(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 104992319 B
(45)授权公告日 2017.10.24

(21)申请号 201510292346.8

(22)申请日 2013.02.25

(65)同一申请的已公布的文献号
申请公布号 CN 104992319 A

(43)申请公布日 2015.10.21

(30)优先权数据
61/604,503 2012.02.28 US
13/523,637 2012.06.14 US

(62)分案原申请数据
201380000186.4 2013.02.25

(73)专利权人 谷歌公司
地址 美国加利福尼亚州

(72)发明人 萨雷尔·科布斯·约斯滕
约翰·约瑟夫
沙恩·亚历山大·法默

(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 周亚荣 安翔

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)
G06Q 20/02(2012.01)
G06Q 20/32(2012.01)

(56)对比文件
CN 102204299 A,2011.09.28,
US 2004250066 A1,2004.12.09,
US 2009307142 A1,2009.12.10,
US 5321242 A,1994.06.14,
US 5872849 A,1999.02.16,
US 6041123 A,2000.03.21,
US 8060449 B1,2011.11.15,

审查员 陈丽娜

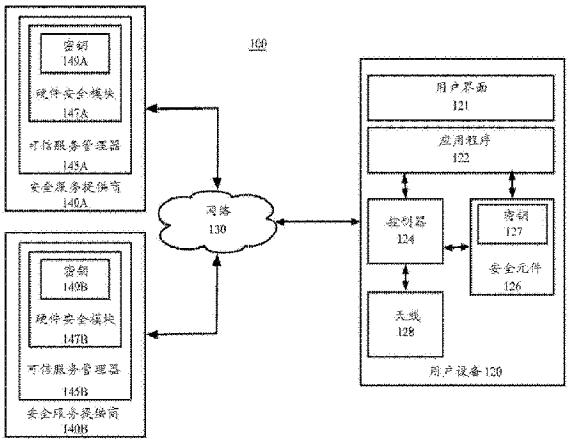
权利要求书4页 说明书10页 附图8页

(54)发明名称

便携式安全元件

(57)摘要

本发明涉及便携式安全元件。在TSM之间转移对安全元件的控制包括在TSM之间建立的区域主密钥，所述区域主密钥促进加密临时密钥。在启动控制的转移之前，TSM创建所述区域主密钥。一旦启动控制的转移，第一TSM就建立通信信道并从安全元件删除其密钥。所述第一TSM创建临时密钥，用在所述第一TSM与所述第二TSM之间建立的区域主密钥加密临时密钥。用设备标识符将所述加密的临时密钥传达到所述第二TSM。所述第二TSM使用所述区域主密钥解密所述临时密钥和使用所述设备标识符识别用户设备。新的TSM建立通信信道并从安全元件删除临时密钥。然后，新的TSM输入其密钥并将其密钥保存在安全元件中。



CN 104992319 B

1.一种用于转移对安全存储器的控制的计算机实现的方法,包括:

由计算机在第一安全服务提供商与第二安全服务提供商之间创建主密钥,其中所述主密钥促进将对安全存储器的控制从所述第一安全服务提供商转移到所述第二安全服务提供商;

由所述计算机接收将对所述安全存储器的控制从所述第一安全服务提供商转移到所述第二安全服务提供商的请求;

由所述计算机启动与所述安全存储器的安全通信信道,其中所述安全通信信道是使用驻留在所述安全存储器上的所述第一安全服务提供商已知的访问密钥建立的;

由所述计算机传达从所述安全存储器删除所述访问密钥的指令;

由所述计算机创建临时密钥;

由所述计算机将所述临时密钥传达到所述安全存储器;

由所述计算机使用在所述第一安全服务提供商与所述第二安全服务提供商之间建立的所述主密钥加密所述临时密钥;以及

由所述计算机将所述加密的临时密钥传达到所述第二安全服务提供商以供所述第二安全服务提供商访问所述安全存储器。

2.如权利要求1所述的计算机实现的方法,其中所述计算机是操作第一可信服务管理器的第一安全服务提供商。

3.如权利要求1所述的计算机实现的方法,其中创建所述主密钥包括:

由所述计算机生成所述主密钥的第一部分;

由所述计算机将所述主密钥的所述第一部分输入到驻留在所述第一安全服务提供商上的硬件安全模块中;

由所述计算机生成所述主密钥的第二部分;

由所述计算机将所述主密钥的所述第二部分输入到驻留在所述第一安全服务提供商上的所述硬件安全模块中;

由所述计算机在驻留在所述第一安全服务提供商上的所述硬件安全模块中组合所述第一和第二主密钥部分;以及

由所述计算机破坏各主密钥部分。

4.如权利要求1所述的计算机实现的方法,进一步包括:由所述计算机终止与所述安全存储器的所述安全通信信道。

5.如权利要求1所述的计算机实现的方法,进一步包括:由所述计算机将用户设备标识符传达到所述第二安全服务提供商,其中所述用户设备标识符能够由所述第二安全服务提供商用于识别所述安全存储器。

6.如权利要求1所述的计算机实现的方法,其中将所述加密的临时密钥传达到所述第二安全服务提供商以供所述第二安全服务提供商访问所述安全存储器包括:将所述加密的临时密钥传达到中介安全服务提供商。

7.如权利要求1所述的计算机实现的方法,其中所述第二安全服务提供商为中介安全服务提供商。

8.如权利要求7所述的计算机实现的方法,进一步包括:

由所述第二安全服务提供商使用在所述第一安全服务提供商与所述第二安全服务提

供商之间建立的所述主密钥解密所述临时密钥；

由所述第二安全服务提供商启动与所述安全存储器的安全通信信道，其中所述安全通信信道是使用由所述第二安全服务提供商解密的所述临时密钥建立的；

由所述第二安全服务提供商从所述安全存储器删除所述临时密钥；

由所述中介安全服务提供商创建第二临时密钥；

由所述第二安全服务提供商将所述第二临时密钥传达到所述安全存储器；

由所述中介安全服务提供商使用在所述第二安全服务提供商与第三安全服务提供商之间建立的第二主密钥加密所述第二临时密钥；以及

由所述中介安全服务提供商将所述加密的第二临时密钥传达到所述第三安全服务提供商以供所述第三安全服务提供商访问所述安全存储器。

9.如权利要求1所述的计算机实现的方法，其中所述安全存储器是安全元件。

10.如权利要求1所述的计算机实现的方法，其中所述安全服务提供商是可信服务管理器。

11.一种用于转移对安全存储器的控制的计算机实现的方法，其包括：

由计算机在第一安全服务提供商与中介安全服务提供商之间创建第一主密钥，其中所述第一主密钥促进将对安全存储器的控制从所述第一安全服务提供商转移到所述中介安全服务提供商；

由所述计算机在所述中介安全服务提供商与第二安全服务提供商之间创建第二主密钥，其中所述第二主密钥促进将对所述安全存储器的控制从所述中介安全服务提供商转移到所述第二安全服务提供商；

由所述计算机从所述第一安全服务提供商接收第一临时密钥以将对所述安全存储器的控制从所述第一安全服务提供商转移到所述中介安全服务提供商，其中所述第一临时密钥是由在所述第一安全服务提供商与所述中介安全服务提供商之间建立的所述第一主密钥加密的，并且其中所述第一临时密钥已被保存在所述安全存储器上；

由所述计算机使用在所述第一安全服务提供商与所述中介安全服务提供商之间建立的所述第一主密钥解密所述第一临时密钥；

由所述计算机启动与所述安全存储器的安全通信信道，其中所述安全通信信道是使用所述中介安全服务提供商解密的所述第一临时密钥建立的；

由所述计算机传达从所述安全存储器删除所述第一临时密钥的指令；

由所述计算机创建第二临时密钥；

由所述计算机将所述第二临时密钥传达到所述安全存储器；

由所述计算机使用在所述中介安全服务提供商与所述第二安全服务提供商之间建立的所述第二主密钥加密所述第二临时密钥；以及

由所述计算机将所述加密的第二临时密钥传达到所述第二安全服务提供商以供所述第二安全服务提供商访问所述安全存储器。

12.如权利要求11所述的计算机实现的方法，其中所述计算机是操作所述中介安全服务提供商的移动运营网络。

13.如权利要求11所述的计算机实现的方法，其中创建所述第一和第二主密钥中的一个包括：

由所述计算机生成所述主密钥的第一部分；

由所述计算机将所述主密钥的所述第一部分输入到硬件安全模块中；

由所述计算机生成所述主密钥的第二部分；

由所述计算机将所述主密钥的所述第二部分输入到所述硬件安全模块中；

由所述计算机在所述硬件安全模块中组合各主密钥部分；以及

由所述计算机破坏各主密钥部分。

14.如权利要求11所述的计算机实现的方法，进一步包括：由所述计算机终止与所述安全存储器的所述安全通信信道。

15.如权利要求11所述的计算机实现的方法，进一步包括：由所述计算机将用户设备标识符传达到所述第二安全服务提供商，其中所述用户设备标识符能够由所述第二安全服务提供商用于识别所述安全存储器。

16.一种用于转移对安全存储器的控制的系统，所述系统包括：

用于从第一安全服务提供商接收第一临时密钥以将对安全存储器的控制从所述第一安全服务提供商转移到中介安全服务提供商的装置，其中所述第一临时密钥是由在所述第一安全服务提供商与所述中介安全服务提供商之间建立的第一主密钥加密的；

用于启动与所述安全存储器的安全通信信道的装置，其中所述安全通信信道是使用所述第一临时密钥建立的，并且其中所述第一临时密钥驻留在所述安全存储器上；

用于创建第二临时密钥的装置，其中所述第二临时密钥被输入并保存在所述安全存储器上；以及

用于将所述第二临时密钥传达到第二安全服务提供商的装置，其中所述第二临时密钥是由在所述中介安全服务提供商与所述第二安全服务提供商之间建立的第二主密钥加密的。

17.如权利要求16所述的系统，进一步包括：

用于在所述第一安全服务提供商与所述中介安全服务提供商之间创建所述第一主密钥的装置，其中所述第一主密钥促进将对所述安全存储器的控制从所述第一安全服务提供商转移到所述中介安全服务提供商；以及

用于在所述中介安全服务提供商与所述第二安全服务提供商之间创建所述第二主密钥的装置，其中所述第二主密钥促进将对所述安全存储器的控制从所述中介安全服务提供商转移到所述第二安全服务提供商。

18.如权利要求17所述的系统，进一步包括：用于使用在所述第一安全服务提供商与所述中介安全服务提供商之间建立的所述第一主密钥解密所述第一临时密钥的装置。

19.如权利要求17所述的系统，进一步包括：用于在将所述第二临时密钥传达到所述第二安全服务提供商之前，使用在所述第二安全服务提供商与所述中介安全服务提供商之间建立的所述第二主密钥加密所述第二临时密钥的装置。

20.如权利要求17所述的系统，其中用于创建所述第一和第二主密钥中的一个的所述装置包括：

用于生成所述主密钥的第一部分的装置；

用于将所述主密钥的所述第一部分输入到硬件安全模块中的装置；

用于生成所述主密钥的第二部分的装置；

用于将所述主密钥的所述第二部分输入到所述硬件安全模块中的装置；

用于在所述硬件安全模块中组合各主密钥部分的装置；以及

用于破坏各主密钥部分的装置。

21.如权利要求16所述的系统，进一步包括：用于从所述安全存储器删除所述第一临时密钥的装置。

22.如权利要求21所述的系统，其中用于从所述安全存储器删除所述第一临时密钥的所述装置包括：用于将从所述安全存储器删除所述第一临时密钥的指令传达到所述安全存储器的装置。

23.如权利要求16所述的系统，进一步包括：用于终止与所述安全存储器的所述安全通信信道的装置。

24.如权利要求16所述的系统，进一步包括：用于将用户设备标识符传达到所述第二安全服务提供商的装置，其中所述用户设备标识符能够由所述第二安全服务提供商用于识别所述安全存储器。

25.如权利要求16所述的系统，其中所述安全存储器是安全元件，并且所述安全服务提供商是可信服务管理器。

26.一种用于转移对安全存储器的控制的系统，所述系统包括：

存储设备；以及

处理器，所述处理器被配置为执行存储在所述存储设备中的计算机可执行指令以转移对安全存储器的控制，所述计算机可执行指令包括：

用于从第一安全服务提供商接收第一临时密钥以将对安全存储器的控制从所述第一安全服务提供商转移到中介安全服务提供商的指令，其中所述第一临时密钥是由在所述第一安全服务提供商与所述中介安全服务提供商之间建立的第一主密钥加密的；

用于启动与所述安全存储器的安全通信信道的指令，其中所述安全通信信道是使用所述第一临时密钥建立的；

用于传达从所述安全存储器删除所述第一临时密钥的指令的指令；

用于创建第二临时密钥的指令；

用于将所述第二临时密钥传达到所述安全存储器的指令；以及

用于将所述第二临时密钥传达到第二安全服务提供商以供所述第二安全服务提供商访问所述安全存储器的指令，其中所述第二临时密钥是由在所述中介安全服务提供商与所述第二安全服务提供商之间建立的第二主密钥加密的。

27.如权利要求26所述的系统，所述计算机可执行指令进一步包括：用于终止与所述安全存储器的所述安全通信信道的指令。

28.如权利要求26所述的系统，所述计算机可执行指令进一步包括：用于将用户设备标识符传达到所述第二安全服务提供商的指令，其中所述用户设备标识符能够由所述第二安全服务提供商用于识别所述安全存储器。

29.如权利要求26所述的系统，其中所述安全存储器是安全元件，并且所述安全服务提供商是可信服务管理器。

便携式安全元件

[0001] 分案申请

[0002] 本申请属于申请日为2013年2月25日的中国发明专利申请201380000186.4的分案申请。

[0003] 相关申请案的交叉引用

[0004] 本申请要求于2012年6月14日提交并且标题为“Portable Secure Element”的第13/523,637号美国申请案的优先权，所述申请案要求于2012年2月28日提交并且标题为“Portable Secure Element”的第61/604,503号的美国临时专利申请案的优先权。上述指出的优先权申请案的完整内容以引用方式全部并入本文。

技术领域

[0005] 本公开一般涉及一种移动通信设备，更具体而言涉及用于使用户能够从可用的可信服务管理器(“TSMs”)中选择以完成安全交易、通信和其他任务的方法和系统。

[0006] 发明背景

[0007] 当前的近场通信(“NFC”)生态系统依赖于通常被称为“安全元件”的一个硬件，这个硬件被安装在通信设备上以为金融交易、交通票务、识别和认证、物理安全访问和其他功能提供安全操作环境。安全元件一般包括其自己的具有防干扰微处理器、存储器和操作系统的操作环境。此外，可信服务管理器(“TSM”)安装、供应和个性化安全元件。安全元件具有通常在制造时安装的一个或多个访问密钥。在具有安全元件的设备为最终用户所有时，对应的密钥由TSM共享以使得TSM可以建立安全元件的加密的安全信道来安装、供应和个性化安全元件。以这种方式，即使设备中的主CPU已被损害，安全元件也可以保持安全。

[0008] 当前的NFC系统的一个缺陷是在安全元件与TSM之间存在紧密耦合。对于当前的部署，只有一个TSM有权访问特定安全元件的密钥。因此，最终用户可以选择供应只由一个TSM提供的安全元件特征。这个TSM通常由设备的制造商选择。例如，在购买智能手机的移动网络运营商(“MNO”)(诸如Sprint或Verizon)而不是最终用户的指导下，智能手机制造商可以为智能手机选择TSM。因此，可用于最终用户的TSM特征可能不是最终用户的利益。作为一个实例，MNO可能只与一个付款提供商(诸如万事达信用卡或美国银行)有业务关系。那个TSM可以允许安全元件只从一个付款提供商被供应付款指示。因此，最终用户将无法从其他付款提供商(诸如VISA)访问服务。

发明概要

[0009] 在某些示例性方面，一种在TSM之间转移对安全元件的控制的方法和系统包括在TSM之间建立的区域主密钥，区域主密钥促进在转移过程期间加密临时密钥。在启动控制的转移之前，TSM建立协议和创建区域主密钥。一旦启动控制的转移，第一TSM就建立与安全元件的通信信道和删除其密钥。第一TSM创建临时密钥。用在第一TSM与第二TSM之间建立的区域主密钥加密临时密钥，并且用设备标识符将加密的临时密钥传达到第二TSM。第二TSM使用区域主密钥解密临时密钥和使用设备标识符识别用户设备。新的TSM建立与安全元件的

安全通信信道和删除临时密钥。然后，新的TSM输入其密钥和将其密钥保存在安全元件中。在一个示例性方面，第一TSM可以将对安全元件的控制转移到中介TSM，然后，中介TSM将对安全元件的控制转移到第二TSM。

[0010] 在考虑说明的示例性实施方案(其包括目前提供的执行本发明的最佳模式)的以下详细描述后，本领域的普通技术人员将显而易见示例性实施方案的这些和其他方面、目的、特征和优点。

[0011] 附图简述

[0012] 图1为描绘根据示例性实施方案的用于使用区域主密钥转移对安全元件的控制的系统的操作环境的方框图。

[0013] 图2为描绘根据示例性实施方案的用于针对安全元件的控制的设备介导的转移的系统的操作环境的方框图。

[0014] 图3为描绘根据示例性实施方案的用于使用区域主密钥转移对安全元件的控制的方法的方框流程图。

[0015] 图4为描绘根据示例性实施方案的用于创建区域主密钥的方法的方框流程图。

[0016] 图5为描绘根据示例性实施方案的用于从TSM A到TSM B转移对安全元件的控制的方法的方框流程图。

[0017] 图6为描绘根据示例性实施方案的用于针对安全元件的控制的设备介导的转移的方法的方框流程图。

[0018] 图7为描绘根据示例性实施方案的用于从TSM A到移动网络运营商TSM转移对安全元件的控制的方法的方框流程图。

[0019] 图8为描绘根据示例性实施方案的用于从移动网络运营商TSM到TSM B转移对安全元件的控制的方法的方框流程图。

具体实施方式

[0020] 概述

[0021] 示例性实施方案提供使用户能够使用在TSM之间建立的区域主密钥从一个TSM到另一个TSM转移对安全元件的控制的方法和系统。在启动控制的转移之前，TSM建立协议和创建区域主密钥。区域主密钥促进加密临时密钥，临时密钥用于从一个TSM到另一个TSM的控制转移。在示例性实施方案中，区域主密钥为共享的对称密钥。通过用预共享的对称密钥加密临时密钥，可能发生临时密钥交换。在替代示例性实施方案中，通过利用PKI基础设施，可能发生临时密钥交换，在PKI基础设施中源TSM(例如，TSM A)可以使用目标TSM(例如，TSM B)所公布的公共密钥加密临时密钥。在示例性实施方案中，可以使用由在TSM A与TSM B之间建立的区域主密钥加密的临时密钥将安全元件的控制从TSM A直接转移到TSM B。在替代示例性实施方案中，可以在使用一个或多个临时密钥将对安全元件的控制从TSM A转移到TSM B之前转移到中介机构，诸如移动网络运营商(“MNO”)TSM。在TSM A与MNO TSM之间建立的区域主密钥可以加密第一临时密钥，并且在MNO TSM与TSM B之间建立的区域主密钥可以加密第二临时密钥。在替代示例性实施方案中，单个临时密钥可以用于将控制从TSM A转移到MNO TSM以及到TSM B。

[0022] 一旦启动了控制的转移，TSM A就接收指令和同意将控制转移到第二TSM，例如，

TSM B或中介TSM(诸如MNO TSM)。TSM A建立与安全元件的通信信道和删除其密钥。TSM A创建临时密钥和将临时密钥保存到安全元件。TSM A用在TSM A与第二TSM之间建立的区域主密钥加密临时密钥。用设备标识符将加密的临时密钥传达到第二TSM。第二TSM使用区域主密钥解密临时密钥和使用设备标识符识别用户设备。

[0023] 第二TSM使用临时密钥建立与安全元件的通信信道。一旦建立通信信道,第二TSM就从安全元件删除临时密钥。然后,第二TSM输入其密钥和将其密钥保存在安全元件中,由此负责控制安全元件。在示例性实施方案中,第二TSM为中介TSM,然后使用相同的方法将控制转移到TSM B。在示例性实施方案中,中介TSM为MNO TSM。在替代示例性实施方案中,中介TSM为第三方实体,例如,Google。在又一替代示例性实施方案中,中介TSM为操作系统或操作系统提供商,诸如Android。

[0024] 在结合说明程序流程的图阅读的以下描述中将更详细地解释示例性实施方案的功能性。

[0025] 系统体系结构

[0026] 现在转向附图,其中贯穿图中相似的数字指示相似的(但未必完全相同的)元件,并且详细地描述示例性实施方案。

[0027] 图1为描绘根据示例性实施方案的用于使用区域主密钥转移对安全元件126的控制的系统的操作环境100的方框图。如图1中所描绘,示例性操作环境100包括被配置来经由一个或多个网络130彼此通信的用户设备系统120和两个或更多个安全服务提供商系统140。

[0028] 网络130包括电信装置,网络设备(包括设备120和设备140)可通过所述电信装置交换数据。例如,网络130可作为以下项或可能为以下项的一部分而实现:存储区域网(“SAN”)、个人区域网(“PAN”)、局域网(“LAN”)、城域网(“MAN”)、广域网(“WAN”)、无线局域网(“WLAN”)、虚拟专用网络(“VPN”)、内联网、互联网、蓝牙、NFC,或促进信号、数据和/或消息(一般被称为数据)的通信的任何其他适当的体系结构或系统。在替代示例性实施方案中,安全通信信道130可以包括蜂窝网络。

[0029] 在示例性实施方案中,用户设备系统120可以指的是可以经由电场、磁场或射频场在设备120与另一个设备(诸如智能卡(未图示)或阅读器(未图示))之间通信的智能设备。在示例性实施方案中,用户设备120具有处理能力,例如,存储容量/存储器和可以执行特定功能的一个或多个应用程序122。在示例性实施方案中,非接触式设备120含有操作系统(未图示)和用户界面121。示例性非接触式设备120包括智能电话;移动电话;个人数字助理(“PDAs”);移动计算设备,例如,上网本、平板计算机和iPad;膝上型计算机;以及在每种情况下具有处理和用户界面功能性的其他设备。

[0030] 非接触式设备120也包括安全元件126,其可以存在于可移动智能芯片或安全数字(“SD”)卡内或可以嵌入设备120上的固定芯片内。在某些示例性实施方案中,用户识别模块(“SIM”)卡可以能够托管安全元件126,例如,NFC SIM卡。安全元件126允许驻留在设备120上和可由设备用户访问的软件应用程序(未图示)安全地与安全元件126内的某些功能互动,同时保护存储在安全元件内的信息。安全元件126可以包括在其上运行的执行本文所述的功能性的应用程序(未图示)。

[0031] 安全元件126包括代表智能卡的部件,例如,加密处理器和随机发生器。在示例性

实施方案中，安全元件126在高度安全的系统中在智能卡操作系统(诸如JavaCard开放平台(“JCOP”)操作系统)控制的芯片上包括智能MX型NFC控制器124。在另一示例性实施方案中，安全元件126被配置来包括非EMV型非接触式智能卡作为可选实施方案。

[0032] 安全元件126与用户设备120中的控制器124和应用程序122通信。在示例性实施方案中，安全元件126能够存储加密的用户信息和只允许可信应用程序访问存储信息。控制器124与安全密钥127加密的应用程序互动，以在安全元件126中进行解密和安装。

[0033] 在示例性实施方案中，控制器124为NFC控制器。NFC控制器可以能够发送和接收数据、识别阅读器或智能卡、执行认证和加密功能，以及指导用户设备120将如何根据NFC指定的程序倾听来自阅读器/智能卡的传输或将用户设备120配置成各种省电模式。在替代示例性实施方案中，控制器124为能够执行类似的功能的蓝牙链路控制器或Wi-Fi控制器。

[0034] 应用程序122为存在于用户设备120上或在用户设备120上执行其操作的程序、功能、例行程序、小应用程序或类似实体。例如，应用程序122可以是以下应用程序中的一个或多个：离线付款应用程序、数字钱包应用程序、优惠券应用程序、优惠卡应用程序、另一增值应用程序、用户界面应用程序，或在非接触式设备120上操作的其他适合的应用程序。另外，安全元件126也可以包括安全非接触式软件应用程序，例如，离线付款或其他付款应用程序、安全形式的应用程序122、认证应用程序、付款供应应用程序，或使用安全元件的安全功能性的其他适合的应用程序。

[0035] 用户设备120经由天线128与阅读器/智能卡通信。在示例性实施方案中，一旦已经激活和优先考虑用户设备应用程序122，控制器124就通知用户设备120准备交易的状态。控制器124通过天线128输出无线电信号，或倾听来自阅读器/智能卡的无线电信号。

[0036] 安全服务提供商140充当帮助服务提供商安全地分配和管理应用程序和服务(诸如NFC非接触式应用程序服务)的中介机构。示例性安全服务提供商140包括Gemalto和First Data。安全服务提供商140的可信服务管理器(“TSM”)145通常托管应用程序并且将应用程序安装和供应到用户设备的安全元件126上。每个TSM 145可以接收、存储和利用驻留在用户设备120上的安全元件126的密钥149。在示例性实施方案中，将一个或多个密钥149存储在硬件安全模块(“HSM”)中。通过具有密钥149，TSM 145可以经由安全加密的通信信道访问安全元件126以在安全元件126内安装、供应和定制应用程序。在示例性实施方案中，密钥149允许只通过TSM 147使用当前的访问密钥149来访问和控制安全元件126。例如，一旦将对安全元件126的控制从TSM A 147A转移到TSM B 147B，只有TSM B 147可以使用TSM B密钥149B访问和控制安全元件126。TSM A密钥149A将不允许TSM A 145A访问和控制安全元件126。

[0037] 在某些示例性实施方案中，安全服务提供商140在与安全元件126通信时绕过驻留在用户设备120上的控制器124。例如，在某些UICC/SIM安全元件中，安全服务提供商140经由安装在用户设备120上的无线电CPU(未图示)与安全元件126通信。因此，在某些示例性实施方案中，在将应用程序供应在安全元件126上期间，控制器124的参与可以是可选的。在某些示例性实施方案中，主CPU(未图示)与无线电CPU(未图示)彼此互动以协调访问控制安全元件126。

[0038] 图2为描绘根据替代示例性实施方案的用于针对安全元件的控制的设备介导的转移的系统的操作环境的方框图。示例性操作环境200包括与系统100相同的许多部件，包括

被配置来经由一个或多个网络140彼此通信的用户设备系统120和两个或更多个安全服务提供商系统140。示例性操作环境200也包括移动网络运营商(“MNO”)系统210。

[0039] 在示例性实施方案中,MNO系统210为在将控制从一个TSM 145转移到另一个TSM 145期间充当中介的第三方系统。示例性MNO 210包括TSM 215和一个或多个密钥219。如先前所述,TSM 215和密钥219以与驻留在安全服务提供商140上的TSM 145和密钥149类似的方式运行。在示例性实施方案中,用户设备120经由MNO 210访问网络130。示例性MNO 210包括Verizon、Sprint和AT&T。MNO 210可以经由移动网络(未示出),诸如3G或4G移动通信网络为网络130提供对用户设备120的访问。在替代示例性实施方案中,用户设备120可以经由其他机制,例如,与互联网提供商相关的Wi-Fi、NFC或蓝牙访问网络130。

[0040] 如本说明书中被提及,MNO TSM 215为中介TSM。在示例性实施方案中,中介TSM为MNO TSM 215。在替代示例性实施方案中,中介TSM为第三方实体(诸如Google)或操作系统/操作系统提供商(诸如Android)。在该示例性实施方案中,MNO系统210可以使用任何网络130与用户设备通信,并且中介TSM 215可以经由Wi-Fi与用户设备120通信。

[0041] 下文将参照本文所述的方法进一步详细地描述图1至图2中所示的部件。

[0042] 系统过程

[0043] 图3为描绘根据示例性实施方案的用于使用区域主密钥转移对安全元件126的控制的方法的方框流程图。参照图1中所示的部件描述方法300。

[0044] 在方框305中,TSM A 145A和TSM B 145B创建区域主密钥以促进控制的转移。下文参照在图4中所述的方法更详细地描述创建区域主密钥的方法。

[0045] 图4为描绘根据示例性实施方案的用于创建区域主密钥的方法的方框流程图,如图3的方框305中提及。参照图1中所示的部件描述方法305。

[0046] 在方框410中,TSM A 145A和TSM B 145B同意创建密钥交换区。在示例性实施方案中,在启动对驻留在用户设备120上的安全元件126的控制的转移之前的时间,离线地发生TSM A 145A与TSMB 145B之间的协议。例如,TSM A 145A和TSM B 145B可以创建协议以允许转移对安全元件126的控制,其中TSM A 145A和TSM B145B同意创建区域主密钥以促进此类转移。在示例性实施方案中,区域主密钥可以用于促进在创建密钥后的任何时间多个用户设备从TSMA 145A转移到TSM B 145B,或从TSM B 145B转移到TSM A 145A。

[0047] 在方框420中,TSM A 145A和TSM B 145B生成共享的区域主密钥的第一部分。在示例性实施方案中,在三个分开的部分中创建区域主密钥以便HSM 147组合这些部分。在替代示例性实施方案中,在单个部分中创建区域主密钥。在该实施方案中,可以跳过方框440至方框470中所述的方法。在又一替代示例性实施方案,在多于三个部分中创建区域主密钥。在该实施方案中,可以根据需要重复方框420至方框470中所述的方法。在又一替代示例性实施方案中,在两个部分中创建区域主密钥。在该实施方案中,可以跳过方框460至方框470中所述的方法。

[0048] 在方框430中,将区域主密钥的第一部分注入到TSM A 145A和TSM B 145B的HSM 147。在示例性实施方案中,将区域主密钥部分注入到TSM A 145A的HSM 147A和TSM B 145B的HMS 147B中。在示例性实施方案中,TSM 145输入区域主密钥部分和将这些部分存储在HSM 147中。在示例性实施方案中,一旦将区域主密钥的所有部分存储在HSM 147中,HSM 147就组合这些部分。

[0049] 在方框440中，TSM A 145A和TSM B 145B生成共享的区域主密钥的第二部分。

[0050] 在方框450中，将区域主密钥的第二部分注入到TSM A 145A和TSM B 145B的HSM 147中。在示例性实施方案中，TSM 145输入区域主密钥部分和将这些部分存储在HSM 147中。在示例性实施方案中，一旦将区域主密钥的所有部分存储在HSM 147中，HSM 147就组合这些部分。

[0051] 在方框460中，TSM A 145A和TSM B 145B生成共享的区域主密钥的第三部分。在示例性实施方案中，在三个部分中生成区域主密钥。

[0052] 在方框470中，将区域主密钥的第三部分注入到TSM A 145A和TSM B 145B的HSM 147中。在示例性实施方案中，TSM 145输入区域主密钥部分和将这些部分存储在HSM 147中。在示例性实施方案中，一旦将区域主密钥的所有部分存储在HSM 147中，HSM 147就组合这些部分。

[0053] 在方框480中，将区域主密钥组合在TSM A 145A和TSM B145B的HSM 147内。在示例性实施方案中，创建、输入区域主密钥的三个部分并将这些部分存储在TSM A 145A和TSM B 145B的HSM147中，组合这些部分以创建单个密钥。

[0054] 在方框490中，破坏区域主密钥部分。在示例性实施方案中，一旦组合区域主密钥部分并且创建单个密钥，注入到TSM A 145A和TSM B 145B的HSM 147中的部分各自从HSM 147中被移除并被破坏。

[0055] 从方框490，方法进入图3中的方框310。

[0056] 回到图3，在方框310中，通过TSM A 145A控制驻留在用户设备120上的安全元件126。在示例性实施方案中，TSM A 145A可以使用访问密钥149A访问和控制安全元件126。在示例性实施方案中，可以通过TSM B 145B控制安全元件126，其中将控制从TSM B 145B转移到TSM A 145A。

[0057] 在方框315中，将对安全元件126的控制从TSM A 145A转移到TSM B 145B。下文参照图5中所述的方法更详细地描述将对安全元件126的控制从TSM A 145A转移到TSM B 145B方法。

[0058] 图5为描绘根据示例性实施方案的用于将对安全元件126的控制从TSM A 145A转移到TSM B 145B的方法的方框流程图，如在图3的方框315中提及。参照图1中所示的部件描述方法315。

[0059] 在方框505中，用户(未图示)启动将对安全元件126的控制从TSM A 145A转移到TSM B 145B。在示例性实施方案中，用户可以经由用户界面121访问驻留在用户设备上的应用程序122以启动控制的转移。在替代示例性实施方案中，用户可以通过登记金融卡启动控制的转移，金融卡由安全服务提供商B 140B在用户的数字钱包应用程序中管理。在又一替代示例性实施方案，可以自动地启动控制的转移，用户试图使用用户设备120进行金融付款，其中金融卡由安全服务提供商B 140B管理。

[0060] 在方框510中，驻留在用户设备120上的应用程序122接收用户转移对安全元件126的控制的请求。在示例性实施方案中，应用程序122为安全元件126可携带服务应用程序。

[0061] 在方框515中，应用程序122授权将控制从TSM A 145A转移到TSM B 145B和指示TSM A 145A将对安全元件126的控制转移到TSM B 145B。在示例性实施方案中，安全元件可携带服务应用程序122经由网络130将指令传达到TSM A 145A。

[0062] 在方框520中，TSM A 145A接收指令和同意将对安全元件126的控制转移到TSM B 145B。在示例性实施方案中，TSM A 145A已经预先与TSM B 145B建立关于在TSM之间转移对安全元件126的控制的协议。TSM已经预先创建区域主密钥以促进此类控制的转移。在示例性实施方案中，一旦TSM A 145A接收转移控制的指令，TSM A 145A就会在同意转移控制之前确认在TSM之间的转移协议的存在。

[0063] 在方框525中，TSM A 145A使用存储在安全元件126中的TSM A 145A的现有访问密钥启动与安全元件126的安全通信信道。在示例性实施方案中，安全通信信道是经由网络130。

[0064] 在方框530中，TSM A 145A从安全元件126删除所有TSM A密钥149A。在示例性实施方案中，从安全元件126移除TSM A密钥149A确保TSM A 145A将不再控制或访问安全元件126。

[0065] 在方框535中，TSM A 145A创建临时密钥。在示例性实施方案中，临时密钥不同于先前从安全元件126删除的TSM A密钥149。在示例性实施方案中，临时密钥提供从一个TSM 145到另一个TSM 145的控制的转移。

[0066] 在方框540中，TSM A 145A将临时密钥注入到安全元件126中。在示例性实施方案中，TSM A 145A输入临时密钥并将临时密钥存储在安全元件126中以促进将控制转移到TSM B 145B。

[0067] 在方框545中，TSM A 145A用在TSM A 145A与TSM B145B之间建立的区域主密钥加密临时密钥。在示例性实施方案中，区域主密钥由TSM A 145A和TSM B 145B共享和在方框305中被创建。

[0068] 在方框550中，TSM A 145A将临时密钥与用户设备120标识符一起传达到TSM B 145B，用在TSM A 145A与TSM B 145之间建立的区域主密钥加密临时密钥。在示例性实施方案中，用户设备120标识符可以在访问安全元件126和建立控制之前由TSM B 145B用于识别用户设备120和安全元件126。

[0069] 然后，方法进入图3中的方框320。

[0070] 回到图3，在方框320中，TSM B 145B将临时密钥注入到HSM147B中，用从TSM A 145A接收的区域主密钥加密临时密钥。在示例性实施方案中，TSM B 145B输入临时密钥并将临时密钥保存到HSM 147B中，用区域主密钥加密临时密钥。

[0071] 在方框325中，TSM B 145B使用在TSM A 145A与TSM B 145B之间建立的区域主密钥解密临时密钥。

[0072] 在方框330中，TSM B 145B使用TSM A 145A传达的设备标识符识别用户设备120。在示例性实施方案中，TSM B 145B联络MNO210以使用设备标识符识别用户设备120。在示例性实施方案中，MNO210促进识别用户设备120和安全元件126。

[0073] 在方框335中，TSM B 145B使用临时密钥建立与安全元件126的安全通信信道。在示例性实施方案中，安全通信信道是经由网络130。

[0074] 在方框340中，TSM B 145B从安全元件126删除临时密钥和注入TSM B密钥149B。在示例性实施方案中，TSM B 145B输入TSMB密钥149B和将TSM B密钥149B保存到安全元件126以负责控制安全元件126。在示例性实施方案中，一旦TSM B 145B从安全元件移除临时密钥，TSM A 145A就可以不再访问或控制安全元件。

[0075] 在方框345中，TSM B 145B负责控制安全元件126。在示例性实施方案中，在TSM B 145B输入TSM B密钥149B并将TSM B密钥149B保存到安全元件后的任何适合的时间，终止通信信道。

[0076] 从方框345，方法300结束。

[0077] 图6为描绘根据示例性实施方案的用于针对安全元件126的控制的设备介导的转移的方法的方框流程图。参照图2中所示的部件描述方法600。

[0078] 在方框605中，MNO TSM 215为TSM A 145A和TSM B建立单独的区域主密钥。在示例性实施方案中，可以用先前参照图3至图4的方框305所述的方式执行图6的方框605，除了MNO TSM 215为TSM A 145A和TSM B 145B中的每个单独地执行方法305之外。在示例性实施方案中，MNO TSM 215为中介，其可以包括MNO、第三方实体、操作系统、操作系统提供商，或促进将对安全元件126的控制从一个TSM 145转移到另一个TSM 145的其他TSM。

[0079] 在方框610中，TSM A 145A控制驻留在用户设备120上的安全元件126。在示例性实施方案中，TSM A 145A可以使用访问密钥149A访问和控制安全元件126。在示例性实施方案中，TSM B 145B可以控制安全元件126，其中将控制从TSM B 145B转移到TSM A 145A。

[0080] 在方框615中，将对安全元件126的控制从TSM A 145A转移到MNO TSM 215。下文参照图7中所描述的方法更详细地描述将对安全元件126的控制从TSM A 145A转移到MNO TSM 215的方法615。

[0081] 图7为描绘根据示例性实施方案的用于将对安全元件126的控制从TSM A 145A转移到MNO TSM 215的方法的方框流程图，如图6的方框615中提及。参照图1至图2中所示的部件描述方法615。

[0082] 在示例性实施方案中，可以用先前参照图5的方框505至方框550所述的方式执行图7的方框505至方框550，除了TSM A 145A将对安全元件126的控制转移到MNO TSM 215而不是TSM B 145B之外。在示例性实施方案中，根据先前参照图5的方框505至方框550所述的方法，通过创建由在TSM A 145A与MNO TSM 215之间建立的区域主密钥加密的第一临时密钥，促进将控制从TSM A 145A转移到MNO TSM 215。

[0083] 从图7的方框550，方法615进入图6的方框620。

[0084] 回到图6，在方框620中，将对安全元件126的控制从MNO TSM 215转移到TSM B 145B。下文参照图8中所述的方法更详细地描述从MNO TSM 215到TSM B 145B转移对安全元件126的控制的方法620。

[0085] 图8为描绘根据示例性实施方案的用于从MNO TSM 215到TSM B 145B转移对安全元件126的控制的方法的方框流程图，如图6的方框620中提及。参照图1至图2中所示的部件描述方法620。

[0086] 在方框805中，MNO TSM 215使用在MNO TSM 215与TSM A 145A之间建立的区域主密钥解密第一临时密钥。

[0087] 在方框810中，MNO TSM 215使用设备标识符识别用户设备120。

[0088] 在示例性实施方案中，可以用先前参照图5的方框525至方框550所述的方式执行图8的方框525至方框550，除了是MNO TSM 215而不是TSM A 145A将对安全元件126的控制转移到TSM B 145B之外。在示例性实施方案中，根据先前参照图5的方框525至方框550所述的方法，通过创建由在MNO TSM 215与TSM B 145B之间建立的区域主密钥加密的第二临时

密钥，促进将控制从MNO TSM 215转移到TSM B 145B。

[0089] 从图8的方框550，方法620进入图6的方框625。

[0090] 回到图6，在方框625中，TSM B 145B使用在MNO TSM 215与TSM B 145B之间建立的区域主密钥解密第二临时密钥。

[0091] 在方框630中，TSM B 145B使用由MNO TSM 215传达的设备标识符识别用户设备120。

[0092] 在方框635中，TSM B 145B使用第二临时密钥建立与安全元件126的安全通信信道。在示例性实施方案中，安全通信信道是经由网络130。

[0093] 在方框640中，TSM B 145B从安全元件126删除第二临时密钥。在示例性实施方案中，一旦TSM B 145B从安全元件126移除第二临时密钥，MNO TSM 215就可以不再访问或控制安全元件。

[0094] 在方框645中，TSM B 145B注入TSM B密钥149B。在示例性实施方案中，TSM B 145B输入TSM B密钥149B并将TSM B密钥149B保存到安全元件126以负责控制安全元件126。

[0095] 在方框650中，TSM B 145B负责控制安全元件126。在示例性实施方案中，在TSM B 145B输入TSM B密钥149B并将TSM B密钥149B保存到安全元件后的任何适合的时间，终止通信信道。

[0096] 从方框650，方法600结束。

[0097] 概要

[0098] 可以允许用户限制或以其他方式影响本文公开的特征的操作。例如，用户可以被提供机会来决定采用或决定退出某些数据的集合或使用或某些特征的激活。另外，用户可以被提供机会来改变使用特征的方式，包括对于用户可能具有关于保密性的顾虑的情形。也可以将指令提供到用户以通知用户关于使用信息(包括个人可识别的信息)的策略，和每个用户可能影响使用信息的方式。因此，需要时，通过接收相关广告、提议或其他信息，信息可以用于有益于用户，而不具有泄露个人信息或用户的身份的风险。

[0099] 示例性实施方案的一个或多个方面可以包括实施本文描述和说明的功能的计算机程序，其中在计算机系统中实施计算机程序，计算机系统包括存储在机器可读介质中的指令和执行指令的处理器。然而，应显而易见，可能在计算机程序设计中存在实施示例性实施方案的许多不同的方式，并且不应将示例性实施方案理解为限于任何一组计算机程序指令。此外，熟练的程序设计员将能够写入此类计算机程序以基于应用文本中的附加流程图和相关描述实施实施方案。因此，一组特定的程序代码指令的公开不被认为是充分理解如何制造和使用示例性实施方案所必需的。此外，不应将对计算机执行的动作的任何提及理解为由单个计算机执行，因为超过一个的计算机可以执行动作。

[0100] 在先前提供的实施方案中所述的示例性系统、方法和方框是说明性的，并且在替代实施方案中，在不同的示例性方法之间，某些方框可以用不同的顺序被执行、彼此平行、被完全省略和/或组合，和/或可以在不脱离本发明的范围和精神的情况下执行某些额外的方框。因此，在本文所述的本发明中包括此类替代实施方案。

[0101] 本发明可以用于执行上文所述的方法和处理功能的计算机硬件和软件。如本领域的普通技术人员所了解，可以在可编程计算机、计算机可执行软件或数字电路中实施本文所述的系统、方法和程序。软件可以存储在计算机可读介质上。例如，计算机可读介质可以

包括软盘、RAM、ROM、硬盘、可移动介质、闪存、存储棒、光学介质、磁光介质、CD-ROM等。数字电路可以包括集成电路、门阵列、构建块逻辑、现场可编程门阵列(“FPGA”)等。

[0102] 尽管上文已经详细地描述本发明的具体实施方案，但是描述仅仅是为了说明。除上文所述的以外，在不脱离以下权利要求书中定义的本发明的精神和范围的情况下，本领域的普通技术人员可以进行对应于示例性实施方案的所公开方面的方框和部件的各种修改以及等效方框和部件，权利要求书的范围应被授予最宽泛的解释以便包括此类修改和等效结构。

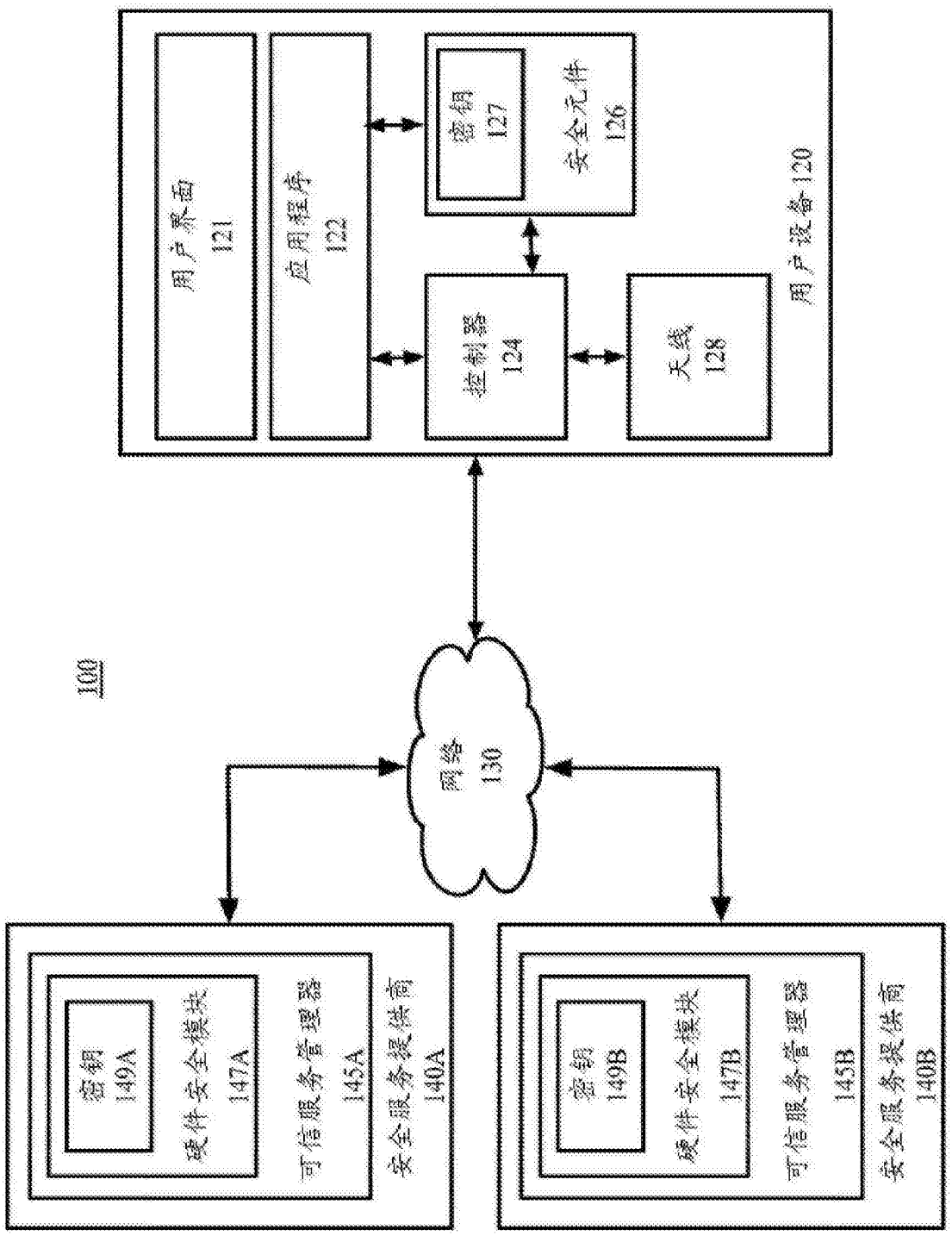

100
用户设备120
用户界面
121
应用程序
122
密钥
127
安全元件
126
控制器
124
天线
128
网络
130
安全服务提供商
140A
可信服务管理器
145A
硬件安全模块
147A
密钥
149A
安全服务提供商
140B
可信服务管理器
145B
硬件安全模块
147B
密钥
149B

图1

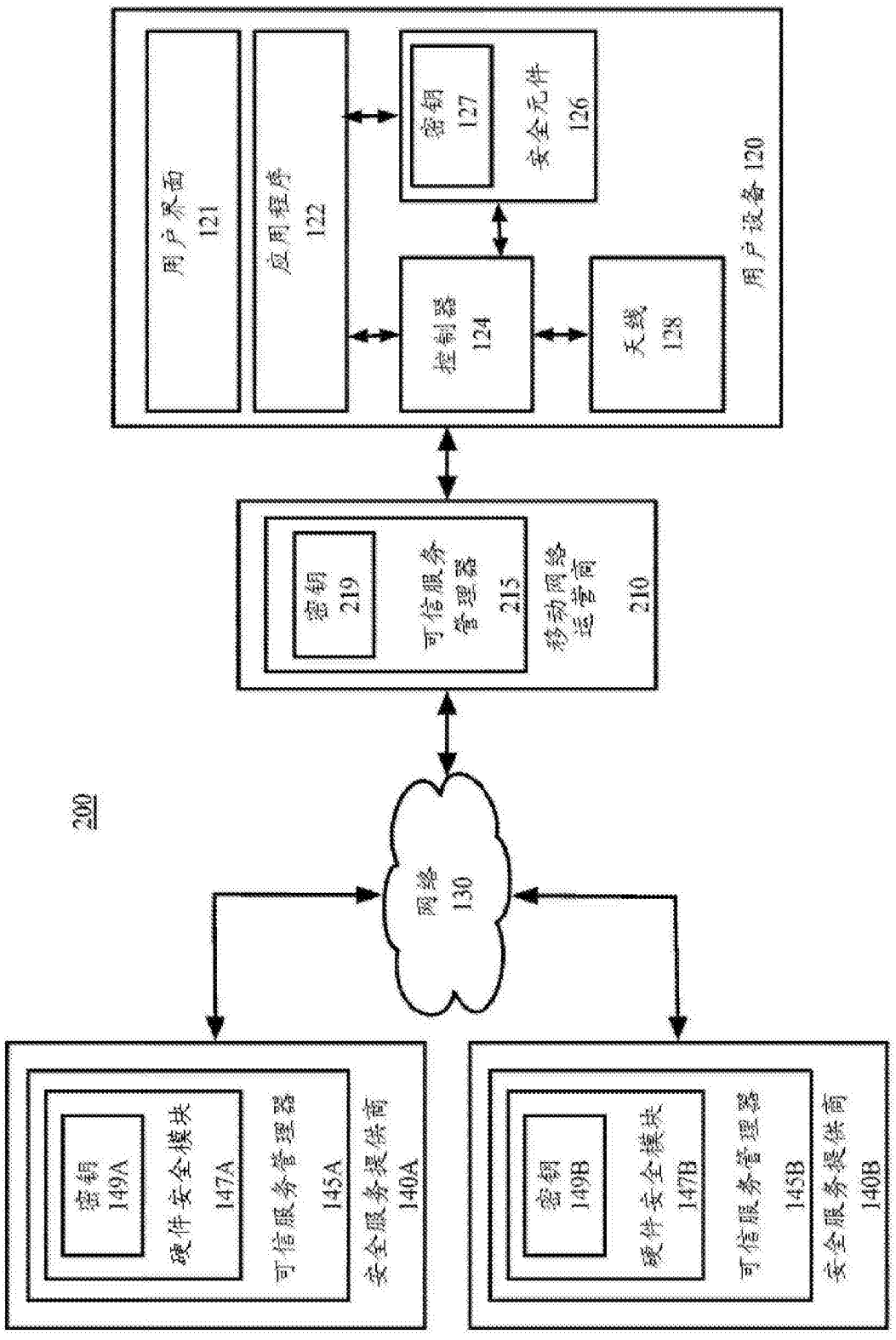

200
用户设备 120
用户界面 121
应用程序 122
密钥 127
安全元件 126
控制器 124
天线 128
移动网络运营商 210
密钥 219
可信服务管理器 215
网络 130
安全服务提供商 140A
密钥 149A
硬件安全模块 147A
可信服务管理器 145A
安全服务提供商 140B
密钥 149B
硬件安全模块 147B
可信服务管理器 145B

图2

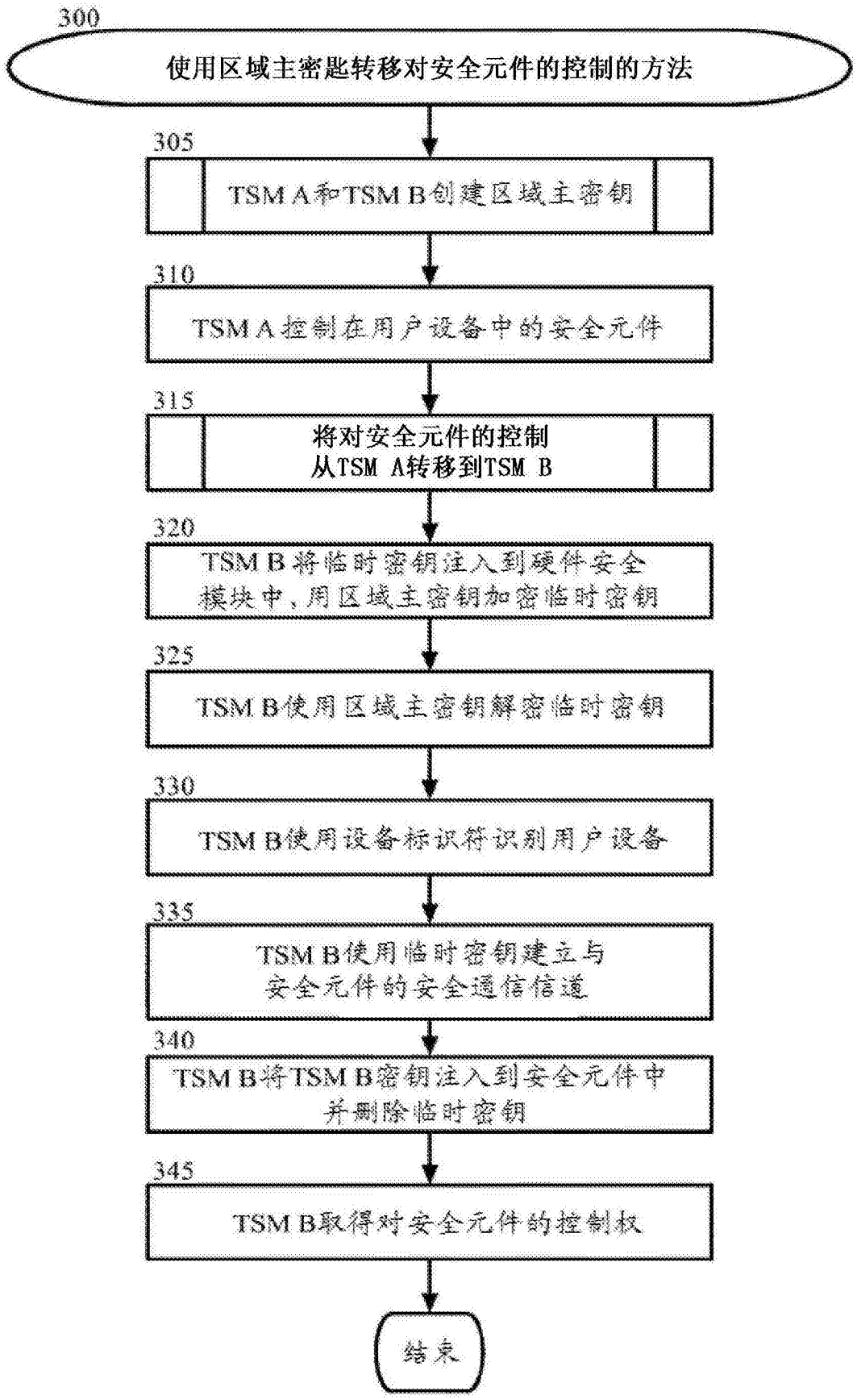

300
使用区域主密匙转移对安全元件的控制的方法
305
TSM A和TSM B创建区域主密钥
310
TSM A控制在用户设备中的安全元件
315
将对安全元件的控制
从TSM A转移到TSM B
320
TSM B将临时密钥注入到硬件安全
模块中，用区域主密钥加密临时密钥
325
TSM B使用区域主密钥解密临时密钥
330
TSM B使用设备标识符识别用户设备
335
TSM B使用临时密钥建立与
安全元件的安全通信信道
340
TSM B将TSM B密钥注入到安全元件中
并删除临时密钥
345
TSM B取得对安全元件的控制权
结束

图3

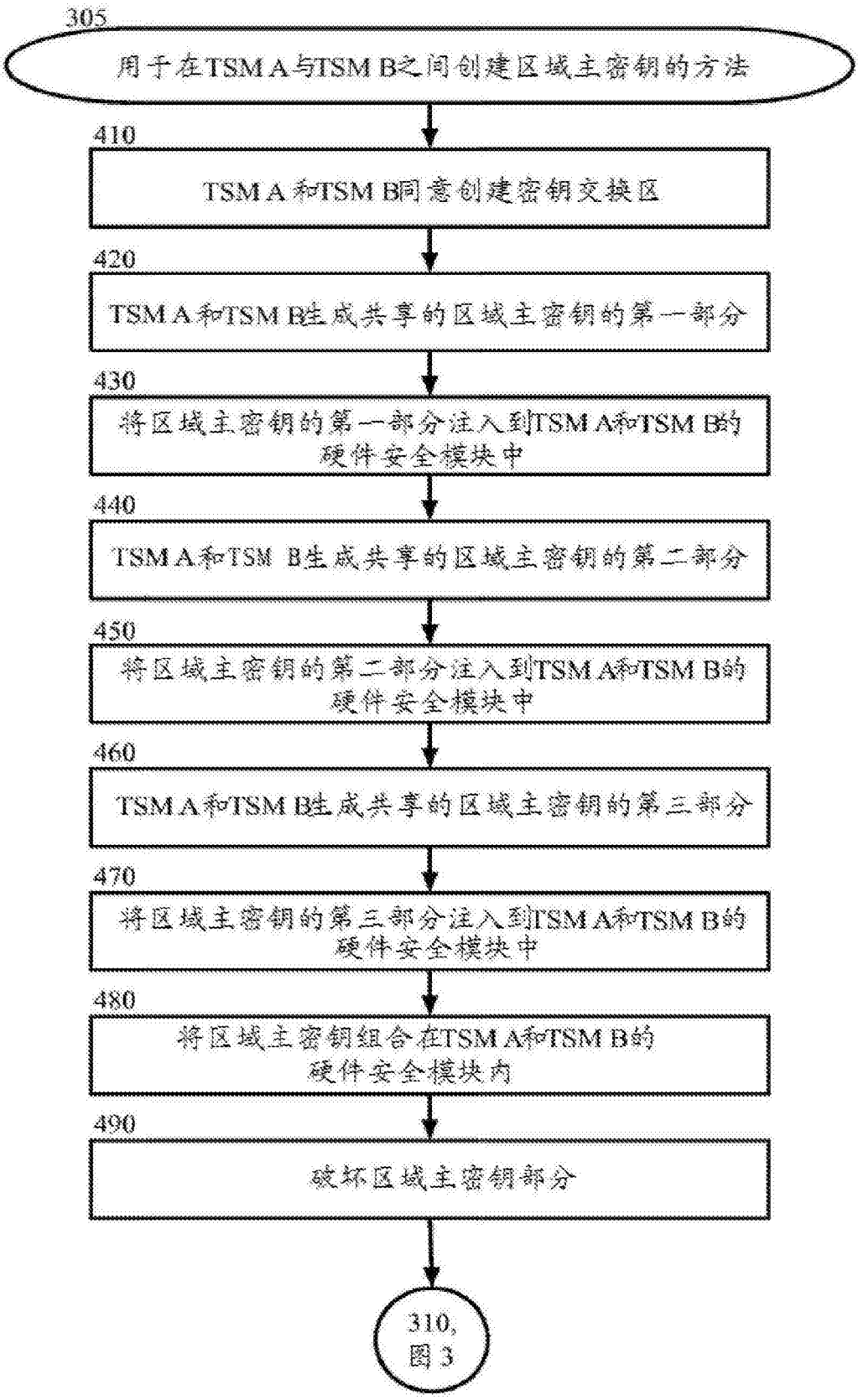

305
用于在TSM A与TSM B之间创建区域主密钥的方法
410
TSM A和TSM B同意创建密钥交换区
420
TSM A和TSM B生成共享的区域主密钥的第一部分
430
将区域主密钥的第一部分注入到TSM A和TSM B的硬件安全模块中
440
TSM A和TSM B生成共享的区域主密钥的第二部分
450
将区域主密钥的第二部分注入到TSM A和TSM B的硬件安全模块中
460
TSM A和TSM B生成共享的区域主密钥的第三部分
470
将区域主密钥的第三部分注入到TSM A和TSM B的硬件安全模块中
480
将区域主密钥组合在TSM A和TSM B的硬件安全模块内
490
破坏区域主密钥部分
310,
图 3

图4

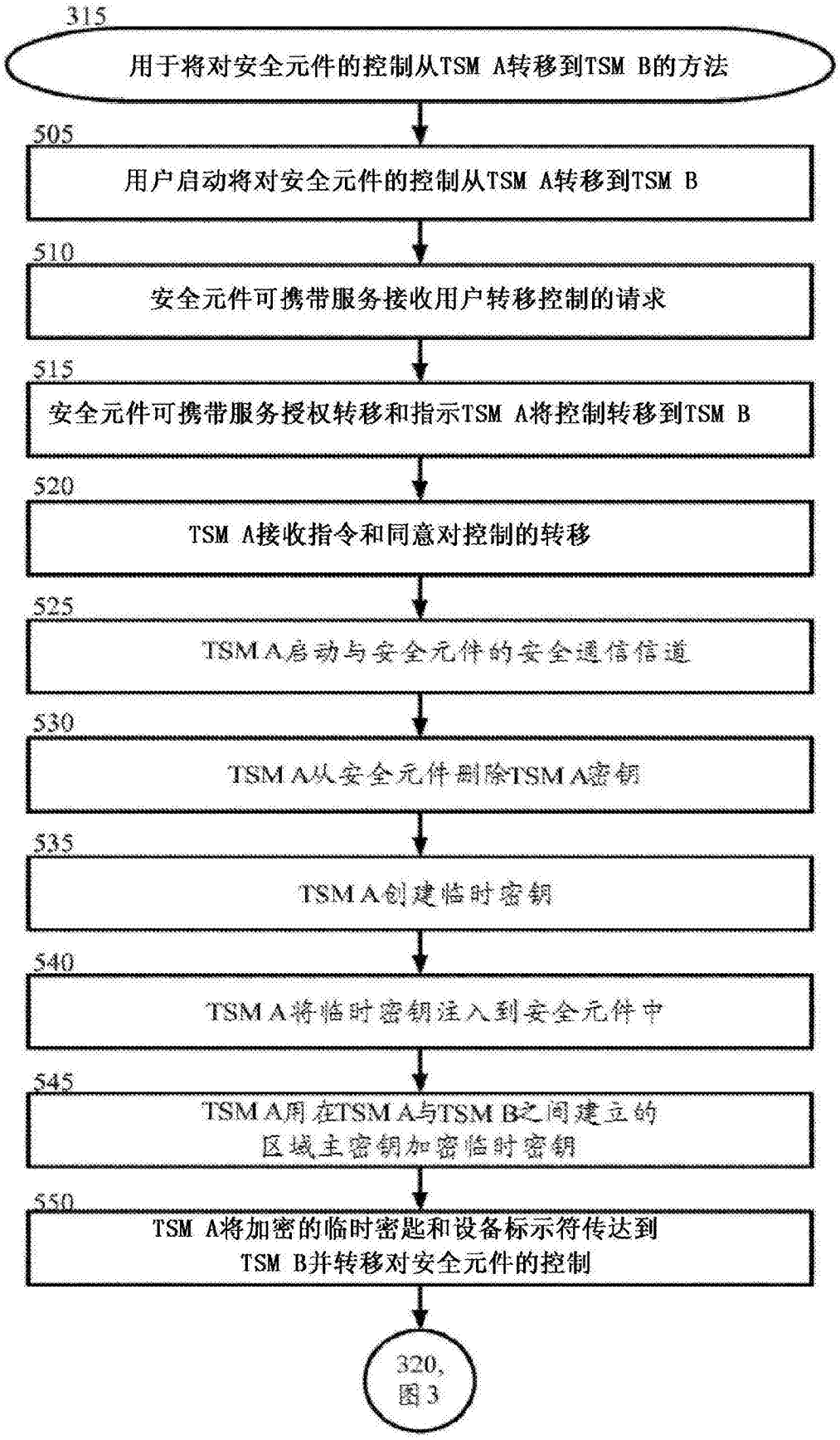

315
用于将对安全元件的控制从TSM A转移到TSM B的方法
505
用户启动将对安全元件的控制从TSM A转移到TSM B
510
安全元件可携带服务接收用户转移控制的请求
515
安全元件可携带服务授权转移和指示TSM A将控制转移到TSM B
520
TSM A接收指令和同意对控制的转移
525
TSM A启动与安全元件的安全通信信道
530
TSM A从安全元件删除TSM A密钥
535
TSM A创建临时密钥
540
TSM A将临时密钥注入到安全元件中
545
TSM A用在TSM A与TSM B之间建立的
区域主密钥加密临时密钥
550
TSM A将加密的临时密匙和设备标示符传达到
TSM B并转移对安全元件的控制
320,
图3

图5

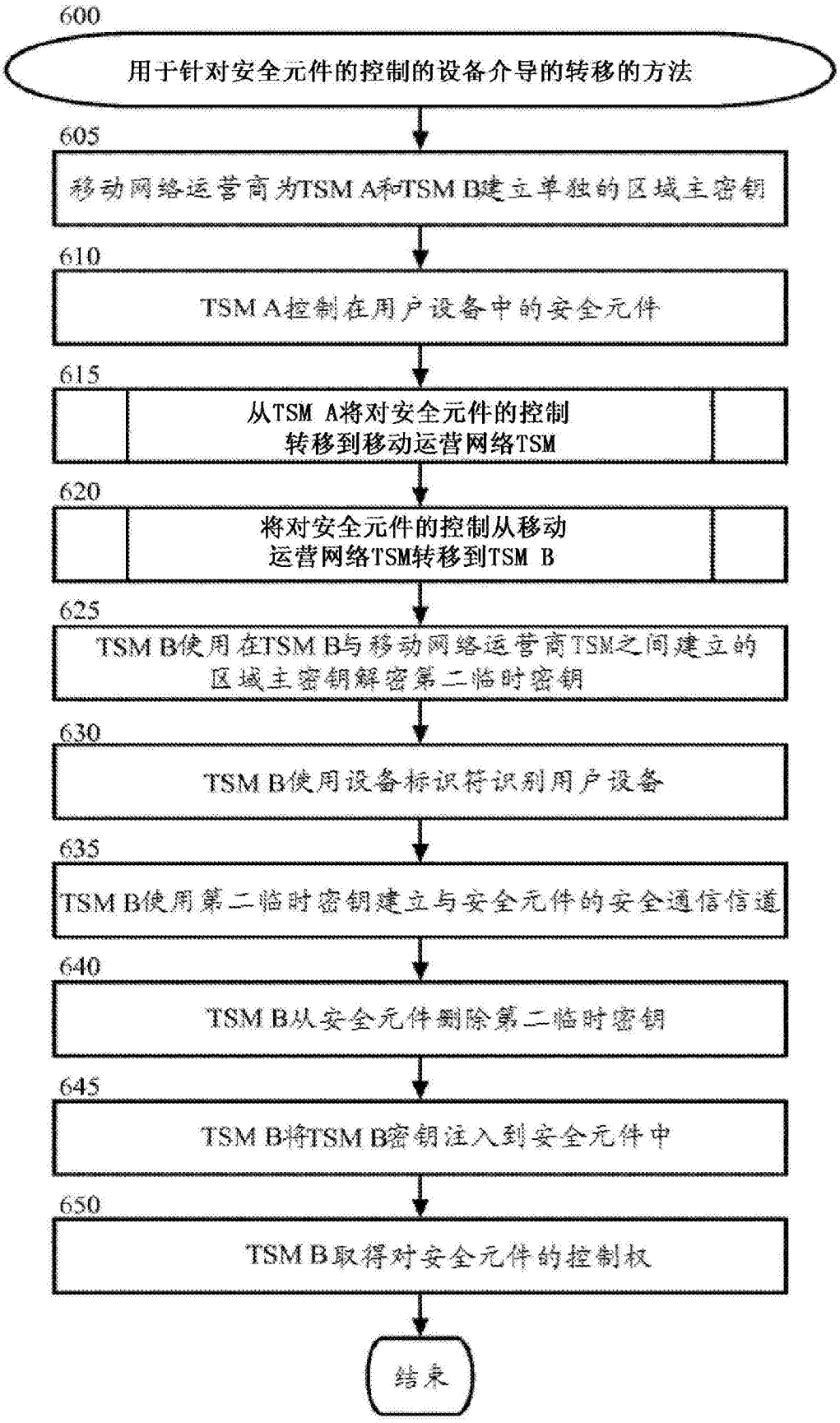

600
用于针对安全元件的控制的设备介导的转移的方法
605
移动网络运营商为TSM A和TSM B建立单独的区域主密钥
610
TSM A控制在用户设备中的安全元件
615
从TSM A将对安全元件的控制
转移到移动运营网络TSM
620
将对安全元件的控制从移动
运营网络TSM转移到TSM B
625
TSM B使用在TSM B与移动网络运营商TSM之间建立的
区域主密钥解密第二临时密钥
630
TSM B使用设备标识符识别用户设备
635
TSM B使用第二临时密钥建立与安全元件的安全通信信道
640
TSM B从安全元件删除第二临时密钥
645
TSM B将TSM B密钥注入到安全元件中
650
TSM B取得对安全元件的控制权
结束

图6

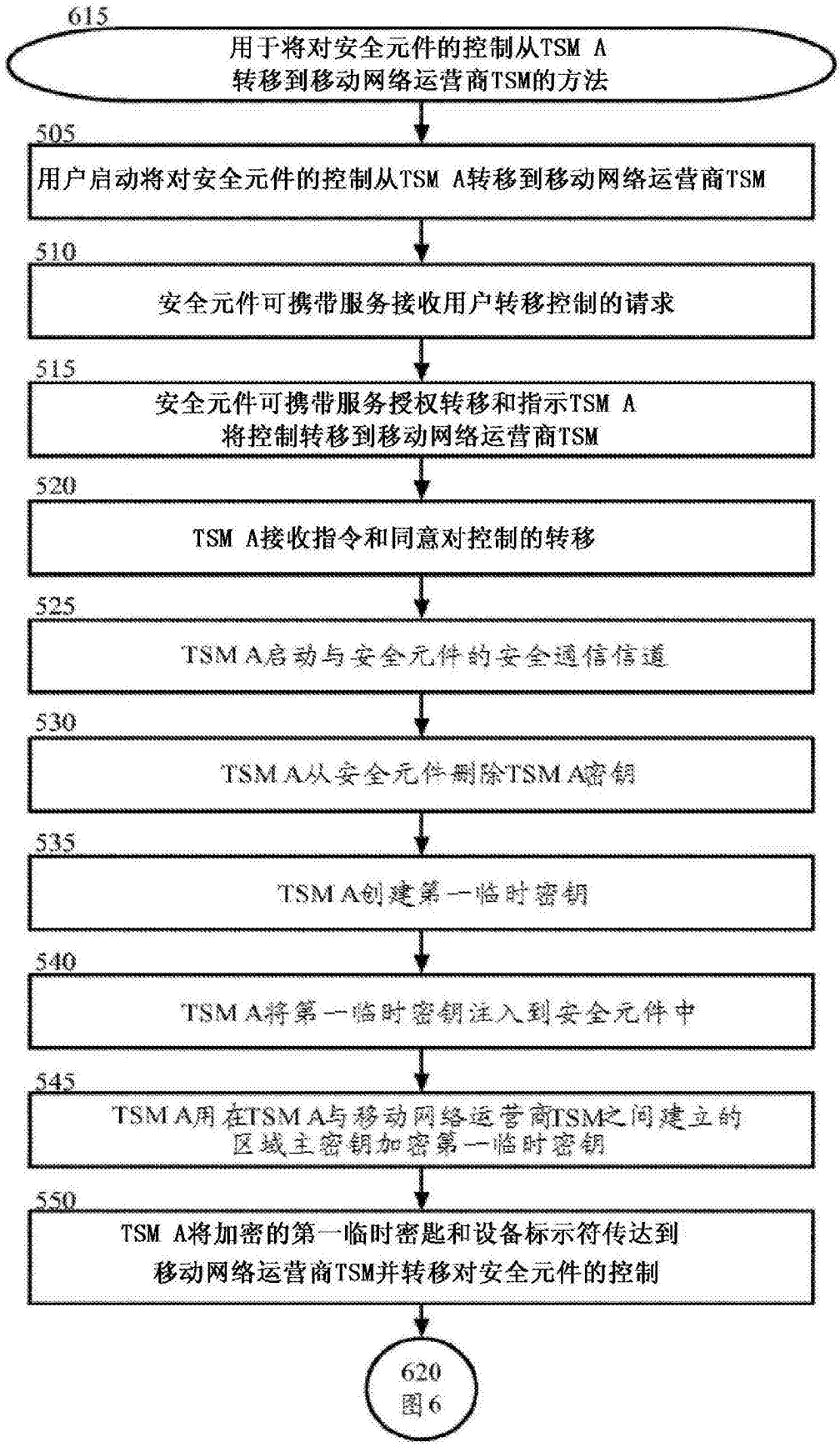

615
用于将对安全元件的控制从TSM A
转移到移动网络运营商TSM的方法
505
用户启动将对安全元件的控制从TSM A转移到移动网络运营商TSM
510
安全元件可携带服务接收用户转移控制的请求
515
安全元件可携带服务授权转移和指示TSM A
将控制转移到移动网络运营商TSM
520
TSM A接收指令和同意对控制的转移
525
TSM A启动与安全元件的安全通信信道
530
TSM A从安全元件删除TSM A密钥
535
TSM A创建第一临时密钥
540
TSM A将第一临时密钥注入到安全元件中
545
TSM A用在TSM A与移动网络运营商TSM之间建立的
区域主密钥加密第一临时密钥
550
TSM A将加密的第一临时密匙和设备标示符传达到
移动网络运营商TSM并转移对安全元件的控制
620
图6

图7

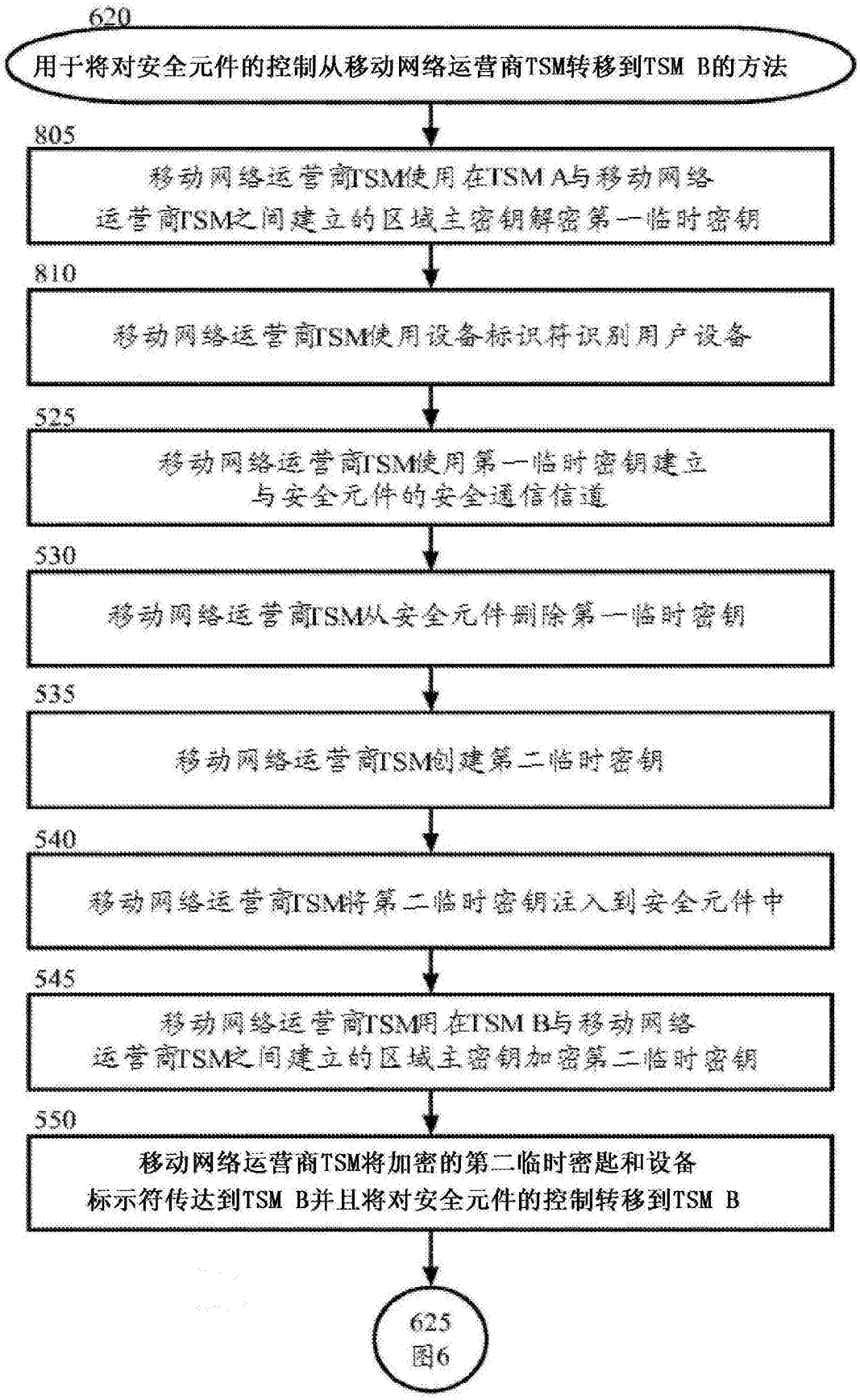

620
用于将对安全元件的控制从移动网络运营商TSM转移到TSM B的方法
805
移动网络运营商TSM使用在TSM A与移动网络运营商TSM之间建立的区域主密钥解密第一临时密钥
810
移动网络运营商TSM使用设备标识符识别用户设备
525
移动网络运营商TSM使用第一临时密钥建立与安全元件的安全通信信道
530
移动网络运营商TSM从安全元件删除第一临时密钥
535
移动网络运营商TSM创建第二临时密钥
540
移动网络运营商TSM将第二临时密钥注入到安全元件中
545
移动网络运营商TSM用在TSM B与移动网络运营商TSM之间建立的区域主密钥加密第二临时密钥
550
移动网络运营商TSM将加密的第二临时密匙和设备标示符传达到TSM B并且将对安全元件的控制转移到TSM B
625
图6

图8