(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112840594 B
(45)授权公告日 2024.12.31

(21)申请号 201880098694.3
(22)申请日 2018.10.15
(65)同一申请的已公布的文献号
申请公布号 CN 112840594 A
(43)申请公布日 2021.05.25
(85)PCT国际申请进入国家阶段日
2021.04.14
(86)PCT国际申请的申请数据
PCT/US2018/055833 2018.10.15
(87)PCT国际申请的公布数据
WO2020/081044 EN 2020.04.23
(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 A·阿艾拜 C·阿艾拜
(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 徐倩 钱慰民
(51)Int.Cl.
H04L 9/08(2006.01)
(56)对比文件
US 2015220917 A1,2015.08.06
WO 2009003080 A1,2008.12.31
审查员 万林青

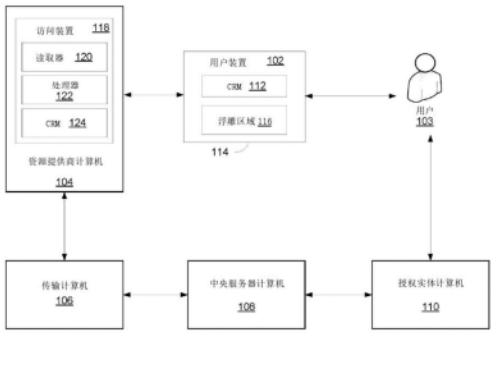
权利要求书3页 说明书19页 附图9页

(54)发明名称

用于为根本不同的数据消息安全地传送敏感数据的技术

(57)摘要

公开了用于安全传送例如标识符之类的敏感数据的系统和方法。一种用户装置可以接收包括终端类型指示符的第一消息。对于所述终端类型指示符的某些值,所述用户装置可以被配置成传输包括第一标识符和加密标识符的请求消息。对于所述终端类型指示符的其他值,所述用户装置可以被配置成至少部分地基于第二标识符的第一部分和所述加密标识符的第二部分来生成模糊标识符。所述用户装置然后可以传输包括所述模糊标识符和所述加密标识符的请求消息。



CN 112840594 B

1.一种计算机实施的方法,包括:

由用户装置从访问装置接收包括终端类型指示符的第一消息;

响应于所述终端类型指示符指示第一终端类型:

从所述用户装置向所述访问装置传输包括第一标识符和加密标识符的第二消息;以及

响应于所述终端类型指示符指示第二终端类型:

由所述用户装置至少部分地基于主账号的第一部分和所述加密标识符的第二部分来生成模糊主账号,其中所述主账号的所述第一部分包括与获取者相关联的标识号;以及

从所述用户装置向所述访问装置传输包括所述模糊主账号和所述加密标识符的所述第二消息。

2.如权利要求1所述的计算机实施的方法,还包括:

由所述用户装置获得存储的计数器值,其中所述加密标识符是进一步利用所述存储的计数器值来生成的;

响应于传输所述第二消息而生成修改后的计数器值;以及

将所述修改后的计数器值存储在所述用户装置处。

3.如权利要求2所述的计算机实施的方法,其中生成所述加密标识符还包括用存储在所述用户装置处的唯一导出密钥来对所述主账号和所述修改后的计数器值进行加密。

4.如权利要求1所述的计算机实施的方法,其中所述加密标识符的所述第二部分包括所述加密标识符的最右边的七个数字。

5.如权利要求1所述的计算机实施的方法,其中所述主账号的所述第一部分包括所述主账号的最左边的八个数字。

6.如权利要求1所述的计算机实施的方法,其中将包括所述第一标识符和所述加密标识符的所述第二消息传输到所述访问装置使所述访问装置:

将所述第一标识符与多个存储的标识符进行比较;

当所述第一标识符被包括在所述多个存储的标识符中时拒绝所述第二消息,其中拒绝所述第二消息使所述用户装置被拒绝访问由所述访问装置管理的资源;以及

当所述第一标识符未被包括在所述多个存储的标识符中时批准所述第二消息,其中批准所述第二消息使所述用户装置被许可访问由所述访问装置管理的资源。

7.如权利要求1所述的计算机实施的方法,其中将包括所述第一标识符和所述加密标识符的所述第二消息传输到所述访问装置使所述访问装置:

生成包括所述第一标识符和所述加密标识符的授权请求消息;并且

将所述授权请求消息传输到授权实体计算机。

8.如权利要求7所述的计算机实施的方法,其中所述授权实体计算机被配置成:

接收包括所述第一标识符和所述加密标识符的所述授权请求消息;

标识与所述第一标识符相关联的存储的标识符;

从所述加密标识符生成解密标识符;

将所述存储的标识符与所述解密标识符进行比较;并且

至少部分地基于将所述存储的标识符与所述解密标识符进行比较来处理所述授权请求消息。

9.如权利要求1所述的计算机实施的方法,其中将包括所述模糊主账号和所述加密标

识符的所述第二消息传输到所述访问装置使所述访问装置：

生成包括所述模糊主账号和所述加密标识符的授权请求消息;并且

将所述授权请求消息传输到授权实体计算机,其中传输包括所述模糊主账号和所述加密标识符的所述授权请求消息使所述授权实体计算机至少部分地基于所述模糊主账号的一部分来导出导出密钥,利用所述导出密钥来从所述加密标识符生成解密标识符,并且利用所述解密标识符来处理所述授权请求消息。

10.一种用户装置,包括：

一个或多个处理器;以及

一个或多个存储器,所述一个或多个存储器存储计算机可执行指令,其中由所述一个或多个处理器执行所述计算机可执行指令使所述用户装置：

从访问装置接收包括终端类型指示符的第一消息;

响应于所述终端类型指示符指示第一终端类型：

向所述访问装置传输包括第一标识符和加密标识符的第二消息;并且

响应于所述终端类型指示符指示第二终端类型：

至少部分地基于主账号的第一部分和所述加密标识符的第二部分来生成模糊主账号,其中所述主账号的所述第一部分包括与获取者相关联的标识号;以及

向所述访问装置传输包括所述模糊主账号和所述加密标识符的所述第二消息。

11.如权利要求10所述的用户装置,其中由所述一个或多个处理器执行所述计算机可执行指令还使所述用户装置：

获得存储的计数器值,其中所述加密标识符是进一步利用所述存储的计数器值来生成的;

响应于传输第二消息而生成修改后的计数器值;并且

将所述修改后的计数器值存储在所述用户装置处。

12.如权利要求11所述的用户装置,其中生成所述加密标识符还包括用存储在所述用户装置处的唯一导出密钥来对所述主账号和所述修改后的计数器值进行加密。

13.如权利要求10所述的用户装置,其中所述加密标识符的所述第二部分包括所述加密标识符的最右边的七个数字。

14.如权利要求10所述的用户装置,其中所述主账号的所述第一部分包括所述主账号的最左边的八个数字。

15.如权利要求10所述的用户装置,其中将包括所述第一标识符和所述加密标识符的所述第二消息传输到所述访问装置使所述访问装置：

将所述第一标识符与多个存储的标识符进行比较;

当所述第一标识符被包括在所述多个存储的标识符中时拒绝所述第二消息,其中拒绝所述第二消息使所述用户装置被拒绝访问由所述访问装置管理的资源;以及

当所述第一标识符未被包括在所述多个存储的标识符中时批准所述第二消息,其中批准所述第二消息使所述用户装置被许可访问由所述访问装置管理的资源。

16.如权利要求10所述的用户装置,其中将包括所述第一标识符和所述加密标识符的所述第二消息传输到所述访问装置使所述访问装置：

生成包括所述第一标识符和所述加密标识符的授权请求消息;并且

将所述授权请求消息传输到授权实体计算机。

17.如权利要求16所述的用户装置,其中所述授权实体计算机被配置成:

接收包括所述第一标识符和所述加密标识符的所述授权请求消息;

标识与所述第一标识符相关联的存储的标识符;

从所述加密标识符生成解密标识符;

将所述存储的标识符与所述解密标识符进行比较;并且

至少部分地基于将所述存储的标识符与所述解密标识符进行比较来处理所述授权请求消息。

18.如权利要求10所述的用户装置,其中将包括所述模糊主账号和所述加密标识符的所述第二消息传输到所述访问装置使所述访问装置:

生成包括所述模糊主账号和所述加密标识符的授权请求消息;并且

将所述授权请求消息传输到授权实体计算机,其中传输包括所述模糊主账号和所述加密标识符的所述授权请求消息使所述授权实体计算机至少部分地基于所述模糊主账号的一部分来导出导出密钥,利用所述导出密钥来从所述加密标识符生成解密标识符,并且利用所述解密标识符来处理所述授权请求消息。

用于为根本不同的数据消息安全地传送敏感数据的技术

背景技术

[0001] 本公开的实施方案涉及使在交易中使用的消息中的敏感数据模糊。这些技术可应用于接触式和/或非接触式智能卡交易。一般来说,非接触式智能卡旨在为客户提供高效的支付方式。智能卡能够向销售点(POS)装置提供所需的信息,以便通过使用例如射频或红外信号来完成交易。POS装置接收所提供的信息并且可以处理交易。

[0002] 由智能卡发送的信息可以包括敏感数据,例如用户的账户标识符(例如,个人账号)。因此,需要安全措施来保护用户免受可能截获此信息的老练欺诈者的伤害。当前的技术可能会有问题,因为整个账户标识符是未加密的。在其他常规技术中,账户标识符可以被加密,但仍然是根据具有已知数据字段的已知协议来传输和/或提供的。智能欺诈者仍然可以容易地标识消息中的加密数据字段,因此更有可能使用信息进行其邪恶行为。另外,使用常规技术,账户标识符可能保持静态,潜在地允许欺诈者跟踪用户的交易。

[0003] 更进一步地,常规系统不限制敏感信息的使用。例如,欺诈者一旦已获得敏感信息,就可以在各种上下文中利用该敏感信息。

[0004] 本发明的实施方案单独地以及共同地解决这些问题和其他问题。

发明内容

[0005] 本发明的实施方案涉及可用于安全地传送与诸如非接触式智能卡之类的用户装置相关联的账户标识符(例如,PAN)的方法、系统、装置和计算机可读介质。在一些实施方案中,用户装置可以存储主账号(PAN)和辅账号(SAN)。可以以不允许跟踪账户标识符以进行隐私保护的方式传送账户标识符(例如,PAN)。有利地,在本发明的实施方案中,账户信息是以安全且不需要以任何显著方式更新现有支付基础设施的方式传送的。

[0006] 在需要静态标识符的上下文中,可以在本文讨论的实施方案中利用附加账户标识符(例如,SAN)。作为示例,预期一些类型的访问装置允许或者拒绝用户几乎实时地访问资源。因此,此类访问装置可以利用静态标识符来对照允许列表和/或阻止列表来检查,以便迅速地允许或拒绝用户对智能卡的访问。可以仅在某些情形下利用附加账户标识符(例如,SAN)。例如,系统可以确保SAN仅可用在涉及终端和/或商家的交易和/或特定类型的交易中。作为非限制性示例,系统可以被配置成确保仅可以在涉及中转终端(例如,中转机构的旋转门)的交易中利用SAN。

[0007] 本发明的一个实施方案涉及一种方法,该方法包括由用户装置从访问装置接收包括终端类型指示符的第一消息。该方法还可以包括,响应于终端类型指示符指示第一终端类型,从用户装置向访问装置发送包括第一标识符(例如,SAN)和加密标识符(例如,从PAN和交易计数器生成的加密标识符)的请求消息。该方法还可以包括,响应于终端类型指示符指示第二终端类型,由用户装置至少部分地基于第二标识符(例如,主PAN)的第一部分和加密标识符的第二部分来生成模糊标识符。该方法还可以包括从用户装置向访问装置传输。在一些实施方案中,请求消息可以包括模糊标识符和加密标识符。

[0008] 本发明的另一实施方案涉及一种用户装置,该用户装置包括:一个或多个处理器;

以及一个或多个存储器,该一个或多个存储器包括计算机可执行指令,这些计算机可执行指令在由一个或多个处理器执行时使用户装置执行操作。这些操作可以包括由用户装置从访问装置接收包括终端类型指示符的第一消息。这些操作还可以包括,响应于终端类型指示符指示第一终端类型,从用户装置向访问装置发送包括第一标识符(例如,SAN)和加密标识符(例如,从主PAN和交易计数器生成的加密标识符)的请求消息。这些操作还可以包括,响应于终端类型指示符指示第二终端类型,由用户装置至少部分地基于第二标识符(例如,主PAN)的第一部分和加密标识符的第二部分来生成模糊标识符。这些操作还可以包括从用户装置向访问装置传输。在一些实施方案中,请求消息可以包括模糊标识符和加密标识符。

[0009] 本发明的另一实施方案涉及一种(非瞬态)计算机可读介质。所述计算机可读介质包括用于执行本文所论述的方法的代码。在一些实施方案中,诸如智能卡之类的用户装置可以包括这种计算机可读介质。

[0010] 下面参考附图进一步详细地描述本发明的这些和其他实施方案。

附图说明

[0011] 图1示出根据一些实施方案的用于处理交易的系统的框图。

[0012] 图2描绘根据一些实施方案的用于在用户装置处生成和存储数据的方法。

[0013] 图3描绘根据一些实施方案的用于从驻留在计算装置(例如,智能卡)上的数据生成唯一导出密钥的方法。

[0014] 图4描绘根据一些实施方案的用于执行离线认证的方法。

[0015] 图5示出根据一些实施方案的用于安全地传送敏感数据的方法的流程图。

[0016] 图6描绘用于在一些实施方案中使用的示例性记录格式。

[0017] 图7描绘用于在一些实施方案中使用的另一示例性记录格式。

[0018] 图8示出根据一些实施方案的用于执行数据验证的方法的流程图。

[0019] 图9示出根据一些实施方案的用于执行数据验证的方法的流程图。

具体实施方式

[0020] 如上所述,在常规支付交易中,账户标识符(例如,个人账户标识符,也称为主PAN)在它从诸如非接触式智能卡之类的用户装置传递到访问装置(例如,POS终端、旋转门读取器等)并且最终通过传统支付处理网络时未被加密。在一些常规技术中,账户标识符可以被加密和/或模糊,然而,加密/模糊数据仍然可以被提供在交易消息的传统数据字段中,因此所述数据字段能容易地标识潜在欺诈者。

[0021] 虽然可以对整个账户标识符进行加密,但并非在所有情况下都可行。如果账户标识符被加密,则常规交易处理系统可能无法成功地处理交易。例如,典型的账户标识符包括银行标识号(BIN)。BIN用于将授权请求消息路由到适当的发行方或支付处理器。如果账户标识符被加密,则BIN将改变。如果BIN改变,则无法将适当的授权请求消息路由到正确的发行方。

[0022] 与对整个账户标识符进行加密相关联的另一限制与和账户标识符中的数字序列相关联的误差校验有关。可以使用校验和算法来实现误差校验,所述校验和算法确定账户标识符的数字是否呈适当的序列。示例校验和算法是模10算法(也称为“Luhn校验”)。

[0023] 因此,对整个账户标识符进行加密至少会破坏BIN、校验和以及通过收据上的打印数字标识账户标识符的能力。

[0024] 本文所述的处理可用于保护发起装置(例如,智能卡)处的账户标识符。如下面将进一步详细说明的,本发明的实施方案仅使账户标识符的一部分模糊,这允许账户的BIN保持未加密并且继续使用Luhn校验。此外,本发明的实施方案不仅还可以用于使典型授权请求消息中的账户标识符模糊,而且还可以确保在消息中的其他地方提供整个加密账户标识符,以便使消息不太可能被标识。

[0025] 本文讨论的技术还使得模糊标识符或SAN能够由用户装置根据交易的上下文(例如,什么类型的终端正在请求信息)来利用。因此,对于与第一组交易类型、终端类型等相关联的交易,可以在交易中利用模糊PAN,然而对于与第二组交易类型、终端类型等相关联的交易,可以利用SAN。当在允许的上下文中利用SAN时,可以将其限制为仅由授权实体处理。对于第一组交易/终端类型交易,可以利用模糊PAN,使得不可以跟踪用户的活动。这些技术使得能够对于离线交易(例如,终端在终端处对智能卡进行认证的交易)以及源自离线交易的后续在线交易利用静态标识符,然而可以对于不需要对方离线认证的在线认证交易利用动态标识符(例如,动态值)。

[0026] 在论述本发明的具体实施方案之前,对某些术语的一些描述可能是有用的。

[0027] “计算装置”(也称为“用户装置”)可以是能够执行计算并且能够与其他装置通信的任何合适的装置。例如智能卡之类的便携式消费装置是计算装置的示例。其他类型的计算装置可能不是便携式的。

[0028] “动态值”是指动态变化的值。计算装置可以维持各种动态值。动态值的示例是应用交易计数器(ATC)。ATC最初可以由计算装置(例如,授权实体)的发行方设置为预定值。此后,可以随着每次交易使ATC递增。替代地,可以随着每次交易使ATC从其初始预定值递减。ATC可以是任何长度的值。此外,发行方可以维持供发行方计算机访问的相应ATC。此相应ATC可用于标识可能出于欺诈目的而重复出现的支付服务。在替代实施方案中,基于交易数据的密码、数字签名或散列值可用于代替存储在计算装置处的ATC,或者与存储在计算装置处的ATC一起使用。

[0029] 其他动态值(例如,数据元素)的示例可以包括一天中的时间、当前交易金额和从终端随机生成的数字等。数据元素是动态的,这意味着它们可以随着每次交易或几乎随着每次交易而改变。动态数据元素可以与用户的计算装置相关和/或通常可以与用户相关。

[0030] “授权实体”可以是授权请求的实体。授权实体的示例可以是发行方、政府机构、文件存储库、访问管理员等。“发行方”通常可以指维持用户账户的业务实体(例如,银行)。发行方也可以向客户发行存储在例如蜂窝电话、智能卡、平板计算机或膝上型计算机之类的用户装置上的支付凭证。“授权实体计算机”可以由授权实体或代表授权实体操作。

[0031] “收单方”通常可以是与特定商家或其他实体具有业务关系的业务实体(例如,商业银行)。一些实体可以执行发行方功能和收单方功能两者。一些实施方案可以涵盖此类单个实体发行方-收单方。收单方可以操作收单方计算机,所述收单方计算机一般也可以被称为“传送计算机”。

[0032] “资源提供商”可以是可提供例如商品、服务、信息和/或访问之类的资源的实体。资源提供商的示例包括商家、访问装置、安全数据访问点等。“商家”通常可以是参与交易并

且可出售商品或服务或提供对商品或服务的访问的实体。“资源提供商计算机”可以是可由资源提供商或代表资源提供商操作的任何合适的计算装置。

[0033] “处理网络计算机”(也称为中央服务器计算机)可以包括用于处理网络数据的服务器计算机。在一些实施方案中,处理网络计算机可以耦合到数据库,并且可以包括用于服务来自一个或多个客户端计算机的请求的任何硬件、软件、其他逻辑或前述项的组合。处理网络计算机可以包括一个或多个计算设备,并且可以使用各种计算结构、布置以及编译中的任一项来服务来自一个或多个客户端计算机的请求。在一些实施方案中,处理网络计算机可以操作多个服务器计算机。在此类实施方案中,每个服务器计算机都可以被配置成处理给定区域的交易或者基于交易数据处理特定类型的交易。

[0034] 处理网络计算机可以包括用于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。示例性处理网络计算机可以包括VisaNet™。包括VisaNet™在内的网络能够处理信用卡交易、借记卡交易和其他类型的商业交易。VisaNet™具体包括处理授权请求的集成支付系统(集成支付系统)以及执行清算和结算服务的Base II系统。处理网络计算机可以使用任何合适的有线或无线网络,包括因特网。

[0035] “授权请求消息”可以是发送到交易处理计算机和/或授权实体计算机(例如,支付卡的发行方)以请求交易授权的电子消息。根据一些实施方案的授权请求消息可符合ISO 8583,其是用于交换与客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他信息。

[0036] “授权响应消息”可以是对由授权实体计算机或交易处理计算机生成的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,其可以是授权实体(例如,发行方银行)响应于电子消息中的授权请求消息(直接或通过交易处理计算机)传回资源提供商计算机的指示交易被批准的代码。所述代码可充当授权的证明。在一些实施方案中,交易处理计算机可以生成授权响应消息或将授权响应消息转发给资源提供商。

[0037] “主账号”(PAN)可以是支付账号的标识符。PAN可以包括一系列字母数字字符(例如,16个)。PAN(或PAN的模糊或加密版本)可以用于发起、授权、结算或解决支付交易。在一些实施方案中,可以对于任何类型的交易利用PAN。

[0038] “-账号”(SAN)可以是支付账户的另一标识符。SAN可以包括一系列字母数字字符(例如,16个)。SAN(或SAN的模糊或加密版本)可以用于发起、授权、结算或解决交易。在一些实施方案中,SAN的使用可以局限于某些类型的交易。例如,当交易包括特定类型的商家(例如,中转机构、中转商家、体育馆商家等)时,当交易由特定终端类型(例如,旋转门等)的终端发起时,和/或当交易是特定类型的交易(例如,中转交易、票价检查交易等)时,可以利用SAN。在一些实施方案中,SAN可以与PAN相关联并且两者都可以与特定用户的账户(例如,由发行方代表用户维护的金融账户)相关联。在一些实施方案中,PAN和相关SAN各自可以包括

相同的8个最左边的数字(例如,与银行标识符号(BIN))相对应。

[0039] “模糊标识符”可以包括作为标识符的模糊版本的标识符(例如,16位PAN)。在一些实施方案中,模糊标识符可以是“保留格式的”,并且可以具有与在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,ISO 8583金融交易消息格式)。在一些实施方案中,模糊标识符可以代替PAN用来发起、授权、结算或解决支付交易,或者在通常将提供原始凭证的其他系统中表示原始凭证。

[0040] “加密标识符”可以包括任何合适的加密值。可以利用任何合适的加密技术例如利用对称和/或不对称加密技术来从标识符(例如,主PAN)生成加密值。在一些实施方案中,可以利用均存储在用户装置处的主PAN和动态值来生成加密标识符。

[0041] 就本申请而言,“支付数据”可以包括:关于金融应用的由支付服务用于执行交易的那些数据元素,以及关于非金融交易的不包括本发明的任何必要数据元素。例如,当支付服务是磁条信用卡交易时,“支付数据”将包括如信用卡行业的普通技术人员所理解的轨道1和/或轨道2数据,例如主账号、到期日期、服务代码和自主数据(discretionary data)。“支付数据”还可以包括唯一卡标识号或服务提供商的唯一标识号。支付数据可以驻存在位于用户装置上的存储器中(例如,信用卡和/或借记卡、智能卡等)。

[0042] “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、小型计算机集群或充当单元的一组服务器。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。

[0043] “处理器”可以指任何合适的一个或多个数据计算装置。处理器可以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。所述CPU可以是微处理器,例如AMD的速龙(Athlon)、钻龙(Duron)和/或皓龙(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)的赛扬(Celeron)、安腾(Itanium)、奔腾(Pentium)、至强(Xeon)和/或XScale;和/或类似处理器。

[0044] “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。此类存储器可以使用任何合适的电气、光学和/或磁性操作模式来操作。

[0045] 图1示出根据一些实施方案的用于处理交易的系统100的框图。系统100可以用于促进图1中描绘的各种计算机之间的数据通信,以用于认证和/或授权金融和非金融交易。系统100包括用户装置102、资源提供商计算机104、传送计算机106、中央服务器计算机108和授权实体计算机110。这些系统和计算机中的每一个可以彼此进行操作性通信。为了简化说明,在图1中示出特定数量的组件。然而,应理解,本发明的实施方案可以包括多于一个每种组件。此外,本发明的一些实施方案可以包括比图1中所示的所有组件少或多的组件。此外,图1中的组件可以通过任何合适的通信介质(包括因特网)使用任何合适的通信协议来进行通信。

[0046] 资源提供者计算机104可以由资源提供者(例如,商家、中转系统等)操作或者代表资源提供者进行操作,并且传送计算机可以与资源提供者相关联。例如,传送计算机可以由负责管理与资源提供商相关联的账户的收单方(例如,金融机构)操作。授权实体计算机110

可以由发行方(例如,另一金融机构)操作。在一些实施方案中,实体既是收单方又是发行方,并且本发明的实施方案包括此类实体。

[0047] 用户装置102可呈任何合适的形式。例如,用户装置102可以是手持式的且紧凑的,使得其能够放到钱包和/或口袋中。用户装置102的示例可以包括智能卡、信用卡和/或借记卡、钥匙链装置等。用户装置102的其他示例可以包括蜂窝电话、个人数字助理(PDA)、寻呼机、支付卡、安全卡、访问卡、智能媒体、应答器等。用户装置102还可以是用于存储零售商店信用等的储值卡。

[0048] 用户装置102可以包括计算机可读介质(CRM)112和主体114。CRM112可以位于主体114上,所述主体可以呈塑料基板、壳体或其他结构的形式。如果用户装置102形式为卡,则它可以具有被浮雕有个人账号(PAN)的浮雕区域116。在一些实施方案中,CRM 112可以存储PAN以及辅账号(例如,SAN)和/或计数器。

[0049] 计算机可读介质112可以是存储数据的存储器,并且可以呈任何合适的形式。示例性CRM 112可以呈磁条、存储器芯片等形式。计算机可读介质112可以以加密或未加密形式电子地存储主和/或加密和/或模糊PAN。

[0050] 中央服务器计算机108可以包括用于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™之类的支付处理网络能够处理信用卡交易、借记卡交易和其他类型的商业交易。VisaNet™具体包括处理授权请求的VIP系统(Visa集成支付系统),和执行清算和结算服务的Base 11系统。

[0051] 中央服务器计算机108可以包括服务器计算机。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、小型计算机集群或充当单元的一组服务器。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。中央服务器计算机108可以使用任何合适的有线或无线网络,包括因特网。

[0052] 资源提供者计算机104还可以具有能够与用户装置102交互的访问装置118(例如,旋转门、门、销售点终端等),或者可以从其接收通信。在图1中,访问装置118可以是资源提供者计算机104的组件并且/或者访问装置118可以由资源提供者计算机访问和/或与资源提供者计算机104通信。在一些实施方案中,访问装置118在本发明的其他实施方案中可能位于任何其他合适的位置处。资源提供商计算机104可以包括由资源提供商(例如,商家)操作的任何合适的计算设备。在一些实施方案中,资源提供商计算机104可以包括一个或多个服务器计算机,所述一个或多个服务器计算机可以托管与资源提供商(例如,商家)相关联的一个或多个网站。在一些实施方案中,资源提供商计算机104可以被配置成通过传送计算机106向中央服务器计算机108发送数据,作为用户(例如,客户)与资源提供商之间的交易的支付验证和/或认证过程的一部分。资源提供者计算机104还可以被配置成生成资源提供者与用户103之间的交易的授权请求消息,并且将这些授权请求消息路由到授权实体计算机110(例如,经由传送计算机106和/或中央服务器计算机108)以进行附加交易处理。

[0053] 根据本发明的实施方案的访问装置可以呈任何合适的形式。访问装置的示例包括销售点(POS)装置、旋转门、门、蜂窝电话、PDA、个人计算机(PC)、平板PC、手持式专用读取器、机顶盒、电子收银机(ECR)、自动柜员机(ATM)、虚拟收银机(VCR)、信息亭、安全系统、访问系统等。

[0054] 访问装置118可以包括读取器120、处理器122和计算机可读介质124。读取器120可以使用任何合适的接触或非接触式操作模式。例如,示例性读卡器可以包括RF(射频)天线、磁条读取器等以与用户装置102交互。

[0055] 在至少一个实施方案中,用户103可以使用用户装置102(例如,信用卡)来在资源提供者计算机104处发起对商品或服务的购买。用户装置102可以与例如POS(销售点)终端之类的访问装置118交互。例如,用户103可以持有信用卡,并且可以通过POS终端中的适当插槽刷卡。替代地,POS终端可以是非接触式读取器,并且用户装置102可以是例如非接触式卡之类的非接触式装置。在此交互期间,用户装置102可以被配置成确定访问装置118是特定类型的终端(例如,POS装置)。如果访问装置118是这种特定类型的终端,则用户装置102可以将存储在用户装置102处的主PAN的模糊版本和主PAN的加密版本提供给访问装置118。

[0056] 然后可以将授权请求消息转发到传送计算机106。传送计算机106通常与业务实体(例如,商业银行)相关联,所述业务实体与特定资源提供商(例如,商家)或其他实体具有业务关系,并且可能涉及交易过程。传送计算机106可以为资源提供商发行和管理账户,并代表资源提供商与授权实体计算机110交换资金。一些实体可以执行授权实体计算机110和传送计算机106两者的功能。本发明的实施方案涵盖此类单实体发行方-收单方计算机。在接收到授权请求消息之后,传送计算机106可以将授权请求消息发送到中央服务器计算机108。然后,中央服务器计算机108可以将授权请求消息转发到用户装置102的授权实体计算机110或代表授权实体行事的第三方实体。

[0057] 中央服务器计算机108可以是包括或操作用于处理(例如,支付处理)的至少一个服务器计算机的网络。中央服务器计算机108中的服务器计算机可以包括处理器和耦合到处理器的计算机可读介质,所述计算机可读介质包括可由处理器执行的代码,用于执行本文所述的功能。在一些实施方案中,服务器计算机可以耦合到数据库,并且可以包括用于服务于来自一个或多个客户端计算机的请求的任何硬件、软件、其他逻辑或前述项的组合。服务器计算机可以包括一个或多个计算设备并且可以使用各种计算结构、布置和编译中的任一项来服务来自一个或多个客户端计算机的请求。在一些实施方案中,中央服务器计算机108可以操作多个服务器计算机。在此类实施方案中,每个服务器计算机都可以被配置成处理给定区域的交易或者基于交易数据处理特定类型的交易。

[0058] 中央服务器计算机108可以包括用于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。中央服务器计算机108可以包括VisaNet™。包括VisaNet™在内的网络能够处理信用卡交易、借记卡交易和其他类型的商业交易。VisaNet™具体包括处理授权请求的集成支付系统(集成支付系统)以及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。

[0059] 中央服务器计算机108可以处理交易请求消息,并且确定交易请求消息的适当目的地(例如,认证计算机)。中央服务器计算机108还可以处理和/或促进交易的清算和结算。

[0060] 授权实体计算机110通常与商业实体(例如,银行)相关联,所述商业实体(例如,银行)为消费者(例如,用户103)发行和维护消费者账户。授权实体计算机110可以为客户账户发行支付装置,包括信用卡和借记卡等。

[0061] 在授权实体计算机或代表授权实体行动的第三方实体接收到授权请求消息之后,授权实体计算机110或代表发行方行动的第三方实体可以确定PAN将被用于交易。例如,授

权实体计算机110可以确定正在授权请求消息中利用模糊PAN,授权请求消息的商家类型指示包括PAN,和/或授权请求消息的交易类型指示包括PAN。在一些实施方案中,可以对照已知辅账户标识符(SAN)的映射来检查包括在授权请求消息中的PAN,并且如果被标识,则可以拒绝授权请求消息。在一些实施方案中,如果在已知SAN的映射中不包括授权请求消息中的PAN(例如,它不是SAN),则还可以处理该消息。一旦确定了正在利用PAN,授权实体计算机就可以处理授权请求消息以许可或者拒绝交易。授权实体计算机可以向中央服务器计算机108发回授权响应消息以指示当前交易是否被授权(或未被授权)。然后,中央服务器计算机108将授权响应消息转发回到传送计算机106。然后,传送计算机106将响应消息发送回资源提供商计算机104。

[0062] 在资源提供商计算机104接收到授权响应消息之后,资源提供商计算机104处的访问装置118接着可以将授权响应消息提供给用户103。响应消息可以由访问装置118显示,或者可以打印在收据上。

[0063] 在一天结束时,常规的清算和结算过程可以由系统100进行。清算过程是指收单方和发行方之间交换财务细节的过程,以促进过账到用户的账户并对用户的结算头寸进行对账。

[0064] 在另一示例性实施方案中,用户103可以利用用户装置102来发起离线交易。例如,用户103可以在具有特定终端类型(例如,指示允许/限制对转系统进行访问的中转旋转门和/或票价检查装置)的访问装置118处呈现用户装置102。在一些实施方案中,访问装置可以是非接触式读取器,并且用户装置102可以是诸如非接触式卡之类的非接触式装置。在一些实施方案中,在呈现用户装置102时访问装置118可以从用户装置102请求认证数据。由于访问装置118具有特定终端类型,用户装置可以提供诸如在用户装置102处存储在CRM 112中的SAN之类的信息。附加地,用户装置可以在提供给访问装置118的数据内提供PAN的加密版本。

[0065] 在授权实体计算机或代表授权实体行动的第三方实体接收到授权请求消息之后,授权实体计算机110或代表发行方行动的第三方实体可以被配置成确定SAN被包括在授权请求消息中。作为示例,授权实体计算机110可以至少部分地基于确定包括在消息中的账号字段中的数据不以7个零结束、确定请求商家与特定商家类型(例如,中转商家类型)相关联和/或授权请求消息指示交易的类型(例如,中转交易)和/或从中生成授权请求消息的终端的类型(例如,中转终端)来确定在授权请求消息中包括SAN。授权实体计算机可以被配置成在不允许SAN使用的交易中拒绝包括SAN的任何授权请求消息。如果在SAN被允许的交易(例如,中转交易、票价交易等)的消息中包括SAN,则授权实体计算机可以继续处理授权请求消息以批准或者拒绝交易。授权实体计算机可以向中央服务器计算机108发回授权响应消息以指示当前交易是否被授权(或未被授权)。然后,中央服务器计算机108将授权响应消息转发回到传送计算机106。然后,传送计算机106将响应消息发送回资源提供商计算机104。

[0066] 在至少一个实施方案中,授权实体可以对用户装置102进行个人化过程。在此个性化过程期间,可以将主导出密钥(MDK)、PAN和SAN存储在用户装置102处(例如,在CRM 112内)。用户装置102可以被配置成执行功能性以从主密钥导出一个或多个唯一导出密钥。在一些实施方案中,用户装置102可以使用主密钥和PAN的至少一部分来导出UDK。例如,可以使用主密钥和PAN的最左边的8个数字来导出UDK。在一些实施方案中,PAN的最左边的8个数

字可以与银行标识号(BIN)相关联。

[0067] 一旦被生成,就可以在任何合适的时间利用UDK来生成加密标识符和/或模糊标识符。在一些实施方案中,UDK可以对整个标识符(例如,PAN)以及诸如计数器、日期、时间和/或交易金额之类的动态值进行加密。作为示例,PAN可以与存储在用户装置102上并且使用UDK和加密算法加密的动态值(例如,交易计数器)级联。在一些实施方案中,可以标识并且使用加密标识符的一部分(例如,最右边的7个数字)以生成模糊标识符。在一些实施方案中,模糊标识符可以包括PAN的原始8个数字(与BIN相对应)、加密标识符的部分和校验和值(例如,与Luhn校验和相对应)。在仍然另外的实施方案中,模糊标识符可以包括PAN的原始8个数字(与BIN相对应)、任何合适数量的填充值(例如,7个零)以及校验和值。可以将模糊标识符和/或加密标识符存储在用户装置102处。

[0068] 在交易(例如,非中转交易)的初始化时,或者在另一合适的时间,用户装置102可以被配置成以数据轨道的形式提供模糊值和加密标识符。数据轨道可以格式化为轨道1或轨道2数据轨道。轨道1(“国际航空运输协会”)存储比轨道2多的信息,并且包含持卡人的姓名以及账号及其他自主数据。当用信用卡获得预订时,此磁道有时由航空公司使用。轨道2(“美国银行协会”(ABA))是目前最常用的。轨道2可由ATM和信用卡校验器读取。ABA设计了轨道2的规格,并且所有世界银行都必须遵守。其包含持卡人的账户、加密PIN以及其他自主数据。

[0069] 在一些实施方案中,模糊值可以在传统上包括用户账号(例如,标签57)的轨道2数据轨道的数据字段中提供。在一些实施方案中,可以在轨道2数据轨道的不同部分中(例如,在标签9F1F(任意数据标签)中、在标签9F7C(客户专用数据标签)中、在标签9F10(发行方应用数据)中、或者在轨道2数据的任何合适的部分中、或者在以上的任何合适的组合中)提供加密标识符。

[0070] 在其他实施方案中,在交易(例如,中转交易)的初始化时,或者在另一合适的时间,用户装置102可以被配置成以数据轨道的形式提供SAN和加密标识符。在一些实施方案中,可以在传统上包括用户的账号(例如,标签57)的轨道2数据轨道的数据字段中提供SAN。在一些实施方案中,可以在轨道2数据轨道的不同部分中(例如,在标签9F1F(任意数据标签)中、在标签9F7C(客户专用数据标签)中、在标签9F10(发行方应用数据)中、或者在轨道2数据的任何合适的部分中、或者在以上的任何合适的组合中)提供加密标识符。

[0071] 根据传统交易处理,访问装置118可以接收轨道2数据轨道并且将数据提供到资源提供商计算机104,然后资源提供商计算机可以通过授权请求消息将轨道2数据的至少一部分转发到传送计算机106。在一些实施方案中,访问装置118可以:生成授权请求消息;包括轨道2数据的至少一部分;并且将授权请求消息直接转发到传送计算机106。

[0072] 在接收后或在另一合适时间,传送计算机106可以将授权请求消息转发到中央服务器计算机108。中央服务器计算机108可以确定加密值存在于授权请求消息中。中央服务器计算机108可以检取存储的UDK和/或使用主导出密钥和模糊标识符的一部分(也包括在授权消息中)导出UDK。UDK可以由中央服务器计算机108使用以对加密值进行解密以获得整个未加密PAN。在一些实施方案中,中央服务器计算机108可以修改授权请求消息以包括未加密PAN,并且将修改的授权请求消息传输到授权实体计算机110以进行进一步处理。

[0073] 在其他实施方案中,中央服务器计算机108和/或授权实体计算机110可以利用模

糊标识符的至少一部分(例如,与BIN相对应的前8个数字)来将未更改的授权请求消息转发到授权实体计算机110。授权实体计算机110可以检取存储的UDK并且/或者利用主导出密钥和模糊标识符的一部分或SAN(也包括在授权消息中)来导出UDK。UDK可以由中央服务器计算机110利用来对加密标识符进行解密以获得整个未加密PAN。中央服务器计算机108和/或授权实体可以利用SAN来查阅指示已知PAN/SAN关联的映射以便检取关联的PAN。可以将关联的PAN与未加密PAN进行比较以证实授权请求消息。

[0074] 授权实体计算机110可以处理授权请求消息并将授权响应消息传输回中央服务器计算机108。在一些实施方案中,授权响应消息可以包括模糊标识符和加密值,并且不包括未加密标识符。

[0075] 中央服务器计算机108可以通过传送计算机106将授权响应消息转发回资源提供商计算机104。在资源提供商计算机104接收到授权响应消息之后,资源提供商计算机104处的访问装置118接着可以将授权响应消息提供给用户103。响应消息可以由访问装置118显示,或者可以打印在收据上。

[0076] 在一天结束时,常规的清算和结算过程可以由系统100进行。

[0077] 通过使用本文所述的技术,实现了用于传送敏感数据(例如,PAN)的更安全的方式。对于需要静态标识符(例如,以基于阻止列表确认或者拒绝访问)的交易,可以利用SAN来执行交易。通过利用SAN并且确保可以仅在特定类型的交易(例如,中转交易、票价交易等)中利用SAN,SAN被保护免受欺诈者的影响。即使欺诈者能够窃听以获得对SAN的访问,系统也将确保SAN仅可能被用于某些类型的交易而非其他交易。对于其他交易(例如,非中转交易),对PAN进行加密并且在非传统数据字段中提供它,并且通常会包括PAN的传统数据字段替代地包括不可能据此确定PAN的模糊值。模糊值仍然可以包括原始BIN,以确保用于授权请求/响应消息的传统路由技术保持不变。如果可能的话,本文所述的技术会使得从授权请求/响应消息中标识PAN变得困难。此外,在一些实施方案中,PAN是使用不断变化的动态值进行加密的。因此,加密值和模糊值可以针对每个授权请求而改变,如果可能的话会使得随着时间的推移难以跟踪特定用户的交易。因此,使用本文所论述的技术,提高了用于传输敏感数据的隐私保护和安全性。

[0078] 图2描绘根据一些实施方案的用于在用户装置(例如,图1的用户装置102)处生成和存储数据的方法200。方法200可以在202处开始,其中授权实体计算机(例如,授权实体计算机110)可以获得主导出密钥。在一些实施方案中,可以利用主导出密钥(MDK)来导出一个或多个唯一导出密钥。授权实体计算机110可以确保用于一个用户装置的MDK对该用户装置而言是唯一的。因此,授权实体计算机110可以管理可以对应于各种用户装置(例如,用户装置102)的许多主导出密钥。

[0079] 在204处,授权实体计算机110可以获得与要使用户装置个性化所针对的用户相对应的个人账号(PAN)。在至少一个实施方案中,PAN可以与用户的由授权实体代表用户管理的金融账户相关联。

[0080] 在206处,授权实体计算机110可以获得和/或生成辅账号(SAN)。如自始至终讨论的,SAN可以受到授权实体计算机110限制,使得可以仅在一种或多种特定类型的交易中利用SAN。作为示例,情况可以是在中转系统或票价检查系统等中,必须迅速地(例如,实时地或近实时地)对用户进行认证。给定系统的上下文,可能不能够足够迅速地执行用户的在线

认证以使得能够几乎实时地访问资源(例如,中转资源)。因此,一些认证系统在访问装置处执行离线认证并且稍后跟进授权请求消息以进行相关交易。可以生成这个SAN以在此类离线认证场景中利用。

[0081] 在208处,授权实体计算机110可以维护指示PAN与SAN之间的关系的账号映射。授权实体计算机110可以被配置成出于如关于图5更详细地讨论的证实目的而利用映射。

[0082] 在210处,授权实体计算机110可以将数据传输到用户装置102。作为示例,授权实体计算机110可以将MDK、PAN和SAN传输到用户装置102。在一些实施方案中,授权实体计算机110可以将数据传输到中间装置,该中间装置然后可以将数据转移到用户装置102。

[0083] 在212处,可以在用户装置102处将数据存储在CRM 112内。在214处,用户装置102可以使用MDK来生成一个或多个唯一导出密钥。作为示例,可以根据关于图3更详细地描述的过程来生成唯一导出密钥(UDK)。应该领会,可以生成一个或多个UDK并且可以出于特定目的利用每个UDK。例如,可以生成UDK以用于报文鉴别,可以生成另一UDK以用于加密,可以生成另一UDK以用于密码生成,并且可以根据图3的过程来生成另一UDK。应该领会,用户装置102可以生成任何合适数量的UDK,或者此类UDK可以替代地由授权实体计算机110在202处或者在任何合适的时间生成。

[0084] 在216处,可以由授权实体计算机110激活用户装置102。在激活时,可以在访问装置处或在线使用用户装置102以便执行各种交易。

[0085] 图3描绘根据一些实施方案的用于从驻留在用户装置(例如,智能卡)上的数据生成唯一导出密钥的方法。所述方法可以由图1的用户装置102使用用户装置102的一个或多个处理器来执行。

[0086] 在至少一个实施方案中,在执行个性化过程(例如,图2的方法200)期间将主导出密钥(MDK)302和标识符304存储在用户装置102处。在一些实施方案中,标识符304可以是个人账号的示例。可以从存在于用户装置102上的此类数据导出UDK 306。

[0087] 作为示例,用户装置102可以被配置成识别标识符308的一部分。在一些实施方案中,标识符308的所述部分可以包括少于整个标识符304。例如,标识符308的所述部分可以包括标识符304的最左边的8个数字。在一些实施方案中,标识符304的最左边的8个数字可以对应于可以被用于支付处理网络(例如,系统100)内的路由目的的银行标识号(BIN)。

[0088] 在一些实施方案中,标识符308的所述部分可以与许多填充比特(例如,填充310)级联以创建预定固定长度的字符串。在一些示例中,级联值的长度可以是128个比特,其中填充包括64个比特并且标识符308的所述部分包括另外64个比特(各自包括8个比特的8个数字),但是级联值不限于为此长度。可以提供级联值以及如输入到数据加密算法312中的MDK302。

[0089] 数据加密算法312可以包括任何合适的加密方法学。例如,数据加密算法312可以利用三重DES加密算法。在一些实施方案中,由通过数据加密算法312进行的加密产生的值是UDK 306。

[0090] 图4描绘根据一些实施方案的用于执行离线认证的方法400。该方法可以在402处开始,其中可以由访问装置118执行发现过程。例如,图1的读取器120可以轮询可能已进入读取器的RF场的非接触式卡的存在。

[0091] 在404处,访问装置118可以与用户装置102一起发起应用选择过程。应用选择过程

可以紧接在用户装置102的激活之后被执行并且是确定将使用由用户装置102和访问装置118(或读取器120)两者支持的应用中的哪一个应用来进行交易的过程。作为示例,访问装置118(例如,访问装置118的读取器120)可以构建相互支持的应用的候选列表。可以标识并且选择来自候选列表的单个应用以处理交易。

[0092] 在406处,可以发起应用处理。例如,访问装置118(或读取器120)可以向用户装置102用信号通知交易处理正在开始。在一些实施方案中,可以通过从访问装置118(读取器120)向用户装置102发送得到处理选项命令来用信号通知交易处理的开始。当发出此命令时,访问装置118可以提供任何合适的数据元素。在一些实施方案中,可以确定由用户装置102和访问装置118(读取器120)相互支持的非接触式路径并且选取一非接触式路径来处理交易。可以依照所选取的非接触式路径来执行后续交易处理。

[0093] 在408处,用户装置102可以将应用数据提供回给访问装置118(读取器120)。在一些实施方案中,用户装置102可以首先接收得到处理选项。响应于命令,用户装置102可以生成任何合适的应用数据。作为示例,可以修改(例如,递增、递减等)存储在用户装置102处的计数器。用户装置102可以利用计数器以及存储的PAN来生成还可以被存储在用户装置102处的加密PAN。如果得到处理选项命令指示访问装置118是特定终端类型(例如,非中转终端类型或存储在用户装置处的第一组终端类型中的终端类型等),则用户装置102可以从所存储的PAN的一部分和加密标识符的一部分生成模糊PAN。可以在此用例中将模糊PAN和加密标识符作为应用数据来提供。然而,如果得到处理选项命令指示访问装置118是另一特定终端类型(例如,中转终端类型或存储在用户装置处的第二组终端类型中的终端类型等),则用户装置102可以将所存储的SAN和加密标识符作为应用数据来提供。

[0094] 在410处,当访问装置118(读取器120)已读取了处理交易所必需的应用数据时,可以认为应用数据的读取完成。在读取时间期间,访问装置118可以确定用于交易的所有强制性数据元素是否由卡返回了。如果没有返回所有强制性数据元素或者如果返回了冗余数据(例如,返回了数据元素的不止一个具体值),则访问装置118(读取器120)可以终止交易。

[0095] 在412处,访问装置118(读取器120)可以处理限制。作为示例,访问装置118(读取器120)可以检查应用期满日期、应用使用,并且/或者可以检查SAN是否在终止异常文件(TEF)上。可以将TEF认为是其中存储有不允许访问资源的SAN的黑名单。如果SAN出现在终止异常文件中,则访问装置118(读取器120)可以被配置成拒绝用户装置102访问(例如,由访问装置118管理的旋转门)并且不再进行进一步处理。

[0096] 然而,如果在TEF中不包括SAN,则方法400可以进行到414,其中可以执行离线数据认证。可以针对访问装置(读取器)支持的离线交易实现离线数据认证,并且可以针对用户装置请求的离线交易执行离线数据认证。在离线数据认证期间,访问装置118(读取器120)可以验证由用户装置102返回的动态签名并且可以对来自用户装置102的数据进行认证。

[0097] 在一些实施方案中,访问装置118(读取器120)可以支持在线交易。在这些实施方案中,访问装置118(读取器120)可以在416处向授权实体计算机110发送授权请求消息(例如,经由图1的传送计算机106和/或中央服务器计算机108)。授权请求消息可以包括存储在用户装置102处的SAN和加密标识符。

[0098] 在418处或者在任何合适的时间接收到授权请求消息时,授权实体计算机110使用预定基于主机的风险管理参数来审查和授权或者拒绝交易。在一些实施方案中,授权实体

计算机110可以被配置成确定交易包括SAN。在一些实施方案中,可以检取授权请求消息的账户标识符字段的值并且将其与包括被映射到对应PAN的所有已知SAN的映射进行比较。如果账户标识符字段的值等于已知SAN,则可以确定交易正在利用SAN。在一些实施方案中,授权实体计算机110可以被配置成允许仅在发起交易的访问装置(例如,访问装置118)具有特定类型或者与访问装置相关联的商家是特定商家类型、或者授权请求消息的交易类型指示允许的交易类型的交易中利用SAN。作为非限制性示例,授权实体计算机110可以被配置成在涉及与非中转终端类型相关联的访问装置(例如,由非中转商家操作的访问装置)的交易中拒绝利用SAN的在线处理,同时对于涉及与中转终端类型相关联的访问装置(例如,由中转商家操作的访问装置120)的交易允许利用SAN的在线处理。

[0099] 在一些实施方案中,包括在授权请求消息中的SAN可以与和加密标识符相对应的PAN相关联。授权实体计算机110可以被配置成检取SAN的与银行标识号(BIN)相对应的最左边的8个数字。授权实体计算机110可以利用与如存储在由授权实体计算机110维护的映射中的SAN相关联的BIN和PAN来导出UDK。使用所导出的UDK,授权实体计算机110可以对授权消息的加密标识符进行解密以确定解密PAN。可以将解密PAN与存储在映射中并且与消息的SAN相关联的PAN进行比较。如果解密PAN与所存储的PAN匹配,则消息可以被认为是有效的,否则是无效的。授权实体计算机110还可以执行传统在线欺诈和信用检查,利用卡生成的密码来执行在线卡认证等。

[0100] 图5示出根据一些实施方案的用于安全地传送敏感数据的方法500的流程图。方法500可以由计算装置(例如,图1的用户装置102、智能卡)执行。计算装置可以包括一个或多个处理器和一个或多个存储计算机可执行指令的存储器,其中由一个或多个处理器执行计算机可执行指令,使得计算装置执行方法500。图5所示和下面描述的步骤可以与图1中的交易处理的描述及其对应描述结合使用。那些描述以引用的方式并入本文中。计算装置可以将一个或多个UDK、第一标识符(例如,辅账号(SAN))、第二标识符(例如,主账号(PAN))、动态值或任何合适的数据存储在计算装置的存储器内。

[0101] 加密标识符可以(例如,由计算装置)以任何合适的类型(例如,在如以上关于图4所讨论的那样从访问装置接收到得到处理选项命令之后)生成。计算装置可以通过使用唯一导出密钥(例如,UDK 206)对第二标识符(例如,PAN)和动态值(例如,计数器、日期、时间等)进行加密来生成加密标识符。在一些实施方案中,第二标识符和动态值可以在被加密之前被级联在一起和/或与附加填充值级联。在一些实施方案中,可以将加密标识符存储在计算装置处(例如,作为诸如标签9F7C(客户专用数据标签)和/或标签9F10(发行方应用数据)之类的轨道1和/或轨道2数据的一部分)处、在标签9F1F(任意数据标签)中、或者在轨道1和/或轨道2数据的任何部分中、或者在以上的任何合适的组合中。附加地,或替代地,可以将加密标识符作为可能在上述标签中的任一个中可获得的被保留以供将来使用的数据字段的一部分或轨道1和/或轨道2数据的另一合适的部分来提供。

[0102] 方法500可以在框502处开始,其中可以由计算装置(例如,智能卡)从访问装置(例如,旋转门)接收请求消息。在一些实施方案中,请求消息可以对应于如以上在图4中描述的得到处理选项命令。访问装置可以是被配置成从用户装置请求数据的任何合适的装置。

[0103] 在504处,计算装置可以至少部分地基于请求消息确定用于请求访问装置的类型指示符。作为示例,请求消息可以包括指示请求由特定类型的终端/访问装置发起的类型指

示符。作为非限制性示例,请求消息可以指示请求装置是诸如地铁系统之类的中转系统内的旋转门。计算装置可以确定类型指示符是否属于第一类型集合(例如,包括中转类型的第一类型集合)。

[0104] 在506处,如果类型指示符被确定为被包括在第一类型集合中或者确定了请求消息由特定类型的终端/访问装置发起,则计算装置可以发送第二消息(例如,到访问装置),所述第二消息包括至少第一标识符(例如,SAN)和从PAN生成/导出的加密标识符。根据一些实施方案,可以将消息提供给访问装置,所述访问装置使计算装置的用户被允许或者拒绝访问资源。作为非限制性示例,诸如中转站中的旋转门之类的访问装置可以基于第一标识符(例如,SAN)允许或者拒绝用户的访问。如以上关于图4所描述的,在一些实施方案中,访问装置(或关联的资源提供者计算机)可以随后生成授权请求消息。授权请求消息可以尤其包括含有第一标识符(SAN)的第一数据字段和含有加密标识符的第二数据字段。在一些实施方案中,授权请求消息被传输到中央服务器计算机(例如,图1的中央服务器计算机108)以进行进一步的授权处理。

[0105] 在508处,如果类型指示符被确定为未被包括在第一类型集合中或者被确定为不是终端/访问装置的特定类型,则可以(例如,由用户装置102)生成模糊标识符。在一些实施方案中,模糊标识符可以包括第二标识符(PAN)的前8个数字、7个零以及Luhn校验和值。在其他实施方案中,可以至少部分地基于第二标识符(例如,PAN)的一部分和加密标识符的一部分来生成模糊标识符。作为示例,模糊标识符可以被生成以包括标识符的前8个数字和加密标识符的后7个数字(或任何合适数目的零)。这仅仅是一个示例,可以使用标识符的更多或更少的数字和加密标识符的更多或更少的数字。类似地,模糊标识符可以包括16个数字或任何合适数目的数字。在一些实施方案中,Luhn校验和值可以根据模糊标识符计算,并且将Luhn校验和值包括为模糊标识符的一部分(例如,正在进行的示例中的最后一个数字,即数字16)。

[0106] 在510处,可以(例如,由用户装置102)提供第二消息(例如,轨道2消息)。在一些实施方案中,消息可以包括至少模糊标识符和加密标识符。根据一些实施方案,可以将消息提供给访问装置(例如,访问装置118),所述访问装置使得授权请求消息被生成(例如,由图1的访问装置118和/或资源提供者计算机104生成)。授权请求消息可以尤其包括含有模糊标识符的第一数据字段和含有加密标识符的第二数据字段。在一些实施方案中,授权请求消息被传输到中央服务器计算机(例如,图1的中央服务器计算机108)以进行进一步的授权处理。

[0107] 图6描绘用于在一些实施方案中使用的示例性记录格式600。例如,记录格式600可以包括含有SAN和加密标识符的轨道2数据(例如,认证数据)。记录格式600可以是关于图5的506描述的第二消息的示例。在一个非限制性示例中,PAN 601可以与用户相关联并且被存储在用户的装置(例如,智能卡)上。在一些实施方案中,SAN 602可以与用户相关联并且被存储在用户的装置上。如图6所图示的,PAN 601和SAN 602可以各自包括16个数字。在一些实施方案中,PAN 601被存储在如由轨道2数据所定义的轨道2数据的标签57处。在一些实施方案中,SAN 602被存储在如由轨道2数据所定义的轨道2数据的标签5A处。

[0108] 可以传统上为SAN 602保留记录格式600的前16个数字(例如,标识符数据字段603)(例如,数字1-16)。接下来,分隔符数据字段604在账户标识符与期满日期数据字段606

之间提供缓冲区。服务代码数据字段608可以接着期满日期数据字段606。个人标识号验证指示符(PVKI)数据字段610和PIN验证信息数据字段614接着。接下来,包括dCVV数据字段614、交易计数器数据字段616和非接触式指示符数据字段618。最后,任意数据字段620接着。任意数据字段可以包括加密值数据字段621和密码版本号数据字段623。加密值数据字段621和密码版本号数据字段623可以包括任何合适数量的数字,而不必是图6中描绘的数字。

[0109] 根据一些实施方案,可以首先利用PAN 601来生成加密值(例如,加密标识符)。作为示例,图1的用户装置102可以被配置成从存储中检取图3的PAN 601和UDK 306。在一些实施方案中,还可以检取交易计数器(或其他动态值)。可以与如输入到加密算法中的UDK 306一起利用PAN和交易计数器(或其他动态值)来生成加密值。在一些实施方案中,可以在输入之前串联PAN和交易计数器(或其他动态值)。可以按记录格式600存储所得的加密值。作为示例,所得的加密值可以如所描绘的那样被存储在任意数据字段620的加密值数据字段621内。在一些实施方案中,任意数据字段620对应于由轨道2标准定义的特定标签(例如,在标签9F1F(任意数据标签)、标签9F7C(客户专用数据标签)中、在标签9F10(发行方应用数据)中、在轨道2数据的任何合适的部分中、或者在以上的任何合适的组合中)。

[0110] 在一些实施方案中,密码版本号数据字段623可以将指示任意数据字段620包括加密值的数字存储在加密值数据字段621内。

[0111] 根据一些实施方案,用户装置102可以被配置成在标识符数据字段603中提供SAN 602。标识符数据字段603的数字16可以包括校验和值(例如,Luhn校验和/值),可以利用所述校验和值(例如,在接收时)以用于验证标识符数据字段603尚未被更改。在一些实施方案中,当用户装置102已确定轨道2数据的请求者与特定终端类型(例如,中转终端类型、与离线认证相关联的终端类型等)相关联时,可以在标识符数据字段603内提供SAN 602。

[0112] 一旦已发起了交易,就可以提供包含在标识符数据字段603内的SAN602以及在任意数据字段620内(例如,在加密值数据字段621处)的加密值(例如,给如上所述的访问装置)。在一些实施方案中,能够递增(或递减)交易计数器并且/或者可以生成新动态值并且将其存储在交易计数器数据字段716中。如果由用户装置102发起另一交易,则可以利用新交易计数器/动态值和PAN 701来重复本文讨论的过程以生成然后可以在后续交易中提供的新加密值和新模糊标识符。

[0113] 图7描绘用于在一些实施方案中使用的另一示例性记录格式700。例如,记录格式700可以包括含有模糊标识符和加密标识符的轨道2数据(例如,支付数据)。记录格式600可以是关于图5的510描述的第二消息的示例。在一个非限制性示例中,PAN 701可以与用户相关联并且被存储在用户的装置(例如,智能卡)上。在一些实施方案中,SAN 702还可以与用户相关联并且被存储在用户的装置上。如图7所图示的,PAN 701和SAN 702可以各自包括16个数字。在一些实施方案中,PAN 701被存储在如由轨道2数据所定义的轨道2数据的标签57处。在一些实施方案中,可以将SAN702存储在如由轨道2数据所定义的轨道2数据的标签5A处。

[0114] 可以为账户标识符的模糊版本(例如,模糊PAN 703、PAN 701的模糊版本)保留记录格式700的前16个数字(例如,标识符数据字段703)(例如,数字1-16)。接下来,分隔符数据字段704在账户标识符与期满日期数据字段706之间提供缓冲区。服务代码数据字段708

可以接着期满日期数据字段706。个人标识号验证指示符(PVKI)数据字段710和PIN验证信息数据字段712接着。接下来,可以包括dCVV数据字段714、交易计数器数据字段716和非接触式指示符数据字段718。最后,任意数据字段720可以接着。任意数据字段可以包括加密值数据字段721和密码版本号数据字段723。加密值数据字段721和密码版本号数据字段723可以包括任何合适数量的数字,而不必是图7中描绘的数字。

[0115] 根据一些实施方案,可以首先利用PAN 701来生成加密值(例如,加密标识符)。作为示例,图1的用户装置102可以被配置成从存储中检取图3的PAN 701和UDK 306。在一些实施方案中,还可以检取交易计数器(或其他动态值)。可以与如输入到加密算法中的UDK 306一起利用PAN701和交易计数器(或其他动态值)来生成加密值。在一些实施方案中,可以在输入之前级联PAN 701和交易计数器(或其他动态值)。可以按记录格式700存储所得的加密值。作为示例,所得的加密值可以如所描绘的那样被存储在任意数据字段720的加密值数据字段721内。在一些实施方案中,任意数据字段720对应于由轨道2标准定义的特定标签(例如,在标签9F1F(任意数据标签)、标签9F7C(客户专用数据标签)中、在标签9F10(发行方应用数据)中、在轨道2数据的任何合适的部分中、或者在以上的任何合适的组合中)。

[0116] 在一些实施方案中,密码版本号数据字段723可以将指示任意数据字段720包括加密值的数字存储在加密值数据字段721内。

[0117] 根据一些实施方案,用户装置102可以被配置成生成模糊PAN 703。作为示例,用户装置102可以获得PAN 701的前8个数字并且将此信息存储在标识符数据字段703的数字1-8中。在一些实施方案中,标识符数据字段703的数字9-15可以包括诸如零之类的填充值。替代地,用户装置102可以被配置成获得加密值的某个部分并且将该部分存储在记录格式700内。例如,可以获得加密值的最后7个数字并且将其存储为标识符数据字段703的数字9-15。标识符数据字段703的数字16可以包括校验和值(例如,Luhn校验和/值),可以利用所述校验和值(例如,在接收时)以用于验证标识符数据字段703尚未被更改。

[0118] 一旦已发起了交易,就可以提供模糊PAN 703和在任意数据字段720内(例如,在加密值数据字段721处)的加密值(例如,给如上所述的访问装置)。能够递增(或递减)交易计数器并且/或者可以生成新动态值并且将其存储在交易计数器数据字段716中。如果由用户装置102发起另一交易,则可以利用新交易计数器/动态值和PAN 701来重复本文讨论的过程以生成然后可以在后续交易中提供的新加密值和新模糊标识符。

[0119] 图8示出根据一些实施方案的用于执行数据验证的方法的流程图。方法800可以由计算装置(例如,图1的中央服务器计算机108和/或授权实体计算机110)执行。计算装置可以包括一个或多个处理器和一个或多个存储计算机可执行指令的存储器,其中由一个或多个处理器执行计算机可执行指令,使得计算装置执行方法800。

[0120] 方法800可以在框802处开始,其中可以接收消息(例如,授权请求消息)。在一些实施方案中,消息可以包括第一标识符(例如,SAN)和加密标识符。图8所示和下面描述的步骤可以与图1中的交易处理的描述及其对应描述结合使用。那些描述以引用的方式并入本文中。

[0121] 在框804处,计算装置可以验证与发起了授权请求消息的请求装置相关联的类型。在一些实施方案中,计算装置可以将包含在授权请求消息中的值(例如,商家名称、地址、类型指示符、终端类型等)与存储在计算装置处或者可被计算装置访问的数据(例如,允许利

用SAN的值)进行比较。如果包含在授权请求消息中的值被包含在所存储的数据中,则计算装置可以允许进一步处理授权请求消息。如果值未被包含在授权请求消息中,则计算装置可以拒绝授权请求消息并且向指示该授权请求消息的请求者传输授权响应消息。

[0122] 在806处,可以利用第一标识符(例如,SAN)来获得预期标识符(例如,主PAN)。在一些实施方案中,计算装置可以查阅指示PAN与SAN之间的已知关联的映射。

[0123] 在808处,计算装置可以利用加密标识符和唯一导出密钥来生成解密标识符。在一些实施方案中,计算装置可以从第一标识符(例如,SAN)的一部分导出唯一导出密钥(UDK)。在一些实施方案中,可以预先从存储装置导出和检取UDK。作为示例,计算装置可以检取第一标识符的最左边的8个数字,并且使用那些数字作为预定加密算法的输入以生成UDK。最左边的8个数字可以对应于银行标识号(BIN)。一旦UDK生成,则可以使用它来对加密标识符进行解密。

[0124] 在810处,计算装置可以被配置成验证解密标识符与预期标识符510匹配。也就是说,解密标识符对应于与如在由计算装置维护的映射内所定义的第一标识符(例如,SAN)相关联的主PAN。

[0125] 在812处,可以由计算装置利用解密标识符来处理消息。作为示例,计算装置可以是中央服务器计算机(例如,图1的中央服务器计算机108)。在这种情况下,处理消息(例如,授权请求消息)可以包括修改消息以包括解密标识符,并且将消息传输到授权实体计算机(例如,授权实体计算机110)以进行进一步处理。在一些实施方案中,计算装置可以是授权实体计算机110。在这种情况下,处理消息可以包括使用包括解密标识符的消息数据来授权交易。处理还可以包括生成指示交易被批准或拒绝的授权响应消息。授权响应消息可以包括加密标识符,并且根据结合图1的上述处理,例如将授权响应消息传输到中央服务器计算机108。

[0126] 图9示出根据一些实施方案的用于执行数据验证的方法的流程图。方法900可以由计算装置(例如,图1的中央服务器计算机108和/或授权实体计算机110)执行。计算装置可以包括一个或多个处理器和一个或多个存储计算机可执行指令的存储器,其中由一个或多个处理器执行计算机可执行指令,使得计算装置执行方法900。

[0127] 方法900可以在框902处开始,其中可以接收消息(例如,授权请求消息)。在一些实施方案中,消息可以包括模糊标识符和加密标识符。图9所示和下面描述的步骤可以与图1中的交易处理的描述及其对应描述结合使用。那些描述以引用的方式并入本文中。

[0128] 在框904处,计算装置可以标识消息包括加密标识符。在一些实施方案中,标识消息包括加密标识符可以包括检查特定数据字段(例如,图3的任意数据字段320)是否有非零值。如果数据字段包含非零值,则计算装置可以推断出加密值存在于消息中。在一些实施方案中,标识消息包括加密标识符可以包括检查特定数据字段(例如,图3的密码版本号数据字段323)是否有非零值(或特定值)。

[0129] 在框906处,计算装置可以利用加密标识符和唯一导出密钥来生成解密标识符。在一些实施方案中,计算装置可以从模糊标识符的一部分导出唯一导出密钥(UDK)。在一些实施方案中,可以预先从存储装置导出和检取UDK。作为示例,计算装置可以检取模糊标识符的最左边的8个数字,并且使用那些数字作为预定加密算法的输入以生成UDK。一旦UDK生成,则可以使用它来对加密标识符进行解密。

[0130] 在框908处,可以由计算装置利用解密标识符来处理消息。作为示例,计算装置可以是中央服务器计算机(例如,图1的中央服务器计算机108)。在这种情况下,处理消息(例如,授权请求消息)可以包括修改消息以包括解密标识符,并且将消息传输到授权实体计算机(例如,授权实体计算机110)以进行进一步处理。在一些实施方案中,计算装置可以是授权实体计算机110。在这种情况下,处理消息可以包括使用包括解密标识符的消息数据来授权交易。处理还可以包括生成指示交易被批准或拒绝的授权响应消息。授权响应消息可以包括加密标识符,并且根据结合图1的上述处理,例如将授权响应消息传输到中央服务器计算机108。

[0131] 技术改进

[0132] 通过使用本文所述的技术,实现了用于传送敏感数据(例如,PAN)的更安全的方式。不仅PAN被加密并且提供在非传统数据字段中,而且通常包括PAN的传统数据字段反而包括不太可能从中确定PAN的模糊值。模糊值仍然可以包括原始BIN,以确保用于授权请求/响应消息的传统路由技术保持不变。如果可能的话,本文所述的技术会使得从授权请求/响应消息中标识PAN变得困难。此外,在一些实施方案中,PAN是使用不断变化的动态值进行加密的。因此,加密值可以针对每个授权请求而改变,如果可能的话会使得随着时间的推移难以跟踪特定用户的交易。因此,这些方法通过确保不能从授权请求/响应消息中标识特定用户和/或账户来提供关于个人数据隐私的改进。

[0133] 本文所述的任何计算装置可以是计算机系统的示例,所述计算机系统可用于实现上述任何实体或组件。此类计算机系统的子系统可以通过系统总线互连。额外子系统包括打印机、键盘、存储装置和监视器,所述监视器耦合到显示器适配器。外围设备和输入/输出(I/O)装置耦合到I/O控制器,并且可以通过本领域已知的许多手段中的任何一种(例如串行端口)连接到计算机系统。例如,I/O端口或外部接口可以用于将计算机设备连接到广域网(例如,因特网)、鼠标输入装置或扫描器。通过系统总线的互连可以允许中央处理器与每个子系统通信,并且控制来自系统存储器或存储装置的指令的执行,以及在子系统之间的信息交换。系统存储器和/或存储装置可以体现计算机可读介质。

[0134] 如所描述,本发明的服务可涉及实施一个或多个功能、过程、操作或方法步骤。在一些实施方案中,所述功能、过程、操作或方法步骤可以实施为由适当地被编程的计算装置、微处理器、数据处理器等执行指令集或软件代码的结果。指令集或软件代码可以存储在由计算装置、微处理器等存取的存储器或其他形式的数据存储元件中。在其他实施方案中,功能、过程、操作或方法步骤可以由固件或专用处理器、集成电路等实施。

[0135] 本申请中描述的任何软件组件或功能可以使用例如常规的或面向对象的技术并且使用任何合适的计算机语言(例如,Java、C++或Perl)实施为由处理器执行的软件代码。软件代码可以存储为例如随机存取存储器(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CD-ROM的光学介质的计算机可读介质上的一系列指令或命令。任何此类计算机可读介质可以驻存在单个计算设备上或单个计算设备内,并且可存在于系统或网络内的不同计算设备上或不同计算设备内。

[0136] 以上描述是说明性的而不是限制性的。在所属领域的技术人员阅读了本公开后,本发明的许多变化将变得显而易见。因此,本发明的范围不应参考以上描述来确定,而是应参考未决的权利要求以及其完整范围或等效物来确定。

[0137] 在不偏离本发明的范围的情况下,任何实施方案的一个或多个特征可以与任何其他实施方案的一个或多个特征组合。

[0138] 除非明确指示有相反的意思,否则“一(a)”、“一个(an)”或“所述”的叙述旨在指示“一个或多个”。

[0139] 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。

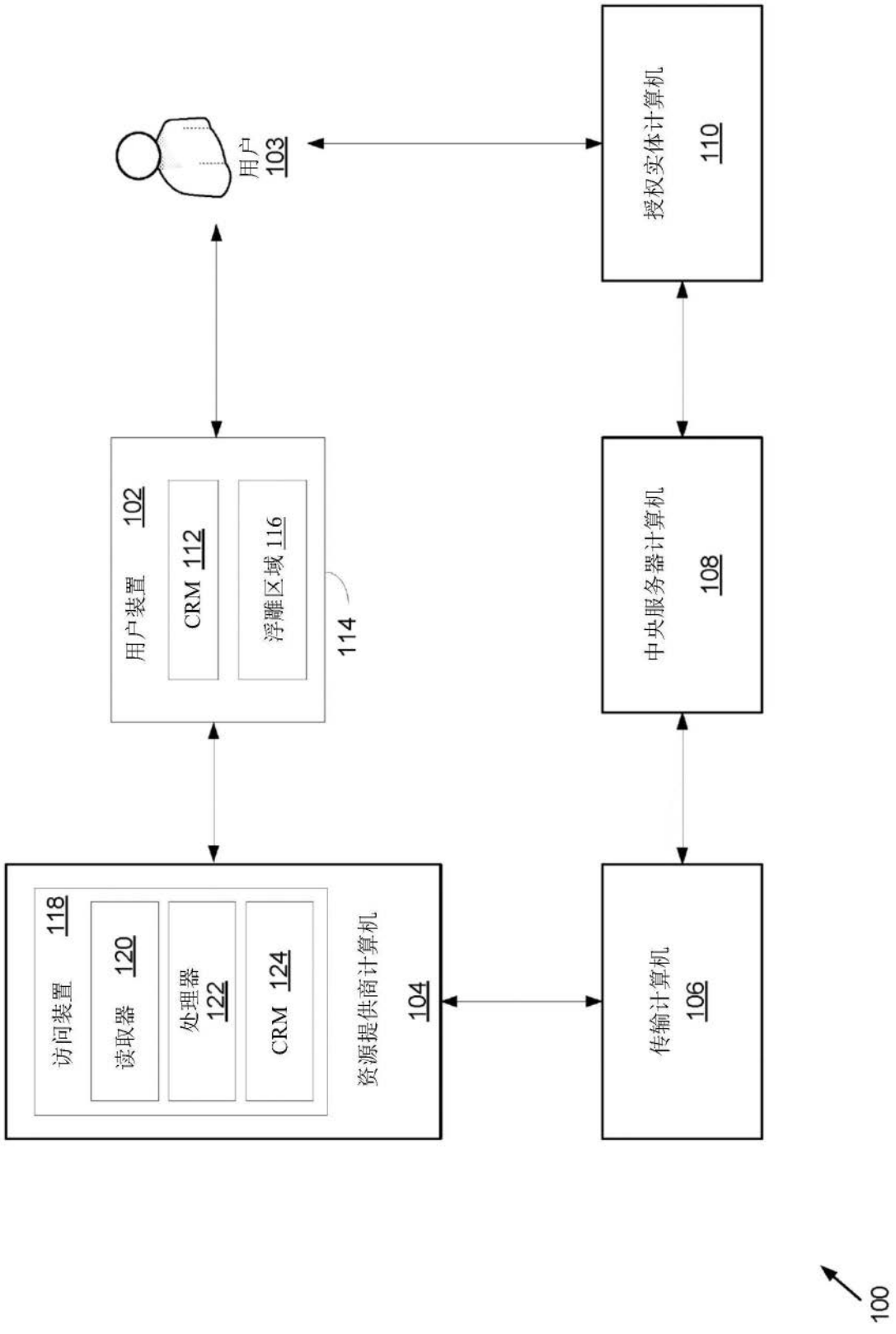

用户
103
授权实体计算机
110
用户装置
102
CRM 112
浮雕区域 116
114
中央服务器计算机
108
访问装置
118
读取器
120
处理器
122
CRM 124
资源提供商计算机
104
传输计算机
106
100

图1

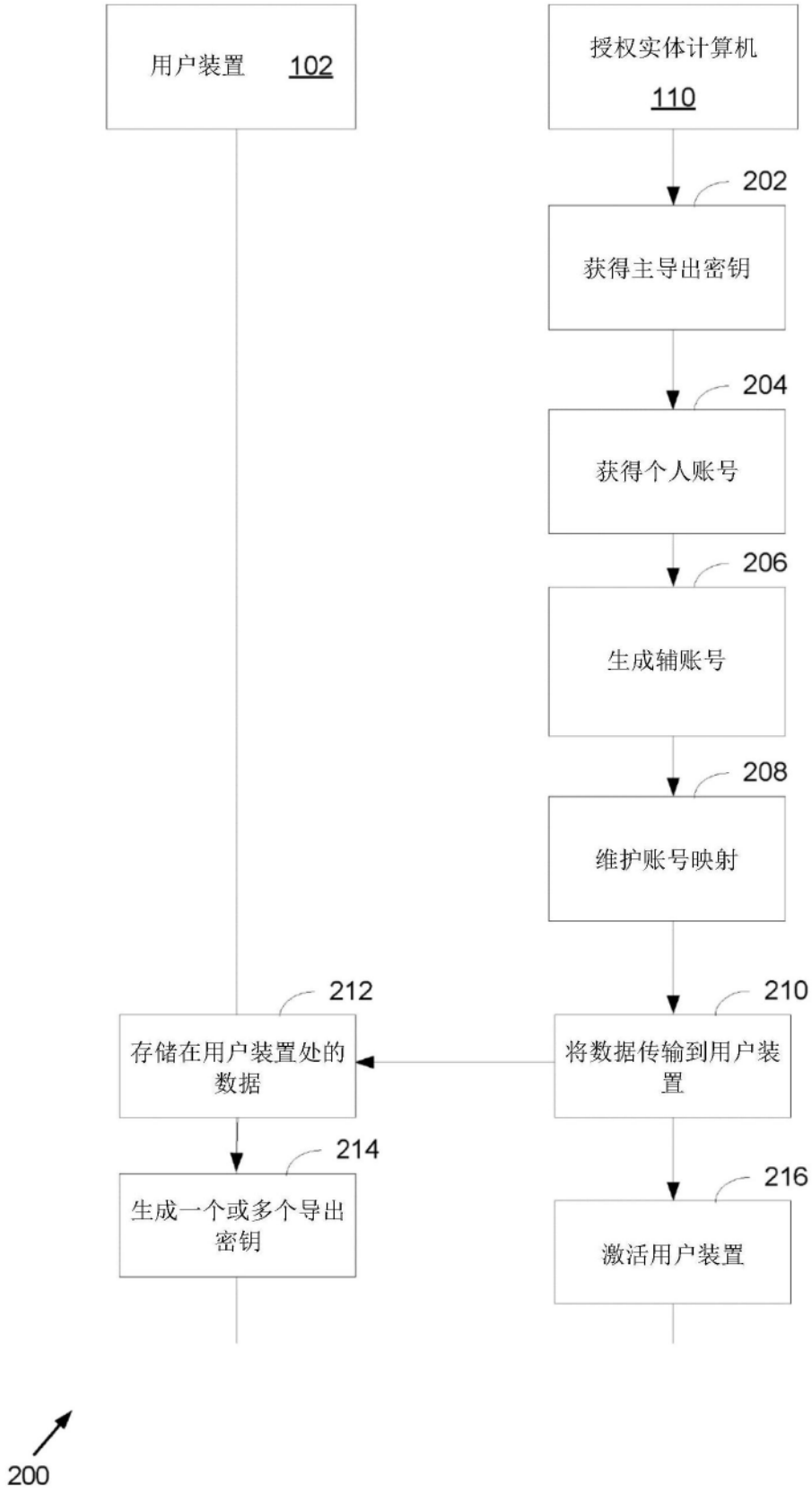

用户装置 102
授权实体计算机 110
202
获得主导出密钥
204
获得个人账号
206
生成辅账号
208
维护账号映射
210
将数据传输到用户装置
212
存储在用户装置处的数据
214
生成一个或多个导出密钥
216
激活用户装置
200

图2

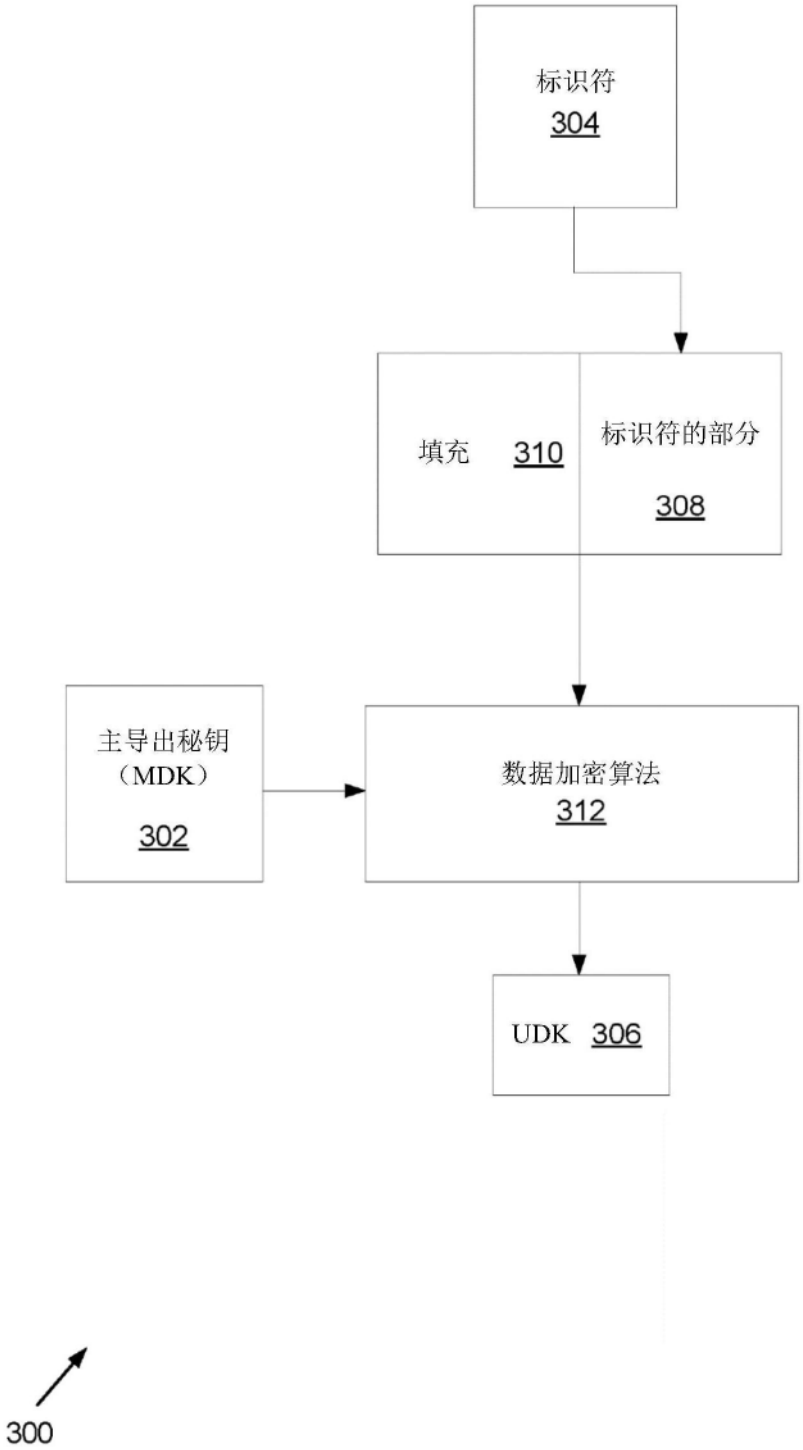


图3

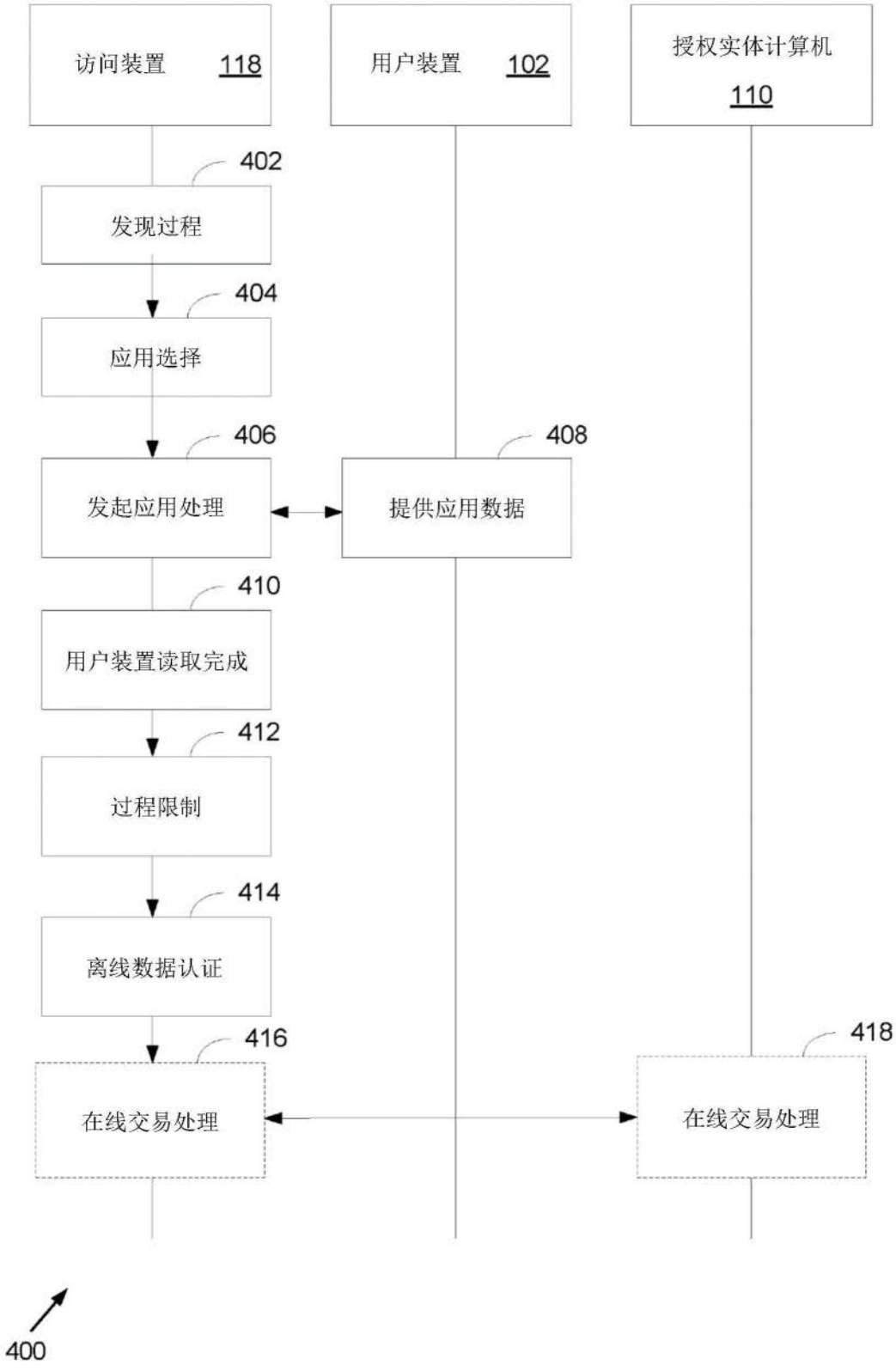

访问装置 118
用户装置 102
授权实体计算机 110
402
发现过程
404
应用选择
406
发起应用处理
408
提供应用数据
410
用户装置读取完成
412
过程限制
414
离线数据认证
416
在线交易处理
418
在线交易处理
400

图4

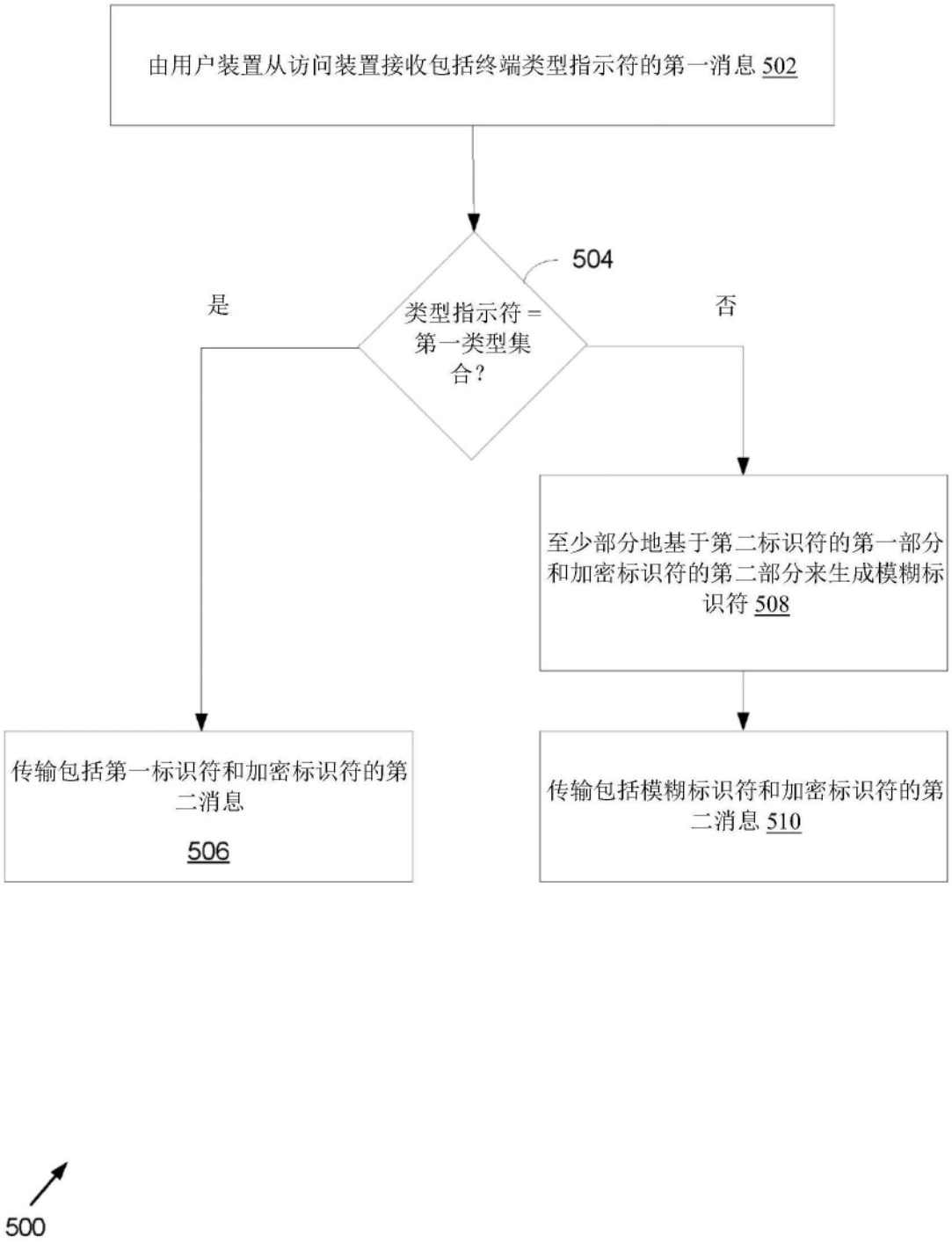

由用户装置从访问装置接收包括终端类型指示符的第一消息 502
504
类型指示符 = 第一类型集合?
是
否
至少部分地基于第二标识符的第一部分和加密标识符的第二部分来生成模糊标识符 508
传输包括第一标识符和加密标识符的第二消息
506
传输包括模糊标识符和加密标识符的第二消息 510
500

图5

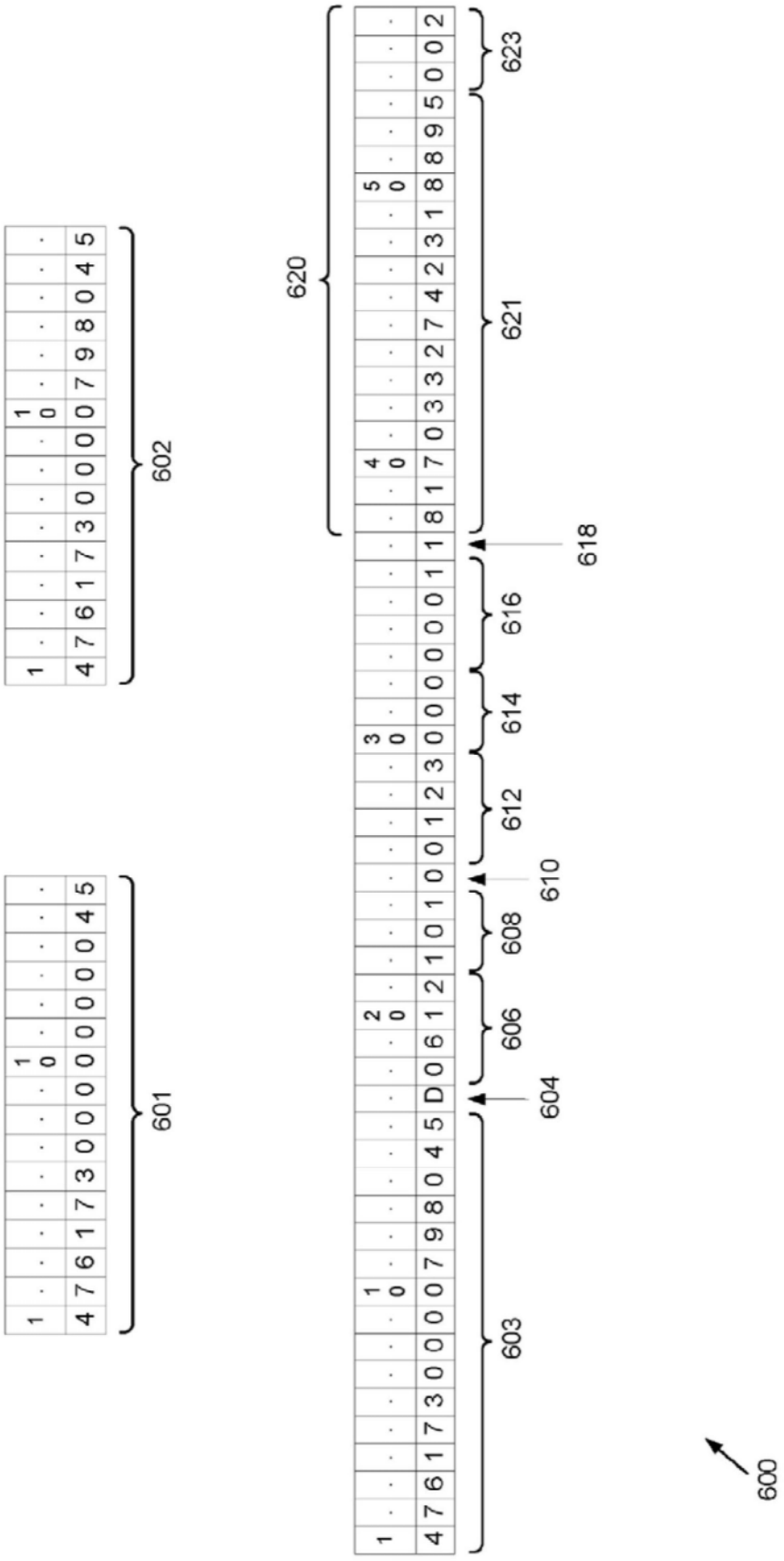


图6

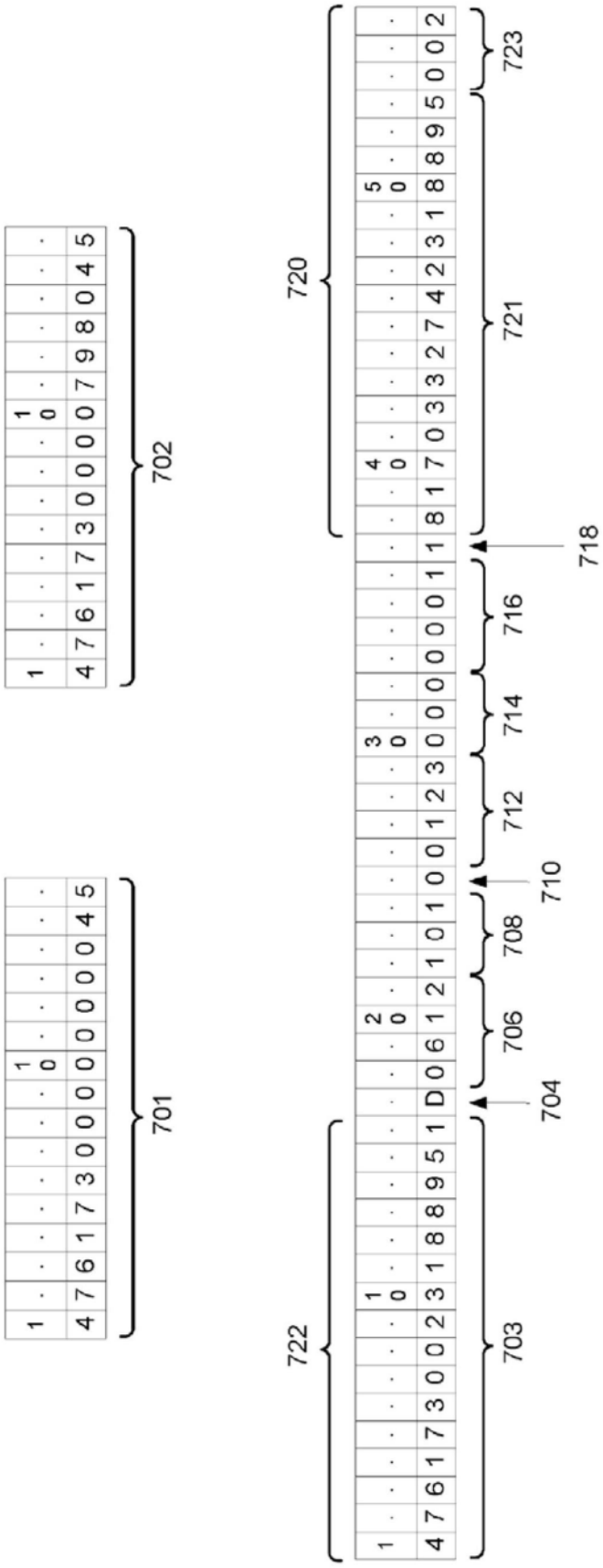


图7

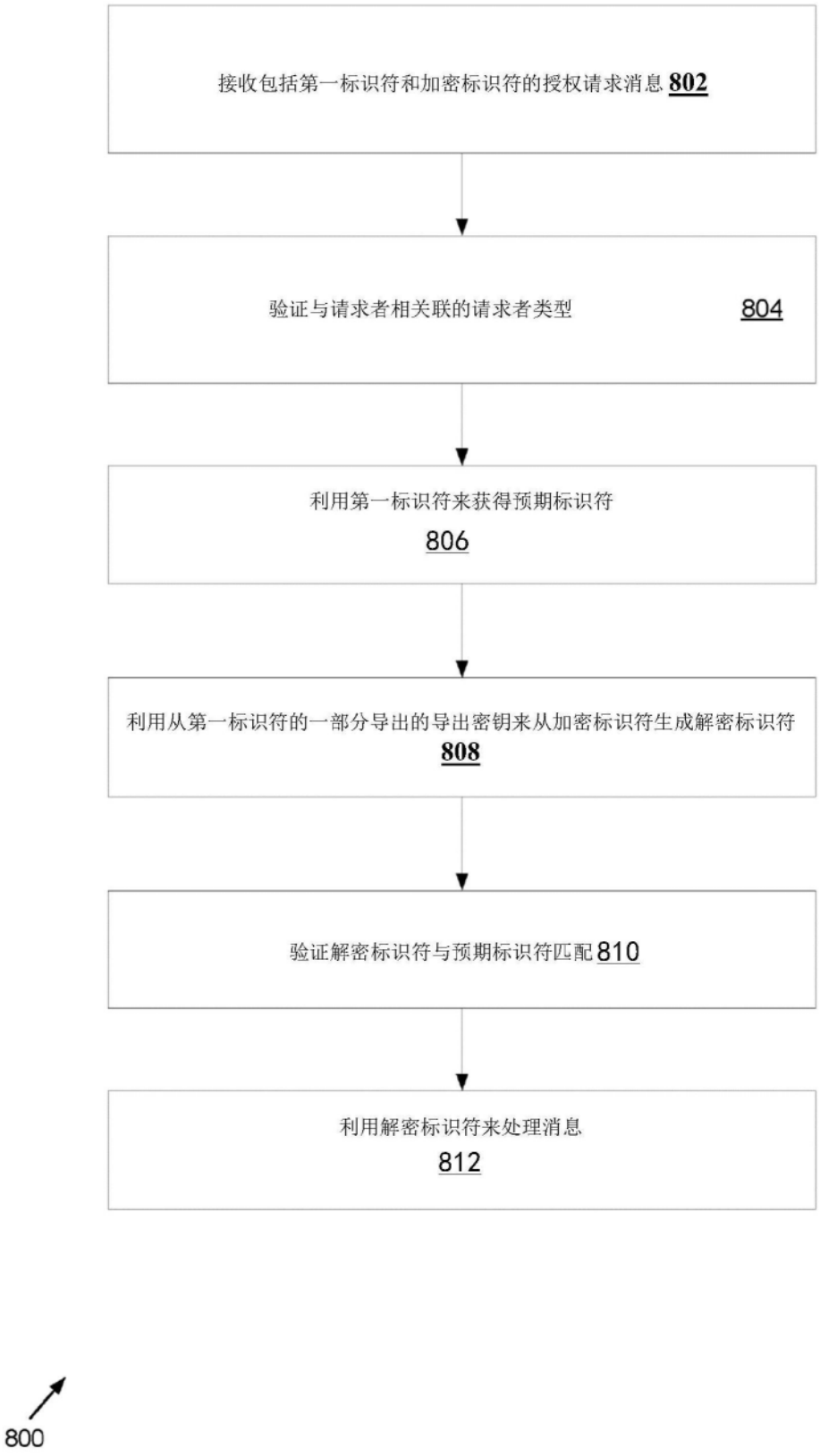

接收包括第一标识符和加密标识符的授权请求消息 802
验证与请求者相关联的请求者类型 804
利用第一标识符来获得预期标识符 806
利用从第一标识符的一部分导出的导出密钥来从加密标识符生成解密标识符 808
验证解密标识符与预期标识符匹配 810
利用解密标识符来处理消息 812
800

图8

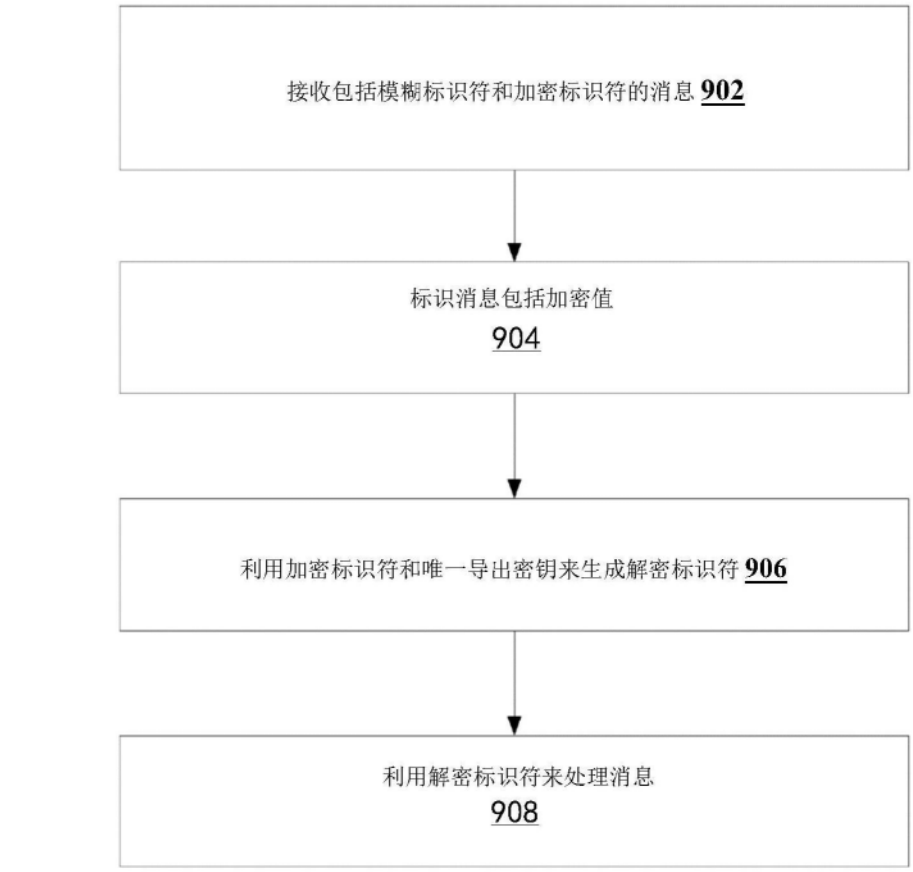

接收包括模糊标识符和加密标识符的消息 902
标识消息包括加密值
904
利用加密标识符和唯一导出密钥来生成解密标识符 906
利用解密标识符来处理消息
908
900

图9