[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
H04L 12/22 (2006.01)

[12] 发明专利说明书

专利号 ZL 200480005677.9

[45] 授权公告日 2009 年 8 月 26 日

[11] 授权公告号 CN 100534090C

[22] 申请日 2004.3.2
[21] 申请号 200480005677.9
[30] 优先权
[32] 2003. 3. 3 [33] EP [31] 03100516.8
[86] 国际申请 PCT/FI2004/000111 2004.3.2
[87] 国际公布 WO2004/080027 英 2004.9.16
[85] 进入国家阶段日期 2005.9.1
[73] 专利权人 诺基亚有限公司
地址 芬兰埃斯波
[72] 发明人 L·皮基维
[56] 参考文献
US2002/0123335A1 2002.9.5
WO02/075677A1 2002.9.26
EP1107627A1 2001.6.13
CN1392743A 2003.1.22
EP1246434A1 2000.10.2
WO02/073552A1 2002.9.19
审查员 刘冬生
[74] 专利代理机构 北京市金杜律师事务所
代理人 吴立明

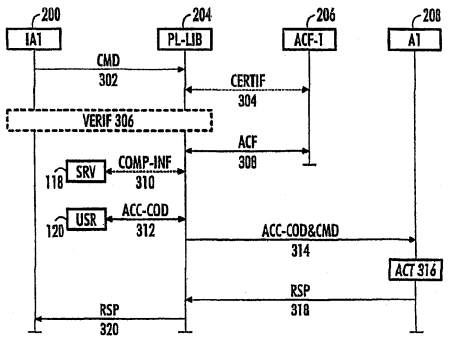
权利要求书 3 页 说明书 10 页 附图 1 页

[54] 发明名称

安全元件命令方法和移动终端

[57] 摘要

本发明涉及一种用于命令移动终端的安全元件的方法，并且涉及一种移动终端。 移动终端安装的应用向移动终端的平台库发布(302)命令。 然后，平台库从安全元件的访问控制文件中读取(308)信息。 在这之后，根据访问控制文件的信息，平台库从用户获得(312)用于安全元件的访问码，并且向安全元件输入(314)获得的访问码和命令。 如果访问码被安全元件核准，那么根据安全元件中的命令执行(316)动作。



1. 一种用于命令移动终端的安全元件的方法，特征在于，所述方法包括:

由所述移动终端安装的应用向所述移动终端的平台库发布（302）命令;

由所述平台库从所述安全元件的访问控制文件中读取（308）信息;

由所述平台库根据所述访问控制文件的信息从用户获得（312）用于所述安全元件的访问码;

由所述平台库向所述安全元件输入（314）所获得的访问码和所述命令；以及

如果所述访问码被所述安全元件核准，那么根据所述安全元件中的命令执行（316）动作。

2. 根据权利要求 1 所述的方法，特征在于，获得包括用存储在所述访问控制文件中的提示信息提示所述用户需要所述访问码。

3. 根据权利要求 1 所述的方法，特征在于，获得包括显示存储在所述访问控制文件中的关于访问码使用的使用信息。

4. 根据权利要求 1 所述的方法，特征在于，获得包括显示存储在所述访问控制文件中的帮助信息。

5. 根据权利要求 1 所述的方法，特征在于，所述方法还包括:

从由存储在所述访问控制文件中的网络地址所标识的服务器下载补充所述访问控制文件的信息的信息。

6. 根据权利要求 5 所述的方法，特征在于，所述方法还包括:

用存储在所述访问控制文件中的安全证书证实所述补充信息。

7. 根据权利要求 5 所述的方法，特征在于，所述方法还包括:

在所述安全元件中和／或在所述移动终端中存储所述补充信息。

8. 根据权利要求 5 到 7 中任一权利要求所述的方法，特征在于，

所述补充信息与所述访问控制文件的信息是不同的语言。

9. 根据权利要求 1 到 7 中任一权利要求所述的方法，特征在于，所述访问控制文件的信息包括码，并且对应于所述码的实际信息项存储在所述平台库中和／或由存储在所述访问控制文件中的网络地址所标识的服务器中。

10. 根据权利要求 1 到 7 中任一权利要求所述的方法，特征在于，所述访问控制文件的信息包括访问码使用指令。

11. 一种移动终端，包括:

平台库（204）;

安装的应用（200）;

用户接口（104）; 以及

安全元件（106）;

特征在于:

所述安装的应用（200）配置成向所述平台库（204）发布命令;

特征在所述平台库（204）配置成从所述安全元件（106）的访问控制文件（206）读取信息，根据所述访问控制文件（206）信息经由所述用户接口(104）从用户获得用于所述安全元件（106）的访问码，并且向所述安全元件（106）输入所获得的访问码和所述命令;以及

所述安全元件（106）配置成在所述安全元件（106）核准所述访问码时根据所述命令执行动作。

12. 根据权利要求 11 所述的移动终端，特征在于，所述用户接口（104）配置成用存储在所述访问控制文件（206）中的提示信息提示所述用户需要所述访问码。

13. 根据权利要求 11 所述的移动终端，特征在于，所述用户接口（104）配置成显示存储在所述访问控制文件(206）中的关于所述访问码使用的使用信息。

14. 根据权利要求 11 所述的移动终端，特征在于，所述用户接口（104）配置成显示存储在所述访问控制文件(206）中的帮助信息。

15. 根据权利要求 11 所述的移动终端，特征在于，所述平台库（204）配置成从由存储在所述访问控制文件（206）中的网络地址所标识的服务器（118）下载补充所述访问控制文件（206）信息的信息。

16. 根据权利要求 15 所述的移动终端，特征在于，所述平台库（204）配置成用存储在所述访问控制文件（206）中的安全证书证实所述补充信息。

17. 根据权利要求 15 所述的移动终端，特征在于，所述平台库（204）配置成在所述安全元件（106）中和/或在所述移动终端（100）中存储所述补充信息。

18. 根据权利要求 15 到 17 中任一权利要求所述的移动终端，特征在于，所述补充信息与所述访问控制文件（206）信息是不同的语言。

19. 根据权利要求 11 到 17 中任一权利要求所述的移动终端，特征在于，所述访问控制文件（206）信息包括码，并且对应于所述码的实际信息项存储在所述平台库（204）中和／或在由存储在所述访问控制文件（206）中的网络地址所标识的服务器（118）中。

20. 根据权利要求 11 到 17 中任一权利要求所述的移动终端，特征在于，所述访问控制文件（206）信息包括访问码使用指令。

安全元件命令方法和移动终端

技术领域

本发明涉及一种用于命令移动终端的安全元件的方法，并且涉及一种移动终端。

背景技术

随着移动终端软件环境的开放并且伴随着 3G(第三代)规范，对于第三方(包括蜂窝运营商和移动终端制造商)为移动终端编制处理终端中的安全元件（通常是智能卡）的应用成为可能。由用户安装在移动终端中的应用可以被称作安装的应用。更持久地驻留在移动终端中的应用通常由制造商在设备制造时安装到移动终端中，并且被称作平台库。在该申请的全文中，我们使用这两个术语：安装的应用和平台库。 通常，用户在她/他得到移动终端之后在移动终端中安装安装的应用，而制造商在向端客户销售移动终端前在移动终端中安装平台库或其一部分。

Java™标准化组织(Java™ Community Process JCP)专家组在称作JSR-177(Java™规范请求 177)的规范中定义了用于移动终端和安全元件的 Java™的编程环境。因为安装的应用，例如 Java™ midlet，可以从多个来源装载入终端，并且那些应用的安全环境不同于安全元件的安全环境，所以需要一种机制，通过这种机制安全元件应用可以定义能够调用在安全元件应用上的命令的安装的应用。

可以在安装的应用上签名，并且移动终端将验证签名从而验证安装的应用的起源。移动终端可以对来自蜂窝运营商、制造商及其它的应用有各自的限制。所以应用的发布者在 midlet 上签名，移动终端验证签名，并且如果签名是蜂窝运营商的签名，那么 midlet 得

到指定用于那个安全域的权利（例如可以进行电话呼叫，可以访问安全元件，但不能写入移动终端操作系统区域）。

移动终端安全元件，例如 SIM（客户身份模块 Subscriber Identity Module）或 USIM（UMTS SIM）卡、终端本身的安全元件或终端附件中的安全元件，需要用于数据的安全存储和处理。数字签名的创建，例如，需要在其中执行操作的非常安全的元件，因为私有密钥不能被泄漏，从而私有密钥不能离开安全元件。安全元件的其它用途是对网络的访问认证、存储电子现金价值或票、或处理金融交易。所以需要安装的应用来访问安全元件以得到这些改进的特点。

基本的问题是，在安全元件中运行的应用本身不能验证访问它的安装的应用具有适当的权利并且是有效的应用。蜂窝运营商想要将 SIM 访问限制到来自运营商本身的应用。攻击应用可以伪造安全码用于访问授权，并且不可能传送整个安装的应用到安全元件来用于验证（实际上可能是这样，给出有效的应用用于验证，但是在访问授权之后攻击应用使用元件）。

EP1246434 公开了一种用于无线通信系统的移动终端以及包括保护以避免在使用期间对于移动终端的一个或多个功能的非授权使用的软件产品。

EP1107627 公开了一种用于保护存储于移动通信设备的存储器中的用户数据的方法，移动通信设备尤其是移动电话。

WO02/075677 涉及一种基于注册数据库的智能卡并且在该数据库中，移动终端应用、基于 SIM 卡的应用、PDA 应用等均可获得访问、创建新条目、读取已存储信息或更新旧信息。

发明内容

本发明的目标是提供一种改进的方法用于命令移动终端的安全元件。

根据本发明的一个方面，提供一种用于命令移动终端的安全元件的方法，该方法包括：由移动终端安装的应用向移动终端的平台

库发布命令；由平台库从安全元件的访问控制文件中读取信息；由平台库根据访问控制文件的信息从用户获得用于安全元件的访问码；由平台库向安全元件输入获得的访问码和命令；以及如果访问码被安全元件核准，那么根据安全元件中的命令执行动作。

本发明的另一目标是提供改进的移动终端。

根据本发明的另一方面，提供一种移动终端，包括平台库；安装的应用；用户接口；以及安全元件；安装的应用配置成向平台库

发布命令；平台库配置成从安全元件的访问控制文件中读取信息，根据访问控制文件的信息经由用户接口从用户获得用于安全元件的访问码，并且向安全元件输入获得的访问码和命令；并且安全元件配置成在安全元件核准访问码的条件下按照命令执行动作。

本发明的实施例在从属权利要求中描述。

本发明提供了若干优点。移动终端不需要知道特定的安全元件的属性，因此，只要安全元件包括带有用于访问码获得的信息的访问控制文件，一个移动终端就可以使用多个不同的安全元件。移动终端的安全性增加了，因为安装的应用不能直接处理安全元件和访问码。本发明允许安全元件定义它自己的安全界限。

附图说明

下面，将参考优选实施例和附图更详细地描述本发明，附图中，

图 1 是示出移动终端结构的简化框图；

图 2 示出控制单元和安全元件的结构；以及

图 3 是示出用于命令移动终端的安全元件的信号序列图。

具体实施方式

参考图 1，描述移动终端 100 的结构示例。移动终端 100 可以是关于普适计算的便携式设备，例如无线电系统中的客户终端，例如移动系统、PDA(个人数字助理)设备，或并入安全元件 106 到其操作的另一电子设备。设备还可以结合多种角色，即，它可以例如是客户终端和 PDA 设备的组合，Nokia®Communicator®是这种设备的一个示例。

在我们的示例中，移动终端 100 是无线电系统中的客户终端，移动终端 100 包括天线 110 和无线电收发信机 108。移动终端 100 能够与无线电系统的网络部分 114 建立双向的无线电连接 112。无线电收发信机 108 是例如现有技术的移动台收发信机，它在例如 GSM(全

球移动通信)系统，GPRS(通用分组无线业务)系统或 UMTS(通用移动电信系统)中操作。

通常的移动终端 100 包括以下部件作为它的用户接口 104，移动终端 100 的用户 120 用它来与移动终端交互：键盘、显示器、麦克风和扬声器。移动终端 100 的电源一般是可充电电池。

移动终端 100 包括控制单元 102，它控制和监视终端及其各个部分的运行。目前，控制单元 102 一般实现为带软件的处理器，但是不同的硬件实现方式也是可能的，例如由分立的逻辑部件组成的电路或一个或多个专用集成电路(ASIC)。这些不同实现方式的组合也是可能的。当选择实现方式时，本领域的技术人员考虑，例如，设备的尺寸和功耗、必需的处理性能、制造成本和生产量的要求集。

接下来，参考图 2，示出控制单元 102 和安全元件 106 的结构。控制单元 102 包括安装的应用 200、202 和平台库 204。安全元件 106 包括安全元件应用 208、212 和访问控制文件 206、210、214。

移动终端 100 的用户 120 可以在她/他得到移动终端 100 之后在移动终端中安装一个或多个安装的应用 200、202。用户 120 可以例如经由因特网 116 和无线电系统的网络部分 114 从服务器 118 下载安装的应用，如图 1 所示。例如服务器 118 可以是 WWW 服务器(万维网)。安装的应用 200、202 以编程语言来编写。这种语言的一个示例是 Java™ 编程语言。JCP 开发了专门用于移动终端的 MIDP(移动信息设备简档)体系结构。编程环境被称作 J2ME™(Java™ 2 平台微型版)。在 MIDP 体系结构中，最底层是移动终端 100 的硬件。在硬件之上是包括操作系统和 Java™ 虚拟机的本机系统软件。操作系统可以是例如 Symbian™ 操作系统。制造商或运营商在移动终端 100 销售给端客户之前在移动终端 100 中安装平台库 204 或其中的部分。因此，在 MIDP 体系结构中，平台库 204 提供到由本机系统软件提供的的服务的接口，也称为 API(应用编程接口)。在 MIDP 体系结构中，安装的应用 200、202 可以用 Java™ 编程语言来编写，并且它们

可以被称作 midlet(比较: Java™ 中的 applet)。

安全元件 106 用于数据的安全存储和处理。安全元件 106 中的数据可以通过向安全元件 106 发布命令来访问和/或处理。一些命令可以是这样: 执行它们不需要访问码。通常，由于存储在安全元件 106 中的数据的机密性，命令必须带有由用户 120 提供的访问码。访问码通常是密码或口令。访问码有时称作 PIN(个人识别号)码。

给安全元件 106 的需要访问码的命令例如是数字签名的创建、对网络的访问认证、电子现金值或票的存储、金融交易处理。安装的应用 200 配置成向平台库 204 发布命令。平台库 204 配置成从安全元件 106 的访问控制文件 206 中读取信息。访问控制文件的信息包括访问码使用指令。安全元件 106 中的每个应用 208、212 具有它自己的访问控制文件 206、210，或安全元件 106 中的应用也可以使用安全元件 106 的公共访问控制文件 214。如果安全元件 106 的 A1 应用 208 的访问控制文件 206 定义需要访问码来执行发布到平台库的命令，那么平台库 204 配置成根据访问控制文件 206 的信息经由用户接口 104 从用户获得用于用户安全元件 106 的访问码。接受访问码后，平台库 204 配置成向安全元件 106 输入获得的访问码和命令。获得的访问码和命令的输入可以组合在一个消息或方法调用或另一适合的机制以在平台库 204 和安全元件 106 之间传送信息，或输入可以通过首先给出两者之一然后给出另一来分别执行。

如果安全元件 106 核准访问码，那么安全元件 106 配置成根据命令执行动作。在我们的示例中，可以这样实现: A1 应用 208 接收访问码，检查访问码与应用 208 已知的或安全元件 106 已知的访问码的匹配，并且如果确认匹配，那么根据命令执行动作。

在一个实施例中，用户接口 104 配置成用存储在访问控制文件 206 中的提示信息提示用户需要访问码。该实施例使平台库 204 能够以一般方式处理访问码获得而不必知道细节。另一优点是访问码询问的一般表现总是看起来相同的，所以用户 120 容易识别现在是要

求机密信息。

在一个实施例中，用户接口 104 配置成显示存储在访问控制文件 206 中的关于访问码使用的使用信息。该实施例告诉用户 120 为什么需要访问码。如果显示的信息与用户对使用的记忆映像不一致，那么她/他可以识别可能是恶意的安装的应用，她/他可以从移动终端 100 的内存中破坏它。

在一个实施例中，用户接口 104 配置成显示存储在访问控制文件 206 中的帮助信息。如果用户 120 不确定，帮助信息可以使机密信息的使用有把握，并且还有助于理解在某阶段命令是可能的。

在实施例中，平台库 204 配置成从由存储在访问控制文件 206 中的网络地址所标识的服务器 118 下载补充访问控制文件 206 的信息的信息。通常，该服务器 118 与下载安装的应用 200 的那里是相同的，但是当然它也可以是另一服务器。平台库 204 可以配置成用存储在访问控制文件 206 中的安全证书来证实补充信息。这是出于安全的原因而进行，这样，补充信息不会包含任何有害的或恶意的部分，例如病毒。平台库 204 还可以配置成在安全元件 106 中和/或在移动终端 100 中存储补充信息，这样，如果将来需要相同的补充信息，就不需要再下载了。

在一个实施例中，补充信息与存储在访问控制文件 206 中的信息是不同的语言。该实施例使调整安全元件需要的内存容量成为可能，因为可能只有一些语言版本存储在访问控制文件 206 中，而另一些语言版本只在需要是才下载。

在一个实施例中，访问控制文件的信息，即提示文本信息、使用文本信息和帮助文本信息，包括码，并且实际的信息项，例如对应于码的文本存储在平台库 204 中和/或在由存储在访问控制文件 206 中的网络地址所标识的服务器 118 中。该实施例节约了安全元件 106 的内存，因为不同的应用可以使用相同的信息项，它只在平台库 204 中存储一次。

参考图 3，说明了一种用于命令移动终端的安全元件的方法。该方法通过由移动终端安装的应用 200 向移动终端的平台库 204 发布 302 命令来开始。根据上面提到的 JSR-177，平台库可以支持两种类型的连接：APDU(应用协议数据单元)连接和 Java™ Card RMI(远程方法调用)连接。如果使用 APDU，那么安装的应用 200 可以使用如下的命令，例如：

```
PerformSecurityElementCommand(command, command data) {
Library internal operation for application access rights verification;
Library internal operation for user prompting;
Library internal operation for command parsing;
Library internal operation for making command call to security element;
Library internal operation for reading security element response;
Library internal operation for giving response to installed application;
}.
```

RMI 可向安装的应用 200 提供一种方法，例如 deduct_account(int amount)，然后可以用例如所述的 APDU 命令将它发送到安全元件 106。

然而，这些只是命令结构的示例，而且其它类型的命令也可以使用，并且除了方法调用，消息接口也可以使用。

接下来，在可选择的操作中，平台库 204 通过验证安装的应用是否有权调用安全元件应用 208 来检查 304 安装的应用对安全元件的访问权。平台库 204 从访问控制文件 206 中读取用于安装的应用验证的证书。安装的应用 200 的数字签名用证书来验证 306。在我们的示例中，验证成功并且安装的应用因此被认证。

然后，平台库 204 从安全元件的访问控制文件 206 中读取 308 信息。在我们的示例中，访问控制文件的信息定义需要访问码来进行命令 302。所以，例如，PIN 和命令 0x02(交易认证)一起使用。访问控制文件的信息还可以表明如何在命令中给出访问码(例如，它是命令的参数 1、参数 2 或数据部分，还是它是命令 0x02 之前的单独

命令 0x01)。因此，访问控制文件的信息包括访问码使用指令。如所示，访问控制文件 206 可以由平台库 204 在 304 和 308 中读取两次。还有一个实施例是可能的，其中访问控制文件 206 在验证 306 和访问码获得 312 之前只读取一次。

在一个实施例中，补充访问控制文件的信息的信息从由存储在访问控制文件中的网络地址所标识的服务器 118 下载 310。补充信息可以用存储在访问控制文件中的安全证书来认证。补充信息可以存储在安全元件和/或在移动终端中。在一个实施例中，补充信息与访问控制文件的信息的语言不同。在一个实施例中，访问控制文件的信息包括码，并且对应于码的实际信息项存储在平台库中和/或在由存储在访问控制文件 206 中的网络地址所标识的服务器 118 中。

接下来，根据访问控制文件的信息，平台库 204 从用户 120 获得 312 用于安全元件的访问码。根据使用的技术，访问码可以根据现有技术的方法来实现：PIN 码，口令、接受指示(例如对于低安全级别项按 OK 键，例如存储在安全元件中的电话簿)、或生物计量认证(例如指纹读取、蛋白质扫描、手指的热和/或压力特性或手掌压力等)。

在一个实施例中，访问码是通过用存储在访问控制文件中的提示信息提示用户需要访问码获得的。提示信息可以定义提示文本“用于网络认证”向用户显示。获得 312 还可以包括显示存储在访问控制文件中的关于访问码使用和/或帮助信息的使用信息。

平台库 204 向安全元件输入 314 获得的访问码和命令；在我们的示例中是向安全元件中的应用 208。平台库 204 可以包括进入向安全元件应用 208 发布的命令的数据部分的访问码，但是也可以使用两个单独的命令。

然后，在安全元件中，在我们的示例中是在应用 208 中，如果访问码被安全元件核准，那么根据命令执行动作。

安全元件或应用 208 向平台库 204 返回应答 318。应答 318 可以

包括反馈(或状态)信息和/或用户信息。最后，平台库320向安装的应用200返回应答320。

应该注意的是，当安装的应用开始于302时，访问码可以已经输入到安全元件。在这种情况下，用户认证有效直到安装的应用200被关闭。访问码也可以是这样：对于每个命令都需要再输入。在这两种情况下，输入的访问码可以在预定的时间周期内保持有效。访问码可以是每个安全元件应用特定的，或若干安全元件应用可以共享一个公共访问码。访问码还可以是命令特定的。

访问控制文件206读取也可以在安装的应用开始于302时执行。在这种情况下，不需要对发布到安全元件106的各个命令来访问访问控制文件206，但是平台库204知道访问条件并且例如对适当的命令执行用户认证312。

可能的是，访问控制文件206或对其的引用在选择安全元件应用208之后被返回。在安全元件106中，应用208、212必须被选择，因为可以有许多应用208、212。在选择之后，选定的应用208处理给安全元件106的命令。

在一些情况下，平台库204不知道需要访问码，并且因此向安全元件106发布没有安全码的命令。然后，安全元件应用208可以返回含访问控制文件206或对其引用的出错消息，于是，平台库204在它检查访问控制文件206的内容之后，可以重新发布命令并且根据访问控制文件206的信息获得访问码。

尽管上文中根据附图、参考示例描述了本发明，显然，本发明并不限于此，而是可以在所附权利要求的范围之内以若干方式进行修改。

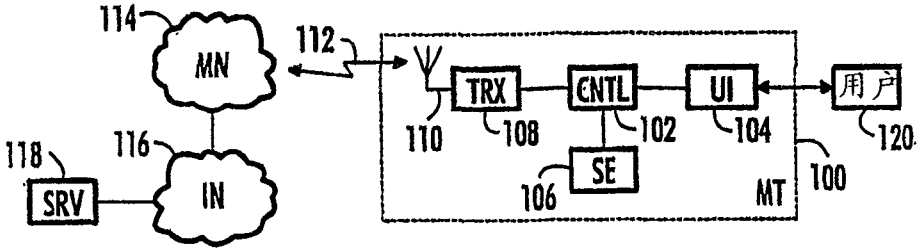

114
MN
112
TRX
CNTL
UI
用户
110
108
102
104
120
118
116
SRV
IN
SE
106
MT
100

图 1

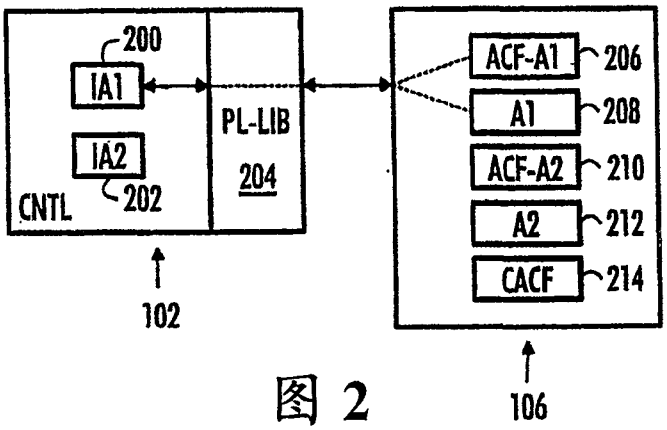
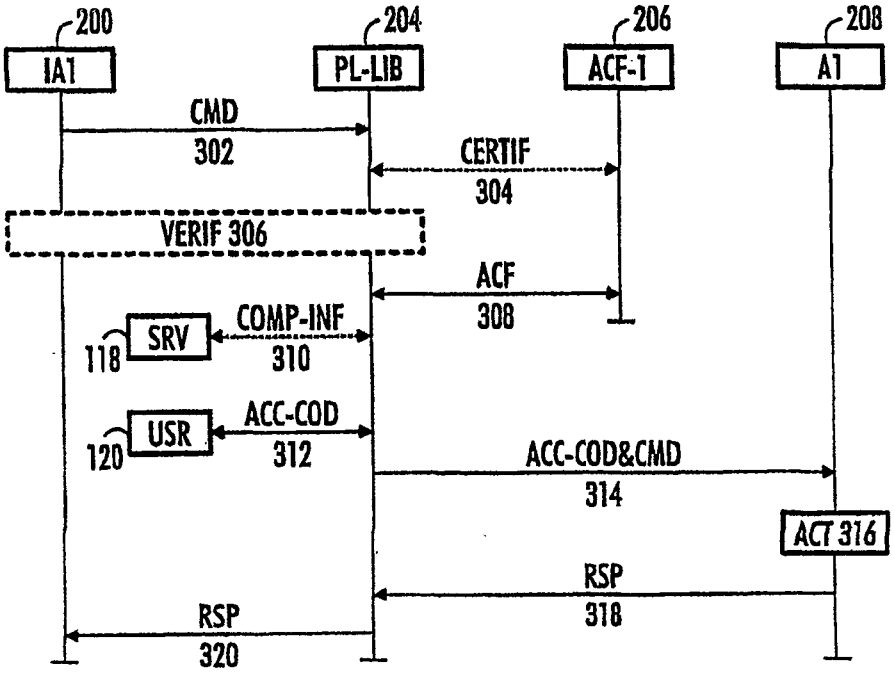

200
IA1
IA2
CNTL
202
PL-LIB
204
102
ACF-A1
206
A1
208
ACF-A2
210
A2
212
CACF
214
106

图 2

图 3


200
IA1
204
PL-LIB
206
ACF-1
208
A1
CMD
302
CERTIF
304
VERIF 306
ACF
308
118
SRV
COMP-INF
310
120
USR
ACC-COD
312
ACC-COD&CMD
314
ACT 316
RSP
318
RSP
320