(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
2011 年 6 月 16 日 (16.06.2011)

PCT

(10) 国际公布号
WO 2011/069325 A1

(51) 国际专利分类号:
G07F 19/00 (2006.01)

(21) 国际申请号: PCT/CN2010/001823

(22) 国际申请日: 2010 年 11 月 15 日 (15.11.2010)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200910200174.1 2009 年 12 月 9 日 (09.12.2009) 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): **李伟 (LI, Wei)** [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)。 **李凯 (LI, Kai)** [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)。 **周文 (ZHOU, Wen)** [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,

[见续页]

(54) Title: METHOD FOR VERIFYING VALIDITY OF PERSONAL IDENTIFICATION NUMBER IN PROXY AUTHORIZATION BUSINESS

(54) 发明名称 : 一种代授权业务中 PIN 正确性验证的方法

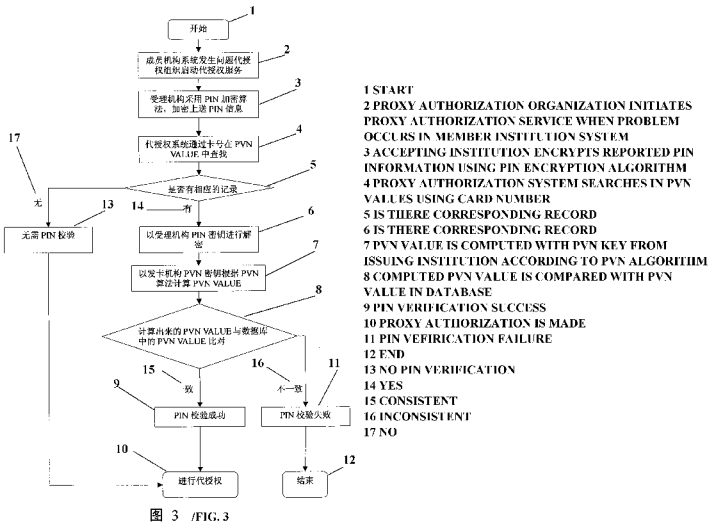

图 3 /FIG. 3

(57) **Abstract**: A method for verifying the validity of a personal identification number(PIN) in proxy authorization business is provided, which comprises: the issuing bank that opens the proxy authorization business encrypts the PIN of every card with a cryptogram using the PIN verification number(PVN) algorithm to acquire the PVN value of every card, and automatically transmits the information about PVN values of all the cards in the format of pairs consisting of card numbers and PVN values, in the form of a file, to the proxy authorization organization that receives and stores it; when the authorization is made by the proxy authorization on behalf of a member banking system that fails to deal with the bank card business, the proxy authorization system decrypts the received encrypted PIN with the key from an accepting bank, regenerates a PVN value with the key from the issuing bank, and compares it with the stored PIN value to verify the validity of the cryptogram. The method reduces the probability of authorization errors in the proxy authorization business and enhances the security of using cards.

[见续页]

WO 2011/069325 A1

HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, 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))。

(57) 摘要:

提供一种代授权业务中个人标识号（PIN）正确性验证的方法，其包括：开通代授权业务的发卡银行采用 PIN 验证号（PVN）算法对每张带密码卡片的 PIN 进行加密，得到每张卡片的 PVN 值，并以（卡号，PVN 值）成对的格式将卡片的 PVN 值信息通过文件形式自动传输给代授权组织，代授权组织收到后进行存储；当成员银行系统无法处理银行卡业务，而由代授权组织为其授权时，代授权系统将收到的加密 PIN 用收单银行的密钥解密，用发卡银行的密钥重新生成 PVN 值，并与存储的 PVN 值比对以验证密码的合法性。该方法减少了代授权业务中错误授权的概率，提高了用卡安全。

一种代授权业务中 PIN 正确性验证的方法

技术领域

本发明涉及银行卡代授权业务，尤其涉及银行卡代授权业务中密码验证的方法。

背景技术

当成员银行系统发生问题无法处理银行卡业务，则需要由代授权组织（例如，中国银联）为其代授权时，为提高代理授权的准确性，需要对卡片的真实性和用卡安全做一定程度的确认，当前的普遍做法是，根据发卡方的要求，对包括卡号长度、卡号校验位、CVN 的信息进行校验。

卡号长度校验是检查，收单银行上送的交易报文中的卡号长度，是否与发卡银行提供的一致。

卡号校验位校验是检查，收单银行上送的交易报文中的卡号的最后一位，是否与标准卡号校验位算法算出来的一样。

CVN 校验是检查，收单银行上送的交易报文中的磁道信息中的 CVN 值是否正确。

卡号长度校验和卡号校验位校验的主要作用是预防误用，CVN 校验则在一定程度上防止了伪卡和假卡的情况。由于国内以密码信用卡为主的支付环境，持卡人普遍以密码方式确保自身账户的安全性，但上述几种方案均无法对卡片密码的正确性进行校验。

本发明提出了一种 PIN 正确性验证的方法，解决了银行卡代授权业务中密码正确性校验的问题，在传统校验方法的基础上再使用本方法，可减少代授权业务中错误授权的概率，提高用卡安全。

发明内容

本发明的目的在于：提供一种代授权业务中 PIN 正确性验证的方法，可减少代授权业务中错误授权的概率，提高用卡安全。

本发明揭示了一种代授权业务中 PIN 正确性验证的方法，当银行卡在交易过程中需要进行代授权时，进行 PIN 验证，包括如下步骤：

步骤 1、发卡银行采用 PVN 算法，使用密钥 KEY_{PVN} 对每张带密卡片的 PIN 进行加密，得到每张卡的 PVN 值；

步骤 2、发卡银行将所有卡片的 PVN 值信息通过文件形式传输给代授权组织，代授权组织收到后，将 PVN 值存入数据库；

步骤 3、发卡银行将持卡人密码修改情况告知代授权组织，代授权组织的系统收到后替换数据库中原有 PVN 值；

步骤 4、当银行卡交易中需要进行代授权时，代授权组织的代授权系统收到加密的 PIN 后，通过卡号在数据库中查找，如果没找到，则说明该卡是不需要进行 PVN 校验的，密码校验通过，如果找到则进行下一步骤；

步骤 5、如果找到，则代授权系统首先对加密的 PIN 进行解密，然后采用 PVN 算法，使用密钥 KEY_{PVN}，计算 PVN 值，并与数据库中所存的 PVN 值进行比对，如果一致则说明 PIN 正确，密码验证通过，否则说明 PIN 不正确，结束交易。

进一步地，在所述步骤 2 中 PVN 值信息是以卡号与 PVN 值成对的格式通过文件形式传输给代授权组织，在所述步骤 3 中持卡人密码修改情况是以卡号与 PVN 值成对的格式通过文件形式传输给代授权组织。

进一步地，所述步骤 4 中代授权组织的代授权系统收到的加密的 PIN，是受理银行以密钥 KEY_{PIN} 对持卡人输入的 PIN 进行加密后上送代

授权组织的，在步骤 5 中，代授权组织的代授权系统通过密钥 KEY_{PIN} 对加密的 PIN 进行解密，所述受理银行是持卡人进行交易的受理单位。

进一步地，所述步骤 3 中持卡人密码修改情况是以设定的频率自动传输给代授权组织，所述设定的频率为每天至少一次。

进一步地，所述步骤 1 中 PVN 值的计算步骤如下：

a、设定 PIN 验证密钥 PVK 的左侧 64 位为密钥 KeyA，右侧 64 位为密钥 KeyB；

b、取卡号右端除校验位以外的 11 位数字、PIN 验证密钥 PVK 的索引号、PIN 明文左端 4 位数字，依次构成一个 16 位数字串，每位数字用压缩 BCD 码表示，形成 1 个 64 位长的二进制计算块 Block；

c、用密钥 KeyA 对 Block 做 DES 加密运算，得到结果 Block1；

d、用密钥 KeyB 对 Block1 做 DES 解密运算，得到结果 Block2；

e、用密钥 KeyA 对 Block2 做 DES 加密运算，得到结果 Block3；

f、对 Block3 从左到右抽取出所有的数字(0 ~ 9)；

g、对 Block3 从左到右抽取出所有的十六进制字符(A ~ F)，并对每一个十六进制字符减十进制 10，使之变为数字；

h、将步骤 f 和 g 得出的数字依次从左至右排列，步骤 g 得出的数字放在步骤 f 得出的数字之后；

i、取步骤 h 结果的前 4 位数字，即为 PVN 值。

通过本发明的方法，解决了代授权业务中密码正确性的校验问题，使得密码卡的代授权更加准确和可靠。

附图说明

图 1 为代授权业务基本流程图;

图 2 为本发明 PVN 信息传递流程图;

图 3 为本发明 PVN 信息校验流程图。

具体实施方式

基于上述情况，我们提出一种代授权业务中 PIN 正确性验证的方法，减少了代授权业务中错误授权的概率，提高了用卡安全，本发明代授权业务的验证方法，是开通代授权业务的发卡银行首先采用代授权组织（例如，中国银联）制定的 PVN（PIN verification number）算法，对每张带密码卡片的 PIN 进行加密，得到每张卡片的 PVN 值（PVN VALUE），并以（卡号，PVN 值）成对的格式将所有卡片的 PVN 值信息通过文件形式自动传输给代授权组织，代授权组织收到后进行存储；当成员银行系统发生问题无法处理银行卡业务，而由代授权组织为其代授权时，代授权系统将收到的加密 PIN，用收单银行的密钥解密，按发卡银行的密钥重新生成 PVN 值，并与存储的 PVN 值比对是否一致，以验证卡片的合法性。

图 1 揭示了代授权业务基本流程，现在银行代授权业务基本流程如下:

1、希望开展代授权业务的成员银行与代授权组织签订代授权协议，明确双方的权利和义务;

2、成员银行将代授权业务开展所需的参数信息（含 PVN 信息）通过文件传输的方式传递至代授权组织;

3、成员银行系统计划内升级或紧急故障停机时，可通知代授权组织，对本行卡的交易进行代授权;

4、代授权组织代授权系统按成员银行的要求，对跨行交易进行代校

验（含 PVN 校验）和额度控制检查，对检查通过的交易直接授权并经转接系统送回受理银行，检查不通过的则交易失败；

5、成员银行系统升级完成或故障解除时，可通知代授权组织解除代授权。

开通代授权业务的发卡银行首先采用 PVN 算法，对每张带密码卡片的 PIN 进行加密，得到每张卡片的 PVN 值，并以（卡号，PVN 值）成对的格式，将所有卡片的 PVN 值信息通过文件形式自动传输给代授权组织，代授权组织收到后进行存储。具体流程如图 2，步骤如下：

1、发卡银行采用 PVN 算法，使用密钥 KEY_{PVN} 对每张带密卡片的 PIN 进行加密，得到每张卡的 PVN 值；

2、发卡银行以卡号，PVN 值对的格式，将所有卡片的 PVN 值信息通过文件形式传输给代授权组织，代授权组织收到后，将 PVN 值存入数据库；

3、发卡银行以设定的频率（例如每天一次，或者每天两次、三次或者更多次，具体时间间隔可以根据需要来设定），自动通过文件形式（以卡号，修改后的 PVN 值成对的格式），将持卡人密码修改情况告知代授权组织，代授权组织的系统收到后替换原有 PVN 值。

成员银行系统升级停机或突发异常不能处理跨行业务时，代授权组织启动代授权服务，图 3 给出了 PVN 校验的处理流程，步骤如下：

1、受理银行采用 PIN 加密算法，以密钥 KEY_{PIN} 对持卡人输入的 PIN 进行加密上送代授权组织，受理银行是指持卡人进行交易的受理单位；

2、代授权组织的代授权系统收到加密的 PIN 后，通过卡号在 PVN 值数据库中查找，如果没找到，则说明该卡是不需要进行 PVN 校验的，密码校验通过；

3、如果找到，则代授权系统首先以密钥 KEYPIN 进行解密，然后采用 PVN 算法，使用密钥 KEY_{PVN}，计算 PVN 值，并与数据库中所存的 PVN 值进行比对，如果一致则说明 PIN 正确，否则说明 PIN 不正确。

其中步骤 2 中，当没找到卡号对应的 PVN 值，则说明该卡是不需要进行 PVN 校验的，密码校验通过，直接进行代授权；在步骤 3 中，如果计算的 PVN 值与数据库中所存的 PVN 值一致，则验证通过，进行代授权，否则拒绝代授权，结束交易。

其中 PVN 算法基本原理，PVN 值的计算步骤如下：

1、设 PIN 验证密钥 PVK（PIN verification key）的左侧 64 位为密钥 KeyA，右侧 64 位为密钥 KeyB;

2、取卡号右端除校验位以外的 11 位数字、密钥 PVK 的索引号、PIN 明文左端 4 位数字，依次构成一个 16 位数字串，每位数字用压缩 BCD 码表示，形成 1 个 64 位长的二进制计算块 Block;

3、用 KeyA 对 Block 做 DES 加密运算，得到结果 Block1;

4、用 KeyB 对 Block1 做 DES 解密运算，得到结果 Block2;

5、用 KeyA 对 Block2 做 DES 加密运算，得到结果 Block3;

6、对 Block3 从左到右抽取出所有的数字(0 ~ 9);

7、对 Block3 从左到右抽取出所有的十六进制字符(A ~ F),并对每一个十六进制字符减十进制 10，使之变为数字;

8、将步骤 6 和 7 得出的数字依次从左至右排列,步骤 7 得出的数字放在步骤 6 得出的数字之后;

9、取步骤 8 结果的前 4 位数字，即为 PVN 值。

通过上述方法，解决了代授权业务中密码正确性的校验问题，使得密码卡的代授权更加准确和可靠，安全级别与当前跨行业务中采用的 PIN 转换方法相当，但不可逆向解密，即通过 PVN 值无法解密出 PIN 的明码，即从事代授权业务的代授权组织不能得到银行卡 PIN 的明码。上述 PVN 算法仅为能够实现本发明目的的算法之一，本领域普通技术人员通过对算法做些简单的数学变化或采用其它类似算法，也能达到等同的目的，均在本发明的保护范围之内。

PVN 校验是代授权业务中需要进行的其中一种校验，用于验证密码正确性方面的，其他校验无法验证密码正确性。但是并不是说只单单进行这一种校验，在代授权业务中其他如前面提及的卡号校验位校验、卡号长度校验、CVN 校验等也需要进行，代授权组织系统会在多种校验均通过的情况下，对交易进行代授权。

同时本发明采用自动文件传输的方式，较快速的解决了持卡人更改 PIN 后带来的校验失败问题，持卡人密码修改情况以设定的频率自动传输给代授权组织，这里设定的频率如果间隔时间太长，容易造成持卡人更改了密码，但是代授权组织的数据库中 PVN 值未更新，造成 PIN 验证失败；如果间隔时间太短，造成频繁的传输文件，因此需要根据实际使用情况做出适当的调整，一般建议每天更新一次。

权利要求

1.一种代授权业务中 PIN 正确性验证的方法，当银行卡在交易过程中需要进行代授权时，进行 PIN 验证，其特征在于，包括如下步骤：

步骤 1、发卡银行采用 PVN 算法，使用密钥 KEY_{PVN} 对每张带密卡片的 PIN 进行加密，得到每张卡的 PVN 值；

步骤 2、发卡银行将所有卡片的 PVN 值信息通过文件形式传输给代授权组织，代授权组织收到后，将 PVN 值存入数据库；

步骤 3、发卡银行将持卡人密码修改情况告知代授权组织，代授权组织的系统收到后替换数据库中原有 PVN 值；

步骤 4、当银行卡交易中需要进行代授权时，代授权组织的代授权系统收到加密的 PIN 后，通过卡号在数据库中查找，如果没找到，则说明该卡是不需要进行 PVN 校验的，密码校验通过，如果找到则进行下一步骤；

步骤 5、如果找到，则代授权系统首先对加密的 PIN 进行解密，然后采用 PVN 算法，使用密钥 KEY_{PVN}，计算 PVN 值，并与数据库中所存的 PVN 值进行比对，如果一致则说明 PIN 正确，密码验证通过，否则说明 PIN 不正确，结束交易。

2.根据权利要求 1 所述的一种代授权业务中 PIN 正确性验证的方法，其特征在于：在所述步骤 2 中 PVN 值信息是以卡号与 PVN 值成对的格式通过文件形式传输给代授权组织。

3.根据权利要求 1 所述的一种代授权业务中 PIN 正确性验证的方法，其特征在于：在所述步骤 3 中持卡人密码修改情况是以卡号与 PVN 值成对的格式通过文件形式传输给代授权组织。

4.根据权利要求 1 所述的一种代授权业务中 PIN 正确性验证的方法，其特征在于：所述步骤 4 中代授权组织的代授权系统收到的加密的 PIN，是受理银行以密钥 KEY_{PIN} 对持卡人输入的 PIN 进行加密后上送代授权组织的；在步骤 5 中，代授权组织的代授权系统通过密钥 KEY_{PIN} 对加密的 PIN 进行解密。

5.根据权利要求 4 所述的一种代授权业务中 PIN 正确性验证的方法，其特征在于：所述受理银行是持卡人进行交易的受理单位。

6.根据权利要求 3 所述的一种代授权业务中 PIN 正确性验证的方法，其特征在于：所述持卡人密码修改情况是以设定的频率自动传输给代授权组织，所述设定的频率为每天至少一次。

7.根据权利要求 1 所述的一种代授权业务中 PIN 正确性验证的方法，其特征在于：所述步骤 1 中 PVN 值的计算步骤如下：

a、设定 PIN 验证密钥 PVK 的左侧 64 位为密钥 KeyA，右侧 64 位为密钥 KeyB;

b、取卡号右端除校验位以外的 11 位数字、PIN 验证密钥 PVK 的索引号、PIN 明文左端 4 位数字，依次构成一个 16 位数字串，每位数字用压缩 BCD 码表示，形成 1 个 64 位长的二进制计算块 Block;

c、用密钥 KeyA 对 Block 做 DES 加密运算，得到结果 Block1;

d、用密钥 KeyB 对 Block1 做 DES 解密运算，得到结果 Block2;

e、用密钥 KeyA 对 Block2 做 DES 加密运算，得到结果 Block3;

f、对 Block3 从左到右抽取出所有的数字(0 ~ 9);

g、对 Block3 从左到右抽取出所有的十六进制字符(A ~ F)，并对每一个十六进制字符减十进制 10，使之变为数字;

h、将步骤 f 和 g 得出的数字依次从左至右排列，步骤 g 得出的数字放在步骤 f 得出的数字之后；

i、取步骤 h 结果的前 4 位数字，即为 PVN 值。

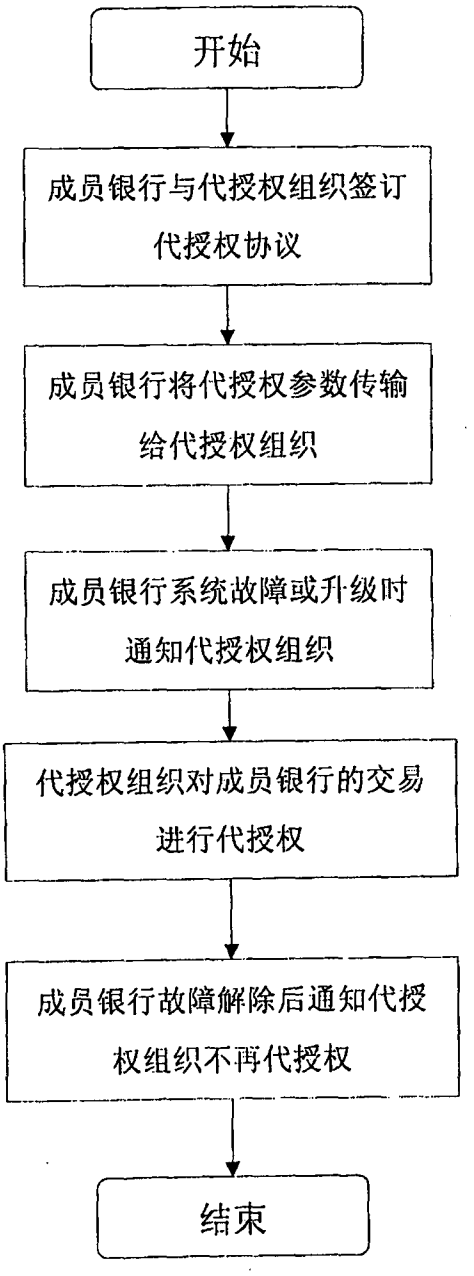
开始
成员银行与代授权组织签订代授权协议
成员银行将代授权参数传输给代授权组织
成员银行系统故障或升级时通知代授权组织
代授权组织对成员银行的交易进行代授权
成员银行故障解除后通知代授权组织不再代授权
结束

图 1

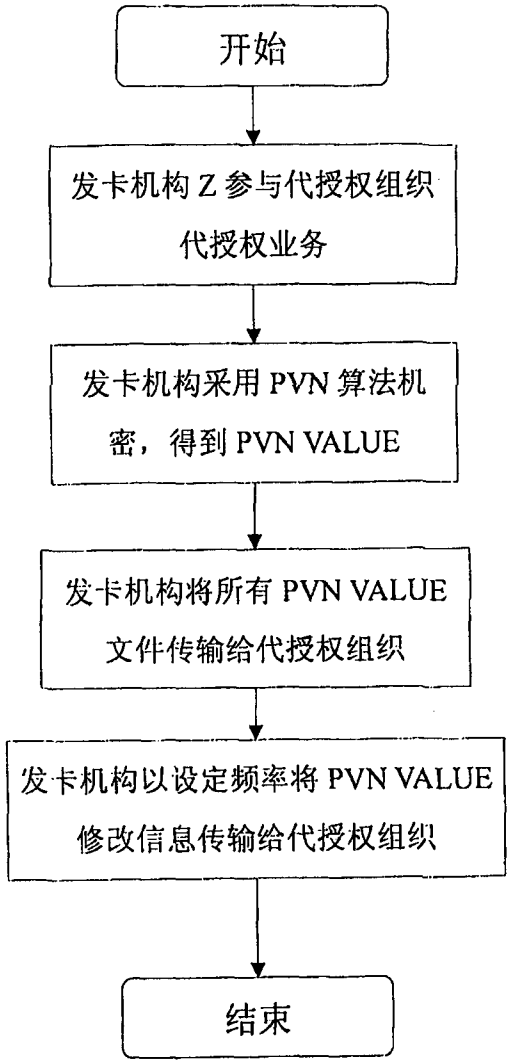
开始
发卡机构 Z 参与代授权组织代授权业务
发卡机构采用 PVN 算法机密，得到 PVN VALUE
发卡机构将所有 PVN VALUE 文件传输给代授权组织
发卡机构以设定频率将 PVN VALUE 修改信息传输给代授权组织
结束

图 2

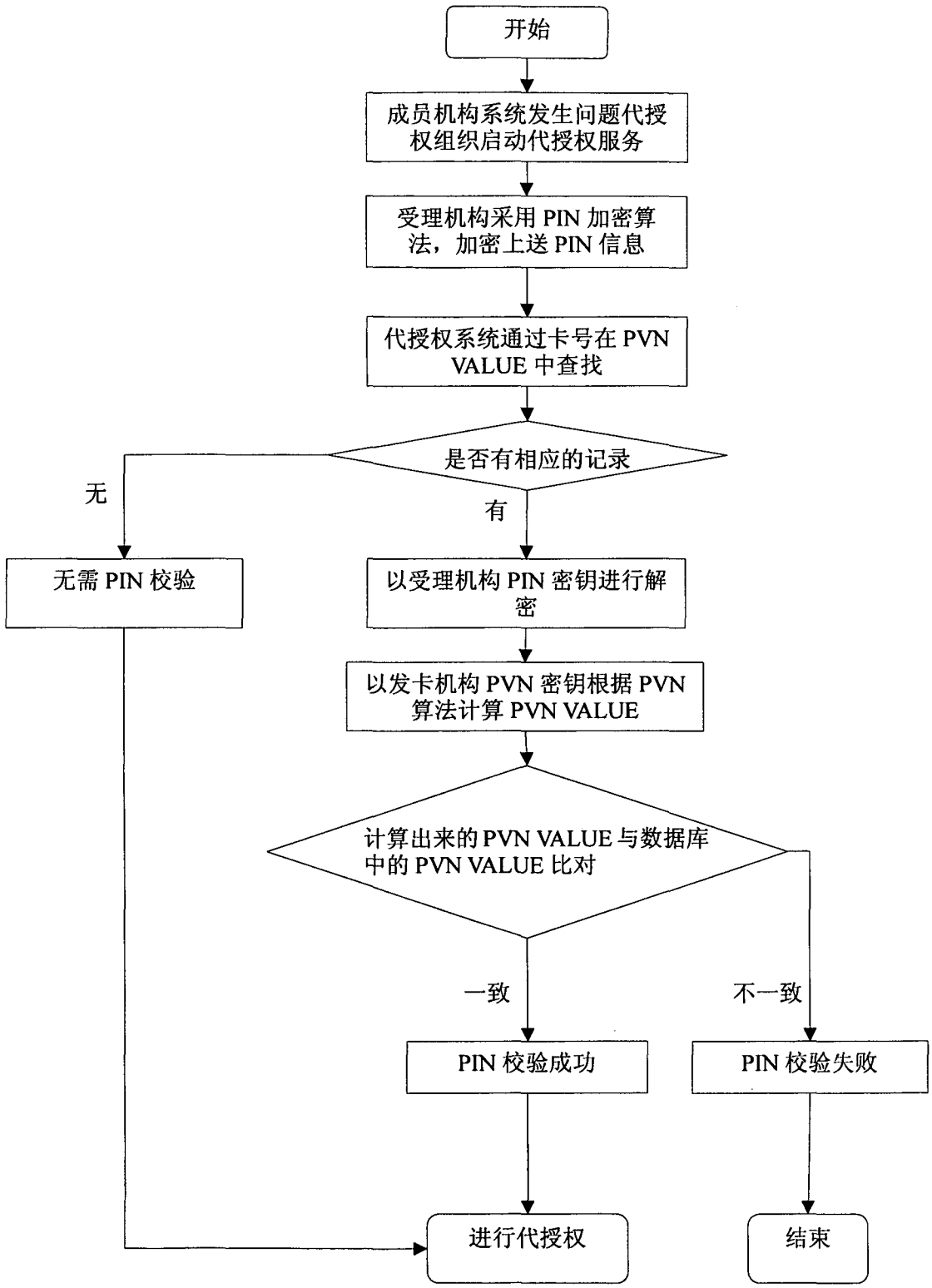
开始
成员机构系统发生问题代授权组织启动代授权服务
受理机构采用 PIN 加密算法，加密上送 PIN 信息
代授权系统通过卡号在 PVN VALUE 中查找
是否有相应的记录
无
有
无需 PIN 校验
以受理机构 PIN 密钥进行解密
以发卡机构 PVN 密钥根据 PVN 算法计算 PVN VALUE
计算出来的 PVN VALUE 与数据库中的 PVN VALUE 比对
一致
不一致
PIN 校验成功
PIN 校验失败
进行代授权
结束

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2010/001823

A. CLASSIFICATION OF SUBJECT MATTER

G07F 19/00(2006.01) i

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: G07F 19/-

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)

CNPAT; CNKI; INTERNET; WPI; EPODOC

PIN, personal w identification w card, key?, encrypt+, decrypt+, card?

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US20080077798A1(NACHTIGALL E H et al.) 27 Mar. 2008(27.03.2008) see the whole document	1-7
A	WO02063580 A2(HARGENS H et al.) 15 Aug. 2002(15.08.2002) see the whole document	1-7
A	CN1260894A(NAT WESTMINSTER BANK PLC) 19 Jul. 2000(19.07.2000) see the whole document	1-7

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 Feb. 2011(11.02.2011)	**24 Feb. 2011 (24.02.2011)**
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 YANG, Jie Telephone No. (86-10) 62411825

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2010/001823

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US20080077798A1	27.03.2008	CA2561077A1	26.03.2008
		WO2009039600A1	02.04.2009
WO02063580A2	15.08.2002	US2002123972A1	05.09.2002
		AU2002241906A1	19.08.2002
		AU2002241906A8	20.10.2005
		WO02063580A3	15.08.2002
CN1260894A	19.07.2000	WO9900775A1	07.01.1999
		ZA9805628A	31.03.1999
		AU8122598A	19.01.1999
		NO996488A	28.02.2000
		EP0992026A1	12.04.2000
		CZ9904726A3	14.06.2000
		SK176199A3	11.07.2000
		BR9810486A	12.09.2000
		HU0003227A2	28.02.2001
		TW411427B	11.11.2000
		NZ501887A	25.05.2001
		KR20010014257A	26.02.2001
		JP2002507297T	05.03.2002
		MX9911836A1	01.05.2002
		CA2295032A1	07.01.1997
		IS5307A	17.12.1999
		TR9903243T2	21.04.2000
		BG104041A	31.05.2000
		EE9900598A	15.08.2000
		PL337533A1	28.08.2000
		MXPA99011836A	19.04.2002

国际检索报告

国际申请号
PCT/CN2010/001823

A. 主题的分类

G07F 19/00(2006.01) i

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：G07F 19/-

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）)

CNPAT；CNKI；INTERNET；WPI；EPODOC

个人标识号，密钥，加密，解密，卡；PIN, personal w identification w card, key?, encrypt+, decrypt+, card?

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	US20080077798A1（NACHTIGALL E H 等）27.3 月 2008（27.03.2008）参见全文	1-7
A	WO02063580A2（HARGENS H 等）15.8 月 2002（15.08.2002）参见全文	1-7
A	CN1260894A（国民西敏寺银行）19.7 月 2000（19.07.2000）参见全文	1-7

☐ 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	国际检索报告邮寄日期
11.2 月 2011(11.02.2011)	**24.2 月 2011 (24.02.2011)**
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	受权官员 **杨洁** 电话号码：(86-10) **62411825**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2010/001823

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US20080077798A1	27.03.2008	CA2561077A1	26.03.2008
		WO2009039600A1	02.04.2009
WO02063580A2	15.08.2002	US2002123972A1	05.09.2002
		AU2002241906A1	19.08.2002
		AU2002241906A8	20.10.2005
		WO02063580A3	15.08.2002
CN1260894A	19.07.2000	WO9900775A1	07.01.1999
		ZA9805628A	31.03.1999
		AU8122598A	19.01.1999
		NO996488A	28.02.2000
		EP0992026A1	12.04.2000
		CZ9904726A3	14.06.2000
		SK176199A3	11.07.2000
		BR9810486A	12.09.2000
		HU0003227A2	28.02.2001
		TW411427B	11.11.2000
		NZ501887A	25.05.2001
		KR20010014257A	26.02.2001
		JP2002507297T	05.03.2002
		MX9911836A1	01.05.2002
		CA2295032A1	07.01.1999
		IS5307A	17.12.1999
		TR9903243T2	21.04.2000
		BG104041A	31.05.2000
		EE9900598A	15.08.2000
		PL337533A1	28.08.2000
		MXPA99011836A	19.04.2002