(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 107181714 B
(45)授权公告日 2021.01.26

(21)申请号 201610133425.9
(22)申请日 2016.03.09
(65)同一申请的已公布的文献号
申请公布号 CN 107181714 A
(43)申请公布日 2017.09.19
(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心
(72)发明人 孙元博
(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥
(51)Int.Cl.
H04L 29/06(2006.01)
G06Q 20/40(2012.01)
G06Q 20/32(2012.01)

(56)对比文件
CN 103714452 A,2014.04.09
CN 104579671 A,2015.04.29
CN 104751334 A,2015.07.01

审查员 丁彬

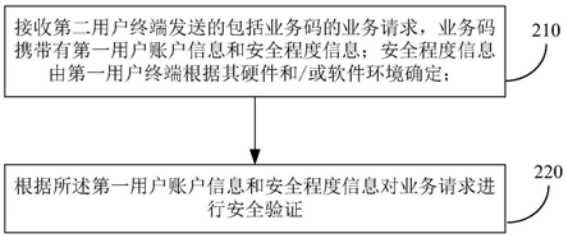
权利要求书5页 说明书10页 附图4页

(54)发明名称

基于业务码的验证方法和装置、业务码的生成方法和装置

(57)摘要

本申请提供一种基于业务码的验证方法，应用在服务器上，包括：接收第二用户终端发送的包括业务码的业务请求，所述业务码携带有第一用户账户信息和安全程度信息；所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定；根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证。通过本申请的技术方案，能够针对用户终端本身具有的安全性来采用对应的验证标准，既能为安全性较差的终端用户提供更多保障，又能为安全性较强的终端用户提供更多便利。



CN 107181714 B

1.一种基于业务码的验证方法,应用在服务器上,其特征在于,包括:

接收第二用户终端发送的包括业务码的业务请求,所述业务码携带有第一用户账户信息和安全程度信息;所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定;其中,第一用户终端根据其硬件和/或软件环境对应的分值确定安全程度信息;或者,根据生成业务码的客户端软件所采用的安全硬件设施和/或操作系统的安全策略确定安全程度信息;或者,按照保存用户端密钥的硬件和/或软件的安全措施确定安全程度信息;

根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证;其中,所述安全程度信息包括:安全级别;所述业务请求中包括:业务额度;

所述根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证,包括:根据所述安全级别确定所允许的业务额度,当所述业务请求中的业务额度超过所允许的业务额度时,不能通过安全验证。

2.根据权利要求1所述的方法,其特征在于,所述业务码中还携带有第一用户终端在生成所述业务码时的位置信息;所述业务请求中还包括:第二用户终端在发送所述业务请求时的位置信息;

所述方法还包括:当第一用户终端的位置信息与第二用户终端的位置信息之间的距离超过距离阈值时,所述业务请求不能通过安全验证;和/或

当第一用户终端的位置信息超出第一用户账户的可信地理区域时,所述业务请求不能通过安全验证。

3.根据权利要求1所述的方法,其特征在于,所述业务码中还携带有第一用户终端的设备标识;所述业务请求中还包括:第二用户终端的设备标识;

所述方法还包括:获取第一用户账户和第二用户账户的绑定终端的设备标识,如果第一用户账户绑定终端的设备标识不同于业务码中第一用户终端的设备标识、或第二用户账户绑定终端的设备标识不同于业务请求中第二用户终端的设备标识,所述业务请求不能通过安全验证。

4.根据权利要求1至3任意一项所述的方法,其特征在于,所述业务码中携带的安全程度信息采用第一用户终端生成的随机密钥进行加密,所述业务码还携带有以第一用户账户的用户端密钥进行加密后的随机密钥密文;

所述方法还包括:采用与第一用户账户的用户端密钥相同或相对应的服务端密钥对业务码中的随机密钥密文进行解密,采用解密得到的随机密钥对业务码中的安全程度信息进行解密。

5.一种基于业务码的验证方法,应用在第二用户终端上,其特征在于,包括:

从第一用户终端获取业务码,所述业务码携带第一用户账户信息和安全程度信息;所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定;其中,第一用户终端根据其硬件和/或软件环境对应的分值确定安全程度信息;或者,根据生成业务码的客户端软件所采用的安全硬件设施和/或操作系统的安全策略确定安全程度信息;或者,按照保存用户端密钥的硬件和/或软件的安全措施确定安全程度信息;

将包括所述业务码的业务请求发送给服务器,供服务器根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证;其中,所述安全程度信息包括:安全级别;所述业务请求中包括:业务额度;所述服务器根据所述安全级别确定所允许的业务额度,当所述业

务请求中的业务额度超过所允许的业务额度时，不能通过安全验证。

6.根据权利要求5所述的方法，其特征在于，所述业务码中还携带有第一用户终端在生成所述业务码时的位置信息；

所述业务请求中还包括：第二用户终端在生成所述业务请求时的位置信息，供服务器根据所述第二用户终端的位置信息和业务码中第一用户终端的位置信息对业务请求进行安全验证。

7.根据权利要求5所述的方法，其特征在于，所述业务请求中还包括：第二用户终端的设备标识，供服务器根据所述第二用户终端的设备标识对业务请求进行安全验证。

8.一种生成业务码的方法，应用在第一用户终端上，其特征在于，包括：

根据本第一用户终端的硬件和/或软件环境确定安全程度信息；其中，第一用户终端根据其硬件和/或软件环境对应的分值确定安全程度信息；或者，根据生成业务码的客户端软件所采用的安全硬件设施和/或操作系统的安全策略确定安全程度信息；或者，按照保存用户端密钥的硬件和/或软件的安全措施确定安全程度信息；

采用第一用户账户信息和安全程度信息，按照预定格式生成业务码；向第二用户终端提供所述业务码，供其在业务请求中将业务码上传到服务器后，由服务器根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证；其中，所述安全程度信息包括：安全级别；所述业务请求中包括：业务额度；所述服务器根据所述安全级别确定所允许的业务额度，当所述业务请求中的业务额度超过所允许的业务额度时，不能通过安全验证。

9.根据权利要求8所述的方法，其特征在于，所述业务码中至少一个组成部分采用第一用户账户的用户端密钥加密；所述用户端密钥与服务器可获得的第一用户账户的服务端密钥相同或相对应。

10.根据权利要求9所述的方法，其特征在于，所述采用第一用户账户信息和安全程度信息，按照预定格式生成业务码，包括：根据预定算法生成随机密钥，采用以随机密钥对安全程度信息进行加密后的密文、以第一用户账户的用户端密钥对随机密钥进行加密后的密文，按照预定格式生成业务码。

11.根据权利要求8所述的方法，其特征在于，所述采用第一用户账户信息和安全程度信息，按照预定格式生成业务码，包括：采用第一用户账户信息、安全程度信息和本第一用户终端在生成业务码时的位置信息，按照预定格式生成业务码。

12.根据权利要求8所述的方法，其特征在于，所述采用第一用户账户信息和安全程度信息，按照预定格式生成业务码，包括：采用第一用户账户信息、安全程度信息和本第一用户终端的设备标识，按照预定格式生成业务码。

13.根据权利要求8所述的方法，其特征在于，所述预定格式包括：2位的业务标识、10字节的第一用户账户信息、20字节的第一用户终端的设备信息和6位的验证凭证，其中：业务标识用来表示所述业务码用于哪种业务类型；第一用户终端的设备信息包括：2字节的版本号、2字节的本第一用户终端上安全硬件的厂商标识、2字节的本第一用户终端上安全传感器的厂商标识、2字节的本第一用户终端上安全识别算法的厂商标识、2字节的本第一用户终端的厂商标识、4字节的由所述终端厂商提供的本第一用户终端的唯一标识、2字节的安全程度信息和4字节的本第一用户终端在生成业务码时的位置信息；验证凭证为将第一用户账户信息和第一用户终端的设备信息输入预定摘要算法后得到的摘要信息；

所述按照预定格式生成业务码，包括：按照所述预定格式组装出业务码的基础数据后，根据预定算法生成随机密钥，采用以随机密钥对至少部分所述基础数据进行加密，再以第一用户账户的用户端密钥对随机密钥进行加密后，将至少部分加密的基础数据和随机密钥的密文组合成业务码。

14.根据权利要求8所述的方法，其特征在于，所述业务码包括：二维码、条形码、或近场通信NFC码。

15.一种基于业务码的验证装置，应用在服务器上，其特征在于，包括：

业务请求接收单元，用于接收第二用户终端发送的包括业务码的业务请求，所述业务码携带有第一用户账户信息和安全程度信息；所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定；其中，第一用户终端根据其硬件和/或软件环境对应的分值确定安全程度信息；或者，根据生成业务码的客户端软件所采用的安全硬件设施和/或操作系统的安全策略确定安全程度信息；或者，按照保存用户端密钥的硬件和/或软件的安全措施确定安全程度信息；

安全程度验证单元，用于根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证；其中，所述安全程度信息包括：安全级别；所述业务请求中包括：业务额度；

所述安全程度验证单元具体用于：根据所述安全级别确定所允许的业务额度，当所述业务请求中的业务额度超过所允许的业务额度时，不能通过安全验证。

16.根据权利要求15所述的装置，其特征在于，所述业务码中还携带有第一用户终端在生成所述业务码时的位置信息；所述业务请求中还包括：第二用户终端在发送所述业务请求时的位置信息；

所述装置还包括：位置信息验证单元，用于当第一用户终端的位置信息与第二用户终端的位置信息之间的距离超过距离阈值时，所述业务请求不能通过安全验证；和/或

当第一用户终端的位置信息超出第一用户账户的可信地理区域时，所述业务请求不能通过安全验证。

17.根据权利要求15所述的装置，其特征在于，所述业务码中还携带有第一用户终端的设备标识；所述业务请求中还包括：第二用户终端的设备标识；

所述装置还包括：设备标识验证单元，用于获取第一用户账户和第二用户账户的绑定终端的设备标识，如果第一用户账户绑定终端的设备标识不同于业务码中第一用户终端的设备标识、或第二用户账户绑定终端的设备标识不同于业务请求中第二用户终端的设备标识，所述业务请求不能通过安全验证。

18.根据权利要求15至17任意一项所述的装置，其特征在于，所述业务码中携带的安全程度信息采用第一用户终端生成的随机密钥进行加密，所述业务码还携带有以第一用户账户的用户端密钥进行加密后的随机密钥密文；

所述装置还包括：随机密钥解密单元，用于采用与第一用户账户的用户端密钥相同或相对应的服务端密钥对业务码中的随机密钥密文进行解密，采用解密得到的随机密钥对业务码中的安全程度信息进行解密。

19.一种基于业务码的验证装置，应用在第二用户终端上，其特征在于，包括：

业务码获取单元，用于从第一用户终端获取业务码，所述业务码携带第一用户账户信息和安全程度信息；所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定；其

中，第一用户终端根据其硬件和/或软件环境对应的分值确定安全程度信息；或者，根据生成业务码的客户端软件所采用的安全硬件设施和/或操作系统的安全策略确定安全程度信息；或者，按照保存用户端密钥的硬件和/或软件的安全措施确定安全程度信息；

业务请求发送单元，用于将包括所述业务码的业务请求发送给服务器，供服务器根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证；其中，所述安全程度信息包括：安全级别；所述业务请求中包括：业务额度；所述服务器根据所述安全级别确定所允许的业务额度，当所述业务请求中的业务额度超过所允许的业务额度时，不能通过安全验证。

20.根据权利要求19所述的装置，其特征在于，所述业务码中还携带有第一用户终端在生成所述业务码时的位置信息；

所述业务请求中还包括：第二用户终端在生成所述业务请求时的位置信息，供服务器根据所述第二用户终端的位置信息和业务码中第一用户终端的位置信息对业务请求进行安全验证。

21.根据权利要求19所述的装置，其特征在于，所述业务请求中还包括：第二用户终端的设备标识，供服务器根据所述第二用户终端的设备标识对业务请求进行安全验证。

22.一种生成业务码的装置，应用在第一用户终端上，其特征在于，包括：

安全程度确定单元，用于根据本第一用户终端的硬件和/或软件环境确定安全程度信息；其中，第一用户终端根据其硬件和/或软件环境对应的分值确定安全程度信息；或者，根据生成业务码的客户端软件所采用的安全硬件设施和/或操作系统的安全策略确定安全程度信息；或者，按照保存用户端密钥的硬件和/或软件的安全措施确定安全程度信息；

业务码生成单元，用于采用第一用户账户信息和安全程度信息，按照预定格式生成业务码；

业务码提供单元，用于向第二用户终端提供所述业务码，供其在业务请求中将业务码上传到服务器后，由服务器根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证；其中，所述安全程度信息包括：安全级别；所述业务请求中包括：业务额度；所述服务器根据所述安全级别确定所允许的业务额度，当所述业务请求中的业务额度超过所允许的业务额度时，不能通过安全验证。

23.根据权利要求22所述的装置，其特征在于，所述业务码中至少一个组成部分采用第一用户账户的用户端密钥加密；所述用户端密钥与服务器可获得的第一用户账户的服务端密钥相同或相对应。

24.根据权利要求22所述的装置，其特征在于，所述业务码生成单元具体用于：根据预定算法生成随机密钥，采用以随机密钥对安全程度信息进行加密后的密文、以第一用户账户的用户端密钥对随机密钥进行加密后的密文，按照预定格式生成业务码。

25.根据权利要求22所述的装置，其特征在于，所述业务码生成单元具体用于：采用第一用户账户信息、安全程度信息和本第一用户终端在生成业务码时的位置信息，按照预定格式生成业务码。

26.根据权利要求22所述的装置，其特征在于，所述业务码生成单元具体用于：采用第一用户账户信息、安全程度信息和本第一用户终端的设备标识，按照预定格式生成业务码。

27.根据权利要求22所述的装置，其特征在于，所述预定格式包括：2位的业务标识、10

字节的第一用户账户信息、20字节的第一用户终端的设备信息和6位的验证凭证，其中：业务标识用来表示所述业务码用于哪种业务类型；第一用户终端的设备信息包括：2字节的版本号、2字节的本第一用户终端上安全硬件的厂商标识、2字节的本第一用户终端上安全传感器的厂商标识、2字节的本第一用户终端上安全识别算法的厂商标识、2字节的本第一用户终端的厂商标识、4字节的由所述终端厂商提供的本第一用户终端的唯一标识、2字节的安全程度信息和4字节的本第一用户终端在生成业务码时的位置信息；验证凭证为将第一用户账户信息和第一用户终端的设备信息输入预定摘要算法后得到的摘要信息；

所述业务码生成单元按照预定格式生成业务码，包括：按照所述预定格式组装出业务码的基础数据后，根据预定算法生成随机密钥，采用以随机密钥对至少部分所述基础数据进行加密，再以第一用户账户的用户端密钥对随机密钥进行加密后，将至少部分加密的基础数据和随机密钥的密文组合成业务码。

28.根据权利要求22所述的装置，其特征在于，所述业务码包括：二维码、条形码、或近场通信NFC码。

基于业务码的验证方法和装置、业务码的生成方法和装置

技术领域

[0001] 本申请涉及网络通信技术领域，尤其涉及一种基于业务码的验证方法和装置、一种业务码的生成方法和装置。

背景技术

[0002] 随着移动互联技术的发展和智能终端的普及，以用户账户为基础的各种近距离业务得到了广阔的发展空间。两个用户可以通过扫描二维码、条形码等实现其账户间的移动支付、账户间的信息共享等业务。

[0003] 近距离业务在为人们带来方便的同时，也具有一定的安全隐患。如果用户的终端遗失，或者二维码等被他人录屏，则可能造成用户的损失，尤其是对移动支付业务而言。因此，一些用户采用带有更多安全硬件设施的终端、或者在终端上安装更为可靠的安全软件，这些用户账户具有更好的安全性。

[0004] 现有技术中，提供近距离业务服务的系统中，在收到带有二维码的业务请求后，服务器采用相同的方式对所有用户账户的业务请求进行验证，而不论与该用户账户绑定的终端是否有更好的安全性。这样，如果采用较为宽松的验证标准，对安全性较差的终端可能造成较大的风险；而采用较为严格的验证标准，又会造成安全性较好的终端用户的诸多不便。

发明内容

[0005] 有鉴于此，本申请提供一种基于业务码的验证方法，应用在服务器上，包括：

[0006] 接收第二用户终端发送的包括业务码的业务请求，所述业务码携带有第一用户账户信息和安全程度信息；所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定；

[0007] 根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证。

[0008] 本申请提供的一种基于业务码的验证方法，应用在第二用户的终端上，包括：

[0009] 从第一用户的终端获取业务码，所述业务码携带第一用户账户信息和安全程度信息；所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定；

[0010] 将包括所述业务码的业务请求发送给服务器，供服务器根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证。

[0011] 本申请提供的一种生成业务码的方法，应用在第一用户的终端上，包括：

[0012] 根据本终端的硬件和/或软件环境确定安全程度信息；

[0013] 采用第一用户账户信息和安全程度信息，按照预定格式生成业务码。

[0014] 本申请还提供了一种基于业务码的验证装置，应用在服务器上，包括：

[0015] 业务请求接收单元，用于接收第二用户终端发送的包括业务码的业务请求，所述业务码携带有第一用户账户信息和安全程度信息；所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定；

[0016] 安全程度验证单元，用于根据所述第一用户账户信息和安全程度信息对业务请求

进行安全验证。

[0017] 本申请提供的一种基于业务码的验证装置，应用在第二用户的终端上，包括：

[0018] 业务码获取单元，用于从第一用户的终端获取业务码，所述业务码携带第一用户账户信息和安全程度信息；所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定；

[0019] 业务请求发送单元，用于将包括所述业务码的业务请求发送给服务器，供服务器根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证。

[0020] 本申请提供的一种生成业务码的装置，应用在第一用户的终端上，包括：

[0021] 安全程度确定单元，用于根据本终端的硬件和/或软件环境确定安全程度信息；

[0022] 业务码生成单元，用于采用第一用户账户信息和安全程度信息，按照预定格式生成业务码。

[0023] 由以上技术方案可见，本申请的实施例中，第一用户终端在生成的业务码中携带由本终端的硬件和/或软件环境决定的安全程度信息，在第二用户终端将第一用户终端生成的业务码在业务请求中上传给服务器后，服务器根据安全程度信息来对业务请求进行验证，从而能够针对用户终端本身具有的安全性来采用对应的验证标准，既能为安全性较差的终端用户提供更多保障，又能为安全性较强的终端用户提供更多便利。

附图说明

[0024] 图1是本申请实施例应用场景的一种网络结构图；

[0025] 图2是本申请实施例中一种应用在服务器上，基于业务码的验证方法的流程图；

[0026] 图3是本申请实施例中一种应用在第二用户的终端上，基于业务码的验证方法的流程图；

[0027] 图4是本申请实施例中一种应用在第一用户的终端上，生成业务码的方法的流程图；

[0028] 图5是本申请应用示例中一种终端与服务器之间的交互流程图；

[0029] 图6是终端或服务器的一种硬件结构图；

[0030] 图7是本申请实施例中一种应用在服务器上，基于业务码的验证装置的逻辑结构图；

[0031] 图8是本申请实施例中一种应用在第二用户的终端上，基于业务码的验证装置的逻辑结构图；

[0032] 图9是本申请实施例中一种应用在第一用户的终端上，生成业务码的装置的逻辑结构图。

具体实施方式

[0033] 本申请的实施例提出一种新的业务码的生成方法，和一种新的基于业务码的验证方法，终端在生成业务码时，在业务码中携带根据硬件和/或软件环境确定的安全程度信息，服务器可以基于终端的安全程度信息来对带有该业务码的业务请求适用不同的验证标准，以解决现有技术中存在的问题。

[0034] 本申请实施例应用场景的一种网络结构如图1所示，第二用户的终端与提供业务

服务的业务系统的服务器通过网络相互可访问，第一用户的终端可以向第二用户的终端提供业务码，第二用户的终端能够以相应的手段获得第一用户的终端提供的业务码。其中，第一用户或第二用户的终端可以是任何具有计算、存储和通信能力的设备，例如可穿戴设备、手机、平板电脑、PC (Personal Computer，个人电脑)、笔记本等；业务码包括条码(如二维码、条形码)、声波码、NFC(Near Field Communication，近场通信)码等，相应的获取业务码的手段包括扫描、接收声波、感应等；服务器可以是一个物理或逻辑服务器，也可以是由两个或两个以上分担不同职责的物理或逻辑服务器、相互协同来实现本申请实施例中服务器的各项功能。本申请实施例对终端、服务器的种类，以及第二用户的终端与服务器之间通信网络的类型、协议等均不做限定。另外，在一些应用场景中，第一用户的终端也可以通过通信网络与服务器相互访问。

[0035] 本申请实施例中，基于业务码的验证方法在服务器上的流程如图2所示，在第二用户的终端上的流程如图3所示；生成验证码的方法在第一用户的终端上的流程如图4所示。其中，第一用户和第二用户在业务系统的服务器上注册有各自的用户账户。

[0036] 在第一用户的终端上，步骤410，根据本终端的硬件和/或软件环境确定安全程度信息。

[0037] 第一用户的终端在收到用户生成业务码的指令后，提取本终端的硬件信息和/或软件信息，按照预置的算法确定安全程度信息。可以根据实际应用场景的需要，来选择用于确定安全程度信息的终端硬件和/或软件信息、以及产生安全程度信息的具体算法，本申请的实施例不做限定。以下举例说明。

[0038] 第一个例子中，可以为终端可能具备的各种安全硬件设施，和/或安全软件预置对应的分值，如果用户在指令生成业务码的过程中将会受益于某个安全硬件设施或安全软件，则将这些硬件设施或软件对应的分值进行加总，以其总和作为安全程度信息。例如，用户需要以指纹解锁终端，则加4分；用户在生成业务码时需要验证虹膜，则加6分；终端安装有安全软件，加3分，等等。此外，完成相同功能的不同的安全硬件设施、和/或安全软件可以对应于不同的分值。

[0039] 第二个例子中，可以根据生成业务码的客户端软件所采用的终端安全硬件设施、和/或所采用的操作系统的安全策略来确定安全程度信息，具体的方式可以参照第一个例子，不再赘述。

[0040] 第三个例子中，第一用户在业务系统中将其终端与其账户进行绑定时，由服务器或第一用户终端生成第一用户账户的用户端密钥和服务端密钥(这两个密钥相同或相对应)，用户端密钥保存在终端上，服务端密钥保存在服务器可以获取的某个网络位置。在生成业务码时，终端采用本地保存的用户端密钥对业务码中至少一个组成部分进行加密。这样，用户端密钥的存储安全性将对业务安全性具有重要的影响，可以按照本终端保存用户端密钥的硬件和/或软件的安全措施来确定安全程度信息。例如，可以将几个安全级别来作为安全程度信息，当本终端保存用户端密钥的位置采取了某项硬件安全措施时，对应于第一安全级别；当本终端保存用户端密钥的位置为操作系统实施某项软件安全策略的存储位置时，对应于第二安全级别；当本终端保存用户端密钥的位置未采取安全措施时，对应于第三安全级别；等等。

[0041] 在第一用户的终端上，步骤420，采用第一用户账户信息和安全程度信息，按照预

定格式生成业务码。

[0042] 用户账户信息包括至少一种可以由服务器唯一确定所对应的用户账户的信息，例如用户在业务系统注册的邮箱、用户名、手机号码、昵称、业务系统为用户分配的用户唯一编码等；此外还可以包括该用户账户的其他信息，如用户类型等等。

[0043] 除第一用户账户信息和安全程度信息外，还可以采用其他的信息来生成业务码，例如本终端的设备标识、当前本终端的位置信息、终端上安全传感器的标识中的一种到多种。

[0044] 可以采用将上述各种信息加密后的密文来生成业务码。可以按照实际应用场景的需求来选择加密的信息、加密方式和所采用的密钥，本申请的实施例不做限定。在一个例子中，终端上保存有第一用户账户的用户端密钥，在确定安全程度信息后，终端按照预定算法生成随机密钥，采用以随机密钥对安全程度信息(或安全程度信息和其他业务码携带的信息)进行加密后的密文、和以第一用户账户的用户端密钥对随机密钥进行加密后的密文，按照预定格式生成业务码。这样，业务码被上传到服务器后，服务器可以根据第一用户账户信息获取与其用户端密钥相同或相对应的服务端密钥，采用服务端密钥对业务码中的随机密钥密文进行解密，得到随机密钥后，用该随机密钥对业务码中的安全程度信息进行解密。

[0045] 业务码的预定格式可以根据业务码的种类、业务类型和实际需求确定。例如，一种业务码的格式可以如表1所示：

[0046]

Tag	UID	DeviceID	VerifyToken

[0047] 表1

[0048] 表1中，Tag为2位(bit)的业务标识，用来表示业务码用于哪种类型的业务；UID为10字节(byte)的用户账户信息；DeviceID为20字节的终端设备信息；VerifyToken为6位的验证凭证，是将UID和DeviceID输入预定摘要算法后得到的摘要信息，预定摘要算法可以是HOTP(HMAC-based One-time Password Algorithm，基于密钥相关的哈希运算消息认证码HMAC 的一次性口令算法)、TOTP(Time-based One-time Password Algorithm，基于时间的一次性密码算法)等等。

[0049] 20字节DeviceID的格式如表2所示：

[0050]

Version	安全厂商	Sensor厂商	算法厂商	终端厂商	HDID	SecLevel	LBS

[0051] 表2

[0052] 表2中，Version为2字节的版本号，用来表示DeviceID的格式版本；安全厂商为2字节的本终端上安全硬件的厂商标识；Sensor厂商为2字节的本终端上安全传感器的厂商标识；算法厂商为2字节的本终端上安全识别算法的厂商标识，安全识别算法用来对传感器的输出进行识别和判定(如识别指纹传感器输出的是否是终端用户的指纹、虹膜传感器输出的是否与预存的虹膜图像相匹配等)；终端厂商为2字节的本终端的厂商标识；HDID为4 字节的由终端厂商提供的本终端的唯一标识，在同一个厂商出产的所有终端中唯一对应于本终端；SecLevel为2字节的安全程度信息；LBS为4字节的当前本终端的位置信息，用来表示在生成本业务码时，本终端所在的位置。

[0053] 在按照上述格式生成业务码时，终端可以先获取表1和表2中每个字段的值，按照

表1和表2的格式将这些字段值组合后得到业务码的基础数据;再采用按照预定算法生成的随机密钥,对至少部分基础数据以随机密钥进行加密(例如可以对DeviceID和VerifyToken加密、或对Tag、UID、DeviceID 和VerifyToken加密、或对HDID、SecLevel和LBS加密等等);然后以第一用户账户的用户端密钥对随机密钥进行加密;将至少部分内容加密后的基础数据、随机密钥密文组合成业务码。

[0054] 在第一用户的终端生成业务码后,采用与业务码的种类相匹配的方式,向第二用户的终端提供该业务码,例如显示二维码或条形码供第二用户的终端扫描,发送声波码、与第二用户的终端进行近场感应以传递NFC码,以便第二用户的终端能够在发送给服务器的业务请求中将业务码上传给服务器,从而可以由服务器根据第一用户账户信息和安全程度信息对业务请求进行安全验证。

[0055] 在第二用户的终端上,步骤310,从第一用户终端获取业务码。

[0056] 第二用户的终端所获取的业务码中携带有第一用户账户信息和安全程度信息,其中安全程度信息由第一用户终端根据其硬件和/或软件环境确定。

[0057] 在第二用户的终端上,步骤320,将包括该业务码的业务请求发送给服务器,供服务器根据业务码携带的第一用户账户信息和安全程度信息对业务请求进行安全验证。

[0058] 在服务器上,步骤210,接收第二用户终端发送的包括业务码的业务请求。

[0059] 第二用户的终端在从第一用户的终端获得业务码后,采用业务码和第二用户账户信息业务请求生成业务请求,发送给服务器。

[0060] 第二用户的终端可以将本终端的设备标识封装在业务请求中发送给服务器,以便服务器根据设备标识来对业务请求进行安全认证。设备标识可以是第二用户终端的硬件识别码,如UUID(Universally Unique Identifier,通用唯一识别码)、终端序列号等;也可以是终端的硬件地址,如MAC(Media Access Control,媒体接入控制)地址、蓝牙地址等;还可以是表2中厂商标识与本终端的唯一标识的组合;通常设备标识与在绑定终端与第二用户账户时向服务器提供的设备标识相同。

[0061] 如果业务码中携带有第一用户的终端在生成该业务码时的位置信息,第二用户的终端可以将生成业务请求时本终端的位置信息封装在业务请求中发送给服务器,这样服务器可以根据第二用户终端的位置信息和第一终端的位置信息对业务请求进行安全验证。

[0062] 在服务器上,步骤220,根据业务码中携带的第一用户账户信息和安全程度信息对业务请求进行安全验证。

[0063] 在收到来自第二用户终端的业务请求后,服务器提取其中的业务码,按照与第一用户的终端生成业务码的方式相匹配的方式解析业务码,得到第一用户账户信息、安全程度信息以及其他业务码携带的信息。本领域技术人员可以根据前述生成业务码的具体方式来得出服务器解析业务码的方式,不再赘述。

[0064] 可以参考实际应用场景中业务对安全性的要求度、用户对安全性的要求度、业务的其他特征等因素,来决定根据业务码中的安全程度信息来验证的具体方式,本申请的实施例不做限定。例如,可以当业务码中的安全程度信息低于某个阈值时,拒绝本次业务请求;再如,可以令不同的安全程度信息采用不同的验证方式,较低的安全程度信息对应于较严格的验证方式;此外,还可以针对不同的用户类型设置不同的验证方式,或者允许用户自行设置其不同安全程度信息要采取的验证方式。

[0065] 在一种实现方式中，业务码中以安全级别来作为安全程度信息，并且在业务请求中包括所请求业务的业务额度。可以对不同的安全级别预设所允许的业务额度，服务器查询业务码携带的安全级别对应的所允许的业务额度，如果业务请求中的业务额度超过了这一额度，则该业务请求不能通过安全验证。

[0066] 服务器还可以从业务请求中提取第二用户账户信息和其他与第二用户账户或第二用户的终端相关的信息，并利用这些信息、以及从业务码中解析出的其他信息来对业务请求进行验证。以下举例说明。

[0067] 如果业务码中携带有第一用户终端的设备标识，服务器在从业务码中解析出第一用户终端的设备标识后，可以采用该设备标识查找与第一用户账户绑定的终端设备中是否有第一用户的终端，如果没有，则该业务请求不能通过安全验证。与某个用户账户绑定的终端设备可以是一个到多个。

[0068] 如果业务请求中包括第二用户终端的设备标识，服务器可以采用该设备标识查找与第二用户账户绑定的终端设备中是否有第二用户的终端，如果没有，则该业务请求不能通过安全验证。

[0069] 如果业务码中携带有第一用户终端在生成业务码时的位置信息，服务器在从业务码中解析出第一用户终端的位置信息后，可以将其与第一用户账户的可信地理区域进行比对，如果超出可信地理区域，则该业务请求不能通过验证。第一用户账户的可信地理区域可以由服务器根据第一用户账户的历史活动区域自动生成，也可以由第一用户自行设置。

[0070] 如果业务码中携带有第一用户终端在生成业务码时的位置信息，并且业务请求中包括第二用户终端的位置信息，服务器可以比较第一用户终端的位置信息与第二用户终端的位置信息之间的距离，如果超过预置的距离阈值，则该业务请求不能通过安全验证。

[0071] 上述各种验证方式可以分别采用，也可以结合采用。

[0072] 可见，本申请的实施例中，第一用户终端根据其硬件和/或软件环境确定安全程度信息，在生成的业务码中携带该安全程度信息，服务器可以从第二终端发送的业务请求中获取业务码，根据安全程度信息来对业务请求进行验证，从而能够针对用户终端本身具有的安全性来采用对应的验证标准，既能为安全性较差的终端用户提供更多保障，又能为安全性较强的终端用户提供更多便利。

[0073] 在本申请的一个应用示例中，消费用户(第一用户)通过其在第三方支付系统中的账户向收单商户(第二用户)的账户进行支付，消费用户的终端 (消费终端)、收单商户的终端(收单终端)与第三方支付系统的服务器之间的交互流程如图5所示。第三方支付系统的每个用户账户都绑定有一个到多个终端设备(以终端标识来识别)，并且在绑定每个终端设备的过程中，服务器与该终端设备上分别保存了该用户账户的公钥(服务端密钥)和私钥(用户端密钥)。

[0074] 在收到消费用户的支付指令后，消费终端根据保存消费用户私钥的存储位置的硬件和软件安全措施确定安全级别，获取当前的地理位置信息，从设备硬件获取终端唯一标识，根据表1和表2的格式组装支付二维码的基础数据。消费终端按照预定的对称密钥算法得到随机对称密钥，以随机对称密钥采用AES256(Advanced Encryption Standard 256，256位高级加密标准)算法的cdc(Cipher Block Chaining，加密块链)模式对基础数据进行加密，得到基础数据的密文。消费终端以消费用户账户的私钥对随机对称密钥进行加密，并

且将基础数据的密文和随机对称密钥的密文组合后生成支付二维码。

[0075] 消费终端将支付二维码显示在屏幕上，供收单终端扫描。

[0076] 收单终端扫描得到消费终端的支付二维码，获取本终端所在的地理位置信息，将本终端的设备标识、本终端的地理位置信息、支付额度和支付二维码封装在支付请求中，发送给服务器。

[0077] 服务器收到支付请求，从中提取支付二维码、支付额度、收费终端的设备标识和收费终端的地理位置信息。对支付二维码，服务器查找该消费用户账户的公钥，以该公钥对随机对称密钥的密文进行解密，再用得到的随机对称密钥对支付二维码的基础数据密文进行解密，得到按照表1和表2格式组装的各项信息，其中包括安全级别、消费终端的设备标识和消费终端的地理位置信息。

[0078] 服务器确认消费终端的设备标识是否是消费用户账户绑定终端的设备标识，以及收单终端的设备标识是否是收单用户账户绑定终端的设备标识，如果至少有一方不是，则该业务请求不能通过安全验证。

[0079] 服务器将消费终端的地理位置信息与消费用户账户的可信地理区域进行比对，如果消费终端的地理位置不在该可信区域内，则该业务请求不能通过安全验证。消费用户账户的可信地理区域由服务器根据该消费用户的历史地理位置记录生成，只有在某个用户账户累计了一定的历史地理位置记录后，服务器生成可信地理区域后才据验证业务请求的安全性，当某个用户账户尚无历史地理位置记录时，不采用可信地理区域作为业务请求的验证依据。

[0080] 服务器计算消费终端的地理位置信息与收单终端的地理位置信息之间的距离，如果超过预设的距离阈值，则该业务请求不能通过安全验证。

[0081] 服务器获取预设的对应于安全级别的允许支付额度，如果本次业务请求的支付额度超过允许支付额度，则该业务请求不能通过安全验证。不同的用户账户可以有相同或不同的允许支付额度。

[0082] 在业务请求通过安全验证后，服务器按照支付额度，将消费用户账户中的款项划转到收单用户账户中。服务器向消费终端和收单终端发送支付成功的消息。对不能通过安全验证的业务请求，服务器向收单终端和消费终端发送支付失败的消息。

[0083] 与上述流程实现对应，本申请的实施例还提供了一种应用在服务器上基于业务码的验证装置、一种应用在用户终端上基于业务码的验证、和一种应用在用户终端上生成业务码的装置。上述装置均可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为逻辑意义上的装置，是通过终端或服务器的CPU(Central Process Unit，中央处理器)将对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，除了图 6所示的CPU、内存以及非易失性存储器之外，终端通常还包括用于进行无线信号收发的芯片等其他硬件，服务器通常还包括用于实现网络通信功能的板卡等其他硬件。

[0084] 图7所示为本申请实施例提供的一种基于业务码的验证装置，应用在服务器上，其特征在于，包括业务请求接收单元和安全程度验证单元，其中：业务请求接收单元用于接收第二用户终端发送的包括业务码的业务请求，所述业务码携带有第一用户账户信息和安全程度信息；所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定；安全程度验证单元用于根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证。

[0085] 可选的，所述安全程度信息包括：安全级别；所述业务请求中包括：业务额度；所述安全验证单元具体用于：根据所述安全级别确定所允许的业务额度，当所述业务请求中的业务额度超过所允许的业务额度时，不能通过安全验证。

[0086] 可选的，所述业务码中还携带有第一用户终端在生成所述业务码时的位置信息；所述业务请求中还包括：第二用户终端在发送所述业务请求时的位置信息；所述装置还包括：位置信息验证单元，用于当第一用户终端的位置信息与第二用户终端的位置信息之间的距离超过距离阈值时，所述业务请求不能通过安全验证；和/或，当第一用户终端的位置信息超出第一用户账户的可信地理区域时，所述业务请求不能通过安全验证。

[0087] 可选的，所述业务码中还携带有第一用户终端的设备标识；所述业务请求中还包括：第二用户终端的设备标识；所述装置还包括：设备标识验证单元，用于获取第一用户账户和第二用户账户的绑定终端的设备标识，如果第一用户账户绑定终端的设备标识不同于业务码中第一用户终端的设备标识、或第二用户账户绑定终端的设备标识不同于业务请求中第二用户终端的设备标识，所述业务请求不能通过安全验证。

[0088] 可选的，所述业务码中携带的安全程度信息采用第一用户终端生成的随机密钥进行加密，所述业务码还携带有以第一用户账户的用户端密钥进行加密后的随机密钥密文；所述装置还包括：随机密钥解密单元，用于采用与第一用户账户的用户端密钥相同或相对应的服务端密钥对业务码中的随机密钥密文进行解密，采用解密得到的随机密钥对业务码中的安全程度信息进行解密。

[0089] 图8所示为本申请实施例提供的基于业务码的验证装置，应用在第二用户的终端上，其特征在于，包括业务码获取单元和业务请求发送单元，其中：业务码获取单元，用于从第一用户的终端获取业务码，所述业务码携带第一用户账户信息和安全程度信息；所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定；业务请求发送单元，用于将包括所述业务码的业务请求发送给服务器，供服务器根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证。

[0090] 可选的，所述业务码中还携带有第一用户的终端在生成所述业务码时的位置信息；所述业务请求中还包括：第二用户终端在生成所述业务请求时的位置信息，供服务器根据所述第二用户终端的位置信息和业务码中第一终端的位置信息对业务请求进行安全验证。

[0091] 可选的，所述业务请求中还包括：第二用户终端的设备标识，供服务器根据所述第二用户终端的设备标识对业务请求进行安全验证。

[0092] 图9所示为本申请实施例提供的一种生成业务码的装置，应用在第一用户的终端上，包括安全程度确定单元和业务码生成单元，其中：安全程度确定单元，用于根据本终端的硬件和/或软件环境确定安全程度信息；业务码生成单元，用于采用第一用户账户信息和安全程度信息，按照预定格式生成业务码。

[0093] 一个例子中，所述业务码中至少一个组成部分采用第一用户账户的用户端密钥加密；所述用户端密钥与服务器可获得的第一用户账户的服务端密钥相同或相对应；所述安全程度信息包括：安全级别；所述安全程度确定单元具体用于：按照本终端保存所述用户端密钥的硬件和/或软件的安全措施来确定安全级别。

[0094] 上述例子中，所述业务码生成单元可以具体用于：根据预定算法生成随机密钥，采

用以随机密钥对安全程度信息进行加密后的密文、以第一用户账户的用户端密钥对随机密钥进行加密后的密文，按照预定格式生成业务码。

[0095] 可选的，所述业务码生成单元具体用于：采用第一用户账户信息、安全程度信息和当前本终端的位置信息，按照预定格式生成业务码。

[0096] 可选的，所述业务码生成单元具体用于：采用第一用户账户信息、安全程度信息和本终端的标识，按照预定格式生成业务码。

[0097] 可选的，所述预定格式包括：2字节的业务标识、n字节的用户账户信息、20字节的终端设备信息和6位的验证凭证，其中：业务标识用来表示所述业务码用于哪种业务类型；终端设备信息包括：2字节的版本号、2字节的本终端上安全硬件的厂商标识、2字节的本终端上安全传感器的厂商标识、2字节的本终端上安全识别算法的厂商标识、2字节的本终端的厂商标识、4字节的由所述终端厂商提供的本终端的唯一标识、2字节的安全程度信息和4字节的当前本终端的位置信息；验证凭证为将用户账户信息和终端设备信息输入预定摘要算法后得到的摘要信息；所述业务码生成单元按照预定格式生成业务码，包括：按照所述预定格式组装出业务码的基础数据后，根据预定算法生成随机密钥，采用以随机密钥对至少部分所述基础数据进行加密，再以第一用户账户的用户端密钥对随机密钥进行加密后，将至少部分加密的基础数据和随机密钥的密文组合成业务码。

[0098] 可选的，所述装置还包括：业务码提供单元，用于向第二用户终端提供所述业务码，供其在业务请求中将业务码上传到服务器后，由服务器根据第一用户账户信息和安全程度信息对业务请求进行安全验证。

[0099] 可选的，所述业务码包括：二维码、条形码、或近场通信NFC码。

[0100] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

[0101] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0102] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0103] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0104] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要

素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0105] 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

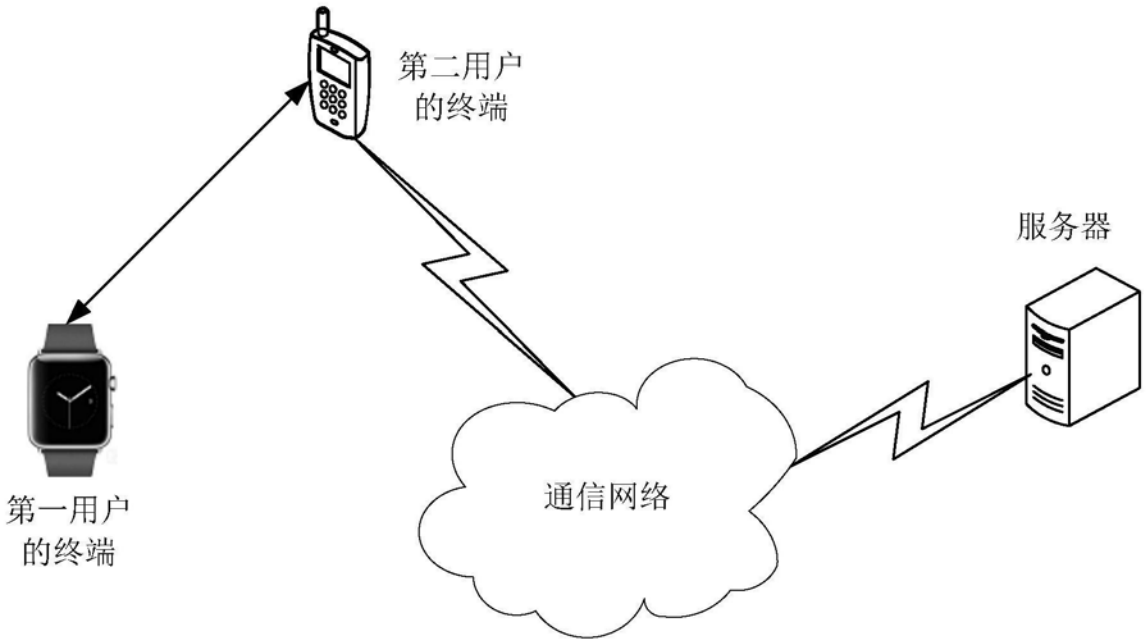

第二用户
的终端
服务器
第一用户
的终端
通信网络

图1

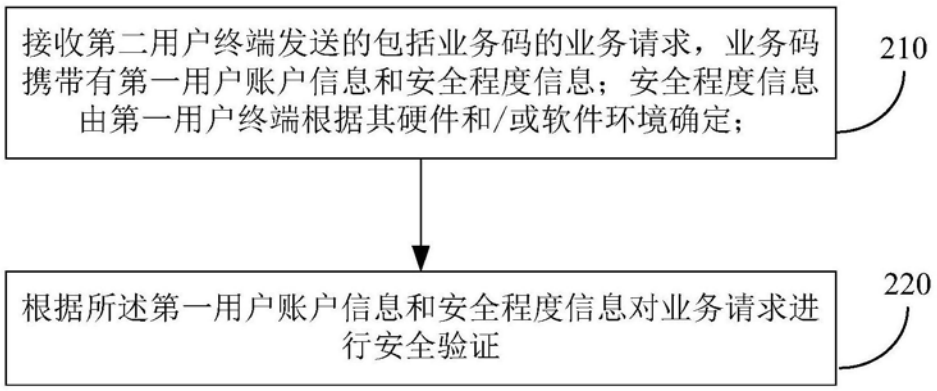

接收第二用户终端发送的包括业务码的业务请求，业务码携带有第一用户账户信息和安全程度信息；安全程度信息由第一用户终端根据其硬件和/或软件环境确定；
210
根据所述第一用户账户信息和安全程度信息对业务请求进行安全验证
220

图2

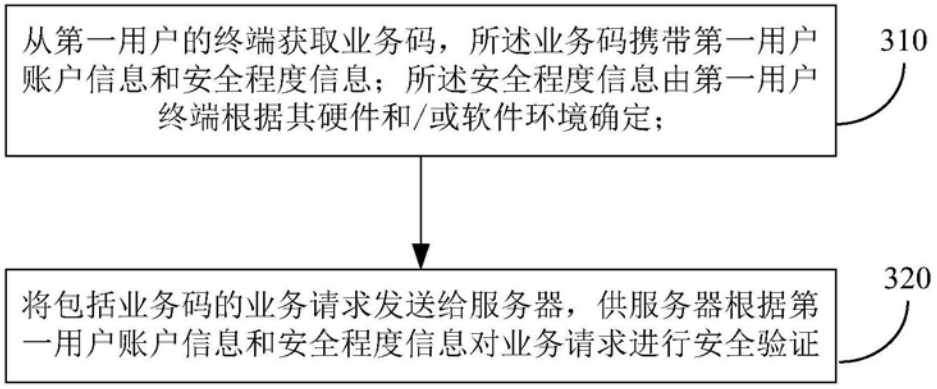

从第一用户的终端获取业务码，所述业务码携带第一用户账户信息和安全程度信息；所述安全程度信息由第一用户终端根据其硬件和/或软件环境确定；
310
将包括业务码的业务请求发送给服务器，供服务器根据第一用户账户信息和安全程度信息对业务请求进行安全验证
320

图3

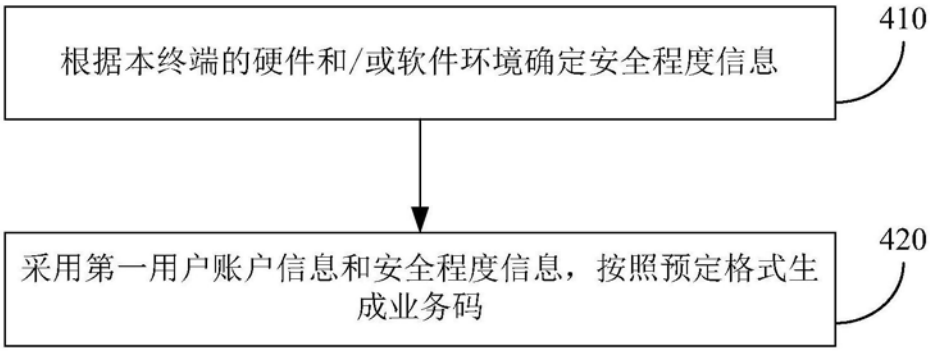

根据本终端的硬件和/或软件环境确定安全程度信息
410
采用第一用户账户信息和安全程度信息，按照预定格式生成业务码
420

图4

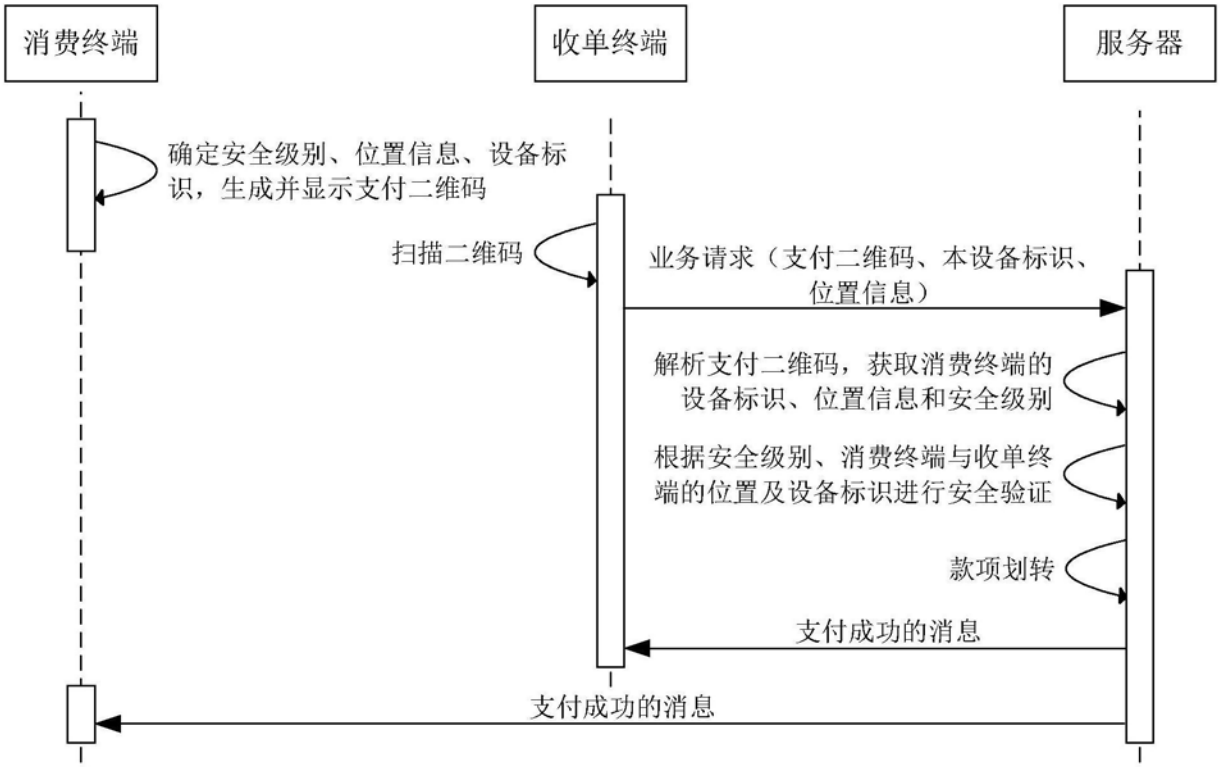

消费终端
收单终端
服务器
确定安全级别、位置信息、设备标识，生成并显示支付二维码
扫描二维码
业务请求（支付二维码、本设备标识、位置信息）
解析支付二维码，获取消费终端的设备标识、位置信息和安全级别
根据安全级别、消费终端与收单终端的位置及设备标识进行安全验证
款项划转
支付成功的消息
支付成功的消息

图5

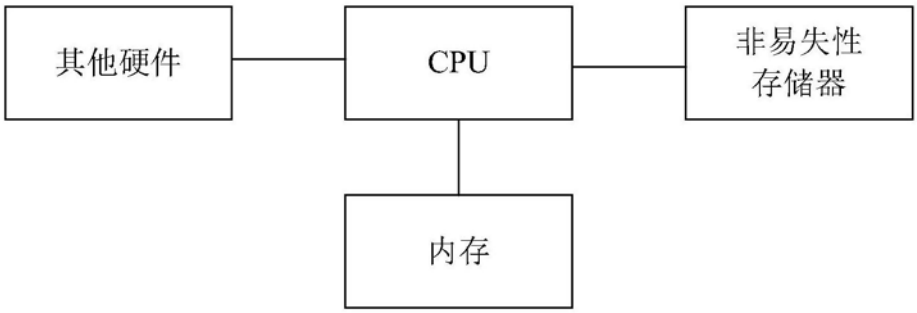


图6

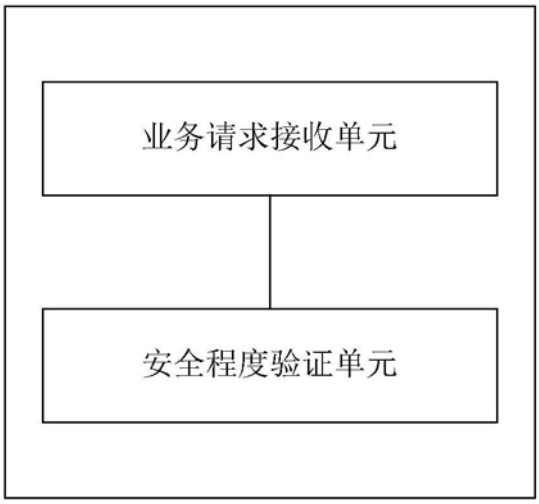


图7

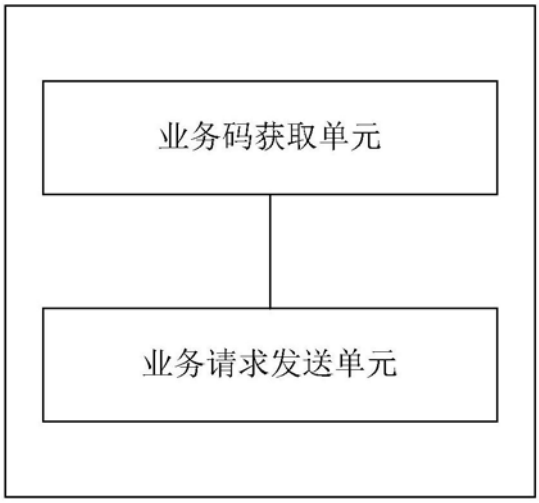


图8

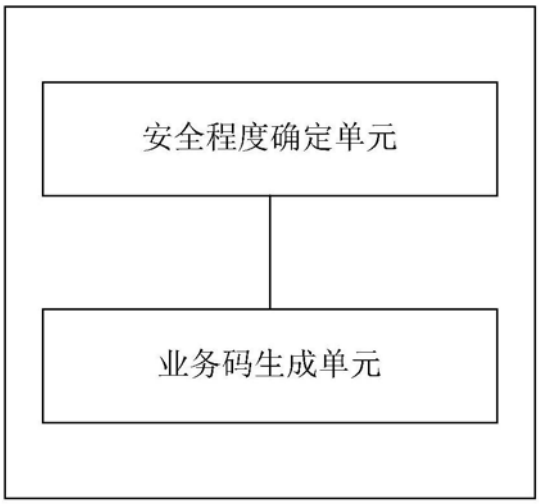


图9