A,2012.02.22,
CN 1776732 A,2006.05.24,
JP 2002056330 A,2002.02.20,

审查员 胡智权

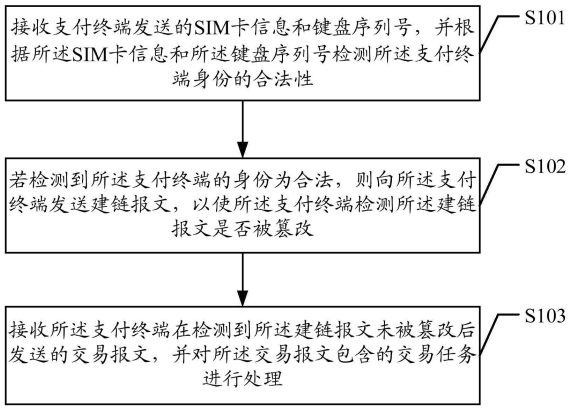
权利要求书3页 说明书12页 附图8页

(54)发明名称

一种基于支付终端的安全认证方法及相关装置

(57)摘要

本发明实施例公开了一种基于支付终端的安全认证方法,包括:接收支付终端发送的SIM卡信息和键盘序列号,并根据所述SIM卡信息和所述键盘序列号检测所述支付终端身份的合法性;若检测到所述支付终端的身份为合法,则向所述支付终端发送建链报文,以使所述支付终端检测所述建链报文是否被篡改;接收所述支付终端在检测到所述建链报文未被篡改后发送的交易报文,并对所述交易报文包含的交易任务进行处理。本发明实施例还公开了一种安全认证装置。采用本发明可通过验证该终端身份的合法性,并在检测到该终端的身份为合法且该终端与服务器之间的通信连接安全可靠时,对该交易任务进行处理,有效地提高了系统的安全性。



CN 104079562 B

1.一种基于支付终端的安全认证方法,其特征在于,包括:

接收支付终端发送的SIM卡信息和键盘序列号,并根据所述SIM卡信息和所述键盘序列号检测所述支付终端身份的合法性;

若检测到所述支付终端的身份为合法,则向所述支付终端发送建链报文,以使所述支付终端检测所述建链报文是否被篡改;

接收所述支付终端在检测到所述建链报文未被篡改后发送的交易报文,并对所述交易报文包含的交易任务进行处理;

其中,所述若检测到所述支付终端的身份为合法,则向所述支付终端发送建链报文,以使所述支付终端检测所述建链报文是否被篡改,包括:

当检测到所述支付终端的身份为合法时,生成同步随机数,并获取通过预设校验算法得到的校验码;

将包含所述同步随机码及校验码的建链报文发送至所述支付终端,以使所述支付终端根据所述同步随机数及校验码检测所述建链报文是否被篡改。

2.如权利要求1所述的方法,其特征在于,所述根据所述SIM卡信息和所述键盘序列号检测所述支付终端身份的合法性,包括:

根据预置的SIM卡信息与键盘序列号之间的映射关系判断所述认证报文中包含的SIM卡信息和所述键盘序列号是否匹配;

若匹配,则确定所述支付终端的身份为合法。

3.如权利要求1所述的方法,其特征在于,所述接收所述支付终端在检测到所述建链报文未被篡改后发送的交易报文,并对所述交易报文包含的交易任务进行处理,包括:

当接收到所述支付终端在检测到所述建链报文未被篡改后发送的交易报文且检测到所述交易报文合法时,生成预设传输形式的交易验证码,所述交易报文包含所述支付终端发起的交易任务,且由工作密钥以及密钥加密密钥进行二级加密处理;

将所述预设传输形式的交易验证码发送给所述支付终端以进行交易认证, 所述预设传输形式的交易验证码包括以语音、短信或数据网络的方式传输的交易验证码;

若接收到所述支付终端返回的交易认证成功消息,则执行所述支付终端发起的交易任务。

4.如权利要求3所述的方法,其特征在于,在所述接收所述支付终端在检测到所述建链报文未被篡改后发送的交易报文,并对所述交易报文包含的交易任务进行处理之前,还包括:

检测所述支付终端发起的交易任务是否为所述支付终端在预设时间范围内的首次交易任务;

若是,则获取由加密机生成的工作密钥,并通过与所述支付终端对应的密钥加密密钥对所述工作密钥进行加密;

将通过密钥加密密钥加密后的工作密钥发送给所述支付终端。

5.一种基于支付终端的安全认证方法,其特征在于,包括:

当支付终端检测到交易任务时,获取当前SIM卡信息及键盘序列号,并将所述SIM卡信息及键盘序列号发送至服务器,以指示所述服务器检测所述支付终端身份的合法性;

若接收到所述服务器在确认所述支付终端的身份为合法后发送的建链报文,则检测所

述建链报文是否被篡改；

若检测到所述建链报文未被篡改，则生成包含所述交易任务的交易报文，并将所述交易报文发送至所述服务器，以使所述服务器对所述交易报文包含的交易任务进行处理；

其中，所述检测所述建链报文是否被篡改，包括：

获取所述建链报文中包含的同步随机数及校验码；

根据所述同步随机数及校验码检测所述服务器发送的建链报文是否被篡改。

6.如权利要求5所述的方法，其特征在于，还包括：

若检测到所述建链报文被篡改，则中断与所述服务器之间的通信连接。

7.如权利要求5所述的方法，其特征在于，所述生成包含所述交易任务的交易报文，并将所述交易报文发送至所述服务器，以使所述服务器对所述交易报文包含的交易任务进行处理，包括：

生成包含所述交易任务的交易报文；

获取工作密钥，通过所述工作密钥对所述交易报文进行加密处理，并将所述交易报文发送至所述服务器，所述工作密钥由密钥加密密钥进行加密；

若接收到所述服务器响应所述交易报文返回的交易验证码，则根据所述交易验证码进行交易认证。

8.一种安全认证装置，其特征在于，包括：

第一检测模块，用于接收支付终端发送的SIM卡信息和键盘序列号，并根据所述SIM卡信息和所述键盘序列号检测所述支付终端身份的合法性；

第一发送模块，用于当所述第一检测模块检测到所述支付终端的身份为合法时，向所述支付终端发送建链报文，以使所述支付终端检测所述建链报文是否被篡改；

交易模块，用于接收所述支付终端在检测到所述建链报文未被篡改后发送的交易报文，并对所述交易报文包含的交易任务进行处理；

其中，所述第一发送模块包括：

信息获取单元，用于当检测到所述支付终端的身份为合法时，生成同步随机数，并获取通过预设校验算法得到的校验码；

报文发送单元，用于将包含所述同步随机码及校验码的建链报文发送至所述支付终端，以使所述支付终端根据所述同步随机数及校验码检测所述建链报文是否被篡改。

9.如权利要求8所述的装置，其特征在于，所述第一检测模块包括：

匹配检测单元，用于接收支付终端发送的SIM卡信息和键盘序列号，并根据预置的SIM卡信息与键盘序列号之间的映射关系判断所述认证报文中包含的SIM卡信息和所述键盘序列号是否匹配；

身份确定单元，用于当所述匹配检测单元检测到所述SIM卡信息与所述键盘序列号相匹配时，确定所述支付终端的身份为合法。

10.如权利要求8所述的装置，其特征在于，所述交易模块包括：

信息生成单元，用于当接收到所述支付终端在检测到所述建链报文未被篡改后发送的交易报文且检测到所述交易报文合法时，生成预设传输形式的交易验证码，所述交易报文包含所述支付终端发起的交易任务，且由工作密钥以及密钥加密密钥进行二级加密处理；

信息发送单元，用于将所述信息生成单元生成的预设传输形式的交易验证码发送给所

述支付终端以进行交易认证，所述预设传输形式的交易验证码包括以语音、短信或数据网络的方式传输的交易验证码；

交易执行单元，用于当接收到所述支付终端返回的交易认证成功消息时，执行所述支付终端发起的交易任务。

11.如权利要求10所述的装置，其特征在于，还包括：

第二检测模块，用于检测所述交易任务是否为所述支付终端在预设时间范围内的首次交易任务；

获取模块，用于当所述第二检测模块检测到所述交易任务为所述支付终端在预设时间范围内的首次交易任务时，获取由加密机生成的工作密钥，并通过与所述支付终端对应的密钥加密密钥对所述工作密钥进行加密；

第二发送模块，用于将通过密钥加密密钥加密后的工作密钥发送给所述支付终端。

12.一种安全认证装置，其特征在于，包括：

信息获取模块，用于当支付终端检测到交易任务时，获取当前SIM卡信息及键盘序列号，并将所述SIM卡信息及键盘序列号发送至服务器，以指示所述服务器检测所述支付终端身份的合法性；

检测模块，用于当接收到所述服务器在确认所述支付终端的身份为合法后发送的建链报文时，检测所述建链报文是否被篡改；

发送模块，用于当所述检测模块检测到所述建链报文未被篡改时，生成包 含所述交易任务的交易报文，并将所述交易报文发送至所述服务器，以使所述服务器对所述交易报文包含的交易任务进行处理；

其中，所述检测模块包括：

获取单元，用于获取所述建链报文中包含的同步随机数及校验码；

信息检测单元，用于根据所述同步随机数及校验码检测所述服务器发送的建链报文是否被篡改。

13.如权利要求12所述的装置，其特征在于，还包括：

中断模块，用于当所述检测模块检测到所述建链报文被篡改时，中断与所述服务器之间的通信连接。

14.如权利要求12所述的装置，其特征在于，所述发送模块包括：

生成单元，用于生成包含所述交易任务的交易报文；

加密单元，用于获取工作密钥，通过所述工作密钥对所述信息生成单元生成的交易报文进行加密处理，并将所述交易报文发送至所述服务器，所述工作密钥由密钥加密密钥进行加密；

认证单元，用于当接收到所述服务器响应所述交易报文返回的交易验证码时，根据所述交易验证码进行交易认证。

一种基于支付终端的安全认证方法及相关装置

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种基于支付终端的安全认证方法及相关装置。

背景技术

[0002] 随着经济的发展和网络技术的逐渐成熟，传统的面对面现金业务已不能支撑人们日益增长的消费需求，由此，基于浏览器或服务器应用方式的电子交易应运而生，有效剥离了银行网点的传统非现金业务，降低了服务成本。

[0003] 随着人们生活节奏的加快，互联网应用、电子商务以及移动支付行业得到蓬勃发展，消费者可在电脑或各种终端设备上通过互联网进行电子交易，与此同时，电子交易的安全性也成为一个尤其要注意的问题。如现有的无线金融转账设备如无线POS机，仅使用了密钥加密的安全认证技术，进行交易时安全性不强。

发明内容

[0004] 本发明实施例所要解决的技术问题在于，提供一种基于支付终端的安全认证方法及相关装置，可有效地提高系统的安全性。

[0005] 为了解决上述技术问题，本发明实施例提供了一种基于支付终端的安全认证方法，包括：

[0006] 接收支付终端发送的SIM卡信息和键盘序列号，并根据所述SIM卡信息和所述键盘序列号检测所述支付终端身份的合法性；

[0007] 若检测到所述支付终端的身份为合法，则向所述支付终端发送建链报文，以使所述支付终端检测所述建链报文是否被篡改；

[0008] 接收所述支付终端在检测到所述建链报文未被篡改后发送的交易报文，并对所述交易报文包含的交易任务进行处理。

[0009] 相应地，本发明实施例还提供了另一种基于支付终端的安全认证方法，包括：

[0010] 当支付终端检测到交易任务时，获取当前SIM卡信息及键盘序列号，并将所述SIM卡信息及键盘序列号发送至服务器，以指示所述服务器检测所述支付终端身份的合法性；

[0011] 若接收到所述服务器在确认所述支付终端的身份为合法后发送的建链报文，则检测所述建链报文是否被篡改；

[0012] 若检测到所述建链报文未被篡改，则生成包含所述交易任务的交易报文，并将所述交易报文发送至所述服务器，以使所述服务器对所述交易报文包含的交易任务进行处理。

[0013] 相应地，本发明实施例还提供了一种安全认证装置，包括：

[0014] 第一检测模块，用于接收支付终端发送的SIM卡信息和键盘序列号，并根据所述SIM卡信息和所述键盘序列号检测所述支付终端身份的合法性；

[0015] 第一发送模块，用于当所述第一检测模块检测到所述支付终端的身份为合法时，

向所述支付终端发送建链报文，以使所述支付终端检测所述建链报文是否被篡改；

[0016] 交易模块，用于接收所述支付终端在检测到所述建链报文未被篡改后发送的交易报文，并对所述交易报文包含的交易任务进行处理。

[0017] 相应地，本发明实施例还提供了一种安全认证装置，包括：

[0018] 信息获取模块，用于当支付终端检测到交易任务时，获取当前SIM卡信息及键盘序列号，并将所述SIM卡信息及键盘序列号发送至服务器，以指示所述服务器检测所述支付终端身份的合法性；

[0019] 检测模块，用于当接收到所述服务器在确认所述支付终端的身份为合法后发送的建链报文时，检测所述建链报文是否被篡改；

[0020] 发送模块，用于当所述检测模块检测到所述建链报文未被篡改时，生成包含所述交易任务的交易报文，并将所述交易报文发送至所述服务器，以使所述服务器对所述交易报文包含的交易任务进行处理。

[0021] 实施本发明实施例，具有如下有益效果：

[0022] 本发明实施例可在执行支付终端发起的交易任务之前，通过验证该终端身份的合法性，并在检测到该终端的身份为合法且该终端与服务器之间的通信连接安全可靠时，对该交易任务进行处理，从而有效地提高了系统的安全性。

附图说明

[0023] 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的前提下，还可以根据这些附图获得其他的附图。

[0024] 图1是本发明实施例的一种基于支付终端的安全认证方法的流程示意图；

[0025] 图2是本发明实施例的另一种基于支付终端的安全认证方法的流程示意图；

[0026] 图3是本发明实施例的一种获取工作密钥的方法的流程示意图；

[0027] 图4是本发明实施例的又一种基于支付终端的安全认证方法的流程示意图；

[0028] 图5是本发明实施例的再一种基于支付终端的安全认证方法的流程示意图；

[0029] 图6是本发明实施例的一种安全认证装置的结构示意图；

[0030] 图7是本发明实施例的另一种安全认证装置的结构示意图；

[0031] 图8是图7的第一检测模块的其中一种结构组成示意图；

[0032] 图9是图7的第一发送模块的其中一种结构组成示意图；

[0033] 图10是图7的交易模块的其中一种结构组成示意图；

[0034] 图11是本发明实施例的又一种安全认证装置的结构示意图；

[0035] 图12是图11的检测模块的其中一种结构组成示意图；

[0036] 图13是图11的发送模块的其中一种结构组成示意图。

具体实施方式

[0037] 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作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。

[0038] 请参见图1，是本发明实施例的一种基于支付终端的安全认证方法的流程示意图，本发明实施例的所述方法可具体应用于服务器中，具体的，所述方法包括：

[0039] S101：接收支付终端发送的SIM卡信息和键盘序列号，并根据所述SIM卡信息和所述键盘序列号检测所述支付终端身份的合法性。

[0040] 所述服务器可以为银行中用于控制金融交易并进行业务处理的服务器，所述支付终端可包括手机、平板电脑、可穿戴设备等设置有SIM(Subscriber Identity Module，用户识别模块)卡的终端设备。在本发明实施例中，所述键盘可具体为密码键盘，该密码键盘设置于该支付终端上，并对应特定的键盘序列号。

[0041] 其中，所述SIM卡信息可包括电话号码、该SIM卡的IMSI(International Mobile Subscriber Identity，国际移动用户识别)码、ICCID(Integrate Circuit Card Identity，集成电路卡识别)码等等。

[0042] 具体实施例中，服务器可在接收到支付终端发送的SIM卡信息及键盘序列号之后，根据该服务器中预置的SIM卡信息及键盘序列号的映射关系判断该接收到的SIM卡信息及键盘序列号是否相匹配，若是，则可判断为身份认证成功，即该支付终端的身份为合法；否则为对该终端的身份认证失败，即终端身份不合法。

[0043] S102：若检测到所述支付终端的身份为合法，则向所述支付终端发送建链报文，以使所述支付终端检测所述建链报文是否被篡改。

[0044] 具体的，本发明实施例可利用同步随机数及校验码技术来保证支付终端与服务器之间的通讯是可信的，不可被篡改的。服务器与该支付终端建立通信连接，且所述支付终端的身份为合法时，可由服务器发送建链报文至该终端，该建链报文中插入由服务器生成的同步随机数以及通过预设的校验算法生成的校验码，以使该终端检验该建链报文是否被篡改。

[0045] S103：接收所述支付终端在检测到所述建链报文未被篡改后发送的交易报文，并对所述交易报文包含的交易任务进行处理。

[0046] 若该支付终端检测到建链报文未被篡改，即终端与服务器之间的通信可信，则可向服务器发送包含当前交易任务的交易报文。该服务器可基于二级密钥以及预设的交易验证码对该交易报文进行认证，并在认证成功时，执行该终端当前发起的交易任务。该预设的交易验证码包括以语音、短信或数据网络的方式传输的交易验证码。

[0047] 实施本发明实施例可在执行支付终端发起的交易任务之前，通过验证该终端身份的合法性，并在检测到该终端的身份为合法且该终端与服务器之间的通信连接安全可靠时，对该交易任务进行处理，从而有效地提高了系统的安全性。

[0048] 请参见图2，是本发明实施例的另一种基于支付终端的安全认证方法的流程示意图，本发明实施例的所述方法可具体应用于服务器中，具体的，所述方法包括：

[0049] S201：接收支付终端发送的SIM卡信息和键盘序列号。

[0050] 其中，该支付终端可包括手机、平板电脑、可穿戴设备等设置有SIM卡的终端设备。在本发明实施例中，所述键盘可具体为密码键盘，该密码键盘设置于该支付终端上，并对应特定的键盘序列号。

[0051] 具体的，该密码键盘内部包含具有加密运算处理功能的专用器件，能够完成报文加密、解密、报文认证计算和验证等操作。该密码键盘与支付终端之间的信息传送以密文的形式进行。

[0052] S202：根据预置的SIM卡信息与键盘序列号之间的映射关系判断所述认证报文中包含的SIM卡信息和所述键盘序列号是否匹配。

[0053] S203：若匹配，则确定所述支付终端的身份为合法。

[0054] 具体的，该服务器可在接收到支付终端发送的SIM卡信息及键盘序列号之后，根据该服务器中预置的映射关系判断该SIM卡信息及键盘序列号是否相匹配来判断该终端的身份是否合法。若是，则可判断为身份认证成功，即该终端的身份为合法；否则为对该终端的身份认证失败，即该终端身份不合法。其中，该支付终端的SIM卡信息唯一，该预置的映射关系包括服务器中存储的各支付终端的SIM卡信息及其对应密码键盘序列号的绑定关系。

[0055] 进一步的，该SIM卡信息可包括与该SIM卡对应的电话号码、IMSI(International Mobile Subscriber Identity，国际移动用户识别)码、ICCID(Integrate Circuit Card Identity，集成电路卡识别)码等等，判断所述认证报文中包含的SIM卡信息和所述键盘序列号是否匹配，可具体为判断是否存在任一项上述的SIM卡信息与所述键盘序列号相匹配，若是，则可判断该终端的身份为合法。

[0056] 进一步的，在服务器完成对该终端身份的认证之后，还可在终端显示屏上显示认证结果，提示终端身份认证为成功或失败。

[0057] S204：生成同步随机数，并获取通过预设校验算法得到的校验码。

[0058] S205：将包含所述同步随机码及校验码的建链报文发送至所述支付终端，以使所述支付终端根据所述同步随机数及校验码检测所述建链报文是否被篡改。

[0059] 具体的，本发明实施例可利用同步随机数及校验码技术来验证支付终端与服务器之间的通讯是否可信、数据是否被篡改。服务器与该支付终端建立通信连接，且所述支付终端的身份为合法时，可由服务器发送建链报文至该终端，该建链报文中插入由服务器生成的同步随机数以及通过预设的校验算法生成的校验码，以进行通信安全验证，即检测终端与服务器之间的通信是否可信。进一步的，可在检测到该同步随机数或校验码满足预设的验证规则比如对该同步随机数或校验码进行预设方式的运算之后，与终端记录的某一校验值相匹配时，确认终端接收到的报文未被篡改。对于该预设的验证规则，本发明实施例不作限定。

[0060] S206：当接收到所述支付终端在检测到所述建链报文未被篡改后发送的交易报文且检测到所述交易报文合法时，生成预设传输形式的交易验证码。

[0061] 所述交易报文包含所述支付终端发起的交易任务，且由工作密钥以及密钥加密密钥进行二级加密处理。

[0062] 若该支付终端检测到建链报文未被篡改，即终端与服务器之间的通信可信，则可向服务器发送包含当前交易任务的交易报文。该服务器在接收到终端发送的交易报文时，触发发起对终端发起的交易任务的交易认证。

[0063] 进一步的，可通过本次链路的通讯报文同步序号，来检测该交易报文是否合法，具体检测方法如下：

[0064] 1)服务器生成建链报文，并携带同步序列号，如0X00，终端记录该同步序列号的值

0X00，并在响应该建链报文返回服务器的建链应答中携带该同步序列号原值即0X00，服务器也记录该同步序列号的值0X00；

[0065] 2)当该终端向服务器发送交易报文时，将所记录的值加一后发送，并记录该加一后的值，即0X01。

[0066] 3)服务器收到该交易报文后，可检查其合法性。具体的，检查规则可设置为当服务器检测到记录的值比收到的值小一时，表示该交易报文是合法的，记录并更新该收到的值0X01；否则，表示为该交易报文非法，可直接丢弃该数据包，并作错误处理。

[0067] 4)服务器在收到终端发送的交易报文之后，可返回接收完成报文至终端时，并在该接收完成报文中携带记录的值0X01。

[0068] S207：将所述预设传输形式的交易验证码发送给所述支付终端以进行交易认证。

[0069] 其中，该预设传输形式的交易验证码包括以语音、短信或数据网络的方式传输的交易验证码。

[0070] S208：若接收到所述支付终端返回的交易认证成功消息，则执行所述支付终端发起的交易任务。

[0071] 若终端对服务器返回的交易验证码验证成功，则可执行该终端当前发起的交易任务，对该交易任务进行处理。

[0072] 进一步的，终端可显示交易认证的结果，如在交易认证失败时，可在终端上对应提示“交易认证失败”。

[0073] 实施本发明实施例可在执行支付终端发起的交易任务之前，通过该终端的SIM卡信息及键盘序列号来验证所述支付终端身份的合法性，并在检测到该支付终端的身份为合法且该终端与服务器之间的通信连接安全可靠时，返回预设的交易验证码至该终端以进行交易认证，并在认证成功时岁该交易任务进行处理，从而有效地提高了系统的安全性。

[0074] 进一步的，请参见图3，是是本发明实施例的一种获取工作密钥的方法的流程示意图，具体的，所述方法包括：

[0075] S301：检测所述支付终端发起的交易任务是否为所述支付终端在预设时间范围内的首次交易任务。

[0076] 具体的，可在服务器对当前支付终端进行身份认证并在检测到该终端的身份为合法之后，进一步检测该终端发起的交易任务是否为预设时间范围内如当天的首次交易任务。

[0077] S302：若是，则获取由加密机生成的工作密钥，并通过与所述支付终端对应的密钥加密密钥对所述工作密钥进行加密。

[0078] 若检测到终端当前发起的交易任务为当天的首次交易任务，服务器可发起签到流程以获取工作密钥，该工作密钥可由金融加密机生成。具体的，该服务器可通过与加密机进行基于以太网的通信来获取该工作密钥。

[0079] 进一步的，该工作密钥还可由密钥加密密钥进行二级加密，该密钥加密密钥由该支付终端和服务器唯一确定。

[0080] S303：将通过密钥加密密钥加密后的工作密钥发送给所述支付终端。

[0081] 实施本发明实施例可在检测到当前终端发起的交易任务为预设时间范围内的首次交易任务时，触发获取工作密钥，并通过密钥加密密钥对该工作密钥进行二级加密后发

送给该终端，以使终端通过该工作密钥对报文进行加密，提升了终端与服务器之间信息传输的可靠性。

[0082] 请参见图4，是本发明实施例的又一种基于支付终端的安全认证方法的流程示意图，本发明实施例的所述方法可具体应用于手机、平板电脑、可穿戴设备等带有SIM卡的终端设备中，具体的，所述方法包括：

[0083] S401：当支付终端检测到交易任务时，获取当前SIM卡信息及键盘序列号，并将所述SIM卡信息及键盘序列号发送至服务器，以指示所述服务器检测所述支付终端身份的合法性。

[0084] 在本发明实施例中，所述键盘可具体为密码键盘，该密码键盘可设置于该支付终端上，并对应特定的键盘序列号，且该支付终端的SIM卡信息唯一。

[0085] 进一步的，该支付终端中还可设置磁条读卡器、热敏打印机等，在进行交易时，可通过该磁条读卡器直接读取交易IC卡相关信息如账户名、卡号等。

[0086] 具体的，密码键盘内部包含具有加密运算处理功能的专用器件，能够完成报文加密、解密、报文认证计算和验证等处理操作。该密码键盘与支付终端之间的信息传送以密文的形式进行。

[0087] S402：若接收到所述服务器在确认所述支付终端的身份为合法后发送的建链报文，则检测所述建链报文是否被篡改。

[0088] 具体的，该支付终端可根据该建链报文中包含的同步随机数及校验码来检测该建链报文是否被篡改，并可在检测到该建链报文未被篡改时，向服务器返回相应的建链应答。进一步的，还可在该建链应答中插入对应的同步随机数及校验码以保证返回的建链应答的安全性。

[0089] S403：若检测到所述建链报文未被篡改，则生成包含所述交易任务的交易报文，并将所述交易报文发送至所述服务器，以使所述服务器对所述交易报文包含的交易任务进行处理。

[0090] 该交易报文由工作密钥以及密钥加密密钥进行二级加密处理。

[0091] 实施本发明实施例可在支付终端检测到交易任务时，通过获取并发送当前SIM卡信息及键盘序列号至服务器，以使该服务器验证所述支付终端身份的合法性，并在检测到该终端身份为合法且该终端与服务器之间的通信连接安全可靠时，发送包含该交易任务的交易报文至服务器以进行处理，有效地提高了系统的安全性。

[0092] 请参见图5，是本发明实施例的再一种基于支付终端的安全认证方法的流程示意图，本发明实施例的所述方法可具体应用于手机、平板电脑、可穿戴设备等带有SIM卡的终端设备中，具体的，所述方法包括：

[0093] S501：当支付终端检测到交易任务时，获取当前SIM卡信息及键盘序列号，并将所述SIM卡信息及键盘序列号发送至服务器，以指示所述服务器检测所述支付终端身份的合法性。

[0094] S502：若接收到所述服务器在确认所述支付终端的身份为合法后发送的建链报文，获取所述建链报文中包含的同步随机数及校验码。

[0095] 具体的，本发明实施例可利用同步随机数及校验码技术来保证支付终端与服务器之间的通信是可信的，不可被篡改的。

[0096] S503:根据所述同步随机数及校验码检测所述服务器发送的建链报文是否被篡改。

[0097] 具体实施例中,服务器在检测到该支付终端的身份为合法之后,可发送建链报文至该终端,该建链报文中插入由服务器生成的同步随机数以及通过预设的校验算法生成的校验码,以进行通信安全验证,即检测终端与服务器之间的通信是否可信。

[0098] 进一步的,终端在接收到服务器发送的建链报文之后,还可对该同步随机数进行预设方式的运算,比如通过网关认证密钥对该同步随机数进行按位异或运算,并将运算结果返回服务器。进一步的,服务器可记录该运算结果,并在终端与服务器之间的来往报文中均插入该同步随机数,在本次链路中断前,可通过对比对接收到的报文所携带的同步随机数进行预设方式的运算所得到的数据是否与该记录的运算结果相一致,来检测终端与服务器之间的通信报文是否被篡改,并在不一致时,中断本次连接。对于本发明实施例终端或服务器端根据同步随机数及校验码进行报文检测的方法,本发明不作限定。

[0099] 进一步的,若检测到终端与服务器之间的通信不可信,安全验证失败时,可分为两种情况,服务器发送报文到终端的报文验证失败,则终端可直接显示通讯失败;或者终端发送报文到服务器,服务器验证报文失败,则可返回一个含有报文验证失败信息的报文到终端,此时终端收到报文后可显示通讯失败。

[0100] S504:若检测到所述建链报文未被篡改,生成包含所述交易任务的交易报文。

[0101] 进一步的,若检测到所述建链报文被篡改,则可中断该终端与所述服务器之间的通信连接。

[0102] S505:获取工作密钥,通过所述工作密钥对所述交易报文进行加密处理,并将所述交易报文发送至所述服务器。

[0103] 所述工作密钥(Working Key,WK)可以是该支付终端在预设时间范围内首次发起交易任务时,由服务器下发得到。其中,该工作密钥由密钥加密密钥(Key Encryption Key,KEK)进行二级加密,该KEK由该支付终端和服务器唯一确定,用于对WK进行加密保护。工作密钥包括用于对个人标识码(Personal Identification Number,PIN)加密的PIK(Personal Identification Number Key,个人标识码密钥)、对报文鉴别码(Message Authentication Code,MAC)加密的MAK(Message Authentication Code Key,报文鉴别码密钥)以及对磁道信息加密的TDK(Track Data Key,磁道信息加密密钥)。该WK由服务器端的加密机产生,在该支付终端每次签到时从服务器利用KEK加密后下载,并由KEK加密存储。

[0104] S506:若接收到所述服务器响应所述交易报文返回的交易验证码,则根据所述交易验证码进行交易认证。

[0105] 该交易验证码包括以语音、短信或数据网络的方式得到的交易验证码。

[0106] 实施本发明实施例可在支付终端检测到交易任务时,将当前SIM卡信息及键盘序列号发送至服务器以检测该终端身份的合法性,并在检测到该终端身份为合法且该终端与服务器之间的通信连接安全可靠时,发送包含该交易任务的交易报文至服务器以进行处理。进一步的,还可在检测该终端与服务器之间的通信连接不可靠时,及时地中断终端与服务器之间的连接,有效地提高了系统的安全性。

[0107] 请参见图6,是本发明实施例的一种安全认证装置的结构示意图,本发明实施例的所述装置可具体设置于服务器中,具体的,所述装置包括第一检测模块11、第一发送模块12

以及交易模块13。其中，

[0108] 所述第一检测模块11，用于接收支付终端发送的SIM卡信息和键盘序列号，并根据所述SIM卡信息和所述键盘序列号检测所述支付终端身份的合法性。

[0109] 所述支付终端可包括手机、平板电脑、可穿戴设备等设置有SIM(Subscriber Identity Module，用户识别模块)卡的终端设备。在本发明实施例中，所述键盘可具体为密码键盘，该密码键盘设置于该支付终端上，并对应特定的键盘序列号。

[0110] 其中，所述SIM卡信息可包括电话号码、该SIM卡的IMSI(International Mobile Subscriber Identity，国际移动用户识别)码、ICCID(Integrate Circuit Card Identity，集成电路卡识别)码等等。

[0111] 具体实施例中，第一检测模块11可在接收到支付终端发送的SIM卡信息及键盘序列号之后，根据该服务器中预置的SIM卡信息和键盘序列号的映射关系判断该接收到的SIM卡信息及键盘序列号是否相匹配，若是，则可判断为该支付终端的身份为合法；否则，该终端身份不合法。

[0112] 所述第一发送模块12，用于当所述第一检测模块11检测到所述支付终端的身份为合法时，向所述支付终端发送建链报文，以使所述支付终端检测所述建链报文是否被篡改。

[0113] 具体的，本发明实施例可利用同步随机数及校验码技术来保证支付终端与服务器之间的通讯是可信的，不可被篡改的。服务器与该支付终端建立通信连接，且所述第一检测模块11检测到该支付终端的身份为合法时，可由第一发送模块12发送建链报文至该终端，该建链报文中插入由服务器生成的同步随机数以及通过预设的校验算法生成的校验码，以使该终端检验该建链报文是否被篡改。

[0114] 所述交易模块13，用于接收所述支付终端在检测到所述建链报文未被篡改后发送的交易报文，并对所述交易报文包含的交易任务进行处理。

[0115] 若该交易模块13接收到该终端发送的包含当前交易任务的交易报文，则可基于二级密钥以及预设的交易验证码对该交易报文进行认证，并在认证成功时，执行该终端当前发起的交易任务。该预设的交易验证码包括以语音、短信或数据网络的方式传输的交易验证码。

[0116] 实施本发明实施例可在执行支付终端发起的交易任务之前，通过验证该终端身份的合法性，并在检测到该终端的身份为合法且该终端与服务器之间的通信连接安全可靠时，对该交易任务进行处理，从而有效地提高了系统的安全性。

[0117] 请参见图7，是本发明实施例的另一种安全认证装置的结构示意图，具体的，所述装置包括上述安全认证装置的第一检测模块11、第一发送模块12以及交易模块13，进一步的，在本发明实施例中，如图8所示，所述装置的第一检测模块11可以具体包括：

[0118] 匹配检测单元111，用于接收支付终端发送的SIM卡信息和键盘序列号，并根据预置的SIM卡信息与键盘序列号之间的映射关系判断所述认证报文中包含的SIM卡信息和所述键盘序列号是否匹配。

[0119] 具体实施例中，所述键盘可具体为密码键盘，该密码键盘设置于该支付终端上，并对应特定的键盘序列号。

[0120] 具体的，该密码键盘内部包含具有加密运算处理功能的专用器件，能够完成报文加密、解密、报文认证计算和验证等操作。该密码键盘与支付终端之间的信息传送以密文的

形式进行。

[0121] 身份确定单元112，用于当所述匹配检测单元111检测到所述SIM卡信息与所述键盘序列号相匹配时，确定所述支付终端的身份为合法。

[0122] 具体的，该服务器可在接收到支付终端发送的SIM卡信息及键盘序列号之后，根据该服务器中预置的映射关系判断该SIM卡信息及键盘序列号是否相匹配来判断该终端的身份是否合法。若是，则可判断为身份认证成功，即该终端的身份为合法；否则为对该终端的身份认证失败，即该终端身份不合法。其中，该支付终端的SIM卡信息唯一，该预置的映射关系包括服务器中存储的各支付终端的SIM卡信息及其对应密码键盘序列号的绑定关系。

[0123] 进一步的，在第一检测模块11完成对该终端身份的认证之后，还可在终端显示屏上显示认证结果，提示终端身份认证为成功或失败。

[0124] 进一步的，请参见图9，所述第一发送模块12可以具体包括：

[0125] 信息获取单元121，用于当检测到所述支付终端的身份为合法时，生成同步随机数，并获取通过预设校验算法得到的校验码。

[0126] 报文发送单元122，用于将包含所述同步随机码及校验码的建链报文发送至所述支付终端，以使所述支付终端根据所述同步随机数及校验码检测所述建链报文是否被篡改。

[0127] 具体的，本发明实施例可利用同步随机数及校验码技术来验证支付终端与服务器之间的通讯是否可信的、数据是否被篡改。当第一检测模块11在检测到所述支付终端的身份为合法时，信息获取单元121可生成的同步随机数以及通过预设的校验算法生成校验码，报文发送单元122发送建链报文至该终端，以进行通信安全验证，即检测终端与服务器之间的通信是否可信，该建链报文中插入了信息获取单元121生成的该同步随机数及校验码。终端在接收到服务器发送的建链报文之后，可根据所述同步随机数及校验码检测所述建链报文是否被篡改。

[0128] 进一步的，请参见图10，所述交易模块13可以具体包括：

[0129] 信息生成单元131，用于当接收到所述支付终端在检测到所述建链报文未被篡改后发送的交易报文且检测到所述交易报文合法时，生成预设传输形式的交易验证码。

[0130] 所述交易报文包含所述支付终端发起的交易任务，且由工作密钥以及密钥加密密钥进行二级加密处理。

[0131] 若该支付终端检测到建链报文未被篡改，即终端与服务器之间的通信可信，信息生成单元131在接收到终端发送的包含当前交易任务的交易报文时，触发发起对终端发起的交易任务的交易认证，生成预设传输形式的交易验证码。

[0132] 信息发送单元132，用于将所述信息生成单元131生成的预设传输形式的交易验证码发送给所述支付终端以进行交易认证。

[0133] 其中，该预设传输形式的交易验证码包括以语音、短信或数据网络的方式传输的交易验证码。

[0134] 交易执行单元133，用于当接收到所述支付终端返回的交易认证成功消息时，执行所述支付终端发起的交易任务。

[0135] 进一步的，终端可显示交易认证的结果，如在交易认证失败时，可在终端上对应提示“交易认证失败”。

[0136] 进一步可选地，在本发明实施例中，所述装置还可以包括：

[0137] 第二检测模块14，用于检测所述交易任务是否为所述支付终端在预设时间范围内的首次交易任务。

[0138] 具体的，可在第一检测模块11对当前支付终端进行身份认证并在检测到该终端的身份为合法之后，进一步通过第二检测模块14检测该终端发起的交易任务是否为预设时间范围内如当天的首次交易任务。

[0139] 获取模块15，用于当所述第二检测模块14检测到所述交易任务为所述支付终端在预设时间范围内的首次交易任务时，获取由加密机生成的工作密钥，并通过与所述支付终端对应的密钥加密密钥对所述工作密钥进行加密。

[0140] 若第二检测模块14检测到终端当前发起的交易任务为当天的首次交易任务，服务器可发起签到流程以获取工作密钥，该工作密钥可由金融加密机生成。具体的，该第二检测模块14可通过与加密机进行基于以太网的通信来获取该工作密钥。

[0141] 进一步的，该工作密钥还可由密钥加密密钥进行二级加密，该密钥加密密钥由该支付终端和服务器唯一确定。

[0142] 第二发送模块16，用于将通过密钥加密密钥加密后的工作密钥发送给所述支付终端。

[0143] 实施本发明实施例可在执行支付终端发起的交易任务之前，通过该终端的SIM卡信息及键盘序列号来验证所述支付终端身份的合法性，并在检测到该支付终端的身份为合法且该终端与服务器之间的通信连接安全可靠时，返回预设的交易验证码至该终端以进行交易认证。进一步的，可在检测到终端当前发起的交易任务为预设时间范围内的首次交易任务，触发获取工作密钥并发送给该终端，并在认证成功时岁该交易任务进行处理，从而有效地提高了系统的安全性。

[0144] 请参见图11，是本发明实施例的另一种安全认证装置的结构示意图，本发明实施例的所述装置具体设置于手机等携带有SIM卡的终端设备中，具体的，所述装置包括：

[0145] 信息获取模块21，用于当支付终端检测到交易任务时，获取当前SIM卡信息及键盘序列号，并将所述SIM卡信息及键盘序列号发送至服务器，以指示所述服务器检测所述支付终端身份的合法性

[0146] 在本发明实施例中，所述键盘可具体为密码键盘，该密码键盘可设置于该支付终端上，对应特定的键盘序列号，且该支付终端的SIM卡信息唯一。

[0147] 具体的，密码键盘内部包含具有加密运算处理功能的专用器件，能够完成报文加密、解密、报文认证计算和验证等处理操作。该密码键盘与支付终端之间的信息传送以密文的形式进行。

[0148] 检测模块22，用于当接收到所述服务器在确认所述支付终端的身份为合法后发送的建链报文时，检测所述建链报文是否被篡改。

[0149] 具体的，该检测模块22可根据该建链报文中包含的同步随机数及校验码来检测该建链报文是否被篡改，并可在检测到该建链报文未被篡改时，向服务器返回相应的建链应答。进一步的，还可在该建链应答中插入对应的同步随机数及校验码以保证返回的建链应答的安全性。

[0150] 发送模块23，用于当所述检测模块22检测到所述建链报文未被篡改时，生成包含

所述交易任务的交易报文，并将所述交易报文发送至所述服务器，以使所述服务器对所述交易报文包含的交易任务进行处理。

[0151] 该交易报文由工作密钥以及密钥加密密钥进行二级加密处理。

[0152] 实施本发明实施例可在支付终端检测到交易任务时，通过获取并发送当前SIM卡信息及键盘序列号至服务器，以使该服务器验证所述支付终端身份的合法性，并在检测到该终端身份为合法且该终端与服务器之间的通信连接安全可靠时，发送包含该交易任务的交易报文至服务器以进行处理，有效地提高了系统的安全性。

[0153] 可选地，请参见图12，所述检测模块22可以进一步包括：

[0154] 获取单元221，用于获取所述建链报文中包含的同步随机数及校验码。

[0155] 具体的，本发明实施例可利用同步随机数及校验码技术来保证支付终端与服务器之间的通信是可信的，不可被篡改的。

[0156] 信息检测单元222，用于根据所述同步随机数及校验码检测所述服务器发送的建链报文是否被篡改。

[0157] 具体实施例中，服务器在检测到该支付终端的身份为合法之后，可发送建链报文至该终端，以进行通信安全验证，即检测终端与服务器之间的通信是否可信，该建链报文中插入由服务器生成的同步随机数以及通过预设的校验算法生成的校验码。

[0158] 具体的，获取单元221在接收到服务器发送的建链报文之后，可对该同步随机数进行预设方式的运算，比如通过网关认证密钥对该同步随机数进行按位异或运算，并将运算结果返回服务器。进一步的，服务器还可记录该运算结果，并在终端与服务器之间的来往报文中均插入该同步随机数，在本次链路中断前，服务器可通过对比对接收到的报文所携带的同步随机数进行预设方式的运算所得到的数据是否与该记录的运算结果相一致，来检测信息是否被篡改，并在不一致时，中断本次连接。

[0159] 进一步的，在本发明实施例中，所述装置还可以包括：

[0160] 中断模块24，用于当所述检测模块22检测到所述建链报文被篡改时，中断与所述服务器之间的通信连接。

[0161] 进一步的可选地，若检测模块22检测到所述建链报文被篡改，则可通过中断模块24中断该终端与所述服务器之间的通信连接。

[0162] 可选地，请参见图13，所述发送模块23可以进一步包括：

[0163] 生成单元231，用于生成包含所述交易任务的交易报文。

[0164] 加密单元232，用于获取工作密钥，通过所述工作密钥对所述信息生成单元231生成的交易报文进行加密处理，并将所述交易报文发送至所述服务器，所述工作密钥由密钥加密密钥进行加密。

[0165] 所述工作密钥(Working Key，WK)可以是该支付终端在预设时间范围内首次发起交易任务时，由服务器下发得到。其中，该工作密钥由密钥加密密钥(Key Encryption Key，KEK)进行二级加密，该KEK由该支付终端和服务器唯一确定，用于对WK进行加密保护。工作密钥包括用于对个人标识码(Personal Identification Number，PIN)加密的PIK(Personal Identification Number Key，个人标识码密钥)、对报文鉴别码(Message Authentication Code，MAC)加密的MAK(Message Authentication Code Key，报文鉴别码密钥)以及对磁道信息加密的TDK(Track Data Key，磁道信息加密密钥)。该WK由服务器端

的加密机产生，在该支付终端每次签到时从服务器利用KEK加密后下载，并由KEK加密存储。

[0166] 认证单元233，用于当接收到所述服务器响应所述交易报文返回的交易验证码时，根据所述交易验证码进行交易认证。

[0167] 该交易验证码包括以语音、短信或数据网络的方式得到的交易验证码。

[0168] 实施本发明实施例可在支付终端检测到交易任务时，将当前SIM卡信息及键盘序列号发送至服务器以检测该终端身份的合法性，并在检测到该终端身份为合法且该终端与服务器之间的通信连接安全可靠时，发送包含该交易任务的交易报文至服务器以进行处理。进一步的，还可在检测该终端与服务器之间的通信连接不可靠时，及时地中断终端与服务器之间的连接，有效地提高了系统的安全性。

[0169] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

[0170] 以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

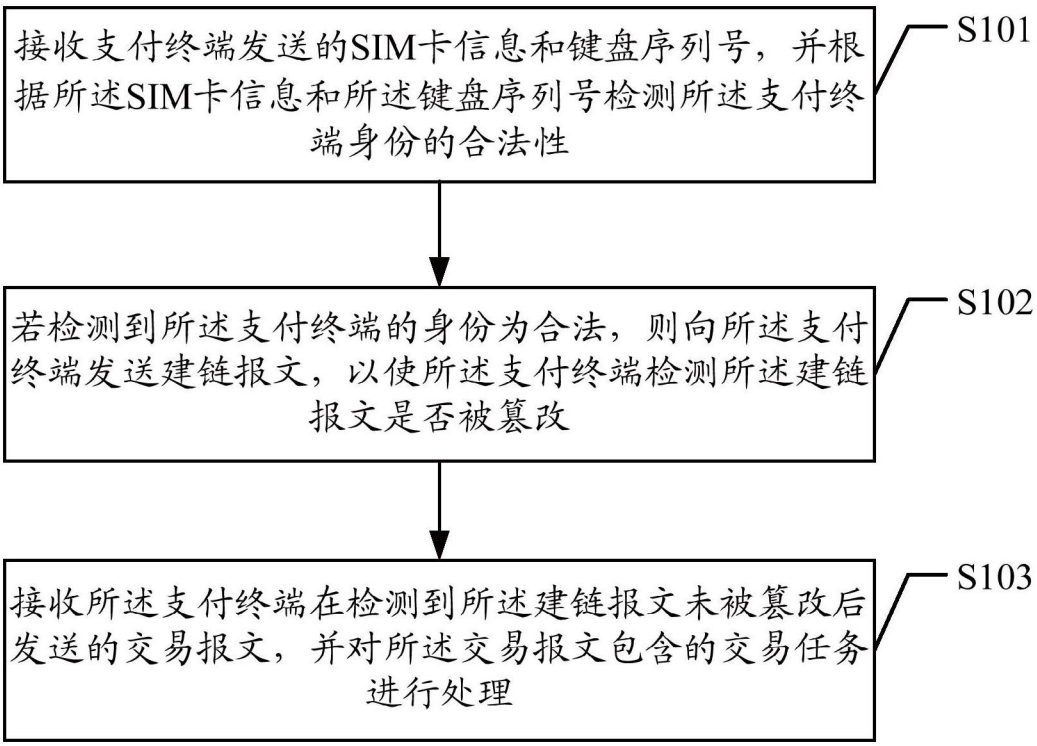

接收支付终端发送的SIM卡信息和键盘序列号，并根据所述SIM卡信息和所述键盘序列号检测所述支付终端身份的合法性
S101
若检测到所述支付终端的身份为合法，则向所述支付终端发送建链报文，以使所述支付终端检测所述建链报文是否被篡改
S102
接收所述支付终端在检测到所述建链报文未被篡改后发送的交易报文，并对所述交易报文包含的交易任务进行处理
S103

图1

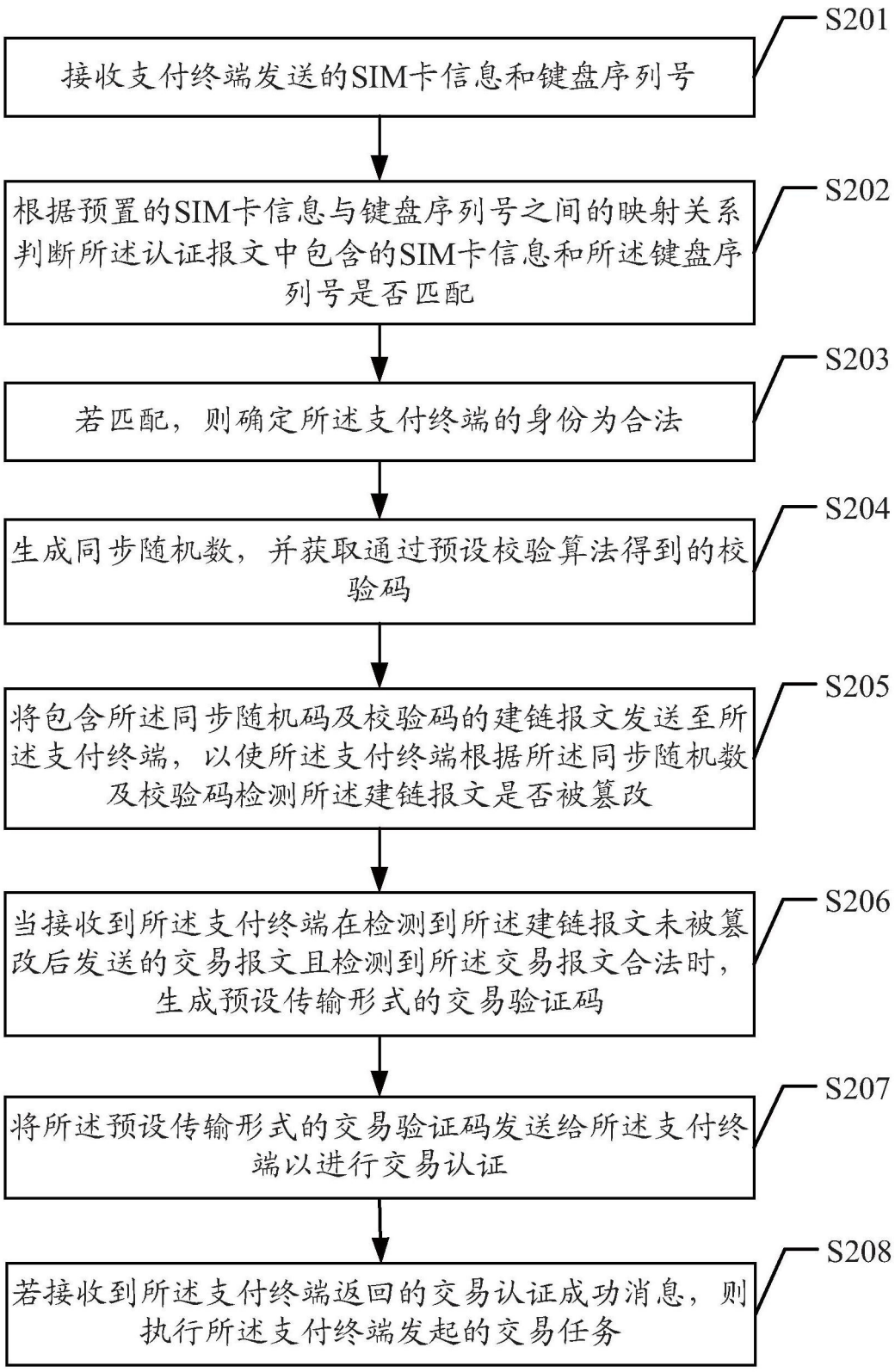

S201
接收支付终端发送的SIM卡信息和键盘序列号
S202
根据预置的SIM卡信息与键盘序列号之间的映射关系判断所述认证报文中包含的SIM卡信息和所述键盘序列号是否匹配
S203
若匹配，则确定所述支付终端的身份为合法
S204
生成同步随机数，并获取通过预设校验算法得到的校验码
S205
将包含所述同步随机码及校验码的建链报文发送至所述支付终端，以使所述支付终端根据所述同步随机数及校验码检测所述建链报文是否被篡改
S206
当接收到所述支付终端在检测到所述建链报文未被篡改后发送的交易报文且检测到所述交易报文合法时，生成预设传输形式的交易验证码
S207
将所述预设传输形式的交易验证码发送给所述支付终端以进行交易认证
S208
若接收到所述支付终端返回的交易认证成功消息，则执行所述支付终端发起的交易任务

图2

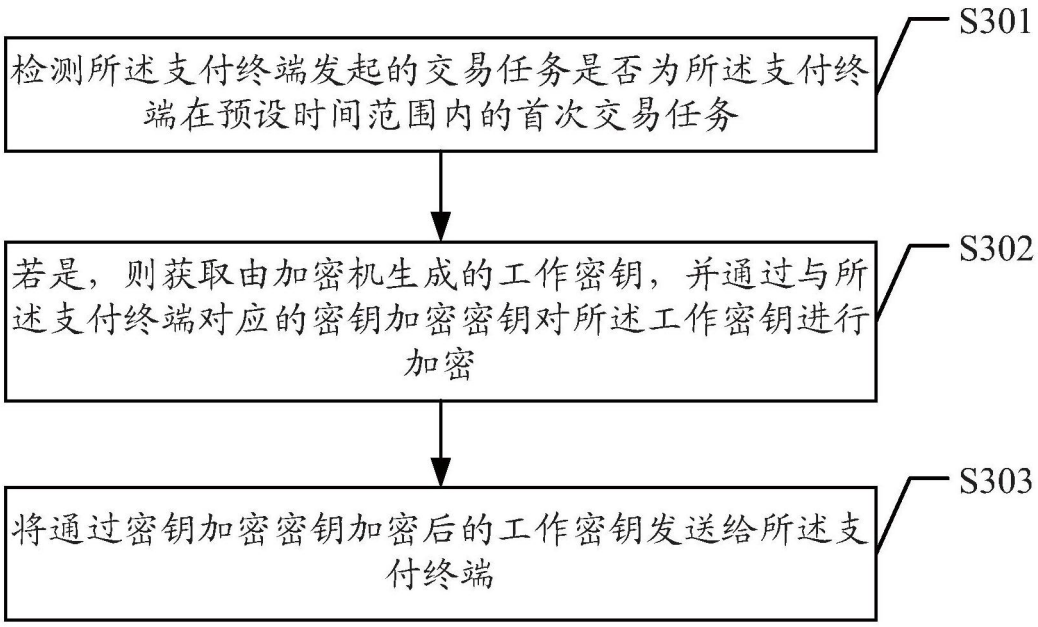

S301
检测所述支付终端发起的交易任务是否为所述支付终端在预设时间范围内的首次交易任务
S302
若是，则获取由加密机生成的工作密钥，并通过与所述支付终端对应的密钥加密密钥对所述工作密钥进行加密
S303
将通过密钥加密密钥加密后的工作密钥发送给所述支付终端

图3

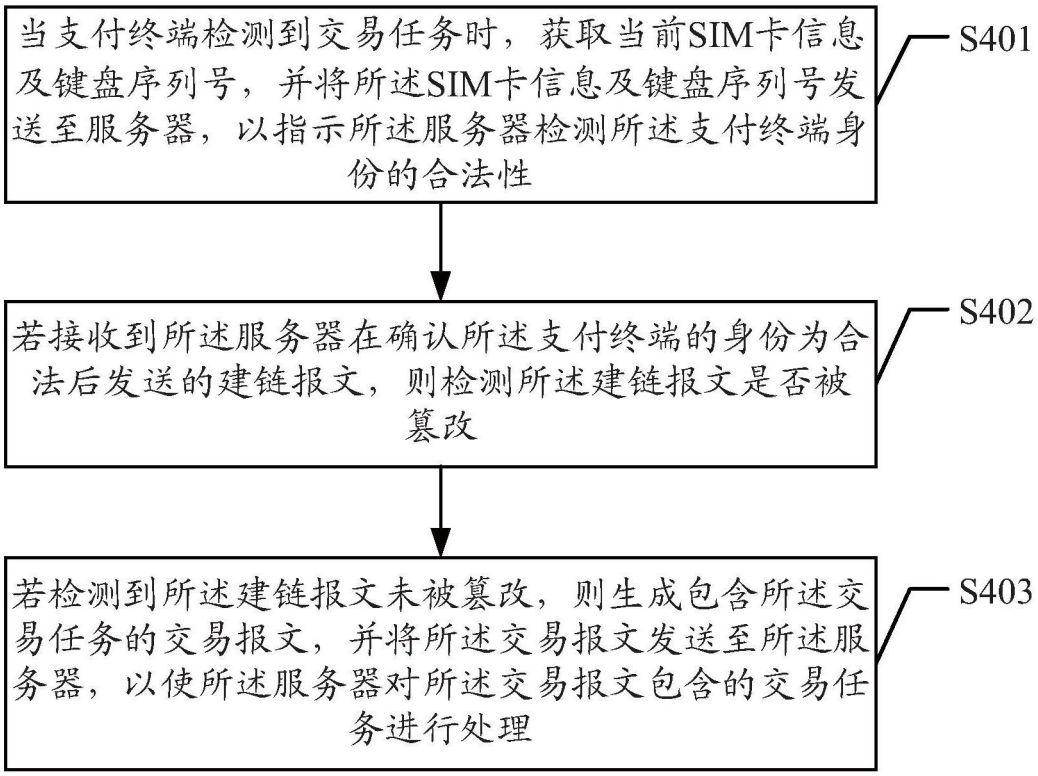

S401
当支付终端检测到交易任务时，获取当前SIM卡信息及键盘序列号，并将所述SIM卡信息及键盘序列号发送至服务器，以指示所述服务器检测所述支付终端身份的合法性
S402
若接收到所述服务器在确认所述支付终端的身份为合法后发送的建链报文，则检测所述建链报文是否被篡改
S403
若检测到所述建链报文未被篡改，则生成包含所述交易任务的交易报文，并将所述交易报文发送至所述服务器，以使所述服务器对所述交易报文包含的交易任务进行处理

图4

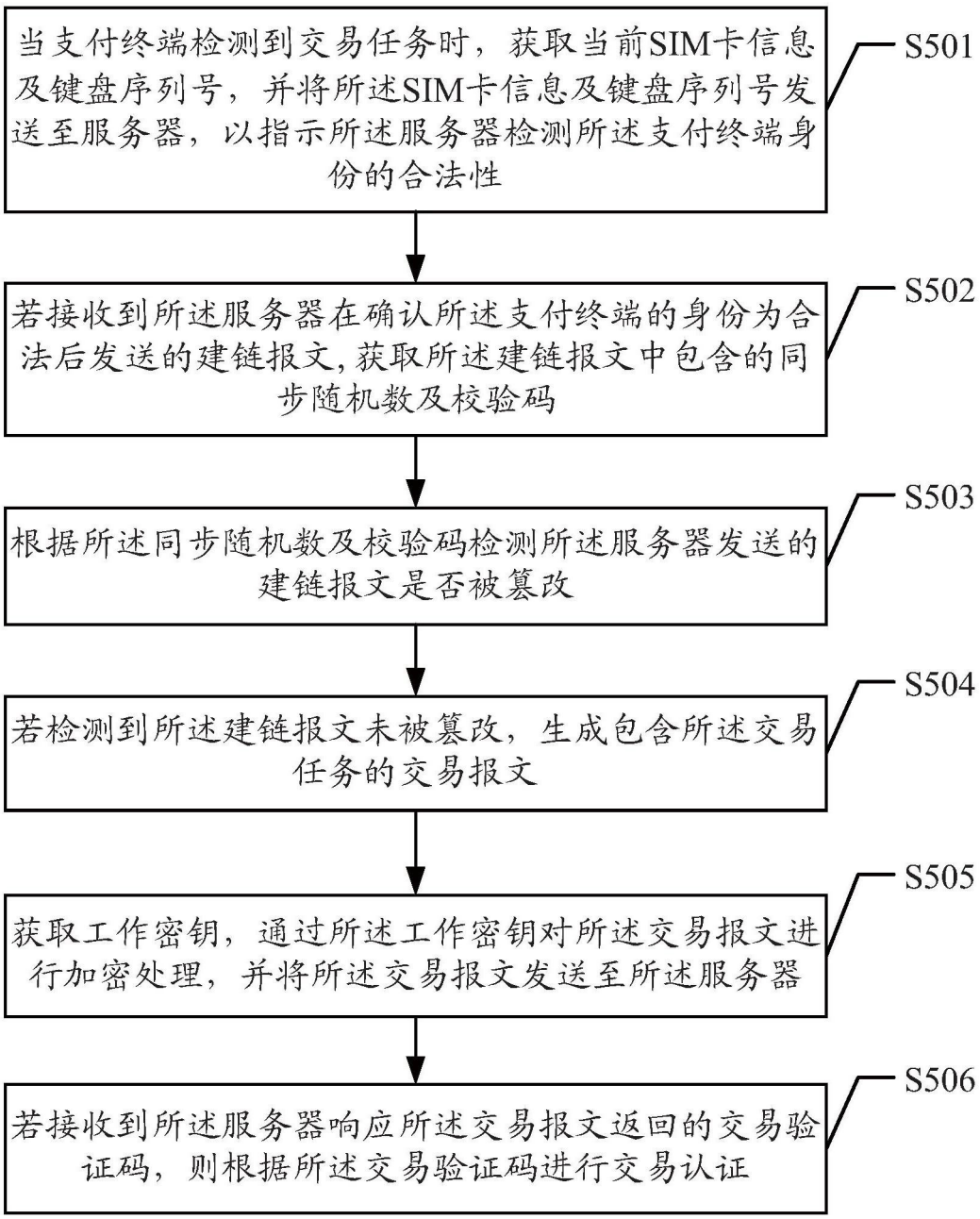

当支付终端检测到交易任务时，获取当前SIM卡信息及键盘序列号，并将所述SIM卡信息及键盘序列号发送至服务器，以指示所述服务器检测所述支付终端身份的合法性
S501
若接收到所述服务器在确认所述支付终端的身份为合法后发送的建链报文，获取所述建链报文中包含的同步随机数及校验码
S502
根据所述同步随机数及校验码检测所述服务器发送的建链报文是否被篡改
S503
若检测到所述建链报文未被篡改，生成包含所述交易任务的交易报文
S504
获取工作密钥，通过所述工作密钥对所述交易报文进行加密处理，并将所述交易报文发送至所述服务器
S505
若接收到所述服务器响应所述交易报文返回的交易验证码，则根据所述交易验证码进行交易认证
S506

图5

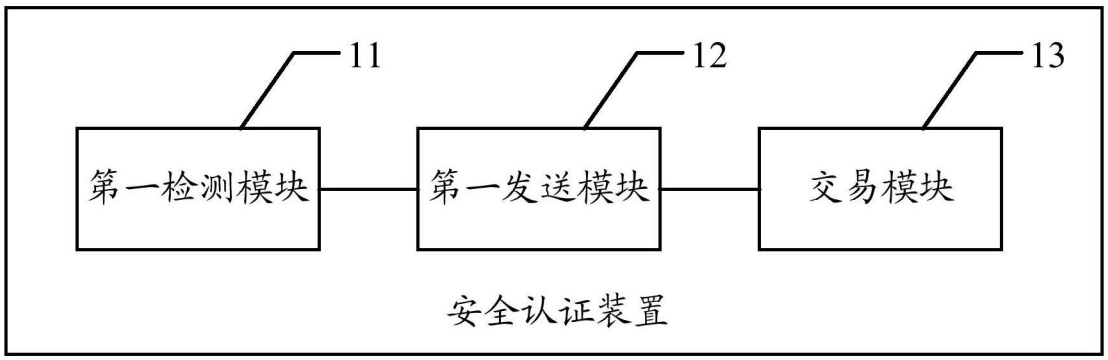

11
12
13
第一检测模块
第一发送模块
交易模块
安全认证装置

图6

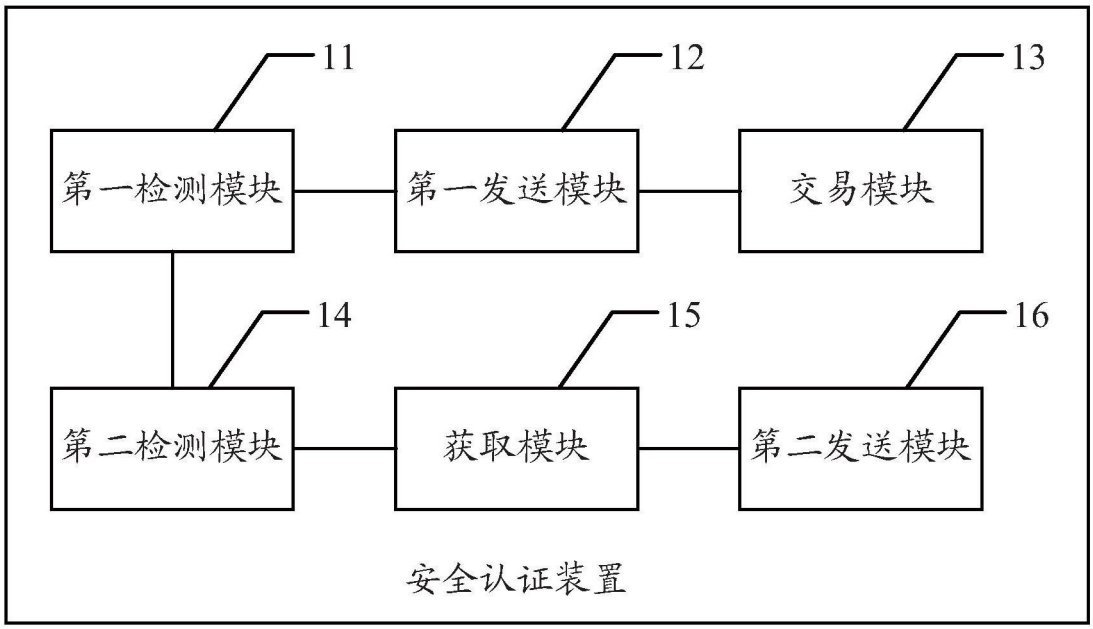

11
12
13
第一检测模块
第一发送模块
交易模块
14
15
16
第二检测模块
获取模块
第二发送模块
安全认证装置

图7

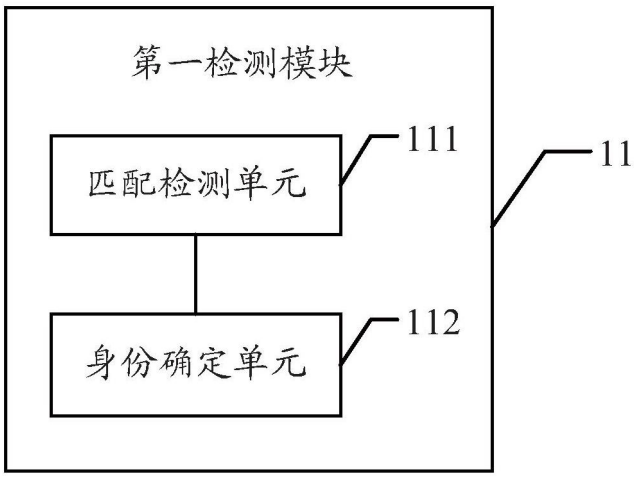

第一检测模块
匹配检测单元
111
11
身份确定单元
112

图8

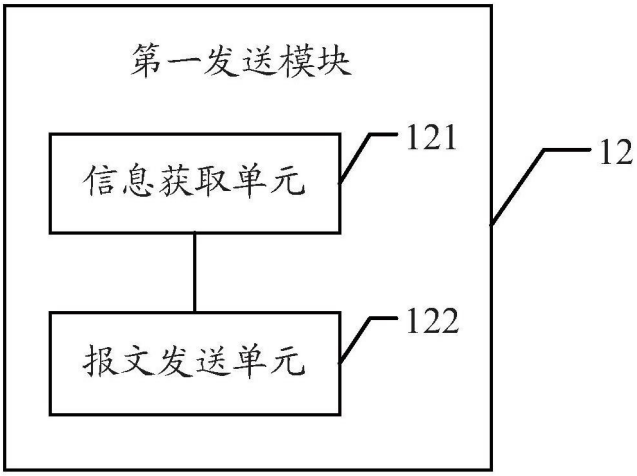

第一发送模块
信息获取单元
121
12
报文发送单元
122

图9

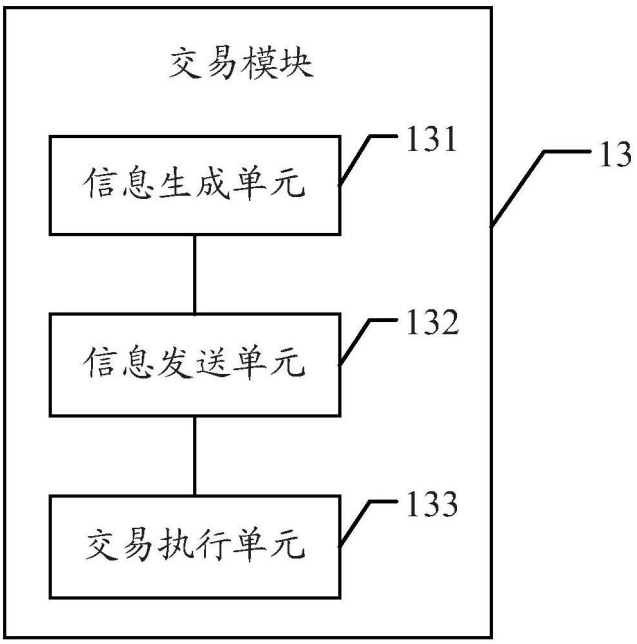

交易模块
信息生成单元
131
13
信息发送单元
132
交易执行单元
133

图10

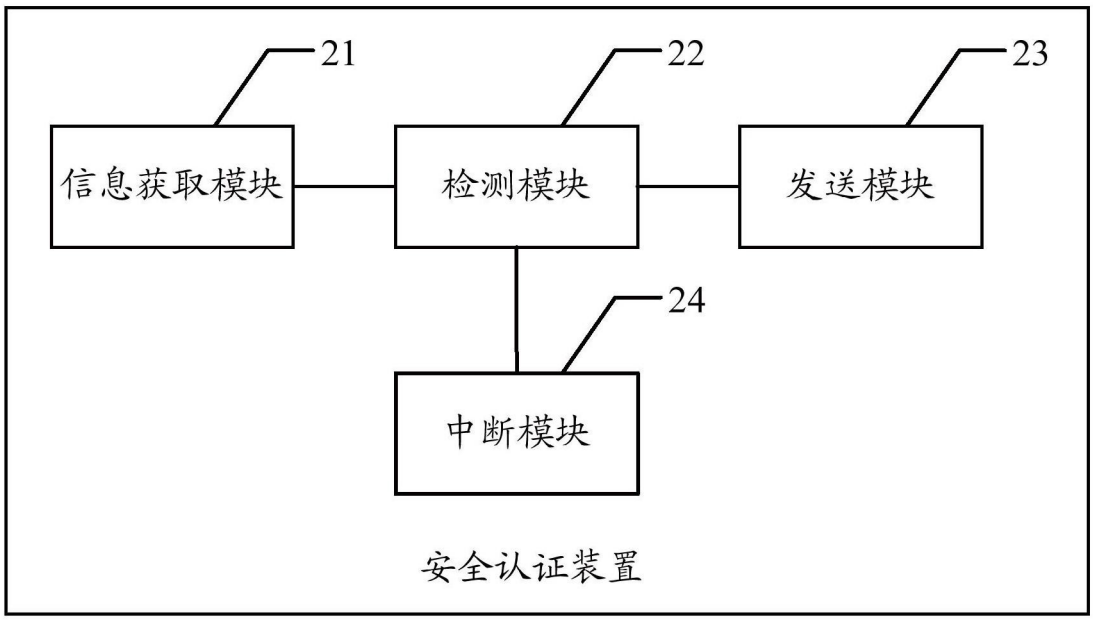

21
22
23
信息获取模块
检测模块
发送模块
24
中断模块
安全认证装置

图11

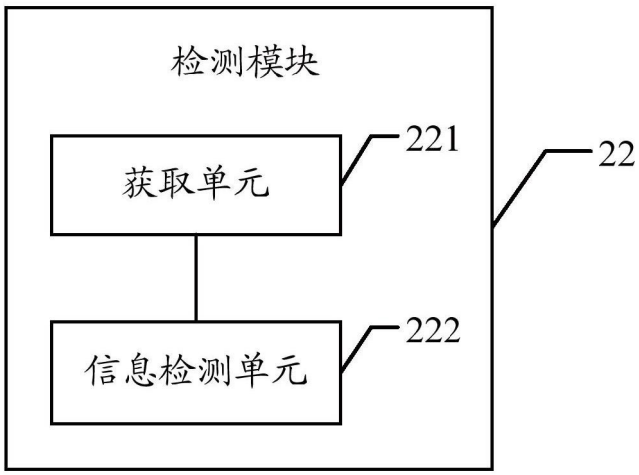


图12

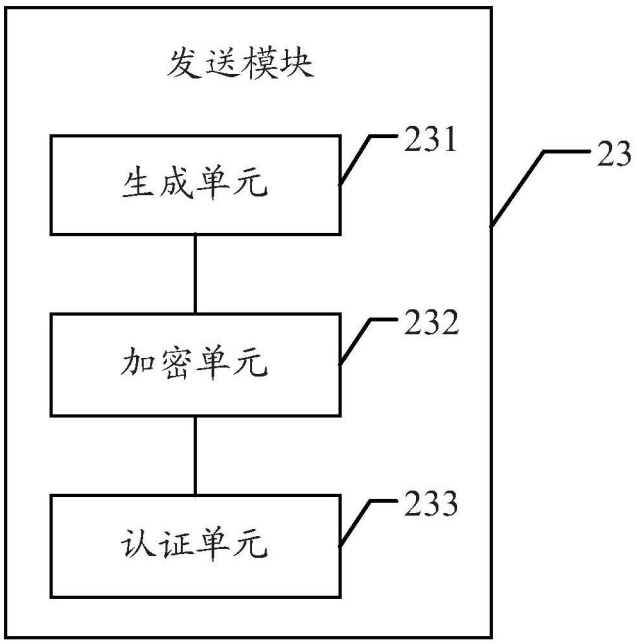


图13