(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 103065240 A
(43)申请公布日 2013.04.24

(21)申请号 201310010304.1

(22)申请日 2013.01.11

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部

(72)发明人 滕志猛 周苏静 张世伟

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 田红娟 龙洪

(51)Int.Cl.
G06Q 20/02(2012.01)

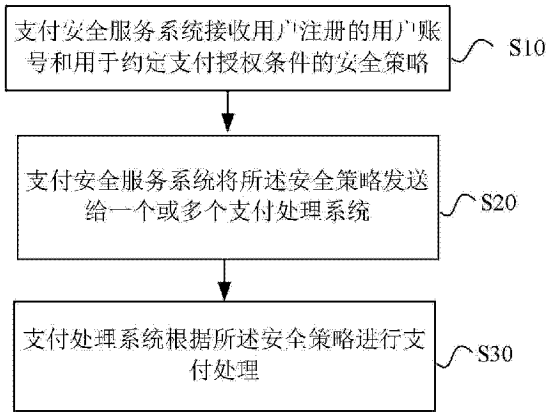
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种移动支付处理方法和系统

(57)摘要

本发明提供一种移动支付处理方法及系统，该方法包括：支付安全服务系统接收用户注册的用户账号和用于约定支付授权条件的安全策略；所述支付安全服务系统将所述安全策略发送给一个或多个支付处理系统；所述支付处理系统根据所述安全策略进行支付处理。本发明通过在第三方支付安全服务系统处注册安全策略，能够统一用户在多个支付处理系统的支付安全策略，保障用户进行移动支付的安全和便利性。



CN 103065240 A

1. 一种移动支付处理方法，包括：

支付安全服务系统接收用户注册的用户账号和用于约定支付授权条件的安全策略；

所述支付安全服务系统将所述安全策略发送给一个或多个支付处理系统；

所述支付处理系统根据所述安全策略进行支付处理。

2. 如权利要求 1 所述的方法，其特征在于：所述安全策略包括以下支付安全参数中的一个或多个：

支付额度、支付请求时间范围、支付请求发起频率、支付请求发起地点。

3. 如权利要求 2 所述的方法，其特征在于：所述安全策略还包括：

一个或多个授权终端号码，所述支付授权终端号码用来标识授权请求的接收方和授权请求响应的发送方。

4. 如权利要求 3 所述的方法，其特征在于：所述支付处理系统根据所述安全策略进行支付处理包括：

所述支付处理系统如判断用户的支付请求不满足所述支付安全参数，则向所述授权终端号码发送授权请求。

5. 一种支付安全服务系统，包括：

第一模块，接收用户注册的用户账号和用于约定支付授权条件的安全策略；

第二模块，用于将所述安全策略发送给一个或多个支付处理系统。

6. 如权利要求 5 所述的支付安全服务系统，其特征在于：所述安全策略包括以下一个或多个支付安全参数：

支付额度、支付请求时间范围、支付请求发起频率、支付请求发起地点。

7. 如权利要求 6 所述的支付安全服务系统，其特征在于：所述安全策略还包括：

一个或多个授权终端号码，所述支付授权终端号码用来标识授权请求的接收方和授权请求响应的发送方。

8. 一种支付处理系统，包括：

第一模块，用于接收支付安全服务系统下发的安全策略；

第二模块，用于根据所述安全策略进行支付处理。

9. 如权利要求 8 所述的支付处理系统，其特征在于：所述安全策略包括一个或多个授权终端号码和 / 或以下支付安全参数中的一个或多个：

支付额度、支付请求时间范围、支付请求发起频率、支付请求发起地点。

10. 如权利要求 9 所述的支付处理系统，其特征在于：所述第二模块包括：

第一单元，用于接收到用户的支付请求后，判断所述支付请求是否满足所述支付安全参数；

第二单元，用于在所述第一单元判断不满足所述支付安全参数的情况下，向所述授权终端号码发送授权请求。

一种移动支付处理方法和系统

技术领域

[0001] 本发明涉及信息技术领域，尤其涉及信息技术领域中的移动支付处理方法和系统。

背景技术

[0002] 移动支付是通过移动终端设备进行的金融活动。随着智能手机的普及和移动支付的便捷性，移动支付开始成为市场热点。但是支付的安全性始终是影响移动支付普及的重要因素。

[0003] 目前有很多针对保障移动支付的安全性的解决方案。例如一种现有技术要求用户事先注册一个移动终端号码，用户请求支付时，支付系统将支付链接发送到用户预注册的移动终端上，用户从这个移动终端点击链接，输入支付密码，完成支付。

[0004] 另一种现有技术在用户从一个终端发出支付请求时，远端接收支付请求的服务器首先发送一个一次性授权确认码给用户预注册的移动终端，用户从发出支付请求的终端输入授权确认码，完成支付。

[0005] 还有一种现有技术允许用户分别设置单笔消费、日消费、月消费的额度，当来自用户的支付请求超出额度时不允许交易，以此保护用户的支付安全。

[0006] 还有一种现有技术允许用户预先设置一个和用户用以移动支付的终端不同的密保手机号码，当用户忘记支付密码时，通过密保手机找回或重设密码，减少用户移动支付终端丢失和用户支付密码过于简单可能带来的安全隐患。

[0007] 这些技术都是针对同一个支付系统设置的，而随着第三方支付商和银行、移动运营商等机构的积极介入，用户面对大量的移动支付系统，分别注册、配置必然会给用户带来一些使用上的不便。

发明内容

[0008] 本发明要解决的技术问题是提供一种移动支付处理方法及系统，以统一用户在多个支付处理系统的支付安全策略，增加用户使用移动支付时的便利性，增强移动支付的安全性。

[0009] 为了解决上述技术问题，本发明提供了一种移动支付处理方法，包括：

[0010] 支付安全服务系统接收用户注册的用户账号和用于约定支付授权条件的安全策略；

[0011] 所述支付安全服务系统将所述安全策略发送给一个或多个支付处理系统；

[0012] 所述支付处理系统根据所述安全策略进行支付处理。

[0013] 进一步地，上述方法还具有下面特点：所述安全策略包括以下支付安全参数中的一个或多个：

[0014] 支付额度、支付请求时间范围、支付请求发起频率、支付请求发起地点。

[0015] 进一步地，上述方法还具有下面特点：所述安全策略还包括：

[0016] 一个或多个授权终端号码，所述支付授权终端号码用来标识授权请求的接收方和授权请求响应的发送方。

[0017] 进一步地，上述方法还具有下面特点：所述支付处理系统根据所述安全策略进行支付处理包括：

[0018] 所述支付处理系统如判断用户的支付请求不满足所述支付安全参数，则向所述授权终端号码发送授权请求。

[0019] 为了解决上述问题，本发明还提供了一种支付安全服务系统，包括：

[0020] 第一模块，接收用户注册的用户账号和用于约定支付授权条件的安全策略；

[0021] 第二模块，用于将所述安全策略发送给一个或多个支付处理系统。

[0022] 进一步地，上述系统还具有下面特点：所述安全策略包括以下一个或多个支付安全参数：

[0023] 支付额度、支付请求时间范围、支付请求发起频率、支付请求发起地点。

[0024] 进一步地，上述系统还具有下面特点：所述安全策略还包括：

[0025] 一个或多个授权终端号码，所述支付授权终端号码用来标识授权请求的接收方和授权请求响应的发送方。

[0026] 为了解决上述问题，本发明还提供了一种支付处理系统，包括：

[0027] 第一模块，用于接收支付安全服务系统下发的安全策略；

[0028] 第二模块，用于根据所述安全策略进行支付处理。

[0029] 进一步地，上述系统还具有下面特点：所述安全策略包括一个或多个授权终端号码和/或以下支付安全参数中的一个或多个：

[0030] 支付额度、支付请求时间范围、支付请求发起频率、支付请求发起地点。

[0031] 进一步地，上述系统还具有下面特点：所述第二模块包括：

[0032] 第一单元，用于接收到用户的支付请求后，判断所述支付请求是否满足所述支付安全参数；

[0033] 第二单元，用于在所述第一单元判断不满足所述支付安全参数的情况下，向所述授权终端号码发送授权请求。

[0034] 本发明提供一种移动支付处理方法及系统，通过在第三方支付安全服务系统处注册安全策略，能够统一用户在多个支付处理系统的支付安全策略，保障用户进行移动支付的安全和便利性。

附图说明

[0035] 图 1 为本发明实施例的支付安全服务系统的示意图；

[0036] 图 2 为本发明实施例的支付处理系统的示意图；

[0037] 图 3 为本发明实施例的一种移动支付处理方法的流程图；

[0038] 图 4 为本发明一应用示例的支付系统的示意图。

具体实施方式

[0039] 为使本发明的目的、技术方案和优点更加清楚明白，下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中

的特征可以相互任意组合。

[0040] 为了更好地理解本发明，下面结合附图和具体实施例对本发明作进一步地描述。

[0041] 图 1 为本发明实施例的支付安全服务系统的示意图，如图 1 所示，本实施例的支付安全服务系统包括：

[0042] 第一模块，接收用户注册的用户账号和用于约定支付授权条件的安全策略；

[0043] 第二模块，用于将所述安全策略发送给一个或多个支付处理系统。

[0044] 其中，所述安全策略包括以下一个或多个支付安全参数：

[0045] 支付额度、支付请求时间范围、支付请求发起频率、支付请求发起地点。

[0046] 其中，所述安全策略还可以包括：

[0047] 一个或多个授权终端号码，所述支付授权终端号码用来标识授权请求的接收方和授权请求响应的发送方。

[0048] 图 2 为本发明实施例的支付处理系统的示意图，如图 2 所示，本实施例的支付处理系统包括：

[0049] 第一模块，用于接收支付安全服务系统下发的安全策略；

[0050] 第二模块，用于根据所述安全策略进行支付处理。

[0051] 其中，所述第二模块包括：

[0052] 第一单元，用于接收到用户的支付请求后，判断所述支付请求是否满足所述支付安全参数；

[0053] 第二单元，用于在所述第一单元判断不满足所述支付安全参数的情况下，向所述授权终端号码发送授权请求。

[0054] 图 3 为本发明实施例的一种移动支付处理方法的流程图，如图 3 所示，本实施例的方法包括以下步骤：

[0055] S10、支付安全服务系统接收用户注册的用户账号和用于约定支付授权条件的安全策略；

[0056] S20、支付安全服务系统将所述安全策略发送给一个或多个支付处理系统；

[0057] S30、支付处理系统根据所述安全策略进行支付处理。

[0058] 本发明实施例通过在第三方支付安全服务系统处注册安全策略，能够统一用户在多个支付处理系统的支付安全策略，保障用户进行移动支付的安全和便利性。

[0059] 图 4 为本发明一应用示例的支付系统的示意图，如图 4 所示，该系统包括支付安全服务系统 101，一个或多个支付处理系统 102，多个用户 103，多个用户授权终端 104，多个用户支付终端 105，多个商户 106。支付处理系统 102 和支付安全服务系统 101 是逻辑上的区分，不排除两者合二为一的场景。

[0060] 所述移动支付方法包括如下步骤：

[0061] 步骤 S110：用户 103 在支付安全服务系统 101 处注册一个用户账号和安全策略，至少包括支付安全参数，还可可以包括授权终端号码；

[0062] 支付安全参数用来约定支付处理系统 102 触发授权请求的条件，例如，当支付金额超过某个额度时，或支付频率超过某个次数时，或支付请求时间在允许的某个时间范围之外时，等等。授权终端号码用来指定授权请求的接收方和授权请求响应的发送方。如果安全策略不包括授权终端号码，授权请求的接收方和授权请求响应的发送方由支付处理系

统 102 按照其他约定指定；

[0063] 步骤 S111：或者自发地，或者应支付处理系统 102 的请求，支付安全服务提供商 101 向支付处理系统 102 下发用户的安全策略；

[0064] 步骤 S112：用户 103 在商户 106 处下交易订单，商户 106 将支付请求发送给支付处理系统 102；

[0065] 步骤 S113：支付处理系统 102 根据用户的安全策略，向用户授权终端 104 发送授权请求，用户授权终端 104 返回授权请求响应；

[0066] 步骤 S114：如果支付处理系统 102 收到来自用户授权终端 104 的授权请求响应是允许授权，就和用户支付终端 105 进行支付流程，如对用户进行认证，支付处理，支付处理结果反馈；支付处理系统 102 还可把支付处理结果反馈给商户 106；

[0067] 步骤 S115：商户 106 通知用户支付终端 105 订单的支付处理结果，或者反过来。

[0068] 用户在支付安全服务系统 101 处注册支付安全参数，除了常规的单笔消费额度、日消费额度、月消费额度的配置，用户还可配置支付请求时间范围、支付请求发起频率、支付请求发起地点等。

[0069] 所述支付请求时间范围可以是用户允许支付请求发起的时间范围，也可以是不允许支付请求发起的时间范围，时间范围的设定实例包括按小时设定，如每天几点到几点，按日期设定，如设定为某一天到某一天，或按小时和按日期的结合。

[0070] 所述支付请求发起频率是某个时间段内支付请求发起的次数，可以是每小时、每天、每月发起的支付请求次数。

[0071] 所述支付请求发起地点包括用户支付终端 105 和 / 或商户 106 的网络地址、地理位置等。网络地址、地理位置可以是确定的地址，也可以是地址范围。实施例包括设定用户支付终端 105 的网络接口物理地址（MAC 地址）或互联网协议地址（IP 地址）；商户 106 的 IP 地址范围为某个国家境内。

[0072] 当支付请求涉及的金额在允许的额度之外时，和 / 或支付请求发生在不被允许的时间范围内时，和 / 或支付请求的频率超出设定频率时，和 / 或支付请求发起的地点在允许的地点之外时，支付处理系统 102 触发授权请求的发送，请求授权终端号码予以授权。

[0073] 本发明应用场景实例，例如未成年人进行移动支付，其监护人可以为其设定支付安全参数，还可以把自己的移动终端号码设定为授权终端号码，当未成年人进行的支付请求在设定的支付安全参数以外时，监护人收到支付处理系统发送的授权请求，从而监控未成年人的异常支付情况。本发明还可用于其他需要授权的移动支付场景。

[0074] 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块 / 单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

[0075] 以上仅为本发明的优选实施例，当然，本发明还可有其他多种实施例，在不背离本发明精神及其实质的情况下，熟悉本领域的技术人员当可根据本发明作出各种相应的改变和变形，但这些相应的改变和变形都应属于本发明所附的权利要求的保护范围。

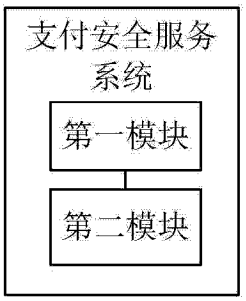

支付安全服务系统
第一模块
第二模块

图 1

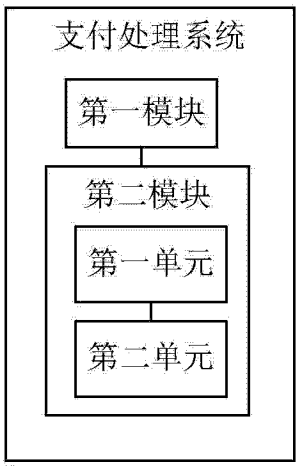

支付处理系统
第一模块
第二模块
第一单元
第二单元

图 2

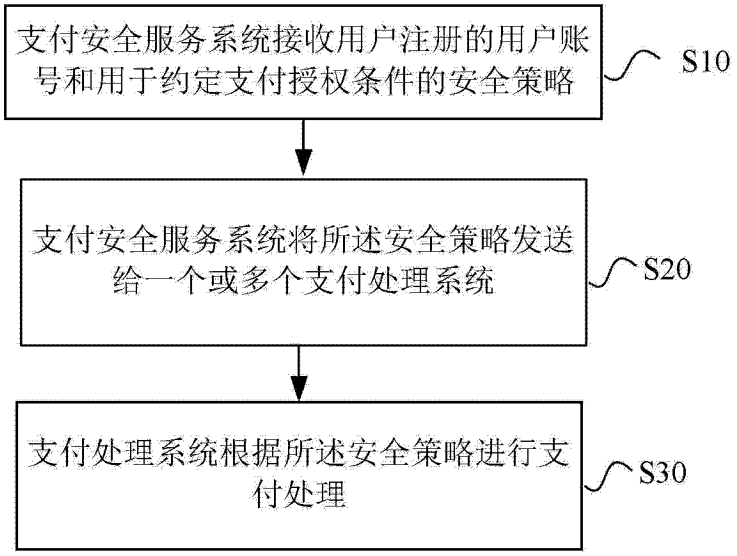

支付安全服务系统接收用户注册的用户账号和用于约定支付授权条件的安全策略
S10
支付安全服务系统将所述安全策略发送给一个或多个支付处理系统
S20
支付处理系统根据所述安全策略进行支付处理
S30

图 3

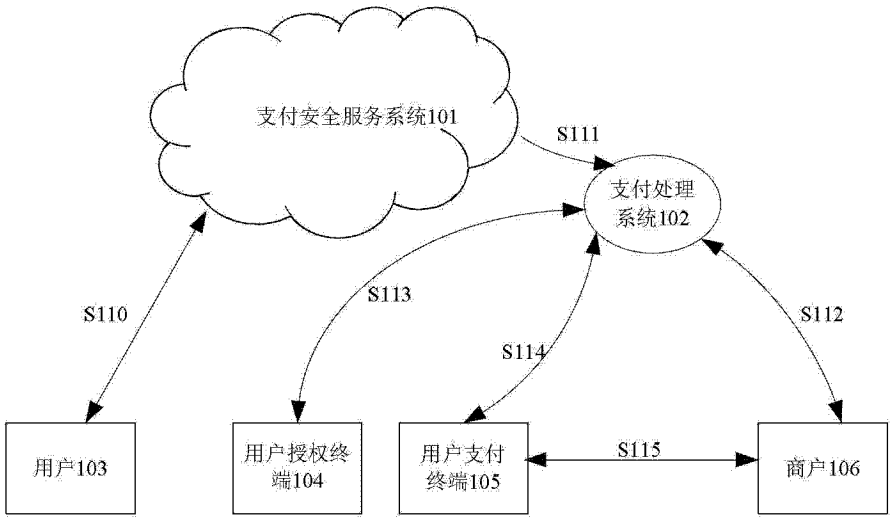

支付安全服务系统101
S111
支付处理系统102
S110
S113
S114
S112
用户103
用户授权终端104
用户支付终端105
S115
商户106

图 4