

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(43) 国际公布日
2010 年 12 月 29 日 (29.12.2010)

PCT

(10) 国际公布号
WO 2010/148646 A1

- (51) 国际专利分类号:
G06Q 20/00 (2006.01) G06Q 30/00 (2006.01)
- (21) 国际申请号: PCT/CN2010/000926
- (22) 国际申请日: 2010 年 6 月 24 日 (24.06.2010)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
200910053763.1 2009 年 6 月 25 日 (25.06.2009) CN
- (71) 申请人 (对除美国外的所有指定国): 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。
- (72) 发明人: 及
- (75) 发明人/申请人 (仅对美国): 陈贤强 (CHEN, Xian-qiang) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。
- (74) 代理人: 中国专利代理 (香港) 有限公司 (CHINA PATENT AGENT (H.K.) LTD); 中国香港特别行政区湾仔港湾道 23 号鹰君中心 22 号楼, Hong Kong (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。
- 本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) Title: METHOD FOR SAFELY AND AUTOMATICALLY DOWNLOADING TERMINAL MASTER KEY IN BANK CARD PAYMENT SYSTEM AND THE SYSTEM THEREOF

(54) 发明名称: 一种银行卡支付系统中主密钥安全自动下载的方法及其系统

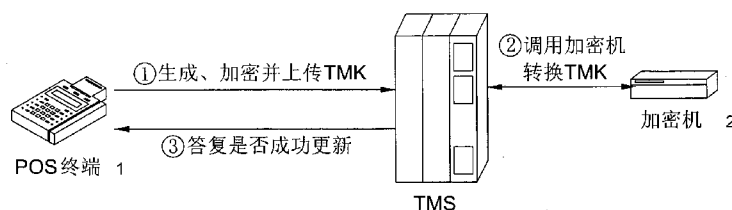


图 3 / Fig. 3

- 1 POS TERMINAL
2 SECURITY MODULE
① CREATE ENCRYPT AND UPLOAD TMK
② SECURITY MODULE IS CALLED TO CONVERT TMK
③ WETHER UPDATING IS SUCCESSFUL OR NOT IS ANSWERED

(57) Abstract: A method for safely and automatically downloading terminal master key (TMK) in bank card payment system and the system thereof are provided. The bank card payment system includes a point of sale (POS) terminal, a terminal manage system (TMS), a pin pad and a hardware and security module. A couple of public and private keys are created after the security module is called by the TMS, and then the TMK is created after the pin pad is called by the POS terminal. The TMK is encrypted with the TMS's public key and then is uploaded to the TMS. The TMK is decrypted with the private key after the security module is called by the TMS and then is stored.

[见续页]

WO 2010/148646 A1



(57) 摘要:

一种银行卡支付系统中主密钥(TMK)安全自动下载的方法及其系统,银行卡支付系统包括销售点(POS)终端,终端管理系统(TMS),密码键盘和硬件加密机。TMS 调用加密机产生一对公私密钥,POS 终端调用密码键盘随即生成 TMK,并用 TMS 的公钥进行加密后上传给 TMS,TMS 调用加密机并用私钥解密 TMK 后存储。

一种银行卡支付系统中主密钥安全自动下载的方法及其系统

技术领域

本发明涉及银行卡支付系统，尤其涉及银行卡支付系统中主密钥的安全保护方式。

背景技术

银行卡（Bank Card）作为支付工具越来越普及，通常的银行卡支付系统，包括销售点终端（Point Of Sale: POS），终端管理系统（Terminal Manage System: TMS），密码键盘（PIN PAD）和硬件加密机（Hardware and Security Module: HSM）。

其中 POS 终端能够接受银行卡信息，具有通讯功能，并接受柜员的指令而完成金融交易信息和有关信息交换的设备；TMS 系统对属下的 POS 终端进行集中管理，包括参数下载，密钥下载，接受、处理或转发 POS 终端的交易请求，并向 POS 终端回送交易结果信息的集中管理及交易处理系统；密码键盘（PIN PAD）是对 TMK、PIK 和 MAK 进行安全存储保护，以及对 PIN 进行加密保护的安全设备；硬件加密机（Hardware and Security Module: HSM）是对传输的数据进行加密的外围硬件设备，用于 PIN 的加密和解密、验证报文和文件来源的正确性以及存储密钥。个人标识码（Personal Identification Number; PIN），即个人密码，是在联机交易中识别持卡人身份合法性的数据信息，在计算机和网络系统中任何环节都不允许 PIN 以明文的方式出现；终端主密钥（Terminal Master Key; TMK）：POS 终端工作时，对工作密钥进行加密的主密钥，保存在系统硬件中，只能使用，不能读取；工作密钥（working key; WK），也称为数据密钥，通常包括 PIN 加密密钥（简称 PIK）和报文鉴别 MAC 计算的密钥（简称

MAK), 工作密钥必须经常更新, 在联机更新的报文中用终端主密钥(TMK) 对工作密钥进行加密, 形成密文后再进行传输。

POS 终端广泛应用于银行卡支付场合, 比如商场购物、酒店授权等, 是一种不可或缺的现代化支付手段, 已经融入人们的正常生活。银行卡(特别是借记卡)一般都由持卡人设置了 PIN, 在进行支付过程中, POS 终端除了上送银行卡的磁道信息等资料之外, 还要求持卡人输入 PIN 供发卡银行验证持卡人身份合法性, 以确保银行卡支付安全, 保护持卡人的财产安全。为了防止 PIN 泄露或被破解, 要求从终端到发卡银行整个信息交互过程中, 全程对 PIN 进行安全加密保护, 不允许在计算机和网络系统中的任何环节, PIN 以明文的方式出现。为此, 目前能接受输入 PIN 的 POS 终端都要求配备密钥管理体系。

POS 终端的密钥体系分成二级: 终端主密钥(TMK)和工作密钥(WK)。其中 TMK 在 WK 更新的过程中对 WK 进行加密保护, 每台 POS 终端与 TMS 之间共享唯一的 TMK, 必须要有安全保护措施, 保证只能写入硬件设备并参与运算, 不能被读取; WK 包括用于对 PIN 加密的 PIK 和进行报文鉴别(MAC)的 MAK 两部分, 均由 TMS 调用加密机产生, 在 POS 终端向 TMS 签到时下载, 并利用 TMK 加密传输和存储, 其加密算法都是使用安全级别很高的 3DES 算法。具体工作密钥下载流程如图 1 所示:

POS 终端向 TMS 发起签到请求;

TMS 调用加密机随机生成用 TMK 加密的 PIK 和 MAK;

POS 终端接收从 TMS 返回的 PIK 和 MAK 密文, 并存入密码键盘。

在银行卡支付过程中, 通过键盘输入时, 由密码键盘利用 PIK 对持卡人输入的 PIN 进行加密之后上送给 TMS, 然后 TMS 再对加密后的 PIN 通过调用加密机进行转换之后转发给发卡银行进行授权处理, 整个传输过程中确保 PIN 都是利用硬件进行加密保护, 其加密使用的 3DES 加密算法也

是目前为止应用广泛安全级别很高的加密算法之一,通常应用在金融行业。

从上面的工作密钥下载过程中可以看出, TMK 是一个很关键的根密钥。如果 TMK 被截取, PIK、MAK 甚至 PIN 都可以利用 3DES 算法进行破解, 将严重威胁银行卡支付安全。所以, TMK 能否安全下载到 POS 终端, 也就成为一个密码安全保护的关键步骤。下面我们把目前现有的 TMK 下载方法归纳如下:

由 TMS 生成 TMK 明文, 手工方式直接输入到 POS 终端的密码键盘。这种方式存在很大的安全漏洞, 具体操作人员很容易截取 TMK 明文, 并且, 还存在手工输入错误的可能性, 严重影响后续的工作密钥下载和 PIN 加密。

IC 卡明文导入, 由 TMS 生成 TMK 明文, 并写入 IC 卡, 由 POS 终端从 IC 卡中读取 TMK 明文存入密码键盘。这种方式也存在很大的安全漏洞, TMK 明文保存在 IC 卡中, 只要拿到 IC 卡读取器, 就可以轻易获取 TMK 明文, 严重影响后续的工作密钥下载和 PIN 加密。

IC 卡密文导入, 由 TMS 生成的 TMK 用指定密钥(简称传输密钥)加密后存入 IC 卡, POS 终端从 IC 卡中读取 TMK 密文后, 再利用存放了传输密钥的 IC 卡进行解密之后再导入密码键盘。这种方式是在 IC 卡明文输入的基础上增强了加密传输功能, 有所改进, 只有具备传输密钥 IC 卡的人员才能获取 TMK 明文, 减少了密钥在传输过程中存在的不安全因素。

母 POS 终端导入, TMS 生成的 TMK 密文, 经特制的 POS 终端(简称母 POS 终端)解密之后, 直接导入与母 POS 终端通过串口连接的 POS 终端, 减少了密钥导入过程中的不安全因素。这种方式的安全级别等同于 IC 卡密文导入方式, 但存在终端携带不方便、很难在商户的现场直接导入 TMK 等缺点。

综上所述, 对以上现有的 TMK 下载方法存在的主要缺点归纳如下:

手工输入方式存在人为失误的可能性。

明文输入存在严重的安全漏洞，也很容易被获取，特别是通过人工操作的人员。

IC 密文导入和母 POS 导入虽然部分解决了传输过程中的安全隐患，但是传输密钥 IC 卡和母 POS 的保管，以及携带环节仍然存在比较大的安全隐患。

以上所有 TMK 下载手段均需要人工干预直接操作 POS 终端，即需要技术支持人员到布放 POS 终端的现场才能完成下载任务，人工成本比较高，特别是在 POS 终端数量比较多、故障终端机比较严重的情况下。

发明内容

本发明的目的在于：提供一种主密钥安全自动下载的方法，解决主密钥下载过程中的安全隐患。

一种银行卡支付系统中主密钥 TMK 安全自动下载的方法，所述银行卡支付系统包括销售点终端 POS，终端管理系统 TMS，密码键盘和硬件加密机。TMS 调用加密机产生一对公私密钥，POS 终端调用密码键盘随机生成主密钥 TMK，并用 TMS 的公钥进行加密后上传给 TMS，TMS 调用加密机并用私钥解密 TMK 后存储。

进一步地，所述 TMS 调用加密机生成一对公私密钥，其中私钥在加密机中保存，公钥保存在 TMS 的数据库中，POS 终端发起公钥下载请求，并接收 TMS 返回的公钥，并将所述公钥存入密码键盘。

进一步地，TMS 接收到从 POS 终端传来的加密过的 TMK 后，由 TMS 调用加密机，利用私钥对 TMK 解密后将 TMK 明文直接存入加密机。当所述加密机不具有存储功能时，将 TMK 明文通过 TMS 预先设置的 3DES 密钥，对 TMK 进行加密后存储在 TMS 的数据库中。

进一步地，在 TMS 与 POS 终端的报文接口中定义一个 TMK 是否需要更新的标记，在正常情况下，所述标记设置为“无需更新”，当需要 POS 终端更新 TMK 时，只要 POS 终端向 TMS 发起任何请求，包括签到、交易等，则由 TMS 在报文接口中将“需要更新”标记设置在报文中，当 POS 终端在处理完 TMS 的正常应答之后，如果检测到“需要更新”的标记已经生效，则随后就会进行 TMK 的更新，完成 TMK 密钥的自动更新。TMS 完成 TMK 的解密和存储后，答复 POS 终端是否已经更新 TMK 成功。

本发明揭示了一种实现主密钥安全下载的银行卡支付系统，包括销售点终端 POS，终端管理系统 TMS，密码键盘和硬件加密机，所述的 TMS 调用加密机产生一对公私密钥，其中私钥在加密机中保存，公钥保存在 TMS 的数据库中。所述的密码键盘存储从 TMS 下载的公钥，所述密码键盘随机产生 TMK 主密钥并利用从 TMS 下载的公钥进行加密。所述的加密机将采用公钥加密的 TMK 用私钥解密后存储或者解密后转换成 3DES 加密并存储。

进一步地，在 TMS 与 POS 终端的报文接口中定义一个 TMK 是否需要更新的标记，当需要 POS 终端更新 TMK 时，只要 POS 终端向 TMS 发起任何请求，包括签到、交易等，则由 TMS 在报文接口中将“需要更新”标记设置在报文中，当 POS 终端在处理完 TMS 的正常应答之后，如果检测到“需要更新”的标记已经生效，则随后就会进行 TMK 的更新，完成 TMK 密钥的自动更新；其他正常使用情况下，所述标记定义为“无需更新”。

本发明 TMK 是随机产生的，传输过程也是封闭的，TMK 明文不会出现在安全存储设备（密码键盘和加密机）之外，在传输过程中都是利用公钥进行加密，TMK 密文在 TMS 的加密机中才能解开，由于这种非对称的加密算法的安全性很高，就算被截取到密文也很难破解，完全解决了现有 TMK 下载过程中存在的安全漏洞。

附图说明

图 1 为现有技术的工作密钥下载流程;

图 2 为本发明公钥下载流程;

图 3 为本发明 TMK 更新流程。

具体实施方式

为了解决上述现有 TMK 下载过程中存在的缺陷, 本发明提出了一种安全自动下载 TMK 的方法。对 TMK 的下载完全由 TMS 集中控制和管理, 与 POS 终端的数据交换自动完成, 在整个交换过程中, 无需人工干预, 既大大减少了人力成本, 同时也保证了 TMK 传输过程的安全可靠。

为了确保 TMK 的安全传输, 本方法中引入了公私密钥这种非对称加密算法。这种加密算法的思路是: 首先由 TMS 调用加密机产生一对公私密钥, 其中私钥保存在加密机中, 公钥保存在 TMS 的数据库中, 供 POS 终端下载, 下载流程示意如图 2 所示, 步骤如下:

TMS 调用加密机生成一对公私密钥, 其中私钥在加密机中保存, 公钥保存在 TMS 的数据库中;

POS 终端发起公钥下载请求;

POS 终端接收 TMS 返回的公钥, 并存入密码键盘。

在前面所述的 TMK 导入方法中, 都是由 TMS 生成 TMK, 利用一些加密手段传输到 POS 终端, 再由 POS 终端按照对应的解密手段获取 TMK 明文之后存入密码键盘, 不管加密手段如何先进, 都无法避免黑客或者内部人员根据同样的解密手段截取 TMK 明文。

在本文提出的设计方法中, 则是采用反向生成 TMK 的方法, 其具体过程是: TMK 由 POS 终端在密码键盘中随机生成, 利用前面下载的 TMS 公钥, 直接在密码键盘中完成加密之后上传给 TMS, 再由 TMS 调用加密

机，利用私钥对 TMK 解密后将 TMK 明文直接存入加密机，明文不会出现在加密机之外。对于不直接存储 TMK 的加密机，则通过 TMS 预先设置的 3DES 密钥，对 TMK 进行加密后存储在 TMS 的数据库中。经过这种转换处理之后，即可与现有的 POS 终端密钥管理体系衔接在一起，对后续的 PIK 和 MAK 更新、PIN 加密过程都是透明的，无需人工干预。这种方法的 TMK 更新流程如图 3 所示，具体步骤如下：

POS 终端调用密码键盘提供的指令随机生成 TMK，并用 TMS 的公钥进行加密后上传给 TMS；

TMS 调用加密机，用私钥解密 TMK 后存入加密机，对于不直接存储 TMK 的加密机，则用 TMS 预先设置的 3DES 密钥加密 TMK 后存储在 TMS 的数据库中，供后续的 PIK 和 MAK 交换使用；

TMS 答复 POS 终端是否已经更新 TMK 成功。

从上面的整个更新流程来看，TMK 是随机产生的，传输过程也是封闭的，TMK 明文不会出现在安全存储设备（密码键盘和加密机）之外，在传输过程中都是利用公钥进行加密，TMK 密文在 TMS 的加密机中才能解开，由于这种非对称的加密算法的安全性很高，就算被截取到密文也很难破解，完全解决了上述现有 TMK 下载过程中存在的安全漏洞。

为了实现这种随机产生 TMK 的更新流程，需要在现有的密码键盘上增加两个指令：

- 1) 存储从 TMS 下载的公钥；
- 2) 随机产生 TMK 密钥并利用从 TMS 下载的公钥进行加密。

对加密机来说，则需要增加一个指令：

将采用公钥加密的 TMK 用私钥解密后存储或者解密后转换成 3DES 加密并存储在 TMS 数据库中。

从本文介绍的 TMK 更新流程来看, TMK 的更新流程是由 POS 终端发起的, 为了实现其自动化管理的要求, 需要在 TMS 与 POS 终端的报文接口中定义一个 TMK 是否需要更新的标记, 即定义如下:

1) 无需更新

2) 需要更新

在正常情况下, 所述正常情况是指已经生成有 TMK, 系统正常使用中, 不需要更新 TMK 时, 该标记设置为“无需更新”。当需要 POS 终端更新 TMK 时, 比如对新安装的 POS 终端, 或者原有的 TMK 使用已经过期时, 只要 POS 终端向 TMS 发起任何请求, 包括签到、交易等, 则由 TMS 在报文接口中将“需要更新”标记设置在报文中, 当 POS 终端在处理完 TMS 的正常应答之后, 如果检测到“需要更新”的标记已经生效, 则随后就会自动触发 TMK 的更新流程, 完成 TMK 密钥的自动更新。由此看来整个 TMK 更新过程, 所有控制和管理都在 TMS 上完成, 不再需要人工干预和安排专业的技术支持人员到 POS 终端现场更新 TMK。如果在“无需更新”状态下, TMS 收到 POS 终端发起的更新 TMK 密钥的请求, 则直接拒绝, 以避免该 POS 终端的资料被复制或盗用到其他 POS 终端上使用。在 POS 终端发生故障并且确实需要更新 TMK 密钥的情况下, 则由 TMS 设置该 POS 终端的标记为“需要更新”, 让 POS 终端自动完成 TMK 更新流程。

本发明所介绍的 TMK 密钥安全自动下载方法, 只需要对现有的密码键盘和加密机中增加三个简单指令, 即可实现了 TMK 的自动化下载和安全管理要求, 既避免了现有 TMK 下载过程中存在的安全隐患, 又减少了人工干预, 是一种安全可靠、行之有效的方法。

这种方法的特点是: 利用了目前安全性很高, 且应用广泛的非对称加密算法, 不仅可以广泛应用到现有的 POS 终端, 也适用于其他存在类似密钥体系的自动终端, 比如 ATM 终端、缴费终端等, 具有很好的商用价值, 值得推广。

权 利 要 求

1. 一种银行卡支付系统中主密钥 TMK 安全自动下载的方法, 所述银行卡支付系统包括销售点终端 POS, 终端管理系统 TMS, 密码键盘和硬件加密机, 其特征在于: TMS 调用加密机产生一对公私密钥, POS 终端调用密码键盘随机生成主密钥 TMK, 并用 TMS 的公钥进行加密后上传给 TMS, TMS 调用加密机并用私钥解密 TMK 后存储。

2. 根据权利要求 1 所述的一种银行卡支付系统中主密钥 TMK 安全自动下载的方法, 其特征在于: TMS 调用加密机生成一对公私密钥, 其中私钥在加密机中保存, 公钥保存在 TMS 的数据库中。

3. 根据权利要求 1 所述的一种银行卡支付系统中主密钥 TMK 安全自动下载的方法, 其特征在于: POS 终端发起公钥下载请求, 并接收 TMS 返回的公钥, 并将所述公钥存入密码键盘。

4. 根据权利要求 1 所述的一种银行卡支付系统中主密钥 TMK 安全自动下载的方法, 其特征在于: TMS 接收到从 POS 终端传来的加密过的 TMK 后, 由 TMS 调用加密机, 利用私钥对 TMK 解密后将 TMK 明文直接存入加密机。

5. 根据权利要求 1 所述的一种银行卡支付系统中主密钥 TMK 安全自动下载的方法, 其特征在于: TMS 接收到从 POS 终端传来的加密过的 TMK 后, 由 TMS 调用加密机, 利用私钥对 TMK 解密后将 TMK 明文通过 TMS 预先设置的 3DES 密钥, 对 TMK 进行加密后存储在 TMS 的数据库中。

6. 根据权利要求 1 所述的一种银行卡支付系统中主密钥 TMK 安全自动下载的方法, 其特征在于: 在 TMS 与 POS 终端的报文接口中定义一个 TMK 是否需要更新的标记。

7. 根据权利要求 6 所述的一种银行卡支付系统中主密钥 TMK 安全自动下载的方法, 其特征在于: 当需要 POS 终端更新 TMK 时, 只要 POS 终

端向 TMS 发起任何请求，包括签到、交易等，则由 TMS 在报文接口中将“需要更新”标记设置在报文中，当 POS 终端在处理完 TMS 的正常应答之后，如果检测到“需要更新”的标记已经生效，则随后就会如权利要求 1 所述进行 TMK 的更新，完成 TMK 密钥的自动更新；其他正常使用情况下，所述标记定义为“无需更新”。

8. 根据权利要求 1 所述的一种银行卡支付系统中主密钥 TMK 安全自动下载的方法，其特征在于：TMS 完成 TMK 的解密和存储后，答复 POS 终端是否已经更新 TMK 成功。

9. 一种实现主密钥安全下载的银行卡支付系统，包括销售点终端 POS，终端管理系统 TMS，密码键盘和硬件加密机，其特征在于：所述的 TMS 调用加密机产生一对公私密钥，所述的密码键盘存储从 TMS 下载的公钥，所述密码键盘随机产生 TMK 主密钥并利用从 TMS 下载的公钥进行加密。

10. 根据权利要求 9 所述的一种实现主密钥安全下载的银行卡支付系统，其特征在于：所述的加密机将采用公钥加密的 TMK 用私钥解密后存储或者解密后转换成 3DES 加密并存储。

11. 根据权利要求 9 所述的一种实现主密钥安全下载的银行卡支付系统，其特征在于：所述的一对公私密钥，其中私钥在加密机中保存，公钥保存在 TMS 的数据库中。

12. 根据权利要求 9 所述的一种实现主密钥安全下载的银行卡支付系统，其特征在于：在 TMS 与 POS 终端的报文接口中定义一个 TMK 是否需要更新的标记。

13. 根据权利要求 12 所述的一种实现主密钥安全下载的银行卡支付系统，其特征在于：当需要 POS 终端更新 TMK 时，只要 POS 终端向 TMS 发起任何请求，包括签到、交易等，则由 TMS 在报文接口中将“需要更新”

标记设置在报文中，当 POS 终端在处理完 TMS 的正常应答之后，如果检测到“需要更新”的标记已经生效，则随后就会 TMK 密钥的自动更新；其他正常使用情况下，所述标记定义为“无需更新”。

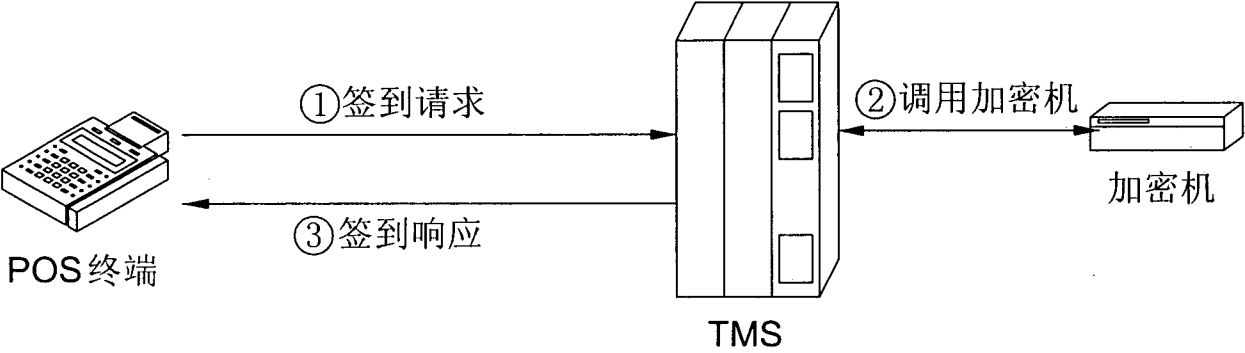


图 1

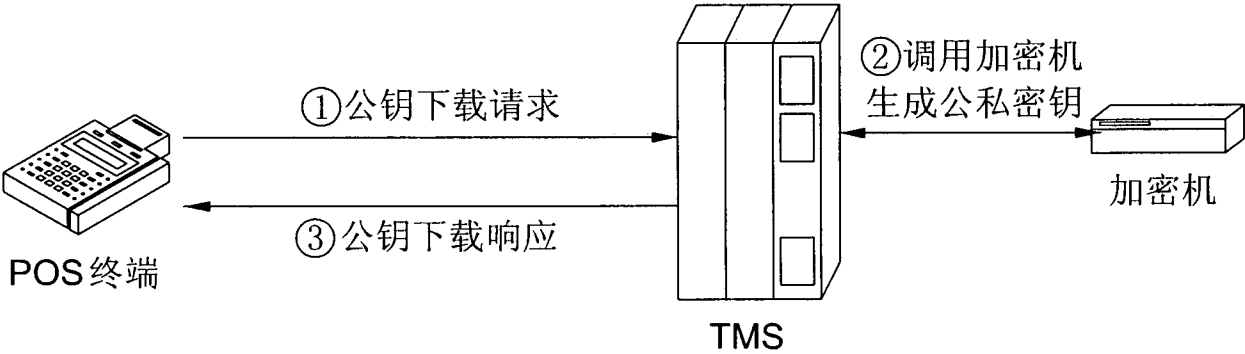


图 2

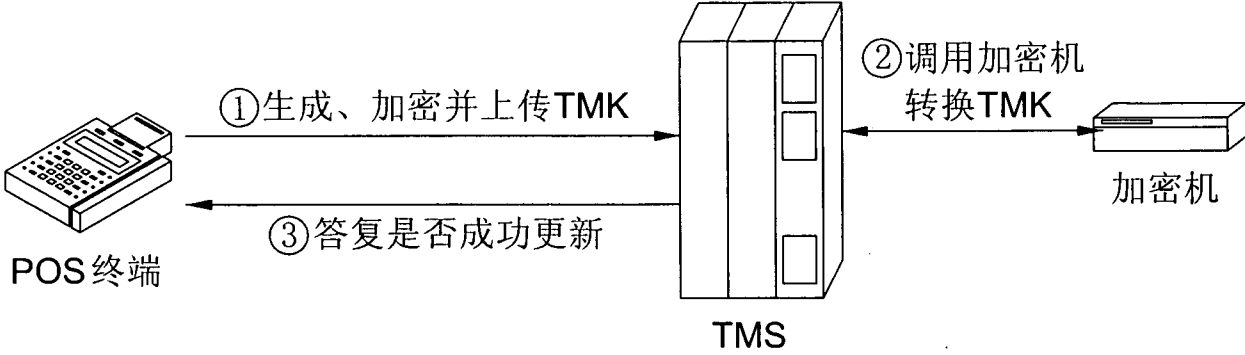


图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2010/000926

A. CLASSIFICATION OF SUBJECT MATTER

SEE EXTRA SHEET

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06Q, G06F, H04M, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI;EPOCOC;CNKI;CNPAT: bank card, payment, secret, key, private, decrypt, store, memory, download, POS, manage, pin pad

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN101436280A(BEIJING HUADA ZHIBAO ELECTRONIC SYSTEM) 20 May 2009 (20.05.2009) the whole document	1-11
A	CN1835007A(TONGPU COMMUNICATION TECH CO LTD) 20 Sep. 2006 (20.09.2006) the whole document	1-11
A	CN101048790A(SK TELECOM CO LTD)3 Oct. 2007 (03.10.2007) the whole document	1-11
A	CN101359383A(CHINA MOBILE GROUP GUANGDONG CO LTD ZHUH) 4 Feb. 2009 (04.02.2009) the whole document	1-11
A	WO2004104725A2(IPDC L L C et al.) 2 Dec. 2004 (02.12.2004) the whole document	1-11
A	CA2457263A1(ZAHIR AZAMI BAHAM SEYED et al.)11 Aug. 2004 (11.08.2004) the whole document	1-11

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&”document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 13 Sept. 2010 (13.09.2010)	Date of mailing of the international search report 30 Sep. 2010 (30.09.2010)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer LI, Yuan Telephone No. (86-10)62085846

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2010/000926

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101436280A	20.05.2009	NONE	
CN1835007A	20.09.2006	NONE	
CN101048790A	03.10.2007	WO2006022513A1	02.03.2006
		KR20060018792A	02.03.2006
		EP1784772A1	16.05.2007
		AU2005275633A1	02.03.2006
		INKOLNP200700657E	06.07.2007
		JP2008511067T	10.04.2008
		BRPI0515237A	15.07.2008
		US2008189186A1	07.08.2008
		KR100930457B1	08.12.2009
		CA2577682A	02.03.2006
		RU2007110824A	10.10.2008
		NZ553995A	30.07.2010
		RU2381557C2	10.02.2010
CN101359383A	04.02.2009	NONE	
WO2004104725A2	02.12.2004	US2003221110A1	27.11.2003
CA2457263A1	11.08.2004	CA2418638A	11.08.2004

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2010/000926

Continuation of second sheet A. CLASSIFICATION OF SUBJECT MATTER:

G06Q20/00 (2006.01) i

G06Q30/00 (2006.01) i

国际检索报告

国际申请号

PCT/CN2010/000926

A. 主题的分类

参见附加页

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: G06Q, G06F, H04M, H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

WPI;EPOCOC;CNKI;CNPAT:银行卡, 支付, 密, 钥, 私钥, 解密, 存储, 下载, POS, 管理, 键盘, bank card, payment, secret, key, private, decrypt, store, memory, download, POS, manage, pin pad

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN101436280A(北京华大智宝电子系统有限公司)20.5 月 2009 (20.05.2009) 全文	1-13
A	CN1835007A(浙江通普通信技术有限公司)20.9 月 2006 (20.09.2006) 全文	1-13
A	CN101048790A(SK 电信有限公司)3.10月2007 (03.10.2007) 全文	1-13
A	CN101359383A(中国移动通信集团广东有限公司)4.2 月 2009 (04.02.2009)	1-13
A	WO2004104725A2(IPDC L L C 等) 2.12 月 2004 (02.12.2004) 全文	1-13
A	CA2457263A1(ZAHIR AZAMI BAHRAM SEYED 等)11.8 月 2004 全文	1-13



其余文件在 C 栏的续页中列出。



见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

13.9 月 2010 (13.09.2010)

国际检索报告邮寄日期

30.9 月 2010 (30.09.2010)

ISA/CN 的名称和邮寄地址:

中华人民共和国国家知识产权局

中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

授权官员

李原

电话号码: (86-10) 62085846

国际检索报告

关于同族专利的信息

国际申请号

PCT/CN2010/000926

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN101436280A	20.05.2009	无	
CN1835007A	20.09.2006	无	
CN101048790A	03.10.2007	WO2006022513A1	02.03.2006
		KR20060018792A	02.03.2006
		EP1784772A1	16.05.2007
		AU2005275633A1	02.03.2006
		INKOLNP200700657E	06.07.2007
		JP2008511067T	10.04.2008
		BRPI0515237A	15.07.2008
		US2008189186A1	07.08.2008
		KR100930457B1	08.12.2009
		CA2577682A	02.03.2006
		RU2007110824A	10.10.2008
		NZ553995A	30.07.2010
		RU2381557C2	10.02.2010
CN101359383A	04.02.2009	无	
WO2004104725A2	02.12.2004	US2003221110A1	27.11.2003
CA2457263A1	11.08.2004	CA2418638A	11.08.2004

(续第 2 页) A. 主题的分类:

G06Q20/00 (2006.01) i

G06Q30/00 (2006.01) i