

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06Q 99/00 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200580028482.0

[43] 公开日 2007 年 10 月 3 日

[11] 公开号 CN 101048794A

[22] 申请日 2005.8.18

[21] 申请号 200580028482.0

[30] 优先权

[32] 2004.8.18 [33] US [31] 60/602,594

[86] 国际申请 PCT/US2005/029758 2005.8.18

[87] 国际公布 WO2006/023839 英 2006.3.2

[85] 进入国家阶段日期 2007.2.25

[71] 申请人 万事达卡国际股份有限公司

地址 美国纽约州

[72] 发明人 J·万克穆勒

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 张鑫

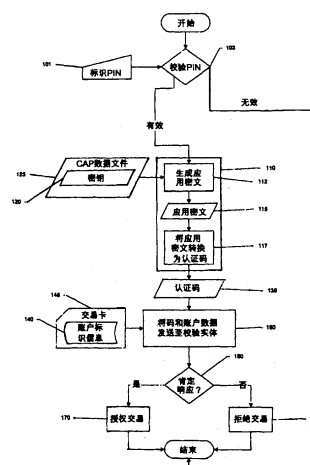
权利要求书 3 页 说明书 10 页 附图 3 页

[54] 发明名称

使用动态授权码授权交易的方法和系统

[57] 摘要

一种用于执行安全交易的方法和装置包括基于不能标识账户的保密数据在移动装置上生成动态认证码。认证码和金融账户标识信息被发送到共享关于该保密数据的信息的验证实体，以授权交易。



1. 一种用于授权交易的方法，所述方法包括：

将账户保密数据与授权数据库中的唯一金融账户标识符相关联；

至少部分地基于与所述账户保密数据相关联的数据生成个人化数据；

将所述个人化数据发送至移动处理设备用于存储，所述移动处理设备不包含所述唯一金融账户标识符；

在授权端接收授权请求以授权交易，所述请求包括所述唯一金融账户标识符和由所述移动处理设备生成的动态认证码；

判断所述动态认证码是否是由包含至少部分地基于与账户保密数据相关联的数据而生成的个人化数据的移动处理设备生成的，其中账户保密数据与授权数据库中的金融账户标识符相关联；以及

根据所述判断步骤授权所述交易。

2. 如权利要求 1 所述的方法，其特征在于，进一步包括：

所述移动处理设备提示输入标识 PIN；以及

在移动处理设备生成所述动态认证码之前，由移动处理设备验证所述标识 PIN。

3. 如权利要求 1 所述的方法，其特征在于，所述账户保密数据是加密密钥。

4. 如权利要求 3 所述的方法，其特征在于，与账户保密数据相关联的所述数据是所述加密密钥。

5. 如权利要求 3 所述的方法，其特征在于，所述加密密钥是私钥，并且与账户保密数据相关联的所述数据是与所述私钥相关联的公钥。

6. 如权利要求 1 所述的方法, 其特征在于, 由所述移动处理设备生成的所述动态认证码至少部分基于存储在所述移动处理设备上的交易计数器。

7. 如权利要求 6 所述的方法, 其特征在于, 所述交易计数器的副本被保存在所述授权数据库中, 所述方法进一步包括校验用于生成所述动态认证码的所述交易计数器是否与所述交易计数器的所述副本相匹配。

8. 如权利要求 6 所述的方法, 其特征在于, 当生成所述动态认证码时, 所述交易计数器递增。

9. 一种用于授权交易的系统, 其特征在于, 所述系统包括:

包含至少一个唯一金融账户标识符以及与所述标识符相关联的账户保密数据的授权数据库;

不包含所述唯一金融账户标识符、用于生成动态认证码的移动处理设备;

用于将个人化数据发送至所述移动处理设备的发射器, 所述个人化数据至少部分地基于与所述账户保密数据相关联的数据;

用于接收授权请求以授权交易的接收器, 所述授权请求包括所述唯一金融账户标识符和动态认证码;

授权处理器, 用于判断所述动态认证码是否是由包含至少部分地基于与账户保密数据相关联的数据而生成的个人化数据的移动处理设备生成的, 其中账户保密数据与认证数据库中的金融账户标识符相关联, 以及根据所述判断步骤授权所述交易。

10. 如权利要求 9 所述的系统, 其特征在于, 所述账户保密数据是加密密钥。

11. 如权利要求 10 所述的系统, 其特征在于, 与账户保密数据相关联的

所述数据是所述加密密钥。

12. 如权利要求 10 所述的系统，其特征在于，所述加密密钥是私钥，并且与账户保密数据相关联的所述数据是与所述私钥相关联的公钥。

13. 如权利要求 9 所述的系统，其特征在于，所述移动处理设备包括交易计数器，并且所述移动处理设备至少部分地使用所述交易计数器来生成所述动态认证码。

14. 如权利要求 13 所述的系统，其特征在于，所述授权数据库进一步包括所述交易计数器的副本，并且所述授权处理器进一步用于校验用于生成所述动态认证码的所述交易计数器是否与所述交易计数器的所述副本相匹配。

15. 如权利要求 13 所述的系统，其特征在于，当生成所述动态认证码时，所述交易计数器递增。

使用动态授权码授权交易的方法和系统

相关申请

本申请要求于 2004 年 8 月 18 日提交的申请号为 60/602, 594 的题为“用于生成支付或金融交易使用的授权码的方法和系统 (Method And System for Generating Authentication Codes For Use in Payment or Financial Transactions)”的美国临时申请的优先权。

背景技术

在远程交易中信用卡和借记卡的使用一直持续增长。无论是通过电话、通过邮件、在零售店、或者通过互联网，共同的是需要不经过面对面的接触而进行交易。然而，远程交易没有面对面交易安全并且欺诈的可能性相对较高，尤其是当交易卡遗失或被窃。

一种最小化欺诈的方法是通过使用个人标识号或者 PIN。用这种方法，在交易时，用户的卡插入或者划过读卡器。读取器从卡上提取特定数据，如账号。接着读卡器要求用户在小键盘上输入他或她的 PIN。PIN 被加密或以其它方式进行保护，而安全的 PIN 数据被发送至授权端，诸如授权计算机，在那里存储着持卡人数据。在授权计算机处，用账户标识数据来查找并获取账户信息，获取的信息被用于校验持卡人输入的 PIN 是否正确。这种方法使欺诈减至最小，因为卡的拥有者必须同时知道保密的 PIN 以完成交易。这种方法的一项缺点是：由于 PIN 是静态的，窃贼可以在合法交易中截取 PIN 并在之后的欺诈交易中重新使用该 PIN。

在另一种本发明人最近建议的方法中，用频繁改变的动态码来取代静态 PIN。这种方法在共同待批的申请号为 60/626,649 的题为“允许使用动态码用于认证的方法和系统(Method And System For Enabling The Use Of Dynamic Codes For Authentication)”的美国专利申请中有更详细的描述，该申请全文被引用并

合并与此。这种方法的一个方面包括使用智能卡和智能卡读取器来生成动态码。智能卡是本领域公知的，其典型地是信用卡状的卡，并包括安全数据存储区域和处理器。在可能交易时，智能卡用智能卡的安全存储器中存储的保密数据生成应用密文。应用密文的生成是本领域公知的，例如，在由 EMVCo.LLC 发布的可在互联网上地址为 <http://www.emvco.com> 看到的题为“用于支付系统的 EMV 集成电路卡规范 (EMV Integrated Circuit Card Specifications for Payment Systems)”的公知的智能卡规范中有更详细的解释，该规范被引用整体上结合于此。接着该数据（或其一部分）被作为动态码发送至授权计算机。授权计算机可基于从授权数据库获取的与账号相关联的账户信息来校验是否该动态码是由与当前使用的账号相关联的智能卡生成以完成交易的。

使用智能卡以增强交易的安全性的一项缺点是与更传统的磁条式卡相比制造相对昂贵。另外，智能卡需要在每次交易中使用智能卡读取器，这就需要对现有的为磁条式卡设计的销售点进行升级。由于这些或其它的原因，智能卡和智能卡读取器尚没有在美国境内广泛使用。

发明内容

本发明使交易可以以更安全的方式被授权而不需要广泛设置智能卡和智能卡读取器。取而代之地，使用持卡者已经拥有的（诸如 PDA 或者手机之类的）移动消费设备的处理能力来生成与具体持卡者账户相关联的动态授权码。移动设备不会包含可以识别与之相关联的具体账户的数据。接着，动态码与账户标识数据一起被发送至认证计算机以校验交易的真实性。

在本发明的一个示例性的实施例中，提供了一种授权交易的方法。该方法需要将账户保密数据与授权数据库中唯一的金融账户标识符相关联，并至少部分地基于与该账户保密数据相关联的数据生成个人化数据。个人化数据被发送至移动处理设备（诸如 PDA 或手机）用于存储于其中，该移动处理设备不包含所述唯一的金融账户标识符。接着，授权端接收到授权请求。该请求包括金融账户标识符和由移动处理设备生成的动态认证码。接着进行判断，判断该认证码是否是由包含至少部分地基于与账户保密数据相关联的数据而生成的个

人化数据的移动处理设备生成的，其中账户保密数据与授权数据库中的金融账户标识符相关联。

附图说明

为了对本发明更全面的理解，下面结合附图给出以下对示例性的实施例的详细描述，在附图中：

图 1 是根据本发明的一个示例性实施例的使用生成的认证码和账户标识信息进行交易的步骤的流程图；

图 2 是用于生成认证码的一个示例性系统的方框图；以及

图 3 是本发明的一个示例性实施例的方框图。

具体实施方式

图 1 是描述本发明的一个示例性实施例的流程图，其限定了使用生成的动态认证码 130 和账户标识信息或唯一金融账户标识符 140 来进行交易。以下描述将基于假设的通过（诸如互联网之类的）计算机网络进行的交易。然而，可以理解的是本发明的实施例不局限于通过计算机网络的交易，而是可以容易地适用于其它类型的交易，诸如通过电话、邮件、面对面、或其它方式的交易。

假设的交易开始于个人计算机（PC）用户使用网络浏览器或类似运行在个人计算机上的应用软件发起请求以购买来自销售商的货物或服务。需要注意的是，任何用于请求或进行交易的设备、系统或方案均可用来替换 PC，这包括诸如 PDA 或手机之类的移动设备。接着用户的请求使销售商的计算机调用授权请求服务器以认证用户的身份并校验交易是否合法。授权请求服务器或授权处理器（其可以是大型机或其它具有处理器、存储器以及通信连接的计算机）提示用户使用他或她的移动处理设备来提供动态授权码。

在步骤 101，用户激活他或她的移动处理设备（诸如个人数字助理（PDA）或手机）并调用功能以生成动态认证码。（在此将更详细讨论的）

移动处理设备包括用于生成动态码的软件或电路。在具体的示例性实施例中，移动设备上的软件或电路具有典型智能卡几乎全部的功能，虽然不具备任何可以直接用于唯一地标识金融或支付账号的数据。在一实施例中，一旦移动设备被激活，用户就会被提示使用小键盘、键盘、或一些其它用于将用户输入接收到移动处理设备中的技术来输入标识 PIN。应当理解的是移动处理设备可以是膝上型计算机或其它个人计算机，也可以是与用于正讨论的假设交易的计算机相同的个人计算机。然而典型的是，执行交易的个人计算机与移动设备是独立的设备。接着在步骤 103，移动设备通过将 PIN 与存储在该设备上的数据相比较来证实该 PIN 是否有效。值得注意地，步骤 101 和 103 不是必需的，但可用于有效地增强授权系统的安全性并阻止欺诈。另外，如此处更为详细讨论的那样，当使用 PIN 时，PIN 输入过程可以被延迟直到用户将与交易有关的其它数据输入到移动设备以后。

在一个示例性实施例中，授权处理器还可为用户提供口令号，或其它用户将输入到他或她的移动处理设备中去的不可预测的数据，该数据随后被用于（典型地与诸如加密密钥之类的其它数据一起）生成动态认证码。该不可预测数据可以是随机数、可以基于当前时间、预测交易额的单项散列、上述的某些组合、或者不能在交易前被轻易预测的任何其它数据。用户还可以被提示将与交易有关的其它数据输入到移动设备中，诸如交易额和货币种类，设备可以使用这一数据以及其它保密数据来生成将成为在此较详细讨论的动态授权码的密文。

在步骤 110，移动处理设备使用（诸如加密密钥之类的）密钥 120 来生成动态认证码 130。密钥 120 可以是 DES 密钥、私钥、公钥、上述的某些组合、或者用于加密或生成用于后续认证的保密消息的任何其它数据。密钥可保存在例如移动处理设备的应用存储器中。如果移动处理设备包括安全或受保护存储器（例如在插入到手机或 PDA 中的订户身份模块（SIM）卡中），则密钥也可以有效地存储在那里。密钥 120 还可被加密或存放在不可被其它处理器、运行在移动设备上的程序或应用程序访问的存储器单元中。例如，密钥可以用（诸如用户 PIN、移动设备序列号、其它数据或

上述组合的)另一密钥加密。值得注意地,移动设备中的安全存储器不是必需的。

移动设备的存储器应不包含任何将标识密钥 120 所对应的账户的信息。特别地,密钥 120 (以及移动设备存储器)不应包含支付账号(PAN)、卡有效期限、典型地存储在交易卡磁条上的卡片轨道数据、账户持有者姓名、或可以唯一标识金融账户的任何其它数据。这样,如果移动设备被窃或被危害,设备不会被用于执行交易,因为不会有任何数据能够标识密钥 120 所对应的金融账户。

在示例性的实施例,密钥 120 与应用简档标识符、应用交易计数器、以及其它数据一起被存放在芯片认证程序(CAP)数据文件 125 中。在 MasterCard 的芯片认证程序规范中可找到更多关于芯片认证程序格式和功能的细节,该规范可以从纽约州 Purchase 的 MasterCard 国际股份有限公司购买许可,其被全文引用并合并于此。在示例性实施例, CAP 数据文件 125 可被加密,并随后通过用户输入的 PIN、从进行解密设备收集的(诸如电话号码或设备序列号之类的)移动设备标识符、或两者组合来解密。这样, CAP 数据文件的使用可被限制为知晓 PIN、被批准的设备、或两者组合的个人。在示例性实施例,(被任选地包含在数据文件 125 中的)交易计数器是顺序计数器,其在每一次生成动态授权码后递增。

生成认证码的步骤 110 可进一步理解为包括在步骤 112 中应用密文 115 的生成。应用密文使用智能卡设计或工作领域中公知的技术(例如以下形式:当提供 GENERATE AC 命令时,兼容 EMV 的智能卡工作)从密钥 120、以及诸如交易计数器之类的其它数据生成。在前述的授权处理器为用户提供不可预测数据的示例性实施例,除密钥 120 和交易计数器以外还基于该不可预测数据来生成应用密文。有关交易的其它数据也可被用于计算应用密文,诸如交易额、交易日期/时间、货币种类等。例如,在一个实施例中,不可预测数据、交易计数器、以及任何其它有关数据可以连接在一起并通过密钥 120 来加密以生成应用密文。认证处理器和/或发行银行可选择哪些数据该用于计算由该发行银行维护的交易账户的应用密文。因此,在

本示例性实施例中，移动设备本质上成为与智能卡的 CAP 规范所描述的类似功能的“软件智能卡”。

在示例性实施例中，应用密文 115 是可由以下数据项目组成的中间数据格式，数据项目以二进制表示并从最高位到最低为连接如下：密文信息数据（8 位）、交易计数器（16 位）、移动处理计算的密文（64 位）、以及发行方应用数据（0-256 位）。发行方应用数据是由维护持卡者账户的金融机构选择的数据并可以是任何数据；然而，对于本发明的目的，较佳的是发行方应用数据不包括能够被用于标识持卡者或与持卡者相关联的金融账户的信息。

由于该中间步骤的输出可能导致数据值最多达到 43 字节的长度（即值的范围从 0 到 2^{344} 或约 3.6×10^{103} ），这作为十进制数而言太大以致于无法提供给用户，该数据在显示给用户之前必须被压缩或限制。事实上，考虑到用户可能需要重新向他们进行交易的计算机上的网络浏览器输入动态码，即使是（形成中间数据的一部分的）64 位的密文在十进制格式中也太长以致无法显示给用户。因此，在步骤 117，中间数据被缩减到更容易管理的数据大小并被呈现给用户。在示例性实施例中，中间密文数据被缩减到 8 个数字字符，使得可能的值在 0 至 99,999,999 范围内。在示例性实施例中，该缩减是通过使用位映射（bitmap）来实现的，该位映射标识在中间数据格式中的哪些位应该被保留并用于计算动态认证码。例如，位映射可标识位 1—15、17—19、以及 21—27 作为从中间计算中保留的位。接着，保留的位被连接在一起并显示为二进制编码的十进制格式（BCD）。用这种方法，为了确保显示给用户的可能值不超过 8 个数字，可以被保留的位的最大数量是 26。保留的准确的位数可根据具体应用和情况而定；然而，授权处理器还必须知道用于选择待保留位的算法，使授权处理器可校验移动处理设备生成的动态认证码。

在示例性实施例中，在生成的最终动态认证码中不包括授权处理器知道的位和数据、或授权服务器可以从它所知道的或在动态认证码中提供的其它数据中得到的数据。例如，如果使用了交易计数器并且认证处理器在

授权数据库中保存有与移动设备相关联的交易计数器的副本，完整的交易计数器不需要被包含在用于生成动态码的数据中。例如，可能仅需要包括该计数器的一些最低位。那样，即使授权数据库中存储的交易计数器的副本与移动设备中的计数器不同步，授权处理器也可以重建交易计数器，并使用从移动设备接收到的动态授权码中有关计数器的部分数据来准确计算它自身版本的密文。

只要保存合理数量的位，中间数据的其它位（包括经计算的密文）也可被排除，以最小化错误认证的可能性，牢记的是授权处理器会使用与移动设备共享的保密信息（即示例性实施例中的密钥）来计算它本身版本的密文、以及交易特定数据，诸如不可预测数字、交易计数器等，并且如果处理器确定（经从移动设备接收的动态授权码证实的）由移动设备计算的密文与（借助前述位映射来隐蔽之后的）由授权处理器计算的密文相匹配，则授权交易。

密文计算的方式可以与在此描述的不同并且有无数种。在一实施例中，密文要求基于由账户持有者的发行银行所选择的数据来进行计算，并将计算的结果用存储在卡上的（诸如加密密钥之类的）保密信息加密。然而，密文生成步骤 110 应产生动态的（而非静态的）、即使对于相同类型和金额的重复交易也不可预测地变化的认证码 130。这会降低偷听者截取动态授权码、并在并不真正由与用于进行交易的金融账户相关联的持卡者所授权的之后的尝试交易中再现该动态授权码的可能性。另外，计算应证实与正用于交易的金融账户相关联的持卡者已授权了该交易。在较佳实施例中，这通过在生成动态认证码之前要求输入 PIN 到设备来实现。

虽然认证码是动态的并且基于（诸如具体交易特点和其它随机和变化数据之类的）各种因素频繁变化，但生成步骤 110 可要求具体认证码的产生在时间上大于一次，而不背离本发明要求的范围。生成步骤 110 可在（诸如 PDA、移动电话或手机、膝上型计算机、或其它设备的）移动处理设备上执行。设备应具有能够执行生成认证码 130 所必需步骤的能力的处理器。移动处理设备还可是智能卡，而生成步骤 110 可由智能卡执行。

如图 2 中所示, 在示例性实施例中, 移动设备包括包含用于生成动态认证码的数据 (包括由设备的用户输入的数据) 的数据储存区域 1030, 诸如 RAM、闪存、硬盘驱动器、或其它存储器。设备还包括认证码生成器 1020, 其可以是被编程为生成基于在此所述的且为本领域技术人员所熟知的任何技术的认证码的处理器。生成器 1020 生成之前所述的动态认证码 130, 并将该码提供给输出设备 1010。该认证码输出设备 1010 可将生成的动态认证码 130 呈现给用户, 诸如通过 LCD 屏幕或其它显示器、通过同步语音技术或声响、或一些其它手段。可选地 (或附加地), 设备 1010 可将认证码 130 通过电线、红外线、或射频信号发送到另一设备 (诸如进行交易的个人计算机或终端) 用于随后发送至授权端。在另一示例性实施例中, 移动设备可通过 (诸如无线通信网络、互联网、或上述组合之类的) 通信网络将动态认证码直接发送至授权端的授权处理器。

另外, 为了有助于标识为之生成认证码 130 的账户 (例如, 设备能够为与设备的用户或多个用户相关联的多个不同账户生成码的情况), 认证码输出设备 1010 可向用户显示或发送增强名称 (promotional name)、图案标记、或标识记号, 以助于用户与设备交互, 以选择合适的要为之生成动态码的账户。

现在回到图 1, (诸如加密密钥之类的) 账户保密数据存储在授权处理器 (未示出) 可以访问的授权数据库中。保密数据对应于具体的与移动处理设备的用户相关联的金融账户 (例如, 信用或借记账户)。授权数据库较佳地仅可由授权处理器和/或维护该用户账户的银行或金融机构 (典型地, 本领域技术人员称为“发行”银行) 访问。如果移动设备被窃或被危害, 持有设备的人不能进行交易, 因为没有某些其它的 (诸如标识了应为货物或服务应向其记账的具体金融账户的主要账号 (PAN)) 的金融账户标识符, 由设备生成的授权码 130 不能被用于认证交易。

因此, 在交易时, 金融账户标识符 140 应用本领域技术人员熟知的各种技术来收集。例如, 账户标识符 140 可存储在磁条式卡 145 或智能卡上, 或通过小键盘、键盘、或其它输入设备由用户输入到设备中来收集。

在步骤 150, 动态授权码 130 (与金融账户标识符数据 140 一起) 被发送到 (诸如授权处理器之类的) 授权端。基于来自授权端的响应 (步骤 160), 交易在步骤 170 被授权或在步骤 180 被拒绝。

如上所述, 授权过程可能需要使用与移动设备所执行的相同的数据和算法在授权端计算动态认证码, 并将计算的结果与接收到的动态码作比较以确定计算的结果与接收到的码相匹配。该过程使用 (诸如加密密钥之类的) 与提供交易的金融账户标识符相关联的保密数据。在实施例中, 分析授权端接收到的动态码以判断该码是否包含移动设备用来计算授权处理器不知道的应用密文的任何数据。例如, 有可能移动设备用交易计数器来计算应用密文, 其中则必须将该计数器同样提供给授权处理器, 使它可以使使用相同的数据来计算它的版本的应用密文。如前所述, 虽然与具体账户或移动设备相关联的交易计数器的副本可以存储在授权数据库中, 或者在授权端, 但由于之前的没有被发送至授权处理器或授权数据库的失败交易, 存储的计数器的副本可能与移动设备上的计数器不同步。因此, 一旦授权处理器从动态认证码中所提供的数据中提取出或重生成任何必需的数据, 授权处理器能使用之前所述的技术来计算动态授权码, 所述技术包括用相关交易数据和 (诸如与账户相关联的加密密钥之类的) 保密账户信息来执行计算。接着如前所述的, 将经计算的码与从移动设备接收到的动态码相比较。

一种将必要的程序和数据部署到移动处理设备中的示例性技术需要部署服务器。在本实施例中, 移动设备的用户访问由用户的发行银行指定的网站, 用户要求将动态认证码生成器应用安装在用户的移动设备上。用户被提示要求与应用和用户的移动设备标识符相关联的 PIN。用户还可被提示要求他或她的金融账户标识符, 或者这一数据可通过某些其它方法来确定。(诸如加密密钥或密钥对之类的) 账户保密数据被生成并与用户的金融账户标识符相关联。接着至少一部分该保密数据 (例如加密密钥或密钥对中的一个或多个密钥) 被存储在与用户的金融账户标识符相关联的授权数据库记录中。

接着基于与之前生成的保密数据相关联的数据来生成个人化数据。例如,加密密钥或密钥对中的一个或多个密钥通过使用之前由用户输入的 PIN 和移动设备标识符来加密(如通过三重 DES 技术)作为临时密钥以生成个人化数据。接着,将个人化数据和任何其它的可执行程序文件从部署服务器发送到移动设备。该通信可通过用户的移动设备和(诸如 PC 之类的)另一计算机之间的直接连接来进行,或者通过使用移动或无线数据网络的空中(OTA)服务器来进行。接着,应用和个人化数据可被放置在移动设备的存储器中,如前所述的那样,在移动设备中它们可被用于生成动态认证码。账户保密数据和任何加密或个人化数据可在或者预定量的时间后或者应用和个人化数据被成功安装之后删去。然而,至少一部分保密数据仍然存储在授权数据库中以在之后的授权请求中使用。

在一实施例中,应用可以能由移动处理设备上的安装的 Java 虚拟机执行的 Java 程序的形式来提供。在一实施例中,为了进一步的安全性,Java 程序命令可被搞混,例如通过使用俄亥俄州 Cleveland 的 Preemptive Solutions 公司的 DashO。

图 3 显示了使用 Java 语言 2090 和 Java 虚拟机(JVM) 2080 的本发明的示例性实施例的方框图。首先,移动设备用户使用(诸如小键盘或键盘之类的)接口 2060 来请求调用动态认证应用。接着 JVM 2080 调用 M-CAP.jar 沙箱(Sandbox) 2020。JVM 2080 提示用户输入 PIN,该 PIN 接着从接口 2060 被接收。然后,Java 应用的 CAP 生成器 2030 部分使用 CAP 数据 2040 根据之前描述的技术来生成 8 位的动态认证码。该 8 位码通过 JVM 2080 返回到电话用户接口 2060。驻于电话存储器 2010 中的 CAP 数据 2040 或 M-CAP JarSandbox 2020 可通过例如来自 <http://www.bouncycastle.org/> 的用于 J2ME 的 Bouncy Castle Crypto API 来加密。

虽然本发明是结合某些较佳实施例来描述的,但本领域技术人员可以理解不背离本发明的精神或范围的各种修改、选择、和替换。本发明的许多其它应用对本领域普通技术人员是显而易见的。

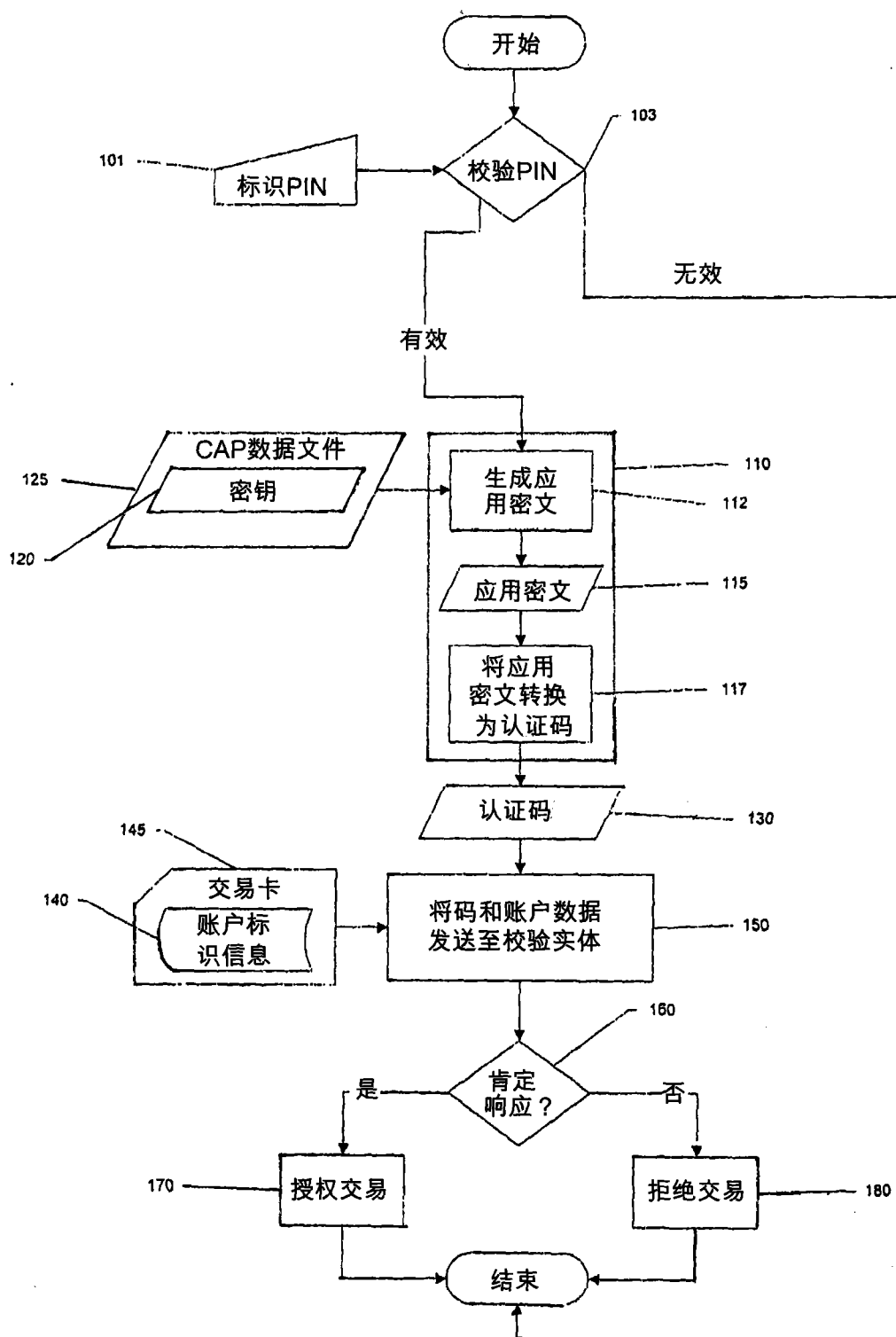


图 1

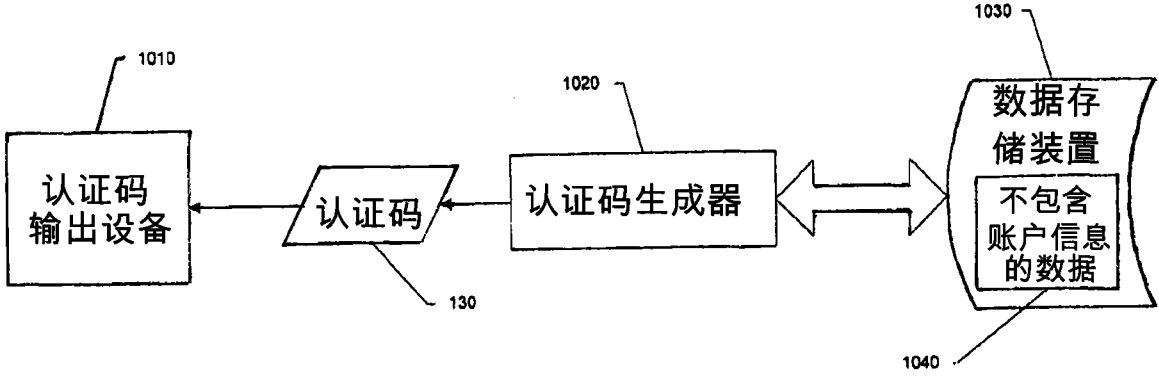


图 2

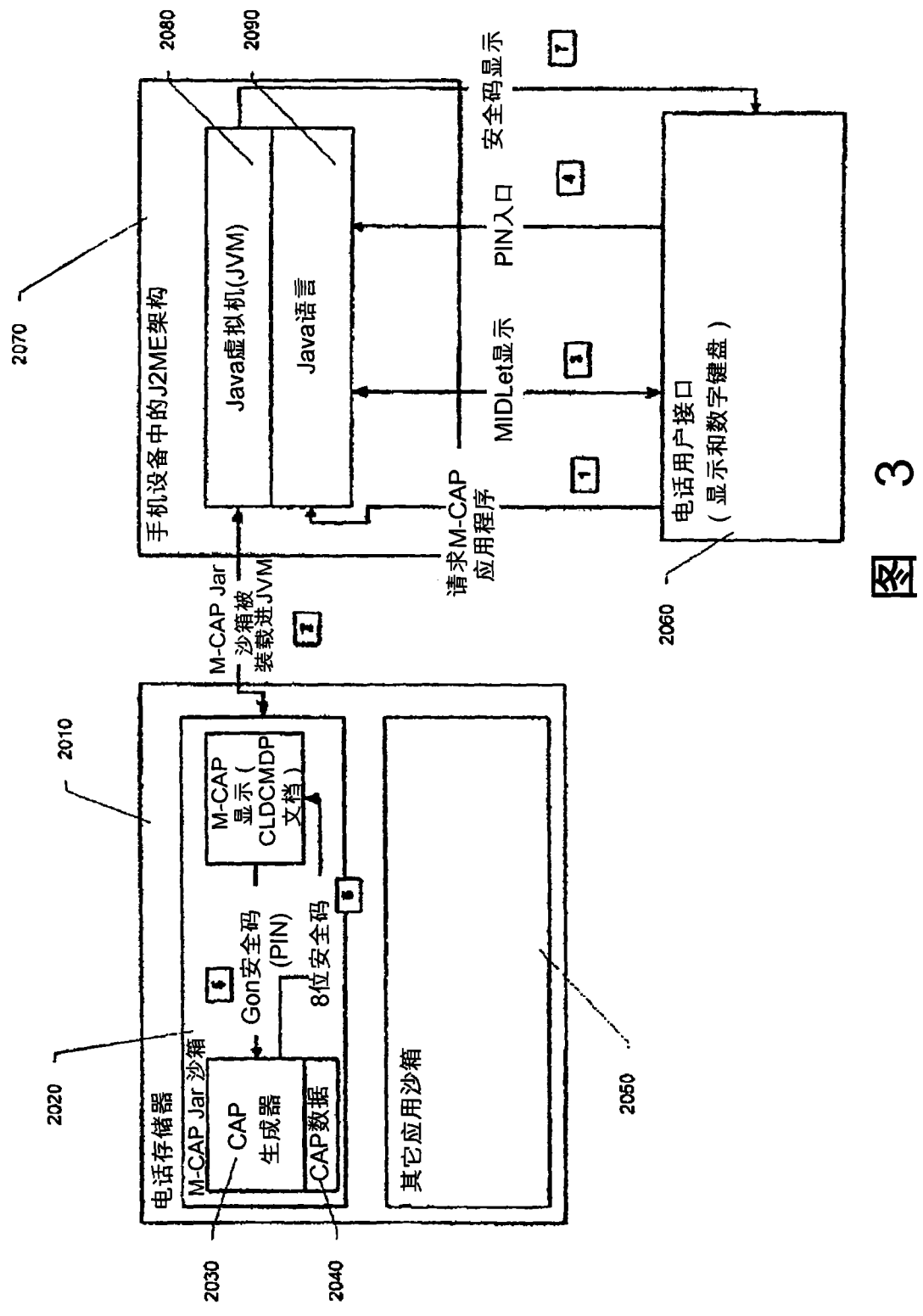


图 3