(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 104036392 A
(43)申请公布日 2014.09.10

(21)申请号 201410294389.5

(22)申请日 2014.06.25

(71)申请人 TCL集团股份有限公司
地址 516006 广东省惠州市仲恺高新技术开发区十九号小区

(72)发明人 田旻

(74)专利代理机构 深圳中一专利商标事务所 44237
代理人 张全文

(51)Int.Cl.
G06Q 20/40(2012.01)

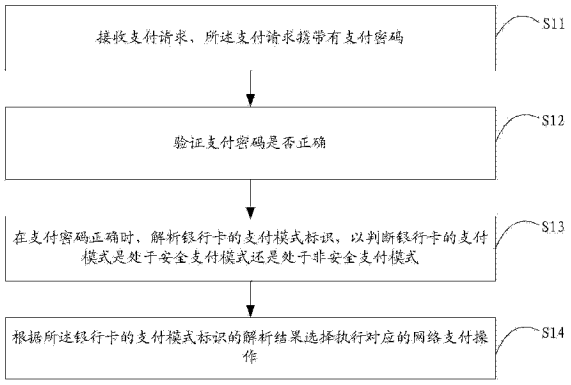
权利要求书2页 说明书7页 附图1页

(54)发明名称

一种网络支付方法及装置

(57)摘要

本发明适用于网络安全领域，提供了一种网络支付方法及装置。所述方法包括：接收支付请求，所述支付请求携带有支付密码；验证支付密码是否正确；在支付密码正确时，解析银行卡的支付模式标识，以判断银行卡的支付模式是处于安全支付模式还是处于非安全支付模式；根据所述银行卡的支付模式标识的解析结果选择执行对应的网络支付操作。本发明实施例能够提高网络支付的安全性。



CN 104036392 A

1. 一种网络支付方法，其特征在于，所述方法包括下述步骤：

接收支付请求，所述支付请求携带有支付密码；

验证支付密码是否正确；

在支付密码正确时，解析银行卡的支付模式标识，以判断银行卡的支付模式是处于安全支付模式还是处于非安全支付模式；

根据所述银行卡的支付模式标识的解析结果选择执行对应的网络支付操作。

2. 如权利要求 1 所述的方法，其特征在于，在所述接收支付请求的步骤之前，包括下述步骤：

接收用户发送的非安全支付模式触发请求；

根据所述非安全支付模式触发请求将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识。

3. 如权利要求 1 所述的方法，其特征在于，验证支付密码是否正确步骤之后还包括：在支付密码不正确时，记录接收的支付请求的次数；

判断记录的接收的支付请求的次数是否大于预设的次数阈值，并在记录的接收的支付请求的次数大于预设的次数阈值时，将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识。

4. 如权利要求 1 所述的方法，其特征在于，所述根据所述银行卡的支付模式标识的解析结果选择执行对应的网络支付操作的步骤具体包括：

在银行卡处于安全支付模式时，执行网络支付操作并发送支付确认信息至智能终端；所述智能终端与银行卡绑定；

在银行卡处于非安全支付模式时，生成并发送动态口令至与银行卡绑定的智能终端，以接收并比较所述与银行卡绑定的智能终端返回的信息，根据比较结果选择是否执行网络支付操作，所述与银行卡绑定的智能终端至少有 2 个。

5. 如权利要求 4 所述的方法，其特征在于，所述生成并发送动态口令至与银行卡绑定的智能终端，以接收并比较所述与银行卡绑定的智能终端返回的信息，根据比较结果选择是否执行网络支付操作的步骤具体包括：

分别根据与银行卡绑定的各个智能终端的国际移动用户识别码 IMSI、与银行卡绑定的各个智能终端的用户预设的信息、时间戳以及随机数，生成各个与银行卡绑定的智能终端对应的动态口令；

将生成的动态口令发送至对应的智能终端，并接收与银行卡绑定的各个智能终端根据接收的动态口令返回的信息；

将接收的信息与保存的上一次发送给与银行卡绑定的各个智能终端的动态口令比较；

在接收的所有信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令都相同时，保存当前生成的动态口令，并执行网络支付操作；

在接收的任一个信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令不相同时，不执行网络支付操作。

6. 如权利要求 5 所述的方法，其特征在于，所述在接收的任一个信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令不相同时，不执行网络支付操作的

步骤具体包括：

在接收的任一个信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令不相同时，不执行本次支付请求对应的网络支付操作；

将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识，所述银行卡在安全模式下和返回与保存的动态口令不相同的信息的智能终端绑定。

7. 一种网络支付装置，其特征在于，所述装置包括：

支付请求接收单元，用于接收支付请求，所述支付请求携带有支付密码；

支付密码验证单元，用于验证支付密码是否正确；

支付模式标识解析单元，用于在支付密码正确时，解析银行卡的支付模式标识，以判断银行卡的支付模式是处于安全支付模式还是处于非安全支付模式；

网络支付操作选择执行单元，用于根据所述银行卡的支付模式标识的解析结果选择执行对应的网络支付操作。

8. 如权利要求 7 所述的装置，其特征在于，所述装置包括：

非安全支付模式触发请求接收单元，用于接收用户发送的非安全支付模式触发请求；

支付模式标识修改单元，用于根据所述非安全支付模式触发请求将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识。

9. 如权利要求 7 所述的装置，其特征在于，所述网络支付操作选择执行单元包括：

支付确认信息发送模块，用于在银行卡处于安全支付模式时，执行网络支付操作并发送支付确认信息至智能终端；所述智能终端与银行卡绑定；

动态口令发送模块，用于在银行卡处于非安全支付模式时，生成并发送动态口令至与银行卡绑定的智能终端，以接收并比较所述与银行卡绑定的智能终端返回的信息，根据比较结果选择是否执行网络支付操作，所述与银行卡绑定的智能终端至少有 2 个。

10. 如权利要求 9 所述的装置，其特征在于，所述动态口令发送模块包括：

动态口令生成模块，用于分别根据与银行卡绑定的各个智能终端的国际移动用户识别码 IMSI、与银行卡绑定的各个智能终端的用户预设的信息、时间戳以及随机数，生成各个与银行卡绑定的智能终端对应的动态口令；

验证信息接收模块，用于将生成的动态口令发送至对应的智能终端，并接收与银行卡绑定的各个智能终端根据接收的动态口令返回的信息；

验证信息比较模块，用于将接收的信息与保存的上一次发送给与银行卡绑定的各个智能终端的动态口令比较；

同意支付模块，用于在接收的所有信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令都相同时，保存当前生成的动态口令，并执行网络支付操作；

网络支付操作停止执行模块，用于在接收的任一个信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令不相同时，不执行本次支付请求对应的网络支付操作；

非安全支付模式标识模块，用于将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识，所述银行卡在安全模式下和返回与保存的动态口令不相同的信息的智能终端绑定。

一种网络支付方法及装置

技术领域

[0001] 本发明属于网络安全领域，尤其涉及一种网络支付方法及装置。

背景技术

[0002] 电子商务是指在互联网、企业内部网和增值网以电子交易方式进行交易活动和相关服务的活动，是传统商业活动各环节的电子化、网络化。随着电子商务的发展，如何实现安全的网络支付已经成为一个热门话题。

[0003] 目前的网络支付方法通常是：网上银行服务器端接收到用户发起的支付请求后，判断用户输入的验证信息是否正确，若正确，则网上银行服务器端提示同意支付，否则，网上银行服务器端提示拒绝支付。但由于木马泛滥，验证信息容易被截获，因此，若在任何时候都是通过判断验证信息是否正确来选择是否完成支付是存在极大的隐患的，安全性较低。

发明内容

[0004] 本发明实施例提供了一种网络支付方法，旨在解决现有方法在网络支付时，银行卡账号安全性较低的问题。

[0005] 本发明实施例是这样实现的，一种网络支付方法，所述方法包括下述步骤：

[0006] 接收支付请求，所述支付请求携带有支付密码；

[0007] 验证支付密码是否正确；

[0008] 在支付密码正确时，解析银行卡的支付模式标识，以判断银行卡的支付模式是处于安全支付模式还是处于非安全支付模式；

[0009] 根据所述银行卡的支付模式标识的解析结果选择执行对应的网络支付操作。

[0010] 本发明实施例的另一目的在于提供一种网络支付装置，所述装置包括：

[0011] 支付请求接收单元，用于接收支付请求，所述支付请求携带有支付密码；

[0012] 支付密码验证单元，用于验证支付密码是否正确；

[0013] 支付模式标识解析单元，用于在支付密码正确时，解析银行卡的支付模式标识，以判断银行卡的支付模式是处于安全支付模式还是处于非安全支付模式；

[0014] 网络支付操作选择执行单元，用于根据所述银行卡的支付模式标识的解析结果选择执行对应的网络支付操作。

[0015] 在本发明实施例中，由于根据银行卡的支付模式选择不同的网络支付操作（银行卡处于安全支付模式时，只需将验证信息发送到绑定的智能终端进行验证，网络支付简单；银行卡处于非安全支付模式时，需要将验证信息发送到多个绑定的智能终端进行验证，网络支付复杂），因此不仅保证了用户在银行卡处于安全支付模式时能够快速完成网上支付，且保证了用户在在银行卡处于非安全支付模式时能够保证银行卡账户的安全。

附图说明

[0016] 图 1 是本发明第一实施例提供的一种网络支付方法的流程图；

[0017] 图 2 是本发明第二实施例提供的一种网络支付装置的结构图。

具体实施方式

[0018] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0019] 本发明实施例中，当接收到一个支付请求时，首先验证该支付请求携带的支付密码是否正确，若正确，则判断用于支付请求对应的银行卡的支付模式，若该银行卡处于安全支付模式，则仅向发起支付请求的智能终端发送一个动态口令，若该银行卡处于非安全支付模式，则除了向安全模式下绑定的智能终端发送一个动态口令之外，还向与该银行卡绑定的其他智能终端发送对应的动态口令，最后通过验证各个智能终端返回的信息选择同意网络支付操作，或者拒绝网络支付操作。为了说明本发明所述的技术方案，下面通过具体实施例来进行说明。

[0020] 实施例一：

[0021] 图 1 示出了本发明第一实施例提供的一种网络支付方法的流程图，在本实施例中，根据银行卡的支付模式是处于安全支付模式还是处于非安全支付模式选择对应的网络支付操作，详述如下：

[0022] 步骤 S11，接收支付请求，所述支付请求携带有支付密码。

[0023] 该步骤中，网上银行服务器端接收用户发送的支付请求，该支付请求携带有用户请求使用支付的银行卡对应的支付密码。

[0024] 优选地，在所述接收支付请求的步骤之前，包括下述步骤：

[0025] A1、接收用户发送的非安全支付模式触发请求。

[0026] A2、根据所述非安全支付模式触发请求将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识。

[0027] 上述步骤 A1 ～ A2 中，若用户感觉到自己泄露了支付密码，或者已经发现自己有不明支付时，主动触发非安全支付模式，以发出非安全支付模式触发请求，提高网上支付的安全性。网上银行服务器端接收到非安全支付模式触发请求后，将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识。其中，银行卡的支付模式有安全支付模式和非安全支付模式，并通过银行卡的支付模式标识进行区分，例如，银行卡的支付模式标识采用“0”表示银行卡处于安全支付模式，采用“1”表示银行卡处于非安全支付模式。

[0028] 步骤 S12，验证支付密码是否正确。

[0029] 该步骤中，网上银行服务器端将接收的支付密码与预先存储的支付密码比较，若相同，判定支付密码正确，若不相同，判定支付密码错误。

[0030] 步骤 S13，在支付密码正确时，解析银行卡的支付模式标识，以判断银行卡的支付模式是处于安全支付模式还是处于非安全支付模式。

[0031] 该步骤中，将当前的银行卡的支付模式标识的值与定义的银行卡的支付模式标识的值比较，以判断当前的银行卡的支付模式。例如，假设当前的银行卡的支付模式标识的值为 1，而定义的银行卡的支付模式标识的值为 1 时表示银行卡处于非安全支付模式，因此，

可判定当前的银行卡的支付模式处于非安全支付模式。

[0032] 优选地，在步骤 S12 之后还包括：在支付密码不正确时：

[0033] B1、记录接收的支付请求的次数；该步骤中，当用户输入的支付密码不正确时，通常会尝试输入其他的数据作为支付密码，这时，网上银行服务器端将记录用户输入的支付密码的次数，即记录接收的支付请求的次数。

[0034] B2、判断记录的接收的支付请求的次数是否大于预设的次数阈值，并在记录的接收的支付请求的次数大于预设的次数阈值时，将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识。该步骤中，网上银行服务器端预先设定一个次数阈值，当接收的支付请求的次数大于该次数阈值时，表明当前的支付密码存在破解风险，则网上银行服务器端修改银行卡的支付模式标识，以触发银行卡的非安全支付模式，提高网上支付的安全性。其中，次数阈值可预设为 3，或者为其他数值，此处不作限定。

[0035] 步骤 S14，根据所述银行卡的支付模式标识的解析结果选择执行对应的网络支付操作。

[0036] 其中，所述根据所述银行卡的支付模式标识的解析结果选择执行对应的网络支付操作的步骤具体包括：

[0037] C1、在银行卡处于安全支付模式时，执行网络支付操作并发送支付确认信息至智能终端；所述智能终端与银行卡绑定。该步骤中，当银行卡处于安全支付模式时，网上银行服务器端直接执行网络支付操作，并将包含本次网上支付发生的时间和金额的支付确认信息发送给发起支付请求的智能终端。例如，假设用户 A 将智能终端 A 与银行卡 X 绑定，用户 A 通过智能终端 A 发起支付请求，则网上银行服务器端在判断支付请求携带的支付密码为正确的支付密码后，将包含本次网上支付发生的时间和金额的支付确认信息发送给智能终端 A。

[0038] C2、在银行卡处于非安全支付模式时，生成并发送动态口令至与银行卡绑定的智能终端，以接收并比较所述与银行卡绑定的智能终端返回的信息，根据比较结果选择是否执行网络支付操作，所述与银行卡绑定的智能终端至少有 2 个。确定与非安全模式下的银行卡绑定的智能终端的一种实施方式是，在安全模式下，智能终端 A 和银行卡 X 绑定，智能终端 B 与银行卡 Y 绑定，且银行卡 X 与 Y 关联形成一个安全域，即当银行卡 X 处于非安全模式时，将动态口令发送到与银行卡 X 关联的其它银行卡对应在安全模式下绑定的其它终端如智能终端 B 进行确认，另一种实施方式是，银行卡 X 在安全模式下与智能终端 A 进行绑定，而在非安全模式下与预先设定的智能终端 A 和智能终端 B 进行绑定，而银行卡 Y 在安全模式下与智能终端 B 进行绑定，而在非安全模式下与预先设定的智能终端 A 和智能终端 B 进行绑定。在第一实施方式下，由于通过关联银行卡确定非安全模式下绑定智能终端，从而当用户将银行卡 Y 在安全模式绑定的智能终端 B 更改为智能终端 C，则银行卡 X 处于非安全模式时直接将对应的动态口令发送给智能终端 A 和 C，无需用户额外将银行卡 X 在非安全模式下关联的智能终端 B 更换为智能终端 C，实现方便。

[0039] 具体地，步骤 C2 通过以下步骤实现：

[0040] C21、分别根据与银行卡绑定的各个智能终端的国际移动用户识别码(International Mobile Subscriber Identification Number，IMSI)、与银行卡绑定的各个智能终端的用户预设的信息、时间戳以及随机数，生成与银行卡绑定的各个智能终端对应

的动态口令。其中，IMSI 是区别移动用户的标志，储存在 SIM 卡中；与银行卡绑定的各个智能终端的用户预设的信息是指各个智能终端的用户自定义的密码，比如用户的生日、手机号码等，每个智能终端的用户预设的信息通常不同；时间戳和随机数都是随机生成的。该步骤中，在计算一个智能终端的动态口令时，将该智能终端的 IMSI、该智能终端的用户预设的信息、时间戳以及随机数作为 hash 函数的输入值，经过 hash 函数对输入值的多次摘录（或称多次迭代，摘录次数为迭代次数 seq），得到 64 位的二进制数，然后将得到的 64 位的二进制数转化为 6 个英文单词，这 6 个英文单词作为该智能终端的用户的动态口令，生成动态口令后，seq = seq-1。通过该方法，使得每次生成的动态口令都不相同，提高了网络支付的安全性。例如，假设在非安全模式下，智能终端 A 与银行卡 X 绑定、智能终端 B 与银行卡 Y 绑定，由于 X 与 Y 的支付活动相互监督，即银行卡 X 与 Y 的支付信息都会发送给该安全域内所有的智能终端，从而在银行卡 X 处于非安全模式时，银行卡 X 与该安全域内智能终端 A 和智能终端 B 绑定，智能终端 A 对应的用户预设的信息为“123456”，智能终端 B 对应的用户预设的信息为“234567”，则在计算智能终端 A 的动态口令时，将该智能终端 A 的 IMSI、该智能终端 A 的用户预设的信息“123456”、随机生成的时间戳以及随机数作为 hash 函数的输入值，再经过 hash 函数对输入值的多次摘录得到该智能终端 A 的动态口令；在计算智能终端 B 的动态口令时，将该智能终端 B 的 IMSI、该智能终端 B 的用户预设的信息“234567”、随机生成的时间戳以及随机数作为 hash 函数的输入值，再经过 hash 函数对输入值的多次摘录得到该智能终端 B 的动态口令。其中，hash 函数以变长的信息作为输入，把输入压缩成一个定长的输出值，由于输入的长度大于输出的长度，因为会有不同的输入产生相同的输出的情况，且即使输入信息只有微小的改变，输出的定长值也会发生很大的变化，使输出的定长值难以破解，从而提高动态口令的安全性。常用的 hash 函数如 MD4，MD5 和 SHA，MD5 是 MD4 的扩展，安全性强于 MD4。

[0041] C22、将生成的动态口令发送至对应的智能终端，并接收与银行卡绑定的各个智能终端根据接收的动态口令返回的信息。该步骤中，网上银行服务器端将根据不同智能终端的信息生成的动态口令发送到对应的智能终端。例如，将根据智能终端 A 的 IMSI、智能终端 A 的用户预设的信息以及随机生成的时间戳、随机数等生成的动态口令发送给智能终端 A；将根据智能终端 B 的 IMSI、智能终端 B 的用户预设的信息以及随机生成的时间戳、随机数等生成的动态口令发送给智能终端 B。当然，若是智能终端 A 发起的支付请求，则还可以选择是否向智能终端 A 发送包含购物的金额、时间等具体购物内容。当生成的动态口令发送至对应的智能终端之后，各个智能终端返回的信息与该各个智能终端的 IMSI 等信息一起以动态口令的格式加密发送到网上银行服务器端，以便该网上银行服务器端确认智能终端的合法性及支付结果的反馈确认。

[0042] C23、将接收的信息与保存的上一次发送给与银行卡绑定的各个智能终端的动态口令比较。该步骤中，网上银行服务器端将接收的信息解码为 64 位密钥，然后结合智能终端的 IMSI 及用户预设的信息等，用相同的函数进行计算，得到一个动态口令，若得到的动态口令与上一次发送给智能终端的动态口令进行比较。

[0043] C24、在接收的所有信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令都相同时，保存当前生成的动态口令，并执行网络支付操作。例如，假设用户 A 将智能终端 A 与银行卡 X 绑定，并且智能终端 B 在非安全模式下也与银行卡 X 绑定（该

智能终端 B 对应的用户通常不是用户 A，且该智能终端 B 与银行卡 Y 绑定），且用户 A 通过智能终端 A 发起支付请求，若智能终端 A 接收的信息与上一次发送给该智能终端 A 的动态口令相同，且智能终端 B 接收的信息与上一次发送给该智能终端 B 的动态口令相同时，保存当前发送给智能终端 A 的动态口令，保存当前发送给智能终端 B 的动态口令。

[0044] C25、在接收的任一个信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令不相同时，不执行网络支付操作。例如，假设智能终端 A、智能终端 B 都与银行卡 X 绑定，且用户通过智能终端 A 发起支付请求，若智能终端 A 接收的信息与上一次发送给该智能终端 A 的动态口令相同，智能终端 B 接收的信息与上一次发送给该智能终端 B 的动态口令不相同，则判定此次支付请求有异常，不执行智能终端 A 发起的支付请求对应的网络支付操作。

[0045] 进一步地，步骤 C25，在接收的任一个信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令不相同时，不执行网络支付操作的步骤具体包括：

[0046] C251、在接收的任一个信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令不相同时，不执行本次支付请求对应的网络支付操作。

[0047] C252、将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识，所述银行卡和返回与保存的动态口令不相同的信息的智能终端绑定。

[0048] 上述步骤 C251 ～ C252 中，假设用户 A 将智能终端 A 与银行卡 X 绑定，并且在非安全模式下智能终端 B 也与银行卡 X 绑定（该智能终端 B 对应的用户通常不是用户 A，假设为用户 B，则该智能终端 B 还与用户 B 的其他银行卡绑定，假设与银行卡 Y 绑定），网上银行服务器端检测到银行卡 X 处于非安全支付模式下，智能终端 B 回复的信息与保存的上一次发送给该智能终端 B 的动态口令不相同时，不执行本次由智能终端 A 发起的支付请求对应的网络支付操作，并且，将该智能终端 B 绑定的银行卡 Y 的支付模式标识修改为该银行卡 Y 处于非安全支付模式的标识。当然，也可以预先设定一个检验次数阈值，当检测到某个智能终端回复的信息与保存的上一次发送给该智能终端的动态口令不相同的次数大于预先设定的检验次数阈值时，才将该智能终端绑定的银行卡的支付模式标识修改为该银行卡处于非安全支付模式的标识。例如，假设智能终端 B 在非安全模式下与银行卡 X、银行卡 Y 绑定，本次银行卡 X 进行支付，且预先设定的检验次数阈值为 3 时，当检测到智能终端 B 回复的信息与保存的上一次发送给该智能终端 B 的动态口令不相同的次数为 4（大于预先设定的检验次数阈值 3）时，才将该智能终端 B 在安全模式下绑定的银行卡 Y 的支付模式（该银行卡 Y 原来的支付模式为安全模式）标识修改为该银行卡处于非安全支付模式的标识。

[0049] 优选地，在银行卡处于非安全支付模式时，除了通过步骤 C2 实现之外，还可以通过以下步骤实现：(1) 发送包含购物内容的金额、时间等具体购物内容、以及验证码至安全模式下绑定的智能终端；(2) 生成并发送动态口令至与银行卡绑定的除安全模式下绑定的智能终端之外的智能终端；(3) 接收并比较安全模式下绑定的智能终端以及除安全模式下绑定的智能终端之外的智能终端返回的信息；(4) 根据比较结果选择是否执行网络支付操作。

[0050] 在本发明第一实施例中，当接收到一个支付请求时，首先验证该支付请求携带的支付密码是否正确，若正确，则判断用于支付的银行卡的支付模式，若该银行卡处于安全支付模式，则仅向安全模式下绑定的智能终端发送一个动态口令，若该银行卡处于非安全支

付模式，则除了向该银行卡对应安全模式下绑定的智能终端发送一个动态口令之外，还向与该银行卡在安全模式下没有绑定但是与该银行卡关联银行卡对应绑定的其他智能终端发送对应的动态口令，最后通过验证各个智能终端返回的信息选择同意网络支付操作，或者拒绝网络支付操作。由于根据银行卡的支付模式选择不同的网络支付操作（银行卡处于安全支付模式时，网络支付简单；银行卡处于非安全支付模式时，网络支付复杂），因此不仅保证了用户在银行卡处于安全支付模式时能够快速完成网上支付，且保证了用户在在银行卡处于非安全支付模式时能够保证银行卡账户的安全。

[0051] 实施例二：

[0052] 图 2 示出了本发明第二实施例提供的一种网络支付装置的结构图，为了便于说明，仅示出了与本发明实施例相关的部分。

[0053] 该网络支付装置包括：支付请求接收单元 21、支付密码验证单元 22、支付模式标识解析单元 23、网络支付操作选择执行单元 24。

[0054] 支付请求接收单元 21，用于接收支付请求，所述支付请求携带有支付密码。其中，支付请求携带有用户请求使用支付的银行卡对应的支付密码。

[0055] 优选地，用户可以主动请求更改银行卡的支付模式标识，此时，所述网络支付装置包括：非安全支付模式触发请求接收单元和支付模式标识修改单元。

[0056] 该非安全支付模式触发请求接收单元用于接收用户发送的非安全支付模式触发请求。该支付模式标识修改单元用于根据所述非安全支付模式触发请求将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识。用户主动触发非安全支付模式，以提高网上支付的安全性。

[0057] 支付密码验证单元 22，用于验证支付密码是否正确。

[0058] 优选地，还包括支付请求次数记录单元，用于在支付密码不正确时，记录接收的支付请求的次数；再判断记录的接收的支付请求的次数是否大于预设的次数阈值，并在记录的接收的支付请求的次数大于预设的次数阈值时，将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识。当接收的支付请求的次数大于该次数阈值时，表明当前的支付密码存在破解风险，则网上银行服务器端修改银行卡的支付模式标识，以触发银行卡的非安全支付模式，提高网上支付的安全性。

[0059] 支付模式标识解析单元 23，用于在支付密码正确时，解析银行卡的支付模式标识，以判断银行卡的支付模式是处于安全支付模式还是处于非安全支付模式。

[0060] 具体地，支付模式标识解析单元 23 将当前的银行卡的支付模式标识的值与定义的银行卡的支付模式标识的值比较，以判断当前的银行卡的支付模式。

[0061] 网络支付操作选择执行单元 24，用于根据所述银行卡的支付模式标识的解析结果选择执行对应的网络支付操作。

[0062] 其中，所述网络支付操作选择执行单元 24 包括：支付确认信息发送模块和动态口令发送模块。

[0063] 该支付确认信息发送模块用于在银行卡处于安全支付模式时，执行网络支付操作并发送支付确认信息至智能终端；所述智能终端与银行卡绑定。其中，支付确认信息包括本次网上支付发生的时间和金额等具体购物信息。

[0064] 该动态口令发送模块用于在银行卡处于非安全支付模式时，生成并发送动态口令

至与银行卡绑定的智能终端，以接收并比较所述与银行卡绑定的智能终端返回的信息，根据比较结果选择是否执行网络支付操作，所述与银行卡绑定的智能终端至少有 2 个。进一步地，所述动态口令发送模块包括：动态口令生成模块、验证信息接收模块、验证信息比较模块、同意支付模块、拒绝支付模块。

[0065] 该动态口令生成模块用于分别根据与银行卡绑定的各个智能终端的国际移动用户识别码 IMSI、与银行卡绑定的各个智能终端的用户预设的信息、时间戳以及随机数，生成各个与银行卡绑定的智能终端对应的动态口令。其中，在计算一个智能终端的动态口令时，将该智能终端的 IMSI、该智能终端的用户预设的信息、时间戳以及随机数作为 hash 函数的输入值，经过 hash 函数对输入值的多次摘录（或称多次迭代，摘录次数为迭代次数 seq），得到 64 位的二进制数，然后将得到的 64 位的二进制数转化为 6 个英文单词，这 6 个英文单词作为该智能终端的用户的动态口令，生成动态口令后，seq = seq-1。

[0066] 该验证信息接收模块用于将生成的动态口令发送至对应的智能终端，并接收与银行卡绑定的各个智能终端根据接收的动态口令返回的信息。其中，发送到不同的智能终端的动态口令通常不同，当然，除了动态口令之外，还可以选择是否向发起支付请求的智能终端发送包含购物的金额、时间等具体购物内容。

[0067] 该验证信息比较模块用于将接收的信息与保存的上一次发送给与银行卡绑定的各个智能终端的动态口令比较。其中，具体的比较过程如下：将接收的信息解码为 64 位密钥，然后结合智能终端的 IMSI 及用户预设的信息等，用相同的函数进行计算，得到一个动态口令，若得到的动态口令与上一次发送给智能终端的动态口令进行比较。

[0068] 该同意支付模块用于在接收的所有信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令都相同时，保存当前生成的动态口令，并执行网络支付操作。

[0069] 该拒绝支付模块用于在接收的任一个信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令不相同时，不执行网络支付操作。进一步地，所述拒绝支付模块包括：网络支付操作停止执行模块和非安全支付模式标识模块。该网络支付操作停止执行模块用于在接收的任一个信息与对应的保存的上一次发送给与银行卡绑定的各个智能终端的动态口令不相同时，不执行本次支付请求对应的网络支付操作。该非安全支付模式标识模块用于将银行卡的支付模式标识修改为标识银行卡处于非安全支付模式的标识，所述银行卡在安全模式下和返回与保存的动态口令不相同的信息的智能终端绑定。由于在检测到智能终端回复的动态口令出现异常时，启动该智能终端绑定的银行卡的非安全支付模式，共同监督，提高该智能终端绑定的银行卡的网上支付的安全性。

[0070] 在本发明第二实施例中，由于根据银行卡的支付模式选择不同的网络支付操作，因此不仅保证了用户在银行卡处于安全支付模式时能够快速完成网上支付，且保证了用户在在银行卡处于非安全支付模式时能够保证银行卡账户的安全。

[0071] 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步骤是可以通过程序来指令相关的硬件来完成，所述的程序可以在存储于一计算机可读取存储介质中，所述的存储介质，如 ROM/RAM、磁盘、光盘等。

[0072] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

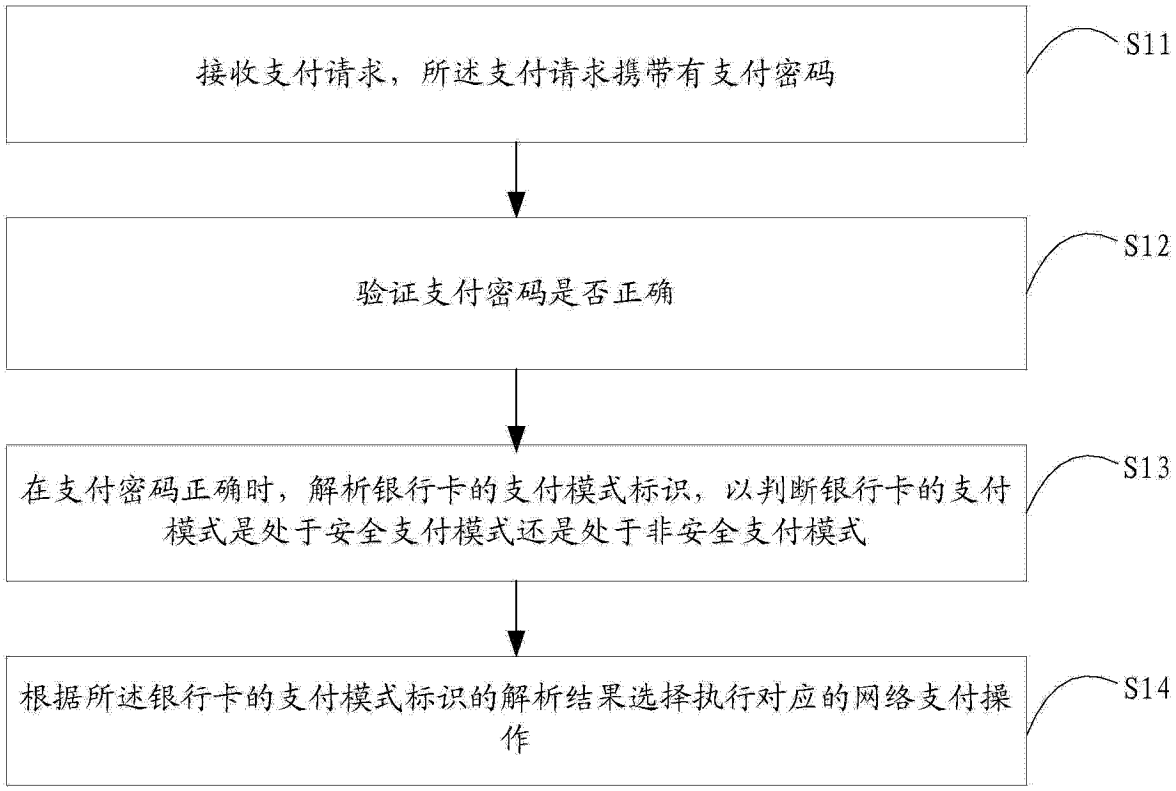

接收支付请求，所述支付请求携带有支付密码
S11
验证支付密码是否正确
S12
在支付密码正确时，解析银行卡的支付模式标识，以判断银行卡的支付模式是处于安全支付模式还是处于非安全支付模式
S13
根据所述银行卡的支付模式标识的解析结果选择执行对应的网络支付操作
S14

图 1

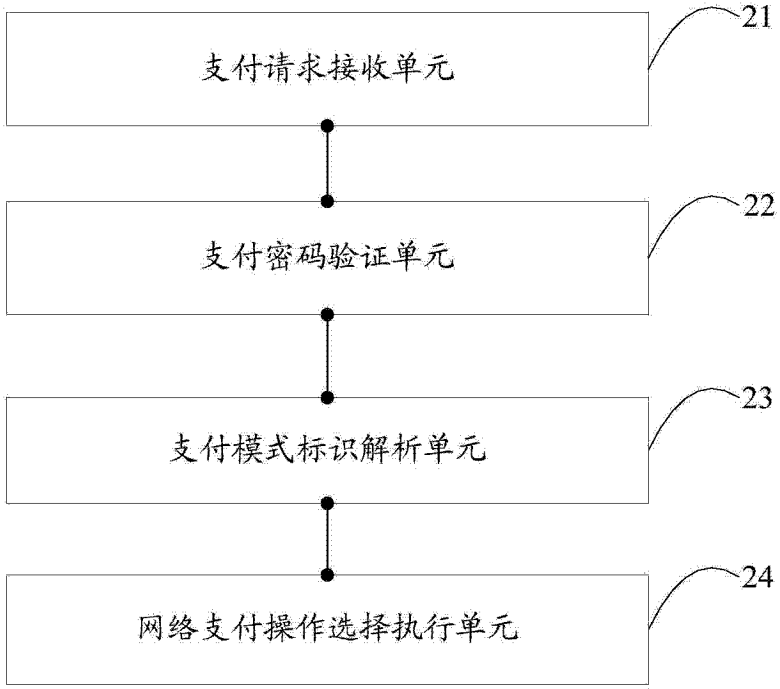

支付请求接收单元
21
支付密码验证单元
22
支付模式标识解析单元
23
网络支付操作选择执行单元
24

图 2