(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 109451487 A
(43)申请公布日 2019.03.08

(21)申请号 201811345502.2

(22)申请日 2014.04.28

(62)分案原申请数据
201480001373.9 2014.04.28

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 随三军

(51)Int.Cl.
H04W 8/24(2009.01)
H04L 29/08(2006.01)

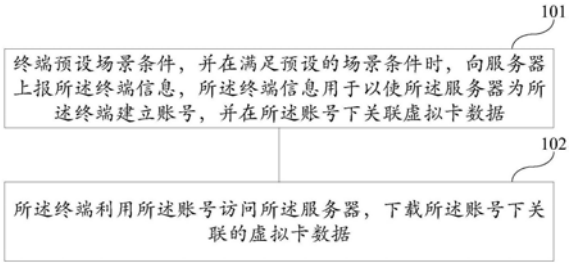
权利要求书2页 说明书13页 附图9页

(54)发明名称

虚拟卡下载方法、终端及中间设备

(57)摘要

本发明实施例提供一种虚拟卡下载方法、终端及中间设备，所述方法包括：终端预设场景条件，并在满足预设的场景条件时，向服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据；所述终端利用所述账号访问所述服务器，下载所述账号下关联的虚拟卡数据；所述场景条件为，所述终端与所述服务器建立通信连接。



CN 109451487 A

1.一种虚拟卡下载方法,其特征在于,所述方法包括:

所述终端与所述服务器建立通信连接,终端向服务器发送终端信息,所述终端信息用于为所述终端在所述服务器建立账号,所述账号关联虚拟卡数据;

所述终端通过所述账号访问所述服务器,通过通信连接下载所述账号关联的虚拟卡数据,所述虚拟卡数据用于安装在所述终端,所述终端通过所述虚拟卡数据应用虚拟卡业务。

2.根据权利要求1所述方法,其特征在于,所述方法还包括:

所述终端与所述服务器协商得到协商密钥,所述协商密钥用于对所述虚拟卡数据加密。

3.根据权利要求2所述方法,其特征在于,所述终端通过所述账号访问所述服务器,下载所述账号关联的虚拟卡数据具体包括:

所述终端接收所述服务器发送的通过所述协商密钥加密的所述虚拟卡数据,通过所述协商密钥对所述虚拟卡数据进行解密,下载所述虚拟卡数据。

4.根据权利要求1-3任一所述方法,其特征在于,所述终端信息包括所述终端的移动设备国际身份码IMEI(International Mobile Equipment Identity)、CPU序列号、或MAC(Media Access Control)地址。

5.根据权利要求1-4任一所述方法,其特征在于,所述方法还包括:所述服务器获取运营商为所述终端提供的虚拟卡数据,将所述虚拟卡数据与所述帐号关联。

6.根据权利要求1-5任一所述方法,其特征在于,所述方法还包括:所述终端接收所述服务器通过短信或彩信方式推送所述虚拟卡数据或所述虚拟卡数据的获取链接。

7.根据权利要求1-6任一所述方法,其特征在于,所述终端通过中间设备与所述服务器建立通信连接。

8.根据权利要求7所述方法,其特征在于,所述终端与所述中间设备通过蓝牙或WIFI方式连接。

9.一种终端,其特征在于,所述终端包括:

第一上报模块,用于在所述终端与所述服务器建立通信连接情况下,向服务器发送终端信息,所述终端信息用于为所述终端在所述服务器建立账号,所述账号关联虚拟卡数据;

第一下载模块,用于通过所述账号访问所述服务器,通过通信连接下载所述账号关联的虚拟卡数据,所述虚拟卡数据用于安装在所述终端,所述终端通过所述虚拟卡数据应用虚拟卡业务。

10.根据权利要求9所述终端,其特征在于,所述终端还包括:

第一协商模块,用于与所述服务器进行加密协商并得到协商密钥,所述协商密钥使所述服务器通过所述协商密钥对所述虚拟卡数据加密;

第一解密模块,用于通过所述协商密钥对所述虚拟卡数据进行解密。

11.根据权利要求10所述终端,其特征在于,所述第一下载模块还用于接收所述服务器发送的通过所述协商密钥加密的所述虚拟卡数据,通过所述协商密钥对所述虚拟卡数据进行解密,下载所述虚拟卡数据。

12.根据权利要求9-11任一所述终端,其特征在于,所述终端信息包括所述终端的移动设备国际身份码IMEI(International Mobile Equipment Identity)、CPU序列号、或MAC(Media Access Control)地址。

13.根据权利要求9-12任一所述终端，其特征在于，，所述第一下载模块还用于接收所述服务器通过短信或彩信方式推送所述虚拟卡数据或所述虚拟卡数据的获取链接。

14.一种终端，其特征在于，所述终端包括：处理器和存储器，其中，

所述存储器用于存储程序；所述处理器用于调用所述程序使得所述终端执行如权利要求1-8中任一项所述的方法。

15.一种计算机可读存储介质，包括指令，其特征在于，当其在计算机上运行时，使得所述计算机执行如权利要求1-8任一所述的方法。

虚拟卡下载方法、终端及中间设备

技术领域

[0001] 本发明涉及通信技术领域，特别涉及虚拟卡下载方法、终端及中间设备。

背景技术

[0002] 虚拟SIM卡(virtual sim card，简称VSIM)是当前移动终端领域中一项全新的概念。从功能上来说，VSIM可以取代现阶段内置于终端中的实体SIM卡。VSIM能够通过网络便捷的下载，为用户使用漫游等业务提供了更多方便。

[0003] 应用VSIM的用户不需要在手机上再插上除归属地SIM卡外的其他实物SIM卡，而是通过新建的号码申请服务器、利用2G/3G或其他制式的通信制式的数据通道，将相当于其他SIM卡的VSIM数据下载并安装到手机，用户便拥有了额外的手机号码。

[0004] 在现有技术中，VSIM的下载均是通过互联网，也就是连接互联网的终端，即可直接通过互联网，从运营商部署的数据服务器中下载VSIM。可见VSIM的下载十分便利，同时制约条件也非常明显，即必须依靠互联网。

[0005] 正是因此，现有技术的缺陷就在于，当用户因漫游、跨服务区等原因无法接入互联网时，便无法正常的下载VSIM并使用相关的业务。

发明内容

[0006] 本发明提供虚拟卡下载方法、终端及中间设备，通过预置虚拟卡或借助中间设备下载虚拟卡的方法，使得所述终端能够在未接入互联网的情况下正常使用VSIM业务。

[0007] 为了解决以上技术问题，本发明采取的技术方案是：

[0008] 第一方面，本发明提供了一种虚拟卡下载方法，所述方法包括：

[0009] 终端预设场景条件，并在满足预设的场景条件时，向服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据；

[0010] 所述终端利用所述账号访问所述服务器，下载所述账号下关联的虚拟卡数据；

[0011] 所述场景条件为，所述终端与所述服务器建立通信连接。

[0012] 在第一方面的第一种可能的实现方式中，所述方法还包括：

[0013] 所述终端与所述服务器进行加密协商并得到协商密钥，所述协商密钥用于使所述服务器利用所述协商密钥对所述账号和虚拟卡数据加密。

[0014] 在第一方面的第二种可能的实现方式中，所述终端利用所述账号向访问所述服务器，下载所述账号下关联的虚拟卡数据具体为：

[0015] 所述终端利用所述协商密钥对所述终端的账号进行解密，并利用所述账号向访问所述服务器；所述终端利用所述协商密钥对所述账号下关联的虚拟卡数据解密，并下载所述虚拟卡数据。

[0016] 第二方面，本发明提供了一种虚拟卡下载方法，所述方法包括：

[0017] 终端与连接到服务器的中间设备建立通信连接；

[0018] 所述终端通过所述中间设备，向所述服务器上报终端信息，所述终端信息用于使

所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据；

[0019] 所述终端利用所述账号访问所述中间设备，下载所述账号下关联的虚拟卡数据。

[0020] 在第二方面的第一种可能的实现方式中，所述终端与中间设备建立通信连接具体为：

[0021] 所述终端与所述中间设备建立近场通信连接。

[0022] 在第二方面的第二种可能的实现方式中，所述方法还包括：

[0023] 所述终端与所述中间设备保存的服务器公钥进行加密协商，并得到协商密钥，所述协商密钥用于使所述服务器或所述中间设备利用所述协商密钥对所述账号和虚拟卡数据加密。

[0024] 在第二方面的第三种可能的实现方式中，所述终端利用所述账号访问所述中间设备，下载所述账号下关联的虚拟卡数据具体为：

[0025] 所述终端利用所述协商密钥对所述终端的账号进行解密，并利用所述账号向访问所述中间设备；所述终端利用所述协商密钥对所述账号下关联的虚拟卡数据解密，并下载所述虚拟卡数据。

[0026] 第三方面，本发明提供了一种虚拟卡下载方法，所述方法包括：

[0027] 中间设备与终端建立通信连接，所述中间设备与服务器连接；

[0028] 所述中间设备接收所述终端上报的终端信息；

[0029] 所述中间设备向所述服务器发送所述终端信息，所述终端信息用于所述服务器为所述终端建立帐号，并确定与所述帐号关联的虚拟卡数据；

[0030] 所述中间设备接收所述终端的访问，向所述终端发送虚拟卡数据。

[0031] 在第三方面的第一种可能的实现方式中，所述中间设备与终端建立通信连接具体为：

[0032] 所述中间设备与终端建立近场通信连接。

[0033] 在第三方面的第二种可能的实现方式中，所述中间设备向所述终端发送虚拟卡数据具体为：

[0034] 所述中间设备查找自身存储中是否保存了所述虚拟卡数据，如果保存则从自身存储中提取并发送所述虚拟卡数据；否则所述中间设备从所述服务器获取所述虚拟卡数据并向所述终端发送。

[0035] 在第三方面的第三种可能的实现方式中，所述方法还包括：

[0036] 所述中间设备利用自身保存的服务器公钥与所述终端进行加密协商，并得到协商密钥，利用所述协商密钥对所述账号和虚拟卡数据加密。

[0037] 在第三方面的第四种可能的实现方式中，所述利用所述协商密钥对所述账号和虚拟卡数据加密具体为：

[0038] 所述中间设备查找自身存储中是否保存了所述协商密钥，如果保存则所述中间设备利用自身存储中的协商密钥进行加密；否则所述中间设备从服务器获取所述协商密钥并加密。

[0039] 第四方面，本发明提供了一种终端，所述终端包括：

[0040] 第一上报模块，用于预设场景条件，并在满足预设的场景条件时，向服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟

卡数据;所述场景条件为,终端与服务器建立通信连接;

[0041] 第一下载模块,用于利用所述账号访问所述服务器,下载所述账号下关联的虚拟卡数据。

[0042] 在第四方面的第一种可能的实现方式中,所述终端还包括:

[0043] 第一协商模块,用于与所述服务器进行加密协商并得到协商密钥,所述协商密钥使所述服务器利用所述协商密钥对所述账号和虚拟卡数据加密;

[0044] 第一解密模块,用于利用所述协商密钥对所述终端的账号进行解密,利用所述协商密钥对所述账号下关联的虚拟卡数据解密。

[0045] 第五方面,本发明提供了一种终端,所述终端包括:

[0046] 通信模块,用于与连接到服务器的中间设备建立通信连接;

[0047] 第二上报模块,用于通过所述中间设备,向所述服务器上报终端信息,所述终端信息用于使服务器为所述终端建立账号,并在所述账号下关联虚拟卡数据;

[0048] 第二下载模块,用于利用所述账号访问所述中间设备访问,下载所述账号下关联的虚拟卡数据。

[0049] 在第五方面的第一种可能的实现方式中,所述终端还包括:

[0050] 第二协商模块,用于与所述中间设备保存的服务器公钥进行加密协商,并得到协商密钥,所述协商密钥用于使所述服务器或所述中间设备利用所述协商密钥对所述账号和虚拟卡数据加密;

[0051] 第二解密模块,用于利用所述协商密钥对所述终端的账号进行解密,利用所述协商密钥对所述账号下关联的虚拟卡数据解密。

[0052] 第六方面,本发明提供了一种中间设备,所述中间设备包括:

[0053] 连接模块,用于与终端建立通信连接,与服务器连接;

[0054] 上报模块,用于接收所述终端上报的终端信息,向所述服务器发送所述终端信息,所述终端信息用于所述服务器为所述终端建立帐号,并确定与所述帐号关联的虚拟卡数据;

[0055] 交换模块,用于接收所述终端的访问,向所述终端发送虚拟卡数据。

[0056] 在第六方面的第一种可能的实现方式中,所述交换模块包括:

[0057] 查询单元,用于查找存储模块中是否保存了所述虚拟卡数据;

[0058] 存储单元,用于存储所述虚拟卡数据并向所述终端发送;

[0059] 获取单元,用于在存储模块中未保存所述虚拟卡数据时,从所述服务器获取所述虚拟卡数据并保存在所述存储单元。

[0060] 在第六方面的第二种可能的实现方式中,所述中间设备还包括:

[0061] 加密模块,用于利用自身保存的服务器公钥与所述终端进行加密协商,并得到协商密钥,利用所述协商密钥对所述账号和虚拟卡数据加密。

[0062] 第七方面,本发明提供了一种终端,所述终端包括:处理器、发送器和接收器;所述处理器与所述发送器连接;所述处理器与所述接收器连接;其中,

[0063] 所述处理器用于,预设场景条件,所述场景条件为,所述终端与所述服务器建立通信连接;

[0064] 所述发送器用于,在满足预设的场景条件时,向服务器上报终端信息,所述终端信

息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据；利用所述账号访问所述服务器；

[0065] 所述接收器用于，在所述发送器利用所述帐号访问所述服务器后，下载所述账号下关联的虚拟卡数据。

[0066] 在第七方面第一种可能的实现方式中，所述处理器还用于，与所述服务器进行加密协商并得到协商密钥，所述协商密钥用于使所述服务器利用所述协商密钥对所述账号和虚拟卡数据加密；利用所述协商密钥对所述终端的帐号进行解密；利用所述协商密钥对所述账号下关联的虚拟卡数据进行解密；

[0067] 所述发送器具体用于，在所述处理器利用所述协商密钥对所述终端的帐号进行解密后，利用所述帐号访问所述服务器；

[0068] 所述接收器具体用于，在所述处理器利用所述协商密钥对所述账号下关联的虚拟卡数据进行解密后，下载所述帐号下关联的虚拟卡数据。

[0069] 第八方面，本发明提供了一种终端，所述终端包括：处理器、发送器和接收器；所述处理器与所述发送器连接；所述处理器与所述接收器连接；其中，：

[0070] 所述处理器用于，与连接到服务器的中间设备建立通信连接；

[0071] 所述发送器用于，通过所述中间设备，向所述服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据；利用所述账号访问所述服务器；

[0072] 所述接收器用于，在所述发送器利用所述帐号访问所述服务器后，下载所述账号下关联的虚拟卡数据。

[0073] 在第八方面第一种可能的实现方式中，所述处理器还用于，与所述中间设备保存的服务器公钥进行加密协商，并得到协商密钥，所述协商密钥用于使所述服务器或所述中间设备利用所述协商密钥对所述账号和虚拟卡数据加密；利用所述协商密钥对所述终端的账号进行解密；利用所述协商密钥对所述账号下关联的虚拟卡数据进行解密；

[0074] 所述发送器具体用于，在所述处理器利用所述协商密钥对所述终端的帐号进行解密后，利用所述帐号访问所述服务器；

[0075] 所述接收器具体用于，在所述处理器利用所述协商密钥对所述账号下关联的虚拟卡数据进行解密后，下载所述帐号下关联的虚拟卡数据。

[0076] 第九方面，本发明提供了一种中间设备，所述中间设备包括：处理器、发送器和接收器；所述处理器与所述发送器连接；所述处理器与所述接收器连接；其中，

[0077] 所述处理器用于，与终端建立通信连接，与服务器连接；

[0078] 所述发送器用于，向所述服务器发送所述终端信息，所述终端信息用于所述服务器为所述终端建立帐号，并确定与所述帐号关联的虚拟卡数据；向所述终端发送虚拟卡数据；

[0079] 所述接收器用于，收所述终端上报的终端信息；接收所述终端的访问。

[0080] 在第九方面第一种可能的实现方式中，所述处理器还用于，查找自身存储中是否保存了所述虚拟卡数据，如果保存则从自身存储中提取所述虚拟卡数据；

[0081] 所述接收器还用于，在未保存所述虚拟卡数据时，从所述服务器获取所述虚拟卡数据。

[0082] 在第九方面第二中可能的实现方式中，所述处理器还用于，利用自身保存的服务器公钥与所述终端进行加密协商，并得到协商密钥，利用所述协商密钥对所述账号和虚拟卡数据加密。

[0083] 第十方面，本发明提供了一种终端，所述终端包括：存储器；所述存储器用于，保存预设的虚拟卡数据。

[0084] 在第十方面第一种可能的实现方式中，所述终端还包括：处理器，数据传输模块；所述处理器与所述存储器连接；所述处理器与所述数据传输模块连接；其中，在所述存储器保存预设的虚拟卡数据之前，

[0085] 所述数据传输模块用于，与第一设备建立物理连接；

[0086] 所述处理器用于，在所述数据传输模块与所述第一设备建立物理连接后，经由所述数据传输模块获取预设的虚拟卡数据。

[0087] 通过以上技术方案可知，本发明存在的有益效果是：通过预设场景条件，使终端与服务器建立通信连接的时候预先下载虚拟卡数据；或者通过近场通信连接中间设备与终端，使得所述中间设备间接的连接所述终端与服务器，从而使所述终端无需互联网而完成虚拟卡数据的下载，避免了用户在急需使用虚拟卡业务时恰巧终端未接入互联网，从而妨碍虚拟卡业务应用的特殊情况。

附图说明

[0088] 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。

[0089] 图1-2为本发明实施例所述方法流程图；

[0090] 图3为本发明实施例所述终端结构示意图；

[0091] 图4-5为本发明另一实施例所述方法流程图；

[0092] 图6-7为本发明又一实施例所述方法流程图；

[0093] 图8为本发明实施例所述终端结构示意图；

[0094] 图9为本发明实施例所述中间设备结构示意图；

[0095] 图10为本发明实施例所述终端接收示意图；

[0096] 图11-12为本发明实施例所述终端和中间设备的结构示意图；

[0097] 图13为本发明实施例所述终端结构示意图。

具体实施方式

[0098] 为了使本技术领域的人员更好地理解本发明实施例的方案，下面结合附图和实施方式对本发明实施例作进一步的详细说明。

[0099] 在现阶段，终端从服务器下载虚拟卡(即VSIM)数据往往是依靠互联网，特别是移动互联网。如果终端一直保持入网状态，那么所述终端即可以在需要开始应用虚拟卡业务的时候，随时下载虚拟卡数据，十分方便快捷。不过单纯依靠互联网进行虚拟卡数据下载的方式，所受的限制也是很明显的。假如终端处在漫游、跨服务区等特殊场景下的时候，不能

或者不便于保持入网，则无法开始应用虚拟卡业务。

[0100] 并且在很多时候，用户正是在漫游、跨服务区等特殊场景下，才会急需应用虚拟卡业务。可见单纯依靠互联网下载虚拟卡数据的方式，存在着比较大的弊端。这也是本发明中所要解决的问题。

[0101] 参见图1所示，为本发明所述方法的一个具体的实施例，本实施例中描述了终端一侧下载虚拟卡数据的过程，所述方法具体包括以下步骤：

[0102] 步骤101、终端预设场景条件，并在满足预设的场景条件时，向服务器上报所述终端信息，所述终端信息用于以使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据。

[0103] 为了避免用户在急需使用虚拟卡业务时恰巧终端未接入互联网，从而妨碍虚拟卡业务应用的特殊情况，本实施例中预先为所述终端设置场景条件，使得中端在所述场景条件下，自动触发虚拟卡数据的下载流程。

[0104] 本实施例中所述场景条件为，所述终端与所述服务器建立通信连接。也就是说，所述终端将在网络状况良好的时候自动的触发虚拟卡数据的下载，提前获得所述的虚拟卡数据。这样就可以在有需求时，直接开始应用虚拟卡业务。

[0105] 还需要说明的是，上述所谓的终端与服务器之间的通信连接，不仅限于互联网连接；凡是能够实现虚拟卡数据下载的通信连接均涵盖在本实施例的整体方案之下，此处无需具体的限定。

[0106] 在虚拟卡数据下载流程触发之后，所述终端首先向所述服务器上报终端信息。所述终端信息可以包括终端的IMEI(International Mobile Equipment Identity，即移动设备国际身份码)、CPU序列号及MAC(Media Access Control)地址等表明终端身份的信息。所述服务器接收到终端信息之后，根据所述终端信息为所述终端建立一个账号，所述账号即固定的对应着所述终端。同时所述服务器获取运行商为所述终端提供的虚拟卡数据，将所述虚拟卡数据关联到所述账号之下，以便于后续供所述终端下载。所谓将虚拟卡数据关联到账号之下，也就是意味着能够通过所述账号直接的调用所述虚拟卡数据，当终端访问所述账号时即可直接从所述账号中下载自身所需的虚拟卡数据。

[0107] 步骤102、所述终端利用所述账号访问所述服务器，下载所述账号下关联的虚拟卡数据。

[0108] 在所述服务器为所述终端建立了对应的账号，并关联了虚拟卡数据之后；所述终端使用账号向所述服务器进行访问时，所述服务器即可验证所述终端中包含的终端信息(查询所述终端的IMEI、CPU序列号及MAC地址等)，进而供所述终端进行访问。然后，所述终端通过所述通信连接下载所述终端账号之下关联的虚拟卡数据。

[0109] 通过以上技术方案可知，本实施例存在的有益效果是：通过预设场景条件，使在终端与服务器建立通信连接的时候预先下载虚拟卡数据，避免了用户在急需使用虚拟卡业务时恰巧终端未接入互联网，从而妨碍虚拟卡业务应用的特殊情况。

[0110] 在本发明的一个实施例中，所述服务器可以为运营商服务器，所述终端在预设场景条件下下载所述帐号下关联的虚拟卡数据可具体为：所述终端在预设场景下经由所述运营商服务器的数据传输通道下载虚拟卡数据。例如，所述运营商服务器获知所述终端的通用集成电路卡(Universal Integrated Circuit Card，UICC)的帐号信息，所述运营商服务

器可以短信或彩信方式推送所述虚拟卡数据或所述虚拟卡数据的获取链接。在预设的场景条件，即所述终端与所述运营商服务器可建立通信连接时，所述终端接收所述运营商服务器发送的短信或彩信，经由终端与运营商服务器之间的数据传输通道预先下载所述虚拟卡数据，以便于在终端无法与服务器连接且急需使用虚拟卡业务时可调用所述虚拟卡数据。

[0111] 参照图2所示，为本发明所述方法的另一个具体实施例，本实施例在图1所示实施例的基础之上，扩充了协商加密的技术方案。本实施例中所述方法包括以下步骤：

[0112] 步骤201、终端预设场景条件，并在满足预设的场景条件时，向服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据。

[0113] 所述场景条件为，所述终端与所述服务器建立通信连接。

[0114] 步骤202、所述终端与所述服务器进行加密协商并得到协商密钥，所述协商密钥用于使所述服务器利用所述协商密钥对所述账号和虚拟卡数据加密。

[0115] 本实施例中，在建立了账号并在账号下关联了虚拟卡数据之后，为保证所述账号和虚拟卡数据的安全性，所以结合了协商加密的技术方案。所述加密协商具体为DH协商(密钥交换协议/算法(Diffie-Hellman)。所述DH协商为现有的加密技术，其原理可以简要的概括为，双方利用DH算法协商得到对称的协商密钥，进而利用所述协商密钥进行加密和解密。所述终端与所述服务器进行DH协商之后得到协商密钥，本实施例中，所述协商密钥包括两个密钥对，即服务器公钥与服务器私钥、终端公钥与终端私钥。根据DH协商的原理，本步骤中所述服务器利用其中的服务器公钥、服务器私钥和终端公钥三者对所述账号和账号关联的虚拟卡数据进行加密。

[0116] 步骤203、所述终端利用所述协商密钥对所述终端的账号进行解密，并利用所述账号向访问所述服务器；所述终端利用所述协商密钥对所述账号下关联的虚拟卡数据解密，并下载所述虚拟卡数据。

[0117] 由于所述账号及虚拟卡数据已经加密，所以所述终端必须在解密之后才能够访问账号并下载虚拟卡数据。根据DH协商的原理，本步骤中终端利用终端公钥、终端私钥和服务器公钥对账号和虚拟卡数据进行解密。需要说明的是，所述账号和所述虚拟卡数据均利用所述协商密钥进行了加密，也就是说，终端需先对所述账号进行解密，才可以执行访问并下载虚拟卡数据，还需再对虚拟卡数据进行解密，才能够最终利用所述虚拟卡数据实现虚拟卡相关的业务。

[0118] 通过以上技术方案可知，本实施例存在的有益效果是，通过在所述方法中结合协商加密的技术方案，确保了终端账号和虚拟卡数据的安全性。

[0119] 参见图3所示，为本发明所述终端的一个具体实施例。本实施例中，所述终端即是以图1-2所示方法完成虚拟卡数据下载的设备。所述终端包括：

[0120] 第一上报模块301，用于预设场景条件，并在满足预设的场景条件时，向服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据；所述场景条件为，终端与服务器建立通信连接。

[0121] 第一下载模块302，用于利用所述账号访问所述服务器，下载所述账号下关联的虚拟卡数据。

[0122] 第一协商模块303，用于与所述服务器进行加密协商并得到协商密钥，所述协商密

钥使所述服务器利用所述协商密钥对所述账号和虚拟卡数据加密。

[0123] 第一解密模块304，用于利用所述协商密钥对所述终端的账号进行解密，利用所述协商密钥对所述账号下关联的虚拟卡数据解密。

[0124] 通过以上技术方案可知，本实施例中所述终端存在的有益效果是：通过预设场景条件，使在所述终端与所述服务器建立通信连接的时候预先下载虚拟卡数据，避免了用户在急需使用虚拟卡业务时恰巧终端未接入互联网，从而妨碍虚拟卡业务应用的特殊情况；通过结合协商加密的技术方案，确保了终端账号和虚拟卡数据的安全性。

[0125] 图1-3所示的三个实施例，描述了通过场景条件解决现有技术问题的方法以及相应的终端。不过在本发明实施例中，还提供了利用终端与服务器之间的中间设备，解决相关技术问题的技术方案，将在以下的几个实施例中具体介绍：

[0126] 参照图4所示，为本发明实施例所提供的虚拟卡下载方法的另一个具体实施例，本实施例中描述了终端一侧下载虚拟卡数据的过程，所述方法具体包括以下步骤：

[0127] 步骤401、终端与连接到服务器的中间设备建立通信连接。

[0128] 本实施例中，所述终端可以在没有通信网络可以直接连接到所述服务器的时候，可以通过所述中间设备间接的与所述服务器连接并通信。所述终端与所述中间设备利用近场通信(例如蓝牙、wifi等)的方式连接。

[0129] 所述中间设备可以认为是所述服务器部署上的延伸，天然的与所述服务器存在连接关系。每个中间设备在通信层面上将覆盖一定的范围(能够达成近场通信的范围)。未入网的终端如果需要下载虚拟卡数据，使用虚拟卡业务，需要置于所述中间设备的覆盖范围之内，通过不受到网络影响的近场通信连接所述中间设备，也就相当于能够实现与所述服务器的通信。由此解决了终端未入网便无法下载虚拟卡数据的问题。

[0130] 步骤402、所述终端通过所述中间设备，向所述服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据。

[0131] 步骤403、所述终端利用所述账号访问所述中间设备，下载所述账号下关联的虚拟卡数据。

[0132] 本实施例中，所述终端将直接的与所述中间设备进行通信；不过具体为终端建立账号并提供虚拟卡数据的设备，依然是服务器。所以所述终端信息的上报，以及虚拟卡数据的下载，均是需要利用所述中间设备在终端和服务器之间进行中转。除此之外，本实施例中其余的技术特征均和图1所示实施例一致。

[0133] 参见图5所示，为本发明所述方法的具体实施例。对应图4所示实施例，本实施例将从所述中间设备的一个描述所述下载过程。本实施例中所述方法具体为：

[0134] 步骤501、中间设备与终端建立通信连接，所述中间设备与服务器连接。

[0135] 可以近似的认为，所述中间设备相当于是所述服务器延伸部署的通信热点，在所述中间设备的通信覆盖范围内，所述终端无需接入互联网，就能够正常的下载虚拟卡数据，应用虚拟卡业务。当所述服务器部署大量的中间设备，不断的提高中间设备的覆盖率，就可以实现所述终端随时随地进行虚拟卡数据的下载。

[0136] 步骤502、所述中间设备接收所述终端上报的终端信息；所述中间设备向所述服务器发送所述终端信息，所述终端信息用于所述服务器为所述终端建立帐号，并确定与所述帐号关联的虚拟卡数据。

[0137] 步骤503、所述中间设备接收所述终端的访问，向所述终端发送虚拟卡数据。

[0138] 通过图4-5所示技术方案可知，本实施例存在的有益效果是：通过近场通信连接所述中间设备与所述终端，使得所述中间设备间接的连接所述终端与所述服务器，从而使所述终端无需互联网而完成虚拟卡数据的下载，避免了用户在急需使用虚拟卡业务时恰巧终端未接入互联网，从而妨碍虚拟卡业务应用的特殊情况。

[0139] 图4-5所示实施例，为利用所述中间设备完成虚拟卡数据下载的技术实施例。而为了提高所述技术方案的安全性，同理可在所述技术方案的基础上结合加密协商的优化方案。具体如下：

[0140] 参照图6所示，为本发明所述虚拟卡下载方法的又一个具体实施例，本实施例中所述方法包括：

[0141] 步骤601、终端与连接到服务器的中间设备建立通信连接。

[0142] 步骤602、所述终端通过所述中间设备，向所述服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据。

[0143] 步骤603、所述终端与所述中间设备保存的服务器公钥进行加密协商，并得到协商密钥，所述协商密钥用于使所述服务器或所述中间设备利用所述协商密钥对所述账号和虚拟卡数据加密。

[0144] 本实施例中，所述加密协商同样为DH协商。所述终端具体将与所述服务器的公钥进行DH协商，不过本实施例中所述终端不再与所述服务器直接连接，所以所述中间设备中保存所述服务器公钥，代替所述服务器与所述终端进行DH协商。

[0145] 所述DH协商为现有的加密技术，之前的实施例中已经介绍，在此不赘述其原理。所述终端与所述服务器公钥进行DH协商之后得到协商密钥，所述中间设备和所述服务器均应该留存有所述协商密钥。本实施例中，所述协商密钥包括两个密钥对，即服务器公钥与服务器私钥、终端公钥与终端私钥。根据DH协商的原理，本步骤中所述中间设备利用其中的服务器公钥、服务器私钥和终端公钥三者对所述账号和账号关联的虚拟卡数据进行加密。

[0146] 步骤604、所述终端利用所述协商密钥对所述终端的账号进行解密，并利用所述账号向访问所述中间设备；所述终端利用所述协商密钥对所述账号下关联的虚拟卡数据解密，并下载所述虚拟卡数据。

[0147] 由于所述账号及虚拟卡数据已经加密，所以所述终端必须在解密之后才能够访问账号并下载虚拟卡数据。根据DH协商的原理，本步骤中终端利用终端公钥、终端私钥和服务器公钥对账号和虚拟卡数据进行解密。

[0148] 参见图7所示，为本发明所述为所述方法的再一个具体实施例，对应图6所示实施例，本实施例将从中间设备的一个描述所述下载过程。本实施例中所述方法具体为：

[0149] 步骤701、中间设备与终端建立通信连接，所述中间设备与服务器连接，并保存所述服务器的公钥。

[0150] 步骤702、所述中间设备接收所述终端上报的终端信息；所述中间设备向所述服务器发送所述终端信息，所述终端信息用于所述服务器为所述终端建立帐号，并确定与所述帐号关联的虚拟卡数据。

[0151] 步骤703、所述中间设备利用自身保存的服务器公钥与所述终端进行加密协商，并得到协商密钥，利用所述协商密钥对所述账号和虚拟卡数据加密。

[0152] 一般而言，所述中间设备代替所述服务器与所述终端进行加密协商之后，自身应该留存所述协商密钥，但也不排除协商密钥只留存在所述服务器中，而所述中间设备并未保存的情况。所以加密过程中，所述中间设备查找自身存储中是否保存了所述协商密钥，如果保存则所述中间设备利用自身存储中的协商密钥进行加密；否则所述中间设备从服务器获取所述协商密钥并加密。

[0153] 步骤704、所述中间设备接收所述终端的访问，查找自身存储中是否保存了所述虚拟卡数据，如果保存则从自身存储中提取并发送所述虚拟卡数据；否则所述中间设备从所述服务器获取所述虚拟卡数据并向所述终端发送。

[0154] 所述终端完成对应的解密过程，向中间设备进行访问，请求下载虚拟卡数据。此时所述中间设备需要先查找自身是否保存了所述终端需要下载的虚拟卡数据；如果保存即直接提供下载，如果未保存，则所述中间设备需要先从所述服务器中获取所述虚拟卡数据，再提供下载。

[0155] 通过以上技术方案可知，图6-7所示实施例存在的有益效果是：通过在所述方法中结合协商加密的技术方案，确保了所述终端账号和虚拟卡数据的安全性。

[0156] 对应图4-7所示实施例，以下还将相应的公开一种终端和一种中间设备。所述终端和中间设备用以实现图4-7所示的方法。具体如下：

[0157] 参照图8所示，所述终端包括：

[0158] 通信模块801，用于与连接到服务器的中间设备建立通信连接。

[0159] 第二上报模块802，用于通过所述中间设备，向所述服务器上报终端信息，所述终端信息用于使服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据。

[0160] 第二下载模块803，用于利用所述账号访问所述中间设备访问，下载所述账号下关联的虚拟卡数据。

[0161] 第二协商模块804，用于与所述中间设备保存的服务器公钥进行加密协商，并得到协商密钥，所述协商密钥用于使所述服务器或所述中间设备利用所述协商密钥对所述账号和虚拟卡数据加密。

[0162] 第二解密模块805，用于利用所述协商密钥对所述终端的账号进行解密，利用所述协商密钥对所述账号下关联的虚拟卡数据解密。

[0163] 参照图9所示，所述中间设备包括：

[0164] 连接模块901，用于与终端建立通信连接，与服务器连接。

[0165] 上报模块902，用于接收所述终端上报的终端信息，向所述服务器发送所述终端信息，所述终端信息用于所述服务器为所述终端建立帐号，并确定与所述帐号关联的虚拟卡数据。

[0166] 交换模块903，用于接收所述终端的访问，向所述终端发送虚拟卡数据。

[0167] 所述交换模块包括：

[0168] 查询单元931，用于查找存储模块中是否保存了所述虚拟卡数据。

[0169] 存储单元932，用于存储所述虚拟卡数据并向所述终端发送。

[0170] 获取单元933，用于在存储模块中未保存所述虚拟卡数据时，从所述服务器获取所述虚拟卡数据并保存在所述存储单元。

[0171] 加密模块904，用于利用自身保存的服务器公钥与所述终端进行加密协商，并得到

协商密钥，利用所述协商密钥对所述账号和虚拟卡数据加密。

[0172] 图8-9所示实施例存在的有益效果是：通过近场通信连接所述中间设备与所述终端，使得所述中间设备间接的连接所述终端与所述服务器，从而使所述终端无需互联网而完成虚拟卡数据的下载，避免了用户在急需使用虚拟卡业务时恰巧终端未接入互联网，从而妨碍虚拟卡业务应用的特殊情况；通过在所述方法中结合协商加密的技术方案，确保了终端账号和虚拟卡数据的安全性。

[0173] 在本发明的一个实施例中，所述终端可通过与服务器的交互预置虚拟卡数据。参照图10所示，本实施例中所述终端具体如下：

[0174] 所述终端包括：处理器1001、发送器1002、接收器1003和存储器1004(图中未示)；所述处理器1001与所述发送器1002连接；所述处理器1001与所述接收器1003连接；其中，

[0175] 所述处理器1001用于，预设场景条件，所述场景条件为，所述终端与所述服务器建立通信连接；

[0176] 所述发送器1002用于，在满足预设的场景条件时，向服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据；利用所述账号访问所述服务器；

[0177] 所述接收器1003用于，在所述发送器1002利用所述帐号访问所述服务器后，下载所述账号下关联的虚拟卡数据。

[0178] 所述处理器1001还用于，与所述服务器进行加密协商并得到协商密钥，所述协商密钥用于使所述服务器利用所述协商密钥对所述账号和虚拟卡数据加密；利用所述协商密钥对所述终端的帐号进行解密；利用所述协商密钥对所述账号下关联的虚拟卡数据进行解密；

[0179] 所述发送器1002具体用于，在所述处理器1001利用所述协商密钥对所述终端的帐号进行解密后，利用所述帐号访问所述服务器；

[0180] 所述接收器1003具体用于，在所述处理器1001利用所述协商密钥对所述账号下关联的虚拟卡数据进行解密后，下载所述帐号下关联的虚拟卡数据。

[0181] 所述存储器1004用于，保存所述终端信息，所述虚拟卡数据和所述协商密钥。

[0182] 在本发明的一个实施例中，所述终端可通过中间设备间接的与服务器的交互预置虚拟卡数据。参照图11-12所示，本实施例中所述终端和中间设备具体如下：

[0183] 参见图11所示，所述终端包括：处理器1101、发送器1102、接收器1103和存储器1104(图中未示)；所述处理器1101与所述发送器1102连接；所述处理器1101与所述接收器1103连接；其中，：

[0184] 所述处理器用于，与连接到服务器的中间设备建立通信连接；

[0185] 所述发送器用于，通过所述中间设备，向所述服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据；利用所述账号访问所述服务器；

[0186] 所述接收器用于，在所述发送器利用所述帐号访问所述服务器后，下载所述账号下关联的虚拟卡数据。

[0187] 所述处理器还用于，与所述中间设备保存的服务器公钥进行加密协商，并得到协商密钥，所述协商密钥用于使所述服务器或所述中间设备利用所述协商密钥对所述账号和

虚拟卡数据加密;利用所述协商密钥对所述终端的账号进行解密;利用所述协商密钥对所述账号下关联的虚拟卡数据进行解密;

[0188] 所述发送器具体用于,在所述处理器利用所述协商密钥对所述终端的帐号进行解密后,利用所述帐号访问所述服务器;

[0189] 所述接收器具体用于,在所述处理器利用所述协商密钥对所述账号下关联的虚拟卡数据进行解密后,下载所述帐号下关联的虚拟卡数据。

[0190] 所述存储器用于,保存所述终端信息,所述虚拟卡数据和所述协商密钥。

[0191] 参见图12所示,所述中间设备包括:处理器、发送器、接收器和存储器;所述处理器与所述发送器连接;所述处理器与所述接收器连接;其中,

[0192] 所述处理器用于,与终端建立通信连接,与服务器连接;

[0193] 所述发送器用于,向所述服务器发送所述终端信息,所述终端信息用于所述服务器为所述终端建立帐号,并确定与所述帐号关联的虚拟卡数据;向所述终端发送虚拟卡数据;

[0194] 所述接收器用于,收所述终端上报的终端信息;接收所述终端的访问。

[0195] 所述处理器还用于,查找自身存储中是否保存了所述虚拟卡数据,如果保存则从自身存储中提取所述虚拟卡数据;

[0196] 所述接收器还用于,在未保存所述虚拟卡数据时,从所述服务器获取所述虚拟卡数据。

[0197] 所述处理器还用于,利用自身保存的服务器公钥与所述终端进行加密协商,并得到协商密钥,利用所述协商密钥对所述账号和虚拟卡数据加密。

[0198] 所述存储器用于,保存所述终端信息、所述服务器公钥、所述协商密钥和所述虚拟卡数据。

[0199] 在本发明的一个实施例中,所述终端可预先保持虚拟卡数据。参照图13所示,所述终端包括:

[0200] 存储器;所述存储器用于,保存预设的虚拟卡数据。

[0201] 所述终端还包括:处理器,数据传输模块;所述处理器与所述存储器连接;所述处理器与所述数据传输模块连接;其中,在所述存储器保存预设的虚拟卡数据之前,

[0202] 所述数据传输模块用于,与第一设备建立物理连接;

[0203] 所述处理器用于,在所述数据传输模块与所述第一设备建立物理连接后,经由所述数据传输模块获取预设的虚拟卡数据。

[0204] 本实施例中,所述终端可在终端本地预置虚拟卡数据。具体地,如图13所示,所述终端可包括存储器,所处存储器用于,保存预设的虚拟卡数据。本发明实施例为另一种预置虚拟卡的数据,可不需与服务器进行数据交互获取虚拟卡数据,而是直接在终端本地预置一个或多个虚拟卡数据,例如在终端出厂时便在存储器中保存一个或多个虚拟卡数据。

[0205] 进一步地,在本发明实施例的一种实现方式中,如图13所示,所述终端还包括:处理器,数据传输模块;所述处理器与所述存储器连接;所述处理器与所述数据传输模块连接;其中,在所述存储器保存预设的虚拟卡数据之前,所述数据传输模块用于,与第一设备建立物理连接;所述处理器用于,在所述数据传输模块与所述第一设备建立物理连接后,经由所述数据传输模块获取预设的虚拟卡数据。具体地,所述终端在终端出厂时可不包括虚

拟卡数据，或者仅包括固定类型的虚拟卡数据。所述终端包括数据传输模块，所述数据传输模块用于与第一设备建立物理连接，例如所述数据传输模块可以为USB接口，所述第一设备可以为笔记本电脑，在所述终端的USB接口与所述笔记本电脑通过USB数据线连接后，所述处理器通过该终端与该笔记本电脑之间的USB数据传输通道，获取笔记本电脑上保存的虚拟卡数据。所述终端经由物理连接的方式获取虚拟卡数据。

[0206] 还需要说明的是，在本发明的所有说明书附图当中，带有箭头的线段喻意为信号沿箭头方向的流动，双向箭头的线段则表示信号的双向交互；而上述线段的存在与否，并非等同于模块之间实际连接关系的存在与否；基于本发明说明书表述的需要，在终端内部模块之间的物理连接或者其他形式的连接，未在附图中具体的给出。

[0207] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到上述实施例方法中的全部或部分步骤可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者诸如媒体网关等网络通信设备，等等)执行本发明各个实施例或者实施例的某些部分所述的方法。

[0208] 需要说明的是，本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于设备及系统实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的设备及系统实施例仅仅是示意性的，其中作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0209] 以上所述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，均包含在本发明的保护范围内。

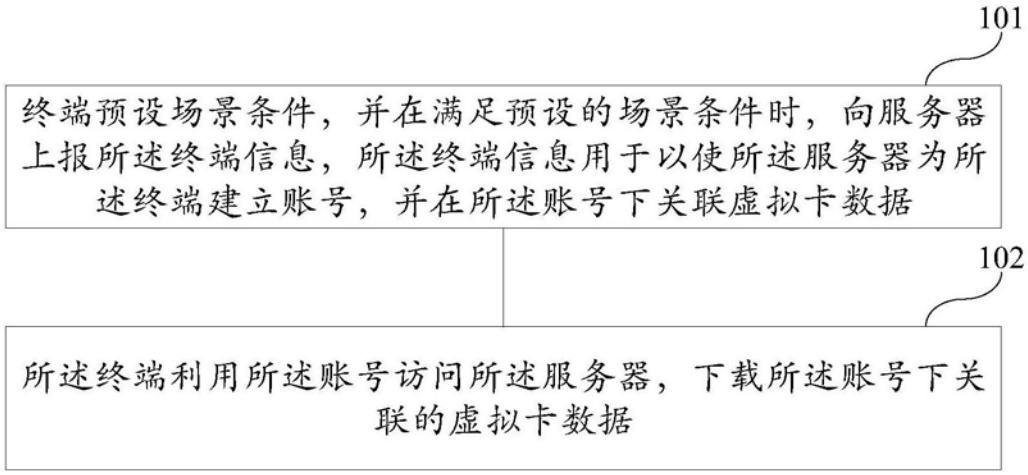

101
终端预设场景条件，并在满足预设的场景条件时，向服务器上报所述终端信息，所述终端信息用于以使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据
102
所述终端利用所述账号访问所述服务器，下载所述账号下关联的虚拟卡数据

图1

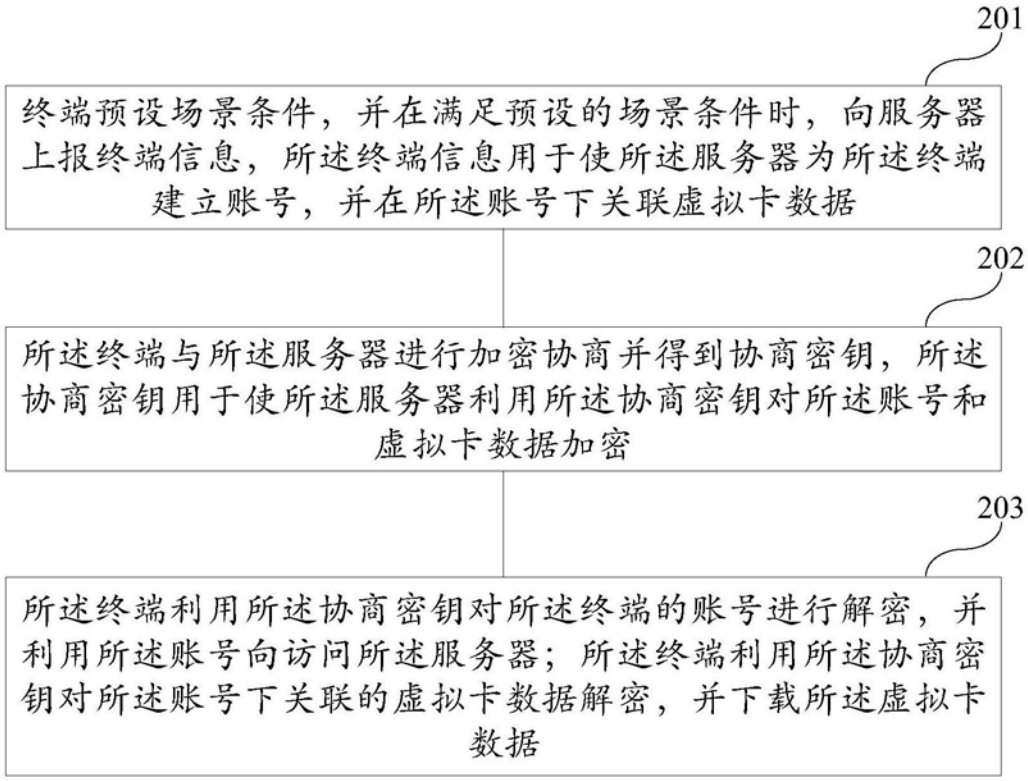

201
终端预设场景条件，并在满足预设的场景条件时，向服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据
202
所述终端与所述服务器进行加密协商并得到协商密钥，所述协商密钥用于使所述服务器利用所述协商密钥对所述账号和虚拟卡数据加密
203
所述终端利用所述协商密钥对所述终端的账号进行解密，并利用所述账号向访问所述服务器；所述终端利用所述协商密钥对所述账号下关联的虚拟卡数据解密，并下载所述虚拟卡数据

图2

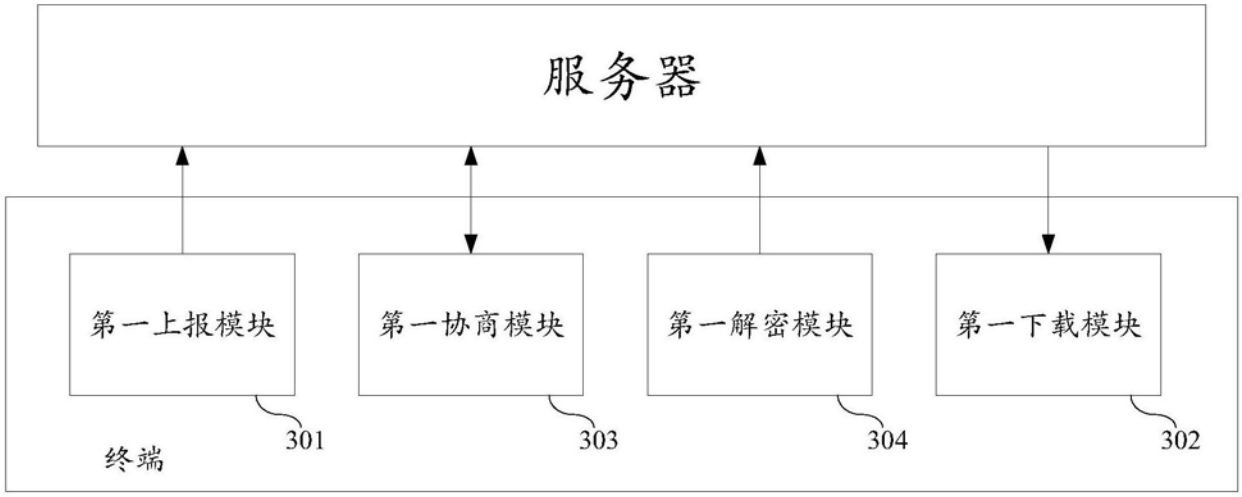

服务器
第一上报模块
第一协商模块
第一解密模块
第一下载模块
301
303
304
302
终端

图3


401
终端与连接到服务器的中间设备建立通信连接
402
所述终端通过所述中间设备，向所述服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据
403
所述终端利用所述账号访问所述中间设备，下载所述账号下关联的虚拟卡数据

图4

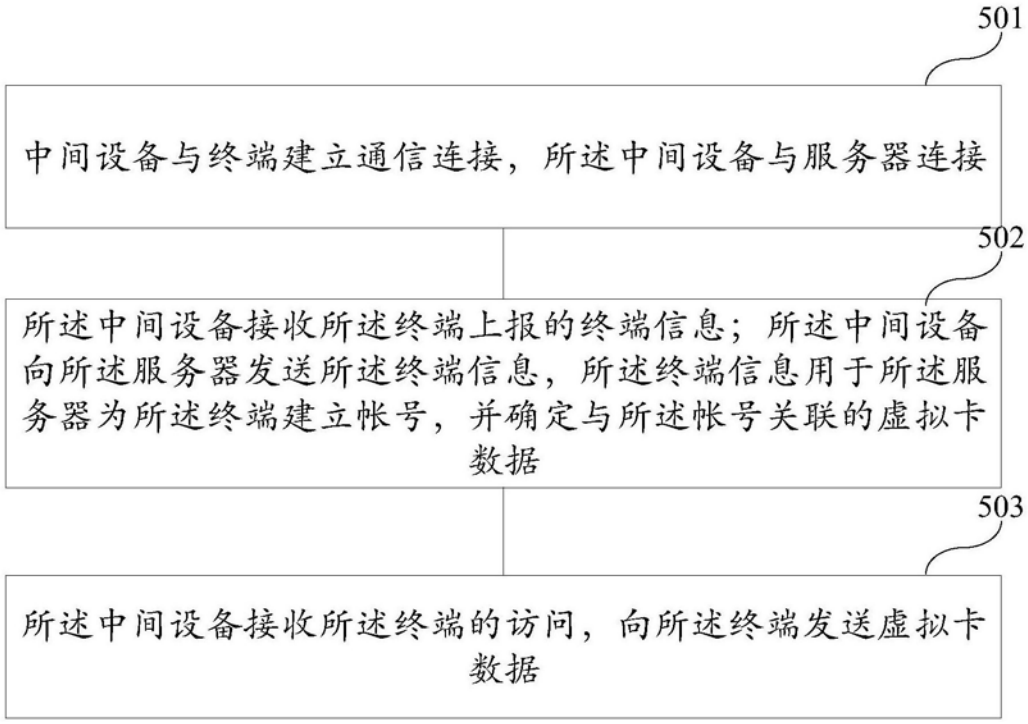

501
中间设备与终端建立通信连接，所述中间设备与服务器连接
502
所述中间设备接收所述终端上报的终端信息；所述中间设备向所述服务器发送所述终端信息，所述终端信息用于所述服务器为所述终端建立帐号，并确定与所述帐号关联的虚拟卡数据
503
所述中间设备接收所述终端的访问，向所述终端发送虚拟卡数据

图5

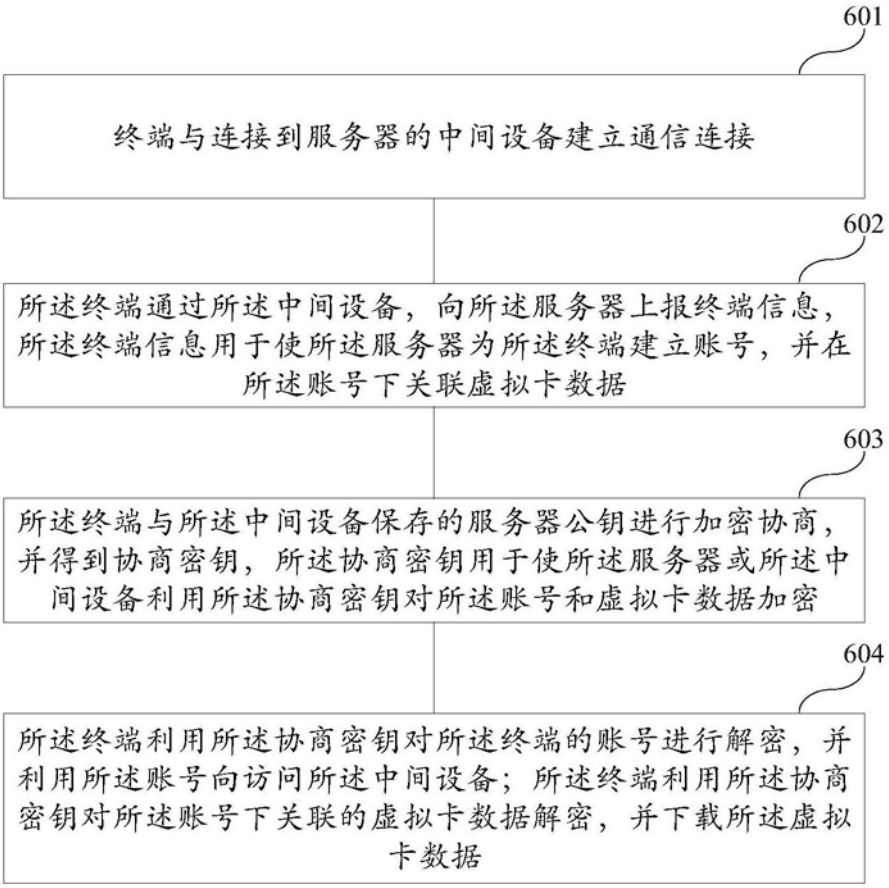

601
终端与连接到服务器的中间设备建立通信连接
602
所述终端通过所述中间设备，向所述服务器上报终端信息，所述终端信息用于使所述服务器为所述终端建立账号，并在所述账号下关联虚拟卡数据
603
所述终端与所述中间设备保存的服务器公钥进行加密协商，并得到协商密钥，所述协商密钥用于使所述服务器或所述中间设备利用所述协商密钥对所述账号和虚拟卡数据加密
604
所述终端利用所述协商密钥对所述终端的账号进行解密，并利用所述账号向访问所述中间设备；所述终端利用所述协商密钥对所述账号下关联的虚拟卡数据解密，并下载所述虚拟卡数据

图6

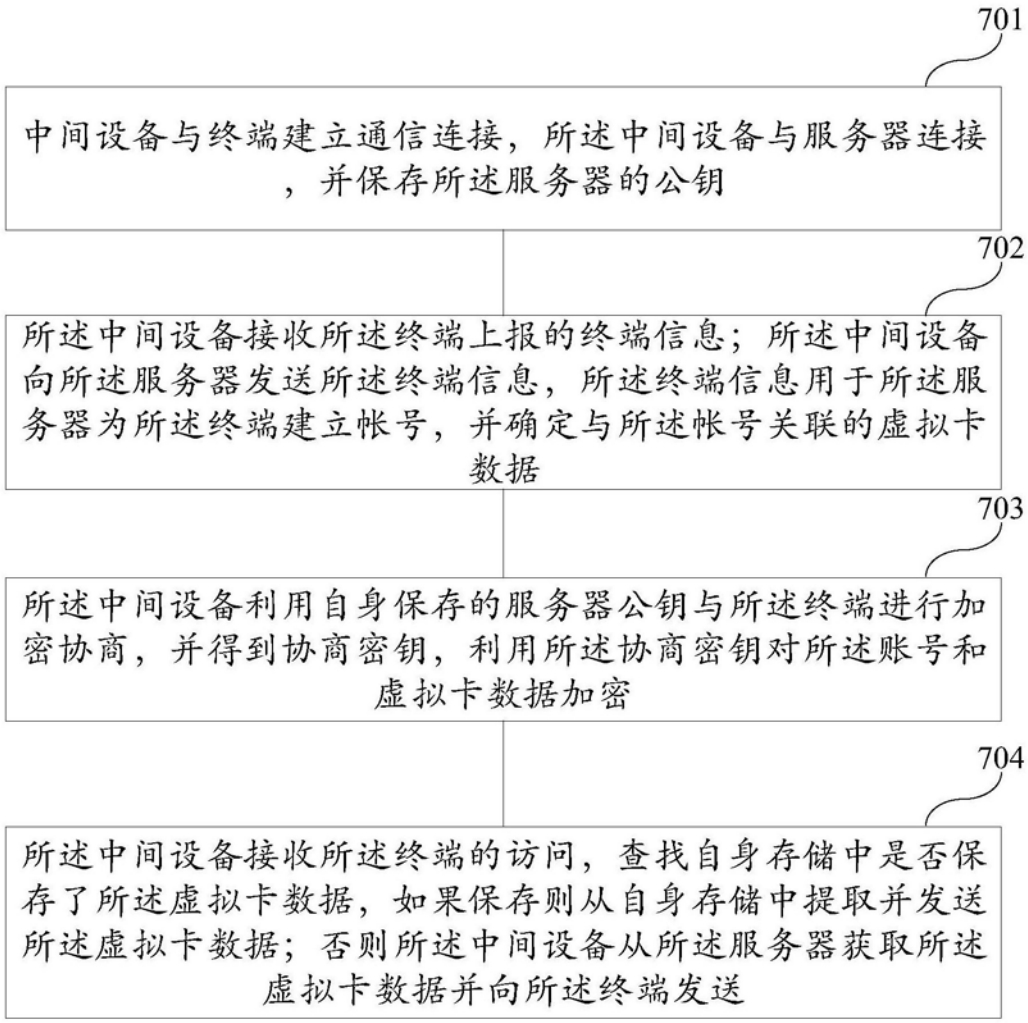

701
中间设备与终端建立通信连接，所述中间设备与服务器连接，并保存所述服务器的公钥
702
所述中间设备接收所述终端上报的终端信息；所述中间设备向所述服务器发送所述终端信息，所述终端信息用于所述服务器为所述终端建立帐号，并确定与所述帐号关联的虚拟卡数据
703
所述中间设备利用自身保存的服务器公钥与所述终端进行加密协商，并得到协商密钥，利用所述协商密钥对所述账号和虚拟卡数据加密
704
所述中间设备接收所述终端的访问，查找自身存储中是否保存了所述虚拟卡数据，如果保存则从自身存储中提取并发送所述虚拟卡数据；否则所述中间设备从所述服务器获取所述虚拟卡数据并向所述终端发送

图7

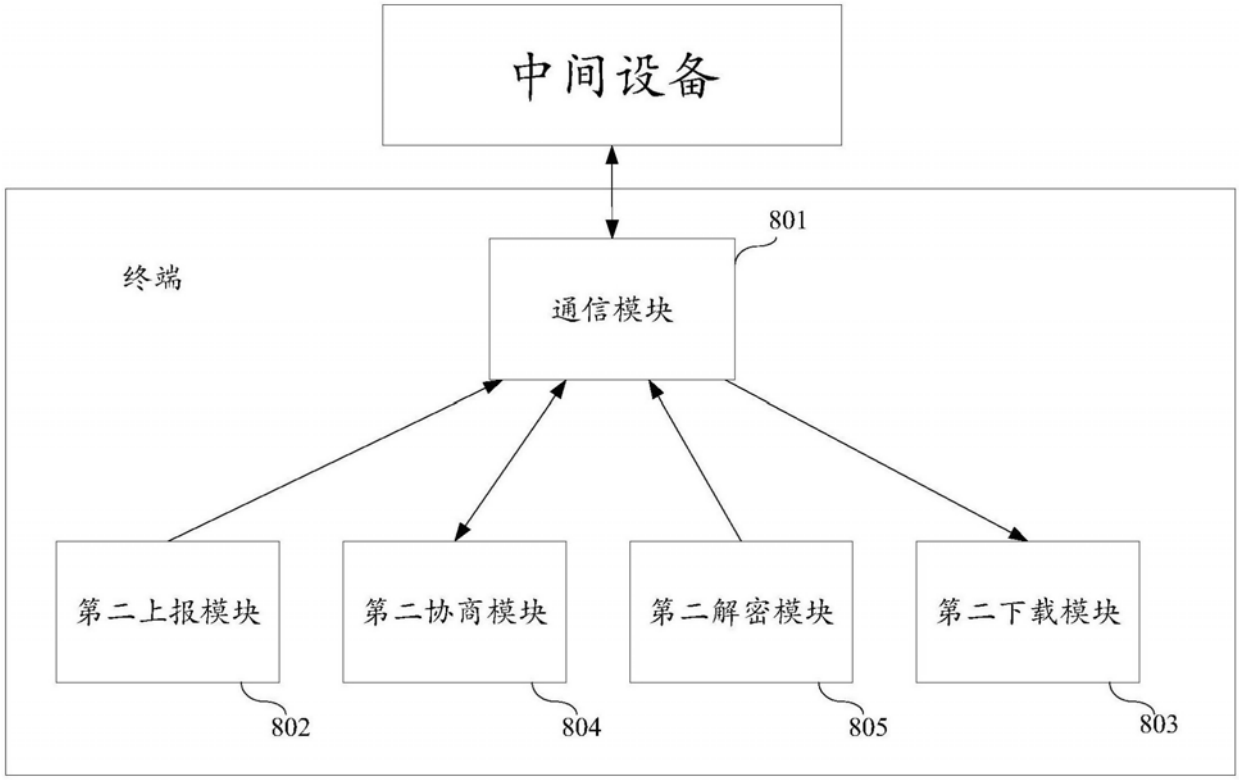


图8

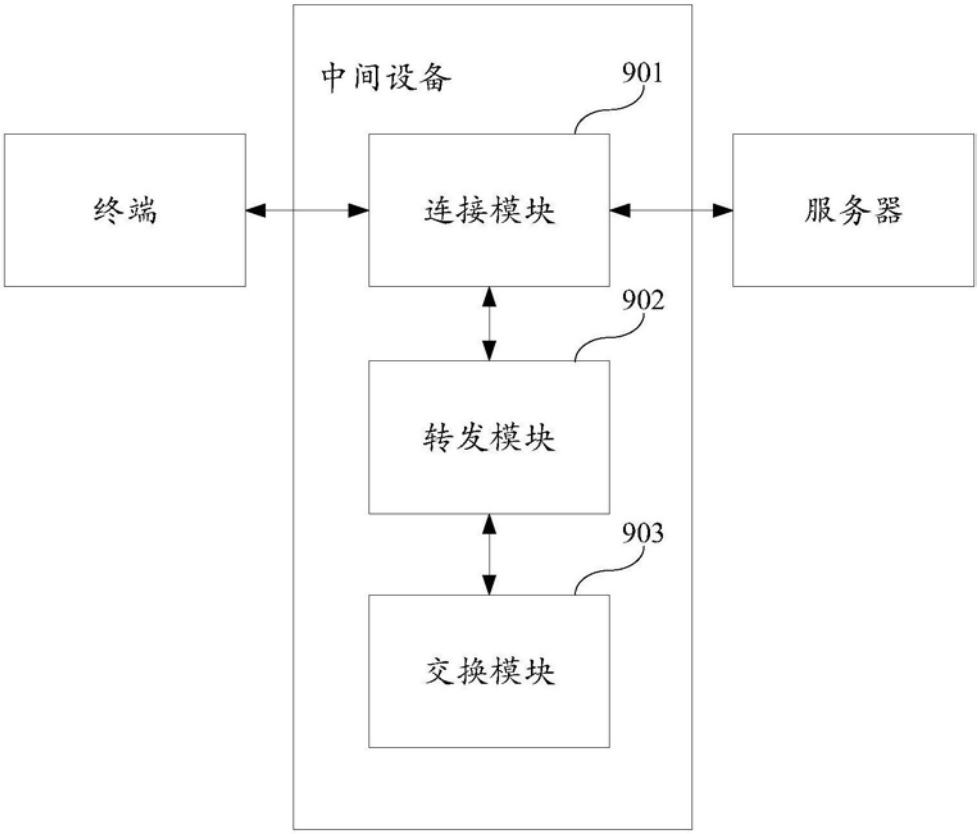


图9

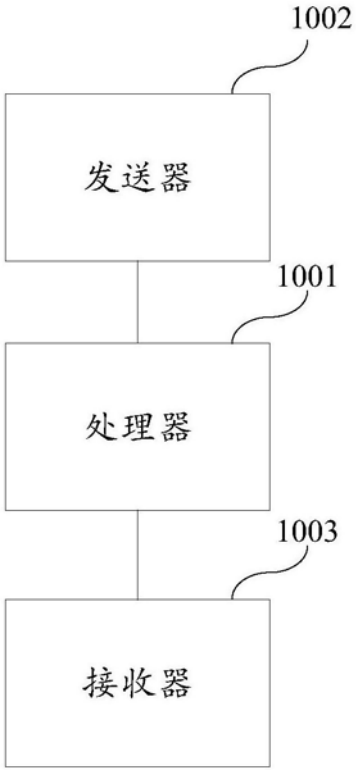


图10

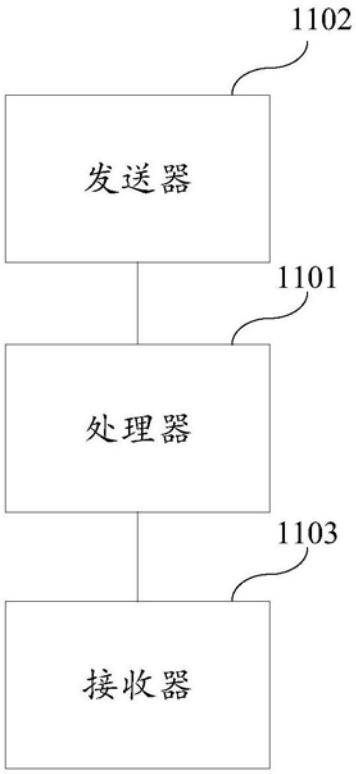


图11

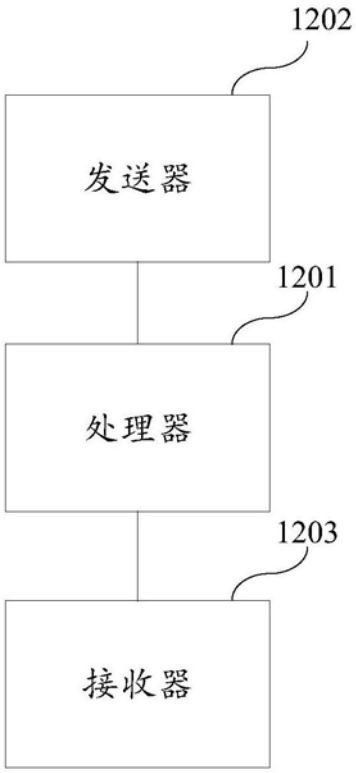


图12

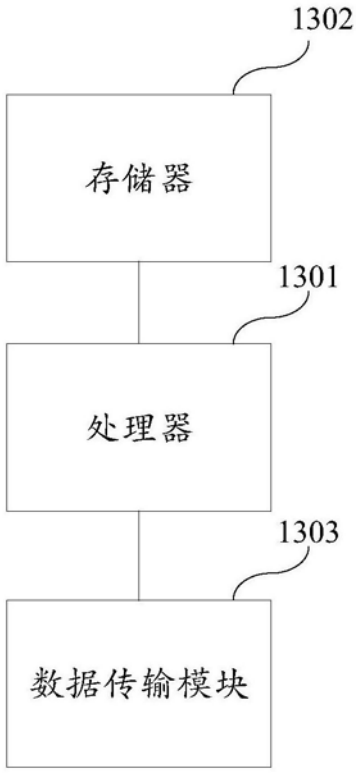


图13