[19] 中华人民共和国国家知识产权局

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

[12] 发 明 专 利 说 明 书

专利号 ZL 200610112506.7

[45] 授权公告日 2008 年 7 月 16 日

[11] 授权公告号 CN 100403831C

[22] 申请日 2006.8.22

[21] 申请号 200610112506.7

[73] 专利权人 大唐微电子技术有限公司

地址 100094 北京市海淀区永嘉北路 6 号

[72] 发明人 王 鹏

[56] 参考文献

US2004/0005912A1 2004.1.8

WO2006/072746A1 2006.7.13

CN1547403A 2004.11.17

US2006/0105809A1 2006.5.18

CN1298614A 2001.6.6

审查员 采 健

[74] 专利代理机构 北京安信方达知识产权代理有限公司

代理人 龙 洪 霍育栋

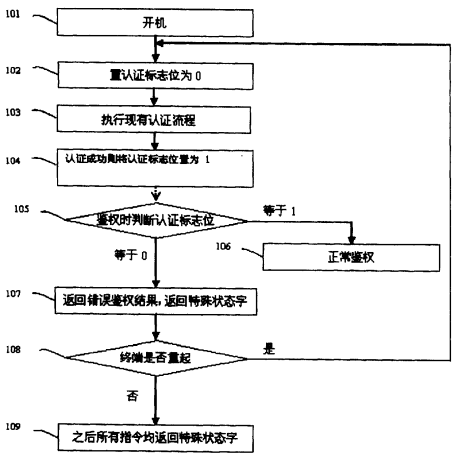
权利要求书 1 页 说明书 6 页 附图 2 页

[54] 发明名称

解决终端与用户识别模块认证漏洞的方法

[57] 摘要

本发明提出一种解决终端和用户识别模块认证漏洞的方法，包含以下步骤：(a)终端开机后，用户识别模块设置初始认证标志；(b)用户识别模块和终端之间执行认证流程；(c)若认证成功，用户识别模块重新设置认证标志为认证成功标志；(d)用户识别模块与网络进行鉴权操作时，判断认证标志，若为认证成功标志，则鉴权正常进行；否则，禁止该终端对该用户识别模块的使用。 本文提出的方法，相对于现有技术，增加了设置认证标志的处理方法，从根本上杜绝了非专用终端对专用用户识别模块的非法使用，提高了这类特殊应用的机密性和安全性。



1、一种解决终端和用户识别模块认证漏洞的方法，包含以下步骤：

（a）终端开机后，用户识别模块设置初始认证标志；

（b）用户识别模块和终端之间执行认证流程；

（c）若认证成功，用户识别模块重新设置认证标志为认证成功标志；

（d）用户识别模块与网络进行鉴权操作时，判断认证标志，若为认证成功标志，则鉴权正常进行；否则，禁止该终端对该用户识别模块的使用。

2、如权利要求 1 所述的方法，其特征在于：所述步骤（d）中，通过用户识别模块返回错误鉴权结果并返回特殊状态字，且在随后的指令中均返回特殊状态字，禁止终端对用户识别模块的使用。

3、如权利要求 2 所述的方法，其特征在于：所述特殊状态字为使终端重启，或使终端停止与用户识别模块的交互的状态字。

4、如权利要求 3 所述的方法，其特征在于：所述特殊状态字为指示与应用无关的错误的状态字。

5、如权利要求 1 所述的方法，其特征在于：所述步骤（d）中，通过用户识别模块返回错误鉴权结果并执行主动式命令 refresh 要求终端重启，禁止终端对用户识别模块的使用。

6、如权利要求 1 所述的方法，其特征在于：所述步骤（d）中通过用户识别模块在随后每条指令执行时不执行原有流程，直接跳出流程，禁止终端对用户识别模块的使用。

7、如权利要求 1 所述的方法，其特征在于：所述步骤（a）中初始认证标志和步骤（c）中认证成功标志为用户识别模块支持范围内任意值。

解决终端与用户识别模块认证漏洞的方法

技术领域

本发明属于移动通信领域，特别涉及一种解决终端与用户识别模块认证漏洞的方法。

背景技术

随着电信增值类业务的发展，利用用户识别模块实现的特殊应用，种类越来越多。其中有一类应用，由于为使用者提供了较低资费或较多的增值服务，因此需要实现此类应用的用户识别模块和终端在终端开机时完成机卡认证。只有正确完成了认证流程，这类应用才能被正常使用，从而保证了此类应用的机密性和安全性。

专用终端与专用用户识别模块的认证，是特殊应用执行的前提。完成了机卡认证，表示专用用户识别模块被使用在专用终端上。反之如果认证失败，则表明终端为非法终端，用户识别模块不应允许其模块内应用的正常执行。

由于在非法终端上需要第一时间内终止机卡交互，因此，终端与用户识别模块的认证过程，是利用 Terminal Profile 指令实现的。由 Gsm11.14 规范可知，Terminal Profile 指令的执行是用户识别模块执行主动式命令的必备前提。因此利用该指令完成机卡认证，能够有效保证认证的及时性。

现有机卡认证流程如图 1 所示。终端开机后，发送 Terminal Profile 指令，用户识别模块执行指令，返回状态字 0X91XX。终端发送 Fetch 指令接收主动式命令数据。用户识别模块返回主动式命令 Get Input 的数据，同时利用该主动式命令向终端传送用户识别模块产生的随机数。终端接收到主动式命令 Get Input 的数据后，对用户识别模块产生的随机数进行加密运算，并通过 Terminal Response 指令返回加密结果。用户识别模块接收终端传送的加密数据后，利用相同的加密算法，对终端的计算结果进行验证。如果验证成功，用户识别模块在随后与网络的鉴权操作中执行正常流程，保证用户正常

使用通讯网络；如果验证失败，用户识别模块执行主动式命令 Display text，显示“专用用户识别模块只能用于专用终端！”的提示文本，并且在随后的鉴权操作中给出错误的鉴权计算结果，以禁止非专用终端使用专用用户识别模块。

以上流程为终端与用户识别模块开机认证的基本流程。当符合此流程的用户识别模块用于大多数非专用终端时，由于终端发送的 Terminal Response 指令中不包含终端对随机数的加密结果，因此用户识别模块显示“专用用户识别模块只能用于专用终端！”的提示文本，并且仍然执行 Get Input 主动式命令要求终端进行认证。循环往复的认证过程，可以达到对非定制终端的限制作用，使其无法正常使用。

但有某些终端（Phase 2 类型），开机后不发送 Terminal Profile 指令，或开机发送 Terminal Profile 指令但不支持主动式命令，或仅在开机过程执行完毕后才支持主动式命令。在这几种情况下，终端与用户识别模块的认证流程无法执行。若用户识别模块认为只要流程能进行到鉴权就认为终端合法，则会执行正确鉴权且允许使用特定的服务。目前商用产品基本都采用该方案，即只要流程执行到鉴权，用户识别模块都会计算正确鉴权结果并通过终端传送给网络。

在开机过程中，用户识别模块与网络需要进行鉴权操作。网络会根据该过程中用户识别模块返回的鉴权结果的正确性，开放或禁止用户对网络的使用。在实际应用过程中，考虑到用户识别模块有较高的安全性，同时由于用户的不断增大对网络带来的压力，网络对用户识别模块的鉴权会采用“选择性鉴权”方式。即网络不是对用户识别模块的每一次鉴权结果都进行判断，而是采取分时或计数等方式对用户多次鉴权过程的某一次进行真正完整意义上的鉴权操作。在这种情况下，非专用终端如果通过了开机过程的交互流程，但未完成认证，则在随后的鉴权过程中，即使用户识别模块返回错误的鉴权计算结果给网络，但由于“选择性鉴权”的原因，本次鉴权仍然有可能通过网络认证，用户同样能够正常使用网络，正常使用终端。

现有的机卡认证流程，在常用终端中可以得到执行，非专用终端无法通过用户识别模块的认证，无法登陆网络。但也有一类终端，开机后没有按照

用户识别模块要求的认证方法正确执行认证流程。终端避开了此类特殊应用要求的认证过程，在具有“选择性鉴权”网络中仍然有可能通过网络认证，用户同样能够正常使用网络，违背了专用用户识别模块只能在专用终端中使用的初衷。这类终端的存在，影响并限制了运营商开展某些特殊应用服务。同时，由于已经投入市场的这类用户识别模块存在安全性原因，因此运营已商蒙受了一定的经济损失。

发明内容

本发明提供一种解决现有非定制终端在具有“选择性鉴权”属性的网络环境下，有可能避开认证，非法使用某些服务的终端与用户识别模块认证漏洞的方法。

本发明提出的解决终端和用户识别模块认证漏洞的方法，包含以下步骤：（a）终端开机后，用户识别模块设置初始认证标志；

（b）用户识别模块和终端之间执行认证流程；

（c）若认证成功，用户识别模块重新设置认证标志为认证成功标志；

（d）用户识别模块与网络进行鉴权操作时，判断认证标志，若为认证成功标志，则鉴权正常进行；否则，禁止该终端对该用户识别模块的使用。

在一实施例中，所述步骤（d）中通过用户识别模块返回错误鉴权结果并返回特殊状态字，且在随后的指令中均返回特殊状态字，从而禁止终端对用户识别模块的使用。所述特殊状态字为使终端重启，或使终端停止与用户识别模块的交互的状态字。所述特殊状态字为指示与应用无关的错误的状态字。

在一实施例中，所述步骤（d）中通过用户识别模块返回错误鉴权结果并执行主动式命令 refresh 要求终端重启，从而禁止终端对用户识别模块的使用。

在一实施例中，所述步骤（d）中用户识别模块在随后每条指令执行时不执行原有流程，从而禁止终端对用户识别模块的使用。

所述步骤（a）中初始认证标志和步骤（c）中认证成功标志可以为用户

识别模块支持范围内任意值。

本发明提出的解决用户识别模块与终端认证漏洞的方法，相对于现有技术，增加了设置认证标志的处理方法，当终端与用户识别模块未进行认证，或认证不成功，则认证标志不变，无法在随后的网络鉴权过程中返回正确的鉴权结果，且通过返回特殊状态字，或发送主动式 refresh 命令，或跳出流程不执行指令等方法，使终端重启或终止终端和用户识别模块的交互，从而从根本上杜绝了非专用终端在具有“选择性鉴权”属性的网络中，对专用用户识别模块的非法使用，提高了这类特殊应用的机密性和安全性，有效保证了电信运营商的经济利益，为需要机卡认证支持的应用的推广奠定了良好的技术基础。

附图说明

图 1 为现有技术中终端与用户识别模块的认证流程图；

图 2 为本发明实施例终端与用户识别模块的认证流程图。

具体实施方式

下面结合附图和实施例对本发明作进一步说明。

图 2 是本发明实施例终端和用户识别模块的认证流程图，其主要步骤如下：

步骤 101：终端开机；

步骤 102：置认证标志位为 0；

步骤 103：执行认证流程，即图 1 中从终端发送 Terminal profile 指令至用户识别模块到终端发送 Terminal Response 指令至用户识别模块，用户识别模块进行认证之间的流程；

步骤 104：若认证成功则将认证标志位设为 1；

步骤 105：用户识别模块与网络进行鉴权操作时判断认证标志位，若为 1，执行步骤 106；若为 0，则执行步骤 107；

步骤 106：正常鉴权，认证结束；

步骤 107：用户识别模块返回错误鉴权结果，返回特殊状态字，如 0x6F00、0x6E00 等，此类状态字指示了与应用无关的错误。用户识别模块执行 APDU 指令时，返回此类特殊状态字会使终端重启，或使终端停止与用户识别模块的交互，提示“用户识别模块错误”等内容，从而禁止非法终端对专用用户识别模块的使用。

返回上述状态字后，终端一般会立刻重启或提示错误。只是不同终端可能会在不同指令执行时收到特殊状态字而重启或提示错误。本发明并不局限于上述列出的状态字，只要能达到限制终端对用户识别模块使用的任意特殊状态字都可以采用。

步骤 108：用户识别模块判断终端是否重启，如果是，则执行步骤 102；如果不是，则执行步骤 109；

步骤 109：用户识别模块在执行所有指令时均返回特殊状态字，至终端重启或终端停止与用户识别模块交互。

在本发明另一实施例中，用户识别模块也可以在步骤 107 或 109 时，通过发送主动式命令——refresh，要求终端执行重启操作，从而禁止非法终端对用户识别模块的正常使用。

在本发明又一实施例中，用户识别模块可以在步骤 107 时，通过执行所有指令时都不执行指令原来的流程，而直接跳出流程，令指令无法实现原有的功能，从而禁止非专用终端对专用用户识别模块的正常使用。在本实施例中，在用户识别模块跳出流程后，终端不重启，没有图 2 中的步骤 108 和 109。

对于背景技术中提到的开机后不发送 Terminal Profile 指令，或开机发送 Terminal Profile 指令但不支持主动式命令，或仅在开机过程执行完毕后支持主动式命令的终端来说，由于没有执行认证流程，因此开机后“认证标志位”始终为 0；另外，对于支持开机主动式命令的终端，即使能够执行认证流程，但由于在认证过程中没有执行专用终端特有的数据加密流程，因此认证无法

成功，开机后“认证标志位”同样始终为0。因此，对于所有非专用终端，从执行鉴权指令开始，用户识别模块通过对每条指令均返回特殊状态字，或执行 refresh 主动式命令，或不实现指令原有功能直接跳出流程，使终端停止与用户识别模块的交互，或使终端重启，从而从根本上杜绝了非专用终端在具有“选择性鉴权”属性的网络中，对专用用户识别模块的非法使用。

本发明采用的认证标志除了上述的认证标志位外，还可以为用户识别模块支持范围内任意值，只要设置初始标志位值和认证成功后标志位值不同即可。

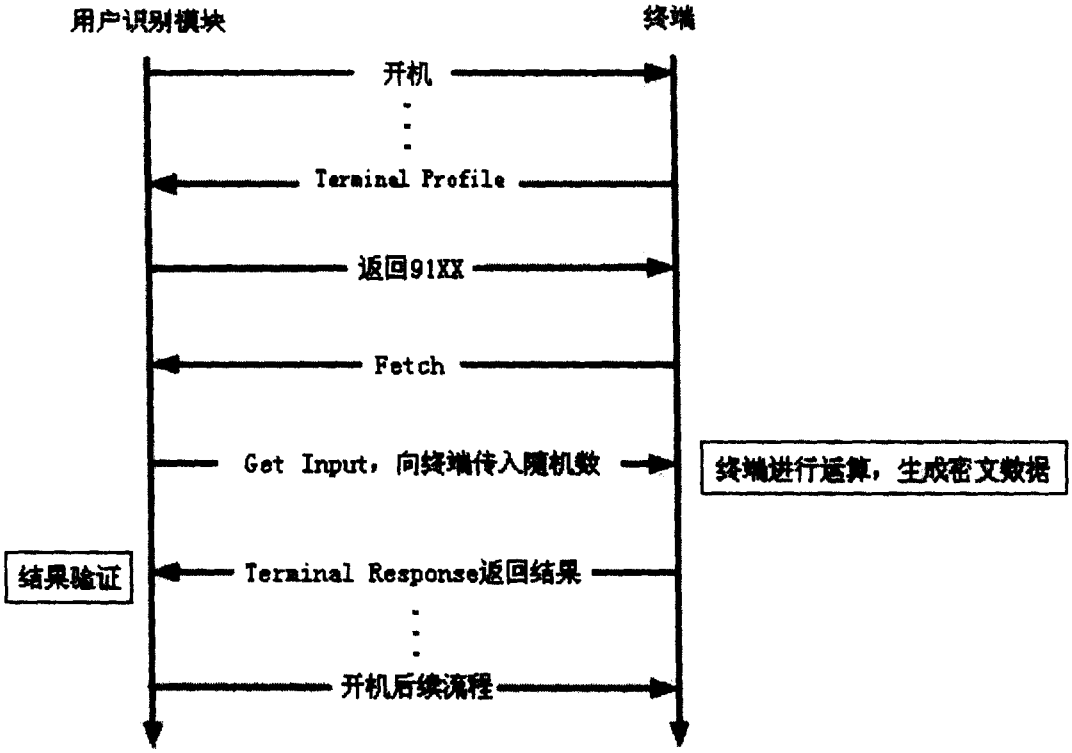

用户识别模块
终端
开机
Terminal Profile
返回91XX
Fetch
Get Input，向终端传入随机数
终端进行运算，生成密文数据
结果验证
Terminal Response返回结果
开机后续流程

图 1

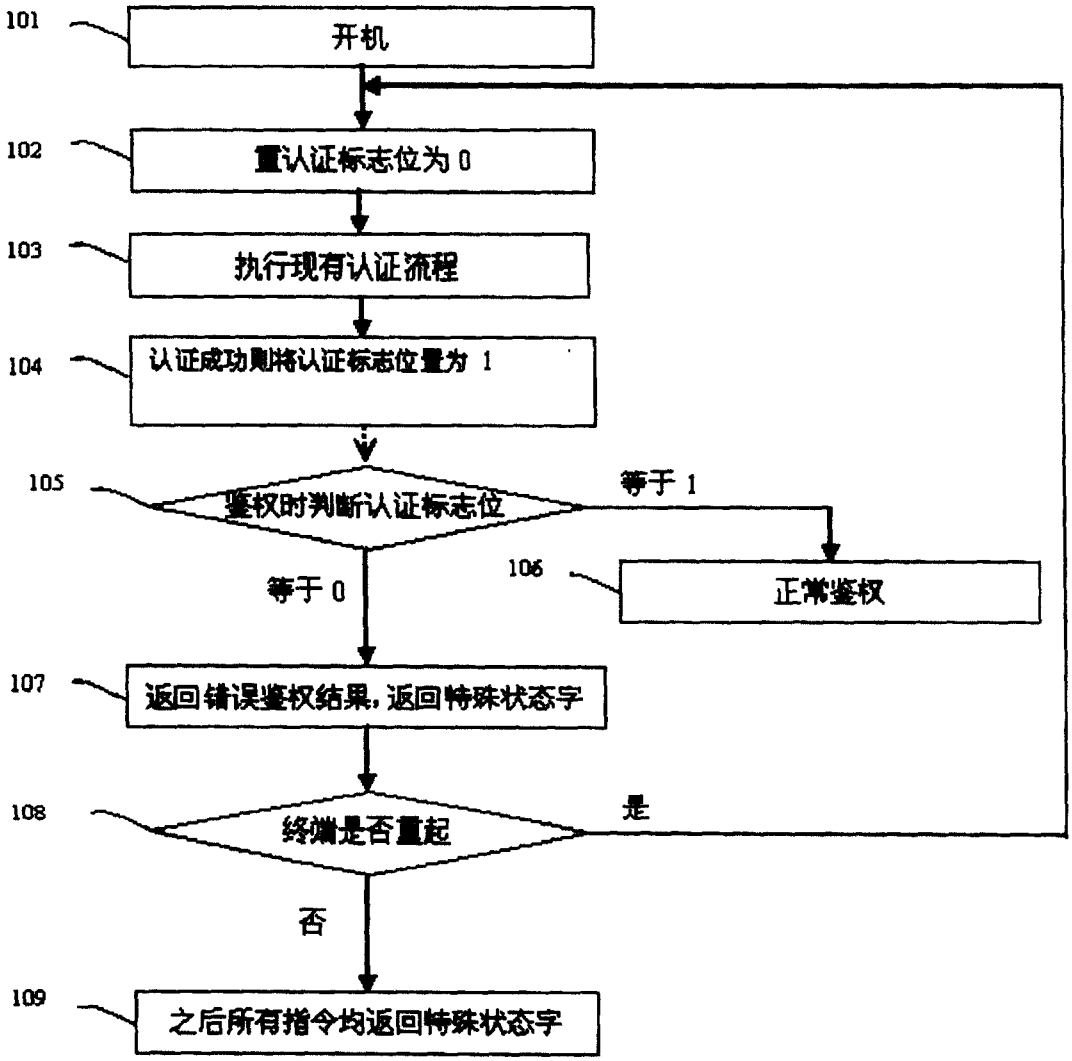

101
开机
102
重认证标志位为 0
103
执行现有认证流程
104
认证成功则将认证标志位置为 1
105
鉴权时判断认证标志位
等于 1
106
正常鉴权
等于 0
107
返回错误鉴权结果，返回特殊状态字
108
终端是否重起
是
否
109
之后所有指令均返回特殊状态字

图 2