[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 03826989.9

[45] 授权公告日 2008 年 1 月 23 日

[11] 授权公告号 CN 100363855C

[22] 申请日 2003.7.4 [21] 申请号 03826989.9
[86] 国际申请 PCT/IB2003/002661 2003.7.4
[87] 国际公布 WO2005/003938 英 2005.1.13
[85] 进入国家阶段日期 2006.2.28
[73] 专利权人 诺基亚有限公司
地址 芬兰埃斯波
[72] 发明人 L·帕特罗 P·科夫塔
[56] 参考文献
CN1393006A 2003.1.22
US6148083A 2000.11.14
CN1360448A 2002.7.24
US6178508B1 2001.1.23
审查员 蔡 萍

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 杨 凯 王 勇

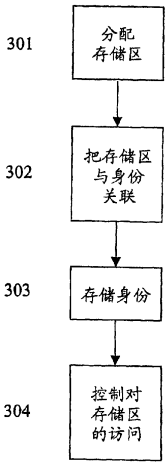
权利要求书 3 页 说明书 10 页 附图 3 页

[54] 发明名称

密钥存储管理方法、装置及其系统

[57] 摘要

本发明涉及用于允许多个应用在具有访问受到严格控制的安全环境(104、204、211)的装置(100、200)中管理其各自数据的方法及系统。本发明的概念是，在装置(100、200)的安全环境(104、204、211)内分配(301)存储区。存储区与应用的身份关联(302)，关联的身份存储(303)在安全环境(104、204、211)中，以及通过验证关联的身份与访问应用的身份之间的对应来控制(304)对存储区的访问。这是有利的，因为访问应用在分配的存储区中读取、写入和修改例如密码密钥、中间密码计算结果和口令的对象是可能的。



1. 一种用于允许多个应用在具有安全环境（104、204、211）的装置（100、200）中管理其各自数据的方法，所述安全环境由包括至少一个存储电路的组件构成，并且所述安全环境位于用于为所述多个应用提供安全存储的所述装置内，对所述安全环境（104、204、211）的访问受到严格控制，所述方法包括以下步骤：

对于所述多个应用中的每一个：

在所述安全环境（104、204、211）内分配（301）存储区；

把所述存储区与应用的身份关联（302）；

把所关联的身份存储（303）在所述安全环境内；以及

通过验证所关联的身份与访问应用的身份之间的对应来控制（304）对所述存储区的访问。

2. 如权利要求 1 所述的方法，其特征在于，应用的身份是通过私有密钥创建的数字签名，所述数字签名附加到所述应用，以及通过用与所述私有密钥对应的公共密钥验证所述数字签名来执行所述身份的验证。

3. 如权利要求 1 或 2 所述的方法，其特征在于，为第一方的应用执行分配（301）存储区、把所述存储区与应用的身份关联（302）、存储（303）所关联的身份以及控制（304）对所述存储区的访问的步骤，以及随后为与所述第一方无关的第二方的应用执行相同的步骤（301、302、303、304）。

4. 如权利要求 1 所述的方法，其特征在于，所述多个应用中的至少一个应用处于所述装置（100、200）的外部，并且向所述装置（100、200）发送命令，指示所述装置（100、200）执行在所述安全环境（104、204、211）内分配（301）存储区以及把所述存储区与所述至少一个应用的身份关联（302）的步骤，所述至少一个应用的身份附加到所述命令。

5. 如权利要求 1 所述的方法，其特征在于，所述装置（100、200）存储可信认证机构发布的数字证书。

6. 如权利要求 1 所述的方法，其特征在于，所述安全环境（104、204、211）包括智能卡（211）。

7. 一种用于允许多个应用在具有安全环境（104、204、211）的装置（100、200）中管理其各自数据的系统，所述安全环境由包括至少一个存储电路的组件构成，并且所述安全环境位于用于为所述多个应用提供安全存储的所述装置内，对所述安全环境（104、204、211）的访问受到严格控制，所述系统包括:

用于在所述安全环境（104、204、211）内为所述多个应用中的每一个分配（301）存储区的部件（103、203）;

用于把每个存储区与相应应用的身份关联（302）的部件（103、203）;

用于在所述安全环境（104、204、211）内存储（303）所关联的每个应用的身份的部件（103、203）; 以及

用于通过验证所关联的身份与访问应用的身份之间的对应来控制（304）对所述存储区的访问的部件（103、203）。

8. 如权利要求 7 所述的系统，其特征在于，应用的身份是通过私有密钥创建的数字签名，所述数字签名附加到所述应用，以及通过用与所述私有密钥对应的公共密钥对所述数字签名解密，来执行所述身份的验证。

9. 如权利要求 7 所述的系统，其特征在于，所述多个应用中的至少一个应用处于所述装置（100、200）的外部，并且设置成向所述装置（100、200）发送命令，指示所述装置（100、200）在所述安全环境（104、204、211）内分配（301）存储区以及把所述存储区与所述至少一个应用的身份关联（302），所述至少一个应用的身份附加到所述命令。

10. 如权利要求 7 所述的系统，其特征在于，所述装置（100、

200）设置成存储认证机构发布的数字证书。

11. 如权利要求 7 所述的系统，其特征在于，所述安全环境（104、204、211）包括智能卡（211）。

12. 一种用于提供数据安全性的电路（101、201），所述电路（101、201）包含至少一个处理器（103、203）以及至少一个存储电路（104、204、211），以及所述电路（101、201）包括:

所述存储电路（104、204、211）中的至少一个存储区，与电路安全性相关的受保护数据处于所述存储区中;

模式设定部件，设置成将所述处理器（103、203）设定为至少两种不同操作模式之一，所述模式设定部件能够改变所述处理器（103、203）的操作模式;

设置在所述至少一个存储电路（104、204、211）中的安全控制寄存器，设置成当在所述安全控制寄存器中设定第一处理器操作模式时使所述处理器（103、203）能够访问所述受保护数据所在的所述存储区；以及

设置在所述至少一个存储电路（104、204、211）中的安全控制寄存器，设置成当在所述安全控制寄存器中设定第二处理器操作模式时阻止所述处理器（103、203）访问受保护数据所在的所述存储区。

13. 一种电子数据处理装置（100、200），包括如权利要求 12 所述的用于提供数据安全性的电路（101、201）。

14. 如权利要求 13 所述的装置（100、200），其特征在于，所述装置是移动电信终端。

密钥存储管理方法、装置及其系统

技术领域

本发明涉及用于允许多个应用在具有访问受到严格控制的安全环境的装置中管理其各自数据的方法及系统。

背景技术

例如移动电信终端、便携计算机和 PDA 的各种电子装置要求对例如应用程序、密码密钥、密码密钥数据资料、中间密码计算结果、口令、外部下载的数据的鉴权部件等的安全相关组件的访问。经常需要这些组件以及它们的处理在电子装置内保密。理想情况是，它们应当被尽可能少的人知道。这是因为在知道这些组件的情况下如移动终端的装置可能被篡改。对这些类型的组件的访问可能帮助有恶意的攻击者操纵终端。

因此，引入安全执行环境，在这种环境中，电子装置中的处理器能够访问安全相关组件。对安全执行环境的访问、在其中进行处理以及从其中退出应当小心控制。包括这种安全环境的先有技术的硬件往往封闭在防篡改包装内。对这种类型的硬件进行探测或执行测量和测试应当是不可能的，这可能导致暴露安全相关组件及其处理。

JSR 118 专家组提出的 Java™ 2 Micro Edition 版本 2.0 的“移动信息装置简档”定义实现移动信息装置（MID）的开放式第三方应用开发环境所需的增强体系结构及关联的应用程序接口（API）。MID 的示例包括蜂窝电话、双向寻呼机和无线允许 PDA。如果装置确定 MID 应用可以是可信的，则按照装置的安全策略的指示允许进行访问。通过对应用的签署者进行鉴权，签署的应用可能成为可信的。

移动信息装置简档提供应用在所谓的记录存储器中永久地存储数据并在以后对其进行检索的机制。记录存储器包括在应用的多次调用时将保持持久的记录的集合。移动信息装置平台负责尽最大努力在包括重新启动、更换电池等的平台的常规使用中维护应用的记录存储器的完整性。记录存储器在平台相关位置创建，它们不受应用影响。

在先有技术中，当在不同的多方访问的装置中执行安全相关操作时，其中多方通过不同的应用程序访问装置，相互独立的不同的非协调多方各希望在装置中管理其自己的例如密码密钥、密码密钥数据资料、中间密码计算结果和口令的密码数据，这产生许多不同的问题。例如，安全执行环境通常有其指定的拥有者。安全执行环境例如可通过通常设置在移动电话中的智能卡的形式来提供。智能卡的指定拥有者是卡发行者，以及正是卡发行者决定哪些应用程序被卡接受并处理，例如什么软件最初加载到卡中以及卡遵守什么类型的命令。这导致以下问题：卡发行者被赋予作为唯一的卡管理者的支配角色，并且可禁止其它各方将智能卡再用于其自己的目的。一般来说，通过不是所述智能卡的管理者的一方的应用来创建智能卡上的对象要求管理者的许可。这是有问题的，因为通常需要在线连接到管理方、即卡发行者的服务器。此外，即使在卡上建立了对象，对象的访问控制基本上是不存在的；要么对象对于可访问该卡的所有应用是全局可用的，要么它仅对于卡管理者的应用是可用的。

发明内容

本发明的一个目的是，通过提出一种在其中不同各方在相互无关的安全环境中存储和访问其自己的各自数据并且无需安全环境管理者的监控是可能的系统及方法，来提供对上面给出问题的解决方案。

这个目的通过本发明来实现。

根据本发明的第一方面，提供一种方法，其中，在安全环境内分配存储区。存储区与应用的身份关联。此外，关联的身份存储在安全环境内，以及通过验证关联的身份与访问应用的身份之间的对应来控制对存储区的访问。

根据本发明的第二方面，提供一种系统，其中，部件设置成在安全环境内分配存储区以及把存储区与应用的身份关联。此外，部件设置成在安全环境内存储关联的身份，以及通过验证关联的身份与访问应用的身份之间的对应来控制对存储区的访问。

根据本发明的第三方面，提供一种至少一个存储区所在的电路。存储区包含与电路安全性相关的受保护数据。模式设定部件设置成把处理器设定为至少两种不同的操作模式之一。模式设定部件能够改变处理器操作模式。存储电路访问控制部件设置成当设定第一处理器操作模式时使处理器能够访问受保护数据所在的存储区。此外，存储电路访问控制部件设置成当设定第二处理器操作模式时阻止所述处理器访问受保护数据所在的所述存储区。

本发明的概念是，在装置的安全环境内分配存储区。例如，装置可包括移动电信终端、便携计算机、PDA 等。在装置中，存储区与应用的身份关联。应用或应用程序被认为是设计成在装置中执行特定功能的程序，并且还可与其它应用交互以在装置中执行特定功能。应用可由不同的多方提供，例如运营商、设备制造商、第三方应用开发商、服务提供商等。应用可以是自制造时驻留在装置中的程序和/或在操作期间下载到装置的程序。关联的身份存储在安全环境中，以及通过验证关联身份与访问应用程序的身份之间的对应来控制对存储区的访问。

本发明是有利的，因为在安全环境中存储的关联的身份对应于访问应用的身份的情况下访问应用读取、写入和修改例如密码密钥、密码密钥数据资料、中间密码计算结果和口令的对象是可能的。在对存储区的后续访问时，将要求应用标识其自己。存储区中的数据

是由具有对应于与存储区关联的身份的身份的任何应用可访问及可修改的。因此，具有与关联的身份对应的身份的任何应用能够管理存储区，例如读取、写入和修改存储区，限制对它的访问，把存储区与新的身份关联，等等。因此，分配的存储区的管理者是整个安全环境存储区的子集的管理者，具有在必要时对存储区解除分配的能力。

此外，本发明是有利的，因为不仅不同的应用访问装置的安全环境是可能的，而且不同的各方因而可访问分配的存储区，而无需与安全执行环境的管理者交互。如果安全执行环境变为以可移动方式设置在如移动电话的装置中的智能卡形式，则管理者通常是卡的发行者。在环境例如由永久设置在装置中的集成电路组成的情况下，管理者通常是装置的制造商。卡发行者（和/或装置制造商）、即“主”管理者仍然能够通过处在卡上/装置中的特定软件来控制该卡，因为驻留在安全环境中的某些应用程序优先于其它应用程序。在移动电信终端中，应当存在引导软件，该软件包括终端的主要功能性。没有这个软件就不可能把终端引导到正常操作模式。通过控制这个引导软件，因而还可能优先于其它应用。因此，主管理者例如可阻止应用请求过多的存储或者根据需要完全禁用存储区分配。

根据本发明的一个实施例，应用的身份是例如通过取应用代码的散列值并用私有密钥对散列值加密而创建的数字签名。负责应用的一方则可提供数字签名，并且把相应的公共密钥与签署的应用一起分发。然后，通过用与所述私有密钥对应的公共密钥对应用的散列值解密来执行身份的验证。这是一种平稳且直接的提供身份的方法。仅仅可能的是，有权访问私有密钥的一方正确地标识其自己。对散列值加密优于用不对称密钥加密整个应用代码的一个优点在于，需要较少的计算。

根据本发明的另一个实施例，为第一方应用分配第一存储区，该存储区与第一方应用身份关联，关联的第一身份存储在安全环境

中，以及通过验证第一方应用身份与访问应用的身份之间的对应来执行对存储区的访问控制。随后，为第二方应用分配第二存储区，该存储区与第二方应用身份关联，关联的第二身份存储在安全环境中，以及通过验证第二方应用身份与访问应用的身份之间的对应来执行对存储区的访问控制。第一方和第二方彼此无关，因而不同的各方可在安全环境中分配存储区，而无需联络安全环境管理者。第二方应用可占用第一方应用的分配的存储区是可能的，只要装置授权第二方应用进行这种操作。例如，要被占用的存储区可能曾经由提供装置的用户不再需要的服务的服务提供商分配。

根据本发明的又一个实施例，应用位于装置外部，并且向装置发送命令，指示装置执行在安全环境内分配存储区以及把存储区与应用的身份关联的步骤，其中的应用身份附加到命令。它的优点是，一方可向装置发送命令，以及装置将分配存储区并将它与应用的身份关联，因而，应用不需要加载到装置中以进行分配，分配而是可在应用远离装置的情况下执行。

根据本发明的另一个实施例，装置存储认证机构（CA）发布的数字证书。证书在公共密钥基础结构中用于向基础结构中包含的参与者确保证书的持有者经过可信认证机构授权。CA 验证数字证书的请求者提供的信息，以及在成功验证的情况下，CA 可向请求者发布证书。证书由 CA 签署，并且例如包含证书持有者的公共密钥、持有者名称以及关于证书拥有者的其它信息。

本发明通过一种用于允许多个应用在具有安全环境的装置中管理其各自数据的方法，所述安全环境由包括至少一个存储电路的组件构成，并且所述安全环境位于用于为所述多个应用提供安全存储的所述装置内，对所述安全环境的访问受到严格控制，所述方法包括以下步骤：对于所述多个应用中的每一个：在所述安全环境内分配存储区；把所述存储区与应用的身份关联；把所关联的身份存储在所述安全环境内；以及通过验证所关联的身份与访问应用的身份

之间的对应来控制对所述存储区的访问。

本发明还提供一种用于允许多个应用在具有安全环境的装置中管理其各自数据的系统，所述安全环境由包括至少一个存储电路的组件构成，并且所述安全环境位于用于为所述多个应用提供安全存储的所述装置内，对所述安全环境的访问受到严格控制，所述系统包括：用于在所述安全环境内为所述多个应用中的每一个分配存储区的部件；用于把每个存储区与相应应用的身份关联的部件；用于在所述安全环境内存储所关联的每个应用的身份的部件；以及用于通过验证所关联的身份与访问应用的身份之间的对应来控制对所述存储区的访问的部件。

本发明还提供一种用于提供数据安全性的电路，所述电路包含至少一个处理器以及至少一个存储电路，以及所述电路包括：所述存储电路中的至少一个存储区，与电路安全性相关的受保护数据处于所述存储区中；模式设定部件，设置成将所述处理器设定为至少两种不同操作模式之一，所述模式设定部件能够改变所述处理器的操作模式；设置在所述至少一个存储电路中的安全控制寄存器，设置成当在所述安全控制寄存器中设定第一处理器操作模式时使所述处理器能够访问所述受保护数据所在的所述存储区；以及设置在所述至少一个存储电路中的安全控制寄存器，设置成当在所述安全控制寄存器中设定第二处理器操作模式时阻止所述处理器（103、203）访问受保护数据所在的所述存储区。

本发明还提供一种电子数据处理装置，包括如上所述的用于提供数据安全性的电路。

当仔细阅读了所附权利要求和以下描述，本发明的其它特征和优点会变得清楚。本领域的技术人员知道，本发明的不同特征可被组合以创建除了以下所述之外的实施例。还可能的是，进行所述实施例的组合以创建新的实施例。许多不同的变更、修改和组合对于本领域的技术人员将变得清楚。

附图概述

将参照附图更详细地描述本发明，附图包括:

图 1 示出用于提供数据安全性的装置体系结构的框图，在这种体系结构中可有利地应用本发明;

图 2 示出另外配置了可移动智能卡的用于提供数据安全性的装置体系结构的框图，在这种体系结构中可有利地应用本发明; 以及

图 3 示出根据本发明用于在安全环境中分配存储区的流程图。

本发明的优选实施例说明

用于提供数据安全性的一种装置体系结构如图 1 所示。在本申请人的国际专利申请 PCT/IB02/03216 中还公开了这样一种系统，通过引用将该申请结合于本文中。该装置以 ASIC（专用集成电路）101 的形式来实现。体系结构的处理部分包含 CPU 103 和数字信号处理器（DSP）102。ASIC 101 包含在如移动电信终端、便携计算机、PDA 等的电子设备 100 中，并且被认为是设备 100 的“大脑”。

安全环境 104 包括 ROM 105，从其中引导 ASIC 101。这个 ROM 105 包含引导应用软件和操作系统。驻留在安全环境 104 中的某些应用程序优先于其它应用程序。在可设置 ASIC 101 的移动电信终端中，应当存在引导软件，该软件包括终端的主要功能性。没有这个软件就不可能把终端引导到正常操作模式。它的优点是，通过控制这个引导软件，还可能控制各终端的初始激活。

安全环境 104 还包括 RAM 106，用于存储数据和应用、即受保护数据。RAM 106 优选地存储用于在安全环境 104 内部执行安全关键操作的较小尺寸的应用的所谓受保护应用以及诸如密码密钥、中间密码计算结果和口令之类的对象。通常，使用受保护应用的方式将允许“常规”应用向某个受保护应用请求服务。新的受保护应用可在任何时间下载到安全环境 104 中，如果它们驻留在 ROM 中则不

是这样。安全环境 104 的软件控制受保护应用的下载和执行。只有签署的受保护应用才被允许运行。受保护应用可访问安全环境 104 中的任何资源，并且它们还可与常规应用进行通信以提供安全服务。

在安全环境 104 中包括熔断存储器 107，它包含在制造期间产生并编程到 ASIC 101 中的唯一随机号。这个随机号用作特定 ASIC 101 的身份，以及还用于导出密码操作的密钥。此外，以安全控制寄存器形式的存储电路访问控制部件设置在安全环境 104 中。安全控制寄存器的目的是根据寄存器中设定的模式来赋予 CPU 103 对安全环境 104 的访问权或者阻止 CPU 103 访问安全环境 104。CPU 103 的操作模式可通过应用软件在寄存器中设定，从而产生体系结构无需依靠外部信号的事实。从安全性来看，这是优选的，因为通过控制应用软件，处理器模式的设定也可受到控制。还可能让外部信号（未示出）连接到 ASIC 101，通过该信号设定安全控制寄存器是可能的。通过利用外部信号，模式改变可轻松快速地执行，这在测试环境中可以是有利的。这两种模式设定部件、即应用软件以及外部信号的组合是可行的。

该体系结构还包括标准桥接电路 109，用于限制总线 108 上的数据可见性。该体系结构应当封闭在防篡改包装中。对这种类型的硬件进行探测或执行测量和测试应当是不可能的，这可能导致暴露安全相关组件及其处理。DSP 102 有权访问其它外设 110，例如直接存储器存取（DMA）单元、RAM、闪速存储器，并且在 ASIC 101 的外部可提供附加处理器。

用于提供数据安全性的装置体系结构的另一个实施例如图 2 所示，其中，相应的参考标号表示结合图 1 所述的相应元件。图 2 所示的体系结构与图 1 所示的体系结构相比的差别在于，电子设备 200 设置了可移动智能卡 211、例如用户身份模块（SIM）卡，它也被认为是安全环境。

为了安全的目的，移动终端 200 以及智能卡 211 存储可信 CA 发

布的数字证书。证书用于向与移动终端 200 和/或智能卡 211 进行通信的参与者确保证书的持有者经过可信 CA 授权。CA 签署证书，并且证书持有者必须拥有与 CA 的私有密钥相对应的公共密钥，以便验证 CA 签署的证书是否有效。注意，不同的装置可持有来自不同 CA 的证书。在那种情况中，不同的 CA 必须相互执行某种通信、例如交换它们自己的公共密钥。证书是本领域的技术人员众所周知的，以及众所周知的标准证书是 CCITT 建议 X.509 中包含的证书。

图 3 示出流程图，说明如何在图 2 所示的智能卡中分配存储区。注意，还可能在图 1 和图 2 中所述的 ASIC 101、201 的安全环境中分配存储区。无论是使用 ASIC 101、201 的安全环境还是智能卡 211 提供的安全环境，分配存储区的过程均相同。在步骤 301，移动终端 200 接收在智能卡 211 中分配存储区的请求。请求可通过加载到终端的应用进行，但还可通过处于移动终端外部的应用进行。随后，在步骤 302，应用的证书由 ASIC 201 的 CPU 203 进行检查，以确保应用是可信的。应用的身份（下面会进行描述）与分配的存储区关联并存储在智能卡 211 中。关联可以是极为直接的，例如，身份被关联到智能卡中的两个确定地址之间分配的存储区。此外，在步骤 303，关联的身份存储在智能卡 211 中。

在步骤 304，应用进行访问智能卡 211 中分配的存储区的请求；ASIC 201 的 CPU 203 检查请求应用的身份。请求应用的身份优选地是通过取应用代码的散列值并用私有密钥对散列值加密来创建的数字签名。例如运营商、第三方应用开发商或服务提供商的负责应用的一方则可提供数字签名，并且把相应的公共密钥与签署的应用一起分发。然后，通过在 ASIC 201 的安全环境中用与应用私有密钥对应的公共密钥对应用的散列值解密，由 CPU 203 执行身份的验证。通过验证卡 211 中存储的关联的身份与访问应用的身份之间的对应，由 CPU 203 来控制对智能卡 211 中分配的存储区的访问。

存在用于标识应用的多种方法，并且是本领域的技术人员已知

的。对应用代码使用散列函数并签署散列代码和/或使用证书是可能的，如上所述。仅依靠证书也是可能的，但是，附加的密码操作是可行的，以获取更高的安全等级。其它可能的方法包括签署应用本身、使用平台产生的标识号等。

当在智能卡 211 或者在 ASIC 201 的安全环境中分配了存储区时，授权的访问应用可在分配的存储区中读取、写入和修改对象，例如密码密钥、密码密钥数据资料、中间密码计算结果和口令。授权的访问应用因而可被看作是分配的存储区的管理者，具有在必要时对存储区解除分配的能力。

参照图 3，通过执行图中的步骤，第一存储区可由第一应用进行分配。随后，可为第二应用分配第二存储区，这些应用具有不同的身份。因此，不同的各方可在安全环境 204、211 中分配其各自的存储区，而无需联络安全环境管理者。

虽然参照本发明的特定示范实施例对本发明进行了描述，但本领域的技术人员将清楚许多不同的变更、修改等。因此，所述实施例不是意在限制如所附权利要求限定的本发明的范围。

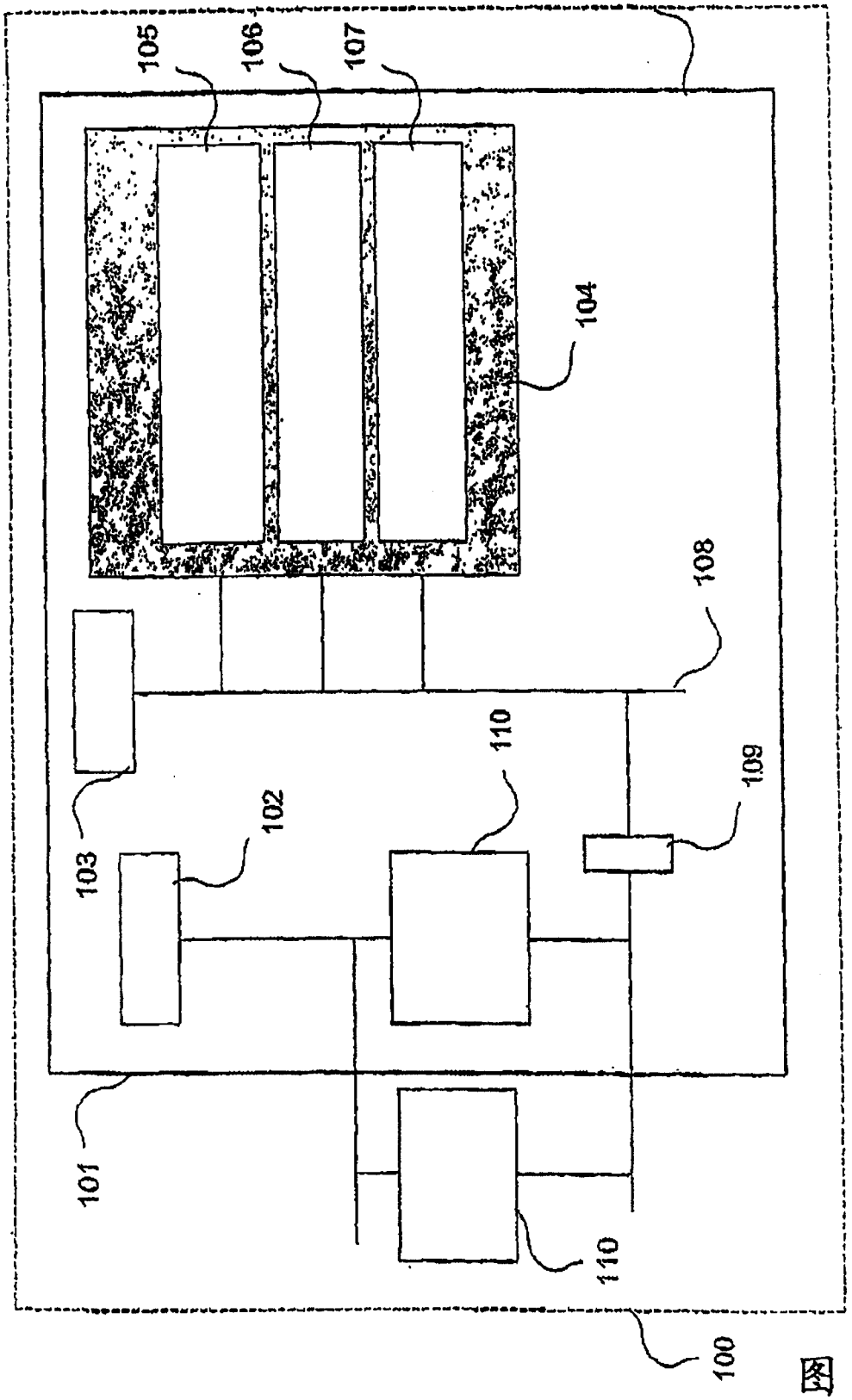


图 1

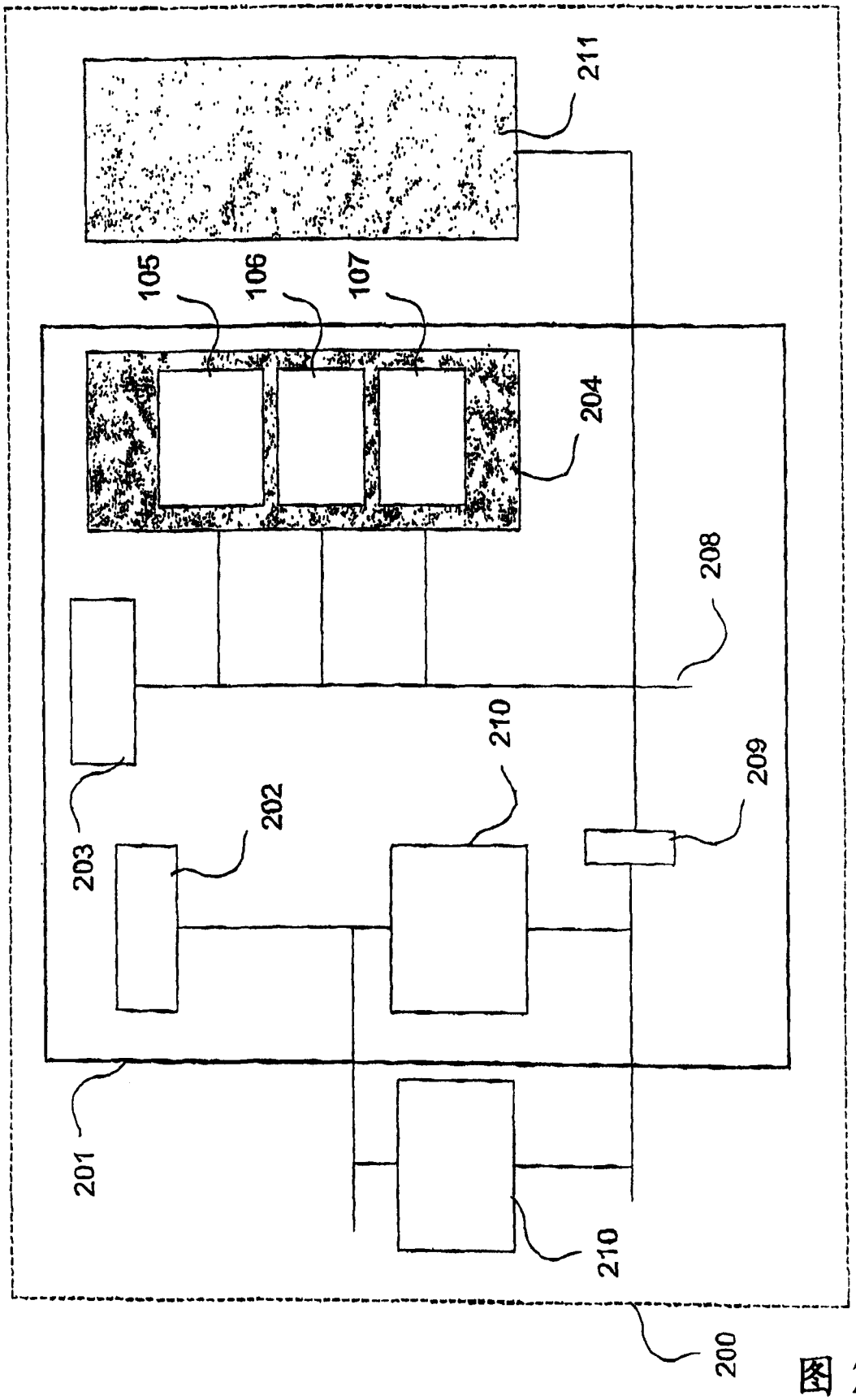


图 2

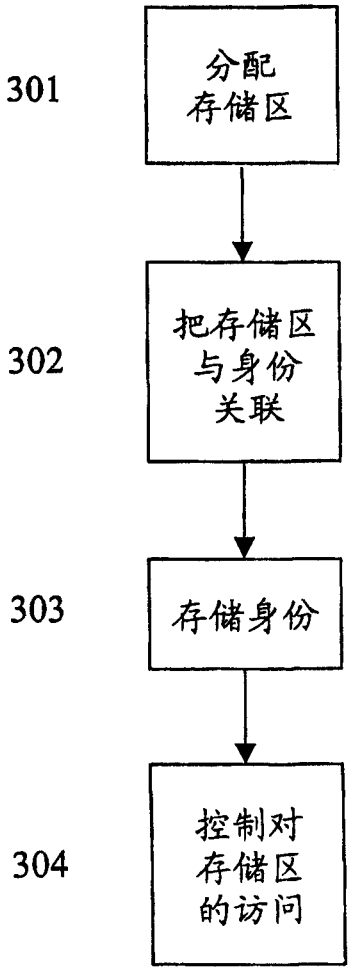


图 3