



(12)发明专利

(10)授权公告号 CN 103270782 B

(45)授权公告日 2016.10.12

(21)申请号 201180061627.2

(73)专利权人 摩兹杜柯飞乐-韩国有限公司

(22)申请日 2011.12.20

地址 韩国京畿道城南市

(65)同一申请的已公布的文献号

(72)发明人 郑企道 洪亨准 金炫辰

申请公布号 CN 103270782 A

(74)专利代理机构 北京铭硕知识产权代理有限公司 11286

(43)申请公布日 2013.08.28

代理人 韩明星 金玉兰

(30)优先权数据

(51)Int.Cl.

61/428,852 2010.12.30 US

H04W 12/04(2009.01)

13/310,063 2011.12.02 US

H04W 12/06(2009.01)

(85)PCT国际申请进入国家阶段日

(56)对比文件

2013.06.20

WO 2009125141 A3, 2010.01.21,
CN 101822025 A, 2010.09.01,
CN 101379757 A, 2009.03.04,

(86)PCT国际申请的申请数据

审查员 孙珍珍

PCT/KR2011/009867 2011.12.20

权利要求书2页 说明书8页 附图5页

(87)PCT国际申请的公布数据

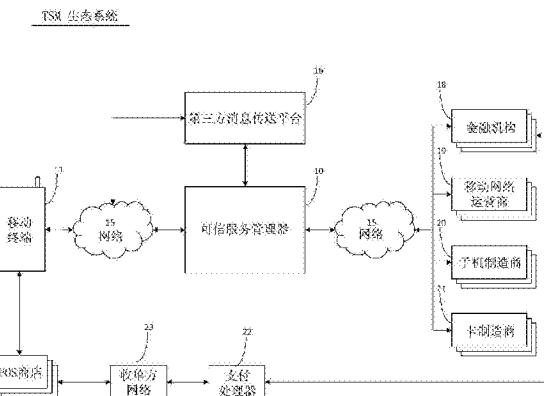
W02012/091350 EN 2012.07.05

(54)发明名称

针对存储在移动通信终端中的敏感财务信息的安全容器的系统和方法

(57)摘要

一种用于保护移动终端的非通用集成电路卡(UICC)类型安全元件(SE)中的信息空中下载(OTA)的方法,所述方法包括:接收用于初始化移动终端的OTA代理的请求;初始化OTA代理;接收用于保护信息的请求;使用OTA代理保护非UICC类型SE中的请求的信息。一种用于重构移动钱包应用的方法,所述方法包括:接收用于重构用户的移动钱包应用的请求;将存储的与所述用户相关联的移动钱包应用信息发送到移动终端;接收移动终端信息和SE信息;将存储的与移动钱包应用信息相关联的应用发送到移动终端。一种用于保护非UICC类型SE中的信息OTA的移动终端,所述移动终端包括:OTA代理,用于从TSM接收保护命令;非UICC SE。



1. 一种用于保护移动终端的非通用集成电路卡(UICC)类型安全元件(SE)中的信息的方法,包括:

从推送服务器接收用于初始化移动终端的空中下载(OTA)代理的请求;

初始化OTA代理,其中,初始化OTA代理的步骤包括:唤醒OTA代理;使用OTA代理将移动终端信息和SE信息发送到可信服务管理器(TSM);

从TSM接收用于保护存储在SE中的信息的请求;

使用OTA代理保护存储在SE中的信息,其中,SE是非UICC类型SE,其中,保护SE中的请求的信息的步骤包括:删除存储在非UICC类型SE中的信息,

其中,在保护请求的信息之前准备用于保护信息的SE,包括:检索移动终端信息和SE信息,其中,所述SE信息包括SE状态和SE类型;基于SE状态接收密钥;使用所述密钥访问所述SE。

2. 如权利要求1所述的方法,还包括:

请求OTA代理的安装;

接收OTA代理安装信息;

在移动终端中安装OTA代理。

3. 如权利要求2所述的方法,其中,从TSM接收OTA代理安装信息。

4. 如权利要求3所述的方法,其中,SE信息包括SE状态和SE类型。

5. 如权利要求1所述的方法,其中,用于保护信息的请求包括应用协议数据单元(APDU)命令。

6. 如权利要求5所述的方法,其中,保护非UICC类型SE中的请求的信息的步骤包括:执行用于保护请求的信息的APDU命令,其中,非UICC类型SE包括微型安全数字(SD)、嵌入式SE或不支持短消息服务端对端(SMS-PP)协议或承载独立协议(BIP)的SE。

7. 如权利要求1所述的方法,其中,保护SE中的请求的信息的步骤还包括:锁定对存储在非UICC类型SE中的信息的访问。

8. 如权利要求1所述的方法,其中,移动终端信息包括国际移动设备识别码(IMEI)、移动设备识别码(MEID)和移动用户综合业务数字网号码(MSISDN)中的至少一个。

9. 如权利要求1所述的方法,其中,保护存储在SE中的信息的步骤包括:响应于SE状态是操作系统(OS)原生的确定,TSM向SE提供初始发行者主密钥和最终发行者主密钥中的至少一个。

10. 如权利要求1所述的方法,其中,保护存储在SE中的信息的步骤包括:响应于SE状态被初始化的确定,TSM将最终发行者主密钥提供给SE。

11. 如权利要求1所述的方法,其中,使用所述密钥访问所述SE的步骤还包括:TSM处理用于实现SE的配置的协议,SE类型是微型安全数字(SD)类型。

12. 一种用于在可信服务管理器(TSM)中认证移动终端的方法,包括:

从移动终端接收经由移动终端的空中下载(OTA)代理发送的移动终端信息和安全元件(SE)信息;

将接收的信息与存储的移动终端信息和SE信息进行比较;

基于接收到的SE信息发送密钥以访问SE,其中,所述密钥包括初始发行者主密钥和最终发行者主密钥中的至少一个;

基于比较结果发送命令，
其中，SE是非通用集成电路卡(UICC)类型SE，
其中，基于比较结果发送命令的步骤包括：发送用于删除存储在移动终端的SE中的信息的命令。

13. 如权利要求12所述的方法，其中，移动终端信息包括国际移动设备识别码(IMEI)、移动设备识别码(MEID)和移动用户综合业务数字网号码(MSISDN)中的至少一个。

14. 如权利要求12所述的方法，其中，SE信息包括卡图像编号(CIN)、卡参考编号(CRN)、卡产品生命周期(CPLC)和卡序列号(CSN)中的至少一个。

15. 如权利要求12所述的方法，其中，发送用于删除存储在移动终端的SE中的信息的命令的步骤还包括：响应于接收的信息与存储的信息不同，发送所述命令。

16. 如权利要求12所述的方法，其中，基于比较结果发送命令的步骤还包括：响应于接收的信息与存储的信息不同，发送用于锁定对存储在移动终端的SE中的信息的访问的命令。

17. 一种用于保护非通用集成电路卡(UICC)类型安全元件(SE)中的信息空中下载(OTA)的移动终端，包括：

OTA代理，被配置为连接到可信服务管理器(TSM)，并从TSM接收保护命令，其中，OTA代理被配置为将移动终端信息和SE信息发送到TSM；

其中，OTA代理还被配置为基于发送到TSM的SE信息，从TSM接收密钥以访问SE，其中，所述密钥包括初始发行者主密钥和最终发行者主密钥中的至少一个，

其中，保护命令是用于删除存储在非UICC类型SE中的信息的命令或用于锁定对存储在非UICC类型SE中的信息的访问的命令。

18. 如权利要求17所述的移动终端，其中，SE信息包括SE状态和SE类型。

19. 如权利要求18所述的移动终端，其中，OTA代理还被配置为接收用于准备将被配置的SE的协议，SE类型是微型安全数字(SD)类型。

20. 如权利要求17所述的移动终端，其中，非UICC类型SE包括：

非接触式卡小程序；

与所述非接触式卡小程序相应的钱包管理小程序，其中，钱包管理小程序包括与非接触式卡小程序相关联的账户号码、截止日期和安全码中的至少一个。

针对存储在移动终端中的敏感财务信息的安全容器的系统和方法

技术领域

[0001] 下面的描述涉及移动终端中的敏感数据的保护。

背景技术

[0002] 随着移动技术领域的最近发展,移动终端的尺寸和重量变得显著减小,因而增加了它们的便携性并促进了用户始终携带移动终端的倾向。随着移动终端(例如,移动电话和其它移动装置)正在变得被更广泛地使用,移动终端已从仅仅具有通信功能的移动终端稳步发展为合并各种高级功能(诸如,电子邮件、计算机办公应用功能、视频电话以及最近的移动支付功能)的终端。尽管将各种消费者友好的应用集成到移动终端可向其用户提供便利,但它也引起了关于这些移动终端的安全性关注。

[0003] 与这些移动终端的错放、丢失、盗窃相关的不当使用以及可能发生的其它事故提高了与移动终端的更强可用性相关的安全性关注。为了缓解这些安全性关注,已提出各种技术以在移动终端被错放或被盗时,远程锁定移动终端以禁用它们的功能。使用这些技术,如果移动终端在正常操作状态下将被锁定,则其功能可被禁用,因此使得可减少存储在移动终端中的私人信息的不当使用或盗窃。

[0004] 然而,随着技术的进步,盗窃人群的才智也得到发展。更多受过教育的盗窃犯可通过“越狱”来容易地闯入被远程锁定的移动终端,以检索敏感信息。因此,仅从使用方面锁定设备或应用不再是足够的,必须做得更多以防止存储在移动终端内的敏感数据的盗用。

[0005] 另外,随着可移除安全元件(SE)的引入,安全领域里的另一个复杂情况被提出。因为这些存储敏感信息的SE中的很多SE可能在它们可被锁定之前被移除,所以这些装置上的简单的锁定安全特征(feature)可能并不足够。

[0006] 数据删除的方法可用于提供可靠的安全性。然而,在当前,SE中的远程数据删除限于符合工业标准短消息服务-端对端(SMS-PP)协议或承载独立协议(BIP)的SE(即,通用集成电路卡(UICC)类型SE)。在装置拥有者具有不允许经由工业标准协议的访问的SE(诸如,微型(安全数字)SD卡或嵌入式SE(即,非UICC类型SE))的情况下,SE中的远程数据删除可能不可行。

[0007] 最后,即使敏感的存储数据已经能够被删除,在重新获得/替换丢失的移动终端时也没有替换丢失的数据的容易方式。因此,即使丢失并随后替换了存储敏感信息的移动终端,也必须从头开始使用所有的应用和存储的数据重新安装移动终端。

发明内容

[0008] 本发明的示例性实施例提供一种用于保护存储在非通用集成电路卡(UICC)类型安全元件(SE)空中下载(OTA,over-the-air)中的信息的方法。本发明的示例性实施例还提供一种用于使用可信服务管理器(TSM,Trusted Service Manager)认证移动终端并重构移动钱包应用的方法。

[0009] 在下面的描述中将阐述本发明的另外的特征,还有部分从所述描述将是清楚的,或可通过本发明的实施而得知。

[0010] 本发明的示例性实施例提供一种用于保护移动终端的非UICC类型SE中的信息OTA的方法,所述方法包括:接收用于初始化移动终端的OTA代理的请求;初始化OTA代理;接收用于保护存储在SE中的信息的请求;使用OTA代理保护存储在非UICC类型SE中的信息。

[0011] 本发明的示例性实施例提供一种用于认证移动终端的方法,所述方法包括:从移动终端接收移动终端信息和SE信息;将接收的信息与存储的移动终端信息和SE信息进行比较;基于比较结果发送命令。

[0012] 本发明的示例性实施例提供一种用于重构移动终端的移动钱包应用的方法,所述方法包括:接收用于重构用户的移动钱包应用的请求;将存储的与所述用户相关联的移动钱包应用信息发送到移动终端;接收移动终端信息和SE信息;将存储的与移动钱包应用信息相关联的应用发送到移动终端。

[0013] 本发明的示例性实施例提供一种用于保护非UICC类型SE中的信息空中下载(OTA)的移动终端,所述移动终端包括:OTA代理,被配置为连接到TSM,并从TSM接收保护命令;非UICC类型SE。

[0014] 将理解,前述总体描述和以下详细描述两者是示例性和解释性的,并且意图提供如要求保护的本发明的进一步的解释。从以下详细描述、附图和权利要求,其它特征和方面将是清楚的。

附图说明

[0015] 附图示出本发明的实施例,并且与描述一起用于解释本发明的原理,其中,附图被包括以提供本发明的进一步的理解,并且被合并在本说明书中并构成本说明书的一部分。

[0016] 图1是根据本发明的示例性实施例的可信服务管理器(TSM)生态系统的系统示图。

[0017] 图2是示出根据本发明的示例性实施例的用于从安全元件(SE)和移动钱包应用删除敏感的信用卡证书和相关的移动钱包信息的方法的系统示图。

[0018] 图3是示出根据本发明的示例性实施例的用于同步移动钱包应用以认证访问钱包管理系统的移动终端和SE的方法的系统示图。

[0019] 图4是示出根据本发明的示例性实施例的用于通过推送方法来重构财务信息证书和相关的移动钱包应用的方法的系统示图。

[0020] 图5是示出根据本发明的示例性实施例的用于通过拉取(pull)方法来重构财务信息证书和相关的移动钱包应用的方法的系统示图。

具体实施方式

[0021] 在下文中参照附图来更充分地描述本发明,其中,在附图中示出了本发明的示例性实施例。然而,可以以很多不同的形式实施本发明,本发明不应被解释为限于在此阐述的实施例。相反,这些示例性实施例被提供使得本公开是彻底的,并将把本发明的范围充分传达给本领域的技术人员。将理解:针对本公开的目的,“每个…中的至少一个”将被解释为表示遵循相应语言的包括多个列举的元素的组合的列举的元素的任意组合。例如,“X、Y和Z中的至少一个”将被解释为表示只有X、只有Y、只有Z,或者是X、Y和Z中的两项或更多项的任意

组合(例如,XYZ、XZ和YZ)。在整个附图和详细描述中,除非另有描述,否则相同的附图标号被理解为表示相同的元件、特征和结构。为清楚、说明和方便,这些元件的相对大小和描述可被夸大。

[0022] 图1是根据本发明的示例性实施例的可信服务管理器(TSM)生态系统的系统示图。

[0023] 如图1中所示,采用具有空中下载(OTA)代理配置(provisioning)的TSM技术的示例系统包括:TSM10;移动终端11;网络15;第三方消息传送平台16;金融机构18;移动网络运营商(MNO)19;手机制造商20;卡制造商21。在TSM10可被用户及它的参与者充分使用之前,服务提供商(SP)(诸如,以18-21标识的服务提供商)可经受预注册处理。在示例中,网络15可指蜂窝网络,其中,蜂窝网络可包括一个或多个基站,以使移动终端11能够与其它移动终端或第三方实体进行通信。另外,网络15还可包括任何其它类型的合适的通信网络(诸如,互联网)、传统的有线电话线和其它合适的网络技术。

[0024] 手机制造商20可包括嵌入式安全元件(SE)生产商,卡制造商21可包括微型安全数字(SD)SE(即,非通用集成电路卡(UICC)SE)的生产商。因为不同的SE制造商可提供与为传统的UICC SE装置提供的OTA密钥不同的OTA密钥,所以手机制造商20和卡制造商21可将它们的OTA密钥提供给以上提及的预注册处理中的TSM10以用于将来的处理。可选择地,手机制造商20和卡制造商21可在请求时提供它们各自的OTA密钥,而无需预注册处理。在共同待决(co-pending)的申请61/428,853中提供了预注册处理的更详细的解释。

[0025] 在示例中,OTA代理可在移动钱包应用的使用期间被初始化或被配置为与TSM10连接,以节省技术资源。这样,OTA代理将默认处于睡眠模式,直到为它的使用而被唤醒为止。为了规定唤醒机制,可利用第三方消息传送平台16(例如,云到装置消息传送(C2DM,Cloud to Device Messaging))来唤醒OTA代理,所述OTA代理将依次与TSM10连接以进行使用。如果TSM10将消息连同唤醒命令和识别信息发送到第三方消息传送平台16,则第三方消息传送平台16依次将消息发送到识别的移动终端11以唤醒驻留在移动终端11内的OTA代理。一旦唤醒,OTA代理将连接到TSM10用于配置或其它用途。可选择地,如果期望,则OTA代理可以以较高频率或被连续地连接以避免上述的唤醒处理。

[0026] 如果移动终端11配备有启用近场通信(NFC)的芯片并配置有可使用NFC技术的非接触式卡小程序,则移动终端11的拥有者可通过在相应的销售点(POS)装置挥动(wave)移动终端11来在启用NFC的POS商店进行购买。随后,一旦使用移动终端11进行了购买,收单方(acquirer)网络23和支付处理器22就可一起工作以保证支付在金融机构18获得更新。然而,该终端用户应用不包括描述的TSM生态系统并被示出为提供完整的生态系统的描述。

[0027] 以下参照图2描述一种用于从移动终端的SE删除敏感信息(诸如,信用卡证书)的方法。尽管在此示例性附图中仅描述了用于删除的方法,但将理解,可使用用于保护敏感信息的其它方法(诸如,锁定对存储在SE中的信息的访问)。

[0028] 图2是示出用于从SE删除敏感的信用卡证书的方法的系统示图。针对本公开的目的,尽管在图2-图5中未示出,但将理解,通过如图1中所示的网络15或其它合适的方法提供在外部方或服务提供商(18-21)、TSM10和移动终端11之间进行的任何通信。另外,将理解,敏感信息不限于信用卡信息,针对本公开的目的,参考信用卡信息仅被用作示例。

[0029] 如图2所示,在步骤201,服务提供商(SP)(诸如,金融机构18)做出具有识别信息(诸如,移动用户综合业务数字网(MSISDN))的请求,以从被盗/丢失的移动终端11删除其证

书(例如,信用卡号码、截止日期、安全码、个人识别号码(PIN))。在示例中,可由移动终端11的拥有者或各个SP发起这样的请求。所述请求对于属于特定SP的信用卡信息而言可以是特定的,或者所述请求可用于删除驻留在SE中的所有信用卡信息,否则删除存储在SE内的所有敏感信息。尽管所述请求通常会仅限于属于请求的SP的信用卡信息,但如果各种金融机构达成协议,则还可删除其他同意的SP的信用卡信息。

[0030] 同样,在步骤201,由SP发送的请求可用于锁定包含信用卡证书的整个SE,或仅锁定存储各个信用卡信息的SE内的各个安全域。可由SP指定用于锁定或删除特定安全域的请求,或者可迎合用于锁定或删除特定安全域的请求以满足其他商业规则/要求。另外,尽管在提供的附图中未示出,但可由与TSM10直接接触的移动终端11拥有者发起保护存储在SE中的信息的请求。此外,可由SP按照自己的意志或响应于移动终端11的拥有者的请求发起步骤201中的请求。

[0031] 在步骤202,TSM10从SP接收请求,并在其数据库内将各个移动终端账户更新为“删除”状态。另外,TSM10进行内部查询以验证有问题的移动终端11是否具有已安装的移动钱包应用31(诸如,SK C&C移动钱包应用31)。在示例中,如果TSM10确定SK C&C移动钱包应用31安装在各个丢失/被盗的移动终端11中,则TSM10将请求修改为删除相关的非接触式小程序、驻留在SE内的钱包管理应用(WMA)21信用卡证书(钱包管理小程序)和驻留在SK C&C移动钱包应用31内的小控件。

[0032] 另外,TSM10确定在丢失/被盗的移动终端11上配备的SE的类型。因为微型SD和嵌入式SE(即,非UICC类型SE)无法支持传统的用户识别模块应用工具包(SAT)/通用用户识别模块应用工具包(USAT)/卡应用工具包(CAT)架构,所以由TSM10构造的删除命令可通过OTA代理,以做出对存储在非UICC类型SE(诸如,微型SD或嵌入式SE)中的信息的任意删除。然而,OTA代理还可支持由传统的SAT/USAT/CAT架构支持的SE(诸如,UICC、服务识别模块(SIM)或通用用户识别模块(USIM)(在此统称为UICC))。可在共同待决的申请61/428,851中找到关于OTA代理的更详细的解释。

[0033] 一旦TSM10完成修改用户账户状态,在步骤203,就向移动推送服务器(诸如,云到装置消息传送(C2DM)平台)做出推送请求。

[0034] 在步骤204,移动推送服务器推送消息以唤醒驻留在丢失/被盗的移动终端11中的OTA代理。

[0035] 在步骤205,OTA代理对移动终端11和相关联的SE特定信息(诸如,MSISDN和卡图像编号(CIN,Card Image Number))进行检索,并将它们发送到TSM10。在示例中,SE信息还可包括卡参考编号(CRN)、卡产品生命周期(CPLC)和卡序列号(CSN)。

[0036] 另外,尽管未示出,但是一旦TSM10接收到移动设备和SE信息,TSM10就确认SE的状态。因为存储的SE的处理可基于其状态,所以可在访问存储在SE中的信息之前进行对SE状态的分析和相应处理。更具体地讲,基于SE状态,可执行一些准备步骤以保护用于处理通过OTA代理接收的命令的SE。在示例中,移动终端11中配备的SE可具有以下3种状态中的任意状态:操作系统(OS)原生(native)、被初始化和被保护。如果SE的状态被确定为“被保护”,则可不执行进一步的准备步骤。SE的“被保护”状态可指签发后的预期操作卡生命周期状态。另一方面,如果SE的状态被确定为“被初始化”,则随后TSM10可提供最终发行者主密钥以保护SE。SE的“被初始化”状态可指管理卡产品状态。最后,如果SE的状态被确定为“OS原

生”,则随后可进行预个性化处理,其中,所述预个性化处理可包括向SE提供初始发行者主密钥和最终发行者主密钥。SE的“OS原生”状态可指SE没有被制造商的初始化方法初始化的状态。

[0037] 在SE的状态已被确定之后,可执行对SE类型的分析以确定在OTA代理内应运行的协议的类型,以便配置到识别的SE。如果SE是UICC类型或嵌入式类型,则可访问SE以修改存储在SE中的信息。可选择地,如果SE是微型SD类型,则可执行额外的处理特定协议以访问或修改存储在SE中的信息。由于本领域的普通技术人员理解哪些类型的协议可用于访问微型SD类型,因此在此省略其描述。

[0038] 在步骤206,TSM10处理提供的信息连同“删除”命令并将它们转换为应用协议数据单元(APDU)命令,并且将转换的APDU命令发送到OTA代理。

[0039] 在步骤207,OTA代理将接收的APDU命令中继到信用卡证书可驻留的SE。信用卡证书可作为非接触式卡小程序驻留,并可驻留在钱包管理小程序(WMA)21内。对于关于如何创建相应的WMA21的更多细节,请参考共同相关的申请号61/428,846。

[0040] 一旦已成功处理了“删除”命令,在步骤208,将结果发送到OTA代理。

[0041] 在步骤209,OTA代理将结果中继回TSM10。在步骤210,TSM10依次将通知发送到其请求的结果的SP。

[0042] 如果移动终端11被启动并具有到网络的接收,则可提供图2中公开的“删除”功能。

[0043] 在图3中,提供用于同步驻留在移动终端11内的移动钱包应用31的系统示图。

[0044] 在步骤301,多个外部方或SP可请求使用TSM/钱包管理系统(WMS)对用户的移动钱包应用31配置做出改变,其中,TSM/钱包管理系统(WMS)可存储用户的移动钱包应用31的主要配置。针对本公开的目的,外部方或SP可包括(而不限于)金融机构18、移动网络运营商(MNO)19、手机制造商20和卡制造商21(统称为“服务提供商”或“SP”)。因为移动钱包应用31不会总是打开,所以TSM/WMS可用作中央储存库以允许各种外部方在不考虑用户的对移动钱包应用31的登录状态的情况下做出改变请求。例如,各个外部方或SP可根据它们自己的时间请求将额外的非接触式卡配置到用户的移动钱包应用31,而不考虑用户的状态。

[0045] 类似地,TSM10本身可基于它自己的内部记录自动识别出存储在SE中的非接触式卡小程序截止日期正接近,并提示用户更新非接触式卡小程序信息。在示例中,可通过移动钱包应用31或其它合适的方法(诸如,电子邮件、文本和语音邮件)提示移动终端11的用户。也可由TSM10通过其它方法(诸如,文本、电子邮件、语音邮件或其它提供通知的合适方法)提示用户。响应于提示,移动终端11的用户可通过TSM10系统或通过联系负责即将过期的非接触式卡小程序的SP来重新配置各个非接触式卡小程序。

[0046] 随后,在步骤302,当用户登录到移动终端11上的移动钱包应用31时,驻留在移动钱包应用31内的OTA代理将对特定移动终端11信息和SE特定信息(例如,MSISDN、国际移动设备识别码/移动设备识别码、CIN/集成电路卡识别码(ICCID))进行检索并将它们发送到TSM10以进行分析。

[0047] 在步骤303,TSM10在接收到提供的信息时,使用存储的信息进行由OTA代理提供的信息的内部验证。

[0048] 如果发现提供的手机信息或SE信息与注册的信息冲突,则在步骤304,TSM10记录该事件,并可命令移动钱包应用31锁定或删除敏感信息,直到进一步的验证或澄清可被提

供为止。敏感信息可包括可存储在SE中的与金融机构18相关的账户特定信息(诸如,信用卡号、截止日期、个人识别号码和其它相关信息)。另外,敏感信息还可包括存储在SE中的用户安全信息或其它私人信息。

[0049] 在示例中,小偷可从移动终端11盗取可移除SE(诸如,微型SD),并在用户认识到SE正从他或她的移动终端11丢失之前,在不同的移动终端上使用所述可移除SE。通过使用注册的移动终端标识交叉参照(cross referencing)注册的SE,TSM10将识别出注册的SE是否正被安装在不同的非注册的移动终端11上。另外,应注意,TSM10可以以与在步骤304描述的方式不同的方式处理不一致装置的识别。TSM10可根据由参与方提供的商业规则(诸如,选择提示用户密码、安全密钥或其它验证方法)处理这样的事件。

[0050] 在根据它们的商业规则处理这样的事件时,可由消费者或SP提供额外的或不同的方向。

[0051] 当做出请求配置另一非接触式卡小程序23时,或者每当请求OTA代理与TSM10或等同系统连接时,也可进行该同步检查。

[0052] 图4示出用于重构移动钱包应用31的推送系统的示例性系统示图。一旦用户已经发现或替换可能不再包含所有先前的用户的财务证书的移动终端,装置的用户就会联系SP或TSM10之一以重构其移动钱包应用31以及其中的所有先前存储的内容。针对本公开的目的,移动钱包应用31可包括驻留在移动钱包应用31内的小控件、存储在SE中的非接触式卡小程序23和相关联的WMA21以及可选的OTA代理。然而,移动钱包应用31可包括比在此描述的所有元件的更少的元件或比在此描述的元件更多的元件。

[0053] 在步骤401,移动终端11的用户联系通知获得(procurement)新移动终端11的SP。SP可进行它自己的认证以验证移动终端11的正确用户。类似地,用户还可直接通知MN019或TSM10。

[0054] 一旦SP已经认证了用户,在步骤402,SP就将请求发送到TSM10以使用SP的非接触式应用和相关的证书来重新配置用户的新移动终端11。

[0055] 在步骤403,TSM10执行内部检查以验证用户是否具有在丢失他或她的电话之前配置的任何其它SP账户。如果存在用户拥有的其它SP账户,则针对其配置信息向各个SP做出请求。

[0056] 一旦SP接收到用于配置信息的请求,在步骤404,可进行内部认证和有效性检查,并将必要的信息发送到TSM10以进行处理。

[0057] 在步骤405,进行另一内部检查以验证用户在他或她的移动终端11中先前具有什么移动钱包应用31。移动钱包应用31可包括各种类型(诸如,SKC&C移动钱包应用31或由不同制造商提供的其它移动钱包应用)。

[0058] 在示例中,在步骤406,如果发现先前安装了移动钱包应用31,则随后系统将检索相同版本和与移动钱包应用31相关联的用户偏好设置,以发送给用户。在移动到步骤407之前,可将各个移动钱包应用31连同其配置的用户偏好通过移动推送服务器发送到用户移动终端11。针对本公开的目的,假设移动钱包应用31包括相应的OTA代理,其中,可在接收到应用时由移动终端11安装相应的OTA代理,或可通过单独的处理安装相应的OTA代理。

[0059] 在步骤407,TSM10将用于唤醒OTA代理的推送消息发送到移动推送服务器(诸如,C2DM系统)。在示例中,可在OTA代理之前、与移动钱包应用31同时、或者在移动钱包应用31

之前发送OTA代理。

[0060] 随后,在步骤408,移动推送服务器将接收的唤醒命令中继到OTA代理。

[0061] 在步骤409,OTA代理对移动终端11和SE特定信息(诸如,MSISDN和CIN)进行检索并将它发送到TSM10。

[0062] 一旦TSM10接收到由OTA代理发送的信息,在步骤410,TSM10就对该信息连同配置命令进行处理,并将它们转换为APDU命令以发送到OTA代理。在示例中,配置命令可包括特定指令(诸如,安装或删除特定信息或应用),以及可由金融机构18提供的用于非接触式卡小程序的账户特定信息。此外,当接收到用于非接触式卡小程序或其它敏感信息的账户特定信息时,这样的信息可被复制以配置到WMA21。另外,还由TSM10获得用于移动终端11的移动钱包应用31的相关联的小控件的版本,以直接配置到钱包应用31。

[0063] 接下来,在步骤411,OTA代理将接收的APDU命令转发到可配置信用卡证书、非接触式小程序的SE。如果用户是移动钱包应用31的先前用户,则APDU命令将被中继到与将安装在WMA21内的非接触式小程序相应的配置账户信息,其中,所述WMA21也位于SE之内。另外,将在移动钱包应用31中安装相应的小控件应用,以提供安装的账户的图形显示。

[0064] 一旦已经成功处理了配置命令,在步骤412,就将结果发送回OTA代理。

[0065] 随后,在步骤413,OTA代理将所述结果中继回TSM10,TSM10使用请求的结果更新其系统。

[0066] 在步骤414,将SP配置请求的结果的通知发送到各个SP。

[0067] 与图4类似,如图5中所示,可通过可由移动终端11拥有者发起的拉取机制,重构用户的移动钱包应用31。

[0068] 在步骤501,移动终端11的拥有者尝试从移动终端11重新安装移动钱包应用31,并且从新的移动终端11或替换的移动终端11做出请求。将命令请求连同移动识别信息发送到TSM10。

[0069] 在步骤502,TSM10接收所述请求及其相关的识别信息,发生认证处理以验证用户。可通过密码、安全问题、社会安全号码或通过其它合适的验证方法验证请求的用户。一旦已经正确地识别出用户,就针对现有账户进行检查。如果发现先前已安装移动钱包应用31,则随后系统对相同的版本和与移动钱包应用31相关的用户偏好设置进行检索,并且在步骤503发送给用户用于进行下载。可通过移动推送服务器将各个移动钱包应用31连同其配置的用户偏好发送到用户移动终端11。

[0070] 在示例中,如果确定请求的用户先前不具有移动钱包应用31,则在TSM10中创建新的账户,并通过移动推送服务器将移动钱包应用31发送到移动终端11。针对本公开的目的,假设移动钱包应用31包括相应的OTA代理,其中,可在接收到应用时由移动终端11安装相应的OTA代理,或可通过单独的处理安装相应的OTA代理。

[0071] 接下来,在步骤504,TSM10针对相关的SP账户信息检查请求的用户账户。如果一个或多个SP账户与请求的用户的账户相关联,则可将通知发送到SP,请求将配置信息发送到请求的用户。尽管步骤503和步骤504被配置为单独的步骤,但可一并进行步骤503和步骤504,或者也可按照相反的顺序进行步骤503和步骤504。例如,本公开单独地提供移动钱包应用31和与SP相关的小控件。然而,还可从SP收集所有必要的小控件和移动钱包应用31,使得TSM10可同时将小控件和移动钱包应用31中继到用户。可选择地,如果允许TSM10存储账

户特定信息，则可由TSM10提供移动钱包应用31和小控件，而无需向SP做出额外的请求。

[0072] 一旦SP接收到对配置信息的请求，在步骤505，就可进行内部认证和有效性检查，并将必要的信息发送到TSM10以进行处理。

[0073] 在步骤506，TSM10将用于唤醒OTA代理的推送消息发送到移动推送服务器（诸如，C2DM系统）。尽管示出在OTA代理之前发送移动钱包应用31，但应注意，可与移动钱包应用31同时发送OTA代理，或者可在移动钱包应用31之前发送OTA代理。

[0074] 随后，在步骤507，移动推送服务器将接收的唤醒命令中继到OTA代理。

[0075] 在步骤508，OTA代理收集移动终端11特定信息（诸如，MSISDN和CIN）连同配置命令，并将其发送到TSM10。在示例中，配置命令可包括特定指令（诸如，安装或删除特定信息或应用）和可由金融机构18提供的针对非接触式卡小程序的账户特定信息。可由其它SP或TSM10提供其它敏感信息（诸如，SE的密钥）。可由SP使用作为中介（intermediary）的TSM10实时地提供敏感信息，或者可由SP预先提供敏感信息以存储在TSM10中。

[0076] 一旦TSM10接收到由OTA代理发送的信息，在步骤509，TSM10就处理该信息连同配置命令，将它们转换为APDU命令，并将它们发送到OTA代理。此外，如果接收到包括非接触式卡小程序的账户特定信息的配置命令，则可复制这样的信息以配置到WMA21。另外，针对钱包应用31的相关联的小控件的版本也可被TSM10获得，以被直接配置到移动钱包应用31。

[0077] 接下来，在步骤510，OTA代理将接收的APDU命令中继到可配置信用卡证书、非接触式小程序的SE。如果用户是先前的移动钱包应用31用户，则可将APDU命令中继到与将在WMA21内安装的非接触式小程序相应的配置账户信息，其中，所述WMA21也位于SE内。另外，可在移动钱包应用31中安装相应的小控件应用以提供安装的账户的图形显示。

[0078] 一旦已经成功处理了配置命令，在步骤511，就将结果发送回OTA代理。

[0079] 随后，在步骤512，OTA代理将所述结果中继回TSM10，TSM10将使用所述请求的结果更新其系统。

[0080] 在步骤513，对SP配置请求的结果的通知将被发送到各个SP。

[0081] 对于本领域的技术人员来说清楚的是，在不脱离本发明的精神或范围的情况下，可在本发明中进行各种修改和改变。因此，目的在于如果所述修改和改变落入权利要求及其等同物的范围内，则本发明覆盖本发明的所述修改和改变。

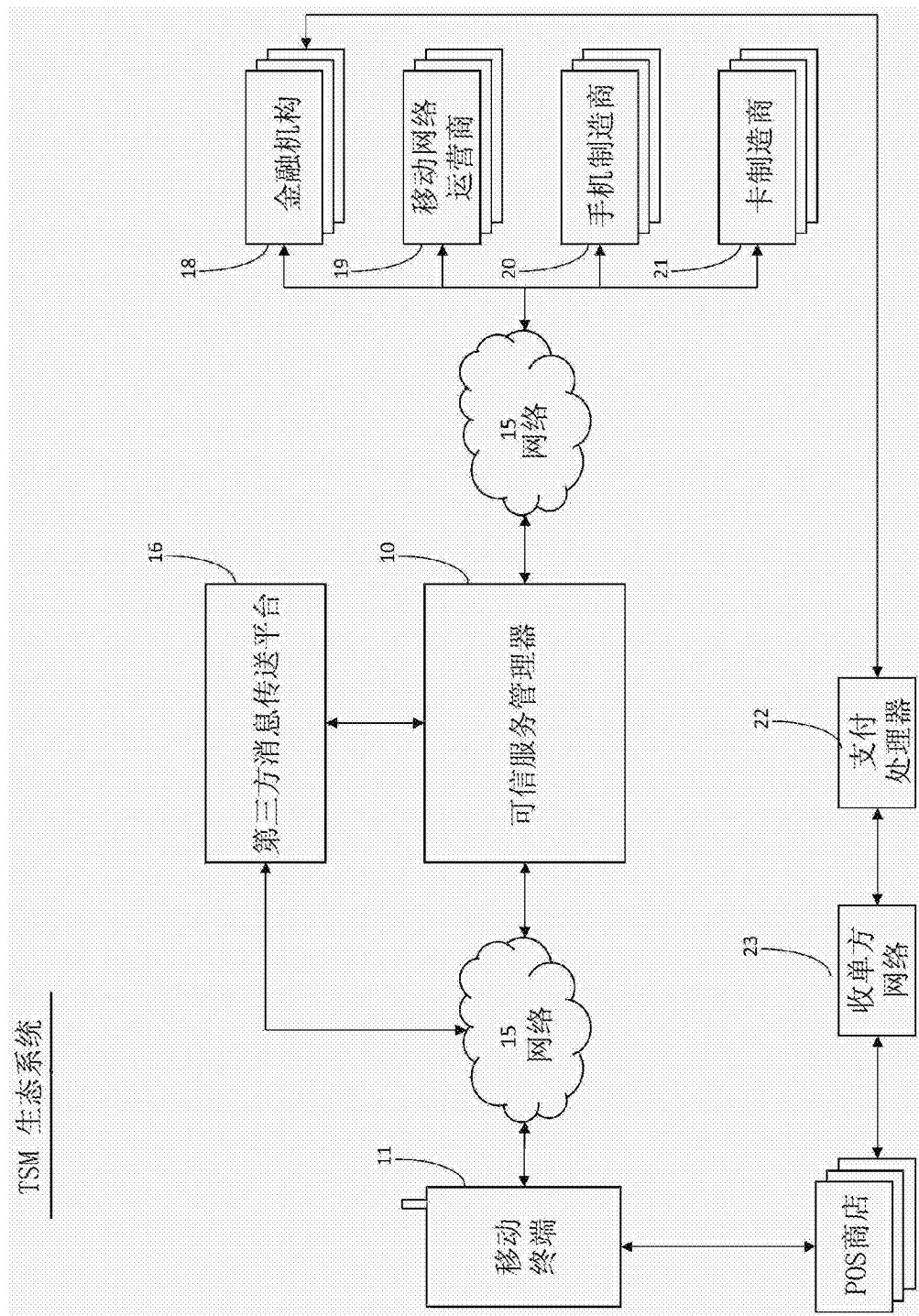


图1

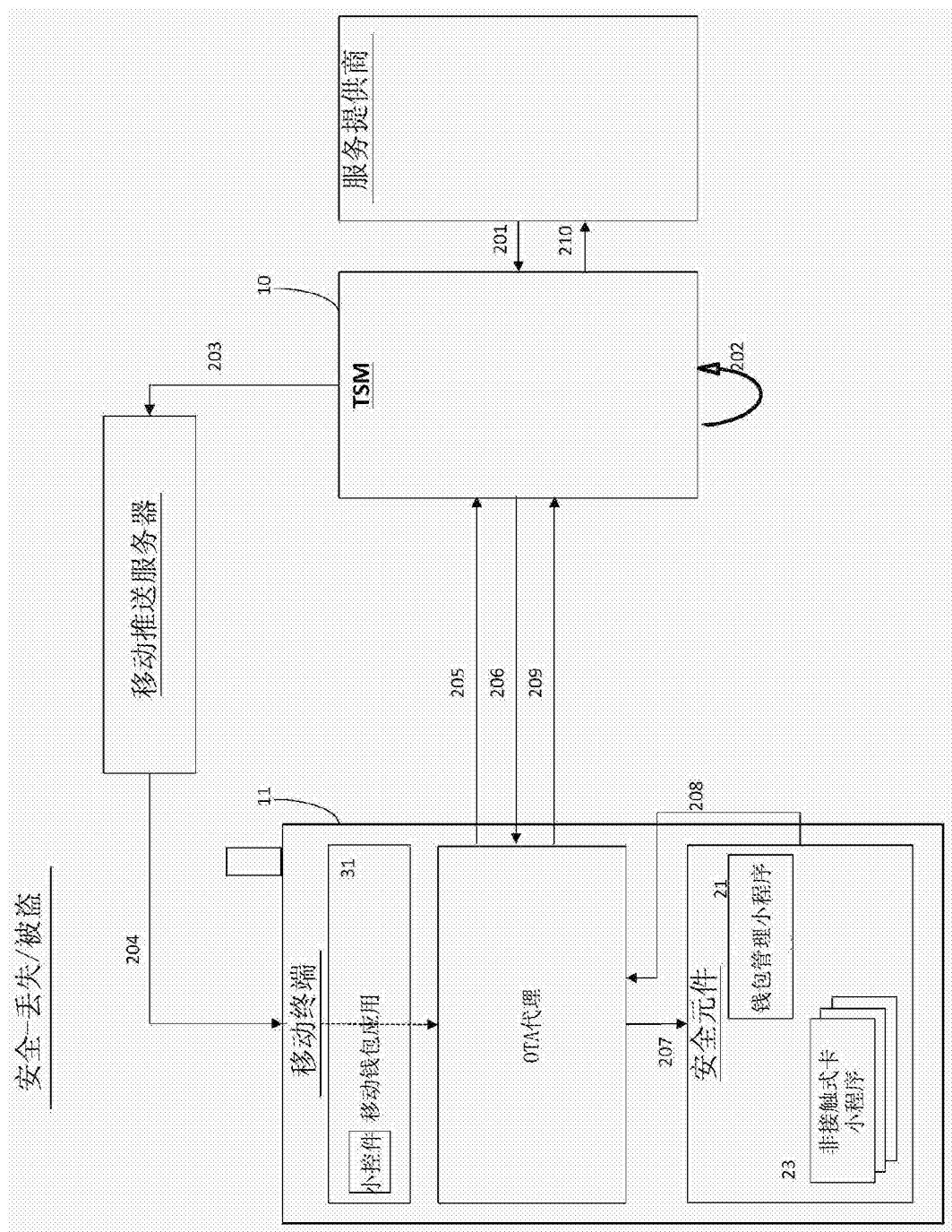


图2

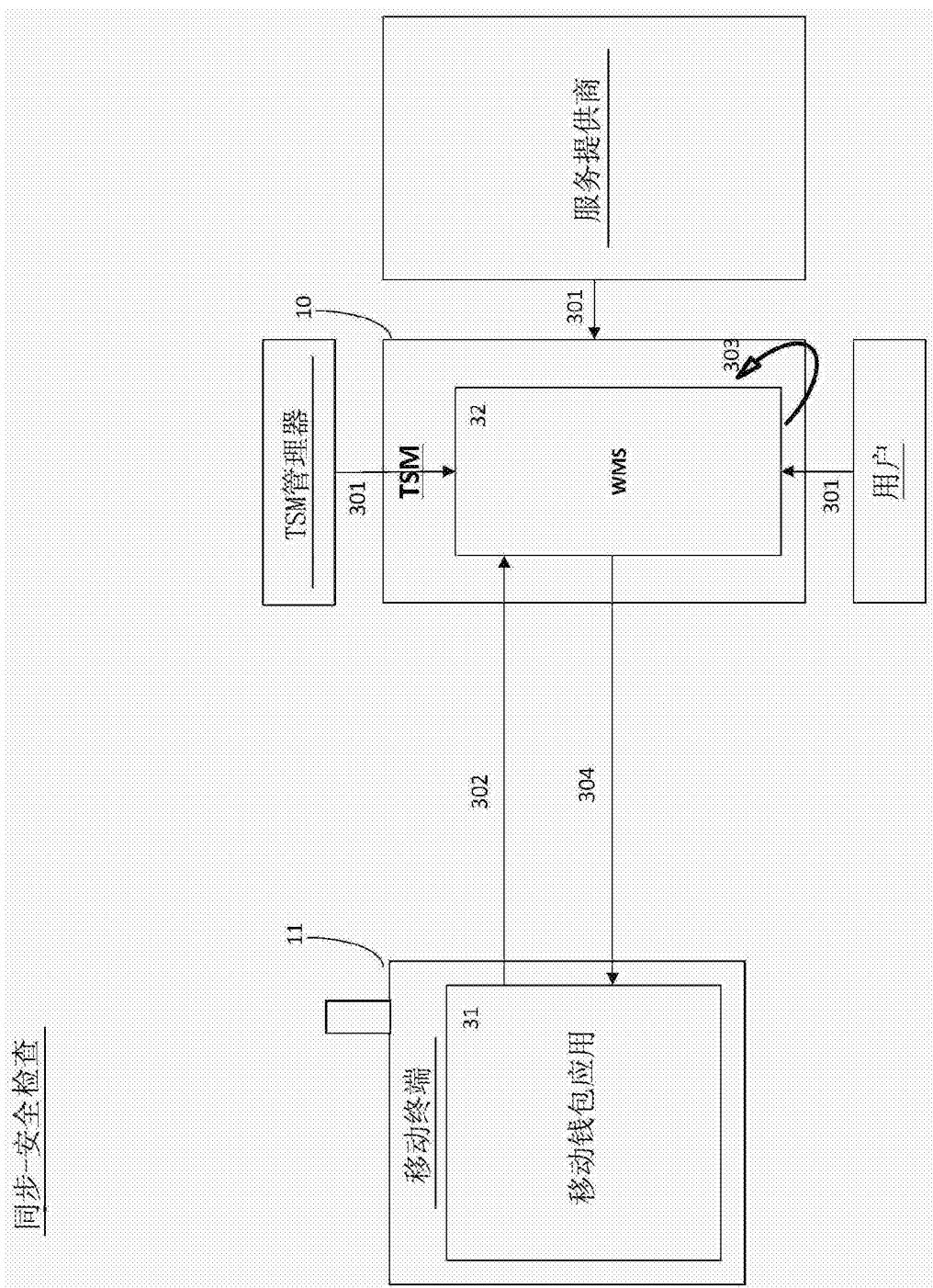


图3

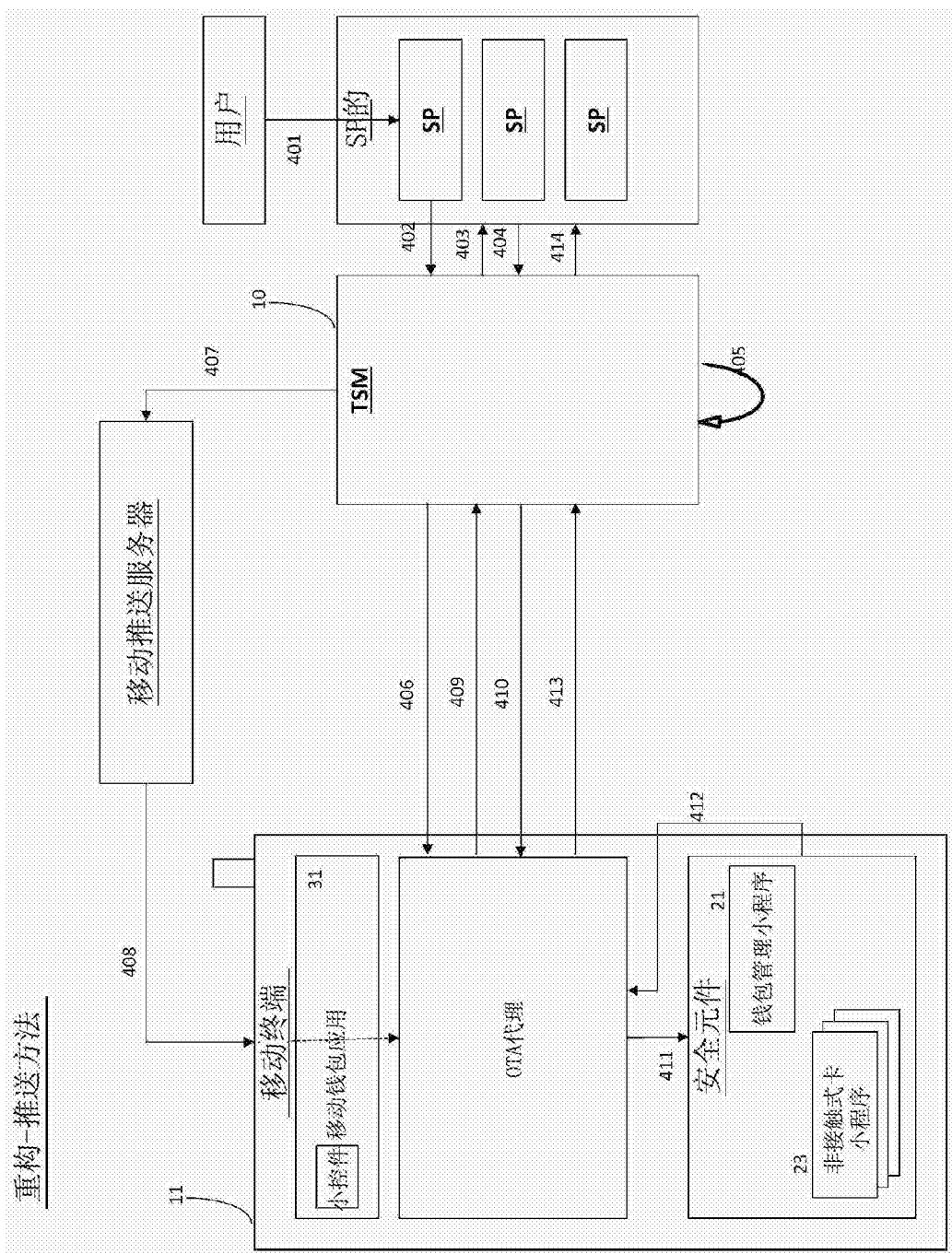


图4

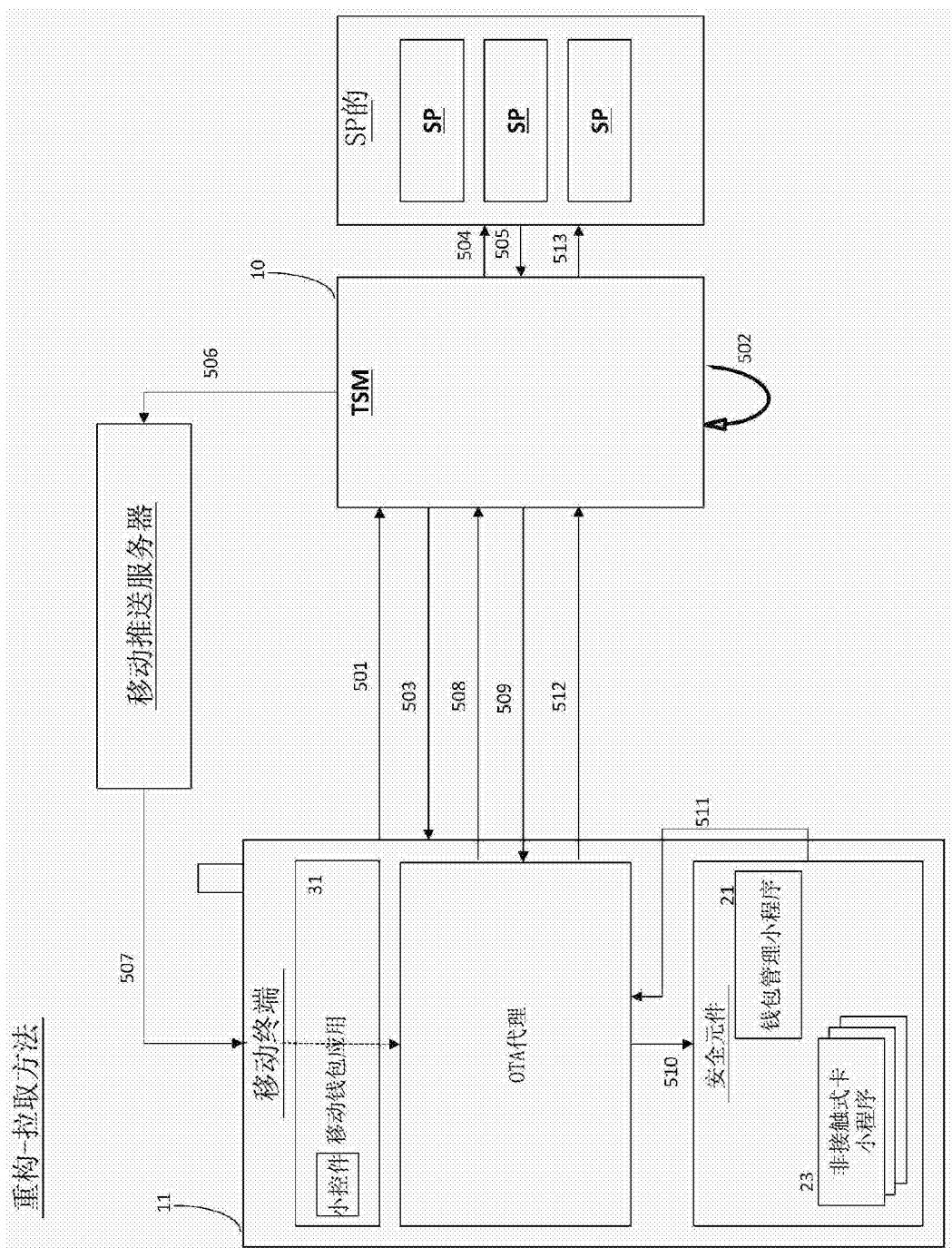


图5