[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/38 (2006.01)
H04Q 7/32 (2006.01)
H04Q 7/22 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810115951.8

[43] 公开日 2008 年 11 月 19 日

[11] 公开号 CN 101309518A

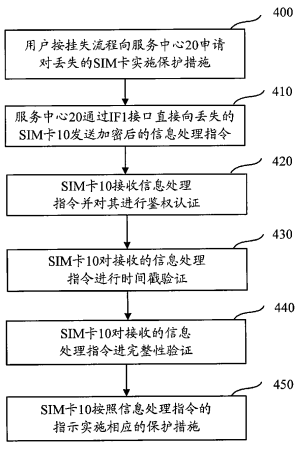
[22] 申请日 2008.6.30
[21] 申请号 200810115951.8
[71] 申请人 中国移动通信集团公司
地址 100032 北京市西城区金融大街 29 号
[72] 发明人 任晓明 李 琳 陆 鸣 乐祖晖 柏洪涛
[74] 专利代理机构 北京同达信恒知识产权代理有限公司
代理人 魏 杉
权利要求书 3 页 说明书 9 页 附图 4 页

[54] 发明名称

对 SIM 卡内信息进行保护的方法、装置及系统

[57] 摘要

本发明公开了一种对 SIM 卡内信息进行保护的方法，该方法为 SIM 卡接收网络侧根据用户的申请内容发送的信息处理指令，该信息处理指令携带命令标识，以及与 SIM 卡进行鉴权认证时需使用的经密钥加密的鉴权信息；所述 SIM 卡接收所述信息处理指令，并根据所述鉴权信息对该信息处理指令进行鉴权认证；所述 SIM 卡确定所述信息处理指令通过鉴权认证后，根据其携带的命令标识确定需实施的保护措施，并执行该保护措施。 这样，信息处理指令便具有了控制 SIM 卡的全部权限，从而可以指示 SIM 卡执行任意一种保护措施，而不再受到权限限制，这便实现了对 SIM 卡的全面保护，大大提高了 SIM 卡的安全性，即使 SIM 卡丢失，也可以避免合法用户遭受严重损失。 本发明同时公开了一种 SIM 卡和一种通信系统。



1、一种对 SIM 卡内信息进行保护的方法，其特征在于，包括步骤：

SIM 卡接收网络侧根据用户的申请内容发送的信息处理指令，该信息处理指令携带命令标识，以及经 SIM 卡密钥加密的鉴权信息；

所述 SIM 卡接收所述信息处理指令，并根据所述鉴权信息对该信息处理指令进行鉴权认证；

所述 SIM 卡确定所述信息处理指令通过鉴权认证后，根据其携带的命令标识确定并执行需实施的保护措施。

2、如权利要求 1 所述的方法，其特征在于，所述 SIM 卡确定接收的信息处理指令通过鉴权认证后，对其进行时间戳验证，并在确定该信息处理指令通过时间戳验证后，执行所述保护措施。

3、如权利要求 1 所述的方法，其特征在于，所述 SIM 卡确定接收的信息处理指令通过鉴权认证后，对进行完整性验证，并在确定该信息处理指令通过完整性验证后，执行所述保护措施。

4、如权利要求 1 所述的方法，其特征在于，所述 SIM 卡确定接收的信息处理指令通过鉴权认证后，在执行保护措施之前，将部分或者全部的用户相关信息发送至指定的终端设备。

5、如权利要 1－4 任一项所述的方法，其特征在于，所述 SIM 卡执行的保护措施包括：对 SIM 卡进行锁定、对 SIM 卡设置 PIN 码、对 SIM 卡内的应用进行锁定、对用户相关信息进行加密，或者将全部或部分用户相关信息进行销毁。

6、如权利要求 5 所述的方法，其特征在于，所述用户相关信息包括用户资料信息、用户应用信息和用户机密信息中的一种或任意组合。

7、一种 SIM 卡，其特征在于，包括：

通信单元，用于接收网络侧发送的信息处理指令，该信息处理指令携带命

令标识，以及经 SIM 卡密钥加密的鉴权信息；

处理单元，用于根据所述信息处理指令携带的鉴权信息对其进行鉴权认证；

执行单元，用于在所述信息处理指令通过鉴权认证后，根据其携带的命令标识确定并执行需实施的保护措施。

8、如权利要求 7 所述 SIM 卡，其特征在于，所述处理单元确定接收的信息处理指令通过鉴权认证后，对其进行时间戳验证；所述执行单元在确定该信息处理指令通过时间戳验证后，执行所述保护措施。

9、如权利要求 7 所述的 SIM 卡，其特征在于，所述处理单元确定接收的信息处理指令通过鉴权认证后，对进行完整性验证；所述执行单元在确定该信息处理指令通过完整性验证后，执行所述保护措施。

10、如权利要求 7 所述的 SIM 卡，其特征在于，所述处理单元确定接收的信息处理指令通过鉴权认证后，在所述执行单元执行保护措施之前，由所述通信单元将部分或者全部的用户相关信息发送至指定的终端设备。

11、如权利要 7－10 任一项所述的 SIM 卡，其特征在于，所述执行单元执行的保护措施包括：对 SIM 卡进行锁定、对 SIM 卡设置 PIN 码、对 SIM 卡内的应用进行锁定、对用户相关信息进行加密，或者将全部或部分用户相关信息进行销毁。

12、一种通信系统，其特征在于，包括：

服务中心，用于根据用户的申请内容向指定的 SIM 卡发送信息处理指令，该信息处理指令至少携带命令标识，以及经 SIM 卡密钥加密的鉴权信息；

SIM 卡，用于接收所述信息处理指令，并根据所述鉴权信息对该信息处理指令进行鉴权认证；以及在确定所述信息处理指令通过鉴权认证后，根据其携带的命令标识确定并执行需实施的保护措施。

13、如权利要求 12 所述的通信系统，其特征在于，所述 SIM 卡确定接收的信息处理指令通过鉴权认证后，对其进行时间戳验证，并在确定该信息处理

指令通过时间戳验证后，执行所述保护措施。

14、如权利要求 12 所述的通信系统，其特征在于，所述 SIM 卡确定接收的信息处理指令通过鉴权认证后，对进行完整性验证，并在确定该信息处理指令通过完整性验证后，执行所述保护措施。

15、如权利要求 12 所述的通信系统，其特征在于，所述 SIM 卡确定接收的信息处理指令通过鉴权认证后，在执行保护措施之前，将部分或者全部的用户相关信息发送至指定的终端设备。

16、如权利要 12－15 任一项所述的通信系统，其特征在于，所述 SIM 卡执行的保护措施包括：对 SIM 卡进行锁定、对 SIM 卡设置 PIN 码、对 SIM 卡内的应用进行锁定、对用户相关信息进行加密，或者将全部或部分用户相关信息进行销毁。

对SIM卡内信息进行保护的方法、装置及系统

技术领域

本发明涉及通信领域，特别涉及一种对SIM卡内信息进行保护的方法、装置及系统。

背景技术

目前，SIM卡的使用已极为普遍，随着SIM卡容量的增大，用户往往将重要的个人信息保存在SIM卡内（如通讯录、彩信、短消息等等），并且，SIM卡作为个人身份识别模块，往往保存有与个人身份相关的重要信息（如数字证书等等）。因此，一旦设置有SIM卡的移动终端丢失，SIM卡内的用户相关信息便有可能被他人窃取，这样，便会给用户造成巨大的损失。

针对上述问题，现有的几种解决方案如下：

1、用户为SIM卡设置PIN码保护；

采用上述解决方案时，若用户忘记设置PIN码保护，则一旦SIM卡丢失，其内部的用户相关信息仍存在被窃取的危险。

2、设置有SIM卡的移动终端丢失后，由该移动终端主动向移动交换中心报告，再由移动交换中心对该移动终端采取相应的控制措施。如：

通过移动终端当前归属的移动交换中心向所述的移动终端发送“信息保护”指令；所述移动终端接收并解码“信息保护”指令，根据“信息保护”指令定义的保护范围对所述移动终端内的信息执行保护操作。

采用上述解决方案时，存在以下缺陷：

参阅图1所示，现有技术下，服务中心（即移动交换中心）下发“信息保护”指令时，需要先将该指令通过IF1接口下发到移动终端内的移动终端保护模块，由该移动终端保护模块通过IF2接口对SIM卡执行保护操作。而实际情况下，移动终端和SIM卡分别具有两个独立的操作系统，即分别具有各自的CPU、OS、

应用程序以及各自的访问控制机制。其中，SIM卡对来自外部的访问（包括移动终端）进行了严格的访问控制，主要是通过严格的密钥体系实现通信双方的权限验证，而移动终端不具有SIM卡上的任何密钥信息。因此，移动终端对SIM卡执行的保护操作是受到严格限制的，也正因为这样，SIM卡才可以由运营商控制，并且成为移动终端中的安全区域。移动终端对SIM卡内信息的访问，也只限于没有保护的信息，以及SIM卡中应用向其开放的信息。而对于有密钥保护的应用和其它信息，移动终端只能对其进行有限访问，或不能访问。因此，SIM卡一旦丢失，移动终端并不能对其保存的全部信息进行保护操作，SIM卡内的信息仍存在被窃取或被盗用的危险。

例如，SIM卡上保存的数字证书是受到密钥保护的，移动终端没有这个密钥，所以不能访问数字证书，但是可以向SIM卡请求签名或身份验证等操作，那么，如果移动终端丢失，非法用户便可以使用该移动终端进行身份验证冒充合法用户，但是合法用户却不能通过服务中心远程指示移动终端把数字证书删除；同样道理，像锁卡、锁定应用这样的操作都不能由移动终端指示SIM卡完成。

显然， 现有的解决方案效果并不理想，SIM卡的丢失仍会给合法用户造成严重损失，使其利益遭受严重侵犯。

发明内容

本发明实施例提供一种对 SIM 卡内信息进行保护的方法、装置及系统，用以在 SIM 卡丢失后，避免因 SIM 卡内信息的泄露而给合法用户造成严重损失。

本发明实施例提供的具体技术方案如下：

一种对 SIM 卡内信息进行保护的方法，包括步骤：

SIM 卡接收网络侧根据用户的申请内容发送的信息处理指令，该信息处理指令携带命令标识，以及经 SIM 卡密钥加密的鉴权信息；

所述 SIM 卡接收所述信息处理指令，并根据所述鉴权信息对该信息处理指

令进行鉴权认证;

所述 SIM 卡确定所述信息处理指令通过鉴权认证后,根据其携带的命令标识确定并执行需实施的保护措施。

一种 SIM 卡,安置在移动终端内,包括:

通信单元,用于接收网络侧发送的信息处理指令,该信息处理指令携带命令标识,以及经 SIM 卡密钥加密的鉴权信息;

处理单元,用于根据所述信息处理指令携带的鉴权信息对其进行鉴权认证,所述 SIM 卡接收所述信息处理指令,并根据所述鉴权信息对该信息处理指令进行鉴权认证;

执行单元,用于在所述信息处理指令通过鉴权认证后,根据其携带的命令标识确定并执行需实施的保护措施。

一种通信系统,包括:

服务中心,用于根据用户的申请内容向指定的 SIM 卡发送信息处理指令,该信息处理指令至少携带命令标识,以及经 SIM 卡密钥加密的鉴权信息;

SIM 卡,安置在移动终端内,用于接收所述信息处理指令,并根据所述鉴权信息对该信息处理指令进行鉴权认证;以及在确定所述信息处理指令通过鉴权认证后,根据其携带的命令标识确定并执行需实施的保护措施。

本发明实施例中,网络侧的服务中心根据用户的申请内容直接向指定的 SIM 卡发送信息处理指令,以指示 SIM 卡执行相应的保护措施,该信息处理指令携带命令标识,以及经 SIM 卡密钥加密的鉴权信息,这样,当信息处理指令通过 SIM 卡的鉴权认证后,便具有了控制 SIM 卡的全部权限,从而可以指示 SIM 卡执行任意一种保护措施,而不再受到权限限制,这便实现了对 SIM 卡的全面保护,大大提高了 SIM 卡的安全性,即使 SIM 卡丢失,也可以避免合法用户遭受严重损失。

另一方面,本发明实施例是针对 SIM 卡进行了技术改造,这样,即使 SIM 卡在丢失后被转移至其他终端也不会影响本发明实例的技术效果,这就进一步

加强了 SIM 卡的安全性。

附图说明

图 1 为本发明现有技术中通信系统体系结构图;

图 2A 为本发明实施例中通信系统体系结构图;

图 2B 为本发明实施例中设置在移动终端内的 SIM 卡功能结构图;

图 3 为本发明实施例中用户申请针对 SIM 卡的信息保护业务流程图;

图 4 为本发明实施例中服务中心指示 SIM 卡处理用户相关信息流程图。

具体实施方式

当设置有 SIM 卡的移动终端丢失后，为了避免因 SIM 卡内信息的泄露而给合法用户造成严重损失；本发明实施例中，SIM 卡接收网络侧（运营商）根据用户的申请内容发送的信息处理指令，该信息处理指令携带命令标识，以及经 SIM 卡密钥加密的鉴权信息；所述 SIM 卡接收所述信息处理指令，并根据所述鉴权信息对该信息处理指令进行鉴权认证;所述 SIM 卡确定所述信息处理指令通过鉴权认证后，根据其携带的命令标识确定并执行需实施的保护措施。

下面结合附图对本发明优选的实施方式进行详细说明。

参阅图 2A 所示，本实施例中，移动通信系统包括服务中心 20 和安置在移动终端内的 SIM 卡 10，其中，

服务中心 20，用于根据用户的申请内容向指定的 SIM 卡 10 发送信息处理指令，该信息处理指令至少携带命令标识，以及与 SIM 卡 10 进行鉴权认证时需使用的，经 SIM 卡密钥加密的鉴权信息;

SIM 卡 10，安置在移动终端内，用于接收所述信息处理指令，并根据所述鉴权信息对该信息处理指令进行鉴权认证；以及在确定所述信息处理指令通过鉴权认证后，根据其携带的命令标识确定并执行需实施的保护措施；其中，用户相关信息包括用户资料信息、用户应用信息和用户机密信息中的一种或任意

组合。本实施例中，安置有 SIM 卡 10 的移动终端可以是手机、笔记本电脑或者个人掌上电脑（PDA）。

参阅图 2B 所示，本实施例中，安置在移动终端内的 SIM 卡 10 包括存储单元 100、通信单元 101、处理单元 102 和执行单元 103，其中，

存储单元 100，用于保存用户相关信息，该用户相关信息可以包含但不限于用户资料信息、用户应用信息（如彩信、短信、通讯录等等）和用户机密信息（如，电子钱包鉴权密钥、数字证书等等；可以是其中的一种或者任意组合）。

通信单元 101，用于接收服务中心 20 下发的信息处理指令，该信息处理指令至少携带命令标识，以及与本 SIM 卡进行鉴权认证时需使用的，经 SIM 卡密钥加密的鉴权信息；

处理单元 102，用于根据所述信息处理指令携带的鉴权信息对其进行鉴权认证，

执行单元 103，用于在信息处理指令通过鉴权认证后，根据其携带的命令标识确定并执行需实施的保护措施。

基于上述系统架构，参阅图 3 所示，本实施例中，用户通过移动终端向服务中心 20 申请针对 SIM 卡 10 的信息保护业务的详细流程如下：

步骤 300：用户向服务中心 20 申请针对 SIM 卡 10 的信息保护业务。

本实施例中，用户可以通过移动终端以发送预设短信的方式或拨打服务电话的方式来完成申请流程，或者，用户还可以直接到营业厅柜台来完成申请流程。

步骤 310：用户通过移动终端从服务中心 20 下载信息保护模块，并将其安装在移动终端内的 SIM 卡 10 中。

步骤 320：SIM 卡 10 对下载的信息保护模块进行验证。

本实施例中，对下载的信息保护模块进行验证时，先采用 HMAC 方式计算出该信息保护模块的验证码（即根据 SIM 卡中预置的密钥计算该信息保护模块的 HASH 值），接着，将计算出的验证码与信息保护模块中携带的验证码进

行比较，判断其是否相同，若是，则认定通过验证并进行后续流程；否则，认定未通过验证，并终止下载流程。

另一方面，应用相关的密钥（以下称应用密钥）也通过上述方式下载到 SIM 卡内，并采用 SIM 卡内预置的密钥加密。

步骤 330：SIM 卡 10 确定下载的信息保护模块通过验证后，向服务中心 20 返回响应消息，并进入等待信息处理指令的状态。

基于上述实施例，用户申请针对 SIM 卡 10 的信息保护业务后，如果将使用该 SIM 卡 10 的移动终端丢失，无论该 SIM 卡 10 是否继续在原移动终端中使用，用户都可以通过服务中心 20 向上述 SIM 卡 10 发送信息保护指令以做相应处理。参阅图 4 所示，本实施例中，用户丢失移动终端后，通过服务中心 20 指示移动终端中的 SIM 卡 10，对其保存的用户相关信息实施保护措施的详细流程如下：

步骤 400：用户向服务中心 20 提出申请，请求对丢失的 SIM 卡 10 实施保护措施。

步骤 410：服务中心 20 向丢失的 SIM 卡 10 发送信息处理指令，该信息处理指令携带有命令标识，以及与 SIM 卡进行鉴权认证时所需的，经 SIM 卡密钥加密的鉴权信息。

本实施例中，上述信息处理指令中携带有命令标识，SIM 卡根据该命令标识确定需要实施何种保护措施，保护措施包含但不限于以下内容：锁定 SIM 卡、对 SIM 卡设置 PIN 码、以及销毁 SIM 卡内的用户相关信息等等。例如，若信息处理指令携带的命令标识为 00，则表示需执行“锁定 SIM 卡”，而若信息处理指令携带的命令标识为 01，则表示需执行“对 SIM 卡设置 PIN 码”。同时，上述信息处理指令中，还携带有与 SIM 卡进行鉴权认证时需使用的，经 SIM 卡密钥加密的鉴权信息，这样，服务中心 20 下发的信息处理指令在通过 SIM 卡的鉴权认证后，便具有了对 SIM 卡进行控制操作的全部权限。

另一方面，上述信息处理指令采用应用密钥进行加密传送。

步骤 420：SIM 卡 10 接收服务中心 20 发送的信息处理指令，并采用应用密钥对其进行解密，以及对解密后的信息处理指令进行鉴权认证。

本实施例中，由于信息处理指令中携带了通过鉴权认证所需的经 SIM 卡密钥加密的鉴权信息，因此，当鉴权认证完成时，该信息处理指令便具有了控制 SIM 卡的全部权限，现有技术下不能通过移动终端指示 SIM 卡完成的保护操作，此时均可实现，例如，指示 SIM 卡锁卡、锁应用等等。

步骤 430：SIM 卡 10 对接收的信息处理指令进行时间戳验证。

所谓时间戳验证，即是将信息处理指令中携带的时间戳和当前时间比对，如果两者差值为未超过设定阈值，则认为该信息处理指令合法，否则，认为该信息处理指令非法，对时间戳的认证可以有效防止指令重放。

步骤 440：SIM 卡 10 对接收的信息处理指令进行完整性验证。

所谓完整性验证，即是采用 HMAC 方式计算该信息处理指令的验证码，并与其携带的验证码进行比对，两者一致则认为指令完整且合法，否则认为指令不完整且非法，对完整性的验证可以有效防止指令被篡改，从而达到了验证信息源的目的。

步骤 450：SIM 卡 10 确定接收的信息处理指令通过验证后，根据其携带的命令标识确定需实施的保护措施，并执行该保护措施。

本实施例中，SIM 卡 10 执行的保护措施可以包含但不限于以下内容：

1、对 SIM 卡进行锁定；

2、对 SIM 卡设置 PIN 码，即若想获得卡内用户相关信息，则需要输入设置的 PIN 码，并在输入次数超过设定阈值时，锁定 SIM 卡；

3、对 SIM 卡内的应用进行锁定；

4、对用户相关信息进行加密，以防止被他人轻易窃取；

5、将全部或部分用户相关信息进行销毁。本实施例中，服务中心 20 可以根据用户提出申请时的指示内容来通知 SIM 卡，是销毁全部用户相关信息还是销毁部分用户相关信息。

上述实施例中，若用户急需获得SIM卡10内保存的用户相关信息，如，通讯录、彩信、电子钱包密钥、数字证书等等，则服务中心20也可以通过信息处理指令指示SIM卡10，完成鉴权认证之后，在实施保护措施之前，先将用户在提出申请时指定的全部或部分用户相关信息发送至指定的终端设备（可以是另一个移动终端或者PC终端）。

另一方面，上述实施例中，步骤430和步骤440的实施只是为了进一步增强操作流程的安全性，若实际应用环境的安全性很高，也可以不执行步骤430和步骤440，或者只执行其中的一种，在此不再赘述。

综上所述，本发明实施例中，服务中心20向SIM卡发送信息处理指令，显然，服务中心20对SIM卡的访问是直接与SIM卡内的管理实体（即信息保护模块）进行通信的，信息保护模块对SIM卡本身具有完全的访问权限，可以实施包括锁卡、锁应用、加密信息、删除信息等等所有保护措施。之所以说运营商可以对SIM卡进行完全控制，是因为运营商（或其它服务商）拥有SIM卡内的密钥（卡主密钥及应用密钥等），因此，无论卡内何种信息，都可以进行以上的各种操作，而不会受类似移动终端的限制。也正因为如此，这种方案可以推广为一种商用的解决方案。

综上所述，本发明实施例中，网络侧的服务中心20根据用户的申请内容直接向指定的SIM卡10发送信息处理指令，以指示SIM卡10执行相应的保护措施，该信息处理指令携带命令标识，以及与SIM卡10进行鉴权认证时需使用的，经SIM卡密钥加密的鉴权信息，这样，当信息处理指令通过SIM卡10的鉴权认证后，便具有了控制SIM卡的全部权限，从而可以指示SIM卡10执行任意一种保护措施，而不再受到权限限制，这便实现了对SIM卡的全面保护，大大提高了SIM卡的安全性，即使SIM卡丢失，也可以避免合法用户遭受严重损失。

此外，即使丢失的SIM卡被转移至其他终端也不会影响本发明实例的技术效果，这就进一步加强了SIM卡的安全性。

显然，本领域的技术人员可以对本发明中的实施例进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明实施例中的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明中的实施例也意图包含这些改动和变型在内。

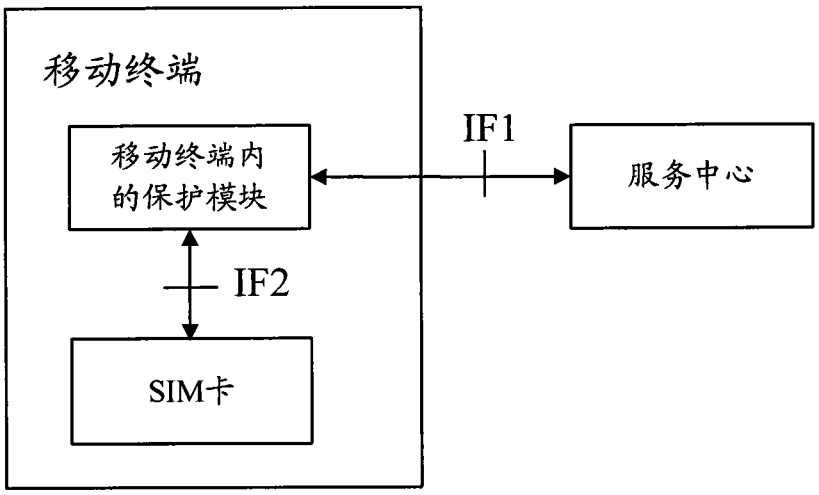


图 1

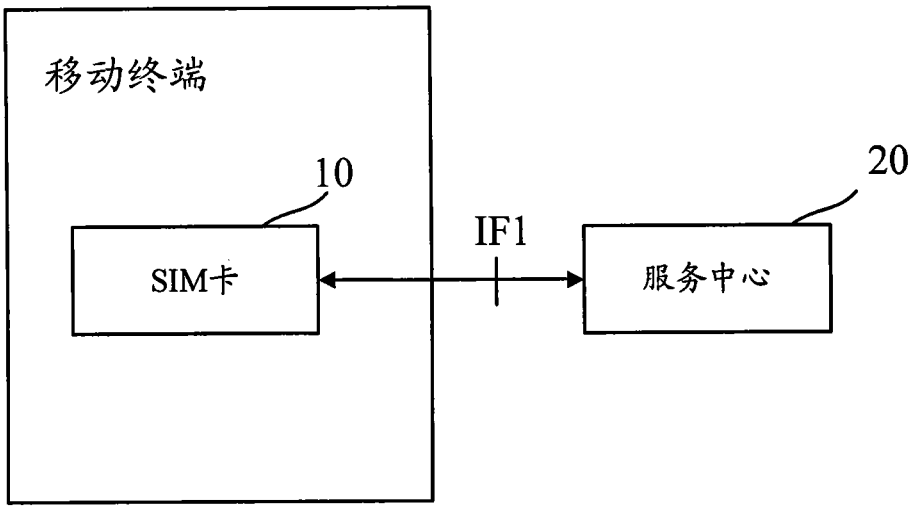


图 2A

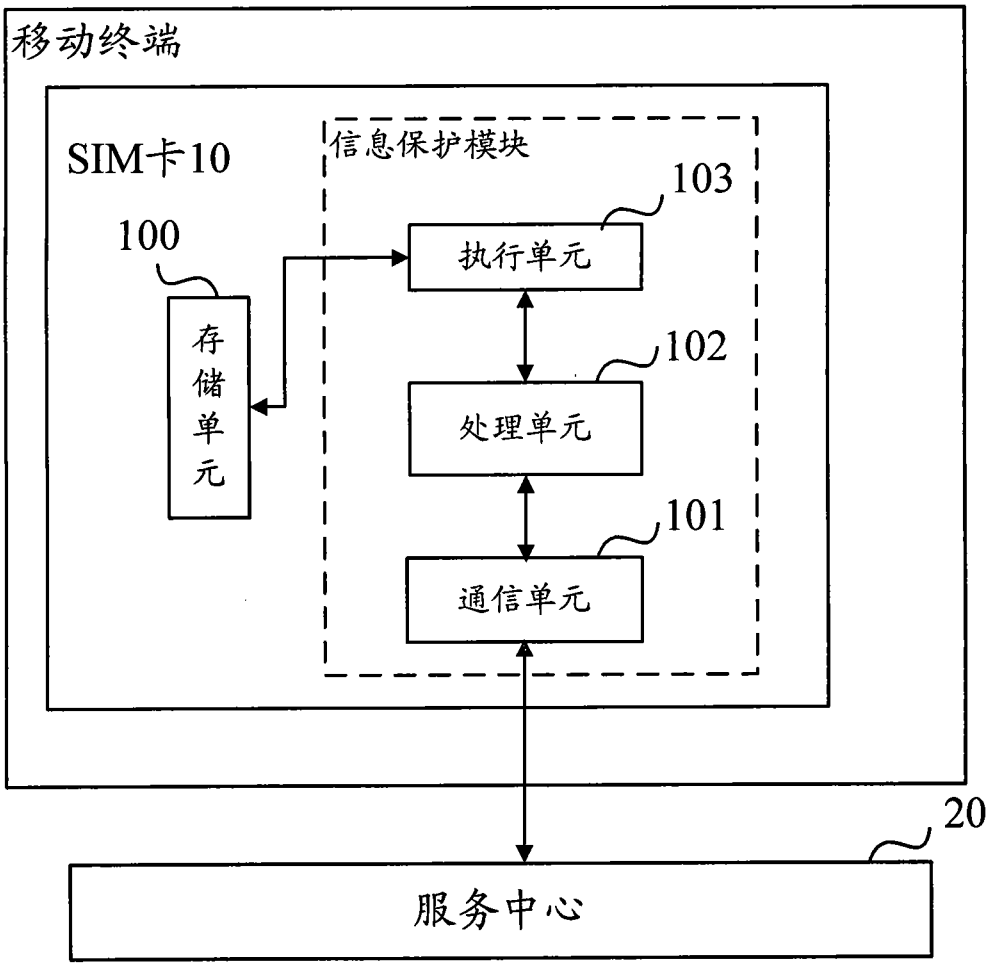

移动终端
SIM卡10
信息保护模块
103
100
执行单元
存储单元
102
处理单元
101
通信单元
20
服务中心

图 2B

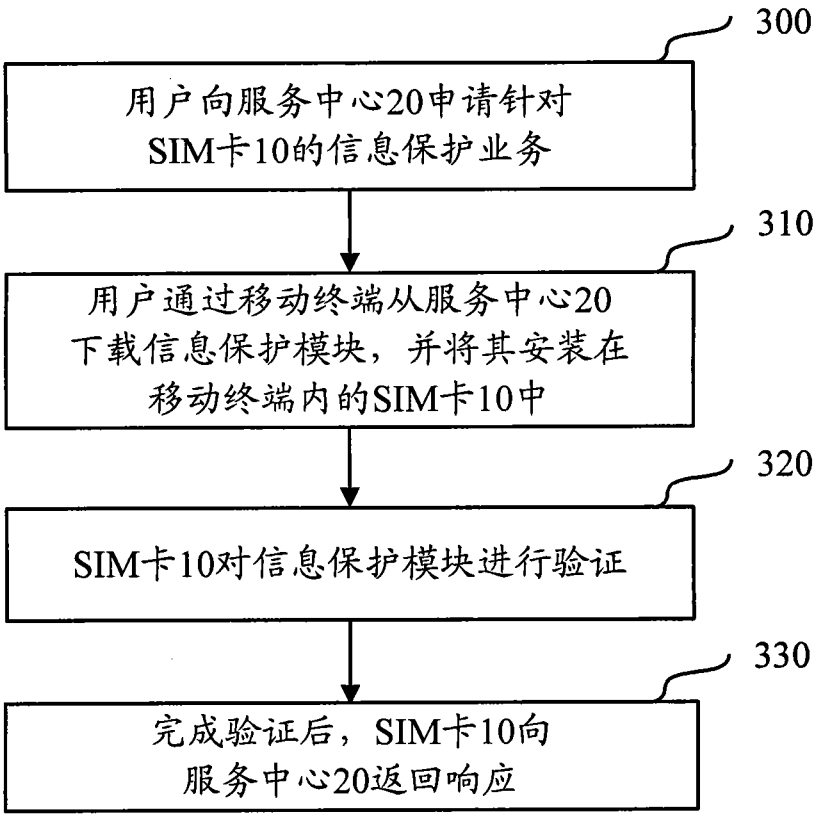

300
用户向服务中心20申请针对SIM卡10的信息保护业务
310
用户通过移动终端从服务中心20下载信息保护模块，并将其安装在移动终端内的SIM卡10中
320
SIM卡10对信息保护模块进行验证
330
完成验证后，SIM卡10向服务中心20返回响应

图 3

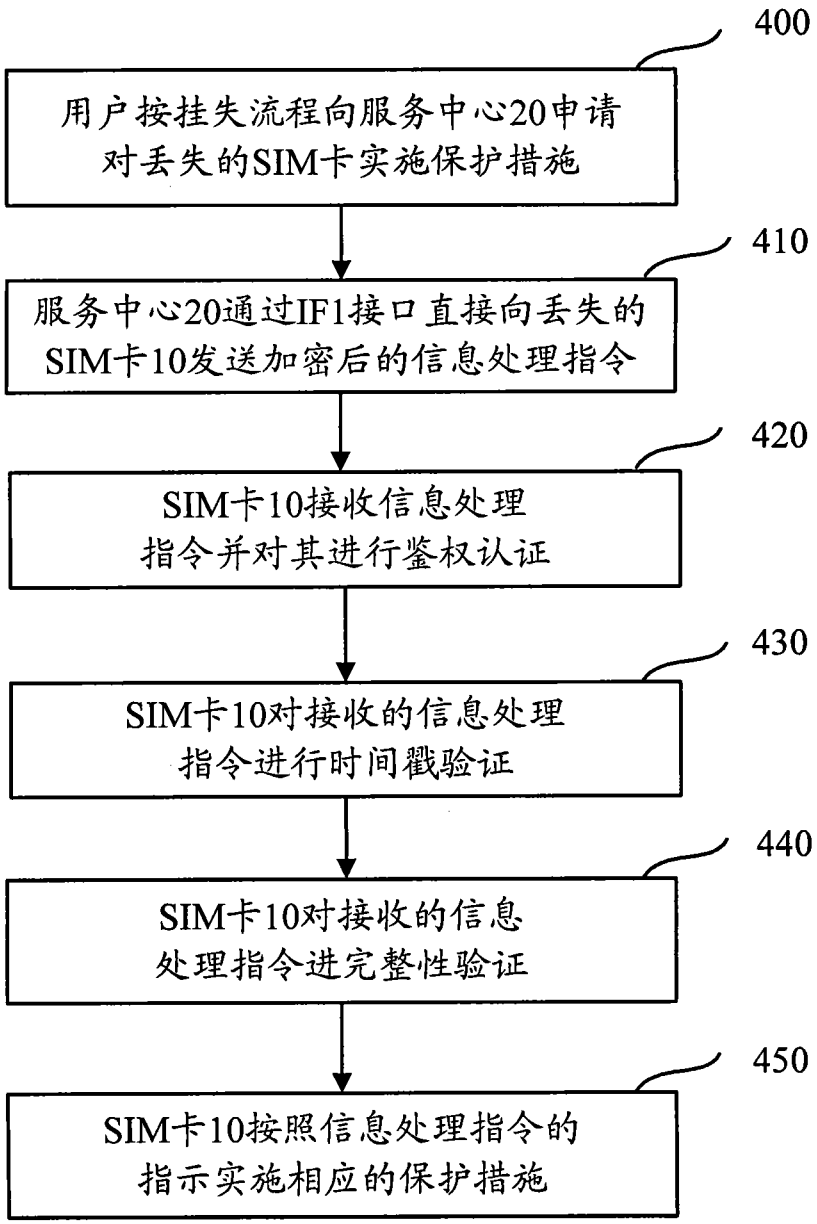

400
用户按挂失流程向服务中心20申请
对丢失的SIM卡实施保护措施
410
服务中心20通过IF1接口直接向丢失的
SIM卡10发送加密后的信息处理指令
420
SIM卡10接收信息处理
指令并对其进行鉴权认证
430
SIM卡10对接收的信息处理
指令进行时间戳验证
440
SIM卡10对接收的信息
处理指令进完整性验证
450
SIM卡10按照信息处理指令的
指示实施相应的保护措施

图 4