(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104094302 B
(45)授权公告日 2018.12.14

(21)申请号 201380008011.8
(22)申请日 2013.01.07
(65)同一申请的已公布的文献号
申请公布号 CN 104094302 A
(43)申请公布日 2014.10.08
(30)优先权数据
61/583,550 2012.01.05 US
61/607,546 2012.03.06 US
61/704,428 2012.09.21 US
(85)PCT国际申请进入国家阶段日
2014.08.04
(86)PCT国际申请的申请数据
PCT/US2013/020580 2013.01.07
(87)PCT国际申请的公布数据
WO2013/103991 EN 2013.07.11

(73)专利权人 维萨国际服务协会
地址 美国加利福尼亚州
(72)发明人 G·鲍威尔 J·F·希茨 P·泰特
K·R·瓦格纳 K·P·考甘蒂
M·珀尔 H·罗德里格斯
S·兹洛斯
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 李玲

(51)Int.Cl.
G06Q 20/38(2006.01)
G06F 21/60(2006.01)
审查员 黄亮

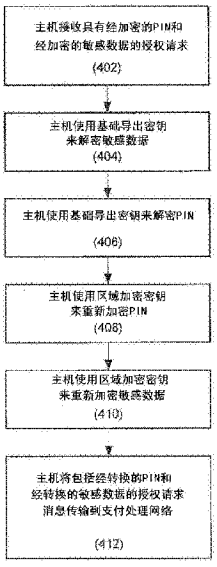
权利要求书3页 说明书14页 附图9页

(54)发明名称

用转换进行数据保护

(57)摘要

公开了用加密来保护与交易相关联的数据的系统和方法。在访问设备处，可用从该访问设备的初始密钥导出的第一密钥加密与支付账户相关联的PIN，并且可用从该初始密钥导出的第二密钥加密与该支付账户相关联的敏感数据。在与主机服务器相关联的安全模块处，可解密授权请求消息的经加密的敏感数据。与该主机服务器相关联的该安全模块可使用与支付处理网络相关联的区域加密密钥来重新加密该敏感数据。包括该经重新加密的敏感数据的经转换的授权请求消息可被商户服务器传输到该支付处理网络。



CN 104094302 B

1.一种用于数据保护的方法,包括:

由访问设备接收个人标识号PIN和敏感数据,所述访问设备具有用从基础导出密钥导出的初始密钥编程的安全模块,所述基础导出密钥与密钥序列号相关联;

由所述访问设备使用从所述初始密钥导出的第一加密密钥对所述PIN进行加密;

由所述访问设备使用从相同的初始密钥导出的第二加密密钥对包括主账号PAN的所述敏感数据进行加密,所述第二加密密钥与所述第一加密密钥不同;以及

向主机服务器传输所述密钥序列号以及包括经加密的PIN和经加密的敏感数据的授权请求消息,

其中,所述主机服务器通过使用所述密钥序列号检取所述基础导出密钥、从所述基础导出密钥导出解密密钥、以及使用所述解密密钥来解密所述经加密的PIN和所述经加密的敏感数据,来处理交易。

2.如权利要求1所述的方法,其中,所述初始密钥是由每交易唯一导出密钥DUKPT密钥管理方案生成的。

3.如权利要求1所述的方法,其中,所述PIN和所述敏感数据中的至少一个是使用三重DES加密算法TDEA进行加密的。

4.如权利要求1所述的方法,其中,所述敏感数据还包括持卡人姓名、持卡人地址、以及自由选择数据中的至少一项。

5.如权利要求1所述的方法,其中,当自由选择数据被包括在经加密的敏感数据中时,自由选择数据的子集保持不加密。

6.如权利要求1所述的方法,其中,加密的PAN被写入所述授权请求消息的PAN字段中,其中,经加密的PAN具有与不加密的PAN相同的格式。

7.如权利要求6所述的方法,其中,不加密的PAN的数位子集在不加密的PAN中保持不加密。

8.如权利要求6所述的方法,其中,所述授权请求消息的有效期字段被经更改的有效期盖写,以便表明所述授权请求消息的所述PAN字段包含加密的PAN。

9.如权利要求1所述的方法,其中,所述访问设备是销售点终端。

10.如权利要求1所述的方法,其中,所述访问设备接收与电子商务交易相关联的信息。

11.一种用于数据保护的方法,包括:

由主机服务器接收授权请求消息,其中,所述授权请求消息包括密钥序列号、经加密的个人标识号PIN、和包括经加密的主账号PAN在内的经加密的敏感数据,其中,使用从初始密钥导出的第一加密密钥对所述PAN进行加密,并且使用从相同的初始密钥导出的第二加密密钥对所述敏感数据进行加密,所述第二加密密钥与所述第一加密密钥不同;

由所述主机服务器使用所述密钥序列号来检取基础导出密钥;

由所述主机服务器从所述基础导出密钥导出解密密钥;

由所述主机服务器来解密经加密的敏感数据;

由所述主机服务器重新加密经解密的敏感数据,其中,敏感数据重新加密使用与第一支付处理网络相关联的第一敏感数据区域加密密钥;以及

由所述主机服务器将第一经转换的授权请求消息传输到所述第一支付处理网络,其中,所述第一经转换的授权请求消息包括经重新加密的敏感数据。

12.如权利要求11所述的方法，进一步包括：

由所述主机服务器解密所述经加密的PIN；以及

由所述主机服务器重新加密经解密的PIN，其中，PIN重新加密使用与所述第一支付处理网络相关联的第一PIN区域加密密钥；以及

其中，所述第一经转换的授权请求消息包括经重新加密的PIN。

13.如权利要求12所述的方法，其中，所述主机服务器被配置成向第二支付处理网络传输第二经转换的授权请求消息，其中，第二PIN区域加密密钥被用于为所述第二经转换的授权请求消息重新加密PIN，并且第二敏感数据区域加密密钥被用于为所述第二经转换的授权请求消息重新加密敏感数据。

14.如权利要求11所述的方法，其中，经加密的PIN是使用基于初始密钥的第一加密密钥变体加密的，并且经加密的敏感数据是使用基于所述初始密钥的第二加密密钥变体加密的。

15.如权利要求14所述的方法，其中，所述初始密钥是由每交易唯一导出密钥DUKPT密钥管理方案生成的。

16.如权利要求11所述的方法，其中，所述主机服务器包括防篡改安全模块。

17.如权利要求11所述的方法，其中，所述主机服务器包括硬件安全模块。

18.如权利要求11所述的方法，其中，所述敏感数据还包括持卡人姓名、持卡人地址、以及自由选择数据中的至少一项。

19.一种用于数据保护的计算机系统，包括：

处理器；以及

耦合到所述处理器的计算机可读介质，其中，所述计算机可读介质包括可由所述处理器执行以便实现如权利要求1-10中任一项所述的方法的代码。

20.如权利要求19所述的系统，其中，所述处理器是安全密码处理器。

21.如权利要求19所述的系统，其中，所述系统包括防篡改安全模块。

22.一种用于数据保护的计算机系统，包括：

处理器；以及

耦合到所述处理器的计算机可读介质，其中，所述计算机可读介质包括可由所述处理器执行以便实现如权利要求11-18中任一项所述的方法的代码。

23.如权利要求22所述的系统，其中，所述处理器是安全密码处理器。

24.如权利要求22所述的系统，其中，所述系统包括防篡改安全模块。

25.如权利要求22所述的系统，其中，所述系统包括硬件安全模块。

26.一种用于数据保护的方法，包括：

接收与个人标识号PIN和主账号PAN相关联的数据；

由访问设备使用从初始密钥导出的第一加密密钥对所述PIN进行加密，所述访问设备具有用从基础导出密钥导出的初始密钥编程的安全模块，所述基础导出密钥与密钥序列号相关联；

由所述访问设备使用从相同的初始密钥导出的第二加密密钥对所述PAN进行加密，所述第二加密密钥与所述第一加密密钥不同，其中，经加密的PAN具有与所述PAN相同的格式；

将经加密的PAN写入授权请求消息的字段，其中，所述字段被指定为接收PAN；

将授权请求消息数据元素用作信号以便标识在所述授权请求消息中存在经加密的PAN;以及

传输包括所述密钥序列号、经加密的PIN和经加密的PAN的所述授权请求消息。

27.如权利要求26所述的方法,其中,所述授权请求消息中的经加密的PAN的数位的子集是所述PAN的未经加密的数位。

28.如权利要求27所述的方法,其中,经加密的PAN的前六个数位与未经加密的PAN的前六个数位相同,并且其中,经加密的PAN的后四个数位与未经加密的PAN的后六个数位相同。

29.如权利要求27所述的方法,进一步包括为经加密的PAN的指定数位计算一值,从而使得未经加密的PAN的最后一个数位与经加密的PAN的最后一个数位相同,并且其中,经加密的PAN的最后一个数位是经加密的PAN的有效校验数位。

30.如权利要求29所述的方法,其中,所述指定数位是经加密的PAN的第十二个数位。

31.如权利要求26所述的方法,其中,所述授权请求消息包括有效期,并且其中,当所述授权请求消息的PAN字段包含经加密的PAN时,所述授权请求消息的有效期字段被经更改的有效期盖写。

用转换进行数据保护

[0001] 相关申请的交叉引用

[0002] 本申请涉及2012年1月5日提交的美国临时申请号61/583,550(代理人案号：79900-819288)，其全部内容通过引用以全部目的结合于此。本申请还涉及2012年3月6日提交的美国临时申请号61/607,546(代理人案号：79900-829470)，其全部内容通过引用以全部目的结合于此。本申请还涉及2012年9月21日提交的美国临时申请号61/704,428(代理人案号：79900-851259)，其全部内容通过引用以全部目的结合于此。

[0003] 发明背景

[0004] 可通过多项措施诸如数据加密在具有基于硬件的安全控件的设备内保护金融账户数据不受未授权访问影响。然而，现有的安全措施诸如加密个人标识号(PIN)可使得敏感数据诸如主账号(PAN)曝光。现有的用于保护敏感数据的解决方案可要求应用不同于那些用于加密PIN数据的密钥管理方案，增加了为金融数据提供安全的商户的负担。

[0005] 商户可通过将所有交易路由到用于支付处理的单个目的地来保护金融账户数据。然而，当路由对交易的授权请求时，商户可能够在多个可用的支付处理网络之间选择支付处理网络。上述可能需要提供基于授权请求消息的路由目的地对授权请求消息中的信息进行解密并且对信息进行重新加密。某些支付处理网络可缺少对敏感数据的加密解决方案。商户可希望使用由第一支付处理网络提供的加密措施同时继续能够将授权请求路由到可替代的支付处理网络。

[0006] 在此描述的实施例解决了这些和其他问题。

[0007] 发明简要概述

[0008] 多种技术提供当在包括多个支付处理网络选项的环境中路由对交易的授权请求时保护敏感数据。

[0009] 在一个实施例中，描述了一种方法。该方法包括由访问设备加密个人标识号(PIN)。PIN加密使用基于初始密钥的第一加密密钥变体。该访问设备使用基于该初始密钥的第二加密密钥变体对敏感数据进行加密。包括经加密的PIN和经加密的敏感数据的授权请求消息被传输到主机服务器。

[0010] 在另一个示例中，一种方法包括在主机服务器接收授权请求消息。通信地连接到主机服务器的安全模块解密该经加密敏感数据。该安全模块使用与该第一支付处理网络相关联的第一敏感数据区域加密密钥重新加密该经解密敏感数据。包括该经重新加密的敏感数据的第一经转换授权请求消息可由主机服务器传输到该第一支付处理网络。在另一个实施例中，在该主机服务器接收的该授权请求消息包括PIN。该安全模块解密该经加密的PIN并且用与该第一支付处理网络相关联的第一PIN区域加密密钥重新加密该经解密的PIN。该第一经转换授权请求消息包括该经重新加密的PIN。在附加实施例中，该安全模块被配置成用于将第二经转换授权请求消息传输到第二支付处理网络。第二PIN区域加密密钥用于为该第二经转换授权请求消息重新加密PIN并且第二敏感数据区域加密密钥用于为该第二授权请求消息重新加密敏感数据。

[0011] 本技术的另一个实施例涉及一种系统。该系统包括处理器以及耦合到该处理器的

计算机可读介质。该计算机可读介质包括代码，该代码可由该处理器执行以实现包括由访问设备加密个人标识号(PIN)的方法。PIN加密使用基于初始密钥的第一加密密钥变体。该访问设备使用基于该初始密钥的第二加密密钥变体对敏感数据进行加密。包括经加密PIN和经加密敏感数据的授权请求消息被传输到主机服务器。

[0012] 本技术的另一个实施例涉及一种系统。该系统包括处理器以及耦合到该处理器的计算机可读介质。该计算机可读介质包括代码，该代码可由该处理器执行以实现包括在主机服务器接收授权请求消息的方法。该授权请求消息包括经加密的敏感数据。通信地连接到主机服务器的安全模块解密该经加密敏感数据。该安全模块使用与该第一支付处理网络相关联的第一敏感数据区域加密密钥重新加密该经解密敏感数据。包括该经重新加密的敏感数据的第一经转换授权请求消息可由主机服务器传输到该第一支付处理网络。

[0013] 在另一个实施例中，一种方法包括接收与个人账户标识符(PAI)相关联的数据。访问设备可加密该PAI。该经加密的PAI可具有与PAI相同的格式。该经加密的PAI被写入授权请求消息的字段。该授权请求消息的该字段是被指定为接收PAI的字段。将授权请求消息数据元素用作信号以便标识在该授权请求消息中存在该经加密的PAI。该访问设备传输该授权请求消息。

[0014] 以下更详细描述这些以及其他实施例。

[0015] 附图简要说明

[0016] 图1示出可在其中实现本技术的实施例的示例性系统。

[0017] 图2示出在访问设备和商户主机加密PIN和敏感数据的说明性流程图。

[0018] 图3是在主机转换敏感数据的说明性流程图。

[0019] 图4是在主机转换PIN和敏感数据的说明性流程图。

[0020] 图5是表格，示出支付设备的轨迹I的结构和内容的说明性规范。

[0021] 图6是表格，示出支付设备的轨迹II的结构和内容的说明性规范。

[0022] 图7是流程图，示出根据实施例的格式保留加密的实现方式。

[0023] 图8是流程图，示出解释数据从而确定是否已经应用格式保留加密。

[0024] 图9描绘计算机系统的说明性高级框图。

[0025] 发明详细描述

[0026] 在此公开的实施例涉及用于保护授权请求消息中的金融数据的技术。可参照以下提供的说明理解用于描述此处的实施例的术语。

[0027] “授权请求消息”可以是对交易进行授权的请求。授权请求消息可被发送给支付账户的发布者以便请求授权用该支付账户进行的交易。商户可生成授权请求消息。授权请求消息可经由捕获器被传输给发布者。

[0028] 授权请求消息可具有定义格式以便促进金融网络内的点之间的请求和响应。例如，授权请求消息可以是标准交换消息，诸如符合国际标准化组织(ISO)8583的消息，其是用于交换电子交易的系统的标准。ISO8583消息可包括消息类型指示符、指示该消息内存在的数据元素的一个或多个位图、以及该消息的数据元素。包括在授权请求消息内的数据可包括从支付设备获得的数据以及与交易、支付账户持有人、以及商户相关的其他数据。例如，授权请求消息可包括个人标识号(PIN)、以及敏感数据，诸如主账号(PAN)、持卡人姓名、以及自由选择数据。附加地，授权请求消息可包括支付设备有效期、货币代码、交易量、商户

交易戳、接受者城市、接受者国籍/国家、银行代码、终端标识、网络标识等等。可使用加密来保护授权请求消息，以便防止数据受损。

[0029] 授权请求消息可包括支付账户标识符。授权请求消息可与便携式消费者设备相关联，诸如信用卡或借记卡。例如，支付账户标识符可以是主账号(PAN)。PAN可以是唯一支付卡号，诸如与信用卡相关联的信用卡账号或者与借记卡相关联的借记账号。PAN可识别发布者以及持卡人账户。当在此使用术语PAN时，将理解到可使用任何支付账户标识符。

[0030] 个人标识号(PIN)可以是在用户和系统之间共享的并且用于为系统对用户进行认证的数字密码。PIN模块可以是用于封装PIN的经加密数据模块。PIN模块可由PIN、PIN长度、以及PAN的子集组成。

[0031] 也被称为“自由选择数据”的发布者自由选择数据(IDD)可以是驻留在支付设备的磁条或芯片内的轨迹1和/或轨迹2中的数据或者以其他方式与支付账户相关联的数据。IDD的长度可变并且可包含消费者和/或卡验证数据，诸如PIN偏移值、PIN验证值(PVV)、卡验证值(CVV)等等。IDD还可包括由卡品牌和/或发布者定义的其他数据，诸如在忠诚计划、舰队数据(fleet data)等等中使用的信息。

[0032] “捕获器”通常是与具体的商户具有商业关系的商业实体(例如，商业银行)。例如，捕获器可向商户银行账户存入资金并且从发布者收回这些资金。

[0033] “发布者”通常是向账户拥有人发布支付设备并且为支付账户提供行政管理功能的商业实体(例如，银行或信用联盟)。某些实体可执行发布者和捕获器功能。支付账户可以是可在交易中使用的任何账户，诸如信用、借记或预付账户。

[0034] “支付设备”可以是指用于发起交易的设备，诸如便携式消费者设备或便携式通信设备。支付设备可与访问设备诸如销售点设备对接以便发起交易。通常，便携式消费者设备是手持式的并且紧凑的，从而使得其可适配到消费者的钱包或口袋中(例如，口袋大小的)。便携式消费者设备的具体示例包括支付卡，诸如智能卡、借记设备(例如，借记卡)、信用设备(例如，信用卡)、或储值设备(例如，储值卡或“预付”卡)。也称为“移动设备”的便携式通信设备可以是例如蜂窝或无线电话(例如，智能电话)、个人数字助理(PDA)、便携式计算机(例如，平板计算机或膝上计算机)、寻呼机、或由支付账户持有人携带的其他便携式设备。

[0035] “访问设备”可以是指从支付设备接收信息以便发起交易的设备。例如，访问设备可以是被配置成用于读取编码在卡格式的便携式消费者设备的磁条或芯片中的账户数据的销售点设备。访问设备的其他示例包括蜂窝电话、PDA、个人计算机、服务器计算机、平板计算机、手持式专用阅读器、机顶盒、电子收银机、自动柜员机(ATM)、虚拟收银机、公用电话亭、安全系统、访问系统等等。访问设备可使用诸如射频(RF)和磁条阅读器类的装置来与支付设备交互。访问设备可以是位于商户的物理位置的设备或可以是虚拟销售点，诸如是电子商务(eCommerce)交易的一部分的网站。在eCommerce交易中，账户拥有者可向便携式通信设备、个人计算机、或能够与商户计算机进行通信的其他设备输入支付账户数据。在其他无卡交易中，诸如邮件订单或电话订单交易中，可向用作访问设备的商户计算机输入信息。在另一个示例中，通信可使用无线通信机制(诸如近场通信(NFC)、RF、红外、光学通信等等)在便携式通信设备的非接触式元件和访问设备(诸如商户设备阅读器或销售点终端)之间发生。

[0036] “支付处理网络”可包括接收授权请求消息的系统。支付处理网络可从授权请求消

息获得信息以便用于确定是否批准与授权请求消息相关联的交易。支付处理网络可向商户发送表明是否批准交易的授权响应消息。在某些实施例中，支付处理网络可执行结算过程，该过程可涉及将交易发布给与用于交易的支付设备相关联的账户以及计算支付设备的每个用户的净借记或信用情况。支付处理网络可由捕获器和/或发布者操作。

[0037] “主机”可以是负责执行商户交易处理、路由决定和/或捕获的一个或多个系统，诸如服务器。主机可驻留在商户、网关、处理器或其他实体处。在某些实施例中，主机可与商户直接交换(MDEX)、增值转销商(VAR)、或其他连接模型相关联。当在此使用术语“商户主机服务器”时，将认识到可使用任何服务器，诸如支付处理器服务器。

[0038] “防篡改”安全模块(TRSM)是结合物理保护以防止损害设备所包含的密码安全参数的设备。TRSM可用于不同的保护等级。防篡改的TRSM可采用物理措施诸如硬箱(hardened casing)以使得入侵设备变得困难。篡改证明TRSM可具有硬件特征以向后续查看者证明入侵尝试，诸如将在入侵设备期间被破坏的密封圈。篡改响应TRSM可被配置成用于检测入侵尝试以及破坏敏感信息，诸如密码安全参数，如果发生了入侵尝试。

[0039] “硬件安全模块”(HSM)是具有安全密码处理器的TRSM，该安全密码处理器可管理数字密钥、加速密码过程和/或为访问服务器应用的关键密钥提供强认证。HSM可提供来自未授权访问的敏感信息的逻辑和物理保护。HSM可以是插入卡或外部安全设备的形式的物理设备。HSM可通信地耦合到主机。

[0040] 支付卡行业数据安全标准(PCI DSS)是可应用于涉及交易处理的实体的一组要求。要求的目的是维护金融数据的安全。

[0041] 每交易唯一导出密钥(DUKPT)是可为每次交易导出唯一交易密钥的密钥管理方案。DUKPT使用通常仅初始化TRSM的那一方和由TRSM加密的消息的接收方已知的基础导出密钥(BDK)。通常用从BDK导出的初始密钥注入TRSM。可从初始密钥导出交易密钥。如果导出密钥受损，未来的和过去的交易数据保持受到保护，因为不能轻易地从导出密钥确定接下来的或之前的密钥。DUKPT可用于加密与电子商务交易相关联的数据，诸如PIN和/或敏感数据。

[0042] 例如，PIN填充可包括用唯一初始密钥和密钥序列号注入的TRSM。PIN填充可为每次交易生成唯一密钥。由PIN生成的授权请求消息可包括经加密PIN分组和密钥序列号。授权请求消息可被从PIN填充传输到具有其自身TRSM的商户主机服务器。商户主机服务器TRSM可使用密钥序列号(KSN)来恢复在生成唯一初始PIN填充密钥时使用的基础导出密钥(BDK)。TRSM可使用BDK和KSN来解密经加密数据。

[0043] 三重数据加密算法(TDEA)(也称为“三重数据加密标准”、“3DES”、“三重DES”、以及“TDES”)是将数据加密标准(DES)密码算法应用到正在被加密的每个数据块三次的分组密码。

[0044] “区域加密密钥”(ZEK)可指示用于加密两个特定点(例如，主机和支付处理网络之间)之间的数据的一个或多个密钥。单独的ZEK可用于PIN和敏感数据。在优选实施例中，ZEK仅用于多方之间的敏感数据加密并且优选地与PIN、MAC或其他特定加密密钥不同。

[0045] “服务器”可包括一个或多个计算机。服务器的多个计算机可经由网络连接(诸如有线、无线、和/或互联网网络连接)通信地耦合。服务器的计算机中的一个或多个可存储数据库。

[0046] PIN和敏感数据的加密和区域转换

[0047] 当支付设备用于交易时，可为交易生成授权请求消息。授权请求消息可包括个人标识号(PIN)以及敏感数据，诸如主账号(PAN)、持卡人姓名、持卡人地址、发布者自由选择数据、或其他敏感数据。敏感数据可以是用支付设备存储的数据，诸如存储在支付设备的磁条中或芯片中。可替代地，存储数据可以是由用户提供给访问设备的数据，诸如由用户在电子商务或其他无卡交易中提供的持卡人地址信息。PIN和敏感数据可由从支付设备接收信息的访问设备加密。可基于注入到访问设备中的初始密钥使用加密密钥变体加密PIN和敏感数据。

[0048] 图1示出本技术的实施例可在其中实现的示例性系统100。系统100包括一个或多个服务器计算机、数据处理子系统以及网络，该网络可用于为交易发起授权请求消息并且将授权请求消息路由到能够批准交易的实体。当仅示出每个组件中的一个时，应当理解的是本技术的实施例可包括每个组件的多于一个。附加地，本技术的某些实施例可包括少于图1中示出的全部组件的组件。而且，图1中的组件可使用任何合适的通信协议经由任何合适的通信介质(包括互联网)通信。

[0049] 在典型的交易中，支付设备102与访问设备104对接以便发起交易。访问设备104可包括访问设备防篡改安全模块(TRSM)106。访问设备TRSM 106可物理地和/或通信地耦合到访问设备104(或可以是其组成组件)。当支付设备102与访问设备104对接时，访问信息可接收与支付设备104相关联的信息，包括敏感数据。在某些实施例中，访问设备104从存储账户信息的设备(诸如便携式通信设备)接收敏感数据和/或PIN。

[0050] 在说明性示例中，支付设备102可以是信用卡而且访问设备104可以是存储在TRSM中的PIN填充。PIN填充可具有用于接收指示PIN密码的数字输入的用户接口以及用于从支付设备的磁条获得轨迹数据的磁条阅读器。

[0051] 在其他实施例中，支付设备信息可以是由访问设备104接收的用户输入。可从支付设备102或从由访问设备106接收的用户输入接收PIN数据。

[0052] 当访问设备104接收到数据诸如PIN和支付设备信息时，TRSM 106可加密数据。在某些情况中，可能需要在加密PIN之前获得PAN。可从自支付设备102接收的信息确定敏感数据诸如PIN、持卡人姓名、持卡人地址、以及自由选择数据。可从由访问设备104从支付设备102获得的轨迹数据解析敏感数据。在某些实施例中，访问设备106通过基于PIN、PIN长度、以及PAN的子集生成PIN分组来加密PIN。访问设备104可经加密敏感数据，包括PAN、持卡人姓名、持卡人地址、自由选择数据、以及任何有待处理为敏感数据的其他信息中的一项或多项。

[0053] 访问设备TRSM 106可存储用于加密数据的初始密钥。对于每次交易，可从初始密钥导出一个或多个交易密钥。可能需要将不同的交易密钥应用于PIN和敏感数据，以便与规定相符，诸如PCI DSS。可使用从初始密钥导出的第一交易密钥加密PIN而且可使用从初始密钥导出的第二交易密钥加密敏感数据。以此方式，可使用相同的密钥管理方案(诸如DUKPT)和相同的加密算法(诸如TDEA)加密PIN和敏感数据。

[0054] 包括经加密PIN数据和经加密敏感数据的授权请求消息可由访问设备104生成并且传输到商户主机服务器108。授权请求消息可包括用于各种类型的数据的指定字段。当向授权请求消息中的数据应用加密时，加密密钥可改变与经加密数据相关联的字段的参数

(诸如数据类型、数据长度等等)。由于参数已改变,可将经加密数据放入新的字段中。例如,授权请求消息可包括大小被确定为容纳PAN的字段。当应用加密时,PAN和其他敏感数据可被放入授权请求消息的一个或多个可替代字段中。可向授权请求消息添加字段以便发信号表明经加密PAN位于经加密PAN字段中。敏感数据诸如PAN、持卡人姓名、以及自由选择数据可在访问设备104被加密并被放入授权请求消息的字段内的单独元素内,诸如ISO格式的授权请求消息的字段53。

[0055] 在某些实施例中,向授权请求消息中的敏感数据应用格式保留加密。例如,当使用格式保留加密时,可用经加密值替换PAN的数位子集,同时PNA的具体数位保持不变。在优选实施例中,PAN的前六个数位和最后四个数位保持不变而中间的数位用经加密值替换。以此方式,授权请求消息可由未被配置成用于处理具有用于存储经加密数据的可替代字段的授权请求消息的支付处理网络处理。为了发信号表明授权请求消息的PAN字段中存在经加密数据,经更改的有效期可被包括在授权请求消息的有效期字段内。例如,授权请求消息可包括与用于交易的支付设备相关联的有效期之后40年的有效期。

[0056] 商户主机服务器108可包括商户主机TRSM 110。商户主机TRSM 110可通信地和/或物理地耦合到商户主机服务器108或可以是其组成组件。在某些实施例中,商户主机TRSM 110可远离商户主机服务器108的处所。为了将交易路由到多个支付处理网络,商户可能需要具有商户主机TRSM 110以便转换授权请求消息中的经加密数据。例如,可能需要在商户主机TRSM 110转换密钥以便符合限制与访问设备TRSM 106相关联的密钥暴露的PCI DSS标准。当商户主机服务器108被配置成用于将授权请求消息路由到多个支付处理网络112-116时,商户主机服务器108可将经加密数据转换成与具体的支付处理网络相关联的区域加密密钥(ZEK)。商户主机服务器108可确定如何基于包含在授权请求消息内的信息路由授权请求消息。例如,包含根据格式保留加密方法加密的PAN的PAN字段的前六个数位可由商户主机服务器108用来确定如何路由授权请求消息。

[0057] 由商户主机TRSM 110进行转换可包括解密从访问设备104接收的授权请求消息内的PIN和敏感数据并且使用一个或多个区域加密密钥(ZEK)重新加密PIN和敏感数据。ZEK可与具体的支付处理网络相关联。ZEK通常是支付处理网络和商户主机服务器108之间的共享密钥。可能需要将不同的ZEK应用到PIN和敏感数据,例如以便符合PCI DSS。转换可由商户主机TRSM 110执行,从而使得经解密的PIN和敏感数据永不暴露给商户主机服务器108。商户主机服务器108可将包括已转换PIN和敏感数据的授权请求消息传输到授权请求消息将被路由到其上的支付处理网络112-116中的一个。

[0058] 在某些实施例中,商户主机服务器108可将授权请求消息路由到未被配置成用于处理经加密数据的支付处理网络。在这种实施例中,经加密敏感数据可被解密并且包括经解密敏感数据的授权请求消息可被从商户主机服务器108传输到支付处理网络。

[0059] 接收授权请求消息的支付处理网络可解密PAN或其他敏感数据并且还可验证PIN。支付处理网络可确定是否授权交易。在某些情况下,授权请求消息可被传输到可确定是否授权交易的发布者服务器。指示是否授权交易的授权响应消息可被从接收授权请求消息的发布者和/或支付处理网络路由回商户主机服务器108。授权响应可由访问设备104显示、打印在收条上、或者以其他方式被传送到支付账户持有人。

[0060] 将理解的是与支付处理网络或其他实体相关联的以及与TRSM相关联的服务器可

代替商户主机服务器108和商户主机TRSM 110。

[0061] 结清和结算过程通常由每个支付处理网络在固定的时间执行。该固定的时间可在网络之间不同。结清过程是交换捕获器和发布者之间的金融细节以便促进既往支付账户持有人的账户以及对消费者的结算情况进行对账。

[0062] 在TRSM内，可使用DUKPT和TDES加密和/或解密数据。将认识到可应用其他密钥管理系统(诸如主/会话和固定密钥)和/或其他加密算法(诸如RSA、DEA、ECIES、AES、或其他加密算法)。

[0063] 图2示出在访问设备和商户主机加密PIN和敏感数据的说明性流程图。在操作202，持卡人可在访问设备104展现支付设备102。在操作204，访问设备104可从支付设备102读取数据，诸如存储在支付设备的磁条内的轨迹数据。从支付设备102读取的数据可包括敏感数据，诸如PAN、持卡人姓名、以及自由选择数据。在操作206，访问设备104可接收PIN，诸如在访问设备104的用户接口接收的PIN。

[0064] 在操作208，访问设备104可使用第一密钥加密PIN。第一密钥可以是从注入到访问设备104的密钥导出的第一交易特定密钥。在操作210，访问设备104可使用第二密钥加密敏感数据。敏感数据可包括PAN、持卡人姓名、自由选择数据、持卡人地址、以及由访问设备104接收的任何其他敏感数据中的一项或多项。第二密钥可以是从注入到访问设备104的密钥导出的第二交易特定密钥。在操作212，访问设备104可生成包括经加密PIN和经加密敏感数据的授权请求消息并且将授权请求消息传输到主机服务器，诸如商户主机服务器108。

[0065] 在某些实施例中，主机设备可从访问设备接收包括经加密敏感数据的授权请求消息。授权请求可或可不包括经加密PIN。例如，访问设备可从信用卡或其他支付设备接收用于不要求PIN号码的交易的敏感数据。在这些实施例中，主机设备可转换敏感数据。

[0066] 图3是在主机转换敏感数据的说明性流程图。在操作302，主机诸如商户主机服务器108从访问设备104接收包括经加密敏感数据的授权请求消息。主机可从授权请求消息解析敏感数据。在操作304，主机可使用从基础导出密钥导出的信息解密敏感数据。为了转换敏感数据，主机可使用从与访问设备104相关联的基础导出密钥导出的信息解密敏感数据，如操作304所指示的，并且使用区域加密密钥重新加密敏感数据，如操作306所指示的。在操作308，主机可将授权请求消息传输到支付处理网络。

[0067] 在某些实施例中，主机可接收包括经加密PIN和经加密敏感数据的授权请求消息。主机可转换PIN和敏感数据。

[0068] 图4是在主机转换PIN和敏感数据的说明性流程图。在操作402，主机诸如商户主机服务器108从访问设备104接收包括经加密PIN和经加密敏感数据的授权请求消息。解密PIN可能需要经解密敏感数据诸如经解密PAN。主机可从授权请求消息解析敏感数据。在操作404，主机可使用从基础导出密钥导出的信息解密敏感数据。主机可从授权请求消息解析PIN。在操作406，主机可使用从基础导出密钥导出的信息并且在某些情况下还使用已解密PAN解密PIN。为了转换PIN，主机可使用区域加密密钥重新加密PIN，如操作408所指示的。在某些实施例中，使用区域加密密钥和已解密PAN重新加密PIN。为了转换敏感数据，主机可使用区域加密密钥重新加密敏感数据，如操作410所指示的。

[0069] 在某些实施例中，单独的区域加密密钥可用于加密PIN和敏感数据。例如，PIN特定的区域加密密钥可用于或被生成用于加密PIN号码，并且敏感数据特定区域加密密钥可用

于或被生成用于加密敏感数据。而且，每个支付处理网络112-116可使用特定于具体的支付处理网络的一个或多个区域加密密钥。因此，当授权请求消息将被路由到第一支付处理网络112时，第一PIN特定的区域加密密钥和第一敏感数据特定的区域加密密钥可用于转换，而且当授权请求消息将被路由到第二支付处理网络114时，第二PIN特定的区域加密密钥和第二敏感数据特定的区域加密密钥可用于转换。

[0070] 商户主机服务器108可确定支付处理网络112-116中的哪一个支付处理网络将接收授权请求消息。在操作412，商户主机服务器108可将包含经转换(经重新加密)PIN和经转换(经重新加密)敏感数据的授权请求消息传输到所确定的支付处理网络。

[0071] 在某些实施例中，商户主机服务器108包括用于允许由商户或支付处理网络限定的特定卡范围的“白名单”支持，以便不受保护。当在访问设备104加密敏感数据时，敏感数据的一部分可被维持在明文中以便在访问设备104使用。例如，自由选择数据字段或支付设备102的磁条上的轨迹数据的其他字段中的某些或全部数据可在授权请求消息中保持未加密。使用自由选择数据字段中的用于忠诚计划、舰艇计划等等的数据的商户可要求该数据对于数据收集或其他目的保持不加密。

[0072] 在某些实施例中，自由选择数据字段中的持卡人姓名和/或数据在加密之前可用于访问设备。例如，如果访问设备或另一个商户设备所执行的应用使用这个敏感数据(例如，在通信地连接到PIN设备的收银机显示持卡人姓名)，敏感数据可在加密之前暴露于商户设备。

[0073] 如以上所讨论的，支付设备内的芯片或磁条可具有保持数据的一个或多个轨迹(通常是三条轨迹，称为“轨迹I”、“轨迹II”、“轨迹III”)。可根据标准化结构将数据格式化。图5和图6是示出用于支付设备轨迹数据的说明性规范的表格。将认识到具有图5和图6中所描述的结构的轨迹数据可被与便携式媒体设备或用于电子商务或其他无卡交易的其他设备上的支付账户相关联地存储。

[0074] 图5是表格，示出支付设备的轨迹I的结构和内容的说明性规范。用基于ASCII的7比特方案编码轨迹1。轨迹1字段可包括开始哨符(诸如“%”)，指示格式化轨迹数据在其开始的位置。

[0075] 格式代码(诸如“B”，指示金融机构)通常是轨迹1内的下一个字符。

[0076] 主账号(PAN)可包括六数位发布者标识号(IIN)、可变长度(最大12个数位)、单独的账号可校验数位。可用分隔符字符(诸如插入符号(^))指示与PAN相关联的数据的结尾。

[0077] 姓名字段可包括单个阿尔法字符(作为姓氏)以及姓氏分隔符。空格字符可被要求将姓名字段而不是姓氏的逻辑元素分隔开。可在姓名字段的最后一个逻辑元素之后编码终止姓名字段的分隔符。如果仅编码姓氏，姓氏之后可以是字段分隔符(FS)，诸如“^”。在某些实施例中，姓名字段包括姓氏、其后是姓氏分隔符(例如，“/”字符)、其后是名或大写首字母、其后是空格、其后是中间名或大写首字母。姓名可附加地在中间名或大写首字母之后包括句号，其后是头衔。姓名通常用分隔符(字符“^”)结束。例如，姓名John C.Smith()可被编码为“SMITH/JOHN C”。

[0078] 轨迹I的有效期字段可具有格式YYMM，其中‘YY’表示年份的最后两个数位并且‘MM’是月份的数字表示。

[0079] 服务代码可以是具有由单独的数位表示的三个子字段的数字字段。通常，服务代

码用于指示发布者对磁条交易的接受标准以及支持如磁条或浮雕所标识的等效应用的相关集成电路是否存在于卡上。服务代码的每个子字段可由其位置(位置1、2和3)表示并且可独立地操作,允许判断其单独的功能。

[0080] 发布者自由选择数据可遵循服务代码。轨迹的结束由结束哨符指示,诸如问号字符(“?”)。在结束哨符之后,可包括纵向冗余校验字符(LRC)。

[0081] 图6是表格,示出支付设备的轨迹II的结构和内容的说明性规范。轨迹II中的字符编码基于以ASCII为基础的5比特方案。轨迹II可包含与轨迹I中所包含的那些字段相似的字段,如上所述,但是可缺少持卡人姓名字段。

[0082] 在某些实施例中,PIN数据可被存储在支付设备的轨迹III上并可从其读取。

[0083] 具有混淆的加密

[0084] 在对与支付设备102相关联的数据字段执行加密后,经加密信息可被存储在授权请求消息的一个或多个替代字段中并且混淆数据可被存储在授权请求消息的原始字段中。例如,可从与支付设备102相关联的PAN、持卡人姓名、以及自由选择数据字段读取数据。混淆数据可被写入为PAN、持卡人姓名、和自由选择数据指定的授权请求消息的字段中并且PAN、持卡人姓名、和自由选择数据的经加密版本可被写入授权请求消息的一个或多个替代字段中。

[0085] 在说明性示例中,对于符合ISO标准的授权请求消息而言,替代字段诸如ISO字段53可被限定为接收经加密数据和相关联的加密属性。ISO字段53的新定义可符合在ISO标准中定义的“复合”字段类型。新字段53可接收经加密PIN分组数据和经加密敏感数据。当向授权请求消息应用区域加密时,可向字段53应用区域加密。

[0086] 当混淆数据被写入授权请求消息的PAN字段时,所保持的PAN字段中的PAN的某些数位可被保持而可混淆PAN的其他数位。例如,PAN的数位子集(“中间六个”数位)可被混淆,而其他数位(诸如PAN的前六个和最后四个数位)保持为明文。可通过例如用数字9替换PAN的数位7-11并且用被计算以便确保PAN的最后一个数位是有效校验数位的数字替换PAN的数位12来执行混淆。因为PAN的剩余数位诸如前六个数位和最后四个数位未被混淆,剩余数位可被用于诸如路由和接收方确定功能。以此方式,被设计成用于处理包含在PAN字段中的数据的系统可正常地起作用,尽管通过混淆中间的六个数位来保护PAN。存储在经加密PAN字段中的经加密PAN可被解密,允许将经解密(原始)PAN写入PAN字段中。

[0087] 格式保留的加密

[0088] 可能令人希望的是在不更改授权请求消息的格式的情况下加密包含在授权请求消息内的数据。例如,某些系统可能未被设计成用于处理具有附加经加密PAN字段的授权请求消息。可向来自与支付设备102相关联的轨迹数据的轨迹1和轨迹2的敏感数据诸如PAN、持卡人姓名以及自由选择数据应用格式保留加密。

[0089] PAN可被加密,从而使得所得经加密PAN具有与原始PAN相同的大小。以此方式,经加密PAN可被写入授权请求消息的原始PAN字段中,并且不要求授权请求消息的替代字段接收经加密PAN。当向PAN应用格式保留加密时,PAN的某些数位可保持未加密。例如,PAN的前六个和最后四个数位可保持未加密,以便允许路由和与包含在这些数位内的数据相关的其他功能。

[0090] 格式保留加密的作用不同于包含有效校验数位的PAN。用于确定有效校验数位的

算法可以如ISO标准中所定义的那样。通常是PAN的最后一个数位的校验位可以是从可用于确定PAN的所有数位是否被正确地接收的消息内的其他数位计算的数位。校验位可用于检测传输错误。在某些实施例中，计算PAN的数位7-12(“中间六个”数位)的最后一个数位，从而使得未经加密PAN的原始最后一个数位仍然是用格式保留加密进行加密的PAN的有效校验数位。当PAN不包含有效校验数位时，可用格式保留加密算法加密所有中间数位。

[0091] 在加密之前，敏感数据可被转换为10基字母表。在已经应用了格式保留加密后，10基字母表中的所得经加密字符可被转换为原始代码集合和原始敏感数据的格式。经转换的加密结果可用于替换授权请求消息内的敏感数据诸如PAN、持卡人姓名、自由选择数据等等的原始字段。

[0092] 通常，从已经向其应用格式保留加密的字段中的数据来看，数据已经被加密将是不明显的。可在授权请求消息的现有数据字段中使用信号以便表明授权请求消息的字段包含经加密数据。为了实现该信号，可用授权请求消息的不包含经加密数据的字段的已修改版本的新内容盖写该字段。例如，授权请求消息的有效期字段中的有效期可被经更改的有效期替换。在一个实施例中，通过向有效期或有效期的一部分添加数字来获得经更改的有效期。例如，数字诸如40可被添加到有效期的年份部分。如果授权请求消息的有效期字段包含有效期“01/13”，表明有效期是2013年1月，数字40可被添加到年份部分13并且所得经更改的有效期“01/53”可被写入有效期字段。如果2013年发生了交易，读取授权请求消息的有效期部分的设备可能够确定有效期是经更改的有效期，因为支付设备通常被发布有低于从发布该卡的日期起20年(例如，1-10年)的有效期。以此为基础，可确定超过当前日期二十年的有效期是经更改的有效期。

[0093] 在某些实施例中，PAN的最后一个数位可不包含有效校验数位。例如，PAN的最后一个数位可不具有ISO/IEC标准7812-1所规定的校验位。当PAN的最后一个数位不是有效校验数位时，在经更改的有效期被写入授权请求消息的有效期字段之前，数字20可被添加到有效期的月份。

[0094] 在某些实施例中，有效期字段可从访问设备104所接收的信息消失。例如，卡读取或密钥输入可具有错误或者以其他方式缺少有效期。在经更改的有效期被写入授权请求消息的有效期字段之前，数字40可被添加到在格式保留加密过程中创建的有效期的月份。

[0095] 以下，描述用于格式保留加密的示例性算法。格式保留加密算法可像格式被保留的流式密码那样运行。例如，格式保留加密可类似于来自国际标准与技术研究所(NIST)标准P800-38A的计数器模式(CTR)，被概括为模n加法而不是模2加法。

[0096] 在格式保留算法中，A可以是具有n个不同的字符的字母表，其中n是大于1的自然数。A*可被标记为具有来自A的元素的字符串集合，包括空字符串。在本说明书中，假设字母表A是集合{0,…,n-1}。如果不是这种情况，需要转换，基于字母表A中的不同字符的数量。该转换可在加密之前发生并且在解密之后再次发生，从而使得加密和解密将永远针对某些大于1的正整数n的形式{0,…,n-1}的字母表有效。

[0097] 格式保留算法可使用SP800-38A中定义的具有分组大小b个比特的分组密钥CIPH(AES或TDEA)的计数器模式(CTR)以及CIPH的加密密钥K、以及一系列计数器分组(在SP800-38A中被称为计数器)T1、T2、…，以便产生一系列输出分组，每个计数器模块一个输出分组。每个输出分组由k个n基数位组成，其中k是必须从区间$\{1,\ldots,\lfloor \log_n 2^b \rfloor\}$选择的可配置参数。出

于以下解释的原因，每个计数器分组是b-7个比特，而不是SP800-38A中的b个比特。还在以下描述如何产生输出分组的机制。

[0098] 为了加密长度为L的明文P，其中1≤L，生成尽可能多的输出分组(但是不需要更多)，从而使得输出分组中的n基数位的总数量是至少L，即，我们计算唯一整数p和r，从而使得$\frac{L}{k} \le p < \frac{L}{k}+1$并且0≤r<k，从而使得L＝pk-r，并且生成输出分组G1、…、Gp。然后，向来自输出分组$G_1 \| G_2 \| \cdots \| G_p$的级联的第i个n基数位添加每个明文n基数位P[i]，从而形成密文的第i个数位：

[0099] $C[i] = (P[i] + (G_1 \| \cdots \| G_p)[i]) \bmod n$。

[0100] 由于k可能不除以L，可忽略最后一个输出分组Gp的某些数位。不使用Gr的最后r个n基数位。

[0101] 为了解密长度为L的密文C，其中1≤L，生成尽可能多的输出分组(但是不需要更多)，从而使得输出分组中的n基数位的总数量超过L，这是用与加密相同的方式完成的。然后，从输出分组G1‖…‖Gp的级联的第i个n基数位减去每个密文n基数位C[i]，从而形成明文的第i个数位：

[0102] $C[i] = (P[i] + (G_1 \| \cdots \| G_p)[i]) \bmod n$。

[0103] 为了进行格式保留加密，至于计数器模式自身，该计数器分组序列必需具有以下特性：该序列中的每个分组不同于另一个分组。这种条件不限于单次加密：跨在给定密钥K下加密的所有报文，所有计数器必须不同。SP800-38A描述了用于生成计数器的方法。

[0104] 给定具有模块长度b的分组密文CIPH，CIPH的密钥K、b-7比特计数器T、自然数n>1，其是将被加密的明文的基数，以及具有$0 < k \le \lfloor \log_n(2^b) \rfloor$的整数k，以如下方式产生由k个n基数位组成的输出分组：

[0105] 7比特计数器S被初始化为0。然后，向S‖T应用CIPHK从而产生具有b个比特的分组B。B被解释为区间$\{0,\cdots,2^b-1\}$中的整数，并且如果$B < n^k$，则接受，否则S增量并且CIPHK被再次应用到S‖T等等，直到B被接受或S等于127。如果S＝127，提高错误，否则B被转换为n基并且是k数位n基输出分组，可能具有多个前导零。假设CIPHK是伪随机置换，每次迭代中B被接受的可能性至少是0.5，并且提高错误的可能性最多是2-128。以下伪代码描述了这种算法：

```
i = 0;
Input_Block = Si ‖ T ;
max_B = (n^k)*((2^b) div (n^k));
B = CIPH(K, Input_Block);
while ( (AsInteger(B) ≥ max_B) AND (i < 127)) {
   i = i+1;
   Input_Block = Si ‖ T ;
   B = CIPH(K, Input_Block);
};
if (i=127) return ERROR;
Output_Block = Convert(B, k, n);
return Output_Block;
```

[0106]

[0107] 在此，假设S0、S1、...、S127枚举了128种不同的7比特组合，假设“AsInteger”取b个比特B[1]、...、B[b]的字符串并且将其转换为整数$\sum_{i=1}^{b}(B[i]\,2^{b-i})$，并且假设“Convert”将B转换为k个n基数位，具有多个前导零，如果必要的话：

```
Convert(B, k, n) {
   M = AsInteger(B);
   for (i=1; i≤k; i++){
      D[i] = M mod n;
      M = M div n;
   };
   return D;
}
```

[0108]

[0109] L的最大值(即，可被加密的最长的明文的比特长度)是$2^{b/2}$。

[0110] 被解释为整数的B的上边界$n^k\left\lfloor \frac{2^b}{n^k} \right\rfloor$被选择为$n^k$的最大可能整数倍数，其使得可统一地从其提取k数位n基数字，假设B的分布是均匀的。

[0111] 图7是流程图，示出根据实施例的格式保留加密的实现方式。参照图7描述的操作可由例如访问设备或主机执行。在操作702，读取PAN。PAN可由访问设备104从支付设备102读取。可替代地，PAN可从授权请求消息的PAN字段读取。

[0112] 在操作704，加密PAN的至少一部分，从而使得经加密PAN的长度等于原始PAN的长度。PAN可由访问设备104或商户主机服务器108加密。在操作706，已加密PAN可被写入授权

请求的PAN字段。在操作708，可从授权请求消息的有效期字段(或从支付设备)读取有效期。在操作710，经更改的有效期可被写入授权请求消息。可通过例如向原始有效期的年份部分添加数字来更改有效期。添加到原始有效期的数字可以是5-99之间的数字，诸如10和50之间的数字，例如40。将认识到可使用可替代算法，诸如从原始有效期减去某个数字。

[0113] 图8是示出解释数据以便确定是否已经应用格式保留加密的流程图。参照图8描述的操作可由例如商户主机服务器108、支付处理网络112-116、发布者、捕获器等等执行。在操作800，接收授权请求消息。例如，可从商户主机服务器108或支付处理网络授权请求消息。在决定菱形802，可确定从授权请求消息读取的有效期字段的有效期的年份部分是否小于距当前日期的具体年份数字，例如，距当前日期20年。如果有效年份小于距当前日期20年，在授权请求消息中不存在对格式保留加密的信号，如804所指示的。如果有效期多于距当前日期20年，可从PAN字段读取PAN的未经加密数据，如操作806所指示的。未经加密PAN数据可用于路由(例如，由商户主机服务器108)、欺诈检测、授权确定、或其他目的。

[0114] 计算机系统

[0115] 图9是可用于实现上述任何实体或组件(例如，访问设备、主机、支付处理网络、捕获器处理器等等)的计算机系统的说明性高级框图。图9中所示的子系统经由系统总线902互连。附加子系统诸如打印机904、键盘906、固定磁盘908、以及监视器耦合到显示器适配器912。耦合到I/O控制器914的外围设备和输入/输出(I/O)设备可通过本领域已知的任何数量的手段(诸如串行端口916)连接到计算机系统。例如，串行端口916或外部接口918可用于将计算机装置连接到广域网，诸如互联网、鼠标输入设备、或扫描仪。经由系统总线902的互连允许处理器920与每个子系统通信并且控制来自系统存储器922或固定磁盘908的指令的执行以及子系统之间的信息交换。系统存储器922和/或固定磁盘908可实现计算机可读介质。

[0116] 如所述，本发明服务可涉及实现一个或多个功能、过程、操作或方法步骤。在某些实施例中，这些功能、过程、操作或方法步骤可被实现为由适当地编程的计算设备、微处理器、数据处理器等等执行指令集或软件代码的结果。该指令集或软件代码可被存储在由计算机设备、微处理器等等访问的存储器中或其他形式的数据存储元件中。在其他实施例中，这些功能、过程、操作或方法步骤可由固件或专用处理器、集成电路等等实现。

[0117] 应当理解的是能够使用模块或集成方式的计算机软件以控制逻辑的形式实现如上所述的本发明。基于在此提供的公开和教导，本领域普通技术人员可知道并认识到用于使用硬件以及硬件和软件的组合实现本发明的其他方式和/或方法。

[0118] 在本申请中所述的任何软件组件或功能可被实现为将被处理器使用任何适当的计算机语言(诸如例如使用例如常规或面向对象的技术的Java、C++或Perl)执行的软件代码。软件代码可被存储为计算机可读介质上的一系列指令或命令，诸如随机存取存储器(RAM)、只读存储器(ROM)、磁介质诸如硬盘驱动器或软盘、或光介质诸如CD-ROM。任何这种计算机可读介质可驻留在单个计算装置上或内，并且可存在于系统或网络的不同计算装置上或内。

[0119] 尽管已经描述了并且在附图中示出了某些实施例，应当理解的是这种实施例仅仅示出而非限制宽泛的发明，并且本发明不应被限制为所示出和描述的特定的构造和安排，因为当学习本公开时，本领域普通技术人员将认识到各种其他修改。

[0120] 对“一种”或“该”的引述旨在指代“一个或多个”，除非相反明确地指明。

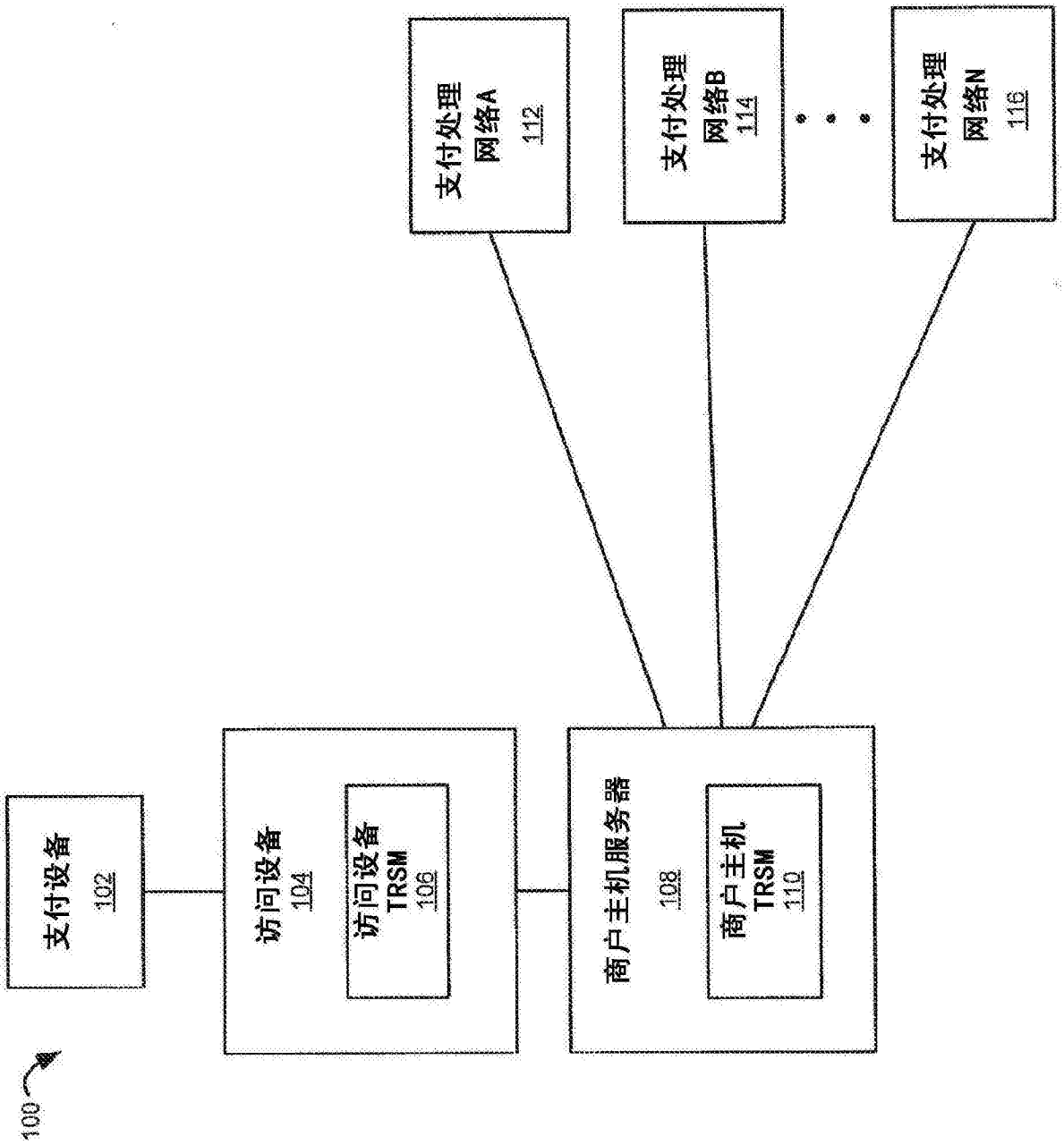

支付处理网络A 112
支付处理网络B 114
支付处理网络N 116
支付设备 102
访问设备 104
访问设备TRSM 106
商户主机服务器 108
商户主机TRSM 110
100

图1

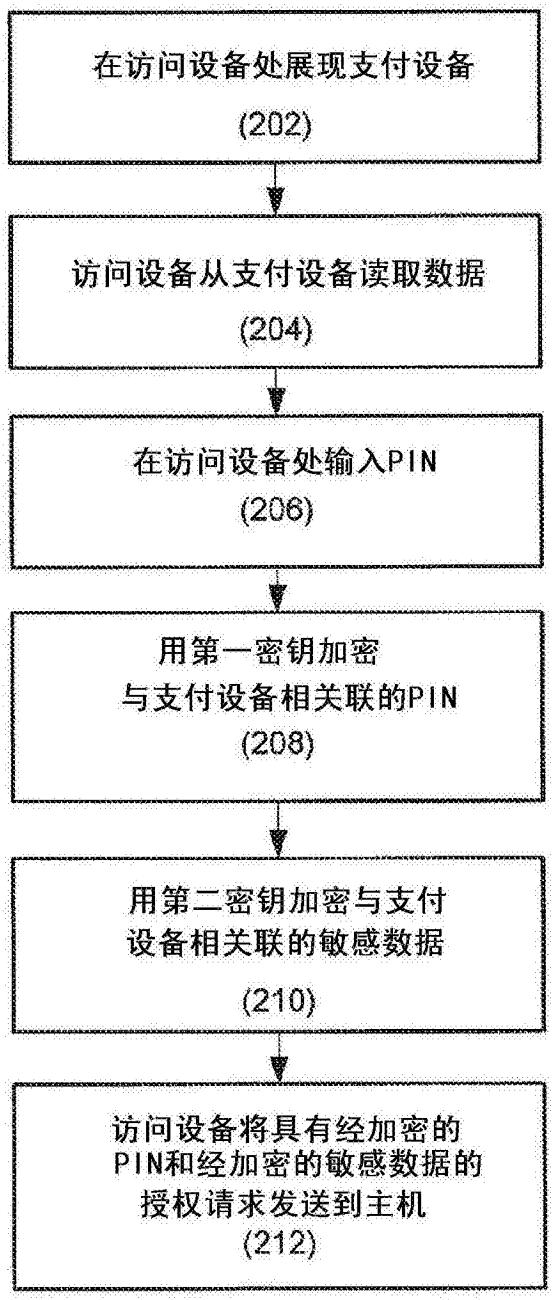

在访问设备处展现支付设备
(202)
访问设备从支付设备读取数据
(204)
在访问设备处输入PIN
(206)
用第一密钥加密
与支付设备相关联的PIN
(208)
用第二密钥加密与支付
设备相关联的敏感数据
(210)
访问设备将具有经加密的
PIN和经加密的敏感数据的
授权请求发送到主机
(212)

图2

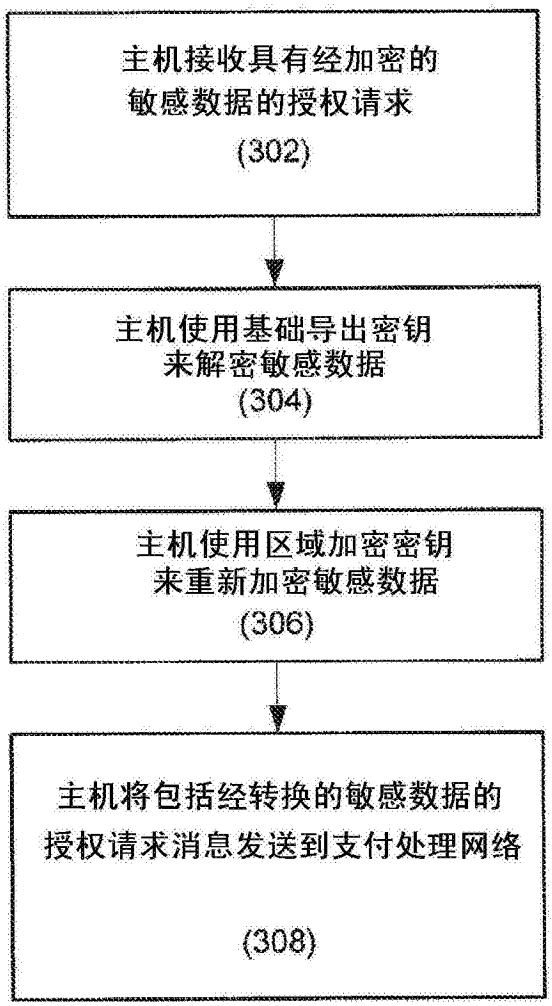

主机接收具有经加密的
敏感数据的授权请求
(302)
主机使用基础导出密钥
来解密敏感数据
(304)
主机使用区域加密密钥
来重新加密敏感数据
(306)
主机将包括经转换的敏感数据的
授权请求消息发送到支付处理网络
(308)

图3

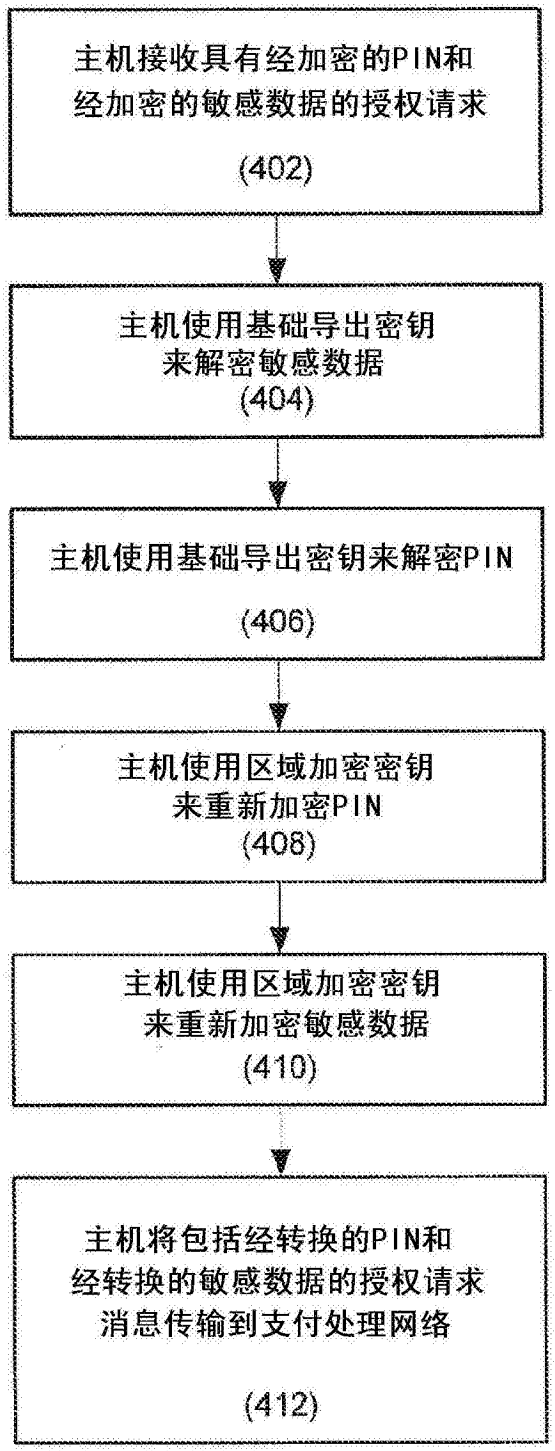
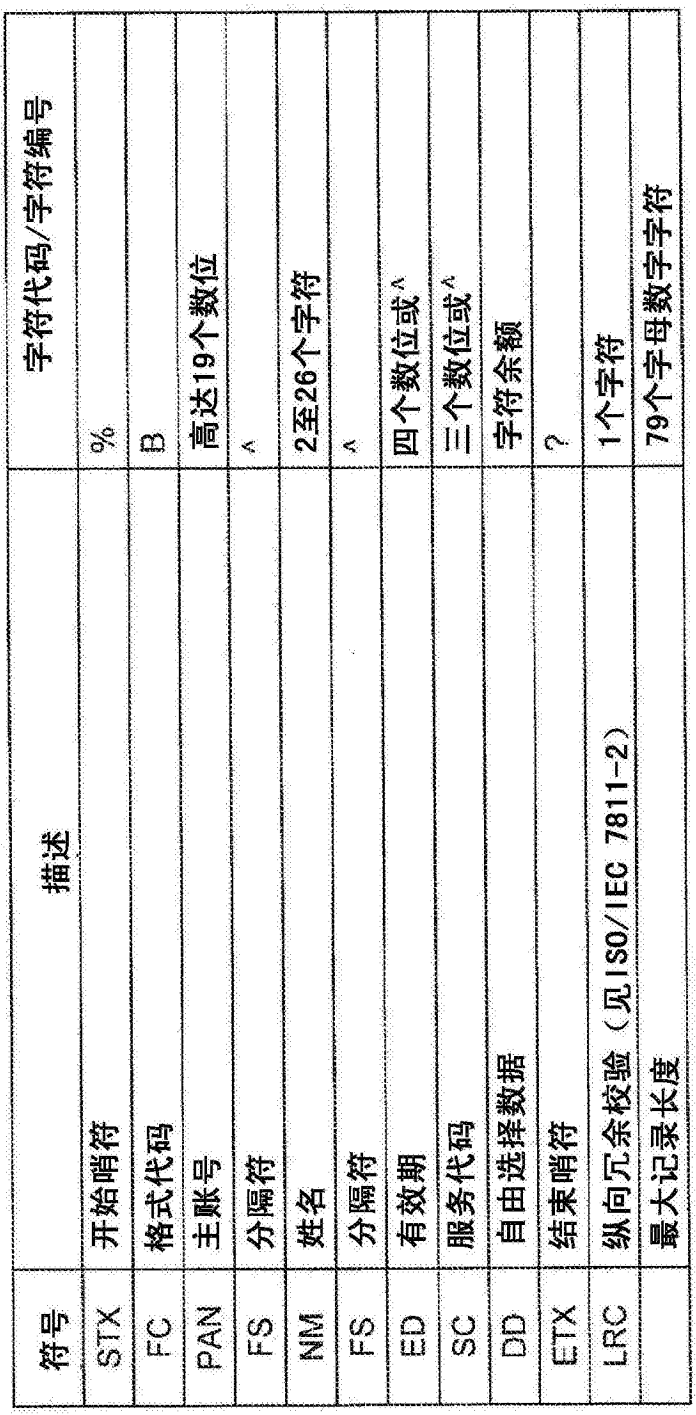
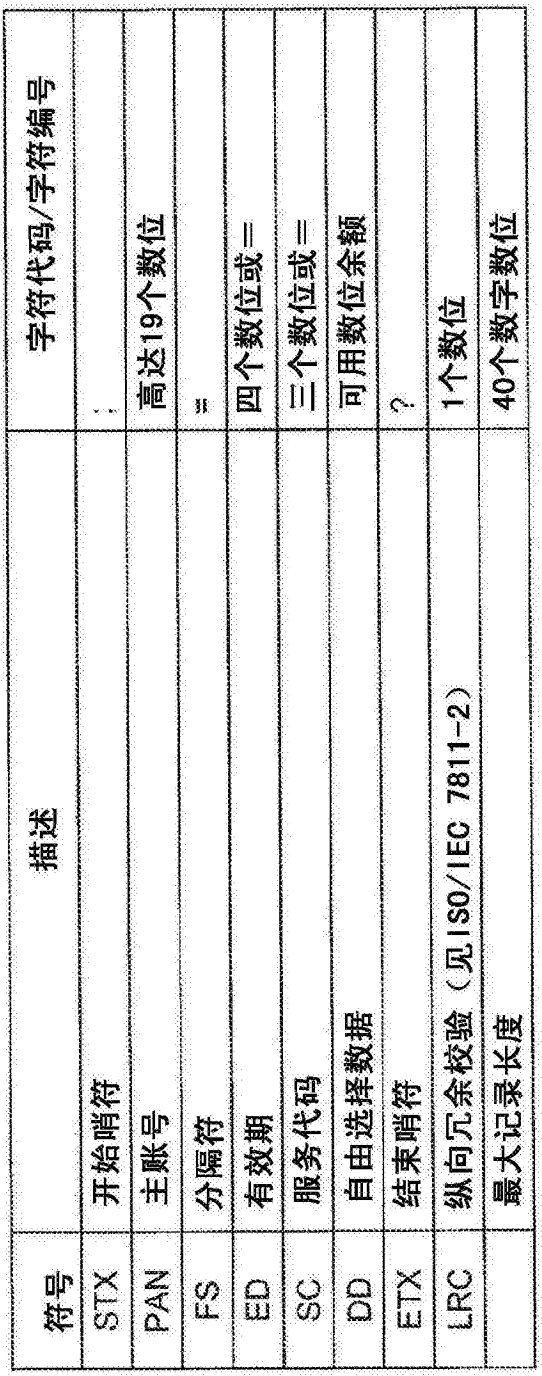

主机接收具有经加密的PIN和
经加密的敏感数据的授权请求
(402)
主机使用基础导出密钥
来解密敏感数据
(404)
主机使用基础导出密钥来解密PIN
(406)
主机使用区域加密密钥
来重新加密PIN
(408)
主机使用区域加密密钥
来重新加密敏感数据
(410)
主机将包括经转换的PIN和
经转换的敏感数据的授权请求
消息传输到支付处理网络
(412)

图4



符号	描述	字符代码/字符编号
STX	开始哨符	%
FC	格式代码	B
PAN	主账号	高达19个数位
FS	分隔符	^
NM	姓名	2至26个字符
FS	分隔符	^
ED	有效期	四个数位或^
SC	服务代码	三个数位或^
DD	自由选择数据	字符余额
ETX	结束哨符	?
LRC	纵向冗余校验（见ISO/IEC 7811-2）	1个字符
	最大记录长度	79个字母数字字符

图5



符号	描述	字符代码/字符编号
STX	开始哨符	;
PAN	主账号	高达19个数位
FS	分隔符	=
ED	有效期	四个数位或=
SC	服务代码	三个数位或=
DD	自由选择数据	可用数位余额
ETX	结束哨符	?
LRC	纵向冗余校验（见ISO/IEC 7811-2）	1个数位
	最大记录长度	40个数字数位

图6

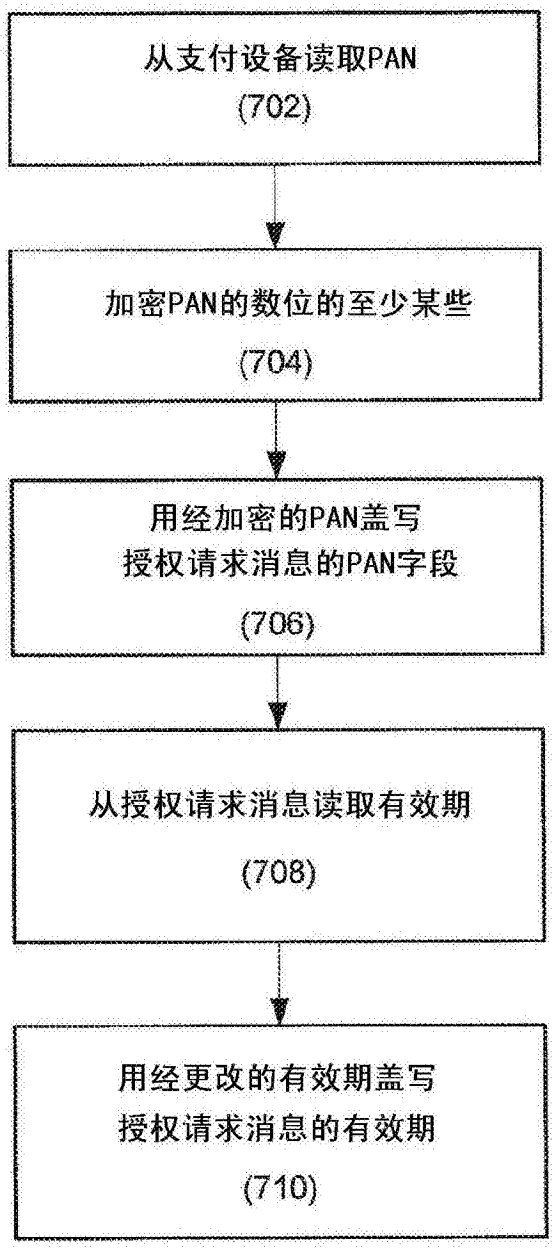

从支付设备读取PAN
(702)
加密PAN的数位的至少某些
(704)
用经加密的PAN盖写
授权请求消息的PAN字段
(706)
从授权请求消息读取有效期
(708)
用经更改的有效期盖写
授权请求消息的有效期
(710)

图7

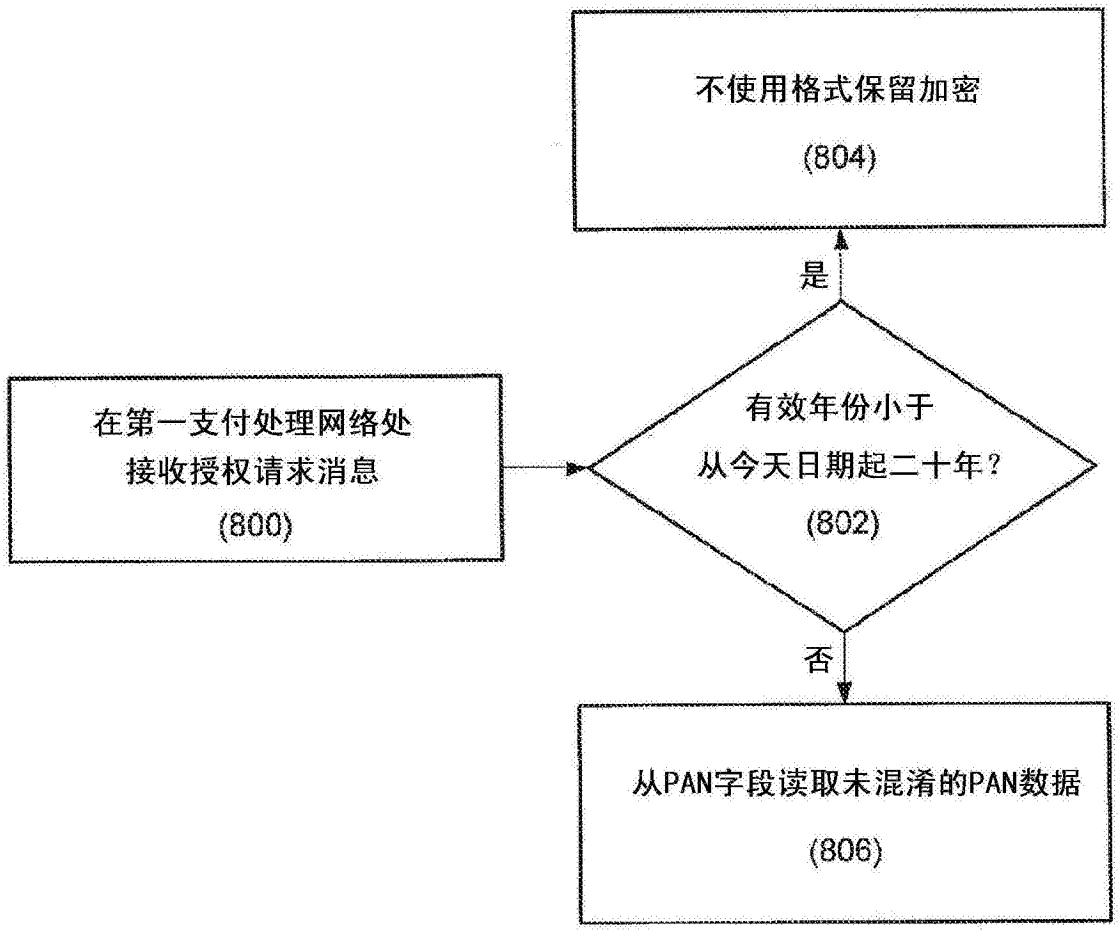

不使用格式保留加密
(804)
是
在第一支付处理网络处
接收授权请求消息
(800)
有效年份小于
从今天日期起二十年？
(802)
否
从PAN字段读取未混淆的PAN数据
(806)

图8

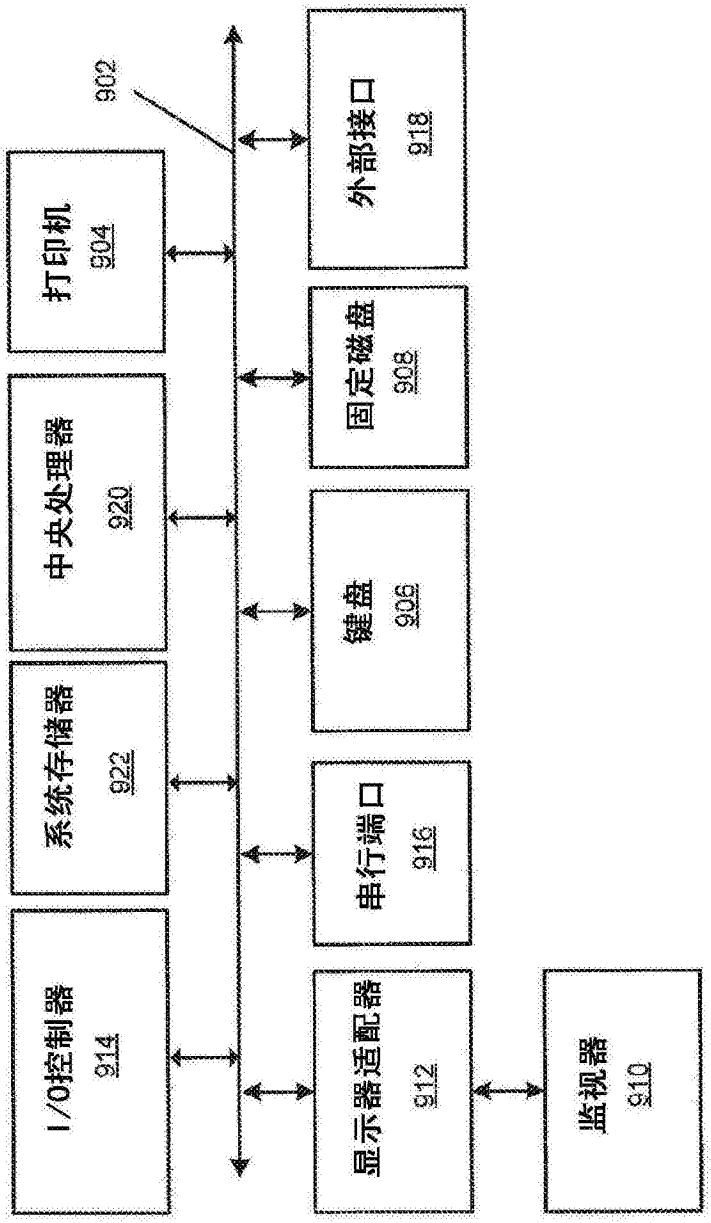

902
打印机
904
中央处理器
920
系统存储器
922
I/O控制器
914
外部接口
918
固定磁盘
908
键盘
906
串行端口
916
显示器适配器
912
监视器
910

图9