(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113196813 B
(45)授权公告日 2024.05.24

(21)申请号 201880100182.6
(22)申请日 2018.12.12
(65)同一申请的已公布的文献号
申请公布号 CN 113196813 A
(43)申请公布日 2021.07.30
(85)PCT国际申请进入国家阶段日
2021.06.11
(86)PCT国际申请的申请数据
PCT/US2018/065239 2018.12.12
(87)PCT国际申请的公布数据
WO2020/122898 EN 2020.06.18
(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 T·贝林杰
(74)专利代理机构 上海专利商标事务所有限公司 31100
专利代理师 钱慰民 张鑫
(51)Int.Cl.
H04W 12/00(2021.01)
H04W 12/0471(2021.01)
(56)对比文件
CN 104662864 A,2015.05.27
WO 2016168339 A1,2016.10.20
WO 2018013431 A2,2018.01.18
审查员 杨丽鲜

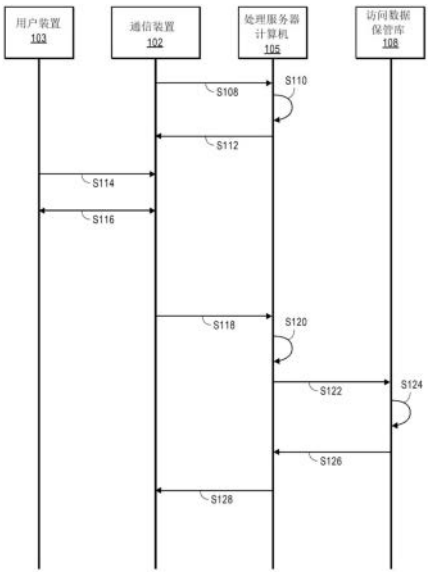
权利要求书2页 说明书15页 附图9页

(54)发明名称

从非接触式装置发起的预配

(57)摘要

公开一种方法。所述方法包括:生成预配访问数据的初始化请求消息;将所述初始化请求发送到服务器计算机;以及由所述通信装置从所述服务器计算机接收动态数据元素。所述方法还包括与用户装置执行消息交换过程,其中在所述消息交换过程期间由所述通信装置从所述用户装置接收密码。所述方法还包括将包括用户装置标识符和所述密码的预配请求消息发送到所述服务器计算机。所述方法还包括由所述通信装置接收所述访问数据。



CN 113196813 B

1.一种用于通信的方法,包括:

由通信装置生成对预配访问数据的初始化请求消息;

由所述通信装置向服务器计算机发送所述初始化请求消息;

由所述通信装置从所述服务器计算机接收动态数据元素;

由所述通信装置与用户装置执行消息交换过程,所述动态数据元素从所述通信装置被发送至所述用户装置,并且其中在所述消息交换过程期间由所述通信装置从所述用户装置接收密码,其中所述密码是通过所述用户装置使用所述用户装置上的密钥至少对所述动态数据元素和用户装置标识符进行加密来生成的;

由所述通信装置向所述服务器计算机发送包括所述用户装置标识符和所述密码的预配请求消息;以及

由所述通信装置从所述服务器计算机接收所述访问数据,

其中向所述通信装置预配的所述访问数据用于通过使所述通信装置与访问装置连接来进行交易。

2.根据权利要求1所述的方法,其中所述通信装置是移动电话并且所述用户装置是卡。

3.根据权利要求1所述的方法,其中所述服务器计算机与访问数据保管库通信,并且其中所述服务器计算机从所述访问数据保管库检取所述访问数据。

4.根据权利要求1所述的方法,其中所述消息交换过程利用获取处理选项和应用程序标识符请求和响应消息。

5.根据权利要求1所述的方法,其中所述通信装置和所述用户装置在彼此间进行短程无线通信时执行所述消息交换过程。

6.根据权利要求1所述的方法,其中所述密钥是从存在于所述用户装置上的数据导出的。

7.根据权利要求1所述的方法,其中数值零在所述消息交换过程中从所述通信装置发送给所述用户装置。

8.一种通信装置,包括:

处理器;以及

耦合到所述处理器的计算机可读介质,所述计算机可读介质包括能由所述处理器执行以用于实施方法的代码,所述方法包括:

生成对预配访问数据的初始化请求消息;

向服务器计算机发送所述初始化请求消息;

从所述服务器计算机接收动态数据元素;

与用户装置执行消息交换过程,其中所述动态数据元素从所述通信装置被发送至所述用户装置,并且在所述消息交换过程期间由所述通信装置从所述用户装置接收密码,其中所述密码是通过所述用户装置使用所述用户装置上的密钥至少对所述动态数据元素和用户装置标识符进行加密来生成的;

向所述服务器计算机发送包括所述用户装置标识符和所述密码的预配请求消息;以及

由所述通信装置从所述服务器计算机接收所述访问数据,

其中向所述通信装置预配的所述访问数据用于通过使所述通信装置与访问装置连接来进行交易。

9.根据权利要求8所述的通信装置,其中所述服务器计算机与访问数据保管库通信,并且其中所述服务器计算机从所述访问数据保管库检取所述访问数据。

10.根据权利要求8所述的通信装置,其中所述消息交换过程利用获取处理选项和应用程序标识符请求和响应消息。

11.根据权利要求8所述的通信装置,其中所述通信装置和所述用户装置在彼此间进行短程无线通信时执行所述消息交换过程。

12.根据权利要求8所述的通信装置,其中所述通信装置是移动电话。

13.根据权利要求8所述的通信装置,其中所述密钥是从所述用户装置上的数据导出的。

14.一种用于通信的方法,包括:

由服务器计算机从通信装置接收对预配访问数据的初始化请求消息;

由所述服务器计算机向所述通信装置提供动态数据元素,所述通信装置随后与用户装置执行消息交换过程,所述动态数据元素从所述通信装置被发送至所述用户装置,并且其中在所述消息交换过程期间由所述通信装置从所述用户装置接收密码,其中所述密码是通过使用所述用户装置上的密钥至少对所述动态数据元素和用户装置标识符进行加密来生成的;

由所述服务器计算机接收包括所述用户装置标识符和所述密码的预配请求消息;以及

由所述服务器计算机提供所述访问数据,

其中向所述通信装置预配的所述访问数据用于通过使所述通信装置与访问装置连接来进行交易。

15.根据权利要求14所述的方法,其中所述通信装置是移动电话并且所述用户装置是卡。

16.根据权利要求14所述的方法,其中所述密码是使用DES或三重DES加密过程而形成的。

17.一种服务器计算机,包括:

处理器;以及

计算机可读介质,所述计算机可读介质包括能由所述处理器执行以执行根据权利要求14至16中任一项所述的方法的代码。

从非接触式装置发起的预配

[0001] 相关申请交叉引用

[0002] 无。

背景技术

[0003] 已知用于将访问数据预配给例如移动电话等通信装置的系统和方法。例如,可将例如安全数据等访问数据预配给通信装置,使得通信装置的用户可使用所述访问数据来访问资源,例如数据、受限区域或商品和服务。

[0004] 然而,现有预配系统和方法存在许多问题。例如,用户可以手动输入要预配到通信装置中的访问数据的标识符(例如,访问代码、账号等),并且通信装置可以从远程服务器计算机请求访问数据。然而,将数据手动输入到通信装置中很繁琐,并且容易发生数据输入错误。另外,手动输入数据可能不太安全。例如,如果将访问数据预配给通信装置所需的标识符被盗取或被未经授权的人从合法用户中被拦截,则未经授权的人可能会向自己的通信装置预配访问数据。

[0005] 本公开的实施例单独地以及共同地解决这些问题和其它问题。

发明内容

[0006] 一个实施例包括一种方法,包括:由通信装置生成预配访问数据的初始化请求消息;由所述通信装置向服务器计算机发送所述初始化请求;由所述通信装置从所述服务器计算机接收动态数据元素;由所述通信装置与用户装置执行消息交换过程,其中在所述消息交换过程期间由所述通信装置从所述用户装置接收密码;由所述通信装置向所述服务器计算机发送包括用户装置标识符和所述密码的预配请求消息;以及由所述通信装置接收所述访问数据。

[0007] 另一实施例包括一种通信装置,包括:处理器;以及耦合到所述处理器的计算机可读介质。所述计算机可读介质包括可由所述处理器执行以用于实施方法的代码。所述方法包括:生成预配访问数据的初始化请求消息;向服务器计算机发送所述初始化请求;从所述服务器计算机接收动态数据元素;与用户装置执行消息交换过程,其中在所述消息交换过程期间由所述通信装置从所述用户装置接收密码;向所述服务器计算机发送包括用户装置标识符和所述密码的预配请求消息;以及接收所述访问数据。

[0008] 另一实施例包括一种方法,包括:由服务器计算机从通信装置接收预配访问数据的初始化请求消息;由所述服务器计算机向所述通信装置提供动态数据元素;所述通信装置随后与用户装置执行消息交换过程,其中在所述消息交换过程期间由所述通信装置从所述用户装置接收密码;由所述服务器计算机将包括用户装置标识符和所述密码的预配请求消息接收到所述服务器计算机;以及由所述服务器计算机提供所述访问数据。

[0009] 关于本公开的实施例的另外细节在具体实施方式和附图中得以描述。

附图说明

[0010] 图1示出根据实施例的系统的框图。

[0011] 图2示出根据实施例的通信装置的框图。

[0012] 图3示出根据实施例的用户装置的图式。

[0013] 图4示出根据实施例的处理服务器计算机的框图。

[0014] 图5示出描绘根据实施例的预配方法的流程图。

[0015] 图6示出描绘通信装置与用户装置之间的消息交换过程的流程图。

[0016] 图7示出根据实施例的用于生成密码的加密过程的框图。

[0017] 图8示出图解说明支付处理系统的框图。

[0018] 图9示出图解说明建筑物访问系统的框图。

具体实施方式

[0019] 实施例可以包括可以将访问数据预配给通信装置的方法和系统。然而,访问数据的预配可以取决于用户拥有合法用户装置。例如,用户装置可以是建筑物访问卡或支付卡。用户可能希望能够使用例如移动电话等通信装置,使得所述通信装置可以像用户装置一样工作。为此,用户需要拥有合法用户装置。用户将使用户装置与通信装置连接。在所述连接期间,将发生消息交换过程,使得移动装置模拟要进行的活动的标准读取器。例如,活动可以是支付交易,并且通信装置可以模拟销售点终端。在另一示例中,活动可以访问例如建筑物等受限位置。通信装置可以被编程以模拟标记读取器。通过允许通信装置模拟预期活动的读取器类型,可以用类似于预期活动将发生的方式来认证用户装置。因此,可以确保被请求预配访问数据的任何服务器计算机将访问数据预配给合法且已授权的通信装置。

[0020] 实施例改进了常规系统。通过要求用户在允许服务器计算机向通信装置预配访问数据之前向所述通信装置提供合法用户装置,可以确保服务器计算机将访问数据预配给合法且已授权的通信装置。另外,在实施例中,由于用户无需将任何数据手动输入到通信装置中,所以与常规系统相比,出现的数据输入错误更少。最后,由于实施例可以使用模拟用户装置的实际活动的消息交换过程,所以可以使用现有的但以不同方式使用的协议来认证用户装置。因此,相比于可能另外需要针对预配功能进行专用编程的系统,实施例可以更容易实施。

[0021] 在论述本公开的一些实施例的细节之前,对一些术语的描述可有助于理解各种实施例。

[0022] “通信装置”(有时被称作移动通信装置或移动装置)可以包括用户可以传输和操作的任何合适的电子装置,所述装置还可以提供与网络远程通信的能力。移动通信装置可以使用移动电话(无线)网络、无线数据网络(例如,3G、4G或类似网络)、Wi-Fi、蓝牙、低功耗蓝牙(BLE)、Wi-Max或可以提供对例如因特网或专用网络等网络的访问的任何其它通信介质来进行通信。移动通信装置的示例包括移动电话(例如,蜂窝式电话)、PDA、平板计算机、上网本、膝上型计算机、可穿戴装置(例如手表)、车辆(例如,汽车和摩托车)、个人音乐播放器、手持式专用读取器等。移动装置可以包括用于执行此类功能的任何合适的硬件和软件,并且还可以包括多个装置或组件(例如,当装置通过与另一装置进行网络共享(即,使用所述另一装置作为调制解调器)而远程访问网络时,一起使用的两个装置可以被认为是单个

移动装置)。

[0023] “非接触式”通信可以是在两个装置之间交换数据而无需这两个装置物理耦合的通信。在不限制前述内容的一般性的情况下,“非接触式”通信可以包括通过近场通信(NFC)收发器、激光、射频、红外通信或其它射频或无线通信协议,例如蓝牙、蓝牙低功耗(BLE)、Wi-Fi、iBeacon等进行的数据发送。

[0024] “用户装置”可以是可以由用户使用的任何合适的装置。“用户装置”可以呈任何合适的形式。用户装置的一些示例包括具有磁条或非接触式元件(例如,包括非接触式芯片和天线)的卡(例如,借记卡、信用卡和预付卡)、挂扣(fob)、可穿戴装置、移动电话、平板计算机等。在一些实施例中,用户装置的功能少于用户所使用的通信装置。例如,在一些实施例中,通信装置可以是具有长程天线的移动电话。用户装置可以是不具有长程天线但具有带有短程天线的非接触式元件的支付卡。

[0025] “资源提供商”可以是在交易期间提供资源(例如,商品、服务、对安全数据的访问、对位置的访问等等)的实体。例如,资源提供实体可以是商家、场所运营商、建筑物所有者、政府实体等。“商家”通常可以是参与交易且可以出售商品或服务或提供对商品或服务的取用的实体。

[0026] “应用程序”可以是用于特定目的的计算机程序。应用程序的示例可以包括交通应用程序、安全数据访问应用程序、银行业务应用程序、数字钱包应用程序等。

[0027] “认证数据”可以包括适于认证实体的任何数据。认证数据可以从用户或用户操作的装置获得。从用户获得的认证数据的示例可以包括PIN(个人标识号)、生物特征数据、密码等。可以从装置获得的认证数据的示例可以包括装置序列号、硬件安全元件标识符、装置指纹、电话号码、IMEI号等。

[0028] “访问数据”可以包括任何合适的数据,所述数据可以用于访问资源或创建可以访问资源的数据。在一些实施例中,访问数据可以是支付账户的账户信息。账户信息可以包括PAN、支付令牌、到期日期和验证值(例如,CVV、CVV2、dCVV、dCVV2)等。在其它实施例中,访问数据可以是可用于激活账户数据的数据。例如,在一些情况下,账户信息可以存储在移动装置上,但是可以直到移动装置接收到特定信息才被激活。在其它实施例中,访问数据可以包括可用于访问位置的数据。此类访问数据可以是赛事的票证信息、用于访问建筑物的数据、交通票证信息等。在其它实施例中,访问数据可以包括用于获得对敏感数据的访问权的数据。访问数据的示例可以包括服务器计算机准予访问敏感数据所需要的代码或其它数据。

[0029] “访问请求”可以包括访问资源的请求。资源可以是物理资源(例如,商品)、数字资源(例如,电子文档、电子数据等)或服务。在一些情况下,可以通过发送包括访问请求数据的访问请求消息来提交访问请求。通常,与请求方相关联的装置可以将访问请求消息发送给与资源提供商相关联的装置。

[0030] “访问请求数据”可以包括关于访问请求或与访问请求相关的任何信息。访问请求数据可以包括访问数据。访问请求数据可以包括可用于处理和/或验证访问请求的信息。例如,访问请求数据可以包括与参与处理访问请求的实体(例如,资源提供商计算机、处理服务器计算机、授权计算机等)相关联的细节,例如实体标识符(例如,名称等)、与实体相关联的位置信息和指示实体类型的信息(例如,类别代码)。示例性访问请求数据可以包括指示访问请求量、访问请求位置、接收到的资源(例如,产品、文档等)、关于接收到的资源的信息

(例如,大小、量、类型等)、资源提供实体数据(例如,资源提供商数据、文档所有者数据等)、用户数据、访问请求的日期和时间、用于进行访问请求的方法(例如,接触式、非接触式等)的信息,以及其它相关信息。

[0031] “访问装置”可以是用于提供对某物的访问的任何合适的装置。访问装置可以采用任何合适形式。访问装置的一些示例包括销售点(POS)装置、蜂窝电话、PDA、个人计算机(PC)、平板PC、手持式专用阅读器、机顶盒、电子收款机(ECR)、自动柜员机(ATM)、虚拟收款机(VCR)、查询一体机、安全系统、访问系统、网站等。访问装置可使用任何合适的接触式或非接触式操作模式,以向用户装置发送或从其接收数据或者与用户装置相关联。在访问装置可以包括POS终端的一些实施例中,可使用任何合适的POS终端并且其可以包括读取器、处理器和计算机可读介质。读取器可包括任何合适的接触式或非接触式操作模式。例如,示例性读卡器可以包括射频(RF)天线、光学扫描器、条形码阅读器或磁条阅读器以与用户装置交互。

[0032] “电子钱包”或“数字钱包”可以包括允许个人进行电子商务交易的电子装置。数字钱包可以存储用户简档信息、凭证、银行账户信息、一个或多个数字钱包标识符等,并且可以用于各种交易中,例如但不限于电子商务交易、社交网络交易、转账/个人支付交易、移动商务交易、邻近支付交易、游戏交易等。数字钱包可以设计为简化购买和支付过程。数字钱包可以允许用户将一个或多个支付卡加载到数字钱包上,以便进行支付而无需输入账号或出示实体卡。

[0033] “凭证”可以是充当价值、所有权、身份或权限的可靠证据的任何合适的信息。凭证可以是一串数字、字母或任何其它合适的字符,以及可用作确认的任何对象或文件。凭证的示例包括价值凭证、标识卡、认证文件、访问卡、口令和其它登录信息等。凭证的其它示例包括主账号(PAN)、个人可标识信息(PII),例如姓名、地址和电话号码等。

[0034] “授权实体”可以是通常使用授权计算机来授权请求的实体。授权实体可以是发行方、政府机构、文件存储库、访问管理员等。“发行方”通常可以包括维持用户账户的商业实体(例如,银行)。发行方还可向用户发行存储在蜂窝电话、智能卡、平板计算机或膝上型计算机等用户装置上的支付凭证。

[0035] “服务提供商”可以是可通常通过服务提供商计算机来提供例如商品、服务、信息和/或访问等资源的实体。服务提供商的示例包括数据提供商、交通机构、商家、数字钱包、支付处理器等。

[0036] “用户”可以包括个别或计算装置。在一些实施例中,用户可以与一个或多个个人账户和/或移动装置相关联。在一些实施例中,用户可以是持卡人、账户持有人或消费者。

[0037] “令牌”可以是凭证的替代值。令牌可以是一串数字、字母或任何其它合适的字符。令牌的示例包括支付令牌、访问令牌、个人标识令牌等。

[0038] “支付令牌”可包括支付账户的标识符,它是账户标识符的替代,例如主账号(PAN)。例如,令牌可以包括可以用作原始账户标识符的替代的一系列字母数字字符。例如,令牌“4900 0000 0000 0001”可以用于代替PAN“4147 0900 0000 1234”。在一些实施例中,令牌可以是“保持格式的”,并可以具有与现有交易处理网络中使用的账户标识符一致的数字格式(例如ISO8583金融交易消息格式)。在一些实施例中,令牌可以代替PAN用来发起、授权、处理或解决支付交易,或者在通常将提供原始凭证的其它系统中表示原始凭证。在一些

实施例中,可生成令牌值,使得可能无法以计算方式从令牌值得到原始PAN或其它账户标识符的恢复。此外,在一些实施例中,令牌格式可被配置成允许接收令牌的实体将其标识为令牌,并识别发行令牌的实体。

[0039] “密钥”可以包括在密码算法中用于将数据变换成另一表示的一条信息。密码算法可以是将原始数据变换成替代表示的加密算法,或将加密信息变换回到原始数据的解密算法。密码算法的示例可包括三重数据加密标准(TDES)、数据加密标准(DES)、高级加密标准(AES)等。“加密密钥”可以包括适合于用密码加密数据的任何数据值或其它信息。“解密密钥”可以包括适于对加密数据进行解密的任何数据值或其它信息。在一些情况下,用于对数据进行加密的相同密钥可以被称为对称加密密钥。

[0040] “会话密钥”可以包括用于对要在两个计算机之间安全传送的数据进行加密或解密的任何密钥。在一些情况下,会话密钥可以从发送实体和接收实体都知道的共享秘密生成。例如,会话密钥可以使用密钥导出函数和共享秘密来导出。会话密钥可以用来保护在请求或响应消息中包括的数据。

[0041] “密码”可以包括一条加密的文字。在一些实施例中,密码可以用于对例如装置或用户等实体进行认证。密码可以包括静态数据、动态数据或使用加密密钥(例如会话密钥或唯一导出密钥)加密的静态数据和动态数据的组合。

[0042] “授权请求消息”可以是发送给支付处理网络和/或支付卡的发行方以请求交易授权的电子消息。根据一些实施例的授权请求消息可符合ISO8583,这是针对交换与用户使用支付装置或支付账户进行的支付相关联的电子交易信息的系统的标准。授权请求消息可以包括可与支付装置或支付账户相关联的发行方账户标识符。授权请求消息还可以包括对应于“标识信息”的额外数据元素,仅作为示例包括:服务代码、CVV(卡验证值)、dCVV(动态卡验证值)、到期日期等。授权请求消息还可以包括“交易信息”,例如与当前交易相关联的任何信息,例如交易金额、商家标识符、商家位置等,以及可用于确定是否标识和/或授权交易的任何其它信息。

[0043] “授权响应消息”可以是由发行金融机构或支付处理网络生成的对授权请求消息的电子消息应答。仅作为示例,授权响应消息可以包括以下状态指示符中的一个或多个:批准-交易被批准;拒绝-交易未被批准;或呼叫中心-响应未决的更多信息,商家必须呼叫免费授权电话号码。授权响应消息还可以包括授权代码,其可以是信用卡发行银行响应于电子消息中的授权请求消息(直接地或通过支付处理网络)返回给商家的访问装置(例如,POS设备)的指示交易被批准的代码。所述代码可充当授权的证据。如上所述,在一些实施例中,支付处理网络可向商家生成或转发授权响应消息。

[0044] “服务器计算机”通常是功能强大的计算机或计算机集群。例如,服务器计算机可以是大型主机、小型计算机群集或像单元一样工作的一组服务器。在一个示例中,服务器计算机可以是耦合到网络服务器的数据库服务器。

[0045] “处理器”可以包括任何合适的一个或多个数据计算装置。处理器可包括一起工作以实现所要功能的一个或多个微处理器。处理器可以包括CPU,所述CPU包括足以执行用于执行用户和/或系统生成的请求的程序组件的至少一个高速数据处理器。CPU可以是微处理器,例如AMD的Athlon、Duron和/或Opteron;IBM和/或摩托罗拉(Motorola)的PowerPC;IBM和索尼(Sony)的Cell处理器;英特尔(Intel)的Celeron、Itanium、Pentium、Xeon和/或

XScale;和/或类似处理器。

[0046] “存储器”可以是可存储电子数据的任何合适的一个或多个装置。合适的存储器可以包括非瞬态计算机可读介质,其存储可由处理器执行以实施所要方法的指令。存储器的示例可包括一个或多个存储器芯片、磁盘驱动器等。此类存储器可使用任何合适的电气、光学和/或磁性操作模式来操作。

[0047] 现在将更详细地描述本公开的一些实施例的细节。

[0048] 图1示出根据本发明的实施例的包括数个组件的系统100。系统100包括用户装置103、通信装置102、通信网络104、处理服务器计算机105和访问数据保管库108,所述用户装置可以与用户101相关联。为了清晰起见,图1中示出特定数目的组件。应理解,本公开的实施例可包括多于一个的每种组件。并且,一些实施例可包括比图1所示的所有组件少或多的组件。

[0049] 用户装置103、通信装置102、处理服务器计算机105和令牌保管库108可全都通过任何合适的通信信道或通信网络104与彼此进行操作性通信。合适的通信网络可以是下列中的任一个和/或组合:直接互连、互联网、局域网(LAN)、城域网(MAN)、作为互联网节点的运行任务(OMNI)、安全定制连接、广域网(WAN)、无线网络(例如,采用协议例如但不限于无线应用协议(WAP)、I-模式等)等。可以使用安全通信协议在计算机、网络与装置之间发送消息,所述安全通信协议例如但不限于:文件传输协议(FTP)、超文本传输协议(HTTP)、安全超文本传输协议(HTTPS)、安全套接层(SSL)、ISO(例如,ISO 8583)等。

[0050] 在一些实施例中,通信装置102可以包括服务提供商应用程序,例如移动钱包应用程序、支付应用程序或访问应用程序,可以向所述服务提供商应用程序预配访问数据以使通信装置102能够进行访问交易。并且,在一些实施例中,用户装置103可以通过非接触式通信与通信装置102进行操作性通信。

[0051] 图2示出根据实施例的通信装置102的框图。在一些实施例中,通信装置102可以是可以用来与外部实体进行通信以及获得对某些资源的访问权的装置。例如,通信装置102可以是手机,其可用于进行支付或获得对位置或安全数据的访问权。参考图2,通信装置102可以包括存在于主体102J内的计算机可读介质102B和存储器102C。主体102J可以呈塑料基底、外壳或其它结构的形式。在一些情况下,存储器102C可以是安全元件,和/或还可以存储例如访问数据的信息,所述访问数据例如令牌、PAN、票证等。存储器102C中的信息可以由通信装置102使用天线102D或非接触式元件接口102I发送给另一装置。

[0052] 通信装置102还可以包括用于处理用户装置102的功能的处理器102A(例如,微处理器)和允许用户查看信息的显示器102G。通信装置102可以进一步包括输入元件102E(例如,触摸屏、键盘、触控板、例如生物特征传感器的传感器等)、扬声器102H和麦克风102F。用户装置102还可以包括用于无线数据传递的天线102D。

[0053] 计算机可读介质102B可以包括可由处理器执行以用于实施根据实施例的方法的代码。例如,计算机可读介质102B可以包括可由处理器102A执行以用于实施方法的代码,所述方法包括:生成预配访问数据的初始化请求消息;向服务器计算机发送初始化请求;从服务器计算机接收动态数据元素;与用户装置执行消息交换过程,其中在消息交换过程期间由通信装置从用户装置接收密码;向服务器计算机发送包括用户装置标识符和密码的预配请求消息;以及接收访问数据。

[0054] 计算机可读介质102B可以包含服务提供商应用程序102B-1、访问装置模拟API 102B-2和预配请求模块102B-3。访问装置模拟API 102B-2可以进一步包含应用程序选择子模块。服务提供商应用程序102B-1可以与处理器102A一起允许用户装置102与服务提供商计算机通信。所述服务提供商计算机可以提供由服务提供商提供的功能。服务提供商应用程序的示例可以包括数字钱包应用程序、支付应用程序、商家应用程序、交通应用程序、用于访问安全数据的应用程序等。

[0055] 通信装置102的操作系统(OS)可以实施一组访问装置模拟API 102B-2,所述API允许服务提供商应用程序102B-1获得对非接触式元件接口102I的访问权以及与用户装置的非接触式元件交换交易数据通信。例如,访问装置模拟API 102B-2可以包括编程函数调用,以允许服务提供商应用程序102B-1接收、处理和响应通信,例如从用户装置的非接触式元件发送的应用程序协议数据单元(APDU)命令。以此方式,通信装置102能够模拟例如标记读取器或POS终端等访问装置的功能。服务提供商应用程序102B-1还可以使预配请求模块102B-3和处理器102A发起、接收、处理和响应与处理服务器计算机105的消息通信,所述消息通信与将访问数据(例如支付令牌)预配给服务提供商应用程序102B-1相关。

[0056] 在一些实施例中,非接触式元件接口102I以具有相关联的无线传递(例如,数据发送)元件的半导体芯片(或其它数据存储元件)的形式实施,所述无线传递元件例如天线。经由蜂窝网络发送的数据或控制指令可以应用于非接触式元件接口102I。非接触式元件接口102I能够使用短程无线通信能力传递和接收数据。因此,通信装置102能够经由蜂窝网络(或任何其它合适的无线网络,例如因特网或其它数据网络)或任何短程通信机构传送和传递数据或控制指令。

[0057] 图3示出根据实施例的用户装置103。用户装置103包括基底103A,例如塑料基底。用于与数据访问或数据传递装置连接的非接触式元件103B可以在用户装置基底103A上或嵌入所述用户装置基底内。非接触式元件103B可以包括芯片,并且能够使用近场通信(NFC)技术或其它短程通信技术来传送和传递数据。用户装置103还可以包括存储器103C,所述存储器可以存储例如账号、到期日期和用户名等用户信息。此类信息也可以印刷或压印在基底103A上。基底103A上还可以具有磁条103D。

[0058] 图4示出根据实施例的处理服务器计算机105的框图。处理服务器计算机105可以包括处理器105A,其可以耦合到系统存储器105B和外部通信接口105C。计算机可读介质105D也可以操作性地耦合到处理器105A。数据库105E还可以与处理器105A进行操作性通信。数据库105E可以包含例如令牌和/或账户数据等访问数据,以及访问数据之间的映射,以及凭证和/或通信装置标识符,例如电话号码、IP地址、装置标识符等。

[0059] 计算机可读介质105D可以包括可由处理器105A执行以执行方法的代码,所述方法包括:由服务器计算机从通信装置接收预配访问数据的初始化请求消息;由服务器计算机向通信装置提供动态数据元素,所述通信装置随后与用户装置执行消息交换过程,其中在消息交换过程期间由通信装置从用户装置接收密码;由服务器计算机将包括用户装置标识符和密码的预配请求消息接收到服务器计算机;以及由服务器计算机提供访问数据。

[0060] 计算机可读介质105D可以包括数个软件模块,包括通信模块105D-1、加密/解密模块105D-2、数据库更新模块105D-3、代码生成模块105D-4、授权模块105D-5、验证模块105D-6和预配模块105D-7。

[0061] 通信模块105D-1可以包括使处理器105A生成消息、转发消息、重新格式化消息和/或以其它方式与其它实体通信的代码。

[0062] 在本发明的实施例中,加密/解密模块105D-2可以包括用于对数据进行加密的任何合适的加密/解密算法。合适的数据加密/解密算法可包括DES、三重DES、AES等。所述加密/解密模块还可以存储加密密钥,这些加密密钥可以与此类加密/解密算法一起使用。加密模块105D-2可以利用对称或不对称加密技术来加密和/或验证数据。加密/解密模块105D-2可以使用的密码密钥可以安全地存储在系统存储器105B中。

[0063] 数据库更新模块105D-3可以包括使处理器105A更新数据库105E的代码。数据库105E可以用账户信息、令牌到凭证到装置信息映射、预配信息等进行更新。

[0064] 动态数据元素生成模块105D-4可以包括使处理器105A生成例如随机数、时间和/或日期等动态数据元素的代码。在一些实施例中,一个或多个动态数据元素可以用作密码的输入数据。

[0065] 授权模块105D-5可以包括可以使处理器105A评估预配请求消息并确定是否应向请求方提供访问数据(例如,支付令牌)的代码。授权模块105D-5还可以包括用于在授权请求和响应消息在例如发行方和收单方等各方之间传递时路由或修改所述授权请求和响应消息的代码。

[0066] 验证模块105D-6可以包括用于验证代码或数据的任何合适的代码。在一些实施例中,验证模块105D-6可以验证从通信装置102接收到的已加密数据包。验证模块105D-6还可以包括用于比较数据以确定是否存在匹配的代码。

[0067] 预配模块105D-7可以包括可由处理器105A执行以向通信装置预配访问数据的代码。

[0068] 图5示出图解说明根据实施例的使用从用户装置103(例如,非接触式支付卡)接收到的认证数据将访问数据安全地预配给通信装置102(例如,移动电话)上的服务提供商应用程序102B-1(例如,访问应用程序、数字钱包应用程序等)的方法的流程图。以下描述还可以参考图1-4中的元件。

[0069] 在步骤S108处,通信装置102的用户可能希望将访问数据提供到通信装置102上的应用程序。具体来说,通信装置102可以生成将访问数据预配给通信装置102上的服务提供商应用程序102B-1(例如,数字钱包应用程序)的初始化请求消息。一旦通信装置102的用户准备好向处理服务器计算机105发送预配初始化请求消息,用户就可以在移动通信装置102上选择适当的指示符。例如,用户可以选择“发送”、“+”、“将卡添加到数字钱包”或在通信装置102的显示器上呈现的任何其它合适的选项。然后,服务提供商应用程序102B-1可以执行预配请求模块102B-3以向处理服务器计算机105发送预配初始化请求消息。可以使用任何合适的电子消息格式将初始化请求消息从通信装置102发送给处理服务器计算机105,所述电子消息格式包括电子邮件、短消息服务(SMS)消息、多媒体信息服务(MMS)消息、超文本传输协议(HTTP)请求消息、发送控制协议(TCP)数据包、网页表单提交等。消息可以被引导到与处理服务器计算机105相关联的任何合适的地址,包括电子邮件地址、电话号码、因特网协议(IP)地址或统一资源定位符(URL)。

[0070] 在步骤S110处,在从通信装置102接收到预配访问数据的初始化请求消息之后,处理服务器计算机105可以通过执行动态数据元素生成模块105D-4来生成动态数据元素。动

态数据元素的实例可以包括应用程序交易计数器(ATC)、随机数、当日时间等。动态数据元素是动态的,因为它们可以(例如,随着每次交互或几乎每次交互)频繁变化。并且,在一些实施例中,处理服务器计算机105可以生成与动态数据元素相关联的会话ID。

[0071] 在步骤S112处,处理服务器计算机105可以将动态数据元素和任选的会话ID发送给通信装置102。通信装置102上的服务提供商应用程序102B-1可以接收动态数据元素,然后提示用户向通信装置102呈现用户装置103(例如,显示消息“将卡轻触手机”)。

[0072] 在步骤S114处,用户可以通过将用户装置103放在通信装置102的非接触式元件接口102I附近而向通信装置102呈现用户装置103。用户可以将用户装置103移动成更接近通信装置102,直到可以在两个装置之间交换数据为止。在一些实施例中,用户装置103可以接触通信装置102。

[0073] 在步骤S116处,通信装置102可以与用户装置103执行消息交换过程。在消息交换过程期间,由通信装置102从用户装置103接收密码。消息交换过程可以是通常在用于访问资源的访问交易期间执行的过程,即使向通信装置预配访问数据的当前请求可能未被视为访问例如商品、服务、位置或安全数据等资源的请求。

[0074] 在一些实施例中,消息交换过程使用增强的数据接口协议在通信装置102与用户装置103之间传送信息。例如,本文中所描述的概念的一个例示性实施方案包括消息交换过程,所述消息交换过程包括APDU命令,例如“获取处理选项”和“应用程序标识符”请求和响应消息。在一些实施例中,消息交换过程包括从通信装置102向用户装置103发送例如0美元的数值。并且,在一些实施例中,用户装置103可以向通信装置102提供交易处理信息,包括主账号(PAN)和与主账号相关联的到期日期。下文参考图6描述关于示例性消息交换过程的另外细节。

[0075] 在一些实施例中,在步骤S116中从用户装置103发送给通信装置102的密码是通过使用用户装置103上的至少一个密钥至少对以下各项进行加密来生成的:通信装置102在步骤S112处从处理服务器计算机105接收到的动态数据元素、来自用户装置103的用户装置标识符,以及任选地数值和其它信息。在一些实施例中,用户装置标识符可以是PAN。

[0076] 密码可以用任何合适的方式生成。例如,在一些实施例中,用户装置103上的至少一个密码密钥是从存在于用户装置103上的数据导出的。在一些实施例中,处理服务器计算机105和用户装置103可以共享对称加密密钥,这些密钥将允许所述处理服务器计算机和所述用户装置对密码进行加密和解密。在其它实施例中,处理服务器计算机105和用户装置103可以分别利用公钥对密码的一部分进行加密和利用私钥对密码的一部分进行解密。所利用的加密可以包括任何类型的加密方法。例如,此加密步骤可以利用DES、三重DES、AES等加密。下文参考图7描述关于示例性密码生成过程的另外细节。

[0077] 在步骤S118处,通信装置102可以将预配请求消息发送给处理服务器计算机105。预配请求消息可以包括用户装置标识符和在步骤S116期间从用户装置103接收到的密码。在一些实施例中,通信装置102可以经由服务提供商应用程序102B-1将预配请求消息提供到处理服务器计算机105,所述服务提供商应用程序随后可以利用预配请求模块102B-2来发送消息。在一些实施例中,预配请求消息可以包括已加密部分(例如,在步骤S116中生成的密码)和未加密部分(例如,可用于在数据库中定位加密密钥的PAN或密钥索引)。未加密部分可用于对已加密部分进行解密和恢复已加密部分中的数据。在一些实施例中,未加密

部分可用于生成用于对已加密部分进行解密的一个或多个密钥。在一些实施例中,通信装置102可以发送在步骤S112处由通信装置102接收到的会话ID作为预配请求消息的未加密部分的部分。这可允许处理服务器计算机105使预配请求消息与处理服务器计算机105在步骤S110中生成的动态数据元素相关联。

[0078] 在步骤S120处,在接收到在步骤S118中由通信装置102发送的预配请求消息后,处理服务器计算机105可以执行解密模块105D-2以执行密码的解密并从密码中恢复动态数据元素。然后,处理服务器计算机105确定在步骤S110处生成的动态数据元素的值是否与恢复的动态数据元素的值匹配。如果恢复的动态数据元素与先前生成的动态数据元素不匹配,则处理服务器计算机105可以将预配请求已失败的消息发送给通信装置102。

[0079] 在步骤S122处,如果在步骤S110处由处理服务器计算机105生成的动态数据元素和在步骤S118处从通信装置102接收到的动态数据元素匹配,则处理服务器计算机105可以将至少包含用户装置标识符的访问数据请求消息发送给访问数据保管库108。在一些实施例中,访问数据请求消息可以包含向通信装置102预配访问数据所需的细节。例如,此类细节可以包括与通信装置102相关联的地址(例如,电话号码)、用户装置103的细节(例如,PAN)、任何其它合适的数据。

[0080] 在步骤S124处,访问数据保管库108可以检取所请求的访问数据。

[0081] 在步骤S126处,令牌保管库108可以将访问数据(例如,令牌)发送给处理服务器计算机105。处理服务器计算机105可以接收访问数据,并且在一些实施例中将经由数据库更新模块105D-3将从令牌保管库108接收到的访问数据和相关信息存储在数据库105E中。此类信息可以包括通信装置102的地址(例如,电话号码)、通信装置102用于接受访问数据的任何数据等。

[0082] 在步骤S128处,处理服务器计算机105的预配模块105D-7可以将在步骤S126处接收到的访问数据发送给通信装置102的服务提供商应用程序102B-1。随后,通信装置102可以用于使用服务提供商应用程序102B-1和向所述通信装置预配的访问数据进行访问交易。在一些实施例中,访问数据可以存储在通信装置102中的安全区域(例如,安全元件)中。并且,在一些实施例中,服务提供商应用程序102B-1可以向用户传送确认消息。例如,确认消息可在通信装置显示器102G上显示“卡已连接”。

[0083] 上文所描述的过程可用于将静态或动态访问数据预配给通信装置102。如果访问数据是动态的,则可以将其提供到通信装置102以用于每次交易或预定次数的交易(例如,每5-10次交易)。这降低了可能由中间人攻击造成的欺诈风险。

[0084] 图6示出图5中用户装置103与通信装置102之间的消息交换过程S116的流程图。图6所示的消息交换过程涉及例如非接触式卡的非接触式装置与POS终端之间的支付交互过程。在其它情境下可以使用其它消息交换过程。在一个实施例中,通信装置102的服务提供商应用程序102B-1可以执行访问装置模拟(ADE)应用程序编程接口(API)102B-2。ADE API可以包括编程函数调用,以允许服务提供商应用程序102B-1模拟访问装置以接收、处理和响应预配通信,例如从用户装置103发送的应用程序协议数据单元(APDU)命令。

[0085] 例如,在一个示例性实施例中,用户装置103是非接触式支付卡。如上文在图5中的步骤S114中所解释,用户可以通过将用户装置103放在通信装置102的非接触式元件接口102I附近而向通信装置102呈现所述用户的用户装置103。当通信装置102检测到用户装置

103的存在时,ADE API102B-2的应用程序选择模块可以通过将可用应用程序请求702发送给用户装置103来发起消息交换过程。在一些实施例中,对可用应用程序702的请求可呈“选择近距离支付系统环境(PPSE)”命令的形式。在此类实施例中,对可用应用程序的请求可以包括用于标识通信装置102的ADE API 102B-2所支持的支付环境的支付环境标识符(例如,PPSE名称,例如“2PAY.SYS.DDF01”)。

[0086] 在接收到可用应用程序请求702后,用户装置103可以通过识别请求中包括的支付环境标识符(例如,PPSE名称)来标识和处理所述请求,并通过将可用应用程序响应704发送回通信装置102的ADE API 102B-2来作出响应。可用应用程序响应704可以包括可用账户应用程序标识符(AID)的列表、与可用AID相关联的应用程序配置选项,并且可以包括近距离支付环境标识符(例如,PPSE名称)作为专用文件名。并且,在一些实施例中,例如在用户装置103可以是移动通信装置的情况下,可用应用程序响应704可以包括与移动应用程序相关联的钱包标识符。在一些实施例中,可用应用程序响应704可呈“选择PPSE”响应的形式,并且可以包括PPSE文件控制信息(FCI)。例如,可用应用程序响应704可以包括非接触式用户装置103上的每一可用AID的目录条目。在一些实施例中,可存在与每一可用AID相关联的钱包标识符。每一目录条目可以包括例如以下信息:AID、与AID相关联的应用程序标签(例如,与AID相关联的助记符,例如“Visa借记”)、指示AID的优先级的应用程序优先级指示符、指示应用程序的内核偏好的内核标识符,和/或与特定AID有关的额外信息。可用应用程序响应704还可以包括其它数据,例如FCI发行方任意数据或任何其它相关信息。

[0087] 通信装置102可以基于接收到的可用AID而确定支持的账户应用程序,并且可以将包括所选AID的“应用程序选择”命令706发送给非接触式用户装置103。

[0088] 另外,在一些实施例中,在接收到应用程序选择消息706后,非接触式用户装置103可以发送终端交易数据请求708以从通信装置102请求完成与所选AID相关联的所选应用程序的预配过程可能需要的交易数据。在一些实施例中,终端交易数据请求708可以呈“选择AID响应”的形式,并且可以包括具有所选AID作为专用文件名的应用程序标识符(AID)文件控制信息(FCI)。终端交易数据请求可以包括(经由ADE API 102B-2,其模拟POS终端)从通信装置102请求适当的数据的交易数据标识符的列表,并且交易数据标识符的列表可以呈处理选项数据对象列表(PDOL)的形式。

[0089] 非接触式用户装置103针对交易请求的交易数据可以包括与通信装置102相关联的实体标识符、终端处理选项(TPO)、金额、通信装置标识符和其它信息。另外,交易数据可以包括先前由处理服务器计算机105生成的动态数据元素(例如,随机数)。在其它实施例中,交易信息可以作为应用程序选择消息706的部分和/或作为可用应用程序请求消息702的部分提供。

[0090] 在接收到终端交易数据请求708之后,通信装置102可以将非接触式用户装置103所请求的终端交易数据710发送给非接触式用户装置103。在一些实施例中,终端交易数据710可以用获取处理选项(GPO)命令的形式发送,并且可以包括在处理选项数据对象列表(PDOL)中的所请求的终端交易数据710。在一些实施例中,终端交易数据710(例如,交易处理选项(TPO))可以包括指示通信装置102支持哪些交易数据类型的TPO指示符。如在一些实施例中所指出,为了通过利用APDU命令来促进预配过程,通信装置102可以将零美元值作为终端交易数据710的部分发送给非接触式用户装置103。应理解,在一些实施例中,所述值可

以是任何金额。

[0091] 一旦用户装置103接收到终端交易数据710,用户装置103就从其非接触式元件103B获得相关卡凭证,并且可以将一组交易处理信息712发送给通信装置102。在一些实施例中,交易处理信息712可以用“获取处理选项”(GPO)响应的形式发送。在一些实施例中,交易处理信息可以包括可由通信装置102用作文件地址以读取存储在用户装置103上的账户数据的一个或多个应用程序文件定位符(AFL),以及可用于指示支付应用程序的能力的应用程序交换配置文件(AIP)。

[0092] 交易处理信息712可以包括任何交易凭证,包括使用交易信息生成的密码、磁道2等效数据(例如,PAN、到期日期)和/或额外数据。例如,可以使用交易信息来生成密码,所述交易信息可以至少包括先前描述的动态数据元素(例如,随机数)、用户装置标识符(例如,PAN),并且任选地包括其它信息,例如会话标识符、例如零美元金额等值以及交易计数器。交易处理信息712还可以包括发行方应用程序数据(IAD)、形状因子指示符(FFI)、卡交易限定符(CTQ)、密码信息数据(CID)和/或应用程序PAN序列号(PAN)。在一些实施例中,发行方应用程序数据(IAD)可以包括指示IAD的长度的长度指示符、指示交易密码的版本的密码版本号(CVN)、可用于标识主密钥(例如,与发行方相关联的主密钥)的导出密钥指示符(DKI),和/或卡验证结果(CVR)。下文参考图7描述关于密码生成过程的另外细节。

[0093] 在通信装置102接收到交易处理信息712之后,通信装置102可以将账户数据请求714发送给用户装置103,以读取可以存储在用户装置103上的额外账户数据。在一些实施例中,账户数据请求714可以呈“读取记录”命令的形式,并且可以包括指示通信装置102尝试读取的账户数据的位置的应用程序文件定位符(AFL)。包括在账户数据请求714中的AFL可以对应于从用户装置103提供到通信装置102的交易处理信息712中的AFL。

[0094] 响应于从通信装置102接收到账户数据请求714,非接触式用户装置103可以将存储在由AFL指示的位置处的账户数据716发送给通信装置102。在一些实施例中,账户数据716可以用“读取记录”响应的形式发送。账户数据716可以包括例如指示发行方对应用程序所允许的使用和服务的限制的应用程序使用控制、持卡人的姓名、客户专用数据、发行方国家代码,和/或可在AFL位置处访问并且存储在用户装置103中的其它账户相关数据。

[0095] 图7示出根据一个实施例的其中用户装置103生成密码的过程的流程图。

[0096] 在一些实施例中,密码生成过程800可以开始于用户装置103利用用户装置103上的第一加密密钥802,使用加密函数806对静态数据元素804进行加密以生成第二加密密钥808。第一加密密钥802可以是与用户账户的发行方相关联的基本密钥,并且基本密钥可以与一组账户相关联。例如,第一加密密钥802可以与针对与此类型的用户装置103相关联的支付服务指定的BIN或PAN范围内的一组账户相关联。每一用户装置103可以在其功能范围内进行个性化以从存在于用户装置103上的数据(例如,静态数据元素804)导出为支付服务所独有的密钥。在一些实施例中,第一加密密钥802可以是与关联于静态数据元素804的账户的发行方相关联的主导出密钥(MDK),并且第一加密密钥802还可以在处理器计算机105处进行维护。

[0097] 静态数据元素804可以包括账户标识信息,例如账户标识符(例如,PAN)、替代的账户标识符(例如,替代的PAN)或替代账户标识符的令牌,并且可以另外包括用户标识信息,例如(例如,当多个用户使用同一账户时)标识账户的特定用户的序列号(例如,PAN序列号

(PSN))。例如,用作加密函数806的输入的账户信息804可以是账户标识信息与用户标识信息的串连,或串连的反转版本。

[0098] 在一些实施例中,从账户信息804生成的第二加密密钥808可以包括各自从账户信息804的不同变体生成的多个部分。例如,第二加密密钥808可以分为两个部分。第二加密密钥808的第一部分可以通过使用第一加密密钥802对账户信息804进行加密来生成。第二加密密钥808的第二部分可以通过使账户信息804反转并使用第一加密密钥802对反转的账户信息进行加密来生成。用于生成第二加密密钥808的加密函数806可以是例如三重数据加密标准(TDES)或其它合适的加密算法,并且可以使用二进制零的初始链式矢量(chaining vector)。在一些实施例中,从账户信息804生成的第二加密密钥808可以对应于账户的唯一导出密钥(UDK)。

[0099] 在一个示例性实施例中,密码生成过程800可以通过使用第二加密密钥808对至少两个动态数据元素810、812进行加密而继续。通过使用至少两个(或更多)动态数据元素来创建密码,盗用者(skimmer)可以确定密码的可能性极低。在一些实施例中,动态数据元素的实例可以包括应用程序交易计数器(ATC)、由处理服务器计算机生成的动态数据元素(例如,随机数)、当日时间等。动态数据元素在这样的意义上是动态的:它们例如随着每次交易或几乎每次交易,或以频繁的时间间隔(例如,每天或每几天)频繁变化。在一些实施例中,动态数据元素810对应于动态数据元素S110,所述动态数据元素S110首先在处理服务器计算机105处生成,在图5中的步骤S112处发送给通信装置102,并且在消息交换过程S116期间由通信装置102进一步发送给用户装置103。应当理解,尽管在一些示例性实施例中,对至少两个动态数据元素进行加密以形成密码,但在一些实施例中,可以仅对一个动态数据元素进行加密。

[0100] 在一些实施例中,可以将预定长度的数字串(未示出)创建为待加密814的输入。此数字串可以是通过在支付服务或PAN的账号的对应最左侧数字上叠加第一动态数据元素(例如,ATC)而创建的。此数字串可以在右侧与第二动态数据元素(例如,在图5的S116中从通信装置102接收到的随机生成的数字)串连以产生串连值。如果必要,在串连值的右侧串连填充字符,以形成具有预定固定长度的数字串。此数字串可以通过使用第二加密密钥808来加密814。在一些实施例中,此数字串可以二等分成两个块。并且,在一些实施例中,加密/解密函数814可以进一步涵盖一系列子步骤(未示出)。在这些子步骤中,由二等分数字串所得的两个块可以各自使用分割的第二加密密钥的一个或两个部分进行加密和/或解密,和/或与所得块进行异或(XOR)运算。这一系列子步骤可以产生交易密码816。

[0101] 一旦向通信装置预配了访问数据,所述访问数据就可以用于进行访问交易。图8和9描述了包括在不同情境下使用通信装置上的访问数据的系统和方法。

[0102] 图8示出其中用户101操作已预配有访问数据(例如,令牌)的通信装置102的交易处理系统的框图。用户101可以使用通信装置102在例如商家等资源提供商处支付商品或服务。商家可以操作资源提供商计算机920和/或访问装置910。商家可以经由收单方所操作的传输计算机930和例如支付处理网络等处理网络940与由发行方操作的授权实体计算机950通信。

[0103] 支付处理网络可以包括用以支持和递送授权服务、异常文件服务以及清算和结算服务的数据处理子系统、网络和操作。示例性支付处理网络可以包括VisaNet™。例如

VisaNet™等支付处理网络能够处理信用卡交易、借记卡交易和其它类型的商业交易。VisaNet™确切地说包括处理授权请求的VIP系统(Visa集成式支付系统),和执行清算和结算服务的Base II系统。支付处理网络可以使用任何合适的有线或无线网络,包括因特网。

[0104] 在访问装置910(例如,POS位置)处使用通信装置102(已通过利用用户装置103而向所述通信装置预配访问数据)的典型支付交易流程可以描述如下。用户101将他或她的通信装置102呈现给访问装置910以支付物品或服务。通信装置102和访问装置910进行交互,使得来自通信装置102的访问数据(例如,PAN、支付令牌、验证值、到期日期等)由访问装置910(例如,经由接触式或非接触式接口)接收。然后,资源提供商计算机920可以经由外部通信接口从访问装置910接收此信息。然后,资源提供商计算机920可以生成授权请求消息,所述授权请求消息包括从访问装置910接收到的信息(即,对应于用户装置103的信息)以及额外交易信息(例如,交易金额、商家特定信息等),并将此信息以电子方式发送给传输计算机930。然后,传输计算机930可以接收、处理授权请求消息并将所述授权请求消息转发到处理网络940以进行授权。

[0105] 大体来说,在进行贷记或借记卡交易之前,处理网络940已经关于发行方的交易的授权方式与每一发行方建立协议。在一些情况下,例如当交易金额低于阈值时,处理网络940可以被配置成基于其具有的关于用户账户的信息而授权交易,而无需生成授权请求消息以及将所述授权请求消息发送给授权实体计算机950。在其它情况下,例如当交易金额高于阈值时,处理网络940可以接收授权请求消息,确定与用户装置103相关联的发行方,并将用于交易的授权请求消息转发到授权实体计算机950以进行验证和授权。一旦交易被授权,授权实体计算机950就可以生成授权响应消息(可以包括指示交易被批准或拒绝的授权代码)并且经由所述授权实体计算机的外部通信接口将此电子消息发送给处理网络940。然后,处理网络940可以将授权响应消息转发到传输计算机930,所述传输计算机又可以随后将包括授权指示的电子消息发送给资源提供商计算机920,然后发送给访问装置910。

[0106] 如果访问数据呈令牌的形式,则处理网络940可以将令牌交换为真实凭证(例如,PAN)。然后,任何授权请求消息可被修改为包括真实凭证,并且所述授权请求消息可以被转发到授权实体计算机950以进行验证。授权实体计算机950可以生成具有批准或拒绝的授权响应消息。授权响应消息可以发送给处理网络940,并且处理网络940可以将凭证替换为令牌。然后,处理网络940可以将授权响应消息发送回访问装置910。

[0107] 在一天结束时或以某个其它合适的时间间隔,可以对所述交易执行资源计算机920、传输计算机930、处理网络940和授权实体计算机950之间的清算和结算过程。

[0108] 图9示出建筑物访问系统以及由用户101操作的通信装置102的框图。已利用非接触式用户装置103(例如,非接触式卡)向通信装置102预配如上文所描述的访问数据(例如,令牌)。通信装置102可以与访问装置1010进行交互,并将访问数据传递到访问装置1010。访问装置1010可以本地验证接收到的访问数据,或者其可以与远程定位的认证服务器计算机(未示出)进行通信。远程定位的认证服务器计算机可以验证访问数据是真实的,并且可以将指示这一点的信号发送回访问装置1010。然后,访问装置1010可以继续让用户101进入建筑物1020。

[0109] 本公开的实施例提供优于常规系统的数个技术优势。例如,通过提供通信装置102可以在预配有访问数据时模拟访问装置910(包括接收、处理和响应来自用户装置103的交

易通信)的机制,这由于允许处理网络940验证用户装置的凭证实际上与真实用户装置103(例如,真实发行的支付卡)相关联而提高了安全性。并且,此机制允许处理网络940验证向通信装置102预配访问数据是在将用户装置103呈现给通信装置102的同一会话内执行的,从而减少了中间人攻击。

[0110] 应理解,本公开的任何实施例都可使用硬件(例如专用集成电路或现场可编程门阵列)和/或使用计算机软件以控制逻辑的形式实施,其中通用可编程处理器是模块化的或集成的。如本文所使用,处理器包括单核处理器、在同一集成芯片上的多核处理器,或在单个电路板上或网络化的多个处理单元。基于本文提供的公开内容和教导,本领域普通技术人员将知道并理解使用硬件以及硬件和软件的组合来实施本公开的实施例的其它方式和/或方法。

[0111] 本申请中描述的任何软件组件或功能可实施为使用例如Java、C、C++、C#、Objective-C、Swift等任何合适的计算机语言或例如Perl或Python等脚本语言使用例如常规的或面向对象的技术的由处理器执行的软件代码。软件代码可作为一系列指令或命令存储在计算机可读介质上以供存储和/或传递,合适的介质包括随机存取存储器(RAM)、只读存储器(ROM)、例如硬盘驱动器或软盘的磁性介质,或例如光盘(CD)或数字通用盘(DVD)的光学介质、闪存存储器等。计算机可读介质可以是此类存储或发送装置的任何组合。

[0112] 此类程序还可以使用适应于经由包括互联网的符合多种协议的有线、光学和/或无线网络进行发送的载波信号来编码和传送。因此,根据本公开的实施例的计算机可读介质可以使用以此类程序编码的数据信号来创建。以程序代码编码的计算机可读介质可与兼容装置一起封装或与其它装置分开提供(例如,通过因特网下载)。任何此类计算机可读介质可以驻存在单个计算机产品(例如,硬盘驱动器,CD或整个计算机系统)之上或其内部,并且可以存在于系统或网络内的不同计算机产品上或其内部。计算机系统可以包括用于将本文中所提及的任何结果提供给用户的监视器、打印机或其它合适的显示器。

[0113] 以上描述是说明性的且不是限制性的。在本领域的技术人员阅读了本公开后,本公开的许多变化将变得显而易见。因此,本公开的范围不应参考以上描述来确定,而是应参考待决的权利要求以及其完整范围或等效物来确定。

[0114] 在不脱离本公开的范围的情况下,来自任何实施例的一个或多个特征可以与任何其它实施例的一个或多个特征组合。

[0115] 除非明确指示为相反情况,否则“一”或“所述”的叙述旨在表示“一个或多个”。

[0116] 上文所提及的所有专利、专利申请、公开和描述都出于所有目的以其全文引用的方式并入本文中。并非承认它们是现有技术。

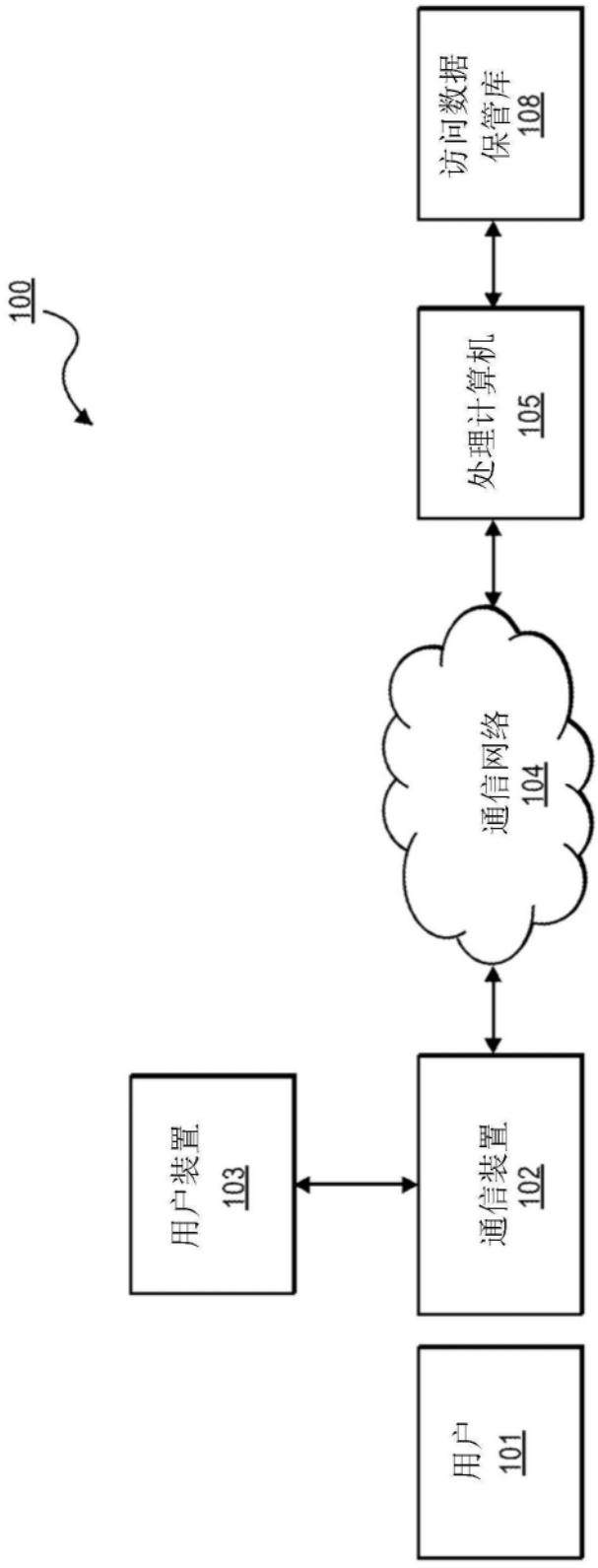


图1

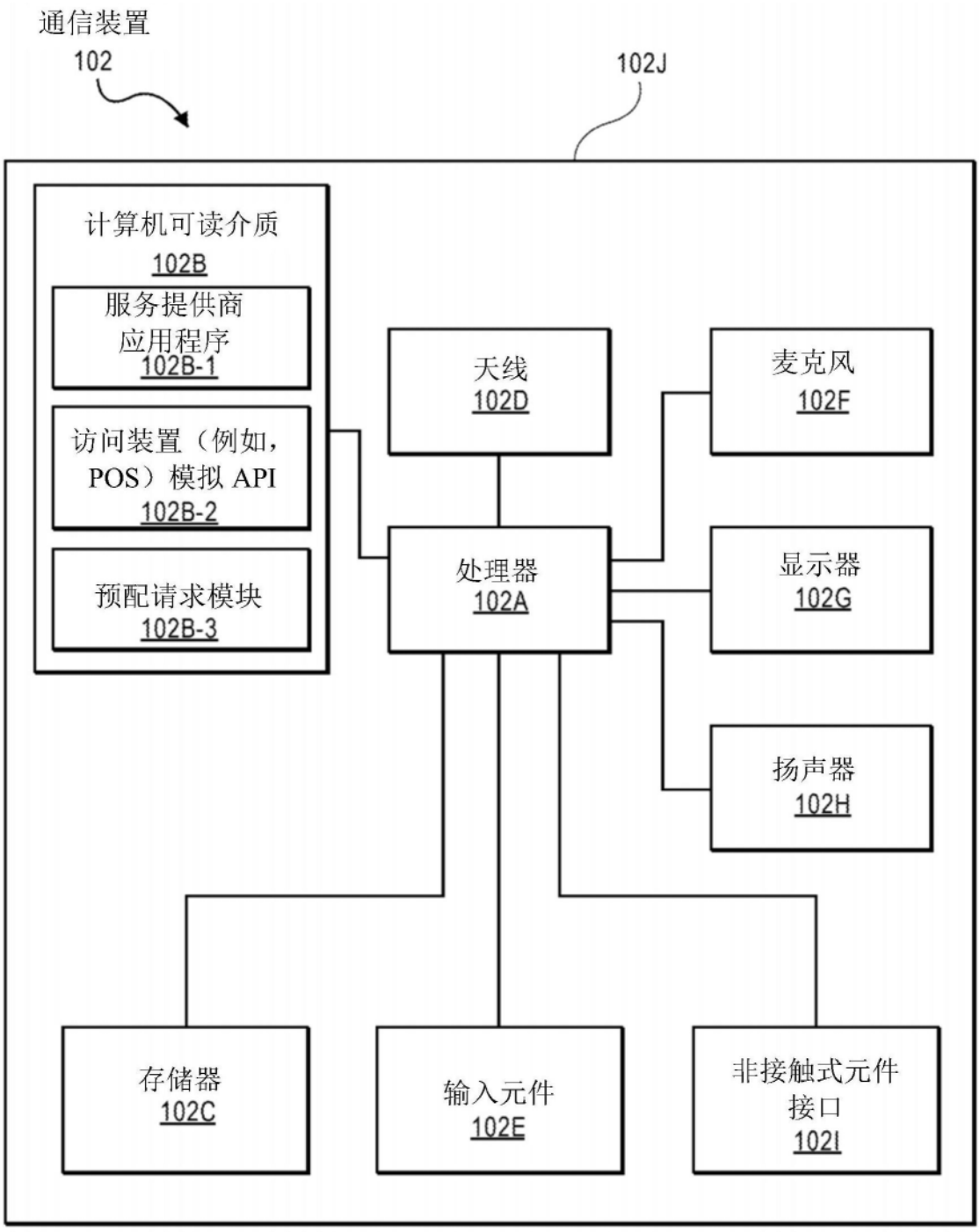

通信装置
102
102J
计算机可读介质
102B
服务提供商
应用程序
102B-1
访问装置（例如，
POS）模拟 API
102B-2
预配请求模块
102B-3
天线
102D
麦克风
102F
处理器
102A
显示器
102G
扬声器
102H
存储器
102C
输入元件
102E
非接触式元件
接口
102I

图2

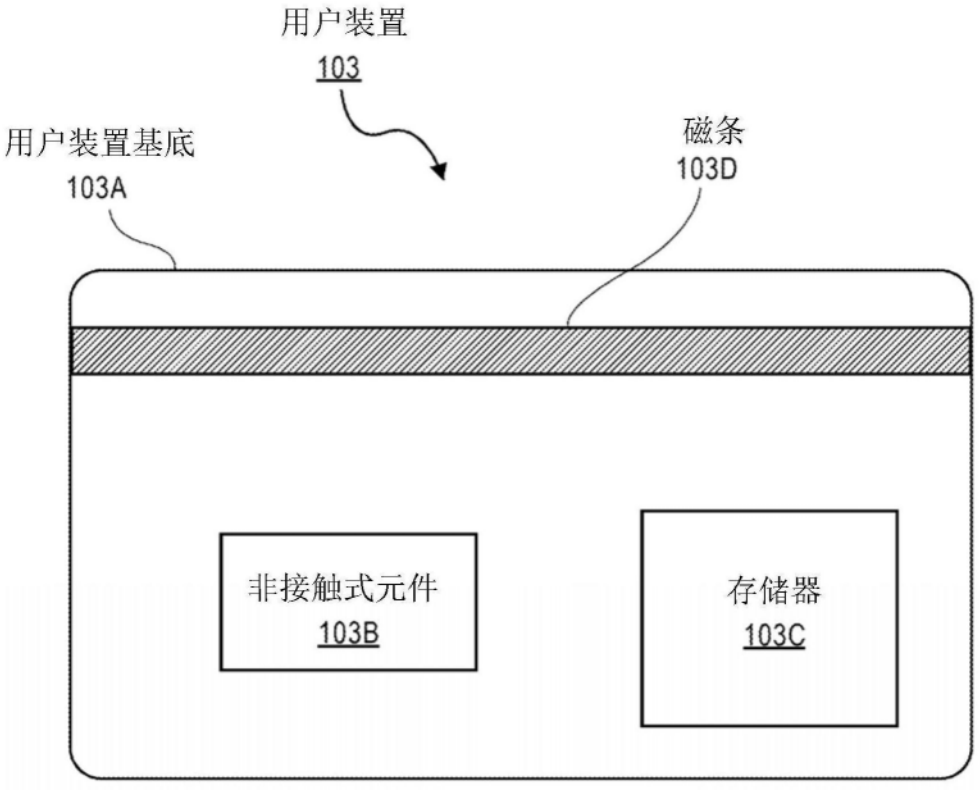


图3

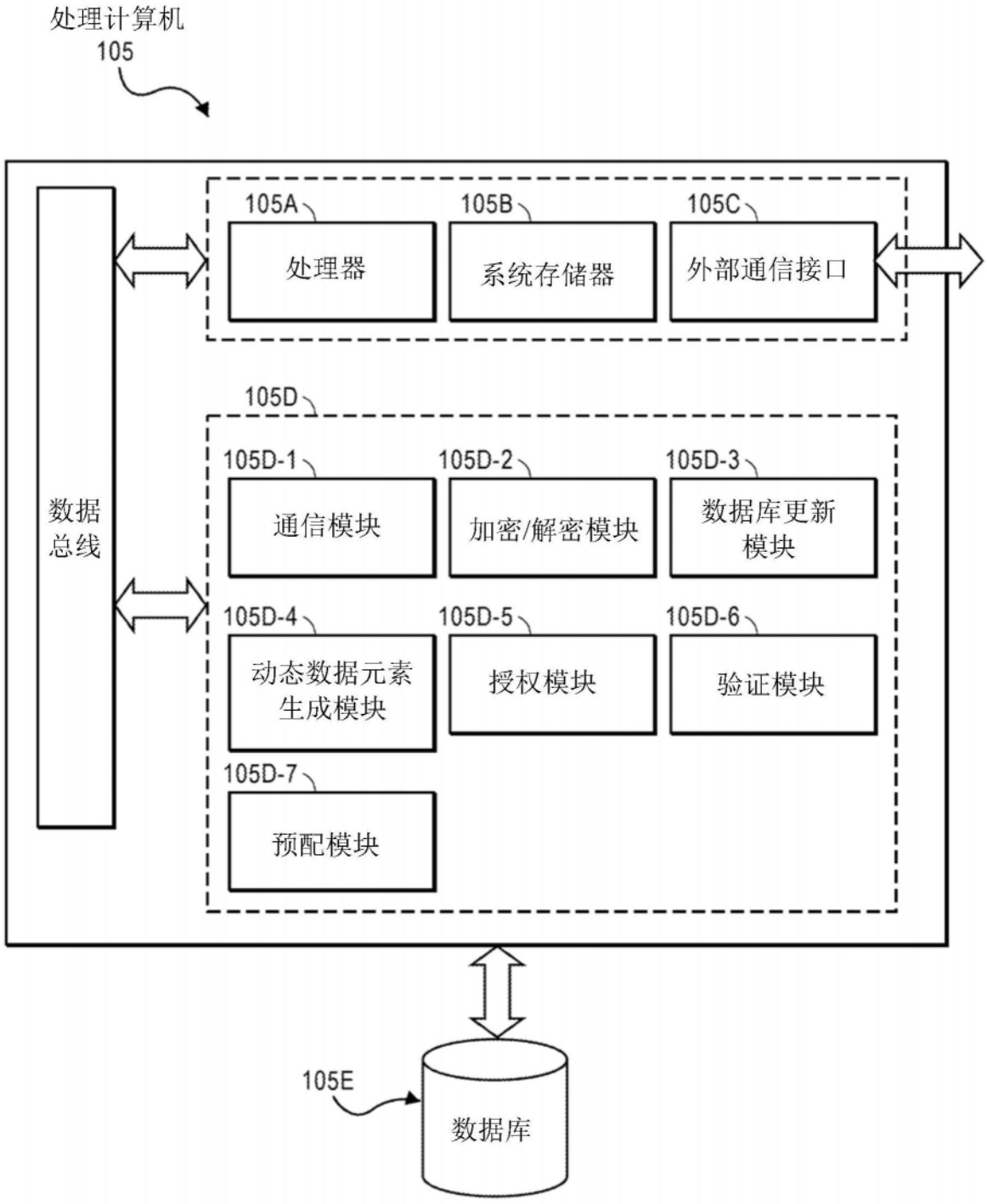

处理计算机
105
105A
处理器
105B
系统存储器
105C
外部通信接口
105D
105D-1
通信模块
105D-2
加密/解密模块
105D-3
数据库更新模块
105D-4
动态数据元素生成模块
105D-5
授权模块
105D-6
验证模块
105D-7
预配模块
数据总线
105E
数据库

图4

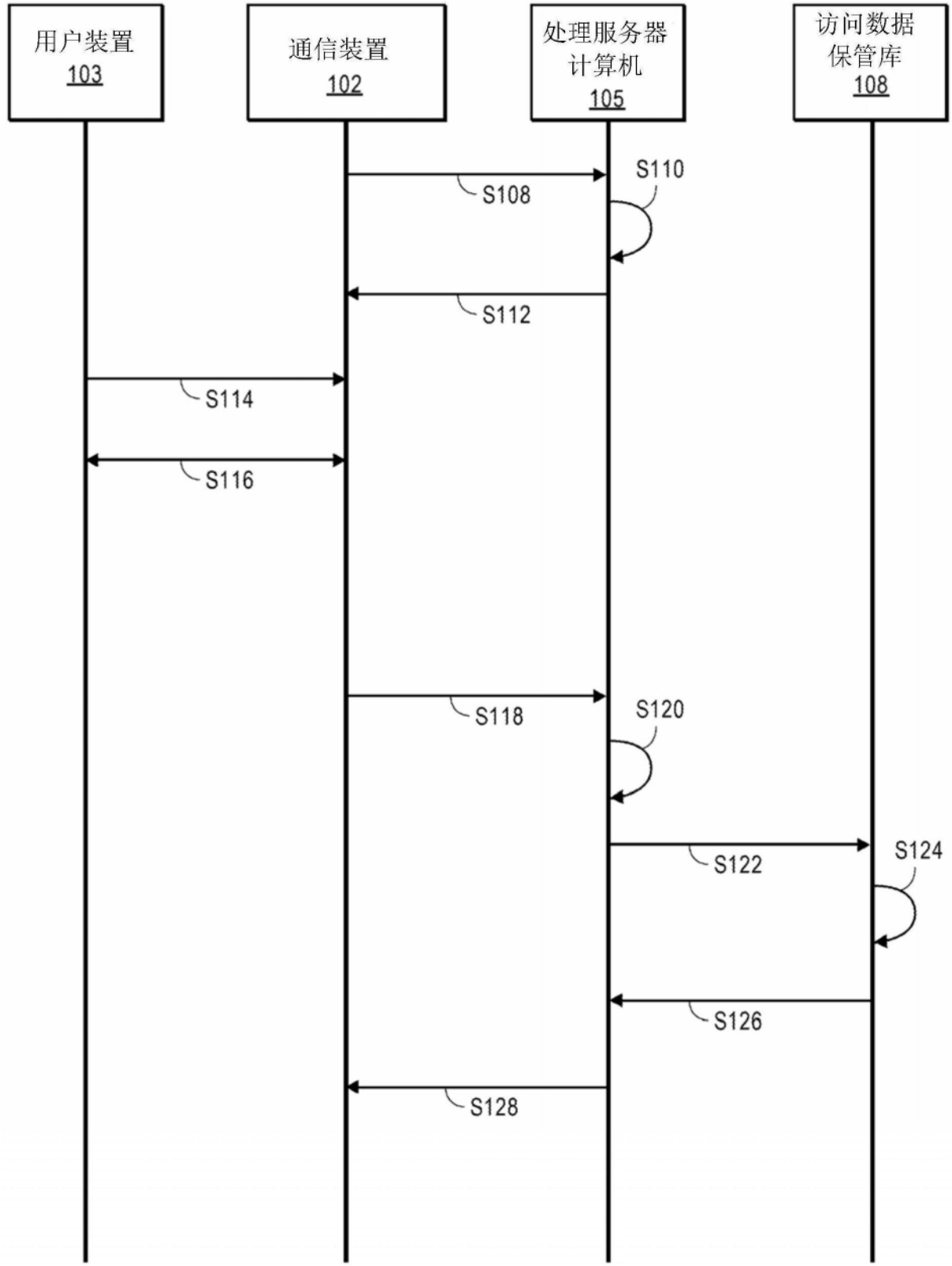

用户装置
103
通信装置
102
处理服务器
计算机
105
访问数据
保管库
108
S108
S110
S112
S114
S116
S118
S120
S122
S124
S126
S128

图5

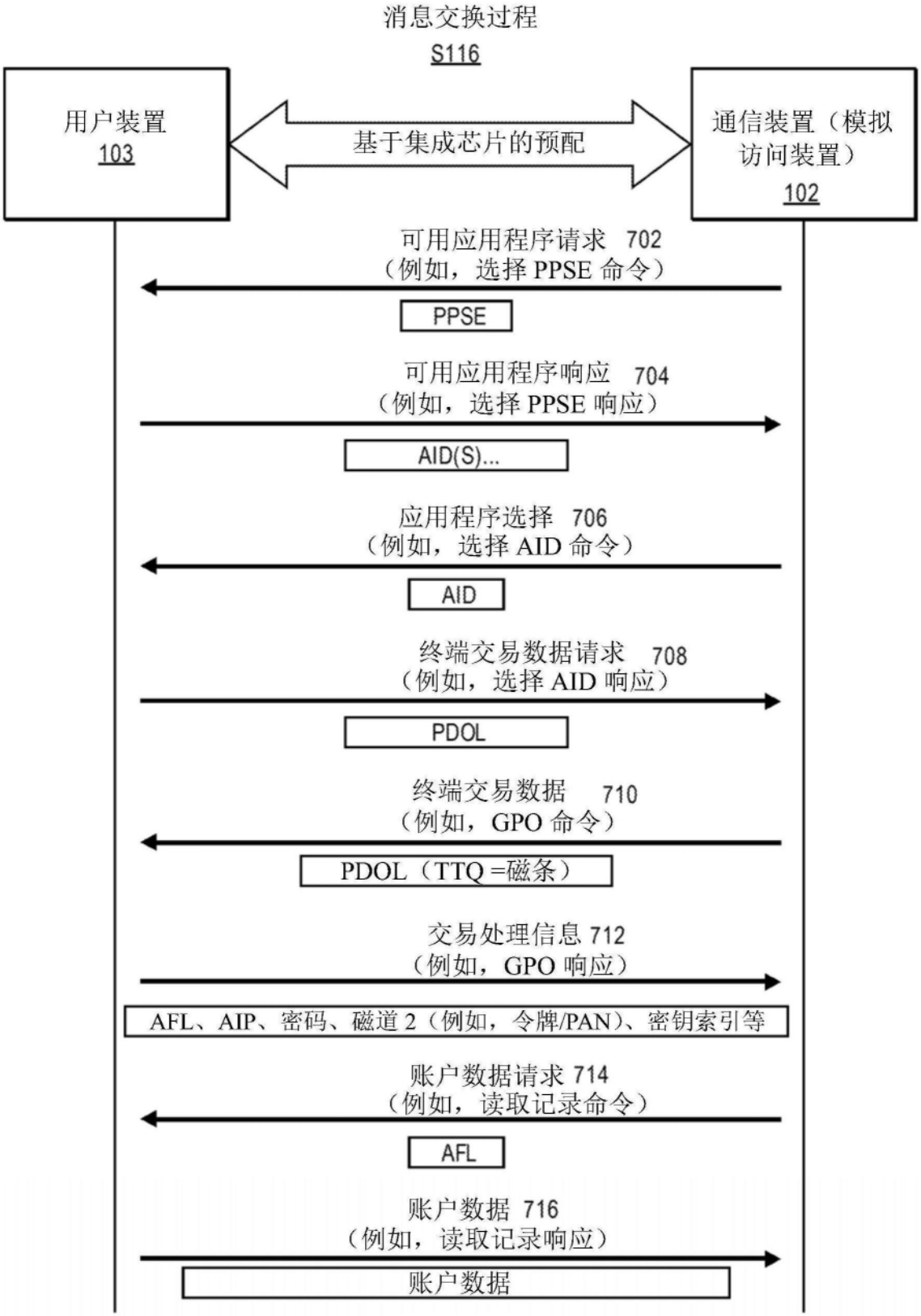

消息交换过程
S116
用户装置
103
基于集成芯片的预配
通信装置（模拟访问装置）
102
可用应用程序请求 702
（例如，选择 PPSE 命令）
PPSE
可用应用程序响应 704
（例如，选择 PPSE 响应）
AID(S)...
应用程序选择 706
（例如，选择 AID 命令）
AID
终端交易数据请求 708
（例如，选择 AID 响应）
PDOL
终端交易数据 710
（例如，GPO 命令）
PDOL（TTQ =磁条）
交易处理信息 712
（例如，GPO 响应）
AFL、AIP、密码、磁道 2（例如，令牌/PAN）、密钥索引等
账户数据请求 714
（例如，读取记录命令）
AFL
账户数据 716
（例如，读取记录响应）
账户数据

图6

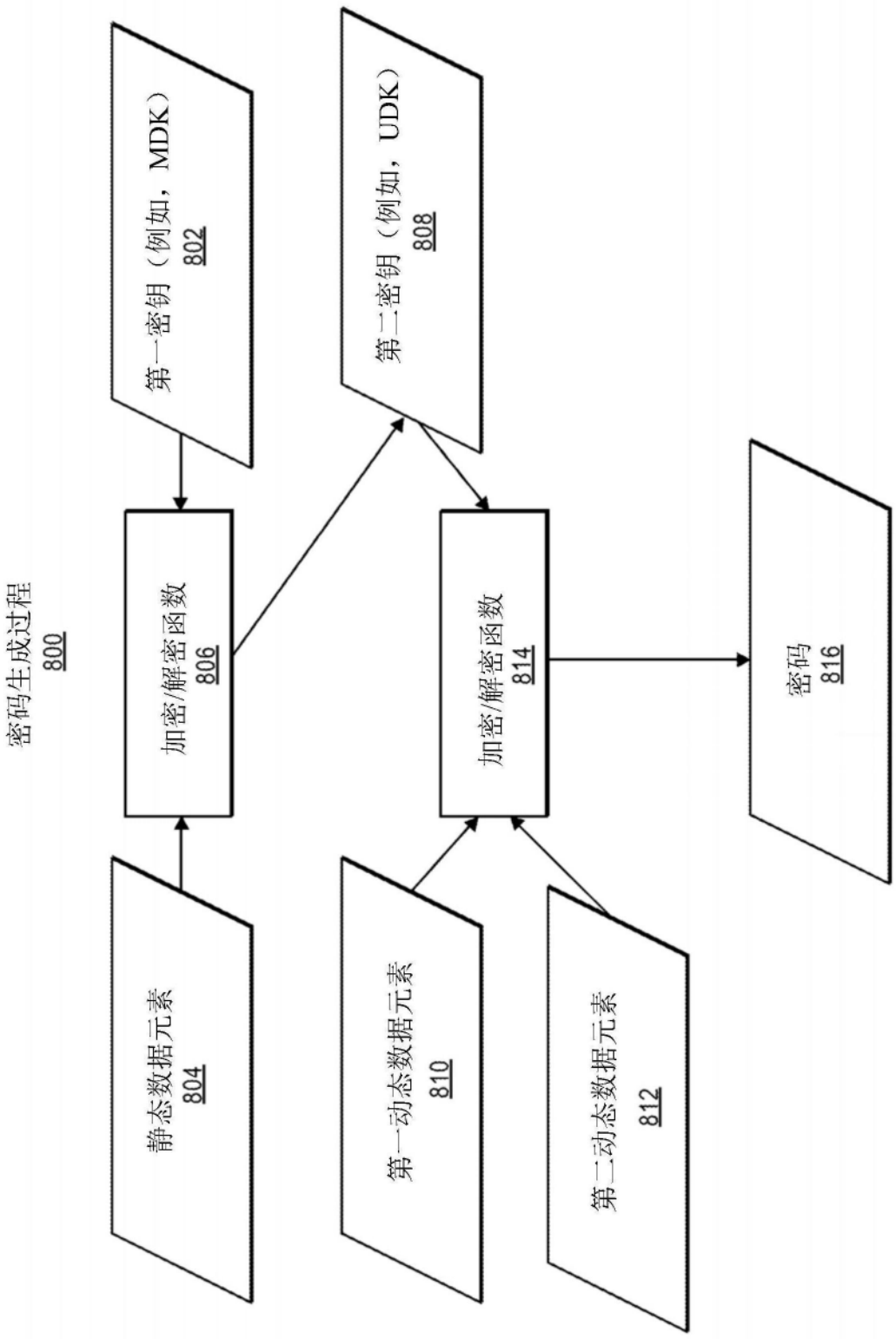

密码生成过程
800
第一密钥（例如，MDK）
802
第二密钥（例如，UDK）
808
加密/解密函数
806
加密/解密函数
814
密码
816
静态数据元素
804
第一动态数据元素
810
第二动态数据元素
812

图7

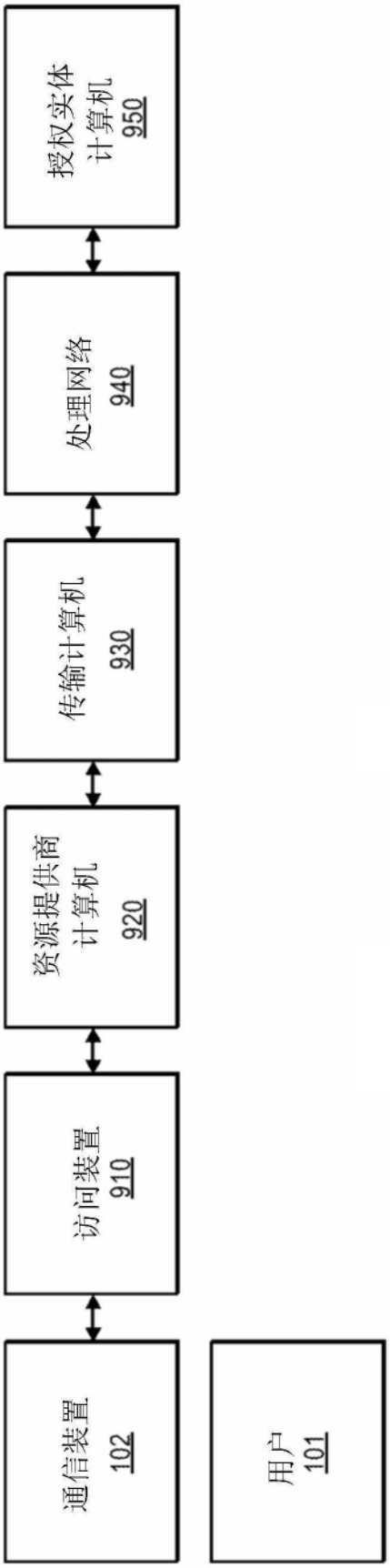

授权实体
计算机
950
处理网络
940
传输计算机
930
资源提供商
计算机
920
访问装置
910
通信装置
102
用户
101

图8

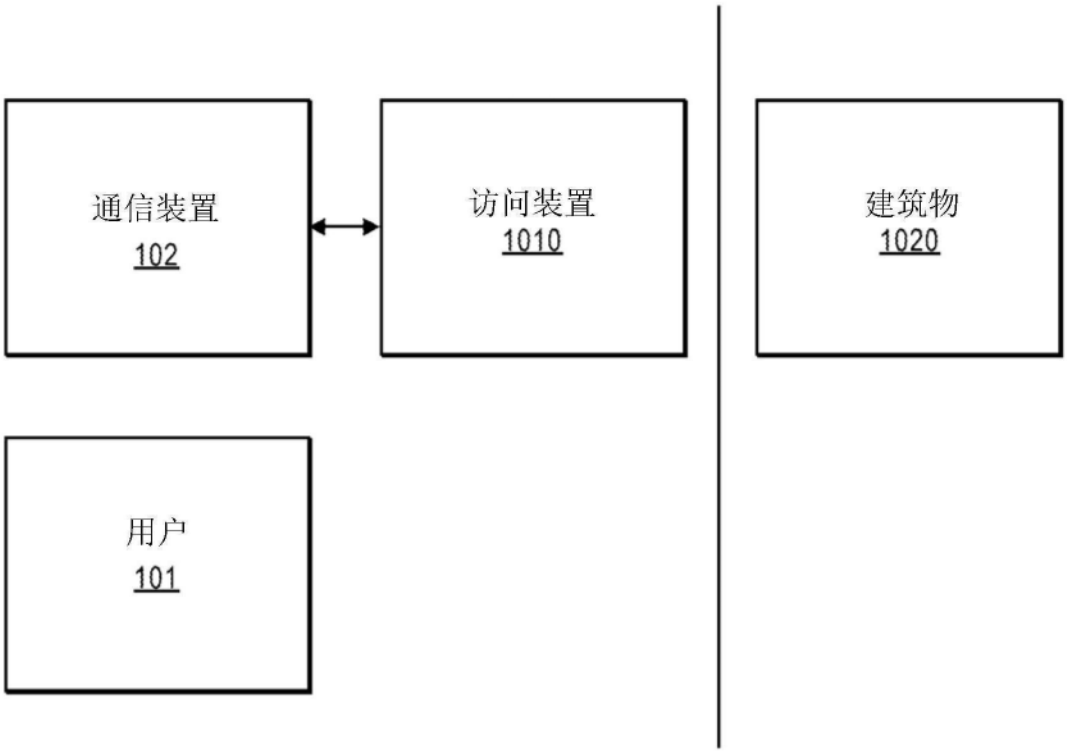


图9