[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)
G06K 19/073 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200380106200.5

[43] 公开日 2006 年 1 月 25 日

[11] 公开号 CN 1726478A

[22] 申请日 2003.12.12
[21] 申请号 200380106200.5
[30] 优先权
[32] 2002.12.16 [33] JP [31] 363597/2002
[86] 国际申请 PCT/JP2003/016000 2003.12.12
[87] 国际公布 WO2004/055680 日 2004.7.1
[85] 进入国家阶段日期 2005.6.15
[71] 申请人 松下电器产业株式会社
地址 日本大阪府
[72] 发明人 高木佳彦 中西良明 佐佐木理 菊地隆文

[74] 专利代理机构 北京市柳沈律师事务所
代理人 黄小临 王志森

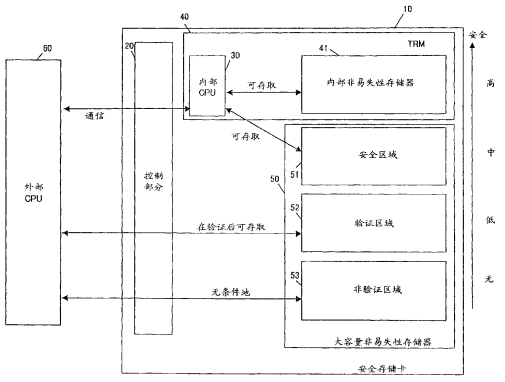
权利要求书 3 页 说明书 15 页 附图 12 页

[54] 发明名称

存储器件和使用存储器件的电子器件

[57] 摘要

一种具有大存储容量和具有等同于 IC 卡的安全级别的存储区域的存储卡。 可以附接到电子器件和与其分离的半导体存储卡(10)具有：非抗窜改(tamper)第一存储器(50)，其包括电子器件可存取的普通区域(52，53)和不可被电子器件直接存取的安全区域(51)；抗窜改的第二存储器(41)，它不被电子器件直接存取。 配置半导体存储卡(10)，使得可以仅仅经由管理对于第二存储器(41)的存取的安全控制部分(30)来存取第一存储器(50)的安全区域(51)。 安全区域(51)不能被外部器件直接存取，因此显出比验证区域(52)更高的安全级别。而且，因为非抗窜改存储器(50)中提供安全区域(51)，因此它可以具有大的存储容量。



1. 一种固定地或可拆卸地连接到电子器件的存储器件，包括:

非抗窜改的第一存储器，其具有可以从所述电子器件存取的普通区域和不能从所述电子器件直接存取的安全区域;

抗窜改的第二存储器，其不能从所述电子器件被直接存取; 和

安全控制部分，用于管理对于第二存储器的存取，

其中，可以仅仅通过安全控制部分来进行从电子器件对第一存储器的安全区域的存取。

2. 按照权利要求 1 的存储器件，其中，在接收到由安全控制部分验证的电子器件的命令时，所述安全控制部分存取安全区域或第二存储器，并且写入或读取数据。

3. 按照权利要求 1 或 2 的存储器件，

其中，加密密钥被存储在第二存储器中，并且

其中，所述安全控制部分使用加密密钥来加密要写入到安全区域中的数据，并且写入被加密的数据，使用加密密钥来解密从安全区域读取的数据。

4. 按照权利要求 1 到 3 的任何一个存储器件，其中，所述安全控制部分计算要写入到安全区域中的数据的散列值，将所述散列值存储在第二存储器中，计算从安全区域读取的数据的散列值，并且将这个散列值与存储在第二存储器中的散列值相比较。

5. 按照权利要求 1 的存储器件，其中，第一存储器的普通区域包括可以仅仅由被总控制部分验证的电子器件存取的验证区域和可以甚至由未被验证的电子器件存取的非验证区域，所述总控制部分用于控制所述存储器件。

6. 按照权利要求 1 到 5 的任何一个的存储器件，其中，用于指示在普通区域和安全区域之间的边界的边界地址信息和用于描述在普通区域和安全区域中的逻辑地址和物理地址之间的关系的逻辑物理地址转换表被管理为第一存储器的地址信息。

7. 按照权利要求 6 的存储器件，其中，第一存储器的地址信息包括用于指示在验证区域和非验证区域之间的边界的边界地址信息和在验证区域和非验证区域中的逻辑物理地址转换表。

8. 按照权利要求 6 或 7 的存储器件，其中，在第一存储器的地址信息管

理区域中记录所述边界地址信息和逻辑物理地址转换表。

9. 按照权利要求 6 的存储器件，其中，按照由安全控制部分验证的电子器件的命令来改变由边界地址信息表示的、在普通区域和安全区域之间的边界。

10. 按照权利要求 7 的存储器件，其中，按照由总控制部分验证的电子器件的命令来改变由边界地址信息表示的、在验证区域和非验证区域之间的边界。

11. 按照权利要求 10 的存储器件，

其中，在验证区域和非验证区域之间的边界的边界地址信息由实际边界地址和排除了安全区域而设置的假定边界地址构成，并且

其中，根据由总控制部分验证的电子器件的命令指定的假定边界地址来改变实际边界地址。

12. 一种用于存取存储器件的电子器件，该存储器件具有作为存储区域的第一区域、第二区域和第三区域，

其中，在接收到对存储器件的存取请求时，所述电子器件：

通过用于控制对存储器件的存取的、存储器件的总控制部分来存取存储器件的非抗窜改存储区域的第一区域；

在以总控制部分和用于控制对第二区域和第三区域的存取的存储器件的安全控制部分验证后，通过安全控制部分来存取除了第一区域之外的非抗窜改存储区域的第二区域；并且

在以安全控制部分验证后，通过所述总控制部分和安全控制部分来存取存储器件的抗窜改存储区域的第三区域。

13. 按照权利要求 12 的电子器件，包括：

第一命令产生部件，用于产生对于第一区域写入或读取数据的命令；

第二命令产生部件，用于产生请求安全控制部分执行处理的命令；

第一验证处理部件，用于获取使用安全控制部分来验证所用的验证密钥，并且使用安全控制部分来执行验证处理。

14. 按照权利要求 12 或 13 的电子器件，其中，不使用总控制部分验证而存取第一区域的部分区域的非验证区域，以及在使用总控制部分验证后，存取除了非验证区域之外的第一区域的部分或全部的验证区域。

15. 按照权利要求 14 的电子器件，包括：

第三命令产生部件，用于产生对验证区域写入或读取数据的命令；

第二验证处理部件，用于获取使用总控制部分来验证所用的验证密钥，并且使用总控制部分来执行验证处理。

存储器件和使用存储器件的电子器件

技术领域

本发明涉及一种诸如半导体存储卡的存储器件和用于对存储器件写/读数据的电子器件，具体涉及保证高度安全性和具有大存储容量的存储介质的实现。

背景技术

包括作为存储介质的非易失性半导体存储器的半导体存储卡（以下称为“存储卡”）与诸如 DVD 的盘式存储介质相比较具有小存储容量，但是不需要大的机械部分，并且，较小和容易手持，而且也具有良好的震动抵抗力，因此近来已经被扩展为适合于便携使用的存储介质的使用范围。

存储卡可以或可以不包含 CPU（微计算机）。在包含 CPU 的存储卡中的 CPU 的功能是执行由外部器件请求的非易失性存储器的读取和写入处理。

存储卡的非易失性存储器也包括用于提高安全级的安全区域。下述的专利文件 1 描述了一种具有非易失性存储器的存储卡，所述非易失性存储器包括：验证区域，它仅仅可以被获得验证成功的外部器件存取；以及可以被任何外部器件存取的非验证区域。使用所述存储卡，加密的音乐内容被存储在非验证区域中，用于解密所加密的音乐内容的解密密钥被存储在验证区域中，由此使得有可能保证音乐内容的版权。

在这样的存储卡中的 CPU 的功能将执行外部器件的验证处理，以使得外部器件除了读取和写入处理之外还可以存取验证区域。

无论如何，在存储卡中的 CPU 的功能限于存储器的读取和写入附属的处理，并且通过外部器件来控制在存储器中记录的数据。

另一方面，包含 CPU 的 IC 卡具有存储区域以及在抗窜改模块中的 CPU。所述抗窜改模块禁止外部器件直接存取存储区域。因此，所述 IC 卡包含抵御复制和伪造的高保密属性，并且用于需要高安全性的数字钱款服务等。

在 IC 卡中的 CPU 的功能涵盖广泛的范围，不仅有存储器读取和写入，而且有外部输入数据的加密、签字产生、签字验证、所输入的个人识别号码

检验等。在IC卡的存储器中记录的数据被在IC卡中的CPU控制。

因此，IC卡的CPU是多功能的，并且与本领域内的存储卡中包含的CPU相比较高度安全。

[专利文件1] JP-A-2001-14441

但是，相对于数字钱款服务的多样性，所述IC卡具有有限的可存储信息容量，服务提供者等要求扩大所述信息容量等。例如，如果为了防止成倍提取数字钱款等的麻烦而试图执行记录电子票据和交易日志的服务，则与现有IC卡的容量相比较必须提供大的信息容量，以便存储累积的电子票据等。

另一方面，在专利文件1中上述的存储卡可以包括在一定程度上大的信息容量，因为可以可变地设置验证区域。但是，所述验证区域是可以被外部器件直接控制的区域，因此，与IC卡相比较，安全级较低。

发明内容

因此，本发明意欲解决在现有技术中包含的问题，本发明的目的是提供一种存储器件，它包括具有大存储容量和与IC卡相同的安全级的存储区域，本发明的目的并且是提供一种使用所述存储器件的电子器件。

按照本发明，固定地或可拆卸地连接到电子器件的存储器件包括：非抗窜改的第一存储器，其具有可以从所述电子器件存取的普通区域和不能从所述电子器件直接存取的安全区域；抗窜改的第二存储器，其不能从所述电子器件被直接存取；和安全控制部分，用于管理对于第二存储器的存取，其中，可以仅仅通过安全控制部分来进行从电子器件对第一存储器的安全区域的存取。

安全区域不能直接被外部器件存取，因此比现有技术中的验证区域具有更高的安全级。而且，因为安全区域被置于非抗窜改的存储器中，因此可以以低成本保留大的存储容量。

而且，按照本发明，用于存取具有作为存储区域的第一区域、第二区域和第三区域的存储器件的电子器件通过用于在接收到对于存储器件的存取请求时控制对存储器件的存取的、存储器件的总控制部分来存取存储器件的非抗窜改存储区域的第一区域，在用安全控制部分验证后通过所述总控制部分和用于控制对于第二区域和第三区域的存取的存储器件的安全控制部分来存取除了第一区域之外的非抗窜改存储区域的第二区域，并且在用安全控制部

分验证后通过所述总控制部分和安全控制部分来存取存储器件的抗窜改存储区域的第三区域。

利用半导体存储卡的存储器件等，所述电子器件可以提供各种服务。

附图说明

图 1 是本发明的一个实施例中的安全存储卡的概念图；

图 2 是示出本发明的所述实施例中的安全存储卡的配置的方框图；

图 3 是本发明的所述实施例中的用于使用安全存储卡的系统的概念图；

图 4 是示出本发明的所述实施例中的读出/写入单元的配置的方框图；

图 5 是示出本发明的所述实施例中的安全存储卡的写入步骤的序列；

图 6 是示出本发明的所述实施例中的安全存储卡的写入步骤的继续的序列；

图 7 是示出本发明的所述实施例中的安全存储卡的另一个写入步骤的序列；

图 8 是示出本发明的所述实施例中的安全存储卡的大容量非易失性存储器的结构的图；

图 9 是示出本发明的所述实施例中的逻辑物理地址转换表的图；

图 10 是示出本发明的所述实施例中的逻辑物理地址转换表的另一个示例的图；

图 11 是示出本发明的所述实施例中的安全存储卡的大容量非易失性存储器的不同结构的图；

图 12 是示出本发明的所述实施例中的逻辑物理地址转换表的不同示例的图。

顺便提及，在附图中的附图标记表示下列：10——安全存储卡；11——IC 部分；12——I/F 部分；13——IC 命令处理部分；14——文件管理部分；15——IC 验证部分；16——存储器管理部分；17——加密和解密电路；18——内部非易失性存储器 I/F 部分；20——控制部分；21——数据 I/F 部分；22——命令 I/F 部分；23——控制验证部分；24——命令处理部分；25——存取控制部分；26——大容量非易失性存储器 I/F 部分；40——TRM；41——内部非易失性存储器；50——大容量非易失性存储器；51——安全区域；52——验证区域；53——非验证区域；60——外部 CPU；61——移动电话；62——ROM；

63——RAM；64——液晶显示部分；65——无线通信部分；66——操作按钮；67——卡 I/F 部分；68——验证电路；69——R/W 单元；70——内部总线；91——充值终端；92——充值服务器；93——支付服务器；94——提供服务器；95——网络；621——命令产生步骤；622——验证密钥组。

具体实施方式

在本发明的实施例中的半导体存储卡（此处称为“安全存储卡”）包括：抗窜改模块（TRM）40，它包括内部非易失性存储器 41；大容量非易失性存储器 50，它包括非验证区域 53、验证区域 52 和安全区域 51；内部 CPU30，用于存取内部非易失性存储器 41 和安全区域 51；控制部分 20，用于与电子器件（读取/写入（R/W）单元）的外部 CPU 60 通信以执行验证处理，并且使得被验证的外部 CPU 60 访问验证区域 52，如在图 1 的概念图中所示。

TRM 40 的非易失性存储器 41 被实现为 EEPROM，所述 EEPROM 可以以例如 16 字节单位进行擦除和写入。大容量非易失性存储器 50 实现为快闪存储器，它可以以 512 字节块单位等而被擦除，并且可以以例如 1 字节单位写入。

外部 CPU 60 可以无条件地访问非验证区域 53，并且当控制部分 20 验证了外部 CPU 60 时可以访问验证区域 52。但是，外部 CPU 60 不能知道安全区域 51 或内部非易失性存储器 41 的存在，并且不能直接地访问安全区域 51 或内部非易失性存储器 41。

仅仅内部 CPU 30 可以访问安全区域 51 和内部非易失性存储器 41。安全区域 51 与内部非易失性存储器 41 不同在：后者位于 TRM 40 中；而前者位于不抗窜改的大容量非易失性存储器 53 中。于是，安全区域 51 与内部非易失性存储器 41 相比较可以具有大的存储容量。相反，它具有比位于 TRM 40 内的内部非易失性存储器 41 更低的安全级别。以从低到高的、非验证区域 53、验证区域 52、安全区域 51 和内部非易失性存储器 41 的顺序来分配四个区域的安全级别。

后面详细说明安全存储卡 10 的配置，并且将讨论使用方式。

所述安全存储卡可以用于例如图 3 所示的音乐提供系统等中。在这个系统中，安全存储卡 10 位于 R/W 单元的移动电话中。所述系统包括：提供服务器 94，用于通过网络 95 来提供音乐；支付服务器 93，用于执行支付处理；

充值服务器 92，用于将数字钱款充值到存储卡 10 中；数字钱款充值终端 91。

如图 4 的方框图所示，移动电话 61 包括：CPU 60，它对应于图 1 中的外部 CPU; ROM 62，预先存储用于验证的验证密钥组 622 和命令产生步骤 621; RAM 63 用作 CPU 60 的工作区域；液晶显示部分 64，用于实现显示屏幕；无线通信部分 65，用于通过网络来进行无线通信；操作按钮 66，它由用户操作；卡 I/F 部分 67，用于将安全存储卡 10 连接到内部总线 70；验证电路 68，用于与安全存储卡 10 进行相互验证，所述部件通过内部总线 70 而连接。

用户首先将数字钱款充值到安全存储卡 10 中。为此，用户将安全存储卡 10 置于充值终端 91 中，并且按照所显示的指令来操作充值终端 91。此时，充值终端 91 请求安全存储卡 10 的内部 CPU 30 来开始钱币接收应用。在接收到来自充值终端 91 的数字钱款的钱币接收处理请求时，开始所述钱币接收应用的内部 CPU 30 确定要将根据所述请求命令将数据写入到内部非易失性存储器 41，并且充值终端 91 报告的钱币量写入内部非易失性存储器 41 中。因此在内部非易失性存储器 41 中存储钱款信息。

也可以以充值服务器 92 来在线充数字钱款，其中放置了安全存储卡 10 的移动电话 61 访问所述充值服务器 92。

接着，用户从移动电话 61 存取提供服务器 94，并且做出购买音乐内容的请求。提供服务器 94 请求用户支付所述音乐内容的价格。在接收到所述请求时，移动电话 61 的 CPU 60 请求安全存储卡 10 的内部 CPU 30 开始支付应用。开始所述支付应用的内部 CPU 30 验证移动电话 61，然后从内部非易失性存储器 41 中记录的数字钱款的剩余量减去从移动电话 61 报告的支付量。然后，提供服务器 94 向移动电话 61 发送电子票据，并且移动电话 61 的 CPU 60 向安全存储卡 10 的内部 CPU 30 发送所述电子票据的存储请求。内部 CPU 30 确定根据所述请求命令将数据写入到安全区域 51 中，并且在安全区域 51 中存储所述电子票据。

当存储在内部非易失性存储器 41 中的信用号被提供到支付服务器 93 时，使用支付服务器 93 来执行所述支付处理。

在完成所述支付后，提供服务器 94 向移动电话 61 发送加密的音乐内容及其解密密钥。移动电话 61 的 CPU 60 确定接收数据，在安全存储卡 10 的验证区域 52 中存储内容解密密钥，并且在安全存储卡 10 的非验证区域 53 中存储所加密的内容。

于是，在所述系统中，在安全存储卡 10 的 TRM 40 的内部非易失性存储器 41 中存储钱款信息，在安全区域 51 中存储电子票据，在验证区域 52 中存储解密密钥，在非验证区域 53 中存储所解密的内容。

图 2 是示出安全存储卡 10 的配置的方框图。安全存储卡 10 大致包括控制部分 20、大容量非易失性存储器 50 和对应于图 1 的 TRM 的 IC 部分 11。大容量非易失性存储器 50 具有非验证区域 53、验证区域 52、安全区域 51 和用于存储区域的地址信息的地址信息管理区域 54。

控制部分 20 包括：数据 I/F 部分 21，用于向和从 R/W 单元 69 传送数据；命令 I/F 部分 22，用于向和从 R/W 单元 69 传送命令；控制验证部分 23，用于验证 R/W 单元 69；控制命令处理部分 24，用于解译所接收的命令，并且响应于所述命令而执行处理；存取控制部分 25，用于控制对于大容量非易失性存储器 50 的存取，并且被用作向和从 IC 部分 11 的数据的传送窗口；大容量非易失性存储器 I/F 部分 26，用于向和从大容量非易失性存储器 50 传送数据。

抗窜改 IC 部分 11 包括：内部非易失性存储器 41；I/F 部分 12，用于向和从控制部分 20 传送数据和命令；IC 命令处理部分 13，用于解译所述命令和响应于所述命令而执行处理；文件管理部分 14，用于管理以文件格式存储在内部非易失性存储器 41 和安全区域 51 中的数据；IC 验证部分 15，用于验证 R/W 单元 69，并且使得被验证的 R/W 单元 69 可以对内部非易失性存储器 41 和安全区域 51 进行数据存取；加密和解密电路 17，用于使用在内部非易失性存储器 41 中存储的密钥来加密/解密对于内部非易失性存储器 41 和安全区域 51 的写/读的数据；内部非易失性存储器 I/F 部分 18，用于对于内部非易失性存储器 41 传送数据。在权利要求中所要求的安全控制部分对应于 IC 命令处理部分 13、IC 验证部分 15、加密和解密电路 17、文件管理部分 14、IC 部分 11 的存储器管理部分 16。

控制部分 20 的控制命令处理部分 24 解译从 R/W 单元 69 接收的命令，并且确定是否所述命令

- 做出存取大容量非易失性存储器 50 的验证区域 52 或非验证区域 53 的请求；
- 做出验证请求；
- 请求 IC 部分 11 来执行处理，并且当所述命令做出存取大容量非易

失性存储器 50 的验证区域 52 或非验证区域 53 的请求时，控制命令处理部分 24 指令存取控制部分 25 来控制对于大容量非易失性存储器 50 的存取；当所述命令请求 IC 部分 11 来执行处理时，控制命令处理部分 24 指令存取控制部分 25 来向 IC 部分 11 传送所述命令；并且当所述命令做出验证请求时，控制命令处理部分 24 指令控制验证部分 23 执行验证处理。

仅仅当控制验证部分 23 已经验证了所述终端时，才允许对于验证区域 52 的存取。

为了控制对于大容量非易失性存储器 50 的存取，存取控制部分 25 参考在大容量非易失性存储器 50 的地址信息管理区域 54 中记录的地址信息。当所述终端（R/W 单元 69）使用大容量非易失性存储器 50 的逻辑地址的规格来做出存取请求时，存取控制部分 25 从在地址信息管理区域 54 中的记录确定被指定的地址属于大容量非易失性存储器 50 的哪个区域，并且仅仅当所述终端已经被验证时才允许对于验证区域 52 的存取请求。

IC 部分 11 的 IC 命令处理部分 13 解译从控制部分 20 发送的命令，并且确定是否所述命令

- 做出对于内部非易失性存储器 41 写/读数据的请求；
- 做出对于安全区域 51 写/读数据的请求；
- 做出验证请求；
- 做出对于任何其他处理的请求。

当所述命令做出开始应用的请求时，IC 命令处理部分 13 内部开始所述应用。

所述应用是从 R/W 单元 69 接收的命令的解译模式，并且在开始所述应用后，由 IC 命令处理部分 13 从 R/W 单元 69 接收的命令被所述 IC 命令处理部分 13 按照在所述应用和 R/W 单元 69 之间确定的解译而解译。

当在开始应用后接收的命令做出验证请求时，IC 命令处理部分 13 指令 IC 验证部分 15 来执行 R/W 单元 69 的验证处理。

当所述命令是在所述内部开始的应用和 R/W 单元 69 之间确定的、用于做出对内部非易失性存储器 41 写/读数据或对安全区域 51 写/读数据的请求时，IC 命令处理部分 13 查看 R/W 单元 69 是否已经在 IC 验证部分 15 中被验证。

如果 R/W 单元 69 已经被验证，则允许所述请求，并且当所述请求是写

入请求时，使用存储目的地信息来向存储器管理部分 16 发送写数据。

用于管理内部非易失性存储器 41 和安全区域 51 的存储器管理部分 16 通过解密和解密电路 17 来加密写入数据（此时，加密和解密电路 17 使用在内部非易失性存储器 41 中存储的加密密钥来加密写数据），然后将要写入内部非易失性存储器 41 中的数据通过内部非易失性存储器 I/F 部分 18 而写入内部非易失性存储器 41，并且向文件管理部分 14 传送写位置信息。存储器管理部分 16 也将要写入到安全区域 51 中的数据通过大容量非易失性存储器 I/F 部分 26 而写入到大容量非易失性存储器 50 的安全区域 51 中。并且向文件管理部分 14 传送写位置信息。

文件管理部分 14 根据从存储器管理部分 16 传送的信息来管理在内部非易失性存储器 41 和安全区域 51 中存储的文件。

当所述请求是读取请求时，IC 命令处理部分 13 在文件管理部分 14 中找到要被读取的数据的文件位置，并且请求存储器管理部分 16 来读取所述文件。

当存储器管理部分 16 从内部非易失性存储器 41 或安全区域 51 读取所述文件时，存储器管理部分 16 通过加密和解密电路 17 来解密数据（此时，加密和解密电路 17 使用在内部非易失性存储器 41 中存储的加密密钥来解密数据），并且向 IC 命令处理部分 13 发送数据。

所解密的数据被发送到控制部分 20，并且从数据 I/F 部分 21 被发送到 R/W 单元 69。

对于大容量非易失性存储器 50 的非验证区域 53、验证区域 52 和安全区域 51 与内部非易失性存储器 41 的写/读条件被布置如下：

- 非验证区域：可以被无条件地存取。可以使用用于存取非验证区域 53 的常用命令来写/读数据。
- 验证区域：所述终端需要被控制部分 20 的控制验证部分 23 验证。当控制验证部分 23 验证所述终端时，使得有可能使用验证区域 52 的逻辑地址来存取验证区域 52。
- 安全区域：所述终端需要被 IC 部分 11 的 IC 验证部分 15（＝IC 部分应用）验证。使得有可能按照在 IC 部分应用和所述终端之间确定的命令来写/读数据（或者使得有可能作为 IC 部分应用的处理的一部分来写/读数据）。不能从所述终端看到安全区域，并且所述终端不能使用安全区域的逻辑地址来

存取安全区域。

• 内部非易失性存储器：内部非易失性存储器的写/读条件与安全区域的写/读条件相同。可以使得用于存取安全区域的验证与用于存取内部非易失性存储器的验证不同。

图 8 示出了大容量非易失性存储器 50 的内部结构。在此，在大容量非易失性存储器 50 的物理地址空间中，非验证区域 53 位于 0000 到(XXXX-1)，验证区域 52 位于 XXXX 到(ZZZZ-1)，并且安全区域 51 位于 ZZZZ 到(YYYY)。指示在安全区域 51 和验证区域 52 之间的边界的第一地址信息是 ZZZZ，并且指示在验证区域 52 和非验证区域 53 之间的边界的第二地址信息是 XXXX。非验证区域 53 的大小是 XXXX，验证区域 52 的大小是 ZZZZ-XXXX，安全区域 51 的大小是 YYYY-ZZZZ+1。

图 9 示出了用于表示在每个区域的物理地址和逻辑地址之间的对应性的“逻辑物理地址转换表”。非验证区域 53 的逻辑地址是 0000 到(XXXX-1)，验证区域 52 的逻辑地址是 0000 到(ZZZZ-XXXX-1)，并且安全区域 51 的逻辑地址是 0000 到(YYYY-ZZZZ)。

地址信息管理区域 54 保存所述区域的第一地址信息、第二地址信息和逻辑物理地址转换表。对于非验证区域 53、验证区域 52 或安全区域 51 的任何一个不能超出所分配逻辑地址边界而指定逻辑地址，但是可以将在所述区域之间的边界移动以扩大或缩小每个区域。

可以当改变第一地址信息时，扩大/缩小安全区域 51。在图 9 的逻辑物理地址转换表中，在非验证区域 53 和验证区域 52 中的逻辑地址顺序是物理地址顺序的正常顺序，并且在安全区域 51 中的逻辑地址顺序是与物理地址顺序相反的顺序。因此，当在验证区域 52 和安全区域 51 之间的边界改变时，仅仅需要校正验证区域 52 和安全区域 51 的逻辑块的结束地址，因此减小了伴随边界改变而重写表的负担，并且使得高速处理成为可能。

下面说明边界改变步骤。

接着，将讨论在安全存储卡中的数据存储步骤。

图 5 和 6 示出了从自其中放置了安全存储卡的终端向提供服务器发送内容购买请求，并且执行价格支付处理以将电子票据存储在安全区域中、在非验证区域中存储加密内容和在验证区域中存储内容解密密钥。

如图 5 所示，所述终端向提供服务器发送内容购买请求（1）。提供服务

器请求所述终端以支付内容的价格（2）。所述终端向安全存储卡 10 的 IC 部分 11 发送命令以请求 IC 部分 11 开始支付应用（3）。控制部分 20 的控制命令处理部分 24 将所述命令识别为提供给 IC 部分的命令，并且向 IC 部分 11 发送所述命令（4）。IC 部分 11 开始所述支付应用，激活 IC 验证部分 15，并且向所述终端返回响应（5）、（6）。所述终端向安全存储卡 10 发送验证请求命令（7），并且控制部分 20 的控制命令处理部分 24 将所述命令识别为提供给 IC 部分的命令，并且向 IC 部分 11 发送所述命令（8）。IC 验证部分 15 验证所述终端（或者提供服务器），并且返回验证结果（9）、（10）。被验证的终端向安全存储卡 10 发送用于指示可支付的数量的支付请求命令（11）。控制部分 20 的控制命令处理部分 24 将所述命令识别为提供给 IC 部分的命令，并且向 IC 部分 11 发送所述命令（12）。IC 验证部分 15 确定要根据“支付请求”命令来向内部非易失性存储器 41 写入所述数据，从内部非易失性存储器 41 中记录的余额减去所述可支付的数量，并且将所述结果重写到内部非易失性存储器 41 中，并且做出处理完成的响应（13）、（14）（如果所述终端在（9）中还没有被验证，则拒绝支付请求）。

所述终端向提供服务器返回响应（15）。提供服务器向所述终端发送电子票据（16）。所述终端向安全存储卡 10 发送电子票据存储请求命令（17）。控制部分 20 的控制命令处理部分 24 将所述命令识别为提供给 IC 部分的命令，并且向 IC 部分 11 发送所述命令。IC 验证部分 15 确定根据“电子票据存储请求”命令来将数据存储在安全区域 51 中，并且通过加密和解密电路 17 来加密所述电子票据，然后将所加密的电子票据存储在安全区域 51 中（18）（如果所述终端在（9）中还没有被验证合格，则拒绝电子数据存储请求）。

在（9）的验证中，IC 验证部分 15 可以分别进行允许“支付请求”的验证和允许“电子票据存储请求”的验证（即，可以要求使用不同密钥的验证）。

如图 6 所示，当指示电子票据已经从 IC 部分 11 存储到所述终端的响应时（19）（20），所述终端请求提供服务器发送内容（21）。提供服务器发送加密的内容和用于解密内容的内容密钥（22）。所述终端确定从提供服务器接收的数据包含要写入到验证区域 52 的内容密钥，并且请求安全存储卡 10 的控制部分 20 以进行验证（23）控制部分 20 的控制命令处理部分 24 解译所述命令，使得控制验证部分 23 验证所述终端，并且返回验证结果（24）。所述终端向验证区域 52 发送内容密钥写入请求（25）。由于所述终端已经被验证，

因此控制部分 20 的存取控制部分 25 允许存取验证区域 52，并且所述内容密钥被写入到验证区域 52 中。在接收到处理完成的响应时（26），所述终端确定要向非验证区域 53 写入所加密的内容，并且请求安全存储卡 10 向非验证区域 53 中写入所述内容（27）。当所加密的内容被写入非验证区域 53 中并且向所述终端返回响应时（28），所述终端向提供服务器发送完成通知（29）。

因此，电子票据被加密和写入到安全区域 51 中，内容密钥被写入到验证区域 52，并且加密的内容被写入非验证区域 53 中。

在图 5 的步骤中，当可支付的数量从内部非易失性存储器 41 中记录的余额减去，并且所述结果被重写到内部非易失性存储器 41 中时（13），可以将可支付的数量写入到安全区域 51 中（13'），如图 7 所示。在如此进行中，可以在安全区域 51 中记录支付日志。

在进行支付应用（3）的验证前或后，可以执行个人标识号检查以识别用户。

接着，将讨论改变在大容量非易失性存储器 50 中的区域之间改变的边界的步骤。在此，示出了这样的情况，其中，在图 8 中的第一地址信息被改变以扩大或缩小安全区域 51。

响应于对于来自其中放置了安全存储卡 10 的终端的请求的响应而进行边界改变。

（1）所述终端请求安全存储卡 10 开始边界改变应用，并且开始所述应用的安全存储卡 10 的 IC 部分 11 激活 IC 命令处理部分 13 和 IC 验证部分 15。所述终端请求 IC 部分 11 验证所述终端，并且 IC 验证部分 15 验证所述终端。这个验证可以与对于存取内部非易失性存储器 41 或安全区域 51 所需要的验证分离，以便仅仅一些特定的终端可以扩大/缩小安全区域 51。

（2）被验证合格的终端向 IC 部分应用（IC 命令处理部分 13）发送改变后的第一地址信息（新 ZZZZ）。

（3）IC 命令处理部分 13 向存储器管理部分 16 传送新的 ZZZZ，并且指令存储器管理部分 16 进行安全区域 51 的边界改变。存储器管理部分 16 校正安全区域 51 和验证区域 52 的逻辑物理地址转换表，以便对应于新的 ZZZZ 值，并且将所述新的 ZZZZ 值和所校正的逻辑物理地址转换表存储在地址信息管理区域 54 中。此时，在图 9 中的安全区域和验证区域的表中，仅仅校正逻辑块的结束地址。

（4）如果扩大安全区域51，则存储器管理部分16擦除作为新安全区域的部分中的数据；如果安全区域51被缩小，则存储器管理部分16擦除作为新的验证区域52的部分中的数据。此时，可以擦除在安全区域和/或验证区域中的所有数据。

（5）IC命令处理部分13向所述终端发送边界改变完成通知。

此时，安全存储卡10的控制部分20可以根据来自IC部分的请求而执行边界改变处理。在这种情况下，所述步骤如下：

（1）所述终端被IC验证部分15验证，如以上（1）中所述。

（1’）所述终端请求安全存储卡10的控制部分20验证所述终端。控制验证部分23按照控制命令处理部分24的指令而验证所述终端以允许改变验证区域的大小。

（2）所述终端向IC命令处理部分13发送改变后的所述第一地址信息（新ZZZZ），如以上在（2）中所述。

（3）IC命令处理部分13请求控制部分命令处理部分24通过存取控制部分25来进行边界地址改变。

（3’）控制部分命令处理部分24将所述ZZZZ值存储在地址信息管理区域54中，并且校正安全区域和验证区域的逻辑物理地址转换表，以便对应于所述ZZZZ值。（但是，如果不进行在（1’）中的验证，则拒绝所述边界地址改变，并且向IC命令处理部分13通知拒绝所述边界地址改变。）

（4）如果扩大了安全区域，则控制部分命令处理部分24擦除作为新安全区域的部分中的数据；如果缩小安全区域，则控制部分命令处理部分24擦除在作为新验证区域的部分中的数据。可以擦除安全区域和/或验证区域中的所有数据。

（5）控制部分命令处理部分24向IC命令处理部分13发送边界改变完成通知，IC命令处理部分13随后向所述终端发送边界改变完成通知（但是，如果在（3’）拒绝了边界地址改变，则向所述终端通知拒绝了边界改变）。

当改变在验证区域和非验证区域之间的边界的第二地址信息时，扩大/缩小验证区域。在这种情况下，步骤如下：

（1）所述终端请求安全存储卡10的控制部分20验证所述终端。控制验证部分23按照控制命令处理部分24的指令而验证所述终端以允许改变验证区域的大小。

（2）所述终端向控制部分 20 发送改变后的所述第二地址信息（新 XXXX）。

（3）控制部分命令处理部分 24 将 XXXX 值存储在地址信息管理区域 54 中，并且校正安全区域和验证区域的逻辑物理地址转换表，以便对应于所述 XXXX 值。（但是，如果不进行（1）中的验证，则拒绝所述边界地址改变，并且向所述终端通知拒绝所述边界地址改变。）

（4）如果扩大了验证区域，则控制部分命令处理部分 24 擦除作为新验证区域的部分中的数据；如果缩小验证区域，则控制部分命令处理部分 24 擦除作为新验证区域的部分中的数据。可以擦除非验证区域和/或验证区域中的所有数据。

（5）控制部分命令处理部分 24 向所述终端发送边界改变完成通知。

在这种情况下，如果在非验证区域 53 中的逻辑地址顺序是物理地址顺序的正常顺序、并且在验证区域 52 中的逻辑地址顺序是与图 10 中所示的逻辑物理地址转换表中的物理地址顺序相反的顺序，则当改变边界时，仅仅需要校正非验证区域和验证区域的逻辑块的结束地址，因此减小了伴随边界改变而重写表的负担，并且使得高速处理成为可能。

可以当执行验证区域的扩大/缩小处理时扩大/缩小所述非验证区域。

在大容量非易失性存储器 50 中，安全区域 51、非验证区域 53 和验证区域 52 可以以如图 11 所示的顺序来放置。图 12 示出了此时的逻辑物理地址转换表的示例。

在这种情况下，为了将安全区域 51 对所述终端隐藏或保持与没有安全区域的存储卡的兼容性，可以提供与实际边界地址不同的“终端假定地址”，如图 11 所示。对于所述终端假定地址，在跳过安全区域的情况下，将非验证区域 53 的顶部假定物理地址设置为 0000（实际上是 XXXX’），将在非验证区域 53 和验证区域 52 之间的边界的假定物理地址设置为 ZZZZ”（实际上是 ZZZZ’），并且将验证区域终止的假定物理地址设置为 YYYY”（实际上是 YYYY’）。所述终端将所述边界地址识别为 ZZZZ”，并且当作出扩大/缩小区域的请求时作出改变地址 ZZZZ”的请求。控制命令处理部分将识 ZZZZ”和 ZZZZ’之间的关系，并且使用被替换为实际的物理地址 ZZZZ’的 ZZZZ”来改变边界。

在本发明的实施例中，已经说明了这样的情况：其中，大容量非易失性

存储器 50 包括作为存储区域的三个区域：非验证区域、验证区域和安全区域，但是大容量非易失性存储器 50 可以除了安全区域之外仅仅包括非验证区域和验证区域之一来做为普通区域。

已经主要说明了其中在安全存储卡的 IC 部分中安装支付应用的情况，但是也可以安装签字产生应用。

在这种情况下，当数据被写入到安全区域中时，写数据的散列值被计算和存储在 IC 部分的内部非易失性存储器中，并且对于所述散列值产生电子签字。当（在解密后）从安全区域读取数据时，再次计算所述散列值，并且在写入时将其与在 IC 部分的内部非易失性存储器中存储的所述散列值相比较，由此检测数据缺陷、窜改等。

当安装这样的功能时，也可以在支付中使用安全存储卡，并且当向一些数据增加电子签字时也可以使用安全存储卡。

作为使用安全存储卡的 R/W 单元，已经说明了在存储卡中的这样的单元，它安装数字内容提供服务应用，并且具有支付功能和内容下载和存储功能，但是，所述 R/W 单元需要下列功能以充分利用安全存储卡：

- 可以产生用于读取和写入安全存储卡的普通区域的命令。
- 可以产生用于请求安全存储卡的 IC 部分执行处理的 IC 命令。
- 可以获取用于使用 IC 部分应用（IC 验证部分）来进行验证的验证密钥，并且使用所述验证密钥而产生验证所需要的数据（由 IC 部分应用提供的随机数的加密或签字的数据）。

如果所述安全存储卡除了所述功能之外，还具有作为普通区域的非验证区域和验证区域，则 R/W 单元需要具有下述能力：

- 产生用于读取和写入验证区域的命令。
- 获取用于使用安全存储卡的控制验证部分来进行验证的验证密钥，并且使用所述验证密钥而产生验证所需要的数据。

如果 R/W 单元（电子器件）在 ROM 等中保存验证密钥，则从其获得验证密钥。如果电子器件不保存验证密钥，则从外部器件（服务器、可移动介质等）接收验证密钥。

如果本发明的安全存储卡 10 的大容量非易失性存储器 50 被替换为任何其他的存储介质，例如诸如硬盘、光盘或磁光盘的非易失性介质，则不必说，可以像在本发明中那样实现大容量高安全性的存储器。

本发明的安全存储卡 10 可以不必被附加到电子器件或从电子器件拆卸，并且可以像例如在具有被嵌入到电子器件中的 IC 芯片的集成类型器件中那样固定地连接到电子器件。安全存储卡 10 不必像卡/芯片的形状，可以是盘或带。所述电子器件（60，61，69）如果能够连接到存储器件则可以是任何电子器件，诸如固定终端、便携终端或移动电话。

即，除了在本发明的实施例中所述的模式之外，响应于使用，各种模式——其中在移动电话中嵌入 IC 芯片、其中在固定终端中置入硬盘等——是可能的。

虽然已经参照特定的实施例详细说明了本发明，但是对于本领域的技术人员显然，可以在不脱离本发明的精神和范围的情况下做出各种改变和修改。

本申请基于 2002 年 12 月 16 日提交的日本专利申请（第 2002-363597 号），在此通过引用将其并入在此。

产业上的应用

从上述的说明显然，本发明的存储器件可以具有在安全级别上等于 IC 卡、并且至今具有大于 IC 卡的存储容量。

所述存储器件作为一个器件包括在安全级别上不同的多个存储区域，并且可以处理数字钱款、音乐提供等各种服务。可以按照需要来改变所述多个存储区域的大小。

本发明的电子器件（R/W 单元）可以提供充分利用所述存储器件的各种服务。

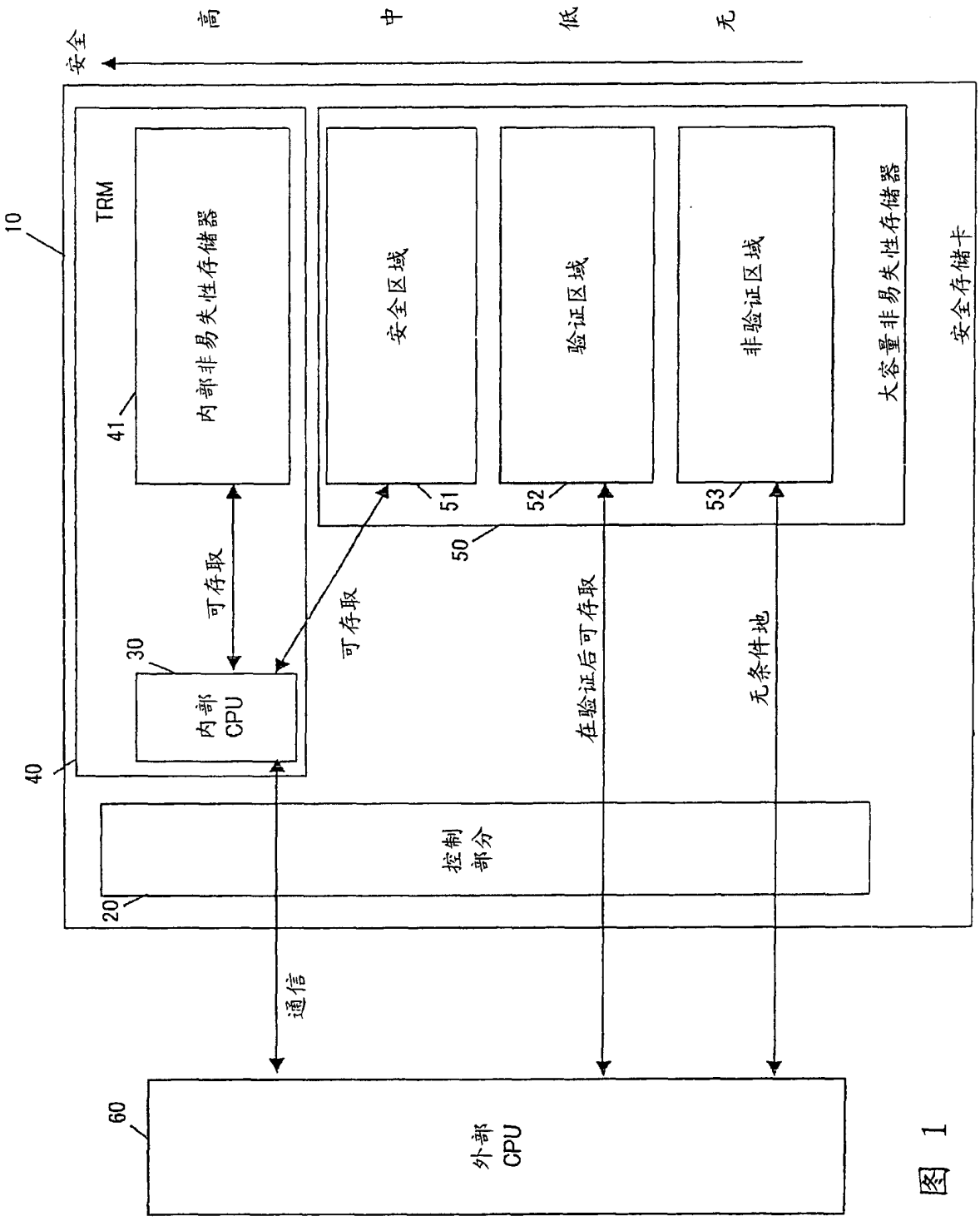

安全
高
中
低
无
10
TRM
内部非易失性存储器
41
安全区域
验证区域
非验证区域
大容量非易失性存储器
安全存储卡
51
52
53
50
可存取
可存取
30
内部
CPU
40
在验证后可存取
无条件地
控制
部分
20
通信
60
外部
CPU

图 1

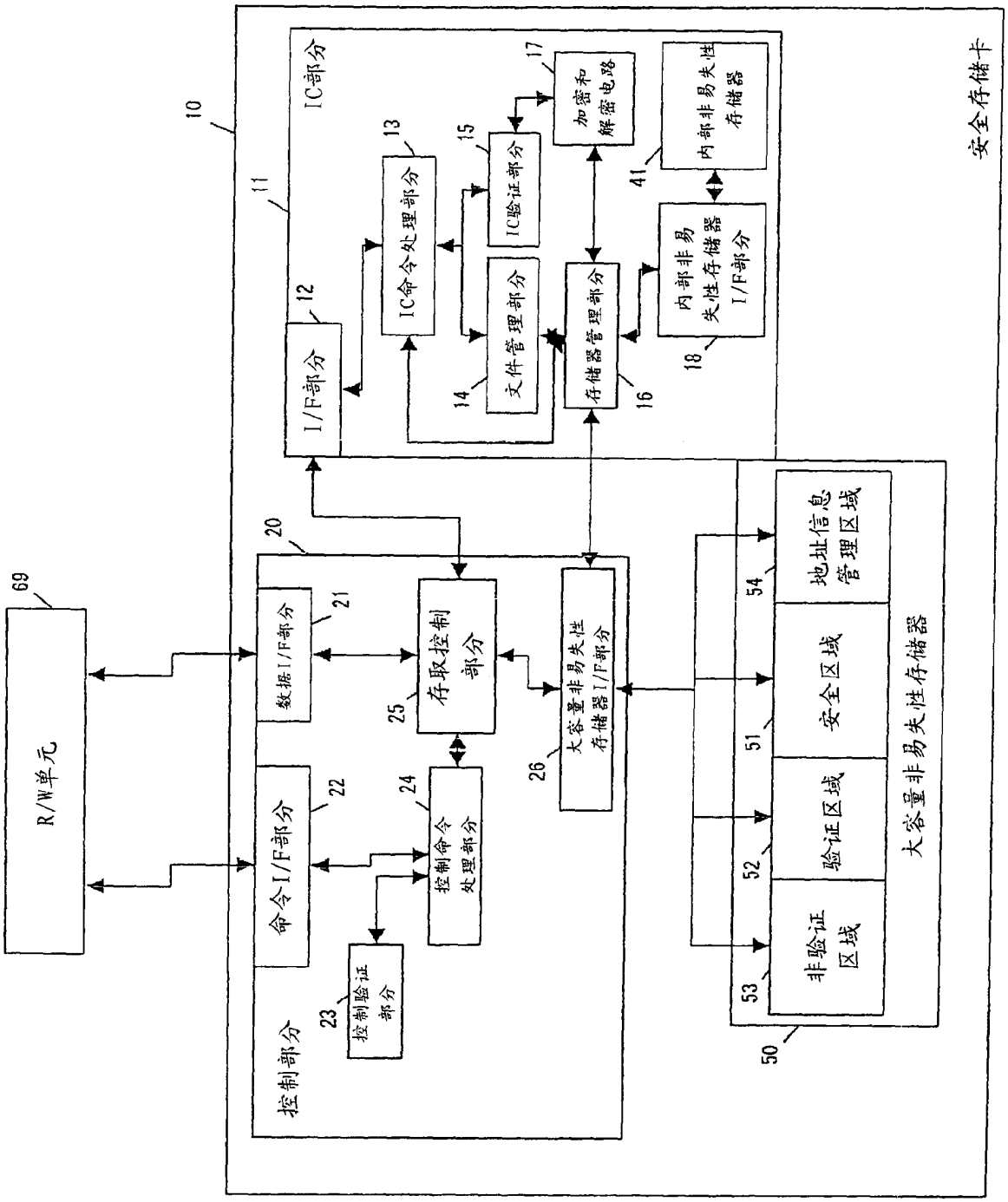

安全存储卡
10
IC部分
11
I/F部分
12
IC命令处理部分
13
文件管理部分
14
IC验证部分
15
存储器管理部分
16
加密和解密电路
17
内部非易失性存储器I/F部分
18
内部非易失性存储器
41
R/W单元
69
控制部分
20
数据I/F部分
21
命令I/F部分
22
控制验证部分
23
控制命令处理部分
24
存取控制部分
25
大容量非易失性存储器I/F部分
26
大容量非易失性存储器
50
非验证区域
53
验证区域
52
安全区域
51
地址信息管理区域
54

图 2

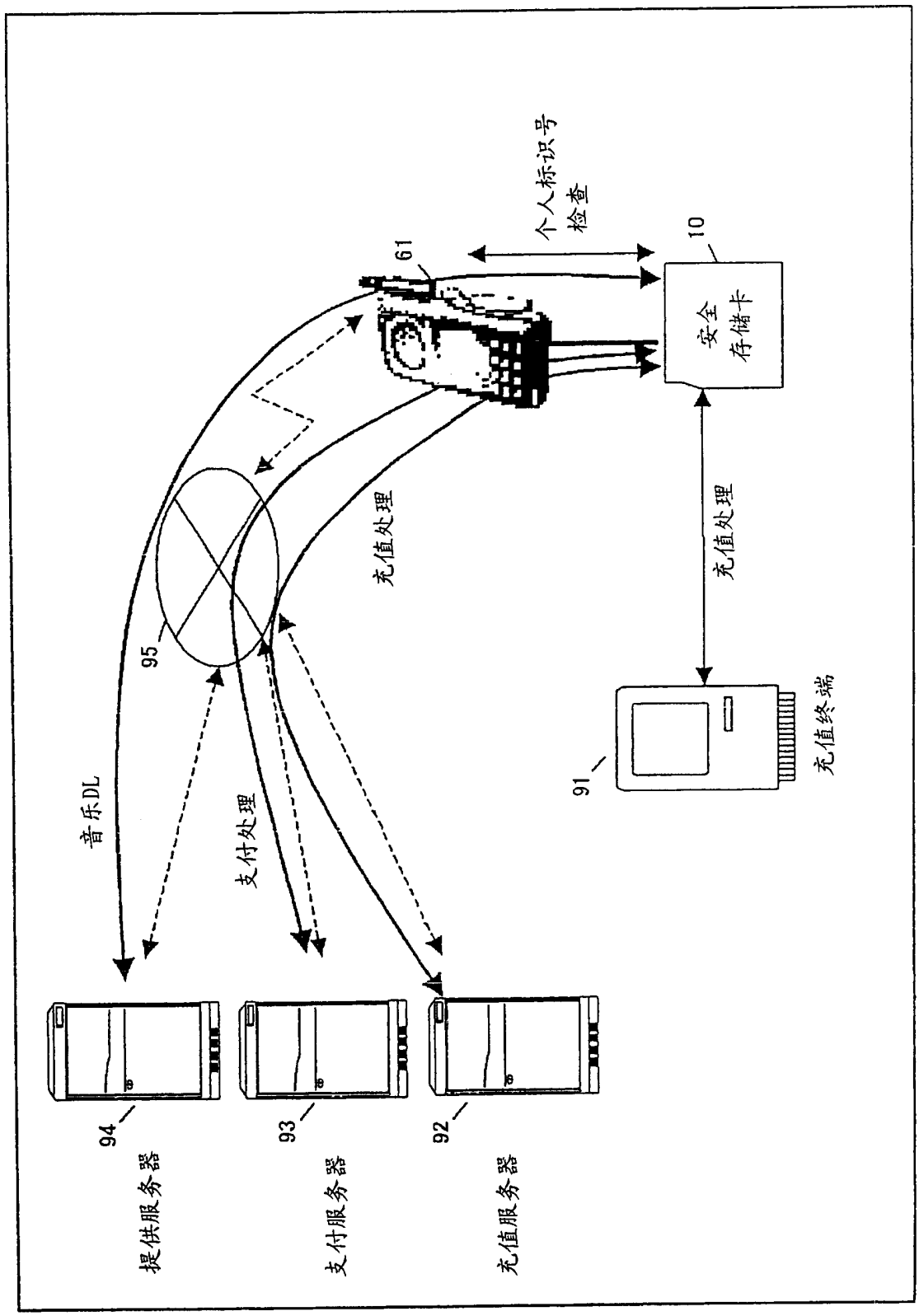

音乐DL
支付处理
充值处理
95
61
个人标识号
检查
10
安全
存储卡
充值处理
91
充值终端
94
提供服务器
93
支付服务器
92
充值服务器

图 3

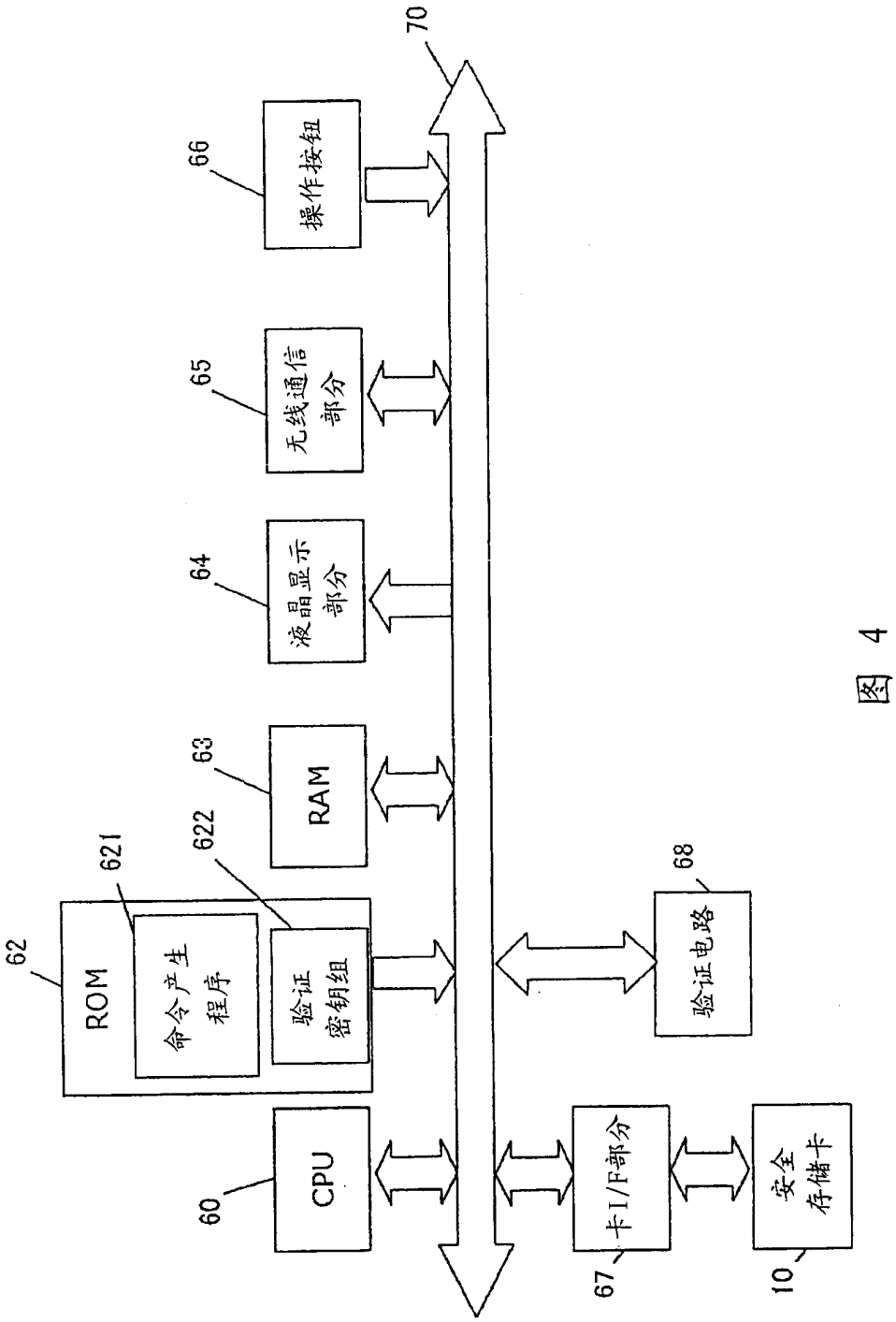

70
66
操作按钮
65
无线通信部分
64
液晶显示部分
63
RAM
62
ROM
621
命令产生程序
622
验证密钥组
68
验证电路
60
CPU
67
卡I/F部分
10
安全存储卡

图 4

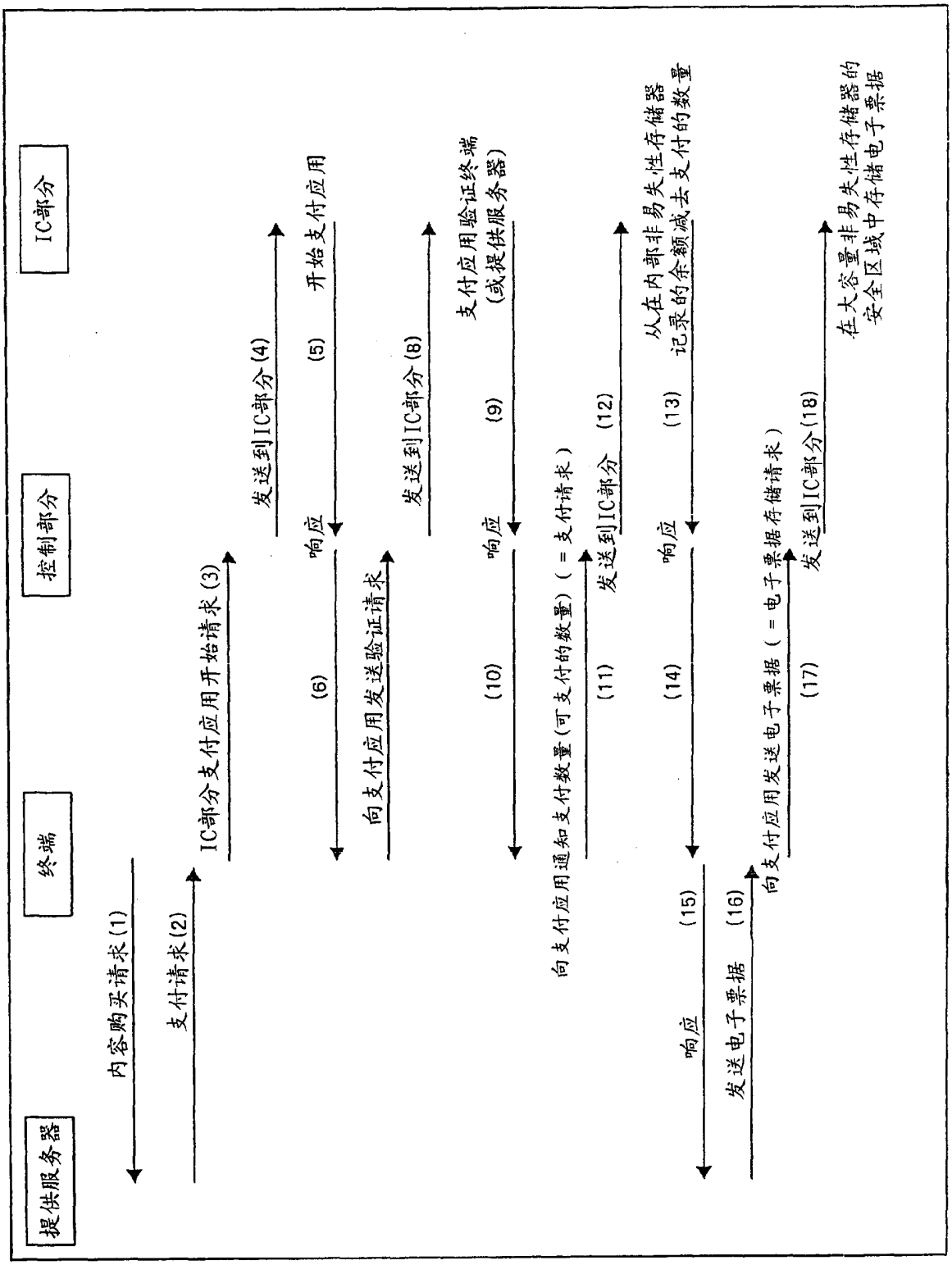

提供服务器
终端
控制部分
IC部分
内容购买请求(1)
支付请求(2)
IC部分支付应用开始请求(3)
发送到IC部分(4)
响应
(5) 开始支付应用
(6)
向支付应用发送验证请求
发送到IC部分(8)
支付应用验证终端
(或提供服务器)
(9)
响应
(10)
向支付应用通知支付数量(可支付的数量)(=支付请求)
发送到IC部分 (12)
(11)
从在内部非易失性存储器
记录的余额减去支付的数量
(13)
响应
(14)
发送电子票据 (16)
响应 (15)
向支付应用发送电子票据(=电子票据存储请求)
发送到IC部分(18)
(17)
在大容量非易失性存储器的
安全区域中存储电子票据

图 5

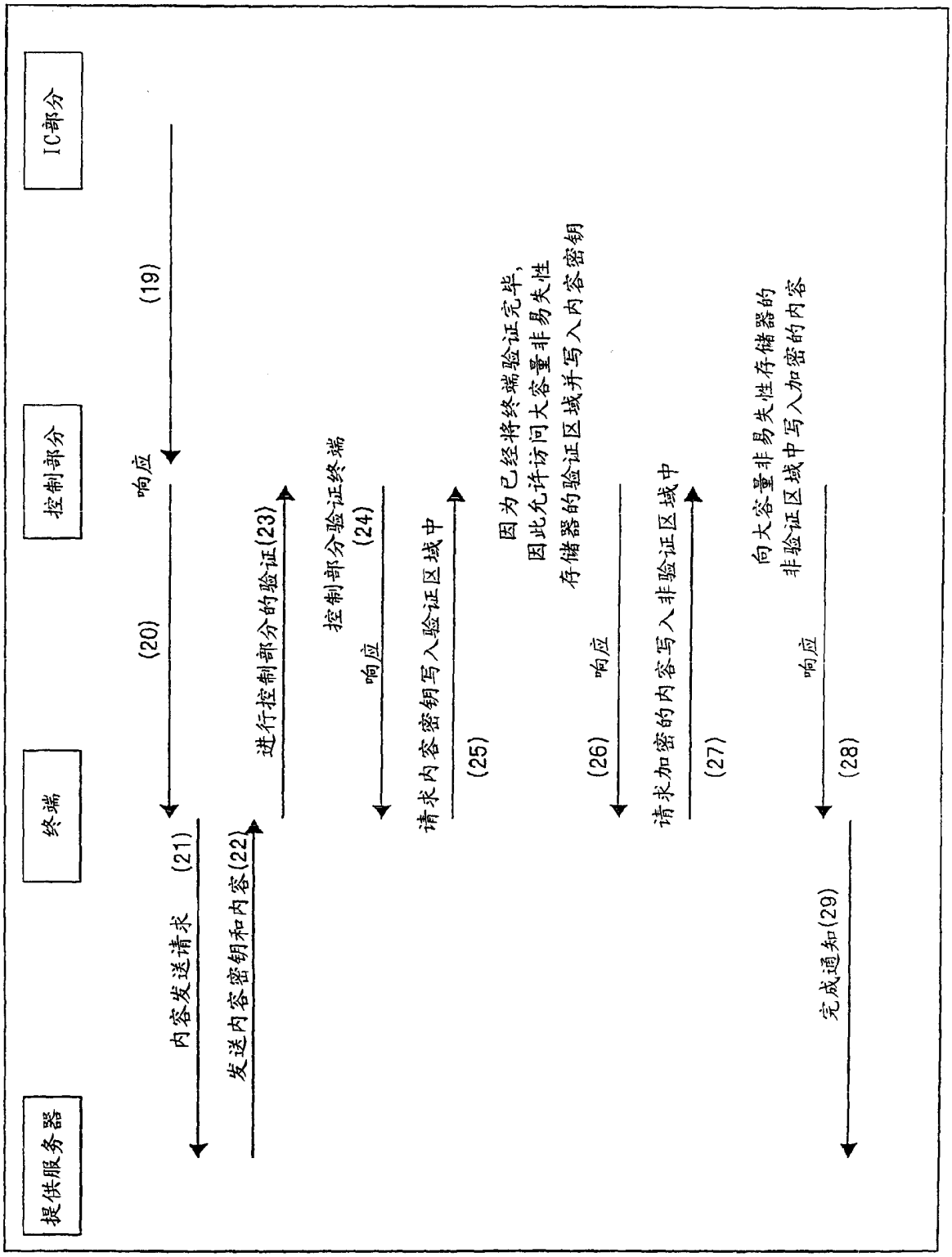

提供服务器
终端
控制部分
IC部分
(19)
响应
(20)
内容发送请求 (21)
发送内容密钥和内容(22)
进行控制部分的验证(23)
控制部分验证终端
(24)
响应
请求内容密钥写入验证区域中
(25)
因为已经将终端验证完毕，
因此允许访问大容量非易失性
存储器的验证区域并写入内容密钥
(26) 响应
请求加密的内容写入非验证区域中
(27)
向大容量非易失性存储器的
非验证区域中写入加密的内容
响应
(28)
完成通知(29)

图 6

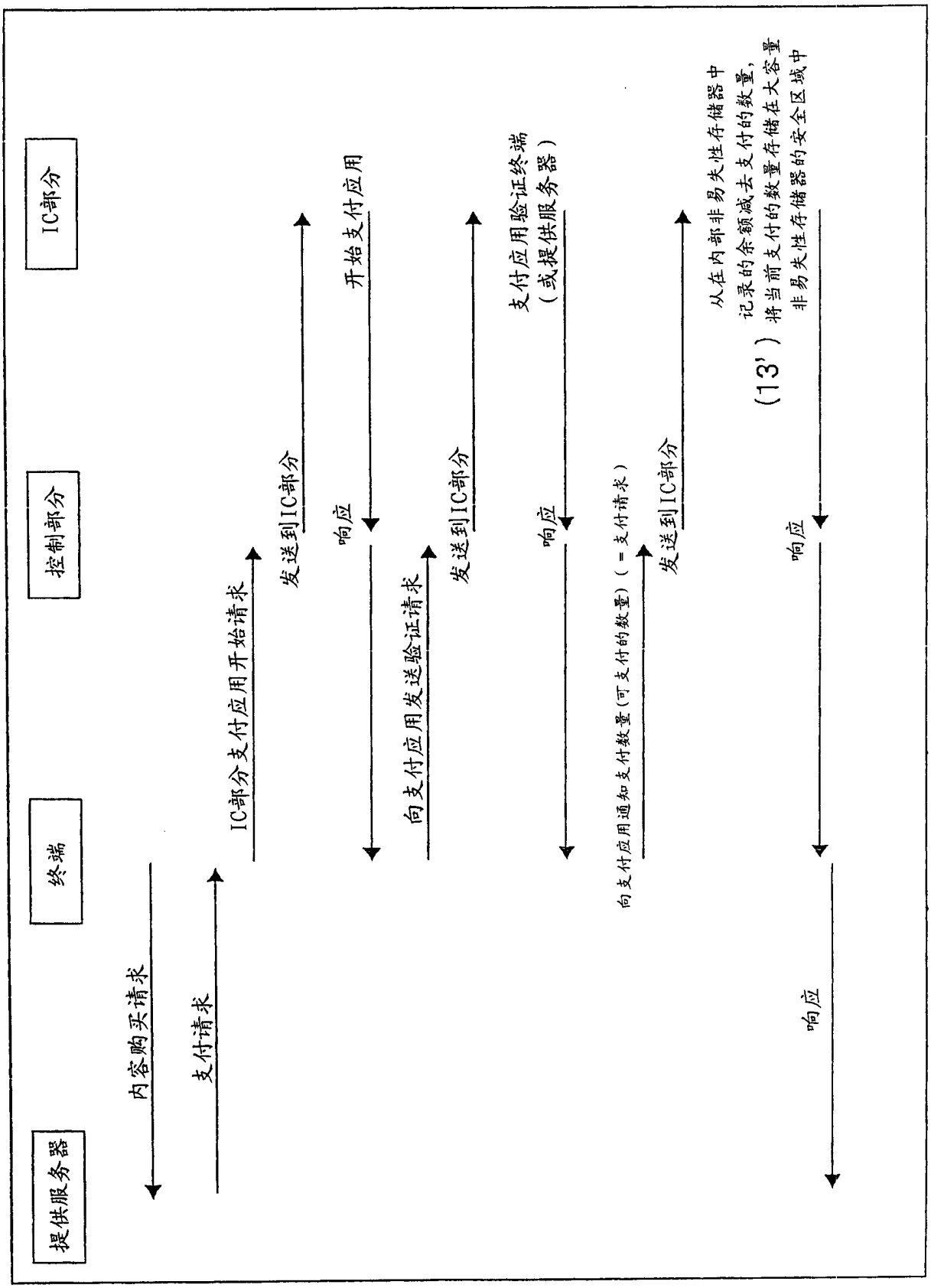

提供服务器
终端
控制部分
IC部分
内容购买请求
支付请求
IC部分支付应用开始请求
发送到IC部分
响应
开始支付应用
向支付应用发送验证请求
发送到IC部分
支付应用验证终端
（或提供服务器）
响应
向支付应用通知支付数量（可支付的数量）（＝支付请求）
发送到IC部分
从在内部非易失性存储器中
记录的余额减去支付的数量，
将当前支付的数量存储在大容量
非易失性存储器的安全区域中
(13')
响应
响应

图 7

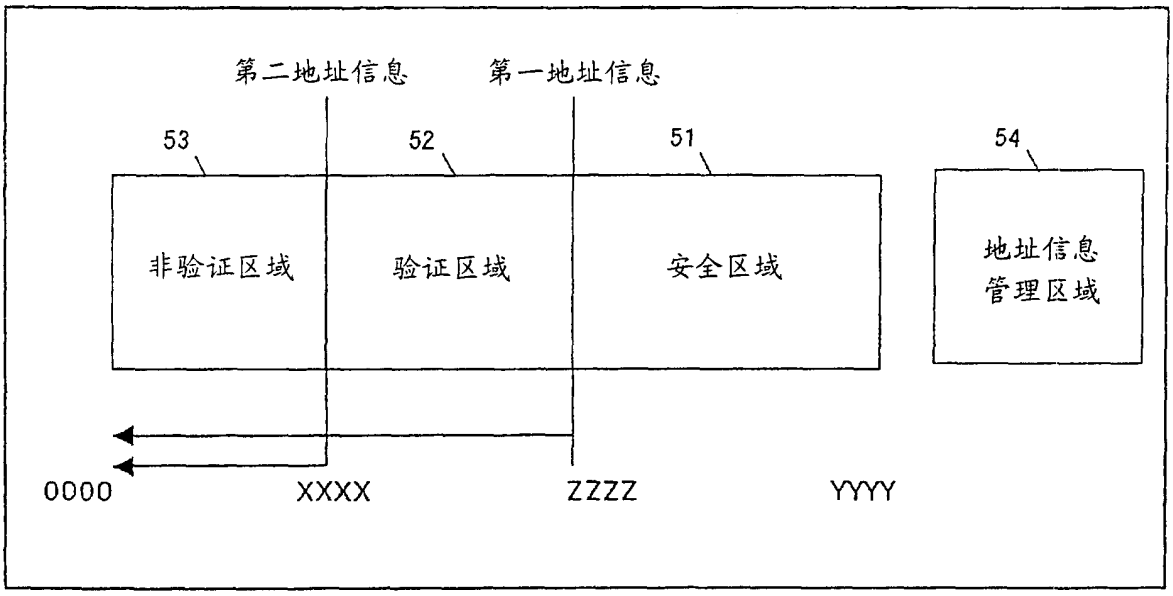

第二地址信息
第一地址信息
53
52
51
54
非验证区域
验证区域
安全区域
地址信息
管理区域
0000
XXXX
ZZZZ
YYYY

图 8

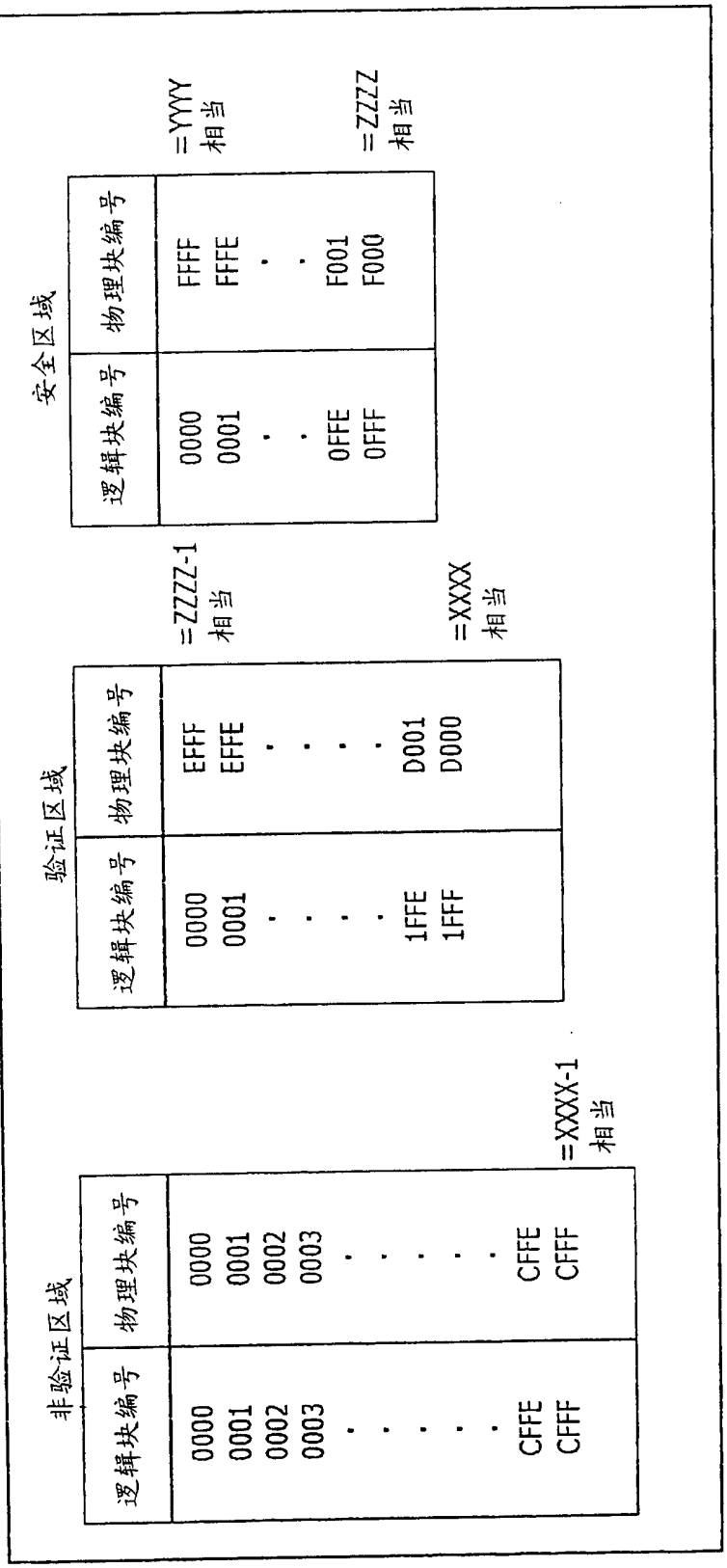

非验证区域
逻辑块编号
物理块编号
0000 0000
0001 0001
0002 0002
0003 0003
CFFE CFFE
CFFF CFFF
=XXXX-1
相当
验证区域
逻辑块编号
物理块编号
0000 EFFF
0001 EFFE
1FFE D001
1FFF D000
=ZZZZ-1
相当
=XXXX
相当
安全区域
逻辑块编号
物理块编号
0000 FFFF
0001 FFFE
OFFE F001
OFFF F000
=YYYY
相当
=ZZZZ
相当

图 9

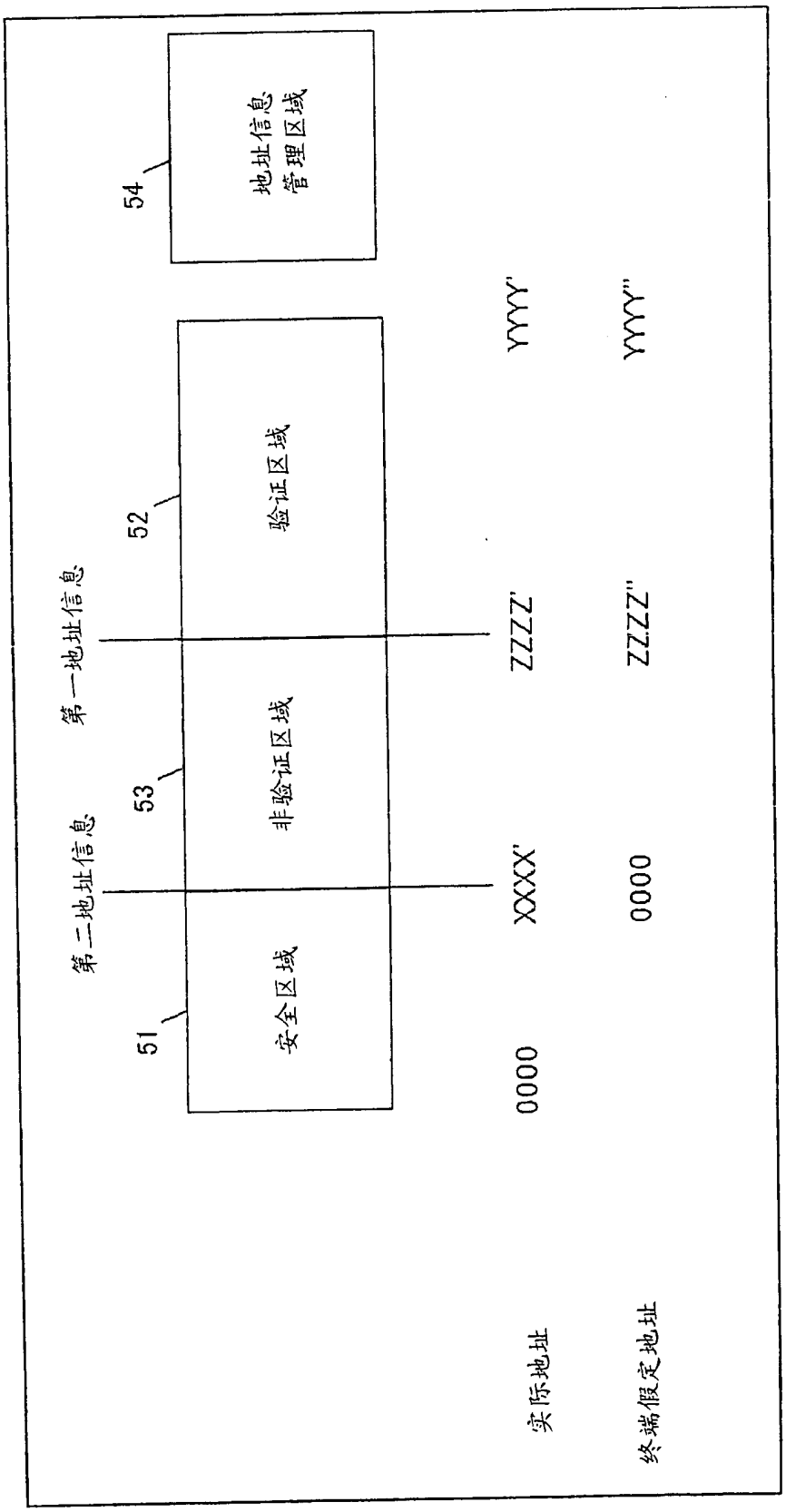

第二地址信息
第一地址信息
51
53
52
54
安全区域
非验证区域
验证区域
地址信息
管理区域
0000
XXXX'
ZZZZ'
YYYY'
0000
ZZZZ''
YYYY''
实际地址
终端假定地址

图 10

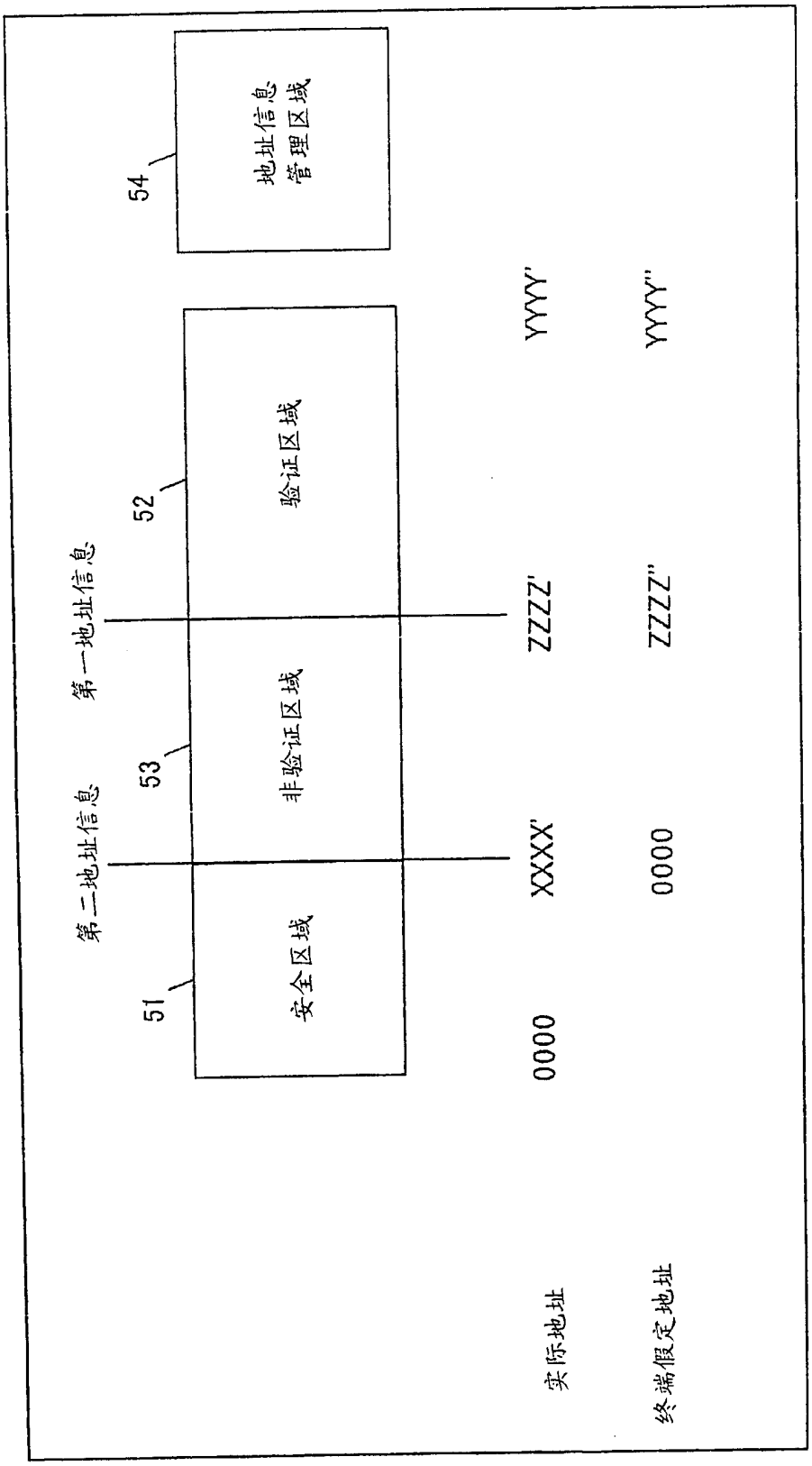

第二地址信息
第一地址信息
51
53
52
54
安全区域
非验证区域
验证区域
地址信息
管理区域
0000
XXXX'
ZZZZ'
YYYY'
0000
ZZZZ''
YYYY''
实际地址
终端假定地址

图 11

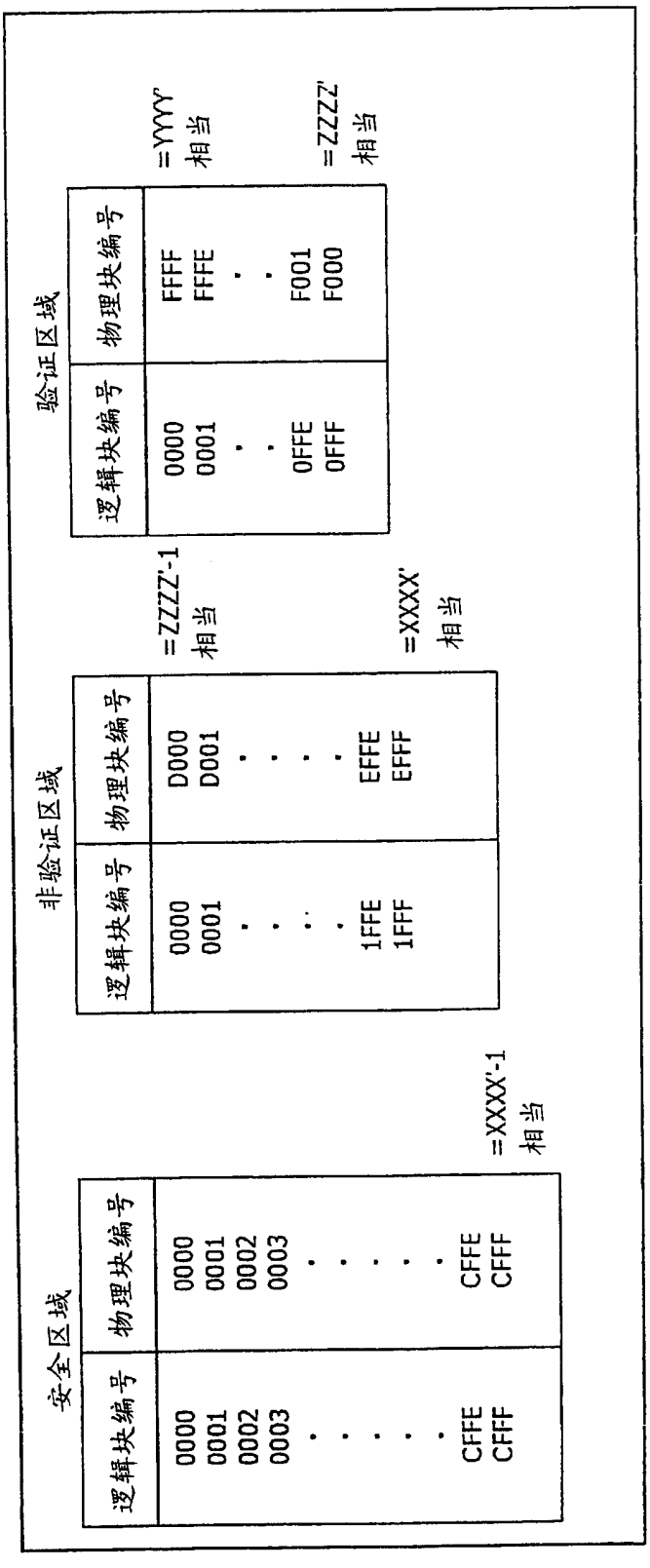

安全区域
逻辑块编号
物理块编号
0000 0000
0001 0001
0002 0002
0003 0003
CFFE CFFE
CFFF CFFF
=XXXX'-1
相当
非验证区域
逻辑块编号
物理块编号
0000 D000
0001 D001
1FFE EFFE
1FFF EFFF
=ZZZZ'-1
相当
=XXXX'
相当
验证区域
逻辑块编号
物理块编号
0000 FFFF
0001 FFFE
0FFE F001
0FFF F000
=YYYY'
相当
=ZZZZ'
相当

图 12