(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 106251148 A
(43)申请公布日 2016.12.21

(21)申请号 201610679621.6

(22)申请日 2016.08.12

(71)申请人 闻进
地址 210018 江苏省南京市玄武区兰园28号5幢102室

(72)发明人 闻进

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)

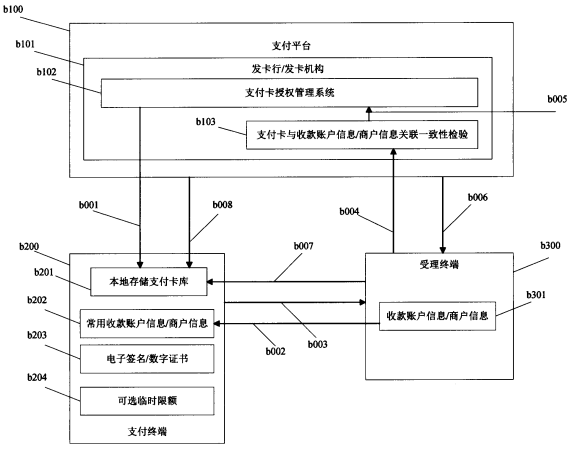
权利要求书1页 说明书3页 附图2页

(54)发明名称

一种交互式获取受理终端信息并关联支付卡信息的安全支付方法

(57)摘要

本发明涉及一种在现有支付系统基础上，通过支付终端与受理终端间交互式获取信息，支付终端获取受理终端上的收款账户信息/商户信息，商户信息至少包含商户号、终端号，并将获取的收款账户信息/商户信息与支付卡信息相关联，并与电子签名/数字证书一起生成用于支付的支付密文，生成的支付密文被限制在合理有效时间内只能在关联了收款账户信息/商户信息的特定受理终端获取使用，使得在合理有效时间内任何盗取支付密文挪作它用的企图失效，同时支付终端从受理终端获取支付授权反馈信息用于更新支付终端本地存储的支付卡库。



CN 106251148 A

1.一种交互式获取受理终端信息并关联支付卡信息的安全支付方法,包括:

支付终端与受理终端间交互式获取信息,支付终端获取受理终端上的收款账户信息/商户信息,商户信息至少包含商户号、终端号,并将获取的收款账户信息/商户信息与支付卡信息相关联,并与电子签名/数字证书一起生成用于支付的支付密文,生成的支付密文被限制在合理有效时间内只能在关联了收款账户信息/商户信息的特定受理终端获取使用,同时支付终端从受理终端获取支付授权反馈信息用于更新支付终端本地存储的支付卡库。

2.如权利要求1所述的方法,其特征在于:通过支付终端与受理终端间交互方式,支付终端从受理终端获取收款账户信息/商户信息,商户信息至少包含商户号、终端号。

3.如权利要求1所述的方法,其特征在于:获取的收款账户信息/商户信息与支付卡信息相关联,并与电子签名/数字证书一起生成用于支付的支付密文,生成的支付密文被限制在合理有效时间内只能在关联了收款账户信息/商户信息的特定受理终端获取使用。

4.如权利要求1所述的方法,其特征在于:支付平台验证获取的限定了只能在特定收款账户信息/商户信息的特定受理终端使用的支付密文和提交此支付密文的受理终端是否一致。

5.如权利要求1所述方法,其特征在于:支付终端从受理终端获取反馈信息用于更新支付终端本地存储的支付卡库。

一种交互式获取受理终端信息并关联支付卡信息的安全支付方法

技术领域

[0001] 本发明涉及一种在现有支付系统基础上，通过支付终端与受理终端间交互式获取信息，支付终端获取受理终端上的收款账户信息/商户信息，商户信息至少包含商户号、终端号，并将其与支付卡信息相关联，生成用于支付的支付密文的安全支付方法，因生成的支付密文在合理有效时间内限制于只能在被关联的特定受理终端获取使用，使得在合理有效时间内任何盗取支付密文挪作它用的企图失效。

背景技术

[0002] 随着支付标记化的引入，主账号信息获得了安全保护，但用于现场交易支付的标记依然受到被盗取挪作它用的风险，如通过无线方式窃取磁性安全传输、RFID-skimming窃取NFC信息、侧摄盗取二维码/条码等。

发明内容

[0003] 本发明的目的就是为了解决上述问题，提供一种通过支付终端与受理终端间交互式获取信息，支付终端获取受理终端上的收款账户信息/商户信息，商户信息至少包含商户号、终端号，并将其与支付卡信息相关联，生成在合理有效时间内限制于只能在关联了收款账户信息/商户信息的特定受理终端获取使用的支付密文，同时支付终端从受理终端获取授权反馈信息更新支付终端本地存储的支付卡库的安全支付方法。

[0004] 本发明的技术方案包括以下步骤：

[0005] 场景一(如图1)，支付卡授权管理系统的支付卡安全控制域中包含收款账户信息/商户信息，商户信息至少包含商户号、终端号的验证项，在支付平台的支付卡授权管理系统里实现支付卡与收款账户信息/商户信息的关联。

[0006] 通过支付终端与受理终端间交互方式，支付终端从受理终端获取收款账户信息/商户信息，商户信息至少包含商户号、终端号，支付终端向支付平台的支付卡授权管理系统申请支付卡，并将获取的受理终端的收款账户信息/商户信息提交到支付卡安全控制域的收款账户信息/商户信息的验证项中，支付平台的支付卡授权管理系统生成需要验证收款账户信息/商户信息的支付卡，分发给支付终端，支付终端将从支付卡授权管理系统分发的需要验证收款账户信息/商户信息的支付卡资料保存在支付终端的本地储存支付卡库，支付终端将支付卡和电子签名/数字证书一起生成支付密文提交给受理终端，受理终端在从支付终端获取支付密文后结合其他信息一起提交给支付平台的支付卡授权管理系统进行授权，支付卡授权管理系统在接收到受理终端提交的支付密文后，验证支付密文是否满足支付卡安全控制域的收款账户信息/商户信息的限制要求和其他授权相关要素的要求，如果都满足授权要求就授权支付许可，如果不满足授权要求就拒绝授权许可，同时反馈相关信息给受理终端，支付终端从受理终端获取授权与否的反馈信息，或者从支付平台获取反馈信息，同时更新本地存储支付卡库。

[0007] 场景二(如图2),在支付终端实现支付卡与收款账户信息/商户信息的关联。

[0008] 通过支付终端与受理终端间交互方式,支付终端从支付平台的支付卡授权管理系统获取支付卡信息,并保存在支付终端的本地存储支付卡库,支付终端从受理终端获取收款账户信息/商户信息,商户信息至少包含商户号、终端号,保存在支付终端的常用收款账户信息/商户信息单元中,支付终端将从受理终端获取的收款账户信息/商户信息和用于本次支付的支付卡信息相关联,作为限制支付卡使用限制范围的安全验证要素,限制了与获取的收款账户信息/商户信息相关联的支付卡只能在被限制的受理终端的合理有效时间内使用,支付终端将相关的支付卡、收款账户信息/商户信息、电子签名/数字证书和可选临时限额一起生成支付密文,受理终端获取支付终端提交的支付密文后,向支付平台申请支付授权,支付平台在接收到受理终端提交的支付密文后,首先验证受到限制只能在相关联的特定收款账户信息/商户信息的受理终端上使用的支付卡和提交授权申请的受理终端是否一致,如果不一致就拒绝授权,如果一致就进入支付卡授权管理系统执行后续授权步骤,同时反馈相关信息给受理终端,支付终端从受理终端获取授权与否的反馈信息,或者从支付平台获取反馈信息,同时更新本地存储支付卡库。

附图说明

[0009] 图1是本发明的场景一的简化流程图。

[0010] 图2是本发明的场景二的简化流程图。

具体实施方式

[0011] 下面结合附图和实施例对本发明作进一步的描述。

[0012] 以二维码支付为例,场景一:

[0013] 步骤a001:支付终端(a200)读取受理终端(a300)上含有收款账户信息/商户信息(a301)的二维码,商户信息至少包含商户号、终端号。

[0014] 步骤a002:支付终端(a200)将获取的收款账户信息/商户信息(a301)提交给支付卡授权管理系统(a102),设置支付卡安全控制域(a103)中的收款账户信息/商户信息。

[0015] 步骤a003:支付卡授权管理系统(a102)将生成的关联了受理终端(a300)上含有的收款账户信息/商户信息(a301),限制只能在特定收款账户信息/商户信息(a301)的受理终端(a300)上使用的支付卡分发给支付终端(a200),并保存在支付终端(a200)的本地存储支付卡库(a201)。

[0016] 步骤a004:支付终端(a200)将获取的支付卡和电子签名/数字证书(a202)一起生成支付密文,并在支付终端(a200)上以二维码呈现,由受理终端(a300)读取。

[0017] 步骤a005:受理终端将读取的支付密文提交给支付平台(a100)的支付卡授权管理系统(a102)申请支付授权,支付卡授权管理系统(a102)验证提交支付密文的受理终端(a300)和受限只能在相关联特定收款账户信息/商户信息的受理终端(a300)使用的支付卡密文的是否一致,及其他授权要素是否满足,决定是否授权支付。

[0018] 步骤a006:将是否授权支付的信息反馈给受理终端(a300)。

[0019] 步骤a007:支付终端(a200)读取受理终端(a300)上以二维码呈现的是否授权支付的反馈信息,更新支付终端(a200)的本地存储支付卡库(a201)。

[0020] 步骤a008:支付终端(a200)从支付平台获取是否授权支付的反馈信息,更新支付终端(a200)的本地存储支付卡库(a201)。

[0021] 步骤a001、步骤a004、步骤a007,支持支付终端(a200)与支付平台(a100)的脱机状态下的使用。

[0022] 以二维码支付为例,场景二:

[0023] 步骤b001:支付终端(b200)从支付平台(b100)的支付卡授权管理系统(b102)申请获得支付卡,并将申请获得的支付卡保存在支付终端(b200)的本地存储支付卡库(b201)。

[0024] 步骤b002:支付终端(b200)读取受理终端(b300)上含有收款账户信息/商户信息(b301)的二维码,商户信息至少包含商户号、终端号,并保存更新支付终端(b200)的常用收款账号信息/商户信息(b202)。

[0025] 步骤b003:支付终端(b200)选取本地存储支付卡库里的支付卡,将选取的支付卡与获取的收款账户信息/商户信息相关联,从而限制被选取的支付卡只能在合理的有效时间内在特定的收款账户信息/商户信息的受理终端上使用,同时和支付终端(b200)的电子签名/数字证书(b203)、可选临时限额(b204)一起生成支付密文,并在支付终端(a200)上以二维码呈现,由受理终端(b300)读取。

[0026] 步骤b004:受理终端(b300)获取支付终端(b200)的支付密文后向支付平台(b100)提交支付授权申请,支付平台(b100)首先由支付卡与收款账户信息/商户信息关联一致性检验(b103)模块检查验证受理终端(b300)提交的支付密文中支付卡关联的特定收款账户信息/商户信息和提交支付密文的受理终端(b300)所属收款账户信息/商户信息(b301)是否一致,如果一致执行后续授权步骤(b005),如果不一致则拒绝支付授权并反馈信息。

[0027] 步骤b005:如果支付卡与收款账户信息/商户信息关联一致性检验通过,则由支付卡授权管理系统执行后续支付授权相关步骤。

[0028] 步骤b006:由支付平台(b100)将是否支付授权的信息反馈给受理终端(b300)。

[0029] 步骤b007:支付终端(b200)读取受理终端(b300)上以二维码呈现的反馈信息,并更新支付终端(b200)的本地存储支付卡库(b201)。

[0030] 步骤b008:从支付平台(b100)获取反馈信息,并更新支付终端(b200)的本地存储支付卡库(b201)。

[0031] 步骤b002、步骤b003、步骤b007,支持支付终端(b200)与支付平台(b100)在脱机状态下的使用。

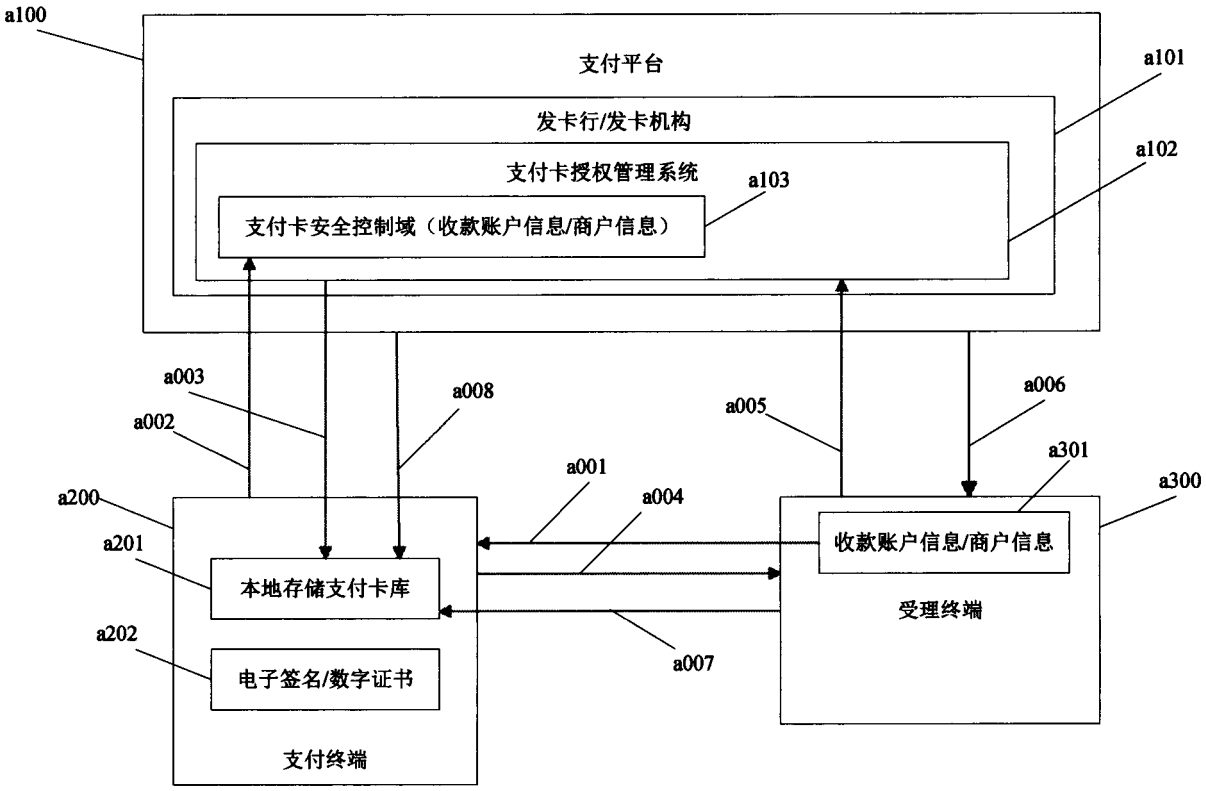

a100
支付平台
a101
发卡行/发卡机构
a102
支付卡授权管理系统
a103
支付卡安全控制域（收款账户信息/商户信息）
a003
a002
a008
a005
a006
a301
a300
a001
a004
a200
a201
本地存储支付卡库
收款账户信息/商户信息
受理终端
a202
电子签名/数字证书
a007
支付终端

图1

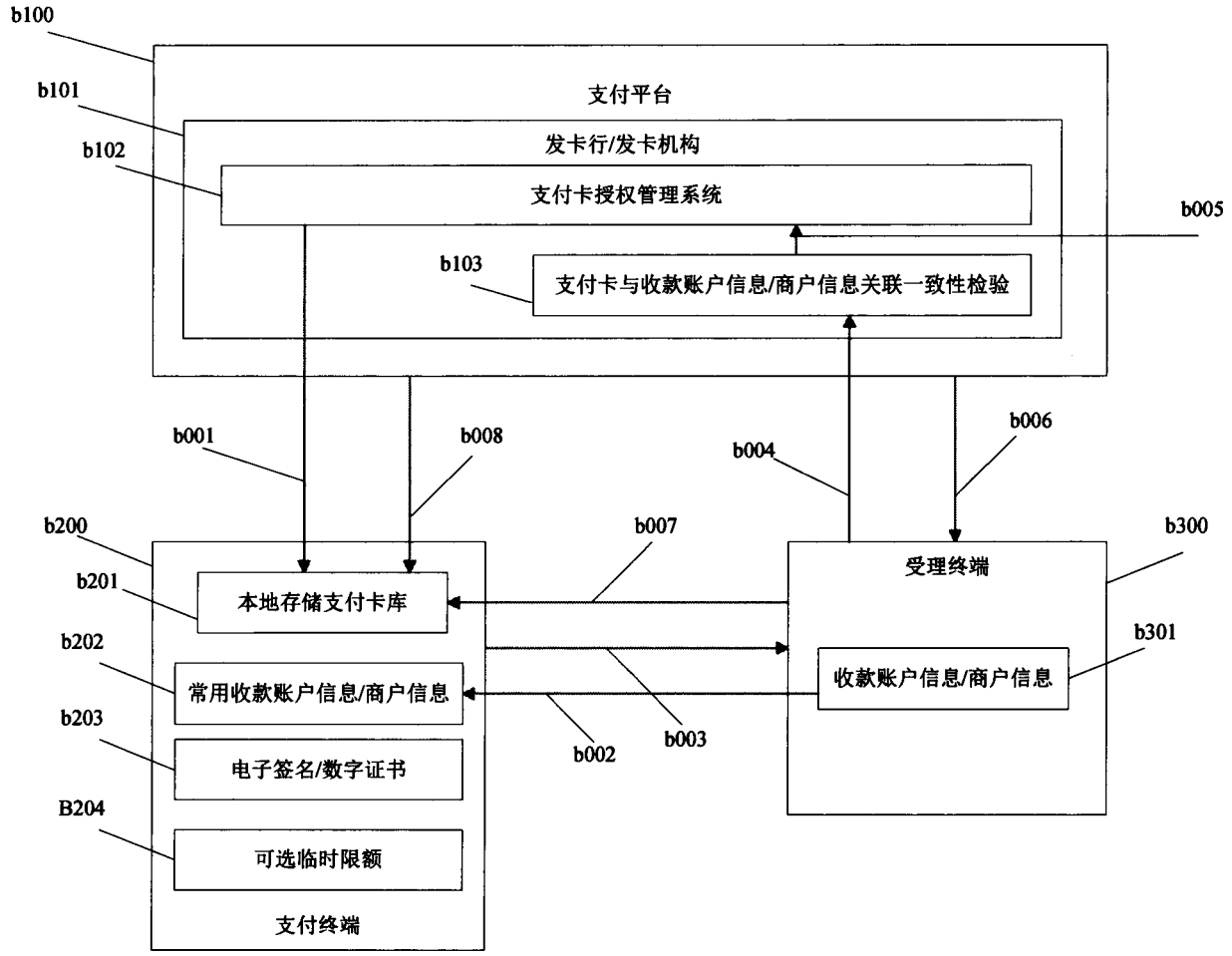

b100
支付平台
b101
发卡行/发卡机构
b102
支付卡授权管理系统
b005
b103
支付卡与收款账户信息/商户信息关联一致性检验
b001
b008
b004
b006
b200
b007
b300
受理终端
b201
本地存储支付卡库
b202
常用收款账户信息/商户信息
b301
收款账户信息/商户信息
b203
电子签名/数字证书
b002
b003
B204
可选临时限额
支付终端

图2