

(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 104320779 A

(43) 申请公布日 2015.01.28

(21) 申请号 201410640240.8

H04B 5/00 (2006.01)

(22) 申请日 2014.11.13

(71) 申请人 熊文俊

地址 610041 四川省成都市武侯区燃灯寺北
街 63 号

(72) 发明人 熊文俊 杨盛麟

(74) 专利代理机构 成都虹桥专利事务所（普通
合伙） 51124

代理人 吴中伟

(51) Int. Cl.

H04W 12/06 (2009.01)

G06Q 20/40 (2012.01)

G06Q 20/16 (2012.01)

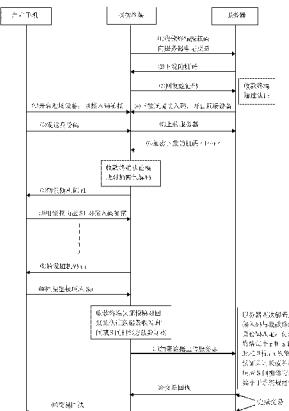
权利要求书4页 说明书9页 附图5页

(54) 发明名称

基于 U/SIM 卡鉴权响应及限时反馈近场通信
认证方法

(57) 摘要

本发明涉及近场通信技术，其为了克服现有技术中的近场通信安全性无法得到保障的问题，提出一种基于移动通信 U/SIM 卡鉴权响应及限时反馈的近场通信认证方法。在本发明中单独制订用于近场交易的认证参数，由本系统服务器下发到移动终端，并由移动终端 APP 调用在网的 U/SIM 卡鉴权运算后将鉴权结果发往服务器预存储。每次近场交易时，服务器均从该预存储的数据中任选随机码下发移动终端，并对移动终端回传的鉴权响应与数据库中该终端预存储的鉴权响应对比，以此来保障交易合法性；并且，本发明为防止手机病毒或黑客远程攻击，针对鉴权响应的安全提出了一套保障流程，即，付款终端必须在系统限定的时限内反馈且为正确的鉴权响应才能认证通过。本发明适用近场交易。



1. 基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法,应用于包括支付终端、收款终端和服务器的系统中;其特征在于,该方法包括以下步骤:

- A. 收款用户利用收款终端向服务器上传其授权码及本次收款款项并申请交易;
- B. 服务器在该授权码对应的数据库中任意选取随机码下发给收款终端;
- C. 收款终端在收到随机码后,以本地数据库中存储的该随机码对应的验证码回复服务器;
- D. 服务器对该验证码进行认证,如果通过认证,则向收款终端下发本次近场通信的通道接入码;
- E. 收款终端开启其近场通信设备,同时对外发送本收款站点名称及本次通道接入码;
- F. 付款用户通过在付款终端上运行近场交易 APP 调用本机身份码并启动终端近场通信设备,在搜索到相应收款终端的近场广播的收款站点名称后,便以所述通道接入码与收款终端建立近场通信链路;
- G. 收款终端获取付款终端的身份码并上传服务器;
- H. 服务器在所述付款终端身份码对应的数据库中任选 n 个随机码 r,并对所述 n 个随机码 r 加密形成加密包,然后在附上所述密钥的编号后下发给收款终端;
- I. 收款终端对所述加密包进行解码,然后通过近场通道将 n 个随机码 r 逐个发送给付款终端,同时记录发送第一个随机码 r 的时间作为第一时间点;
- J. 付款终端在收到第一个随机码 r 时,在其 U/SIM 卡中运算得到对应的鉴权响应 S,并以该鉴权响应 S 对本次交易的近场通道接入码进行加密后发送给收款终端;此后每收到一个随机码 r 均需在其 U/SIM 卡中运算得到对应的鉴权响应 S 并经近场通道回复收款终端,其后才能收到下一个随机码 r;
- K. 收款终端在收到第 n 个随机码 r 对应的鉴权响应 S 时,记录此刻时间作为第二时间点,然后在其本地数据库中任选一个密钥对收到的 n 个鉴权响应 S 及发送第一个随机码 r 的时间和接收到第 n 个鉴权响应 S 的时间进行加密打包并附上本次密钥编号后发送给服务器;
- L. 服务器在收到所述的加密包后,在该收款终端的授权码对应的数据库中以该密钥编号查找对应的密钥对加密包进行解码,然后在付款终端身份码对应的数据库中查找第一个随机码 r 对应的鉴权响应 S 对解码后的数据再次解码,以获得本次交易的近场通道接入码;
- M. 服务器结合近场通道接入码、各个鉴权响应 S 及第一时间点至第二时间点之间的时长进行综合认证,在认证通过后根据本次交易请求信息进入扣款、支付进程;若认证未通过,则取消本次交易。

2. 如权利要求 1 所述的基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法,其特征在于,所述付款终端为用户手机,其在服务器上预存储有本系统认证需要的数据,制备所述认证数据的方式包括:

用户在申请本业务从服务器网页下载近场交易 APP 时,需向服务器进行注册,填入手机号码及运营商名称和其对应的扣款账户或银行卡号,服务器向用户手机下发交易身份码及多个随机码 r;用户手机利用 U/SIM 卡对所述多个随机码 r 进行鉴权运算并向服务器返回对应的多个鉴权响应 S;服务器在收到所述多个鉴权响应 S 后将其存储于该用户手机身

份码对应的数据库中并与所述下发的多个随机码 r 建立对应关系 ;每次近场交易服务器均对移动终端下发所述终端身份码对应数据库中的随机码 r ,并将移动终端对所述随机码 r 返回的鉴权响应 S 与服务器中所述该终端身份码对应数据库中预存储的所述鉴权响应 S 比对,以此对交易的合法性进行认证。

3. 如权利要求 2 所述的基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法,其特征在于,所述服务器中预存储有与收款终端授权码对应的随机码、随机码对应的验证码以及加密密钥、密钥编号和加密算法,并建立与收款终端的授权码对应的对应关系。

4. 如权利要求 2 所述的基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法,其特征在于,本近场通信泛指蓝牙或红外线或声波或 WIFI 或 NFC 近场通道 ;步骤 G 中,收款终端通过扫码方式或近场通道获取付款终端的身份码并上传服务器。

5. 如权利要求 4 所述的基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法,其特征在于,所述收款终端为专用收款终端,所述专用收款终端为内置有独立时钟、CPU 处理器及通信收发模块的独立通信终端,其对外通信接口具备有线宽带和移动无线接口,并在终端内预固化了仅用于验证收款终端身份或资格的随机码及随机码对应的验证码,以及用于交易认证环节的加密密钥、密钥编号及其加密算法 ;所述的独立时钟为北京时间格式的走时时钟,或者是仅对每个鉴权响应 S 间方波数计数的方波发生器。

6. 如权利要求 4 所述的基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法,其特征在于,所述收款终端为普通移动通信终端,在所述终端的 U/SIM 卡或 SD 卡或卡贴上设置有用于进行认证的独立硬件模块,或者将该模块作为 USB、耳机外挂件 ;在该模块上固化有本系统鉴权认证的加密密钥、密钥编号、加密算法和收款授权码,以及对认证数据收发时间标或鉴权响应 S 间的方波数进行记录的计时模块 ;所述独立硬件模块与移动通信终端物理分离,彼此通过蓝牙或红外线连接 ;所述的计时模块为北京时间格式的走时时钟,或者是仅对每个鉴权响应 S 间方波数计数的方波发生器。

7. 如权利要求 1 所述的基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法,其特征在于,步骤 M 中,服务器结合通道接入码、各个鉴权响应 S 及第一时间点至第二时间点之间的时长进行综合认证的具体方法为 :

1) 判断解码后得到的接入码是否与收款终端身份码相匹配,即该接入码是否是发给该收款终端的;

2) 判断收款终端身份码是否与所下发的随机码 r 相匹配,即,随机码 r 是否是发给该收款终端的;

3) 判断每个鉴权响应 S 值是否与服务器上该付款终端身份码对应的鉴权响应 S 相同;

4) 判断第一时间点至第二时间点之间的时长是否小于系统规定值;

只有上述四个条件均满足的情况下,才通过认证。

8. 如权利要求 1 所述的基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法,其特征在于,步骤 H 中,服务器对此 n 个随机码 r 加密形成加密包,然后下发给收款终端的方式为 :在收款终端授权码对应的数据库中任选一密钥对该 n 个随机码 r 进行加密打包,并标明密钥编号后下发给收款终端 ;步骤 I 中,收款终端对加密包进行解码的方式为 :收款终端将收到的数据传输给收款终端内的独立认证模块,由所述的独立认证模块在其数据库中以该密钥编号查询对应的密钥对该加密包进行解码。

9. 如权利要求 1 所述的基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法, 其特征在于, 步骤 J 中, 付款终端在本次交易中完成对 n 个随机码 r 鉴权运算后结束进程并自动关闭近场通信设备, 直到下一次近场交易时, 再重新开启近场通信设备。

10. 基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法, 应用于包括支付终端、收款终端和服务器的系统中; 其特征在于, 该方法包括以下步骤:

A. 收款用户利用收款终端向服务器上传其授权码及本次收款款项并申请交易;

B. 服务器在该授权码对应的数据库中任意选取随机码下发给收款终端;

C. 收款终端在收到随机码后, 以本地数据库中存储的该随机码对应的验证码回复服务器;

D. 服务器对该验证码进行认证, 如果通过认证, 则向收款终端下发本次近场通信的通道接入码;

E. 收款终端开启其近场通信设备, 同时对外发送本收款站点名称及本次通道接入码;

F. 付款用户通过在付款终端上运行近场交易 APP 调用本机身份码并启动终端近场通信设备, 在搜索到相应收款终端的近场广播的收款站点名称后, 以该通道接入码与收款终端建立通信链路;

G. 收款终端以近场通道获取付款终端的身份码并上传服务器;

H. 服务器在所述付款终端身份码对应的数据库中任选 n 个随机码 r, 并对此 n 个随机码 r 加密形成加密包, 然后下发给收款终端;

I. 收款终端对所述加密包进行解码, 然后通过近场通道将 n 个随机码 r 逐个发送给付款终端;

J. 付款终端在收到第一个随机码 r 时, 在其 U/SIM 卡中运算得到对应的鉴权响应 S, 并以该鉴权响应 S 对本次交易的通道接入码进行加密后发送给收款终端; 此后每收到一个随机码 r 均需在其 U/SIM 卡中运算得到对应的鉴权响应 S 并经近场通道回复收款终端, 其后才能收到下一个随机码 r;

K. 收款终端记录每次收到的相邻鉴权响应 S 之间的方波数, 然后在其本地数据库中任选一个密钥对收到的 n 个鉴权响应 S 及相邻鉴权响应 S 之间的方波数进行加密打包并附上本次密钥编号后发送给服务器;

L. 服务器在收到所述的加密包后, 在该收款终端的授权码对应的数据库中以该密钥编号查找对应的密钥对加密包进行解码, 然后在付款终端身份码对应的数据库中查找以第一个随机码 r 对应的鉴权响应 S 对解码后的数据再次解码, 以获得本次交易的近场通道接入码;

M. 服务器结合通道接入码、各个鉴权响应 S 及每相邻鉴权响应 S 之间的方波数进行综合认证: 1) 判断解码后得到的接入码是否与收款终端身份码相匹配, 即, 该接入码是否是发给该收款终端的;

2) 判断收款终端身份码是否与所下发的随机码 r 相匹配, 即, 随机码 r 是否是发给该收款终端的;

3) 判断每个鉴权响应 S 值是否与服务器上该付款终端身份码对应的鉴权响应 S 相同;

4) 判断每相邻鉴权响应 S 之间的方波数是否小于系统规定值;

只有上述四个条件均满足的情况下, 才通过认证, 在认证通过后根据本次交易请求信

息进入扣款、支付进程；若认证未通过，则取消本次交易。

基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法

技术领域

[0001] 本发明涉及近场通信技术,具体涉及一种基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法。

背景技术

[0002] 随着全球移动智能终端的普及,移动互联网应用应声而起,近场交易以其便捷性受到用户的广泛青睐;然而另一方面由于手机病毒泛滥,用户的资金安全受到威胁,也阻碍了近场交易业务的正常发展。

[0003] 因此,本申请有必要提出一种安全性高的近场通信认证方法,以保障近场交易的安全。

发明内容

[0004] 本发明为克服现有技术中的近场通信安全性无法得到保障的问题,提出一种基于 U/SIM 卡鉴权响应及限时反馈近场通信认证方法。

[0005] 本发明解决其技术问题所采用的技术方案是:基于 U/SIM 卡鉴权响应及限时反馈的近场通信认证方法,应用于包括支付终端、收款终端和服务器的系统中;该方法包括以下步骤:

- [0006] A. 收款用户利用收款终端向服务器上传其授权码及本次收款款项并申请交易;
- [0007] B. 服务器在该授权码对应的数据库中任意选取随机码下发给收款终端;
- [0008] C. 收款终端在收到随机码后,以本地数据库中存储的该随机码对应的验证码回复服务器;
- [0009] D. 服务器对该验证码进行认证,如果通过认证,则向收款终端下发本次近场通信的通道接入码;
- [0010] E. 收款终端开启其近场通信设备,同时对外发送本收款站点名称及本次通道接入码;
- [0011] F. 付款用户通过在付款终端上运行近场交易 APP 调用本机身份码并启动终端近场通信设备,在搜索到相应收款终端的近场广播信号的收款站点名称后,便以所述通道接入码与收款终端建立近场通信链路;
- [0012] G. 收款终端获取付款终端的身份码并上传服务器;
- [0013] H. 服务器在所述付款终端身份码对应的数据库中任选 n 个随机码 r,并对所述 n 个随机码 r 加密形成加密包,然后在附上所述密钥的编号后下发给收款终端;
- [0014] I. 收款终端对所述加密包进行解码,然后通过近场通道将 n 个随机码 r 逐个发送给付款终端,同时记录发送第一个随机码 r 的时间节点作为第一时间节点;
- [0015] J. 付款终端在收到第一个随机码 r 时,在其 U/SIM 卡中运算得到对应的鉴权响应 S,并以该鉴权响应 S 对本次交易的近场通道接入码进行加密后发送给收款终端;此后每收到一个随机码 r 均在其 U/SIM 卡中运算得到对应的鉴权响应 S,并经近场通道回复收款终

端,其后才能收到下一个随机码 r ;

[0016] K. 收款终端在收到第 n 个随机码 r 对应的鉴权响应 S 时,记录此刻时间节点作为第二时间节点,然后在其本地数据库中任选一个密钥对收到的 n 个鉴权响应 S 及发送第一个随机码 r 的时间节点和接收到第 n 个鉴权响应 S 的时间节点进行加密打包并附上本次密钥编号后发送给服务器 ;

[0017] L. 服务器在收到所述的加密包后在该收款终端的授权码对应的数据库中以该密钥编号查找对应的密钥对加密包进行解码,然后在付款终端身份码对应的数据库中查找第一个随机码 r 对应的鉴权响应 S 对解码后的数据再次解码获得本次交易的通道接入码 ;

[0018] M. 服务器结合通道接入码、各个鉴权响应 S 及第一时间节点至第二时间节点之间的时长进行综合认证,在认证通过后根据本次交易请求信息进入扣款、支付进程 ;若认证未通过,则取消本次交易。

[0019] 具体的,所述支付终端为用户手机,其存储有认证需要的数据,制备所述认证数据的方式包括 :

[0020] 用户在申请本业务从服务器网页下载近场交易 APP 时,向服务器进行注册,填入手机号码及运营商名称和其对应的扣款账户或银行卡号,服务器向用户手机下发交易身份码及多个随机码 r ;用户手机利用 U/SIM 卡对所述多个随机码 r 进行鉴权运算向服务器返回对应的多个鉴权响应 S ;服务器在收到所述多个鉴权响应 S 后将其存储于该手机身份码对应的数据库中并与随机码 r 建立关联关系。

[0021] 具体的,所述收款终端为专用收款终端,所述专用收款终端为内置有独立时钟、CPU 处理器及通信收发模块的独立通信终端,其对外通信接口具备有线宽带和移动无线接口,并在终端内预固化了仅用于验证收款终端身份或资格的随机码及随机码对应的验证码以及用于交易认证环节的加密密钥、密钥编号及其加密算法,所述的独立时钟可以是北京时间格式的走时时钟,也可以是仅对每个鉴权响应 S 间方波数计数的方波发生器。

[0022] 具体的,所述服务器中预存储有与收款终端中对应的随机码、随机码对应的验证码以及加密密钥、密钥编号和加密算法,并建立与收款终端的授权码对应的关联关系。

[0023] 具体的,所述收款终端为普通移动通信终端,在所述终端的 U/SIM 卡或 SD 卡或卡贴上设置有用于进行认证的独立硬件模块,或者将该模块作为 USB、耳机外挂件 ;在该模块上固化有本系统鉴权认证的加密密钥、密钥编号、加密算法和收款授权码,以及对认证数据收发时间标或鉴权响应 S 间的方波数进行记录的计时模块 ;所述独立硬件模块与移动通信终端通过蓝牙或红外线连接 ;所述的计时模块可以是北京时间格式的走时时钟,也可以是仅对每个鉴权响应 S 间方波数计数的方波发生器。

[0024] 具体的,步骤 M 中,服务器结合通道接入码、各个鉴权响应 S 及第一时间节点至第二时间节点之间的时长进行综合认证的具体方法为 :

[0025] 1) 判断解码后得到的接入码是否与收款终端身份码相匹配,即,该接入码是否是发给该收款终端的 ;

[0026] 2) 判断收款终端身份码是否与所下发的随机码 r 相匹配,即,该随机码 r 是否是发给该收款终端的 ;

[0027] 3) 判断每个鉴权响应 S 值是否与服务器上该付款终端身份码对应的鉴权响应 S 相同 ;

[0028] 4) 判断第一时间点至第二时间点之间的时长是否小于系统规定值；

[0029] 只有上述四个条件均满足的情况下，才通过认证。

[0030] 具体的，步骤 G 中，收款终端通过扫码方式或近场通道获取付款终端的身份码并上传服务器。

[0031] 具体的，步骤 H 中，服务器对此 n 个随机码 r 加密形成加密包，然后下发给收款终端的方式为：在收款终端授权码对应的数据库中任选一密钥对该 n 个随机码 r 进行加密打包，并标明密钥编号后下发给收款终端；步骤 I 中，收款终端对加密包进行解码的方式为：收款终端将收到的数据传输给收款终端内的独立认证模块，由所述独立认证模块在其数据库中以该密钥编号查询对应的密钥对该加密包进行解码。

[0032] 具体的，步骤 J 中，付款终端在本次交易中完成对 n 个随机码 r 鉴权运算后结束进程并自动关闭近场通信设备，直到下一次近场交易时，再重新开启近场通信设备。

[0033] 上述方案中，所述对认证数据收发时间标进行记录是指：记录向付款终端发送的第一个随机码 r 的时间点和收到付款终端反馈的第 n 个鉴权响应 S 的时间节点；此外，对认证数据收发时间标进行记录还可以是对收到的每个相邻鉴权响应 S 之间的方波数进行计数；基于此，本发明还提供了另外一种认证方案，其包括以下步骤：

[0034] A. 收款用户利用收款终端向服务器上传其授权码及本次收款款项并申请交易；

[0035] B. 服务器在该授权码对应的数据库中任意选取随机码下发给收款终端；

[0036] C. 收款终端在收到随机码后，以本地数据库中存储的该随机码对应的验证码回复服务器；

[0037] D. 服务器对该验证码进行认证，如果通过认证，则向收款终端下发本次近场通信的通道接入码；

[0038] E. 收款终端开启其近场通信设备，同时对外发送本收款站点名称及本次通道接入码；

[0039] F. 付款用户通过在付款终端上运行近场交易 APP 调用本机身份码并启动终端近场通信设备，在搜索到相应收款终端的近场广播信号的收款站点名称，以该通道接入码与收款终端建立通信链路；

[0040] G. 收款终端以近场通道获取付款终端的身份码并上传服务器；

[0041] H. 服务器在所述付款终端身份码对应的数据库中任选 n 个随机码 r，并对此 n 个随机码 r 加密形成加密包，然后下发给收款终端；

[0042] I. 收款终端对所述加密包进行解码，然后通过近场通道将 n 个随机码 r 逐个发送给付款终端；

[0043] J. 付款终端在收到第一个随机码 r 时，在其 U/SIM 卡中运算得到对应的鉴权响应 S，并以该鉴权响应 S 对本次交易的通道接入码进行加密后发送给收款终端；此后每收到一个随机码 r 均需在其 U/SIM 卡中运算得到对应的鉴权响应 S，并经近场通道回复收款终端；

[0044] K. 收款终端记录每次收到的相邻鉴权响应 S 之间的方波数，然后在其本地数据库中任选一个密钥对收到的 n 个鉴权响应 S 及相邻鉴权响应 S 之间的方波数进行加密打包并附上密钥编号后发送给服务器；

[0045] L. 服务器在收到所述的加密包后，在该收款终端的授权码对应的数据库中以该密钥编号查找对应的密钥对加密包进行解码，然后在付款终端身份码对应的数据库中查找第

一个随机码 r 对应的鉴权响应 S 对解码后的数据再次解码,以获得本次交易的近场通道接入码;

[0046] M. 服务器结合通道接入码、各个鉴权响应 S 及相邻鉴权响应 S 之间的方波数进行综合认证:1) 判断解码后得到的接入码是否与收款终端身份码相匹配,即,该接入码是否是发给该收款终端的;

[0047] 2) 收款终端身份码是否与所下发的随机码 r 相匹配,即,该随机码 r 是否是发给该收款终端的;

[0048] 3) 判断每个鉴权响应 S 值是否与服务器上该付款终端身份码对应的鉴权响应 S 相同;

[0049] 4) 判断每个相邻鉴权响应 S 之间的方波数是否小于系统规定值;

[0050] 只有上述四个条件均满足的情况下,才通过认证,在认证通过后根据本次交易请求信息进入扣款、支付进程;若认证未通过,则取消本次交易。

[0051] 本发明的有益效果是:本发明在付款用户的移动终端不额外添加任何硬件下,借用移动终端在用的 UICC 卡 U/SIM 的鉴权资源及 2G/3G 互操作的 2G 单向鉴权特性,藉此来保障近场通信的安全。

附图说明

[0052] 图 1 是本系统服务器对收款、付款终端的认证交互流程图;

[0053] 图 2 是普通移动终端作为收款终端时服务器对付款终端 n 次认证流程图;

[0054] 图 3 是本系统服务器与支付服务器账户后台整合示意图。

具体实施方式

[0055] 本发明基于移动通信的 U/SIM 卡 (SIM 卡或 USIM 卡) 的安全鉴权机制,借用移动终端在网的 U/SIM 卡鉴权资源为本系统认证参数进行鉴权认证,以对其鉴权响应值及其响应时隙的甄别,来保障本近场交易系统的安全。

[0056] 由于移动终端 U/SIM 卡的鉴权参数仅能由运营商核心网 EPC 的 AuC/VLR/SGSN 设备掌控、识别,因此本系统需单独制订一套用于本系统近场交易的认证参数,由本系统服务器下发到用户移动终端,并由用户移动终端 APP 调用在网的 U/SIM 卡鉴权模块运算后将鉴权结果发往服务器存储。每次近场交易时服务器均对移动终端下发随机码 r,并将移动终端对该随机码 r 返回的鉴权响应 S 与服务器数据库中对应该终端预存储的认证数据比对,以此对交易的合法性进行认证。

[0057] 制备认证参数的方式如下:

[0058] 用户从服务器网页下载本交易系统 APP 应用时,需填入手机号码、运营商名称及对应的扣款账户或银行卡号,其后服务器便对移动终端下发交易身份码及多个随机码 r。用户将下载的 APP 及本系统随机码 r 和服务器为用户分配的近场交易身份码在本移动终端上安装、运行,其后便开始制备本终端的交易认证数据:若用户使用纯 2G 制式 SIM 卡,则根据 GSM 11.11 规范的 APDU 指令 run gsm algorithm/get respond 在移动终端 SIM 卡中直接对本系统 128bit 的随机码 r 鉴权运算后返回 128bit 的鉴权响应 S。对所下载的随机码 r 鉴权运算完毕后,移动终端便将该些鉴权响应 S 上传服务器。服务器将收到的鉴权响应 S 存储

于该身份码对应的数据库,以建立随机码 r 与鉴权响应 S 的对应关系;若用户使用 2G/3G/LTE 制式的 UICC 复合 USIM 卡,则依据 3GPP TS 的 2G/3G 互操作规范 2G 的单向鉴权特性,移动终端查询 USIM 卡的基本文件 EF 的 EFust(USIM 服务表)的 n° 38“GSM 安全语境”,并利用 APDU 指令的 authenticate req/res 将本系统 128bit 随机码 r 在 USIM 卡中鉴权运算得 res,然后经转换函数 C1、C2 将 res 换算成 128bit 的 gsm 鉴权参数 S,然后由移动终端上传服务器,此后便在服务器建立该移动终端的随机码 r 与鉴权响应 S 的对应关系集。每向 U/SIM 卡输入一个 128bit 随机码 r,便得到一个 128bit 鉴权响应 S,当鉴权运算完毕便删除移动终端内所有的 r 与 S 参数和一切痕迹。每次近场交易时,均由服务器在移动终端身份码数据库任选随机码 r 下发该移动终端,并由移动终端在其 U/SIM 卡对随机码 r 鉴权运算后,将运算的鉴权响应 S 回复服务器,然后由服务器在其数据库中将存储的该随机码 r 对应的鉴权响应 S 作比对。若用户对移动终端上传随机码 r 及鉴权响应 S 存有担忧,可通过单独的 U/SIM 卡读卡器借助电脑辅助运算后通过邮箱发往服务器。对于 3GPP2 通信制式的支付认证数据制备方法,与所述方法相同。

[0059] 在本发明中,用于如 NFC 或图形码近场交易的交易身份码实质是本交易系统的认证码,是用户在服务器网页申请业务时由服务器产生并下发用户移动终端的认证码。该身份码仅用于近场交易而不能作为登陆用户远程网上银行的账号,也即,本近场交易与远程交易在用户端的接入层面彼此账户独立、不能合用的,在服务器上才将该两个帐户合并由服务器将之转换为与用户远程网银共用的支付账户或绑定的银行卡号,以此规避因近场交易系统而造成后台资金被盗的风险,对于本发明系统服务器与支付服务器账户后台整合如图 3 所示。

[0060] 鉴于本交易现场的认证数据是通过近场通道而非有线通道传送,为区分不同用户的交互数据及防范交易现场的非法攻击,服务器需对交易各收款终端下发近场通道接入码,且每次交易接入码均不相同,同时也以此接入码在服务器建立了收款、付款用户的绑定关系。

[0061] 本发明中涉及到的认证系统包括:服务器、收款终端、付款终端三个部分;其交互流程如图 1 所示,实现方式如下:

[0062] 首先,收款终端以其授权码及本次交易收款明细向服务器申请交易,服务器向收款终端下发随机码,收款终端在收到随机码后向服务器回复对应的验证码,服务器对验证码的正确性进行验证,验证通过后服务器向收款终端下发本次近场通道接入码,此时收款终端便开启近场设备;同时,用户付款手机终端也通过启用近场交易 APP 开启近场设备,并以此接入码彼此链接,从而建立与收款终端之间的近场交易通道,并自动调用付款手机终端的身份码经该近场通道发送给收款终端,再由收款终端将身份码上传服务器,接着进入服务器对付款终端进行 n 次鉴权认证的流程:

[0063] 服务器向收款终端下发 n 个付款终端的随机码 r,并由收款终端通过近场通道发送给付款终端。付款终端将第一个随机码 r 在其 U/SIM 卡中算得的鉴权响应 S,并用该鉴权响应 S 对接入码加密后回复收款终端,形成第一次加密,以防止接入码在近场通道被他人截取、篡改,其后对 n-1 个随机码 r 只需回复鉴权响应 S 便可。收款终端收完 n 个鉴权认证数据后,再对该 n 个数据加密打包,形成第二次加密,以防止认证数据收发时间在传输通道被他人截获并篡改,其后附上本次密钥编号后上传服务器。服务器在收到该加密数据包后,

首先在收款终端数据库中以该密钥编号选取对应密钥对收到的加密数据解码,以完成第一次解码。其后在付款终端身份码数据库中选取对应的鉴权响应 S,对解码后的数据再一次解码,以完成第二次解码后获取接入码。其后以第二次解码所得的接入码核对收、付款终的绑定关系。在服务器的 n 次鉴权认证中,付款终端在本次的鉴权运算周期内仅且只接受 n 个随机码 r,在完成本次鉴权运算后便结束进程并自动关闭近场设备。下一次近场交易时,付款终端需重新启动近场设备,此举旨在多收款终端存在环节下,防止收款终端蓄意利用其他智能终端作为中间桥接设备,在盗取正在使用的其他收款终端近场接入接入码后,伺机引诱付款终端链接本机以骗取付款终端的误支付。

[0064] 收款终端与付款终端之间建立的近场通道用于交易终端间交互认证数据,其泛指蓝牙或红外线或声波或 WIFI 或 NFC 无线通道,在收款终端与付款终端彼此建立近场链接后以该通道交互随机码 r 及鉴权认证数据。收款用户在其终端上输入收款金额及购物明细并点击“收款确认”后,收款终端便以其的授权码及本次收款款项向服务器申请交易。若收款终端通过身份认证,服务器便向专用收款终端下发本次近场通信的接入码并开启近场通信设备,同时对外发送本收款站点名称。与此同时,付款用户点击终端交易图标以调用本机身份码并启动近场通信设备,在其搜寻到收款终端的近场广播信号的收款点名称后,便以该接入码与收款终端建立通信链路。付款用户点击“交易确认”确认后,便通过近场通道与收款终端交互认证数据,其后由收款终端将付款终端交互的数据上传服务器。为了防止用户误按“交易确认”键而导致误支付,服务器发出的近场通道接入码有效时间可设为 1 分钟。

[0065] 对于本发明中的收款终端来说,即可以采用专用收款终端,又可以采用普通移动终端作收款终端,下面结合两个实施例对此两种实现方式进行具体说明:

[0066] 实施例一:

[0067] 该类收款终端是由银行或金融机构检测合格后分给发商户,商户需通过审核才能获得交易端口及交易授权码。专用收款终端是内置有独立时钟、CPU 处理器及通信收发模块的独立通信终端,其对外通信接口具备有线宽带和移动无线空口。专用收款终端内预固化了仅用于验证收款终端身份或资格的随机码及其验证码,以及用于交易认证环节的加密密钥、密钥编号及其加密算法,相应地在服务器该终端授权码对应数据库中也存有随机码和验证码,以及加密密钥及密钥编号和加密算法,所述的独立时钟可以是北京时间格式的走时时钟,也可以是仅对每个鉴权响应 S 间方波数计数的方波发生器。

[0068] 基于用户付款终端、专用收款终端和服务器系统的认证方法如下:

[0069] 收款用户在其终端上输入收款金额及购物明细并点击“收款确认”后,收款终端便以其的授权码及本次收款款项向服务器申请交易,于是服务器便在该授权码对应的数据仓库中任选随机码下发专用收款终端,并由专用收款终端以该随机码对应的验证码回复服务器。

[0070] 若收款终端通过身份认证,服务器便向专用收款终端下发本次近场通信的接入码并开启近场通信设备,同时对外发送本收款站点名称。与此同时,付款用户点击终端交易图标以调用本机身份码并启动终端近场通信设备,在其搜寻到收款终端的近场广播的收款点名称后,便以该接入码与收款终端建立通信链路。双方终端以近场通道建立链接后,专用收款终端通过扫码方式或近场通道获取付款终端身份码,其后以授权码向服务器上传本次交易认证数据。服务器收到上传的数据后在付款终端身份码对应的数据库中任选 n 个随机

码 r, 同时在收款终端授权码对应的数据库中任选一密钥对该 n 个随机码 r 加密打包, 并标明密钥编号后下发专用收款终端。专用收款终端将收到的数据转发认证模块, 由认证模块在其数据库中以该密钥编号选取对应的密钥对该加密包解码, 然后经近场通道将第一个随机码 r 发往付款终端, 同时记录发送时间。付款终端将随机码 r 在其 U/SIM 卡中运算得鉴权响应 S, 并以该鉴权响应 S 对本次接入码加密后回传专用收款终端, 形成第一次加密。此后, 专用收款终端认证模块每发送一个随机码 r, 均要有鉴权响应 S 的回复后再才发送下一个随机码 r, 也即, 付款终端只在收到第一个随机码 r 时, 才需返回由第一个鉴权响应 S 加密接入码的数据包, 其余 n-1 个随机码 r 全部回复其对应的鉴权响应 S 值, 接入码的目的是便于服务器辨识收款终端的身份。当 n 个随机码 r 及 n 个鉴权响应 S 交互完毕并记录第 n 个鉴权响应 S 到达时间后, 专用终端认证模块便在数据库中任选一密钥, 对收到的 n 个鉴权响应 S 及第一个随机码 r 的发出时间和第 n 个鉴权响应 S 的接收时间加密打包, 并附上密钥编号后一并发往服务器, 形成第二次加密。或认证模块对收到的每个鉴权响应 S 彼此间的方波计数后, 加密并附上密钥编号发往服务器。服务器收到该加密包后, 在收款终端数据库中以该密钥编号选取对应的密钥对加密包解码, 完成第一次加解码。然后以付款终端数据库中第一个随机码 r 对应的鉴权响应 S 对解码后的数据再次解码, 以获得接入码, 完成第二次加解码, 其后作如下四个研判 :A> 解码后所得的接入码是否与收款终端身份码匹配, 即, 接入码是否是发给该收款终端的 ;B> 款终端身份码是否与所下发的随机码 r 相匹配, 即, 随机码 r 是否是发给该收款终端的 ;C> 每个鉴权响应 S 值应是否与付款终端数据库中的鉴权响应 S 相同 ;D> 认证模块从发出第一次随机码 r 到收到第 n 个鉴权响应 S 的时长是否小于系统规定值, 或每个相邻鉴权响应 S 的方波数是否小于系统规定的方波数。只有以上四个条件均满足系统要求, 才能通过服务器的认证, 否则, 取消本次交易。服务器对 n 个随机码 r 加密下发, 并由认证模块对 n 个鉴权数据加密回传, 旨在防止传输通道中对鉴权数据的时间标或方波数的篡改, 同时也为缩短通信时间。但收款终端认证模块在向付款终端发送随机码 r 时, 却要等到有鉴权响应 S 回复后再发送下一个, 其目的是刻意造成黑客终端去远端用户终端盗取用户 U/SIM 卡鉴权响应 S 的时间加长, 从而因通信异常而被服务器中止进程。如上所述, 由于黑客终端每次鉴权认证均需往返远端用户终端以获取鉴权响应 S, 也即, 其对服务器完成一次鉴权认证的时长约为正常时间的三倍。若设服务器对付款终端 50 次鉴权认证, 则付款终端以其 U/SIM 卡的第一个鉴权响应 S 对接入码加密后回复收款终端, 其余的 49 次每次均只回复鉴权响应 S, 仅当收款终端认证模块收到鉴权响应 S 后, 才发送下一个随机码 r, 若超过规定时间还没回复, 则认证模块通知收款终端向服务器报告交易进程已被中止。如, 设 USIM 卡的机卡数据吞吐率 230k/s, 则 128bit 随机码 r 出入一次 USIM 卡用时 $0.56*2 = 1.1\text{ms}$, 若设卡内 CPU 鉴权运算时间为 100ms, 那么一次近场鉴权运算用时约为 101.1ms, 也即, 每个 r 与 S 对在移动收款终端的近场鉴权交互时长为 101.1ms。而对于黑客终端而言, 由于需回复鉴权响应 S 才能收到下一个随机码 r, 因此其需往返远端用户终端才能获取鉴权响应 S, 若设其单边一次最快 30ms, 则其取一次鉴权响应 S 需用时 $30*2 = 60\text{ms}$, 也即每次鉴权其需多用时 60ms。对于近端用户终端 50 次鉴权认证所需时间为 5s, 同时考虑到远端用户也需约 5s 的鉴权运算时间, 因此对于黑客终端 50 次则多用时 3s ;对于 SIM 卡 57k/s 的机卡数据吞吐率, 其出入 SIM 卡一次的时间约为 4.5ms, 因此近端用户一次鉴权认证的时限可设定为两档 :101.1ms 和 104.5ms, 而黑客终端一次鉴权认证至少也需要

$101.1+60 = 161.1\text{ms}$, 显然不论是对认证时长计时或是对响应 S 间的方波计数, 均会因其超出系统规定值而被服务器取消交易。n 越大, 则黑客终端超时越多, 越易于识别超时。另外, 由于收付款终端交互的认证数据系经 U/SIM 或 SD 卡上独立的认证模块加密打包, 因此在短短的时间内不可能对其解码, 也即, 认证数据的收发时间标不可能被篡改, 那么黑客以盗得他人的身份码与收款商户合谋骗取用户资金便不能得逞。服务器对付款终端进行 n 次鉴权认证时, 付款终端在一个鉴权运算周期内所接受的随机码 r 数也相应地变为 n 个, 以防交易现场其他收款终端“浑水摸鱼”, 保障用户的资金安全。

[0071] 实施例二：

[0072] 移动终端作收款终端时, 其交易端口仍需支付商审核后提供。如上所述, 由于手机终端的通信环境较为复杂, 其与服务器的往返时间不确定, 因此黑客终端可利用此点与收款用户合谋, 同步延缓向服务器的回复时间以造成网络时延的假象, 其目的是为黑客终端到远端用户中病毒的终端获取 U/SIM 卡鉴权响应 S 赢得宝贵的时间。为此需在移动收款终端 U/SIM 或 SD 卡或卡贴上新增设单独的、与移动通信体系无关的独立硬件认证模块, 或 USB/ 耳机孔外挂 / 插件, 以准确地界定并保护认证数据的收发时间节点。该硬件认证模块上固化有不能读出的加密密钥和密钥编号以及加密算法和收款授权码, 硬件认证模块还集成有对外通信接口, 其内部计时模块可单独配置, 也可以取自移动终端, 其作用是对 r 及 S 的收发时间计时或对其相邻 S 间的方波数计数。或者, 该硬件认证模块实体可与移动终端物理分离, 其上配置有低功率蓝牙或红外线通信模块, 该通信模块与移动终端以专属通道连接。相应地, 服务器上该收款授权码对应数据库中, 也预植入了加密密钥、密钥编号及加密算法; 所述的计时模块可以是北京时间格式的走时时钟, 也可以是仅对每个鉴权响应 S 间方波数计数的方波发生器。

[0073] 基于用户付款终端、移动收款终端和服务器系统的认证方法如图 2 所示:

[0074] 移动收款终端以其收款授权码及本次收款金额向服务器提交交易申请, 服务器便对移动收款终端下发随机码 r, 移动收款终端便在本机的 U/SIM 卡进行运算后的鉴权 S 回复服务器, 以便服务器对该收款终端身份或资格的确认。在移动收款终端通过服务器的身份认证后, 服务器便向移动收款终端下发本次近场通道接入码并开启近场通信设备。与此同时, 付款用户点击终端交易图标以调用本机身份码并开启终端近场通信设备, 在搜寻到移动收款终端发出的近场广播收款站点名称后, 便以该接入码与移动收款终端建立通信链路。付款用户点击“交易确认”确认后, 移动收款终端通过近场通道或扫码方式获取付款终端身份码并上传服务器。其后服务器在付款终端身份码数据库中选取 n 个随机码 r, 同时在移动收款终端收款授权码数据库中任选一密钥对该 n 个随机码 r 加密, 在附上该密钥编号后下发移动收款终端。移动收款终端将该加密数据包转发 U/SIM 或 SD 卡或外挂件该独立的硬件认证模块。该硬件认证模块在数据库中选取该密钥编号对应的密钥对该加密数据解码, 然后通过移动收款终端的近场通道向付款终端发出第一个随机码 r, 同时硬件认证模块记录发出的时间。付款终端将第一个随机码 r 在其 U/SIM 卡中鉴权运算得鉴权响应 S, 然后用该鉴权响应 S 对本次接入码加密, 以形成第一次加密, 其后通过近场通道将该加密数据回复移动收款终端, 移动收款终端将收到的数据转发硬件认证模块。此后, 硬件认证模块通过移动收款终端的近场通道向付款终端每发送一个随机码 r, 便需收到付款终端鉴权响应 S 的回复后才发出下一个随机码 r, 直到硬件认证模块内的 n 个随机码 r 发送完毕且收到

回复 S, 同时记录收到最后一个响应 S 时间。鉴权认证数据交互完毕, 硬件认证模块便在其数据库中任选一密钥对已收的 n 个鉴权响应 S 值连同第一次发出随机码 r 时间标和接收第 n 个鉴权响应 S 时间标一起加密打包, 以形成第二次加密, 然后附上本次密钥编号后连同第二次的加密数据一并发往服务器, 或硬件认证模块对收到的每个鉴权响应 S 彼此间的方波计数后, 加密并附上密钥编号发往服务器。服务器收到上传的加密包后, 首先以该密钥编号在收款终端数据库中查得对应的密钥对加密包解码, 完成第一次解码。其后, 在付款终端数据库中查找第一个随机码 r 对应的鉴权响应 S, 对解码后的数据进行第二次解码以获得接入码, 然后作如下四个研判 :A> 解码后所得的接入码应是否与收款终端身份码相匹配, 即, 该接入码是否是发给该收款终端的 ;B> 收款终端身份码是否与所下发的随机码 r 相匹配, 即, 该随机码 r 是否是发给该收款终端的 ;C> 每个鉴权响应 S 值应是否与付款终端身份码数据库中的鉴权响应 S 相同 ;D> 认证模块从发出第一次随机码 r 到收到第 n 个鉴权响应 S 的时长是否小于系统规定值, 或 n 个鉴权响应 S 每相邻间的方波数是否小于系统规定数。只有以上四个条件均满足系统要求, 才能通过服务器的认证, 然后进入扣款、支付进程, 否则, 服务器取消本次交易。如上所述, 服务器对付款终端进行 n 次鉴权, 其目的也是造成黑客终端去远端用户终端盗取用户 U/SIM 卡鉴权响应 S 的时间加长, 从而导致其因通信超时而被服务器中止进程。服务器对付款终端进行 n 次鉴权认证时, 付款终端在一个鉴权运算周期内接受的随机码 r 数也相应地变为 n 个。

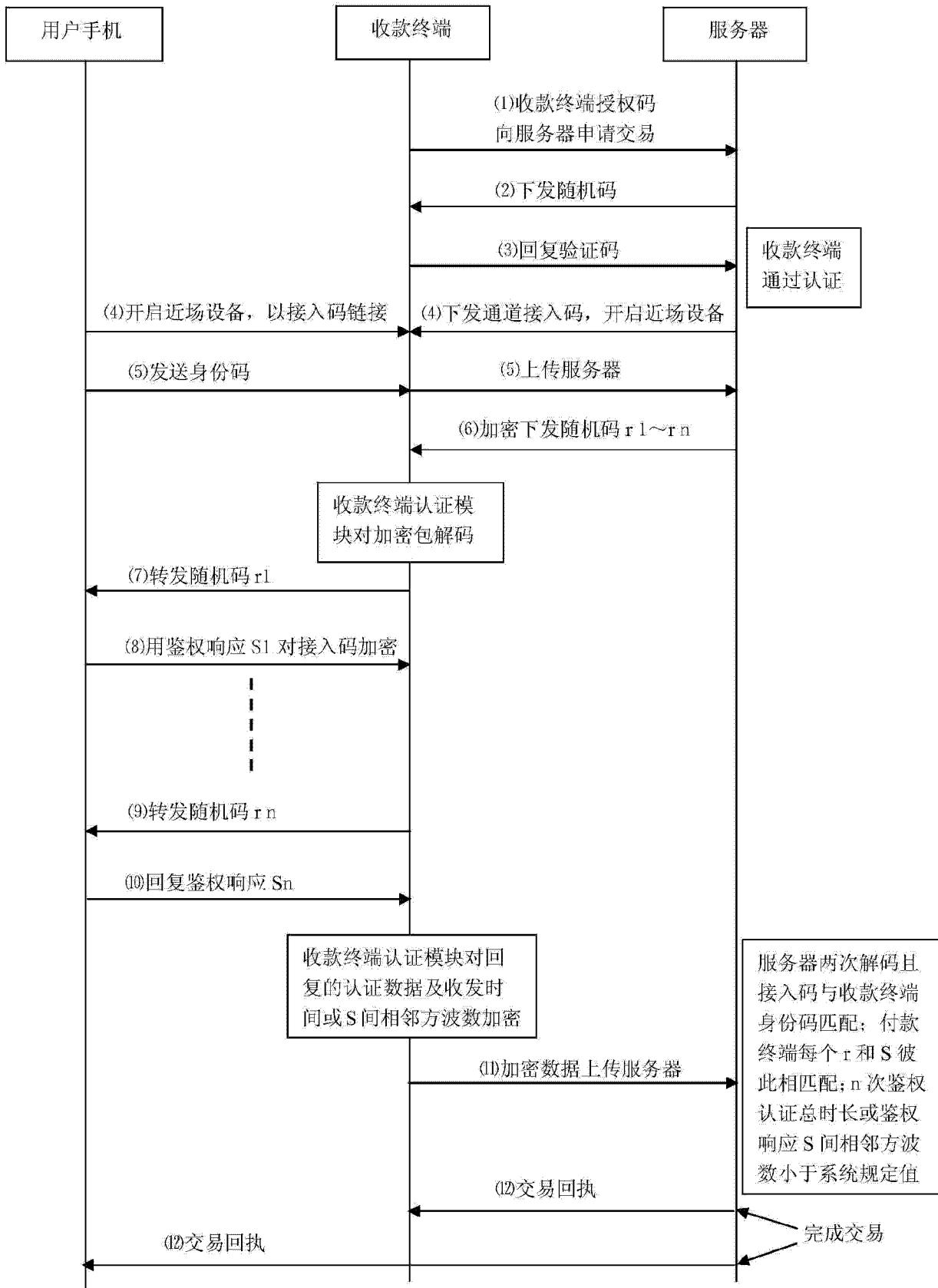
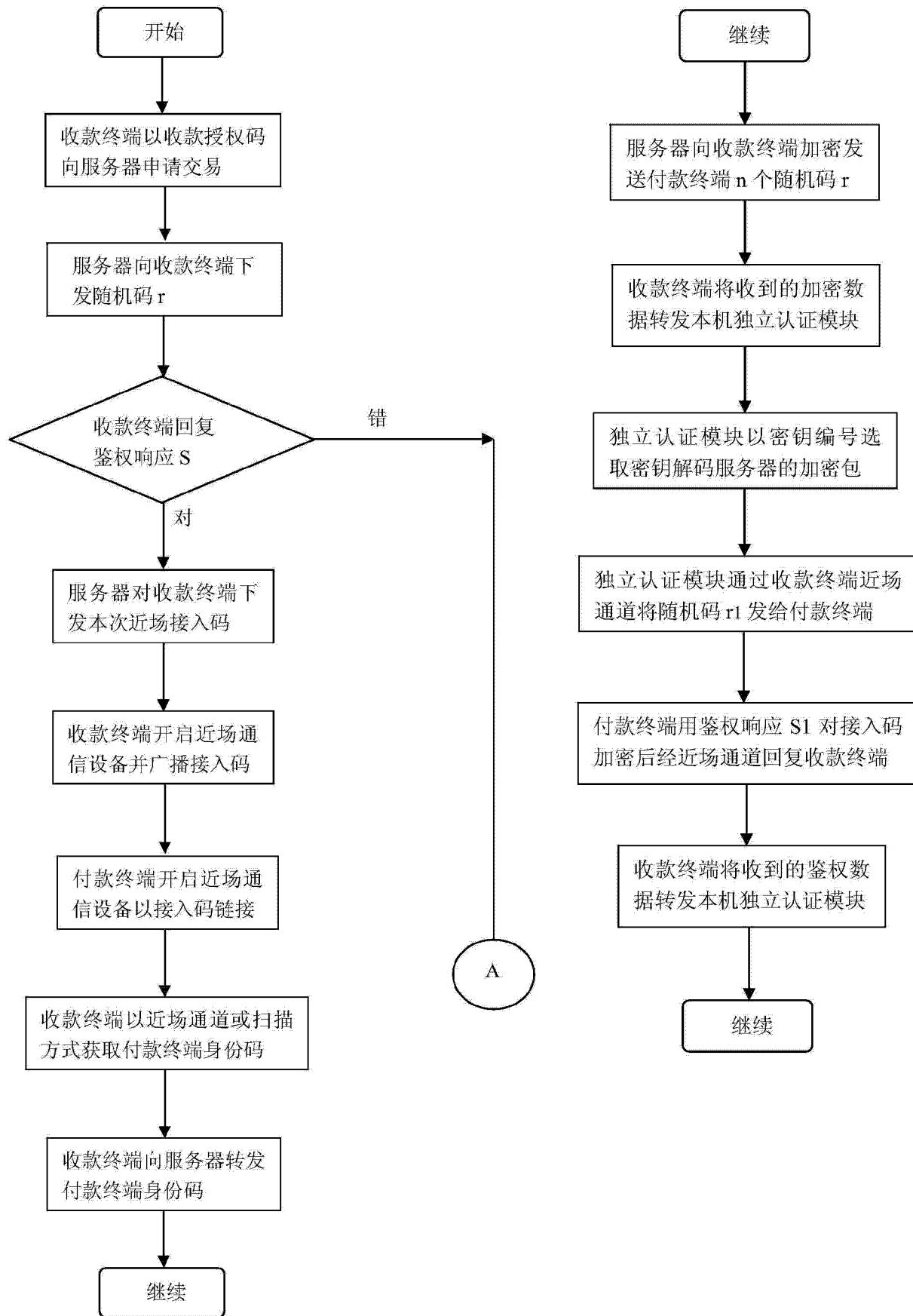
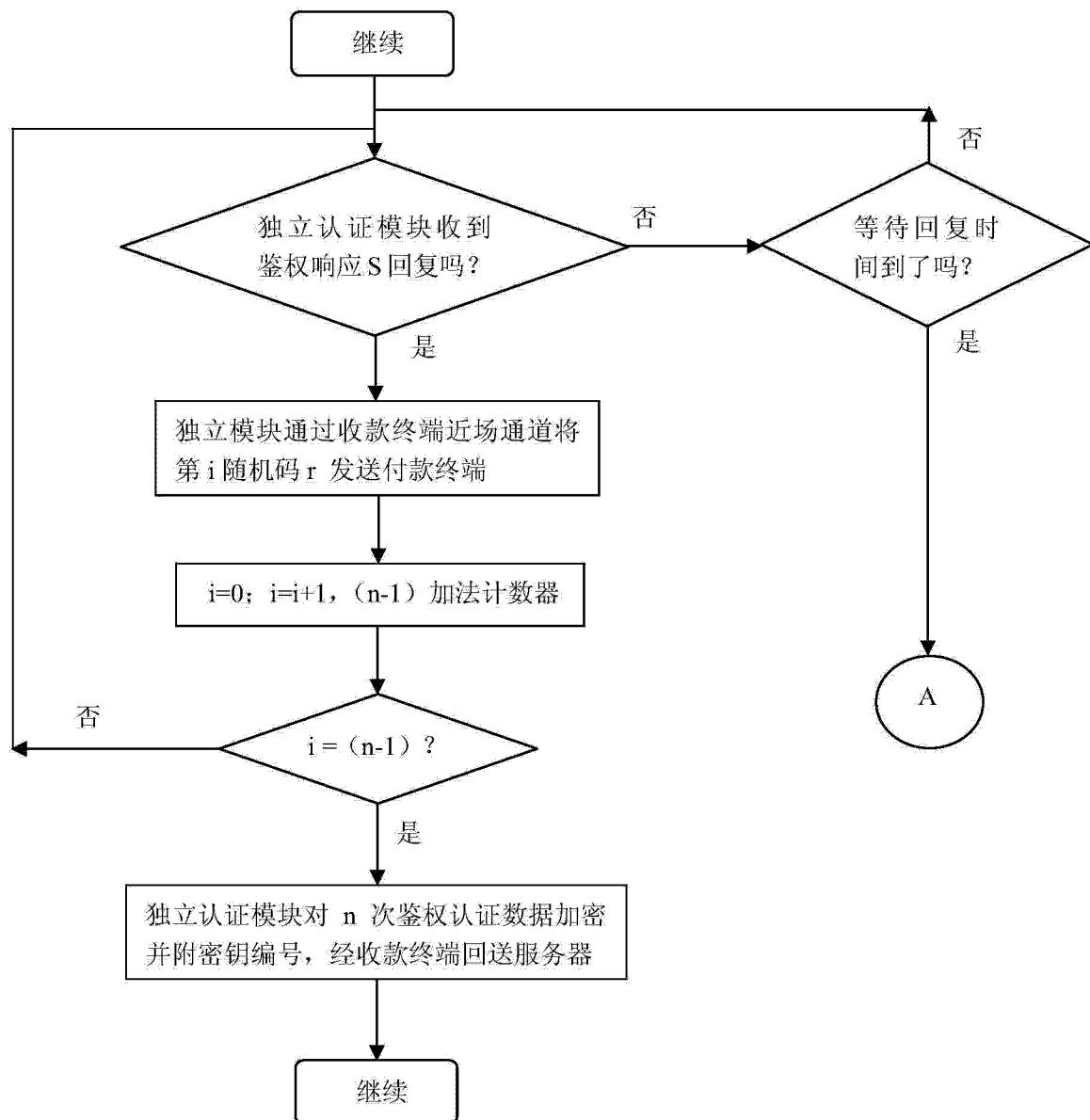


图 1





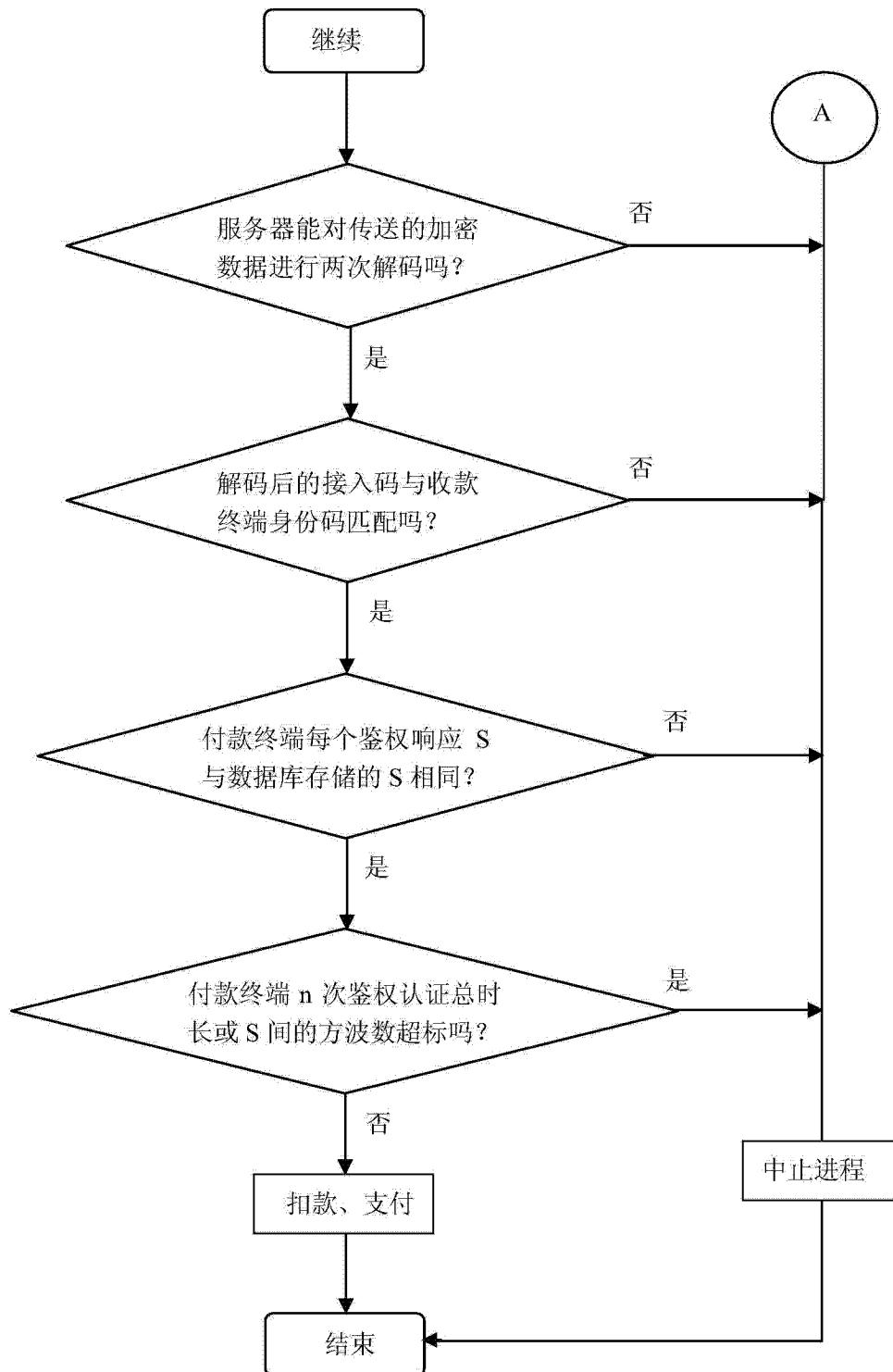


图 2

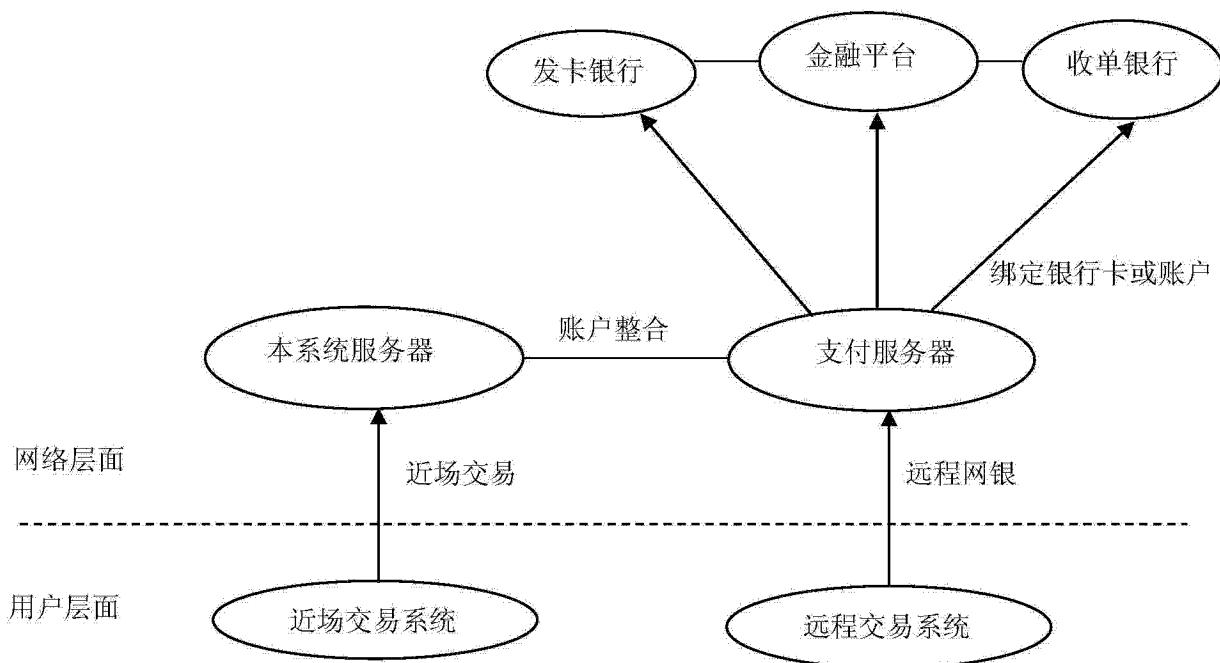


图 3