(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 104412273 B
(45)授权公告日 2017.05.17

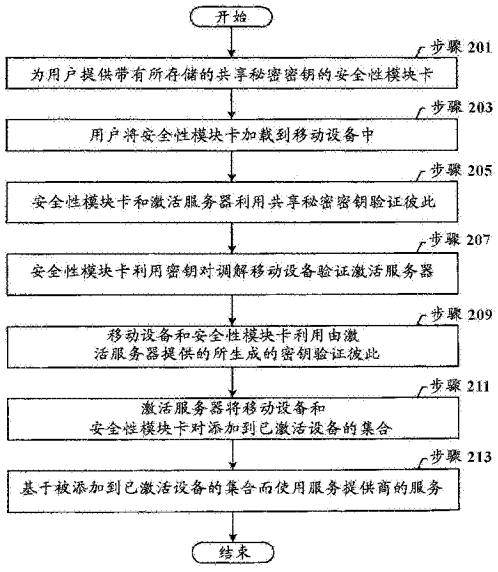
(21)申请号 201380032448.5
(22)申请日 2013.04.08
(65)同一申请的已公布的文献号
申请公布号 CN 104412273 A
(43)申请公布日 2015.03.11
(30)优先权数据
13/459,331 2012.04.30 US
(85)PCT国际申请进入国家阶段日
2014.12.19
(86)PCT国际申请的申请数据
PCT/US2013/035578 2013.04.08
(87)PCT国际申请的公布数据
WO2013/165651 EN 2013.11.07
(73)专利权人 甲骨文国际公司
地址 美国加利福尼亚
(72)发明人 S·汉斯 A·戈拉斯曼
N·伊万诺娃
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 陈新
(51)Int.Cl.
*G06F 21/34*(2006.01)
*G06Q 20/34*(2006.01)
*G07F 7/10*(2006.01)
*H04L 29/06*(2006.01)
*H04W 12/06*(2006.01)
(56)对比文件
US 2009/0172397 A1,2009.07.02,
WO 02/082387 A1,2002.10.17,
审查员 陈玲
权利要求书3页 说明书13页 附图7页

(54)发明名称

用于进行激活的方法和系统

(57)摘要

本发明涉及一种激活方法，其包括：由安全性模块卡利用共享秘密密钥和第一挑战验证激活服务器；调解移动设备对激活服务器的验证；以及利用所生成的密钥对第二挑战进行加密，从而获得已加密的第二挑战。安全性模块卡还向移动设备传送已加密的第二挑战和第三挑战。所述方法还包括：从移动设备接收已加密的第三挑战；对已加密的第三挑战进行解密以获得所接收的第三挑战；基于所接收的第三挑战等于发送给移动设备的第三挑战而验证移动设备；以及向激活服务器发送关于安全性模块卡与移动设备之间的互信的确证。




CN 104412273 B

1.一种用于进行激活的方法,包括:

(a)由安全性模块卡利用共享秘密密钥和第一挑战验证激活服务器;

(b)响应于验证激活服务器,由安全性模块卡调解移动设备对激活服务器的验证,其中所述验证使用第二挑战和密钥对;

(c)由安全性模块卡利用所生成的密钥对第二挑战进行加密,从而获得已加密的第二挑战,其中所生成的密钥由激活服务器生成;

(d)由安全性模块卡向移动设备传送已加密的第二挑战和第三挑战,其中移动设备利用已加密的第二挑战验证安全性模块卡;

(e)由安全性模块卡从移动设备接收已加密的第三挑战;

(f)由安全性模块卡对已加密的第三挑战进行解密,从而获得所接收的第三挑战;

(g)由安全性模块卡基于所接收的第三挑战等于发送给移动设备的第三挑战而验证移动设备;以及

(h)由安全性模块卡向激活服务器发送关于安全性模块卡与移动设备之间的互信的确证,

其中,(a)在(c)之前实施,并且(c)在(h)之前实施。

2.根据权利要求1的方法,其中,验证激活服务器包括:

向激活服务器发送第一挑战;

响应于发送第一挑战,从激活服务器接收第一已加密值;

利用共享秘密密钥对第一已加密值进行解密,从而获得第一值;以及

基于第一值等于第一挑战而认证激活服务器。

3.根据权利要求1或2的方法,还包括:

由安全性模块卡从激活服务器接收第四挑战;

由安全性模块卡利用共享秘密密钥对第四挑战进行加密,从而产生第二已加密值;以及

向激活服务器发送第二已加密值,

其中,激活服务器对第二已加密值进行解密,并且验证已解密的第二已加密值中的第四挑战等于由安全性模块卡接收的第四挑战,从而认证安全性模块卡。

4.根据权利要求1或2的方法,还包括:

发送秘密密钥的秘密密钥标识符,其中激活服务器利用相应的独有秘密密钥与多个安全性模块卡进行通信,其中所述安全性模块卡是所述多个安全性模块卡的其中之一。

5.根据权利要求1或2的方法,其中,(b)和(c)被同时实施。

6.根据权利要求1或2的方法,其中,在将安全性模块卡提供给移动设备的用户之前,将所述秘密密钥存储在安全性模块卡上。

7.根据权利要求1或2的方法,其中,在(a)之前创建GlobalPlatform安全信道以便与安全性模块卡进行通信时,激活服务器认证安全性模块卡。

8.根据权利要求1或2的方法,其中,调解移动设备对激活服务器的验证包括:

将接收自移动设备的第二挑战转发到激活服务器;

从激活服务器接收第一已加密值;

向移动设备发送第一已加密值,

其中，移动设备利用公共密钥对第一已加密值进行解密以获得第一值，其中所述公共密钥处在所述密钥对中；并且

其中，移动设备通过确认由移动设备发送的第二挑战等于第一值中的第二挑战来验证激活服务器。

9.根据权利要求8的方法，还包括：

由安全性模块卡利用共享秘密密钥对已加密的所生成的密钥进行解密，从而获得所生成的密钥；并且

其中，移动设备从第一值中提取出所生成的密钥并且利用所生成的密钥对已加密的第二挑战进行解密，从而获得已解密的第二挑战，并且

其中，移动设备基于由移动设备发送的第二挑战等于已解密的第二挑战来确证安全性模块卡。

10.根据权利要求1或2的方法，其中，激活服务器基于对安全性模块卡的确证以及从安全性模块卡接收到关于互信的确证来确证移动设备。

11.一种用于进行激活的安全性模块卡，所述安全性模块卡包括：

受保护的存储器，其包括共享秘密密钥；以及

卡激活模块，其被配置成：

(a)利用共享秘密密钥和第一挑战验证激活服务器；

(b)响应于验证激活服务器，调解移动设备对激活服务器的验证，其中所述验证使用第二挑战和密钥对；

(c)利用所生成的密钥对第二挑战进行加密，从而获得已加密的第二挑战，其中所生成的密钥由激活服务器生成；

(d)向移动设备传送已加密的第二挑战和第三挑战，其中移动设备利用已加密的第二挑战验证安全性模块卡；

(e)从移动设备接收已加密的第三挑战；

(f)对已加密的第三挑战进行解密，从而获得所接收的第三挑战；

(g)基于所接收的第三挑战等于发送给移动设备的第三挑战而验证移动设备；以及

(h)向激活服务器发送关于安全性模块卡与移动设备之间的互信的确证，

其中，(a)在(c)之前实施，并且(c)在(h)之前实施。

12.根据权利要求11的安全性模块卡，其中，验证激活服务器包括：

向激活服务器发送第一挑战；

响应于发送第一挑战，从激活服务器接收第一已加密值；

利用共享秘密密钥对第一已加密值进行解密，从而获得第一值；以及

基于第一值等于第一挑战而认证激活服务器。

13.根据权利要求11或12的安全性模块卡，其中，卡激活模块还被配置成：

从激活服务器接收第四挑战；

利用共享秘密密钥对第四挑战进行加密，从而产生第二已加密值；

向激活服务器发送第二已加密值，

其中，激活服务器对第二已加密值进行解密，并且验证已解密的第二已加密值中的第四挑战等于由安全性模块卡接收的第四挑战，从而认证安全性模块卡。

14.根据权利要求11或12的安全性模块卡，其中，卡激活模块还被配置成：

发送秘密密钥的秘密密钥标识符，其中激活服务器利用相应的独有秘密密钥与多个安全性模块卡进行通信，其中所述安全性模块卡是所述多个安全性模块卡的其中之一。

15.根据权利要求11或12的安全性模块卡，其中，(b)和(c)被同时实施。

16.根据权利要求11或12的安全性模块卡，其中，在将安全性模块卡提供给移动设备的用户之前，将共享秘密密钥存储在安全性模块卡上。

17.一种用于进行激活的系统，包括：

根据权利要求11到16中的任一项的安全性模块卡；以及

操作上连接到安全性模块卡的移动设备，其包括：

包括所述密钥对中的公共密钥的移动设备存储器；以及

移动设备激活模块，其被配置成：

通过安全性模块卡向激活服务器发送第二挑战；

通过安全性模块卡从激活服务器接收已加密值；

利用公共密钥对所述已加密值进行解密，从而获得一值；以及

验证由移动设备发送的第二挑战等于所述值中的第二挑战，从而验证激活服务器。

18.根据权利要求17的系统，其中，安全性模块卡被嵌入在移动设备中。

19.根据权利要求18的系统，其中，安全性模块卡是安全识别模块(SIM)卡。

20.根据权利要求17到19中任一项的系统，其中，移动设备激活模块还被配置成：

从安全性模块卡接收第三挑战；

产生已加密的第三挑战；以及

向安全性模块卡发送已加密的第三挑战。

# 用于进行激活的方法和系统

## 背景技术

[0001] 移动设备非常普及。为了使用移动设备，通常对移动设备中的订户身份模块卡进行认证。基于所述认证，所述设备可以访问网络上的服务。

## 发明内容

[0002] 一般来说，在一个方面中，本发明涉及一种用于进行激活的方法。所述方法包括：由安全性模块卡利用共享秘密密钥和第一挑战验证激活服务器；响应于验证激活服务器，调解移动设备对激活服务器的验证，其中所述验证使用第二挑战和一个密钥对；以及利用所生成的密钥对第二挑战进行加密，从而获得已加密的第二挑战。所述验证使用第二挑战和一个密钥对，并且所生成的密钥由激活服务器生成。安全性模块卡还向移动设备传送已加密的第二挑战和第三挑战。移动设备利用已加密的第二挑战验证安全性模块卡。安全性模块卡还从移动设备接收已加密的第三挑战，并且对已加密的第三挑战进行解密以获得所接收的第三挑战。安全性模块卡基于所接收的第三挑战等于发送给移动设备的第三挑战而验证移动设备，并且向激活服务器发送关于安全性模块卡与移动设备之间的互信的确证。

[0003] 一般来说，在一个方面中，本发明涉及一种用于进行激活的安全性模块卡。所述安全性模块卡包括受保护的存储器和卡激活模块，所述受保护的存储器包括共享秘密密钥。卡激活模块被配置成：利用共享秘密密钥和第一挑战验证激活服务器；响应于验证激活服务器，调解移动设备对激活服务器的验证，其中所述验证使用第二挑战和一个密钥对；以及利用所生成的密钥对第二挑战进行加密，从而获得已加密的第二挑战。所述验证使用第二挑战和一个密钥对，并且所生成的密钥由激活服务器生成。卡激活模块还被配置成向移动设备传送已加密的第二挑战和第三挑战。移动设备利用已加密的第二挑战验证安全性模块卡。卡激活模块还被配置成：从移动设备接收已加密的第三挑战；对已加密的第三挑战进行解密以获得所接收的第三挑战；基于所接收的第三挑战等于发送给移动设备的第三挑战而验证移动设备；以及向激活服务器发送关于安全性模块卡与移动设备之间的互信的确证。

[0004] 一般来说，在一个方面中，本发明涉及一种系统。所述系统包括安全性模块卡和移动设备。所述安全性模块卡包括受保护的存储器和卡激活模块，所述受保护的存储器包括共享秘密密钥。卡激活模块被配置成：利用共享秘密密钥和第一挑战验证激活服务器；响应于验证激活服务器，调解移动设备对激活服务器的验证，其中所述验证使用第二挑战和一个密钥对；以及利用所生成的密钥对第二挑战进行加密，从而获得已加密的第二挑战。所述验证使用第二挑战和一个密钥对，并且所生成的密钥由激活服务器生成。卡激活模块还被配置成向移动设备传送已加密的第二挑战和第三挑战。移动设备利用已加密的第二挑战验证安全性模块卡。卡激活模块还被配置成：从移动设备接收已加密的第三挑战；对已加密的第三挑战进行解密以获得所接收的第三挑战；基于所接收的第三挑战等于发送给移动设备的第三挑战而验证移动设备；以及向激活服务器发送关于安全性模块卡与移动设备之间的互信的确证。移动设备在操作方面连接到安全性模块卡。移动设备包括移动设备存储器，其包括所述密钥对中的公共密钥以及移动设备激活模块。所述移动设备激活模块被配置成：

通过安全性模块卡向激活服务器发送第二挑战;通过安全性模块卡从激活服务器接收一个已加密值;利用激活服务器的公共密钥对所述已加密值进行解密,从而获得一个值;以及验证由移动设备发送的第二挑战等于所述值中的第二挑战,从而验证激活服务器。

[0005] 通过后面的描述和所附权利要求书,本发明的其他方面将变得显而易见。

## 附图说明

[0006] 图1示出了根据本发明的一个或多个实施例的系统的示意图。

[0007] 图2-5示出了本发明的一个或多个实施例中的流程图。

[0008] 图6示出了本发明的一个或多个实施例中的示例性时序图。

[0009] 图7示出了根据本发明的一个或多个实施例的计算机设备。

## 具体实施方式

[0010] 现在将参照附图来详细描述本发明的具体实施例。为了一致性起见,各幅图中的相同的元件由相同的附图标记标示。

[0011] 在后面对于本发明的实施例的详细描述中阐述了许多具体细节,以便提供对于本发明的更加透彻的理解。但是本领域技术人员将认识到,可以在没有这些具体细节的情况下实践本发明。此外,没有详细描述众所周知的特征,以避免使得描述不必要地复杂化。

[0012] 一般来说,本发明的实施例提供一种用于利用激活服务器来激活移动设备和安全性模块卡的方法和系统。具体来说,各个实施例提供一种用于在移动设备、安全性模块卡和激活服务器之间建立三方互信的方法。在所述三方互信中,激活服务器对安全性模块卡进行确证并且安全性模块卡对激活服务器进行确证,从而使得全部两个组件确认激活服务器和安全性模块卡都没有恶意。类似地,安全性模块卡对移动设备进行确证并且移动设备对安全性模块卡进行确证,从而使得全部两个组件确认移动设备和安全性模块卡都没有恶意。最后,激活服务器对移动设备进行确证并且移动设备对激活服务器进行确证,从而使得全部两个组件确认激活服务器和移动设备都没有恶意。基于三方激活的成功完成,激活服务器存储安全性模块卡和移动设备对的标识,以便激活全部两个设备。换句话说,安全性模块卡和移动设备被存储为一对,从而使得如果安全性模块卡和移动设备当中的任一个或全部两个被不同的安全性模块卡或移动设备替换,则在本发明的一个或多个实施例中实施新的三方激活。在本发明的一个或多个实施例中,可以附加地或替换地在激活服务器通过向安全性模块卡发送请求而触发新的三方激活时实施新的三方激活。

[0013] 在各幅图、说明书和权利要求书中,移动设备与激活服务器之间的通信被描述为通过安全性模块卡来实施。换句话说,安全性模块卡被描述为接收来自激活服务器或移动设备的通信,并且将所述通信转发到移动设备或激活服务器。在本发明的一个或多个实施例中,安全性模块卡可以直接连接到网络,并且对于所述通信的至少一部分充当移动设备与激活服务器之间的中介。在本发明的替换实施例中,当移动设备接收来自激活服务器的通信、将所述通信传送到安全性模块卡以进行预处理并且随后接收来自安全性模块卡的经过预处理的通信时,所述通信被认为是通过安全性模块卡来实施的。同样地,当移动设备将通信传送到安全性模块卡以进行预处理、接收来自安全性模块卡的经过预处理的通信并且将经过预处理的通信传送到激活服务器时,所述通信被认为是通过安全性模块卡来实施

的。这样的预处理例如可以包括对所述通信或消息的全部或一部分进行加密(例如对消息的整个主体进行加密),实施身份管理,添加标识符,生成用于通信会话的加密密钥,以及实施其他此类动作。

[0014] 图1示出了根据本发明的一个或多个实施例的系统的示意图。如图1中所示,所述系统包括激活服务器(100)、移动设备(102)、安全性模块卡(104)和网络(106)。后面将讨论这些组件当中的每一个。

[0015] 在本发明的一个或多个实施例中,激活服务器(100)是包括用以激活移动设备和安全性模块卡对的功能的一个或多个计算设备。在不背离权利要求书的范围的情况下,激活服务器可以包括与激活有关或无关的附加功能。在本发明的一个或多个实施例中,激活服务器(100)由服务提供商(未示出)管理。具体来说,激活服务器(100)被配置成代表服务提供商激活移动设备和安全性模块对。在本发明的一个或多个实施例中,服务提供商可以是基于所述激活为激活服务器提供移动网络服务的通信公司(carrier)。在替换的或附加的实施例中,激活服务器(100)可以独立于通信公司。举例来说,服务提供商可以为移动设备(102)(后面讨论)和/或安全性模块卡(104)提供应用和/或服务。

[0016] 在本发明的一个或多个实施例中,激活服务器(100)包括数据贮存库(108)和激活应用(110)。在本发明的一个或多个实施例中,数据贮存库(108)是用于存储数据的任何类型的存储单元和/或设备(例如文件系统、数据库、表的总集或者任何其他存储机制)。此外,数据贮存库(108)可以包括多个不同的存储单元和/或设备。所述多个不同的存储单元和/或设备可以或者可以不属于相同类型或者位于相同的物理地点。在本发明的一个或多个实施例中,数据贮存库(108)或者其某一部分是安全的。

[0017] 在本发明的一个或多个实施例中,数据贮存库(108)包括用以存储秘密密钥(114)和密钥标识符(112)、私有密钥(116)和已激活设备卡对(118)的功能。秘密密钥(114)在这里也被称作共享秘密密钥,其是被授权查看私有通信的所有各方都知道的密码密钥。在本发明的一个或多个实施例中,秘密密钥(114)的一份拷贝由数据贮存库(108)和安全性模块卡(104)(后面讨论)全部二者存储。具体来说,数据贮存库(108)存储秘密密钥的第一拷贝,安全性模块卡(104)则存储秘密密钥的第二拷贝。在本发明的一个或多个实施例中,秘密密钥(114)是字母数字字符或比特的随机或伪随机串,其被用来对一项或多项通信进行加密和解密。

[0018] 在本发明的一个或多个实施例中,虽然未在图1中示出,但是所述数据贮存库存储多个秘密密钥。在本发明的一个或多个实施例中,每一个秘密密钥(114)与一个密钥标识符(112)相关联。在数据贮存库(108)中的其他密钥当中,密钥标识符(112)唯一地标识相应的秘密密钥(114)。换句话说,密钥标识符(112)是对应于相应的秘密密钥(114)的独有标识符。

[0019] 在本发明的一个或多个实施例中,对于每一个安全性模块卡(104)(后面讨论)存在一个单独的秘密密钥。具体来说,对应于特定的安全性模块卡(104)的秘密密钥不同于对应于任何其他安全性模块卡(104)(未示出)的秘密密钥。在本发明的一个或多个实施例中,每一个秘密密钥对于存储在数据贮存库(108)中的其他秘密密钥而言是独有的。在本发明的替换或附加实施例中,基于被用来生成秘密密钥的具体技术,一些秘密密钥可能在无意中是相同的。在本发明的替换或附加实施例中,对于一整个批次的安全性模块卡可能存在

单独的密钥和密钥标识符。换句话说，不同批次的安全性模块卡分别具有对于其他批次的安全性模块卡而言是独有的秘密密钥和密钥标识符，而相同批次中的安全性模块卡则可以共享秘密密钥和密钥标识符。在这样的情形中，数据贮存库可以对于每一个批次仅存储单一秘密密钥和密钥标识符。

[0020] 在本发明的一个或多个实施例中，私有密钥(116)是仅为通信的发送者所知的密码密钥。具体来说，私有密钥(116)被使用在非对称密钥加密中。换句话说，私有密钥(116)被用来对相应的通信进行加密。私有密钥(116)具有相应的公共密钥(例如公共密钥124(后面讨论))，其可以由密码算法使用来对利用私有密钥加密的通信进行解密。

[0021] 在本发明的一个或多个实施例中，虽然没有在图1中示出，但是私有密钥和公共密钥可以具有相应的密钥对标识符。所述密钥对标识符可以被用来唯一地标识密钥对。举例来说，在本发明的一个或多个实施例中，私有密钥可以与移动设备相关联。对移动设备进行认证的每一个认证服务器可以具有对应于该移动设备的私有密钥的一份拷贝。在这样的情形中，认证服务器和移动设备可以使用密钥对标识符来唯一地标识密钥对中的公共和私有密钥全部二者。

[0022] 继续对于数据贮存库(108)的描述，在本发明的一个或多个实施例中，已激活设备卡对(118)对应于被激活的移动设备和安全性模块卡对的标识符。在本发明的一个或多个实施例中，每一对包括移动设备的标识符和安全性模块卡的标识符。通过把移动设备的标识符和安全性模块卡的标识符存储为一对表明移动设备与安全性模块卡之间的关系。因此，举例来说，如果先前对于特定移动设备被激活的特定安全性模块卡被添加到不同的移动设备，在本发明的一个或多个实施例中，所述特定安全性模块卡和不同的移动设备不处在所述已激活设备卡对中。具体来说，在本发明的一个或多个实施例中，直到建立三方互信，才将所述特定安全性模块卡和不同的移动设备视为一个已激活单元。

[0023] 在本发明的一个或多个实施例中，数据贮存库(108)在操作方面连接到激活应用(110)。激活应用(110)包括对于移动设备和对应于激活服务器(100)的安全性模块卡实施激活的功能。激活应用(110)可以是软件、硬件或者其组合。

[0024] 在本发明的一个或多个实施例中，激活应用可以被实施为用于管理移动设备和安全性模块卡的管理服务器(未示出)的一部分。具体来说，管理服务器可以被配置成管理移动设备和安全性模块卡上的应用和固件。在这样的情形中，管理服务器可以是与图1中所示的激活服务器相同或不同的设备。激活应用可以是用于管理服务器的中间件。作为中间件，激活应用可以被配置成对于管理服务器实施三方激活，并且确认正由管理服务器管理的每一个设备处于已激活设备卡对中。一旦激活应用的激活和确认完成，管理服务器(未示出)的后端软件(未示出)可以对设备实施管理。

[0025] 继续参照图1，移动设备(图1中的MD)(102)是任何类型的便携式计算设备，其包括用以连接到网络(106)的功能。举例来说，所述移动设备可以是智能电话、标准移动电话、平板计算设备或者任何其他便携式设备。在本发明的一个或多个实施例中，移动设备(102)由用户使用。具体来说，用户可以控制移动设备。用户可以是能够访问并且选择移动设备上的特征的任何个人或者个人的群组。在本发明的替换或附加实施例中，移动设备(102)可以由另一台机器使用和控制。在这样的实施例中，移动设备(102)可以在没有用户交互的情况下运作，并且仅与机器或后端系统通信。在本发明的一个或多个实施例中，移动设备(102)包

括未受保护的存储器(120)和移动设备激活模块(122)。在本发明的一个或多个实施例中，移动设备可以包括未在图1中示出的附加组件。

[0026] 在本发明的一个或多个实施例中，未受保护的存储器(120)对应于用于在移动设备上存储数据的存储装置。在本发明的一个或多个实施例中，未受保护的存储器(120)是可以由执行在移动设备(102)上的实际上任何应用访问的存储器。具体来说，未受保护的存储器(120)不包括用于限制对存储器的访问的升高的安全性特征，比如安全性模块卡(104)(后面讨论)的受保护的存储器(126)中的那些特征。在本发明的一个或多个实施例中，未受保护的存储器(120)存储公共密钥(124)。公共密钥(124)是用于对来自激活服务器(100)的通信进行解密的密码密钥。具体来说，公共密钥(124)是用于对利用相应的私有密钥(116)(后面讨论)加密的通信进行解密的密钥。

[0027] 在本发明的一个或多个实施例中，由于移动设备(102)具有未受保护的存储器(120)，因此利用公共密钥(124)而不是任何共享秘密密钥来实施激活步骤意味着如果恶意用户或程序获得所述密钥，系统的安全性不会受到损害。换句话说，由于公共密钥仅被用于解密并且是公共的，因此公共密钥的暴露并不会改变将特定通信认证为来自特定来源的能力。换句话说，在本发明的一个或多个实施例中，无法利用公共密钥对已加密通信进行修改或重新加密。

[0028] 在本发明的一个或多个实施例中，未受保护的存储器在操作方面连接到移动设备激活模块(122)。具体来说，移动设备激活模块(122)包括用以访问未受保护的存储器(120)的功能。移动设备激活模块(122)包括应以实施对于移动设备(102)的激活步骤的功能。移动设备激活模块(122)可以通过硬件、软件或者其某种组合来实施。

[0029] 在本发明的一个或多个实施例中，移动设备激活模块被实施为客户端的一部分。客户端可以被配置成使用服务提供商的服务。举例来说，客户端可以被配置成从管理服务器接收管理操作。激活模块可以是包括用以实施激活步骤并且在允许管理操作继续到客户端之前确认实施了三方激活的功能的客户端部分。客户端可以被配置成使用服务提供商的服务。

[0030] 安全性模块卡(104)对应于具有集成电路并且被用来认证和识别特定用户的受保护设备。在本发明的一个或多个实施例中，由通信公司将安全性模块卡提供给用户。安全性模块卡(104)可以被嵌入在移动设备中。此外，可以从移动设备中移除安全性模块卡。在本发明的一个或多个实施例中，可以通过移除移动设备的封盖或者拔出安全性模块卡来移除安全性模块卡，其中需要或者不需要移除螺钉或其他非永久性固定机制。在本发明的一个或多个实施例中，安全性模块卡能够并且意图在不会损坏移动设备的情况下由用户从移动设备中移除，以便允许很容易地切换到不同的移动设备。在本发明的一个或多个实施例中，安全性模块卡是订户身份模块(SIM)卡。

[0031] 取代将安全性模块卡(104)嵌入在移动设备(102)中，安全性模块卡可以经由有线或无线外部链接在操作方面连接到移动设备(102)。在这样的情形中，所述无线链接可以是经由蓝牙、近场通信链接或者要求移动设备与安全性模块卡之间的紧密距离(例如小于一英尺或者小于五英尺的距离)的其他链接。

[0032] 继续参照图1，安全性模块卡包括受保护的存储器(126)和卡激活模块(128)。受保护的存储器(126)是安全性模块卡上的受保护的物理存储位置。在本发明的一个或多个实

施例中，受保护的存储器(126)只能由运行在安全性模块卡(104)上的应用(例如卡激活模块)访问。受保护的存储器(126)包括用以存储秘密密钥、密钥标识符以及移动设备的标识符的功能。秘密密钥(130)和密钥标识符(132)分别是存储在激活服务器(100)的数据贮存库中的秘密密钥(114)和密钥标识符(112)的拷贝。具体来说，秘密密钥(130)和密钥标识符(132)可以被用来与激活服务器(100)通信。在本发明的一个或多个实施例中，在将安全性模块卡(104)提供给用户之前，将秘密密钥(130)和密钥标识符(132)存储在安全性模块卡(104)上。举例来说，在安全性模块卡为通信公司所拥有时，通信公司可以将秘密密钥(130)和密钥标识符(132)存储在安全性模块卡(104)上。作为另一个实例，在制造安全性模块卡(104)时，可以作为制造处理的一部分将秘密密钥(130)和密钥标识符(132)存储在受保护的存储器(126)中。

[0033] 在本发明的一个或多个实施例中，移动设备的标识符(其在图1中被标记为MD的ID)(134)是对应于移动设备(102)的独有标识符。举例来说，移动设备的标识符(134)可以是国际移动装备身份(IMEI)代码。

[0034] 在本发明的一个或多个实施例中，受保护的存储器(126)在操作方面连接到卡激活模块(128)。卡激活模块(128)包括用以代表安全性模块卡(104)实施激活步骤的功能。卡激活模块(128)可以通过硬件、软件或者其某种组合来实施。在本发明的一个或多个实施例中，卡激活模块(128)被实施为客户端的一部分。具体来说，所述卡可以安装客户端，并且卡激活模块可以是包括用以实施激活步骤并且在允许管理操作从激活服务器和/或移动设备继续之前确认建立了三方互信的功能的客户端部分。客户端可以是小应用程序。在本发明的一个或多个实施例中，客户端是利用Oracle®Java Card技术来实施。

[0035] 在本发明的一个或多个实施例中，网络(106)处于移动设备(102)与激活服务器(100)之间。所述网络例如可以是局域网(LAN)、例如因特网之类的广域网(WAN)、蜂窝网络或者任何其他类型的网络或其组合。在本发明的一个或多个实施例中，网络(106)包括用以传送移动设备(102)与激活服务器(100)之间的通信的功能。

[0036] 虽然图1示出了一种组件配置，但是在不背离本发明的范围的情况下可以使用其他配置。举例来说，可以组合各个组件以产生单一组件。作为另一个实例，由单一组件实施的功能可以由两个或更多组件来实施。

[0037] 图2-5示出了本发明的一个或多个实施例中的流程图。虽然这些流程图中的各个步骤被顺序地给出和描述，但是本领域技术人员将认识到，其中一些或所有步骤可以按照不同顺序来执行，可以被组合或省略，并且其中一些或所有步骤可以被并行地执行。此外，所述步骤可以被主动地或被动地实施。举例来说，根据本发明的一个或多个实施例，一些步骤可以利用轮询来实施或者被中断驱动。作为举例，根据本发明的一个或多个实施例，确定步骤可以不需要处理器处理指令，除非接收到表明该条件存在。作为另一个实例，根据本发明的一个或多个实施例，可以通过实施测试来实施确定步骤，比如检查某一数据值以测试该值是否与所测试的条件一致。

[0038] 图2示出了本发明的一个或多个实施例中的用于进行激活的总体图示。在步骤201中，为用户提供具有所存储的共享秘密密钥的安全性模块卡。举例来说，用户可以联系通信公司(例如亲身联系、通过电话或因特网联系或者通过其他此类中介联系)，并且获得安全性模块卡。作为另一个实例，用户可以通过零售商获得安全性模块卡。在本发明的一个或多

个实施例中，当用户获得安全性模块卡时，安全性模块卡的受保护的存储器包括数据，比如共享秘密密钥。具体来说，共享秘密密钥的第一拷贝可以被存储在安全性模块卡上，并且共享秘密密钥的第二拷贝可以由激活服务器存储。在本发明的一个或多个实施例中，如果秘密密钥对应于某一批次的安全性模块卡，则对应于该批次的秘密密钥被存储在安全性模块卡中。

[0039] 在步骤203中，在本发明的一个或多个实施例中，用户将安全性模块卡加载到移动设备中。用户可以将安全性模块卡加载到移动设备中，这例如是因为用户正在将新的安全性模块卡添加到新的移动设备或者现有的移动设备，或者是因为用户正在将现有的安全性模块卡添加到新的移动设备(例如用户先前尚未将其与安全性模块卡一同使用的移动设备)。当某人代表用户将安全性模块卡加载到移动设备中时，则认为用户将安全性模块卡加载到移动设备中。在本发明的一个或多个实施例中，将安全性模块卡加载到移动设备中会触发激活规程。举例来说，在本发明的一个或多个实施例中，在利用安全性模块卡第一次为带有安全性模块的移动设备通电时，可以使用这里所描述的激活规程。或者，可以通过由用户利用安全性模块卡和移动设备发起第一次通信来触发激活规程。

[0040] 在步骤205中，安全性模块卡和激活服务器利用共享秘密密钥来验证彼此。具体来说，安全性模块卡通过确认激活服务器使用与移动设备相同的共享秘密密钥的拷贝来验证激活服务器。可以按照在后面以及在图3和4中描述的那样来实施可以被用于使得安全性模块卡和激活服务器验证彼此的具体步骤。

[0041] 在本发明的一个或多个实施例中，通过实施用于验证的步骤205，当激活应用是中间件时，可以避免需要将大量卡标识符加载到中间件中。换句话说，在其中较小百分比的安全性模块卡变为激活的系统中，不对大量未被使用的数据进行管理。

[0042] 在图2的步骤207中，安全性模块卡利用密钥对(即私有密钥和相应的公共密钥)调解移动设备验证激活服务器。在本发明的一个或多个实施例中，移动设备通过确认激活服务器正在使用正确的私有密钥来验证激活服务器。

[0043] 在本发明的一个或多个实施例中，激活服务器基于激活服务器已验证了安全性模块卡来验证移动设备。具体来说，在本发明的一个或多个实施例中，一旦激活服务器验证了安全性模块卡并且安全性模块卡完成了对于移动设备的验证，则激活服务器认为移动设备得到验证。换句话说，激活服务器被配置成通过安全性模块卡以传递方式验证移动设备。

[0044] 在本发明的一个或多个实施例中，通过实施步骤207的验证，当激活应用是客户端的一部分并且服务提供商是通信公司时，客户端不需要知晓该客户端必须登记到哪一家通信公司。相反，所述知识存在于安全性模块卡中并且与安全性模块卡布置在一起。可以按照在后面以及在图3-5中描述的那样来实施可以被用于使得移动设备和激活服务器验证彼此的具体步骤。

[0045] 在图2的步骤209中，在本发明的一个或多个实施例中，移动设备和安全性模块卡利用由激活服务器生成的密钥(即所生成的密钥)验证彼此。所述验证允许安全性模块卡和移动设备被彼此安全地认证。当移动设备应用模块和卡激活模块是客户端的一部分时，所述安全认证允许对应的客户端互相验证而无需另外的验证步骤。举例来说，移动设备上的客户端是支付应用并且安全性模块卡上的客户端具有支付信息，安全性模块卡上的客户端可以基于所述互相验证(即互信)为支付应用提供支付信息。可以按照在后面以及在图3和5

中描述的那样来实施可以被用于使得移动设备和安全性模块卡验证彼此的具体步骤。

[0046] 在图2的步骤211中，在本发明的一个或多个实施例中，激活服务器将移动设备和安全性模块卡对添加到已激活设备的集合中。具体来说，激活服务器把移动设备的标识符与安全性模块卡的标识符一起作为一对存储在数据贮存库的已激活设备卡对中。在本发明的一个或多个实施例中，通过将安全性模块卡和移动设备对添加到已激活设备的集合中触发许可事件，从而使得服务提供商可以管理安全性模块卡和移动设备上的应用。

[0047] 在步骤213中，基于被添加到已激活设备的集合中，在本发明的一个或多个实施例中，移动设备和安全性模块卡使用服务提供商的服务。在本发明的一个或多个实施例中，由于三方互信，使得用户确信移动设备和安全性模块卡连接到正确的服务提供商。基于所述互信，服务提供商可以管理移动设备和安全性模块卡。具体来说，基于安全性模块卡验证激活服务器，安全性模块卡可以允许与激活服务器相关联的服务提供商在安全性模块卡和移动设备上实施敏感操作。

[0048] 虽然未在图2中示出，但是可以将移动设备和安全性模块卡对的安全性标识传播到其他系统(例如其他服务提供商、其他内容递送系统)，以用于将内容目标设定到移动设备。

[0049] 图3示出了对应于本发明的一个或多个实施例中的认证的流程图。在本发明的一个或多个实施例中，图3中示出的各个步骤可以由安全性模块卡实施。

[0050] 在步骤301中，接收到来自移动设备的初始化的电力。举例来说，作为移动设备上的供电的一部分，移动设备可以为安全性模块卡的集成电路提供电力。

[0051] 在步骤303中，在本发明的一个或多个实施例中产生第一挑战。在本发明的一个或多个实施例中，基于安全性模块卡确认安全性模块卡和移动设备对尚未被激活而产生第一挑战。在本发明的一个或多个实施例中，可以例如通过随机数生成器或其他技术来实施产生第一挑战。

[0052] 在步骤305中，在本发明的一个或多个实施例中，将第一挑战发送到激活服务器。在本发明的一个或多个实施例中，可以与以下各项当中的一项或多项一同发送第一挑战：共享秘密密钥的密钥标识符，卡激活模块的版本号，计数器值，登记数据和密钥多样化数据，签名算法标识符，以及对应于具有第一挑战的消息的签名。在本发明的一个或多个实施例中，所述计数器可以是在安全性模块卡与激活服务器之间的每一次通信下递增的值。在不背离权利要求书的范围的情况下，可以与附加的或替换的数据一同发送第一挑战。

[0053] 在步骤307中，从激活服务器接收第一已加密值。在步骤309中，利用共享秘密密钥对第一已加密值进行解密以获得第一值。

[0054] 在步骤311中，确定第一挑战是否等于第一值。换句话说，确定第一挑战与第一值是否匹配。如果第一值与第一挑战不相等或不匹配，则所述方法可以结束。具体来说，如果使用不同的密钥或者如果不同的挑战被加密，则利用共享秘密密钥的解密将不会得到相同值的概率非常高。因此，安全性模块卡可以假定激活服务器不具有共享秘密密钥的正确拷贝，因此不可以被信任。或者，虽然未在图3中示出，但是如果所述值不相等，所述流程可以继续到步骤303。举例来说，安全性模块卡可以允许激活服务器再一次进行尝试以考虑到在数据传送中出错的可能性。

[0055] 如果第一挑战等于第一值，则所述流程可以继续到步骤313。在步骤313中，在本发

明的一个或多个实施例中，向激活服务器发送关于互信的确认。具体来说，安全性模块卡可以向激活服务器通知安全性模块卡已验证了激活服务器。在本发明的一个或多个实施例中，可以实施步骤303-313以使得安全性模块卡和激活服务器验证彼此。

[0056] 继续参照图3，在步骤315中从移动设备接收第二挑战。在步骤317中，将第二挑战转发到激活服务器。在本发明的一个或多个实施例中，可以作为安全性模块卡调解本发明的一个或多个实施例中的移动设备与激活服务器之间的验证的一部分来实施步骤315和317。

[0057] 在本发明的一个或多个实施例中，在步骤319中从激活服务器接收已加密的所生成密钥和第二已加密值。可以在来自激活服务器的单一消息或多条消息中接收已加密的所生成密钥和第二已加密值。在本发明的一个或多个实施例中，已加密的所生成密钥是利用共享秘密密钥加密的。在本发明的一个或多个实施例中，在步骤321中利用共享密钥对已加密的所生成密钥进行解密，从而获得所生成的密钥。在步骤323中，使用所生成的密钥来加密在步骤315中接收到的第二挑战。具体来说，将第二挑战和所生成的密钥用作针对加密算法的输入。举例来说，除了将第二挑战的拷贝转发到激活服务器之外，安全性模块卡可以存储第二挑战的拷贝。因此，移动设备可以利用第二挑战来验证激活服务器和安全性模块卡全部二者，正如后面所讨论的那样。

[0058] 继续参照图3，在步骤325中，在本发明的一个或多个实施例中产生第三挑战。具体来说，安全性模块卡可以按照类似于在步骤303中产生第一挑战的方式来产生第三挑战。在本发明的一个或多个实施例中，第三挑战可以由安全性模块卡使用来验证移动设备。

[0059] 在步骤327中，将已加密的第二挑战、第二已加密值和第三挑战发送到移动设备。安全性模块卡可以在单一消息或多条消息中发送已加密的第二挑战、第二已加密值和第三挑战。可以作为调解移动设备与激活服务器之间的验证的一部分来实施针对接收和转发第二已加密值的步骤327和步骤319。

[0060] 在步骤329中，从移动设备接收第三已加密值。在本发明的一个或多个实施例中，在步骤331中利用所生成的密钥对第三已加密值进行解密，从而获得第三值。可以利用第三已加密值和所生成的密钥作为针对对称密钥加密算法的输入来实施对第三已加密值的解密。

[0061] 在步骤333中，确定第三值是否等于或匹配第三挑战。具体来说，安全性模块卡可以确认移动设备使用了由安全性模块卡发送到移动设备的相同挑战和相同的所生成的密钥。在本发明的一个或多个实施例中，移动设备从接收自激活服务器的第二已加密值获得所生成的密钥。换句话说，安全性模块卡不向移动设备发送所生成的密钥，而是仅把来自激活服务器的已加密值转发到包括所生成的密钥的安全性模块卡。因此，向安全性模块卡验证移动设备是基于确认安全性模块卡能够解密来自激活服务器的所生成的密钥。

[0062] 如果第三值与第三挑战不匹配，则所述方法可以在没有建立互信的情况下结束。如果第三挑战与第三已加密值匹配，则所述流程可以继续到步骤335，其中向激活服务器发送关于与移动设备的互信的确证。此外，如果安全性模块卡基于第三挑战验证了移动设备，则激活服务器可以基于对安全性模块卡的先前验证接受所述验证。

[0063] 在本发明的一个或多个实施例中，可以作为移动设备和安全性模块卡的认证的一部分实施关于所生成的密钥和第三挑战的使用的步骤319-333。

[0064] 图4示出了对应于本发明的一个或多个实施例中的激活的流程图。在本发明的一个或多个实施例中，可以例如由激活服务器实施图4中所示出的步骤。

[0065] 在步骤401中，在本发明的一个或多个实施例中，从安全性模块卡接收第一挑战。正如前面所讨论的那样，可以发送第一挑战并且随后与以下各项当中的一项或多项一同接收：共享秘密密钥的密钥标识符，卡激活模块的版本号，计数器值，登记数据和密钥多样化数据，签名算法标识符，以及对应于具有第一挑战的消息的签名。激活服务器可以利用签名算法标识符验证签名，并且验证计数器值与预期的计数器值匹配。附加地或替换地，在本发明的一个或多个实施例中，激活服务器可以使用密钥标识符从数据贮存库获得安全性模块卡的正确的共享秘密密钥。

[0066] 在步骤403中，利用共享秘密密钥对第一挑战进行加密以获得第一已加密值。在本发明的一个或多个实施例中，在步骤405中向安全性模块卡发送第一已加密值。在步骤407中，可以从安全性模块卡接收关于互信的确认。可以作为安全性模块卡和激活服务器验证彼此的一部分实施步骤401-407。

[0067] 虽然没有在图3或4中示出，但是安全性模块卡与激活服务器之间的此类验证可以包括用于使得激活服务器验证安全性模块卡的附加步骤。作为一个实例，这样的步骤可以包括由激活服务器产生并且发送第四挑战，所述第四挑战由安全性模块卡接收。安全性模块卡可以利用共享秘密密钥对第四挑战进行加密从而产生另一个已加密值，并且可以将该已加密值发送到激活服务器。激活服务器可以对所述已加密值进行解密，并且验证所解密的第四挑战与由安全性模块卡接收的第四挑战相匹配，从而认证安全性模块卡。如果所述值匹配，则激活服务器验证安全性模块卡。如果所述值不匹配，则激活服务器不验证安全性模块卡。作为另一个实例，可以由激活服务器在作为开始与安全性模块卡进行通信的一部分创建用以与安全性模块卡通信的GlobalPlatform(全球平台)安全信道时实施所述步骤。

[0068] 继续参照图4，在步骤409中从安全性模块卡接收第二挑战。

[0069] 在步骤411中，激活服务器生成密钥以获得所生成的密钥。可以按照类似于产生挑战的方式实施生成密钥。在步骤413中，激活服务器利用共享秘密密钥对所生成的密钥进行加密，从而获得已加密的所生成密钥。正如前面关于图3所讨论的那样，已加密的所生成密钥由安全性模块卡使用来验证移动设备。

[0070] 继续参照图4，在步骤415中，激活服务器利用私有密钥对所生成的密钥和第二挑战进行加密，从而在本发明的一个或多个实施例中获得第二已加密值。所生成的密钥和第二挑战可以被一同加密或者分开加密。举例来说，在本发明的一个或多个实施例中，可以将第二挑战与所生成的密钥串连，从而获得串连值。可以利用私有密钥作为输入通过对称密钥加密算法来对所述串连值进行加密。正如前面所讨论的那样，在步骤417中通过安全性模块卡向移动设备发送第二已加密值。在本发明的一个或多个实施例中，第二已加密值中的第二挑战由移动设备使用来验证激活服务器。在本发明的一个或多个实施例中，第二已加密值中的所生成的密钥由移动设备使用来验证安全性模块卡。

[0071] 在步骤419中，从安全性模块卡接收关于安全性模块卡与移动设备之间的互信的确证。基于来自安全性模块卡的关于与激活服务器的互信的先前确证，激活服务器与移动设备具有互信。

[0072] 在本发明的一个或多个实施例中，在步骤421中，激活服务器把安全性模块卡和移

动设备对的标识作为已激活对添加到已激活设备的集合中。具体来说，激活服务器将安全性模块卡的标识符和移动设备的标识符存储在数据贮存库中。

[0073] 图5示出了对应于本发明的一个或多个实施例中的激活的流程图。具体来说，例如可以由移动设备实施图5中所示出的各个步骤。

[0074] 在步骤501中，为移动设备通电。在本发明的一个或多个实施例中，通过为移动设备通电引导移动设备，并且随后在步骤503中为安全性模块卡供电。在步骤505中，产生第二挑战。在本发明的一个或多个实施例中，移动设备可以按照类似于安全性模块卡产生第一挑战的方式产生第二挑战。在步骤507中向安全性模块卡发送第二挑战。

[0075] 在步骤509中，从安全性模块卡接收已加密的第二挑战、第二已加密值和第三挑战。在本发明的一个或多个实施例中，在步骤511中利用公共密钥对第二已加密值进行解密，从而获得来自激活服务器的第二挑战和所生成的密钥。在其中激活服务器在产生第二已加密值之前将第二挑战和所生成的密钥串连在一起的实施例中，步骤511还可以包括分割第二挑战和所生成的密钥。

[0076] 在步骤513中，利用所生成的密钥对已加密的第二挑战进行解密，从而获得来自安全性模块卡的第二挑战。在本发明的一个或多个实施例中，移动设备使用第二已加密值中的来自激活服务器的所生成的密钥来对已加密的第二挑战进行解密。

[0077] 在步骤515中，确定来自激活服务器的第二挑战是否等于来自安全性模块卡的第二挑战并且等于所发送的第二挑战。换句话说，确定是否所有三项第二挑战都是相同的。虽然图5示出了单一确定步骤，但是步骤515可以对应于多项确定。如果任一所接收的第二挑战不等于所发送的第二挑战，则移动设备可以确定激活服务器和安全性模块卡当中的任一项或全部两项未被验证，这取决于哪一项第二挑战与所发送的第二挑战不匹配。在这样的情形中，所述流程可以结束。

[0078] 如果各项第二挑战相等，则安全性模块卡和激活服务器在步骤517中被设定为已确证。具体来说，基于所述匹配，移动设备确认安全性模块卡和激活服务器的有效性。

[0079] 在本发明的一个或多个实施例中，在步骤519中利用所生成的密钥对第三挑战进行加密，从而获得已加密的第三挑战。在本发明的一个或多个实施例中，在步骤521中向安全性模块卡发送已加密的第三挑战。因此，安全性模块卡可以利用已加密的第三挑战来验证移动设备。

[0080] 图6示出了本发明的一个或多个实施例中的示例性时序图。下面的实例仅仅是出于解释的目的，而不意图限制本发明的范围。具体来说，在图6中示出并且在后面讨论的实例仅仅是根据本发明的一个或多个实施例的可以被实施的可能步骤以及所述示例性步骤的可能排序的一个实例。在不背离本发明的范围的情况下，可以省略、按照不同顺序实施或者修改其中一些或所有步骤。

[0081] 在后面的实例中，考虑其中移动设备是智能电话(606)并且安全性模块卡是SIM卡(604)的情形。图6出于可读性和简洁的目的包括各种缩写。在图6上包括图例(600)以便解释最常使用的各种缩写当中的每一项。后面将解释其他缩写。此外，图6包括用以表明关于所述时序图的时间方向的时间箭头(608)。

[0082] 对于后面的实例，考虑其中用户去往通信公司并且在签订合约之后获得SIM卡(604)的情形。由于用户不想要通信公司所提供的任何智能电话，因此用户从单独的零售商

获得智能电话(606)。用户将SIM卡(604)插入到智能电话(606)中并且开启(620)智能电话以便为智能电话提供电力。作为引导处理的一部分,SIM卡(604)从智能电话(606)接收电力(621)。由于SIM卡(604)尚未被激活,因此SIM卡开始与激活服务器(602)的激活规程,这受到通信公司的控制。虽然没有在图6的实例中示出,但是SIM卡(604)和激活服务器(602)可以通过首先建立用以创建安全通信会话的GlobalPlatform安全信道来开始激活处理。在所述建立阶段期间,激活服务器(602)可以认证SIM卡(604)。

[0083] 继续描述所述实例,SIM卡产生挑战CH1(622)并且将挑战CH1与共享秘密密钥S的密钥标识符(KeyID)、计数器值(CTR)和签名(SIG)一同发送(623)到激活服务器(602)。在确认计数器值是预期的计数器值之后,激活服务器(602)验证所发送的数据上的签名与预期的签名相匹配,并且利用共享秘密密钥S产生挑战CH1的加密(即进行加密)(624)。激活服务器(602)将挑战CH1的加密发送(625)到SIM卡(604)。

[0084] 在接收到挑战CH1的加密之后,SIM卡(604)利用共享秘密密钥S对所述挑战进行解密,并且验证所发送的挑战CH1与SIM卡(604)所解密的挑战CH1相匹配(626)。相应地,SIM卡(604)向激活服务器(602)发送(627)关于互信的确认(Conf.)。基于所述匹配和激活服务器(602)对SIM卡(604)的先前认证,激活服务器(602)和SIM卡(604)具有互信(628)。

[0085] 此外,智能电话(606)产生挑战CH2(629)。智能电话(606)将挑战CH2(630)以及公共和私有密钥的密钥对标识符(KeyPairID)(630)发送到SIM卡(604)。SIM卡(604)存储挑战CH2的拷贝。此外,SIM卡(604)将挑战CH2和密钥对标识符转发(631)到激活服务器(602)。激活服务器(602)生成密钥k,将挑战CH2和密钥k串连成单一值,利用对应于所述密钥对标识符的私有密钥产生所述单一值的第一加密,并且利用共享秘密密钥S产生密钥k的第二加密(632)。激活服务器(602)将第一加密和第二加密发送(633)到SIM卡(604)。

[0086] SIM卡(604)对利用共享秘密密钥加密的密钥k进行解密,利用已解密的密钥k产生挑战CH2的加密,并且产生挑战CH3(634)。SIM卡发送已加密的挑战CH2,发送挑战CH3,并且把与密钥k串连的挑战CH2的加密转发(635)到智能电话(606)。在本发明的一个或多个实施例中,对挑战和密钥对标识符的转发(631)和已加密串连的转发(635)对应于SIM卡(604)调解智能电话对激活服务器的验证(636)。

[0087] 智能电话(606)利用相应的公共密钥对于与密钥k串连的挑战CH2的加密进行解密,从而获得已解密的串连。智能电话(606)还对所述已解密的串连进行解析,从而从已解密的串连获得挑战CH2,并且验证所获得的挑战CH2等于所发送的挑战(636)。在这一阶段,基于验证二者是相等的,智能电话(606)信任激活服务器(602)。激活服务器(602)可能还不信任智能电话(606)。

[0088] 继续参照图6,智能电话(606)还对利用所生成的密钥k加密的挑战CH2进行解密,并且验证已解密的挑战CH2等于所发送的挑战CH2(637)。所述验证验证出智能电话和安全性模块卡正在使用来自激活服务器的相同的所生成的密钥k。换句话说,智能电话基于确定安全性模块卡能够解密来自激活服务器的所生成的密钥而验证安全性模块卡。基于所述验证,智能电话(606)信任SIM卡(604)。相应地,智能电话利用所生成的密钥k产生(637)挑战CH3的加密,并且将挑战CH3的加密发送(638)到SIM卡(604)。SIM卡(604)对挑战CH3的加密进行解密,并且验证(639)在所述加密中接收的挑战CH3等于所发送的挑战CH3。基于全部两项验证(即637、639),SIM卡(604)和智能电话(606)具有互信(640)。

[0089] 基于互信(640)，智能电话向激活服务器(602)发送关于互信的确证(641)。由于激活服务器(602)已经验证了SIM卡(604)，并且由于所述互信(640)，激活服务器(602)信任智能电话(606)。因此，激活服务器(602)和智能电话(606)具有互信(642)。相应地，激活服务器将智能电话/SIM卡对添加到已激活设备的集合(643)。在本发明的一个或多个实施例中，在这一阶段，与激活服务器(602)相关联的通信公司可以管理智能电话(606)和SIM卡(604)。具体来说，在本发明的一个或多个实施例中，智能电话(606)和SIM卡(604)都信任激活服务器(602)，并且相应地信任通信公司的管理软件以允许通信公司实施特权动作。

[0090] 正如前面所讨论的那样，图6中所示出的步骤仅仅是一个实例，并且不意图限制权利要求书的范围。在不背离本发明的范围的情况下可以实施其他动作。

[0091] 本发明的实施例可以被实施在几乎任何类型的计算设备上，而不管所使用的平台如何。举例来说，激活服务器或移动设备可以对应于计算设备，在后面并且在图7中描述了其中一个或多个组件。举例来说，如图7中所示，计算设备(500)包括一个或多个处理器(502)、相关联的存储器(504)(例如随机存取存储器(RAM)、高速缓冲存储器、闪存等等)、存储设备(506)(例如硬盘、紧致盘驱动器或数字视频盘(DVD)驱动器之类的光学驱动器、闪速记忆棒等等)以及当今的计算机通常所具有的许多其他元件和功能(未示出)。计算设备(500)还可以包括输入装置，比如键盘(508)、鼠标(510)或麦克风(未示出)。此外，计算设备(500)还可以包括输出装置，比如监视器(512)(例如液晶显示器(LCD)、等离子显示器或阴极射线管(CRT)监视器)。计算设备(500)可以通过网络接口连接(未示出)连接到网络(例如局域网(LAN)、因特网之类的广域网(WAN)或者任何其他类型的网络)。本领域技术人员将认识到，存在许多不同类型的计算机系统，并且前面提到的输入和输出装置可以采取其他形式。通常来说，计算设备(500)至少包括对于实践本发明的实施例所必要的最低限度的处理、输入和/或输出装置。

[0092] 此外，本领域技术人员将认识到，前面提到的计算设备(500)的一个或多个元件可以位于远程位置处并且通过网络连接到其他元件。此外，本发明的实施例可以被实施在具有多个节点的分布式系统上，其中本发明的每一个部分(例如数据贮存库、激活应用等等)可以处在分布式系统内的不同节点上。在本发明的一个实施例中，所述节点对应于计算机系统。或者所述节点可以对应于具有相关联的物理存储器的处理器。或者所述节点可以对应于具有共享的存储器和/或资源的处理器或者处理器的微核心。此外，用以实施本发明的实施例的软件指令可以整体上或部分地被临时地或永久性地存储在计算机可读介质上，比如紧致盘(CD)、磁盘、磁带、文件或者任何其他计算机可读存储设备。

[0093] 虽然前面关于有限数目的实施例描述了本发明，但是受益于本公开内容的本领域技术人员将认识到，可以设想到不背离这里所公开的本发明的范围的其他实施例。相应地，本发明的范围应当仅由所附权利要求书限制。

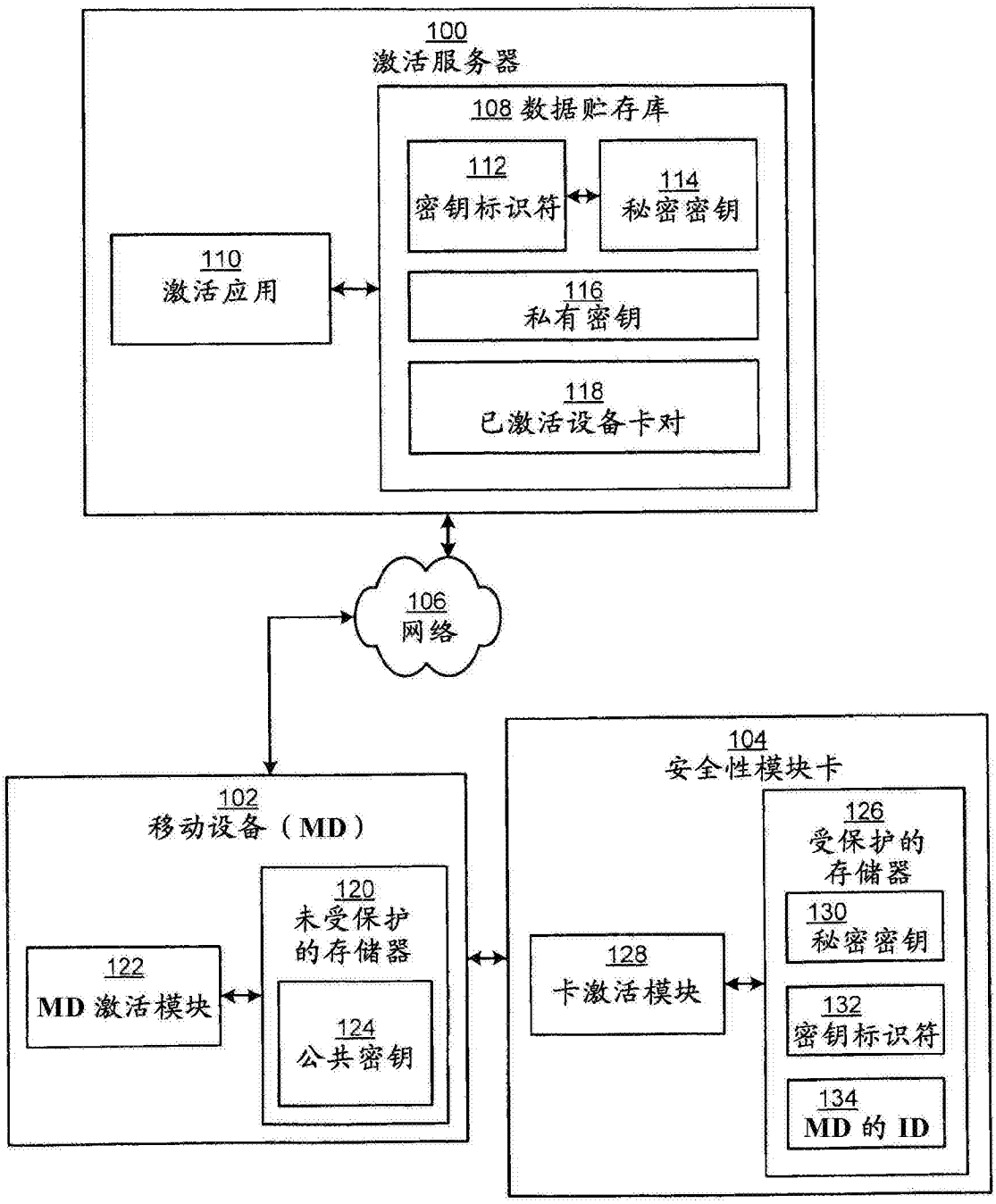

100
激活服务器
108 数据贮存库
112
密钥标识符
114
秘密密钥
110
激活应用
116
私有密钥
118
已激活设备卡对
106
网络
102
移动设备（MD）
120
未受保护的存储器
122
MD 激活模块
124
公共密钥
104
安全性模块卡
126
受保护的存储器
130
秘密密钥
128
卡激活模块
132
密钥标识符
134
MD 的 ID

图1

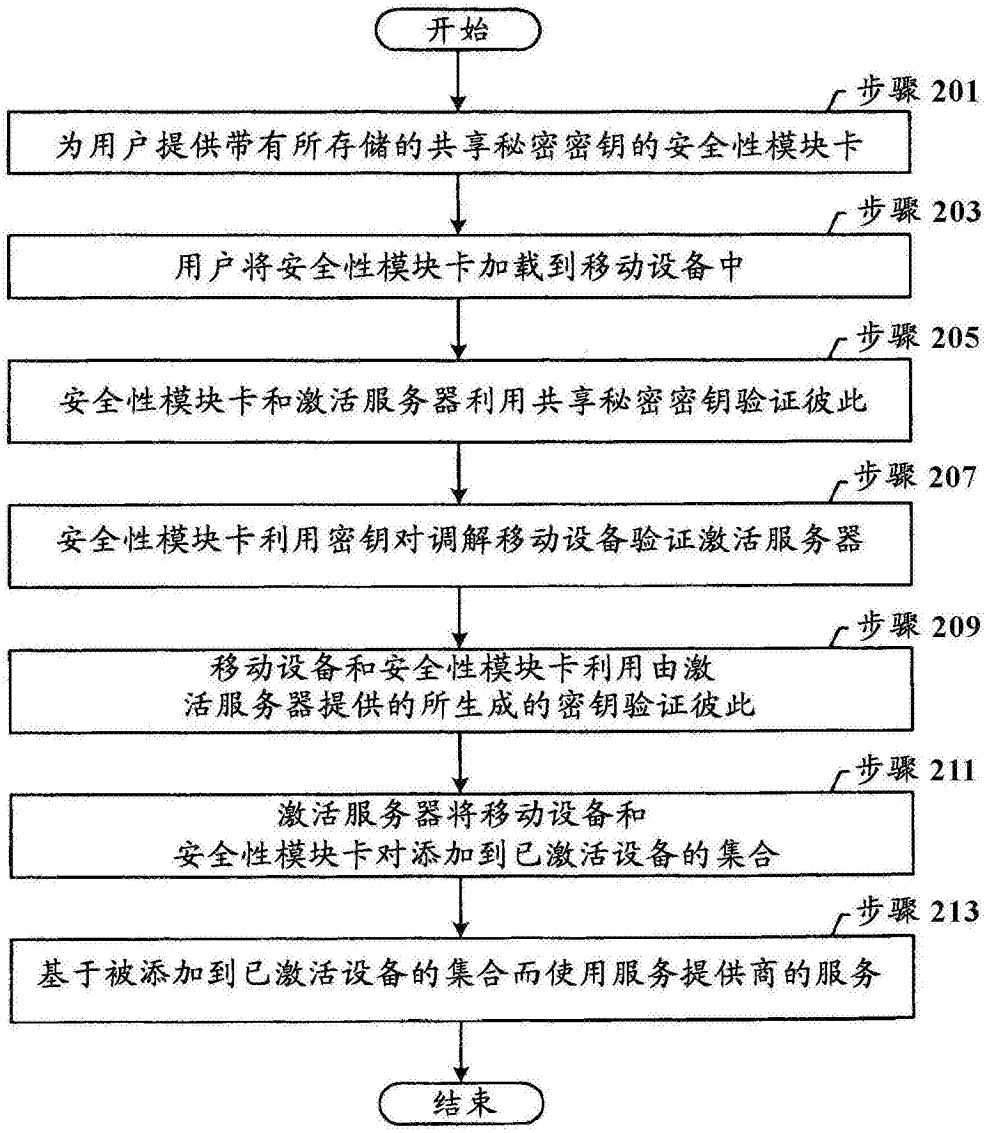

开始
步骤 201
为用户提供带有所存储的共享秘密密钥的安全性模块卡
步骤 203
用户将安全性模块卡加载到移动设备中
步骤 205
安全性模块卡和激活服务器利用共享秘密密钥验证彼此
步骤 207
安全性模块卡利用密钥对调解移动设备验证激活服务器
步骤 209
移动设备和安全性模块卡利用由激活服务器提供的所生成的密钥验证彼此
步骤 211
激活服务器将移动设备和安全性模块卡对添加到已激活设备的集合
步骤 213
基于被添加到已激活设备的集合而使用服务提供商的服务
结束

图2

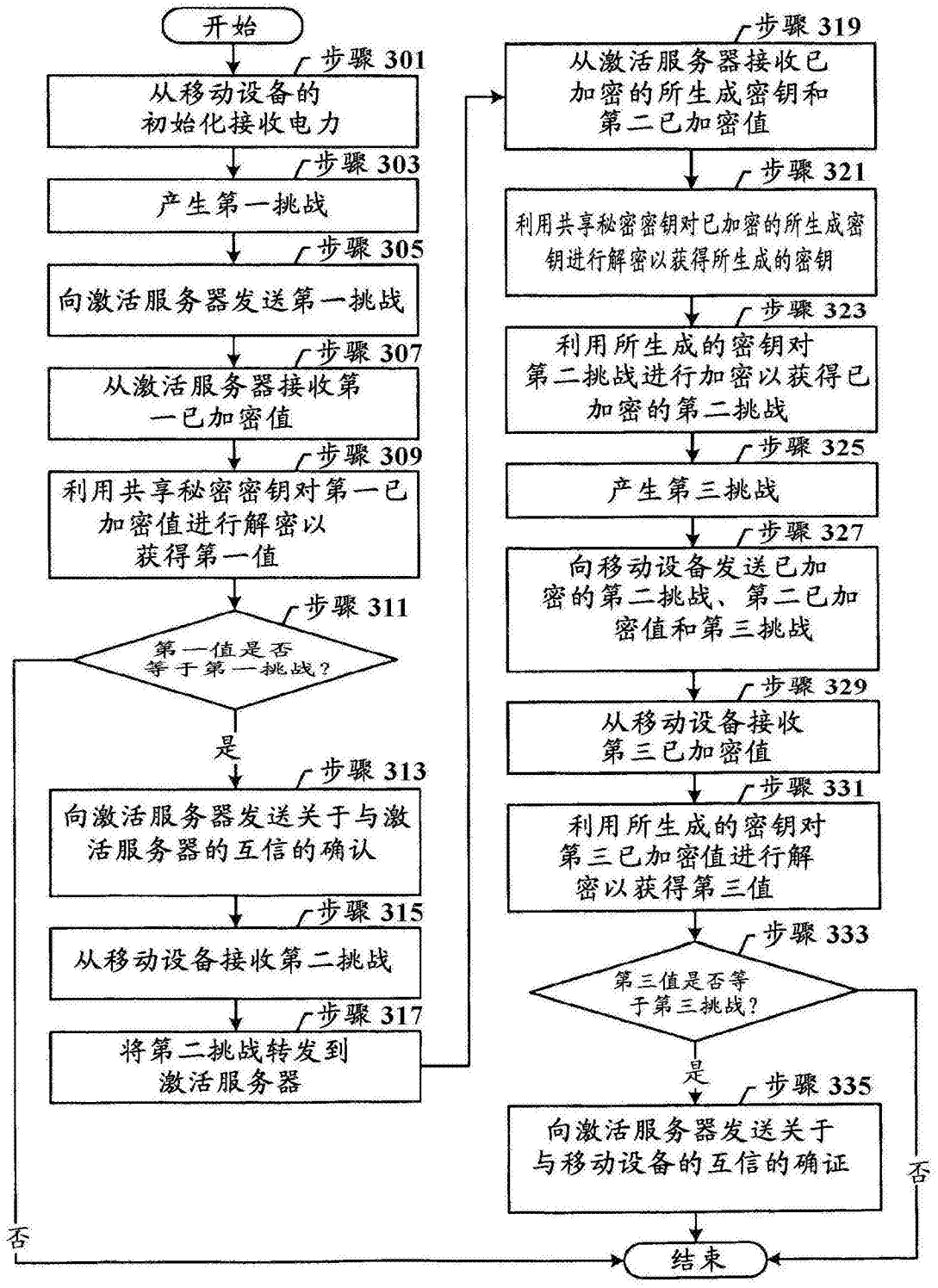

开始
步骤 301
从移动设备的初始化接收电力
步骤 303
产生第一挑战
步骤 305
向激活服务器发送第一挑战
步骤 307
从激活服务器接收第一已加密值
步骤 309
利用共享秘密密钥对第一已加密值进行解密以获得第一值
步骤 311
第一值是否等于第一挑战？
是
否
步骤 313
向激活服务器发送关于与激活服务器的互信的确认
步骤 315
从移动设备接收第二挑战
步骤 317
将第二挑战转发到激活服务器
步骤 319
从激活服务器接收已加密的所生成密钥和第二已加密值
步骤 321
利用共享秘密密钥对已加密的所生成密钥进行解密以获得所生成的密钥
步骤 323
利用所生成的密钥对第二挑战进行加密以获得已加密的第二挑战
步骤 325
产生第三挑战
步骤 327
向移动设备发送已加密的第二挑战、第二已加密值和第三挑战
步骤 329
从移动设备接收第三已加密值
步骤 331
利用所生成的密钥对第三已加密值进行解密以获得第三值
步骤 333
第三值是否等于第三挑战？
是
否
步骤 335
向激活服务器发送关于与移动设备的互信的确证
结束

图3

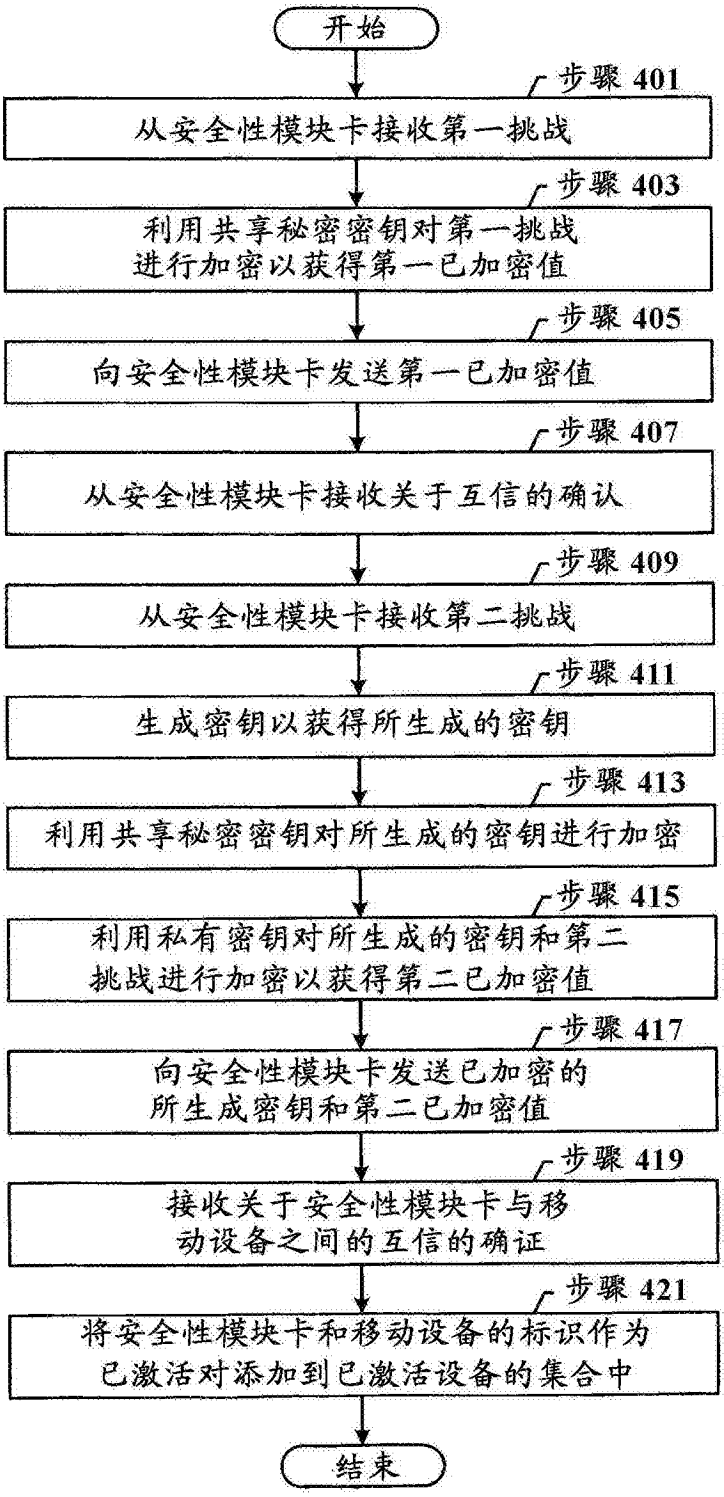

开始
步骤 401
从安全性模块卡接收第一挑战
步骤 403
利用共享秘密密钥对第一挑战进行加密以获得第一已加密值
步骤 405
向安全性模块卡发送第一已加密值
步骤 407
从安全性模块卡接收关于互信的确认
步骤 409
从安全性模块卡接收第二挑战
步骤 411
生成密钥以获得所生成的密钥
步骤 413
利用共享秘密密钥对所生成的密钥进行加密
步骤 415
利用私有密钥对所生成的密钥和第二挑战进行加密以获得第二已加密值
步骤 417
向安全性模块卡发送已加密的所生成密钥和第二已加密值
步骤 419
接收关于安全性模块卡与移动设备之间的互信的确证
步骤 421
将安全性模块卡和移动设备的标识作为已激活对添加到已激活设备的集合中
结束

图4

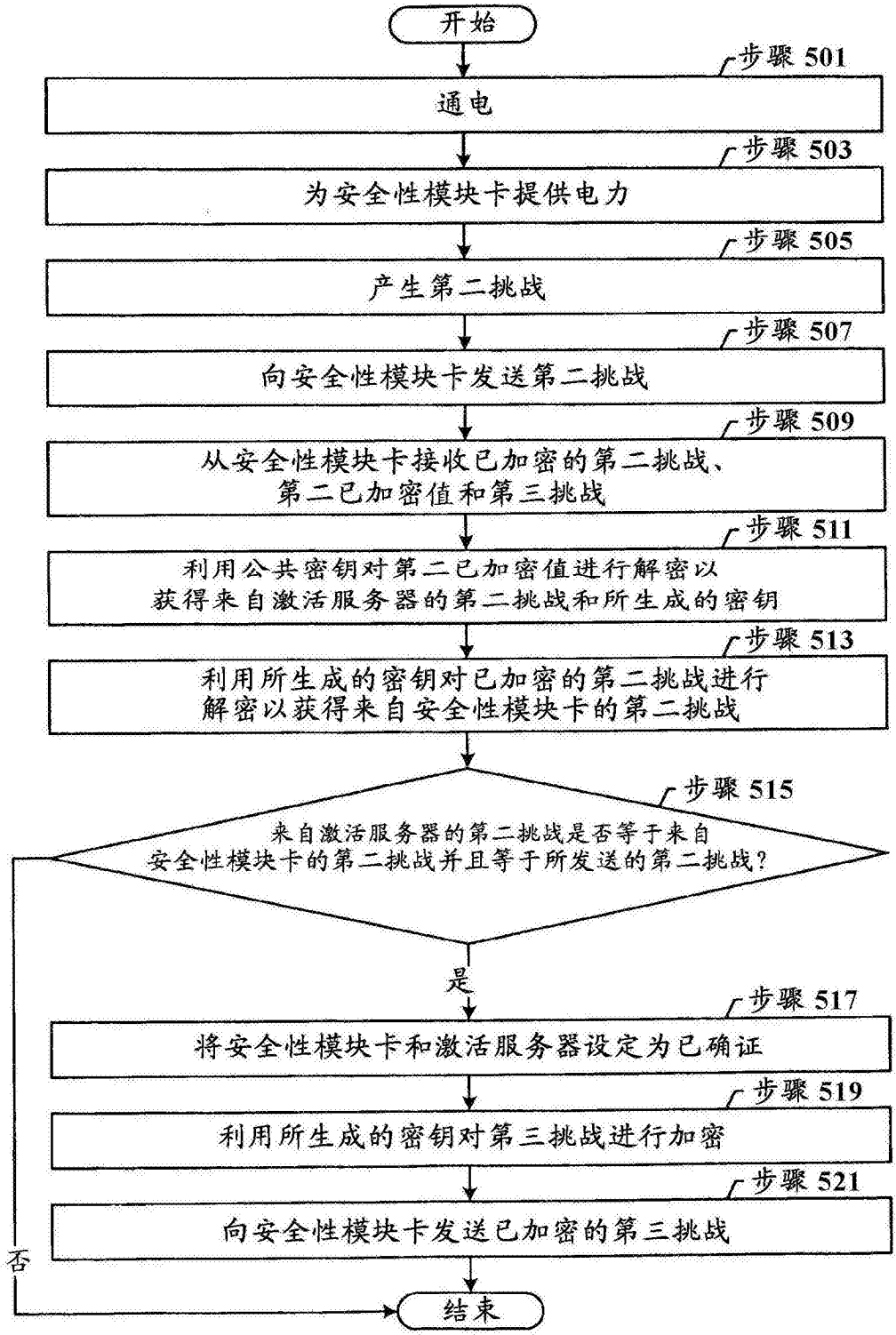

开始
步骤 501
通电
步骤 503
为安全性模块卡提供电力
步骤 505
产生第二挑战
步骤 507
向安全性模块卡发送第二挑战
步骤 509
从安全性模块卡接收已加密的第二挑战、
第二已加密值和第三挑战
步骤 511
利用公共密钥对第二已加密值进行解密以
获得来自激活服务器的第二挑战和所生成的密钥
步骤 513
利用所生成的密钥对已加密的第二挑战进行
解密以获得来自安全性模块卡的第二挑战
步骤 515
来自激活服务器的第二挑战是否等于来自
安全性模块卡的第二挑战并且等于所发送的第二挑战?
是
否
步骤 517
将安全性模块卡和激活服务器设定为已确证
步骤 519
利用所生成的密钥对第三挑战进行加密
步骤 521
向安全性模块卡发送已加密的第三挑战
结束

图5

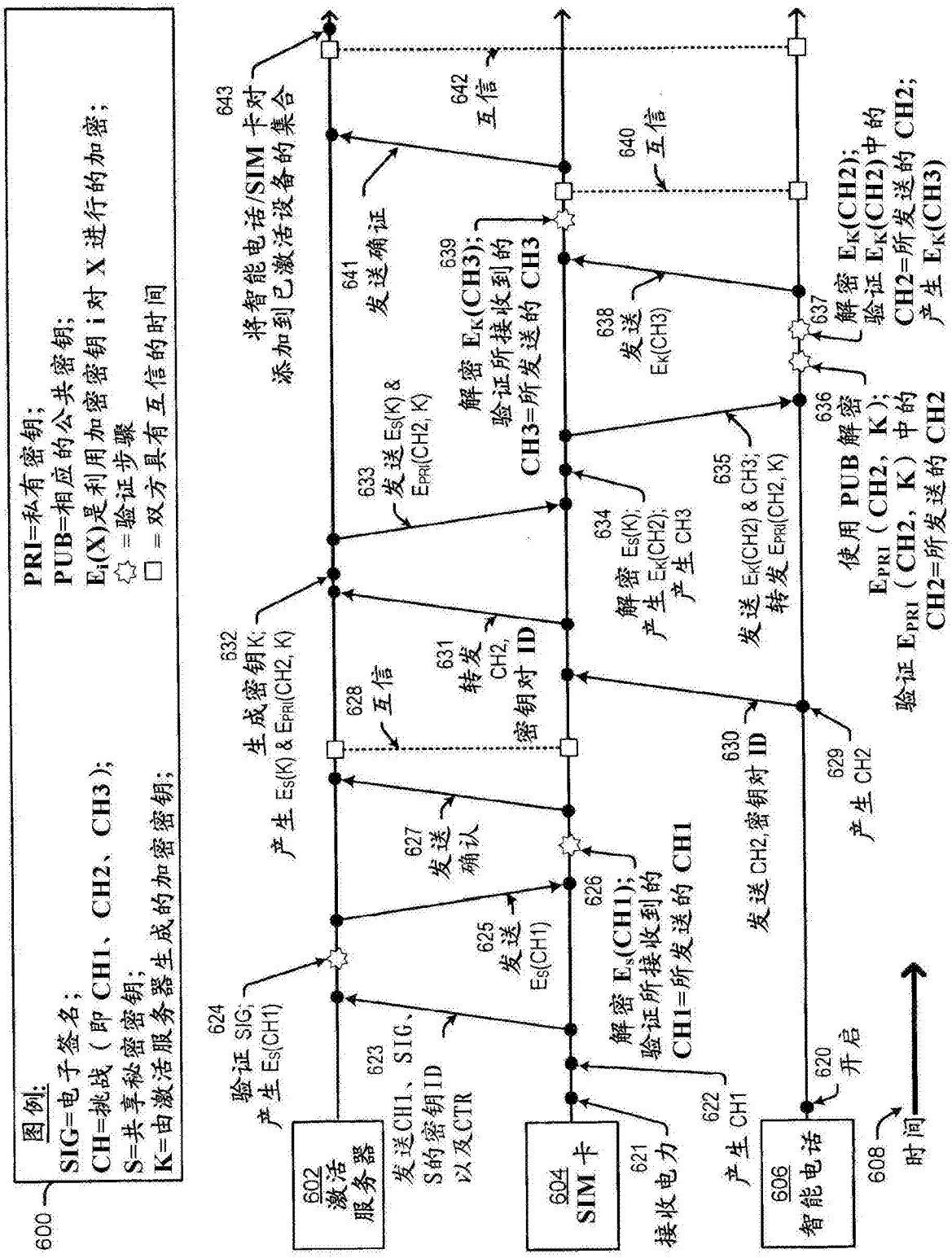

图例:
SIG=电子签名;
CH=挑战(即 CH1、CH2、CH3);
S=共享秘密密钥;
K=由激活服务器生成的加密密钥;
PRI=私有密钥;
PUB=相应的公共密钥;
Ei(X)是利用加密密钥 i 对 X 进行的加密;
☆ =验证步骤
□ =双方具有互信的时间
600
602 激活服务器
604 SIM 卡
606 智能电话
608 时间
620 开启
621 接收电力
622 产生 CH1
623 发送CH1、SIG、S的密钥ID以及CTR
624 验证 SIG;产生 Es(CH1)
625 发送 Es(CH1)
626 解密 Es(CH1);验证所接收到的 CH1=所发送的 CH1
627 发送确认
628 互信
629 产生 CH2
630 发送 CH2,密钥对 ID
631 转发 CH2,密钥对 ID
632 生成密钥K;产生 Es(K) & EPRI(CH2, K)
633 发送 Es(K) & EPRI(CH2, K)
634 解密 Es(K);产生 EK(CH2);产生 CH3
635 发送 EK(CH2) & CH3;转发 EPRI(CH2, K)
636 使用 PUB 解密 EPRI(CH2, K);验证 EPRI(CH2, K)中的 CH2=所发送的 CH2
637 解密 EK(CH2);验证 EK(CH2)中的 CH2=所发送的 CH2;产生 EK(CH3)
638 发送 EK(CH3)
639 解密 EK(CH3);验证所接收到的 CH3=所发送的 CH3
640 互信
641 发送确证
642 互信
643 将智能电话/SIM 卡对添加到已激活设备的集合

图6

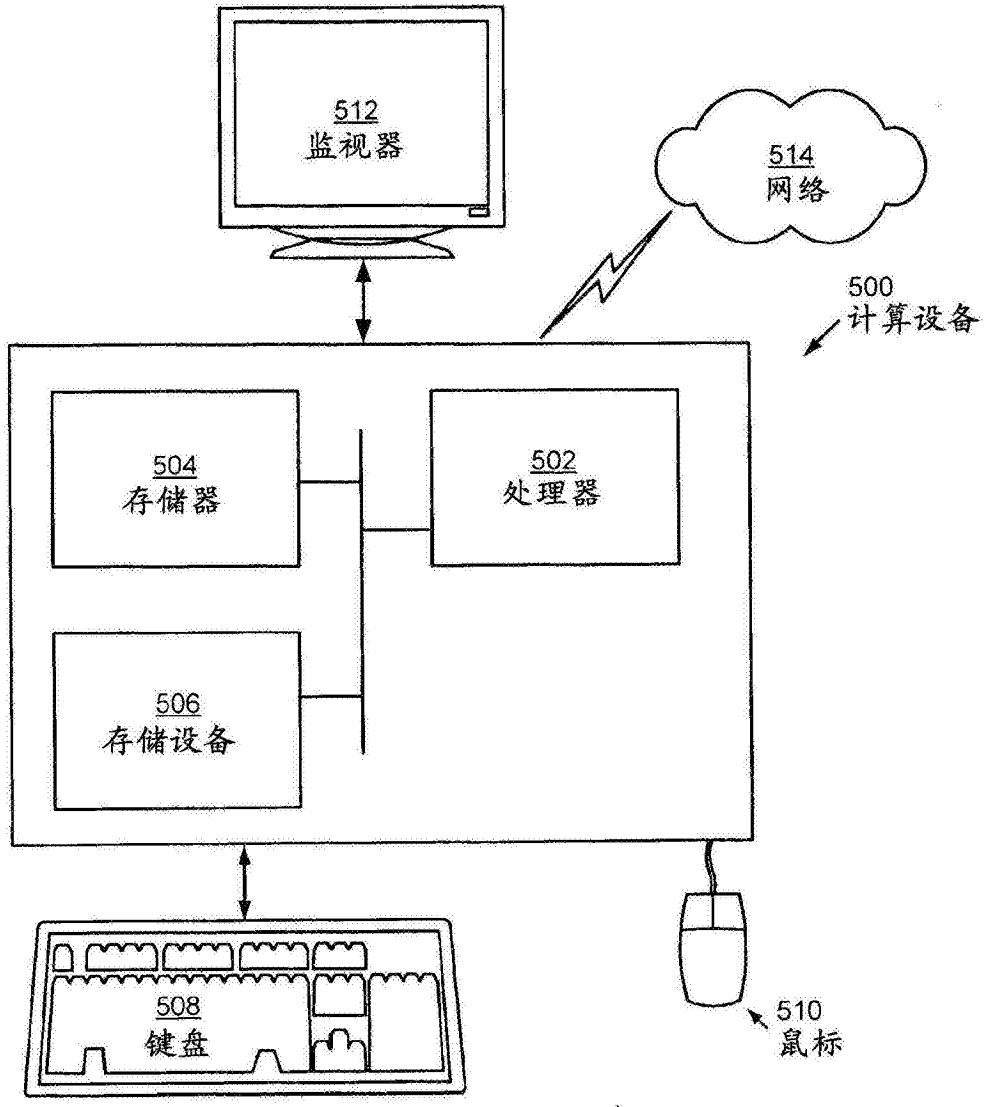



图7