[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G07F 7/10

[12] 发明专利说明书

[21] ZL 专利号 01802736.9

[45] 授权公告日 2005 年 3 月 16 日

[11] 授权公告号 CN 1193321C

[22] 申请日 2001.7.10 [21] 申请号 01802736.9

[30] 优先权

[32] 2000. 7.11 [33] CH [31] 1365/2000

[86] 国际申请 PCT/CH2001/000433 2001.7.10

[87] 国际公布 WO2002/005225 德 2002.1.17

[85] 进入国家阶段日期 2002.5.13

[71] 专利权人 卡巴闭锁系统公开股份有限公司

地址 瑞士韦齐康

[72] 发明人 K·U·克洛萨 R·埃彭伯格

审查员 尹海霞

[74] 专利代理机构 中国专利代理(香港)有限公司

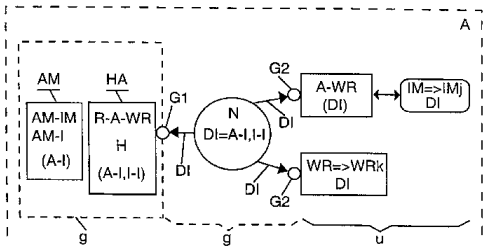
代理人 郑立柱 张志醒

权利要求书 3 页 说明书 13 页 附图 7 页

[54] 发明名称 初始化移动数据载体的方法和设备

[57] 摘要

以该方法在授权系统(A)的范围内在分配的分散的写与读站(WR)上初始化移动数据载体(IM)。在安全环境中(g)中的授权主管(HA)上通过授权单元(AM)产生初始化数据(DI、A－I、I－I)，并且该初始化数据经过网络(N)以安全的通信并以与授权系统(A)一致的安全规则被发送到分散授权的写与读站(A－WR)上，在那里以初始化数据(DI)初始化移动数据载体(IM)，和/或其中初始化数据经过网络被发送到分散的写与读站(WR)，以该初始化数据初始化写与读站。该初始化方法使如此系统的新应用可能性和使用可能成为可能。



ISSN1008-4274

知识产权出版社出版

1. 在授权系统（A）的范围内以分配的分散写与读站（WR）初始化移动数据载体（IM）和/或初始化分散的写与读站（WR）的方法，其特征在于，

在安全环境（g）中通过授权以在授权主管（HA）上的授权单元（AM）产生初始化数据（DI），并且该初始化数据经过网络（N）以安全的通信并以与授权系统一致的安全规则被发送到分散授权的写与读站（A－WR），

并且其中在所述分散授权的写与读站（A－WR）上以初始化数据（DI）相应初始化（IMj）移动数据载体（IM），

和/或初始化数据（DI）经过网络（N）被发送到分散的写与读站（WR），以该初始化数据初始化（WRk）所述分散的写与读站（WR）。

2. 按照权利要求 1 的方法，其特征在于，通过主计算机（H）或通过一个远距离的授权写与读站（R－A－WR）形成授权主管（HA）。

3. 按照权利要求 1 的方法，其特征在于，通过特殊的授权识别媒介（AM－IM）或通过授权数据（AM－I）形成授权单元（AM）。

4. 按照权利要求 1 的方法，其特征在于，一个分散的写与读站（WR）通过在初始化数据（DI）中包含的功能授权数据（A－I－FA）首先变换为一个分散授权的写与读站（A－WR），其接下来可以根据初始化数据初始化移动数据载体（IM）。

5. 按照权利要求 1 的方法，其特征在于，在授权系统（A）的范围内预先规定多个具有同样和/或不同授权级（OLi）的授权主管（HAi）。

6. 按照权利要求 1 的方法，其特征在于，预先规定多个具有同样和/或不同授权级（OLi）的授权单元（AMi）。

7. 按照权利要求 1 的方法，其特征在于，初始化数据（DI）经过多于一个的网络级（N1、N2）和/或经过多于一个的授权主管（HA1、HA2）被传递到所述分散授权的写与读站（A－WR）或者分散的写与读站（WR）上。

8. 按照权利要求 1 的方法，其特征在于，经过安全的专用网络（Np）

传递初始化数据（DI）。

9. 按照权利要求 1 的方法，其特征在于，经过公共网络（No）以密钥和相互的安全门（G1、G2）传递初始化数据。

10. 按照权利要求 1 的方法，其特征在于，以初始化数据（DI2.2）初始化应用扩展(App2.2)。

11. 按照权利要求 1 的方法，其特征在于，以初始化数据（DI3）初始化新的独立应用（App3）。

12. 按照权利要求1的方法，其特征在于，在备有一个系统数据区（CDF）的空移动数据载体中，以初始化数据（DI）进行新初始化应用（App）。

13. 按照权利要求 1 的方法，其特征在于，经过网络（N）在授权主管（HA）和分散授权的写与读站（A－WR）之间存在持续的连接。

14. 按照权利要求 1 的方法，其特征在于，授权主管（HA）和所述分散授权的写与读站（A－WR）之间经过网络（N）的连接仅仅暂时存在并且当数据交换时才出现。

15. 按照权利要求 1 的方法，其特征在于，为了进行初始化，所述分散的写与读站（WR）或者其所有者（12）实施使用者授权（aw）或者识别授权单元（ID－AM）。

16. 按照权利要求 1 的方法，其特征在于，为了进行初始化，数据载体或者数据载体的所有者（13）实施使用者授权（ai）。

17. 按照权利要求 1 的方法，其特征在于，为了经过网络（N）授权初始化、并且为了在所述分散的写与读站（WR）上或者在数据载体（IM）上执行应用，将所述写与读站的所有者的使用者授权（aw）或者数据载体的所有者的使用者授权（ai）用作授权单元。

18. 按照权利要求 1 的方法，其特征在于，移动数据载体（IM）包含一个应用微处理器（AppuP）用于处理应用程序数据（I－I－Cod）。

19. 按照权利要求 1 的方法，其特征在于，数据载体（IM）被设计为无接触的、有源或无源识别媒介。

20. 按照权利要求 1 的方法，其特征在于，由相同的移动数据载体形成移动数据载体（IM）、授权识别媒介（AM－IM）和识别授权单元（ID－

AM）。

21. 按照权利要求 1 的方法，其特征在于，关于在授权的或者在分散的写与读站（A－WR、WR）和/或在移动数据载体（IM）上的事件的状态信息（S－I）经过网络（N）告知相应的授权主管（HA）。

22. 按照权利要求 21 的方法，其特征在于，状态信息（S－I）用于使用或者特许结算。

23. 按照权利要求 1 的方法，其特征在于，对于使用结算或特许结算数据载体（IM）的每次新初始化经过网络（N）告知授权主管（HA）。

24. 按照权利要求 1 的方法，其特征在于，对于使用结算或特许结算在分散的写与读站（WR）上的应用的每次使用经过网络（N）告知授权主管（HA）。

25. 按照权利要求 1 的方法，其特征在于，预先规定经过网络（N）的数据载体（IM）的多级初始化，在授权系统（A）的范围内以体系分级措施实现该多级初始化。

26. 移动数据载体（IMj），具有经过网络（N）授权的、按照权利要求 1 的方法而初始化的应用（App）。

27. 写与读站（WRk），具有经过网络（N）授权的、按照权利要求 1 的方法而初始化的应用（k）。

28. 用于在授权系统（A）的范围内以分配的分散写与读站（WR）初始化移动数据载体（IM）和/或初始化分散的写与读站（WR）的设备，其特征在于，

通过在授权主管（HA）上的授权单元（AM）在一个安全的环境（g）中产生初始化数据（DI），并且初始化数据经过网络（N）以安全的通信并以与授权系统一致的安全规则被发送到分散授权的写与读站（A－WR）上

并且在所述分散授权的写与读站（A－WR）上以初始化数据相应初始化（IMj）移动数据载体（IM）

和/或初始化数据（DI）经过网络（N）发送到分散的写与读站（WR），以该初始化数据初始化（WRk）所述分散的写与读站（WR）。

初始化移动数据载体的方法和设备

技术领域

本发明涉及在授权系统的范围内以分配的分散写与读站初始化移动数据载体的方法和设备。

背景技术

移动数据载体（例如无触点或有触点识别媒介、芯片卡或数值卡等等）使用户能够在分配的写与读站上执行相应的应用、比如寻求帮助（PC 访问）和找寻商品（饮料自动售货机、饭店）或者到保护的范围、建筑物、体育场等等的访问。为了使这些访问或者应用的执行成为可能，在授权系统范围内以相应初始化信息初始化数据载体和分配的写与读站是必要的。

初始化可能涉及应用特殊的数据（例如在数据载体上登记货币价值）并且涉及系统特殊的数据（例如地图出版者号码、在多应用中的数据结构、在数据载体上的存取规则等等）。可以渐渐、一步一步地并且在不同时刻初始化并且也可以改变初始化数据或者应用。

这个初始化是一个安全较严格并且非常复杂的过程，局部显著限制该过程，并且仅仅在安全环境中的位置上进行该过程。对此在 WO 97/34265 中描述了一个实例。其在授权系统 A 的范围内描述了一个具有无接触的无源电数据载体的系统作为具有分配的写和读站 WR 的识别媒介 IM，其中数据载体可能包含多个独立的应用。在此必须根据体系的授权系统的规则初始化每个识别媒介和每个应用。对于数据载体的初始化需要在安全的环境中特殊的编程写与读站以及特殊的授权媒介，并且同样以一个特殊的授权媒介改变或者初始化所有分散的写和读站，以便可以接受其功能。

在这些大部分在不安全的环境中的分散的写与读站上数据载体 IM 的分散初始化在此是不可能的。因此初始化是非常复杂并且受限制的，授权媒介的初始化和管理是同样安全严格和复杂的。

因此在安全环境中具有特殊授权单元的每一个数据载体的已知的中心初始化是非常复杂的、不太灵活并且非常受限制。因此可以初始化并开始使用非分散的在不安全的环境中的新应用和新数据载体。

如果在一个滑雪区域、在该区域中对于不同的应用无接触的识别媒介作为滑雪卡读出、例如一个山区饭馆对于其应用和对于其客户想要在其应用中添加应用扩展、例如诚信应用，为此必须在一个安全环境中以一个初始化设备并且以一个相应的初始化媒介初始化每一个数据载体、也就是说每个滑雪卡，也就是说不是在山区饭馆中而是在山谷下面在滑雪区域中心。这种措施方式当然是不实用的。

在触点卡系统中一种完全另外形式的、经过网络的数据传输，必需由一个唯一的系统中心发出完整的结构和所有授权。从DE 197 20 431 中例如已知了一种用于从中央芯片卡管理系统中电子个人化并初始化芯片卡的方法。通过通信信道在芯片卡控制系统上或者读设备上实现初始化，该读设备物理接触芯片卡并且把数据直接传递给芯片卡。以这样的系统不可以解决下面的任务。

发明内容

因此本发明的任务是，建立一种方法或一个系统，该方法或者系统克服关于数据载体和分散的写与读站的初始化、应用的扩展和新数据载体读出的以前的限制，该方法或者系统形成十分简单、多方面并且安全的初始化方法，并且因此也建立新的使用可能性，并且该方法或者系统也特别使无接触数据载体的应用成为可能。

根据本发明通过根据权利要求1的初始化移动数据载体的方法和按照权利要求28的设备解决该任务。通过经过网络以安全通信和以通过授权单元的授权在安全环境中的远距离授权主管上的初始化十分重要地扩展具有移动数据载体和分散的写与读站的如此系统的另外应用和利用可能性。

从属权利要求涉及具有在关于应用和新数据载体的采用和关于新形式利用、运用和应用的局部方面扩展可能的本发明的改进。关键是，通过经过网络的安全通信并通过在保护的环境中在远距离的授权主管上与授权单

元建立联系保证可靠性，这样原则上所有分散的写和读站也可以在没有保护的环境中用于初始化。这也使完全新的应用成为可能、例如通过分散的写与读站检测并支配特许编号，数据载体的所有人或写与读站的有所人的私人数据的附加检索可以进一步提高分散授权的可靠性。

附图说明

下面根据图和实例进一步阐述本发明。

图 1 指出根据本发明、经过专用网络初始化数据载体的方法的示意图，

图 2 指出经过公共网络初始化数据载体的方法，

图 3 指出经过网络通过在一个具有授权单元的授权主管上的授权初始化数据载体和分散的写与读站的根据本发明的方法，

图 4 指出以授权信息和初始化信息的移动数据载体的初始化，

图 5 指出以授权和初始化信息写与读站的初始化，

图 6 指出在分散的写与读站上授权功能的初始化，

图 7 指出经过网络通过多个授权主管的应用的初始化，

图 8 指出通过多个授权主管经过网络的初始化，

图 9 指出通过多个授权主管经过多个网络级别的初始化，

图 10 指出通过多个授权主管经过多个具有多个授权级别的网络级别的初始化，

图 11 图解指出在具有多个授权或者结构级、在不同授权级上的多个授权主管和具有多个独立用户的授权系统中的结构，

图 12 在一个新数据载体中应用的初始化，

图 13 在一个数据载体中附加应用的初始化，

图 14 经过网络初始化数据载体的授权。

具体实施方式

图 1 至 3 说明了在一个授权系统 A 的范围内在分配的分散写与读站 WR 上初始化移动数据载体 IM 的根据本发明的方法，该方法确定对于写与读站、数据载体、授权主管和授权单元是和的体系规则，这例如在 WO 97/34265

中在具有无接触的识别媒介的系统上描述。可是该已知的系统仅仅用作本发明的可能应用实例。

在图 3 中说明了根据本发明的方法：在适用于所有系统单元的体系授权系统 A 的范围内通过具有在授权主管 HA 上授权单元 AM 的授权在安全环境 g 中实现以分配的分散写与读站 A－WR 初始化移动数据载体和/或初始化分散的写与读站 WR，在该环境中产生初始化数据 DI＝A－I、I－I，并经过网络 N 以安全的通信并且以与授权系统一致的安全规则把初始化数据发送给分散授权的写与读站 A－WR 或发送给分散的写与读站 WR。初始化数据 DI 对此包含由授权单元 AM 输入授权主管的授权信息 A－I 和也输入授权主管 HA 或从该授权主管中调用的初始化信息 I－I。

在分散的写与读站 A－WR 上相应以初始化数据 DI 初始化移动数据载体 IM 并且因此变换为已初始化的数据载体 IMj，或以初始化数据 DI 初始化分散的写与读站 WR 并且变换为已初始化的写与读站：WRK。

图 1 和 2 说明安全通信经过网络 N 直到在不安全环境 u 中的分散的写与读站 A－WR。

在图 1 的实例中对此经过安全的专用网络 Np 实现初始化，以此在写与读站上保证安全的环境。

图 2 指出了根据本发明的、经过公共网络 No 以密钥和双方的安全门 G1 和 G2 的初始化，以便保证经过公共网络的必要的安全通信。

通过经过网络 N 的安全连接通常处于不安全环境 u 中的分散写与读站 WR 或者 A-WR 对于初始化束缚在授权主管 HA 的安全环境中并且因此在安全的环境 g 中进行初始化。在实施初始化之后，可以在写与读站 WR 上象以前在不安全的环境中一样实施以识别媒介 IM 的应用。也仅仅必需暂时对于初始化建立经过网络的安全环境 g。

以图 4-6 清楚描述了不同的初始化过程。在图 4 中首先说明了授权主管 HA 和授权单元的可能实施。

与已知的、例如根据 DE 197 20 431 具有一个唯一的中央授权和组织中心（系统中心）的触点卡系统不同，必须从该中心实施并管理所有初始化，在根据本发明的系统中如此的授权系统中心 A 是不必要的。相反通过遵循体系的授权规则确定该授权系统 A，其中这些授权规则在不同的局部分布的授权主管 HAi 中例如在芯片上或作为程序植入并存储。授权规则或者授权单元 AM 原则上形成一个局部分布的“虚拟授权系统中心”A。通过系统的基本准备或基本初始化确保对于所有写与读站和所有识别媒介附属于系统 A。

为了以初始化信息 I-I（Appi）初始化新的应用具有授权信息 A-I 的与结构级一致的授权是必要的。以授权单元 AM 把与授权系统 A 一致的授权信息 A-I 传递给授权主管 HA。

对此根据图 4 授权主管 HA 例如包括一个具有系统 A 的相应授权规则的主计算机 H 或也包括一个远距离授权写与读站 R-A-WR。授权单元 AM 例如可以包括一个包含授权信息 A-I 的授权识别媒介 AM-IM 或包括例如作为软件（程序）在主机 H 中可以调用或者实施的授权数据 AM-I。在一个物理授权媒介 AM-IM 上通过授权媒介的载体（所有者）实现与安全要求一致的操作。在一个主机 H 中的软件程序 AM-I 的情况下通过用户识别、例如借助于 PIN 代码或生物统计数据或通过分配的特殊识别媒介（ID-AM）保证安全。

在图 4 中描述了数据载体 IM 的初始化。对此授权信息 A-I（j）涉及数据载体 IM 的初始化 j 的授权。在授权主管 HA 中输入、产生或调

用新应用 Appi 的初始化信息 I-I（Appi），并且正如已经描述的经过网络和分散授权的写与读站 A-WR 在数据载体 IMj 中初始化：IMj（具有 Appi）。

图 5 指出了写与读站 WR 的初始化 k。由授权主管 HA 的授权单元 AM 输入、产生或调用授权信息 A-I（k）。初始化信息 I-I（k）同样输入授权主管中。为了经过网络初始化写与读站 WR，也就是说为了变换为 WRk，首先授权信息 A-I（k）从授权主管 HA 传输到写与读站 WR 上，在写与读站上接下来实现初始化信息 I-I（k）的传输。类似于在数据载体上新应用的初始化也可以通过相应的初始化数据 I-I（k）实现写与读站 WR 的初始化，以该初始化在写与读站中例如可以采用附加功能。

图 6 指出了分散的写与读站 WR 变换为授权的写与读站 A-WR 或初始化，以便因此可以实施移动数据载体 IM 的初始化。为此首先必须以授权功能 FA 初始化写与读站。首先授权信息 A-I-FA 从授权单元 AM 输入授权主管 HA 中，接下来实施分散的写与读站 WR 的初始化或者变换为具有授权功能 FA 的授权的写与读站 A-WR。接着象前面一样（图 4）可以通过确定应用 Appi 的授权信息 A-I（j）和相应初始化信息 I-I（Appi）经过网络和分散授权的写与读站 A-WR 在移动数据载体 IM 中进行应用的初始化：IMj 具有 I-I（Appi）。

不必持久激活该授权功能 FA，也可以重新清除该功能，或者中断网络连接或在确定时间或确定数目的初始化之后清除该功能，由此授权的写与读站 A-WR 重新还原为通常的分散写与读站 WR。

在图 4-6 中描述了另外可能的、经过网络 N 可以初始化或者实施的功能。

关于在授权的写与读站 A-WR 上或者在分散的写与读站 WR 上和/或在移动数据载体 IM 上的事件的状态信息 S-I 经过网络告知相应的授权主管，并且在那里例如用于例如使用结算和特许结算。对此例如后面阐述。

作为另外的选择这是可能的，即作为合法用户的授权对于以识别授权单元 ID-AM 的初始化检查其识别 ID-I（图 4、5、14）。

初始化数据 DI 经过网络的安全通信是十分重要的，如此不通过经过网络的数据传输妨碍具有移动数据载体的整个系统的安全。

在经过专用网络 Np 的通信的情况下、例如经过公司网络、提供所希

望的安全。

在经过公共网络传输初始化数据的情况下为此必须以本身已知的方法（密钥和另外的安全要素）保证安全通信。这也适合于经过公共网络和专用网络的组合网络的通信。因此原则上可以应用任意的网络传输初始化数据（比如 LAN、WAN、互联网、内部网和外部网等等）。

也可以经过虚拟的专用网络实现根据本发明的初始化，也就是说使用专用的数据网、公共电信网例如作为公司网，其中密钥和隧道作用原理确保，仅仅授权的用户获得例如经过互联网 IP（互联网协议）、VAP（虚拟私人网络）的访问。

主要是相应保证初始化或者初始化数据的重要通信的可靠性。这不仅关系到经过网络的通信、原则上关于网络的外部安全、而且也关系到在授权系统 A 中内部的安全，该授权系统按照体系定义和应用重要性区分不同体系级 OLi。不仅作为外部而且也作为内部安全必需全部满足与应用或者初始化的重要性一致的安全。对此当然关于网络的外部安全性不小于所希望的内部安全性。

不同的重要级别或者授权级别例如可能是:

象在超市的客户卡上可靠奖金一样附加应用的加载仅仅要求相对低的安全级，因为通过未授权的行为可能的伤害是低的。另一方面例如在 EDV 数据系统中最高保密的使用级的访问权利或完全新的数据载体的初始化和特别是货币价值的记账要求较高的安全级。

图 7 说明了在授权系统 A 的范围内具有多个各具有相应授权单元 AM1、AM2、AM3 的授权主管 HA1、HA2、HA3 的实例，这些授权主管经过网络 N1、N2、N3 发送具有其初始化数据 DI1、DI2、DI3 的其特有的独立应用 App1、App2、App3 给相应分配的授权写与读站 A-WR，在写与读站中相应初始化移动数据载体 IM。对此这些网络可以是不同的，例如 N1 是公共网，N2 是专用网，或二个或多个授权主管也可以使用相同的网络，可是具有其特有的安全规则。当然写与读站必需与授权主管一致，也就是说在该实例中读站 A-WR2 仅仅使用授权主管 HA3，也就是说以相应的应用 App3 分配给该读站 A-WR2，而写与读站 A-WR1 在该实例中被分配或使用所有三个具有其相应应用 App1、App2、App3 的授权主管 HA1、HA2、HA3。类似适合于移动数据载体 IM 的分配，该数据载体也被分配了一个或多个具有相应初始化应用的可能性的授权主

管。

图 8-11 说明了经过多个网络或者经过多级网络（也在统一网络中）初始化、具有多个授权主管 HA 和授权单元 AM 以及具有多个或者不同授权级 OLi 的另外实例。

图 8 指出了具有多个具有授权单元 AM1、AM2 并具有不同应用 App1、App2 的授权主管 HA1、HA2 的实例。相应的初始化数据 DI1、DI2 经过相同网络在同一级中传递给分散授权的写与读站 A-WR 用于在数据载体 IMj 中初始化二个应用 App1、App2。这可以不依赖于授权级 OLi（对于授权主管 HAi 的不同 OLi，授权单元 AMi、应用 Appi）实现。

类似于图 8，图 9 指出了对于多个应用 Appi 的多个授权主管 HA 和授权单元 AM，可是其中经过多级网络 N1、N2 实现在授权的写与读站 A-WR 上的初始化。在相同的网络中或也在不同的网络中形成这些网络级 N1 和 N2。具有授权主管 HA1 的 I-I1 的应用 App1 经过网络级 N1 进入授权主管 HA2 并且没有改变地进一步经过网络级 N2 进入授权的写与读站中。仅仅经过网络级 N2 传递在授权主管 HA2 上的应用 App2。这也不依赖于授权级 OLi。

图 10 指出了类似于图 9 的、具有多个授权主管、应用和网络级的另外实例，其中在此在不同的授权级上描述二个应用，比如应用 App1 在 OLn 上，应用 App2 在 OLn+1 上。该实例在授权主管 HA1 的应用 App1 上表明，在授权主管 HA2 中其也可以补充上 I-I+，如此在数据载体 IMj 中的相应应用与这个应用 App1+一致。

类似于在授权主管中应用的改变或补充在写与读站中、例如按照图 4 在授权的写与读站 A-WR 中也可以用 I-I+改变或补充初始化信息。

图 11 图解指出了在一个具有多级授权或者结构、例如 OLi=OL0 至 OL5、具有在不同授权级上多个授权主管 HA 并具有多个具有独立应用 App1、App2、App3 的独立用户 HA1、HA2、HA3 的授权系统 A 中的结构。最上面的组织级 OL0 与在这样的级一致，在该级上在附属于授权系统 A 的意义上通过不同的授权主管 HAi0 或分配给他们的授权主管 HAi0.1 实现所有写与读站和所有数据载体 IM（例如经过系统数据区 CDF）的基本初始化。系统的授权规则保障在结构级 OL1 上相应独立用户的独立应用 App1、App2、App3 的独立性和相互不可影响性。从紧接着的授权级 OL2 至 OL5 起独立用户本身可以在授权系统 A 的范围内以从属分授

权系统 AS 可以组织并确定其应用。根据阐述的规则在从 OL2 起的这些级上可以形成具有相应授权单元 AM 的授权主管 HA，并且在不同的、局部分布的授权主管 HA 之间可以实现相应的网络连接并经过网络级实现初始化。

对此以授权系统 A 保障，不同授权主管的应用彼此独立并且相互不可影响。在一个数据载体中具有多个独立应用的实例在图 13 中进一步说明。对此首先可以使用无接触的并且无源的识别媒介或者数据载体，其也可以以一定距离与写与读站通信、例如在进口上。

经过网络以在授权系统 A 中的不同体系级并根据不同的安全要求可以实施根据本发明的不同形式的初始化。为此图 12 指出了较高体系级和安全要求的实例，在该实例中以应用新初始化与系统一致的准备好的空移动数据载体。对此通过授权系统 A 的系统数据在系统数据区 CDF 中准备好该数据载体 IM，该数据载体确定并保证对系统 A 附属性，可是该载体在一个为应用准备的应用数据区 ADF 中还不包含应用。在应用数据区 ADF 中以应用 App 的初始化信息 I-I 的新初始化 DI 表明一个第一个上面的初始化级。

图 13 说明了以授权主管 HA3 的初始化数据 DI3 附加初始化新的应用、在此例如应用 App3。

作为另外的实例，图 13 指出了附加于现存应用 App2 借助于相应初始化数据 DI2.2 初始化授权主管 HA2 的应用扩展 App2.2。对于图 13 的数据载体举下面的山区饭馆的实例以在具有多个独立应用 App1、App2、App3 的数据载体中的数据结构并以与授权系统 A 一致的固定数据部分 CDF 对此进行说明。应用 App1 例如是滑雪电梯，应用 App2 是山区饭馆，其想要引入其应用的一个附加扩展 App2.2，并且其把该扩展以相应的初始化 DI2.2 经过网络直接就地、在山区饭馆中通过其写与读站 A-WR 写到顾客的已经现存的滑雪卡或者数据载体 IM 上-不必为此在山谷中把卡带到具有授权媒介的（作为应用 1 的滑雪卡的发行者的）授权写与读站上，这在以前是必须的。

作为另外的实例这个顾客以其滑雪卡在晚上在山谷下面能够以授权主管 HA3 的初始化数据 DI3 重新初始化另外的独立应用 App3、例如进入体育馆，如果在其数据载体上还没有建立这个应用。

作为另外的实施形式图 12 指出了一个移动数据载体，其具有应用微

处理器 AppuP，其包含应用程序数据 I-I-Cod。以如此的、具有集成智能的数据载体可以实现组合的应用，该应用部分包含在写与读站 WR 中，部分包含在数据载体 IM 中，并且允许用户授权 ai 的操作（图 14）。

经过适当安全的网络的根据本发明的初始化可以使完全新的应用和商业模式成为可能，例如通过应用状态信息 S-I 的与初始化联系的商业模式，例如：

1. 对于新初始化的数据载体和新初始化的应用的特许结算：在新数据载体的每个初始化或在数据载体 IM 中的新应用的每个初始化中经过网络在授权主管 HA 中结算特许费。

2. 每个使用的特许结算：如果数据载体在写与读站上使用应用，则对于该使用可以由授权主管 HA（例如一个主机 H）征收特许费。

如果写与读站 WR 经过网络与授权主管 HA 在线连接，则这或者可以连续结算，或者可以周期性实现经过网络的连接。当然使用数据 S-I 可以存储在写与读站 WR 中并且周期性地授权主管 HA 较患并结算。

也可以按应用不仅以持续的网络连接或也仅仅周期性地实现经过网络的根据本发明的初始化和与其联系的通信。对此例如可以通过相应周期性的初始化一再更新时间限制的应用（例如每月）。

图 14 说明了经过网络的可能初始化的不同变体，其中初始化也包含在授权主管 HA、授权的写与读站 A-WR 和识别媒介或者数据载体 IM 之间的初始化通信、或者使用通信和/或识别通信。初始化可以以授权主管 HA 为出发点或也可以由写与读站 A-WR 或由数据载体 IM 的所有者请求初始化。为此按新初始化或者应用的形式使用者授权是必须的，也就是说写与读站的所有者 12 或者数据载体的所有者 13 的同意，该授权例如作为授权单元例如可以是写与读站的所有者 12 的私人数据（aw）或者数据载体的所有者 13 的私人数据（ai）、比如 PIN 代码、生物统计数据等等。类似也适合于通过数据载体在写与读站上的应用的执行。按授权和器适用的形式因此可以

通过写与读站或者其所有者 12 实现用于初始化的使用者授权 aw 或通过数据载体的所有者可以实现用于初始化的使用者授权 ai 或通过附加的识别授权单元 ID-AM 可以实现用于初始化的授权。

一个实施例例如是在作为读卡设备的写与读站上货币卡的存入。在此可以由作为数据载体的货币卡的所有者以其授权、也就是说使用者

授权 ai（例如信用卡号码或 PIN 代码）经过 PC 和互联网存钱。

以根据本发明的方法也可以实施经过网络的多级初始化，例如以多个与授权系统 A 一致的体系分级措施。这说明了分散建立并分配芯片卡作为关于图 11 的数据载体的实例。授权系统 A 的所有者在欧洲例如是具有主位和中心的生产者 HA0，在那里生产空的卡或者数据载体 IM，卡或者数据载体例如包含具有数据区 CDF 的系统基本结构。空的卡经过网络送给作为国家代理机构的子公司 HA0.1、例如在美国，在那里也由作为最上面主管的生产中心 HA0 可以实施另外的基本初始化。子公司 HA0.1 把这些具有独立应用的卡推销给独立的用户，这些用户是授权主管 HA1、HA2、HA3，并且通过应用代码区分其卡，如果子公司 HA0.1 对初始化没有权限，则可以经过在子公司 HA0.1 中的网络通过中心 HA0 初始化这些卡。HA0 和 HA0.1 处于级 OL0。这得出下面的初始化级

HA0→ HA0.1→ HA1

在下一个体系级上通过授权主管 HA1、HA2、HA3（也就是说独立用户）以其所希望的应用 App1、App2、App3 经过另外的结构级再度在分散授权的写与读站 A-WR 上初始化这些卡。通过系统 A 的初始化规则和授权规则和体系分级确保，授权系统 A 的所有者 HA0 可以维持对卡的系统兼容性的支配并且同时对于独立用户 HA1、HA2 等等确保，其从所分配的结构级（例如 OL1）起在其权限的范围内维持对具有其应用的卡的支配。这在结构级 OL1 至 O1n 上得出另外的初始化级，例如

HA1→ HA1.1→ HA1.11→A-WR/IM

具有独立应用的独立用户 HA1、HA2、HA3 等等也处于结构级 OL1。

以给出的实例和实施说明根据本发明的新方法特别可以普遍用于无接触的系统和识别媒介。

在说明书的范围内应用了下面的符号:

N	网络
No	公共网络
Np	专用网络
G1、G2	经过网络的安全通信的安全门
g	安全环境
u	不安全环境

IM	移动数据载体、识别媒介
IMj	初始化的 IM
WR	分散的写与读站
WRk	初始化的 WR
j	涉及 IM
k	涉及 WR
A-WR	分散授权的写与读站
A	授权系统
AS	从属的分授权系统
AM	授权单元
AM-IM	授权的识别媒介
AM-I	授权数据
HA	授权主管，远距离的
H	主计算机
R-A-WR	远距离的授权写与读站
DI	初始化数据
A-I	授权信息
A-I-FA	功能 A-WR 的授权数据
I-I	初始化信息
I-I-Cod	应用程序数据
ID-AM	识别授权单元
ID-I	识别信息
S-I	状态信息
OLi	授权级、结构级
App	应用
AppuP	应用微处理器
CDF	基本数据区、A 的基本结构
ADF	应用数据区
12	WR 的所有者
13	IM 的所有者
aw	WR 的使用者授权
ai	IM 的使用者授权

H0 系统所有者

H0.1 H0 的子公司

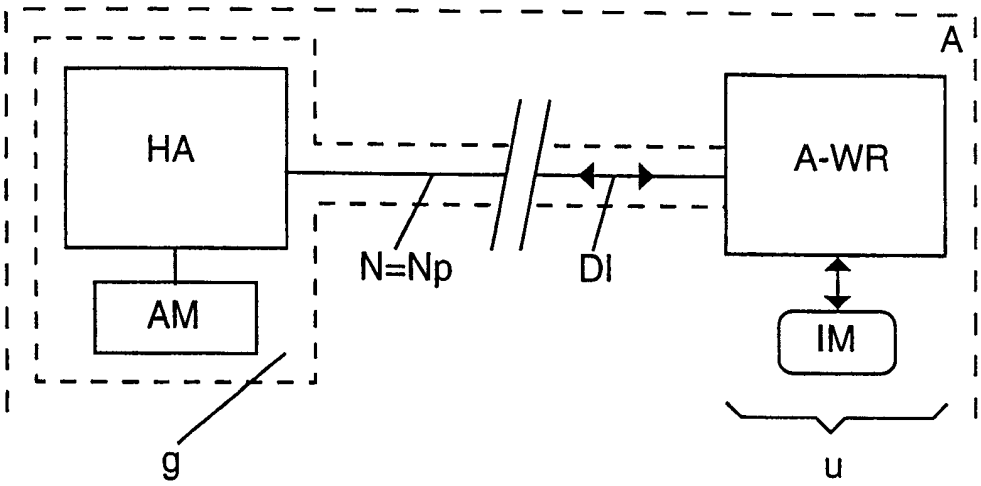


图 1

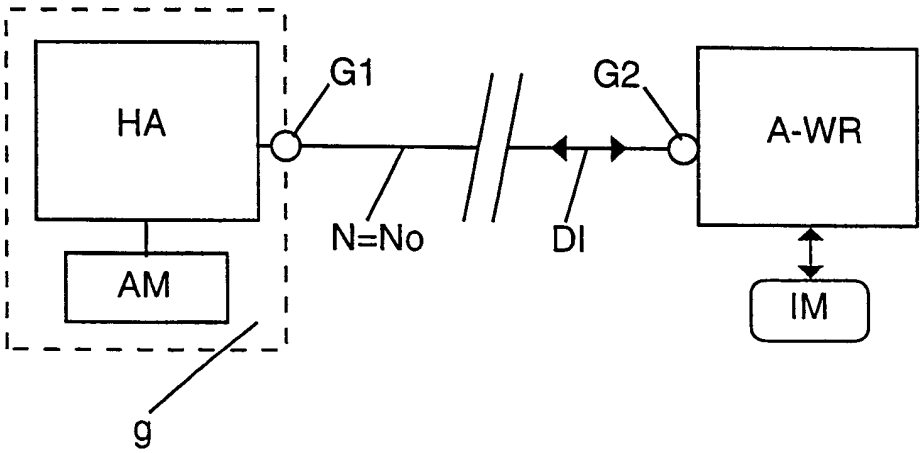


图 2

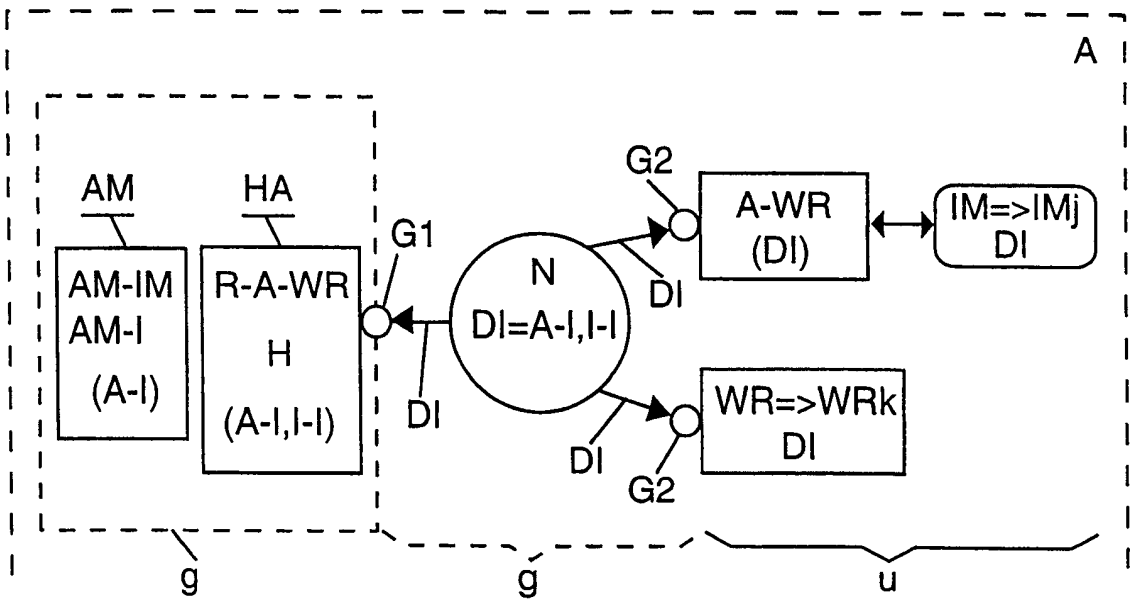

A
AM
HA
AM-IM
AM-I
(A-I)
R-A-WR
H
(A-I,I-I)
G1
DI
N
DI=A-I,I-I
G2
DI
A-WR
(DI)
IM=>IMj
DI
DI
G2
WR=>WRk
DI
g
g
u

图 3

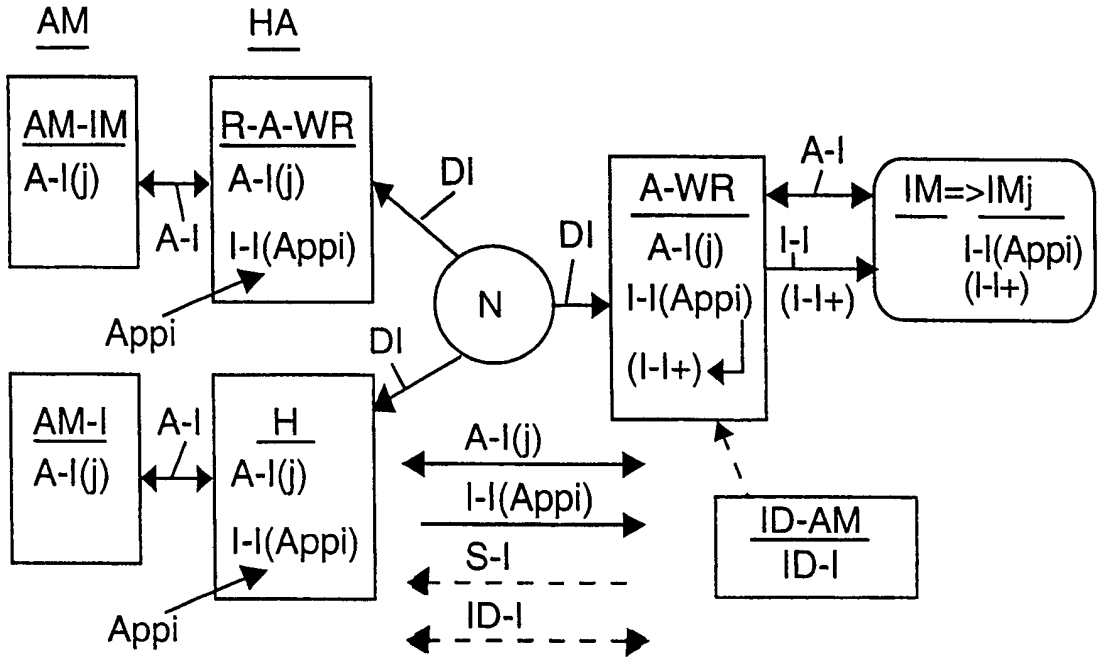

AM
HA
AM-IM
A-I(j)
A-I
R-A-WR
A-I(j)
I-I(Appi)
Appi
DI
N
DI
DI
A-WR
A-I(j)
I-I(Appi)
(I-I+)
A-I
I-I
(I-I+)
IM=>IMj
I-I(Appi)
(I-I+)
AM-I
A-I(j)
A-I
H
A-I(j)
I-I(Appi)
Appi
A-I(j)
I-I(Appi)
S-I
ID-I
ID-AM
ID-I

图 4

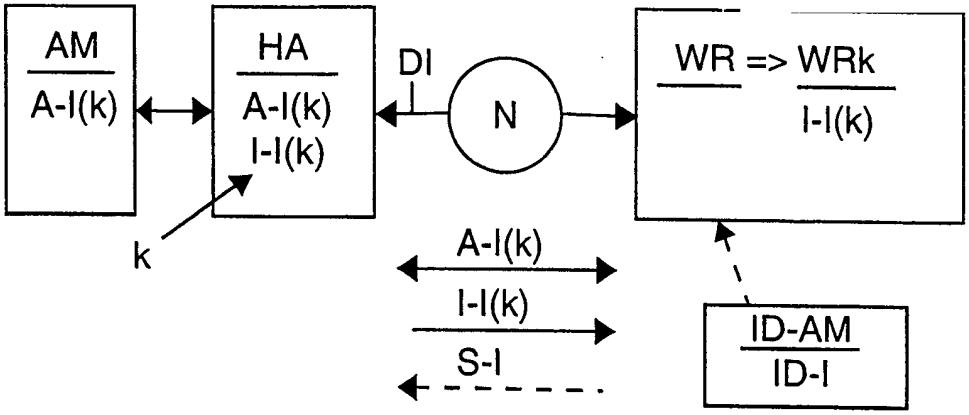

AM
A-I(k)
HA
A-I(k)
I-I(k)
DI
N
WR => WRk
I-I(k)
k
A-I(k)
I-I(k)
S-I
ID-AM
ID-I

图 5

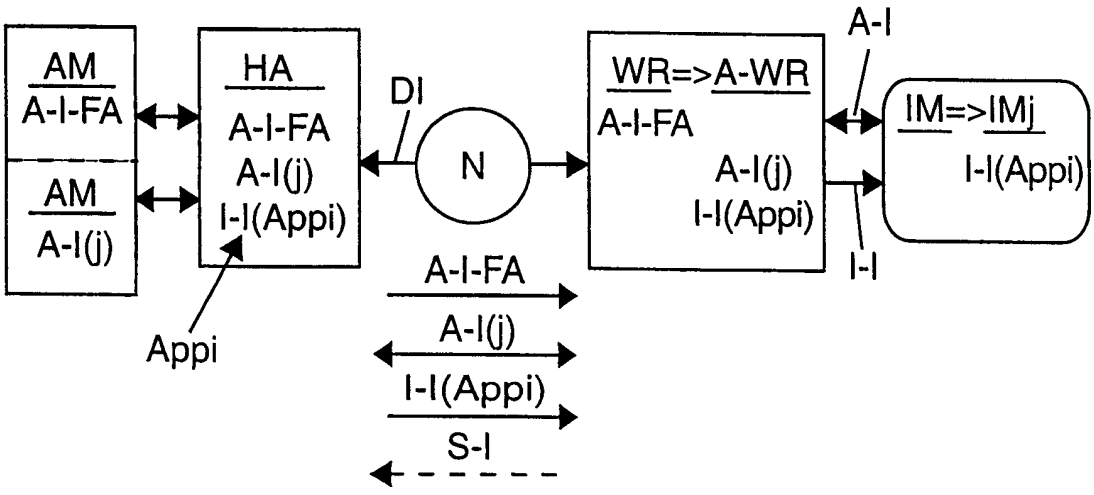

AM
A-I-FA
AM
A-I(j)
HA
A-I-FA
A-I(j)
I-I(Appi)
DI
N
WR=>A-WR
A-I-FA
A-I(j)
I-I(Appi)
A-I
IM=>IMj
I-I(Appi)
I-I
Appi
A-I-FA
A-I(j)
I-I(Appi)
S-I

图 6

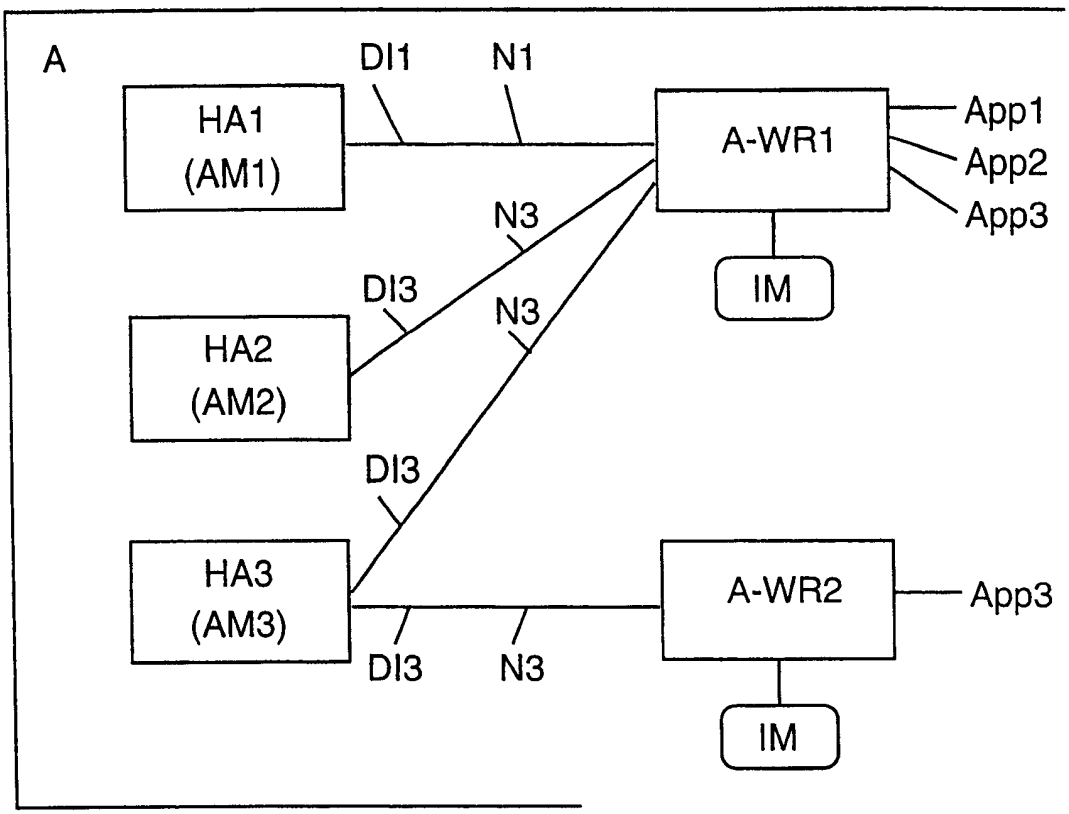

A
DI1
N1
HA1
(AM1)
A-WR1
App1
App2
App3
N3
DI3
IM
HA2
(AM2)
N3
DI3
HA3
(AM3)
A-WR2
App3
DI3
N3
IM

图 7

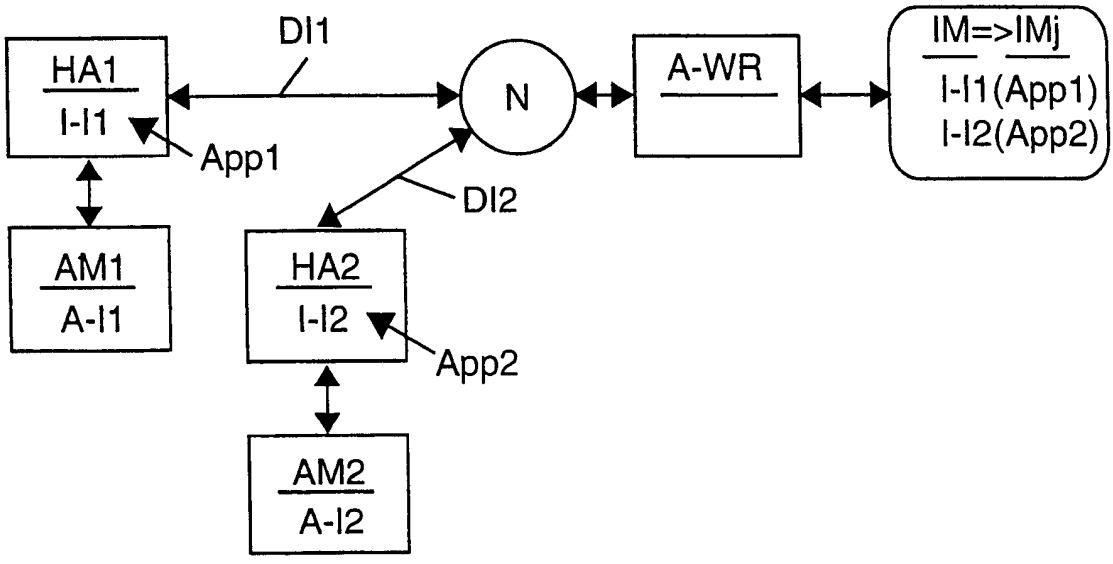

DI1
HA1
I-I1
N
A-WR
IM=>IMj
I-I1(App1)
I-I2(App2)
App1
DI2
AM1
A-I1
HA2
I-I2
App2
AM2
A-I2

图 8

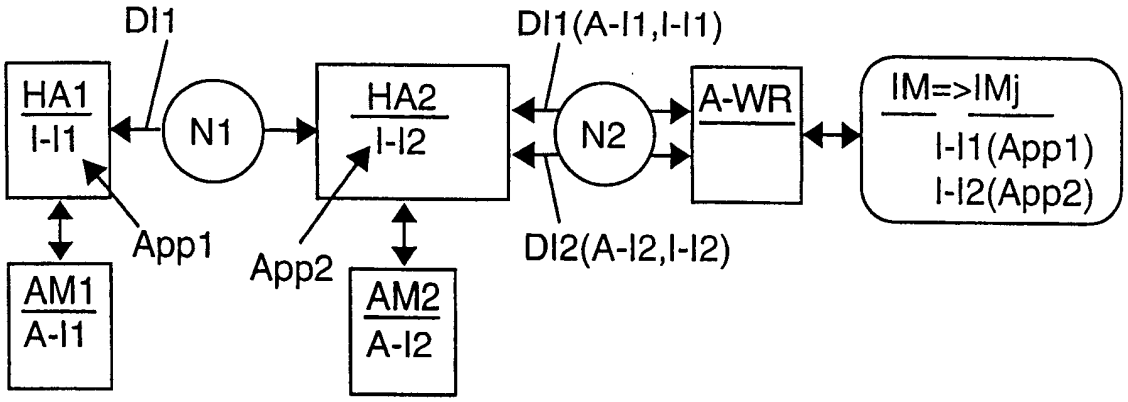

DI1
DI1(A-I1,I-I1)
HA1
I-I1
N1
HA2
I-I2
N2
A-WR
IM=>IMj
I-I1(App1)
I-I2(App2)
App1
App2
DI2(A-I2,I-I2)
AM1
A-I1
AM2
A-I2

图 9

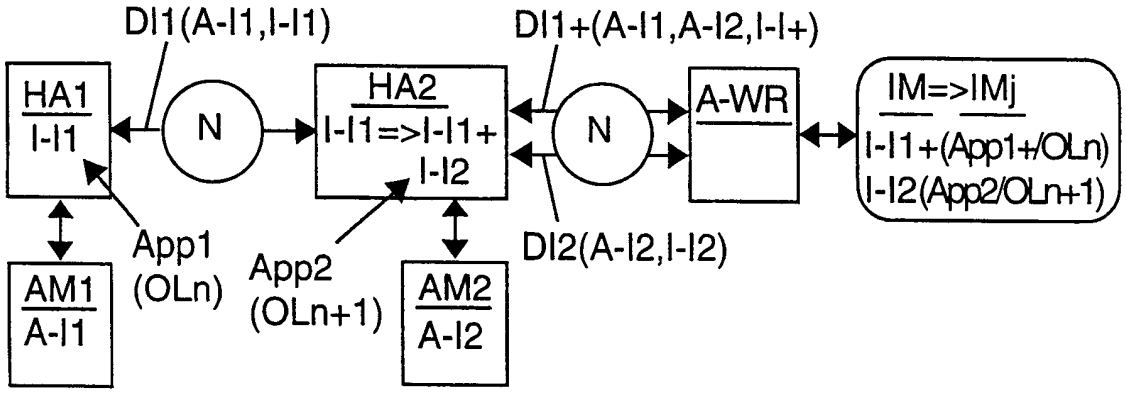

DI1(A-I1,I-I1)
DI1+(A-I1,A-I2,I-I+)
HA1
I-I1
N
HA2
I-I1=>I-I1+
I-I2
N
A-WR
IM=>IMj
I-I1+(App1+/OLn)
I-I2(App2/OLn+1)
App1
(OLn)
App2
(OLn+1)
DI2(A-I2,I-I2)
AM1
A-I1
AM2
A-I2

图 10

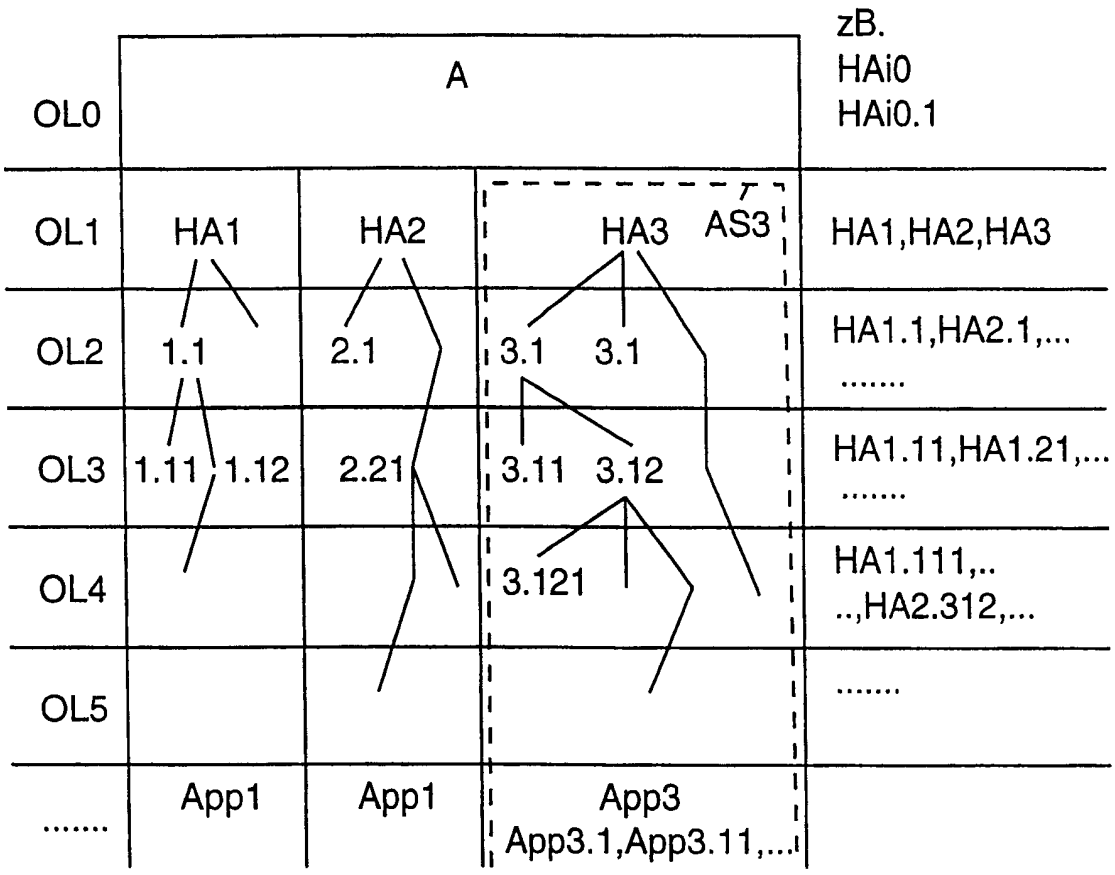

zB.
HAi0
HAi0.1
A
OL0
OL1
HA1
HA2
HA3
AS3
HA1,HA2,HA3
OL2
1.1
2.1
3.1
3.1
HA1.1,HA2.1,...
.....
OL3
1.11
1.12
2.21
3.11
3.12
HA1.11,HA1.21,...
.....
OL4
3.121
HA1.111,..
..,HA2.312,...
OL5
.....
.....
App1
App1
App3
App3.1,App3.11,...

图 11

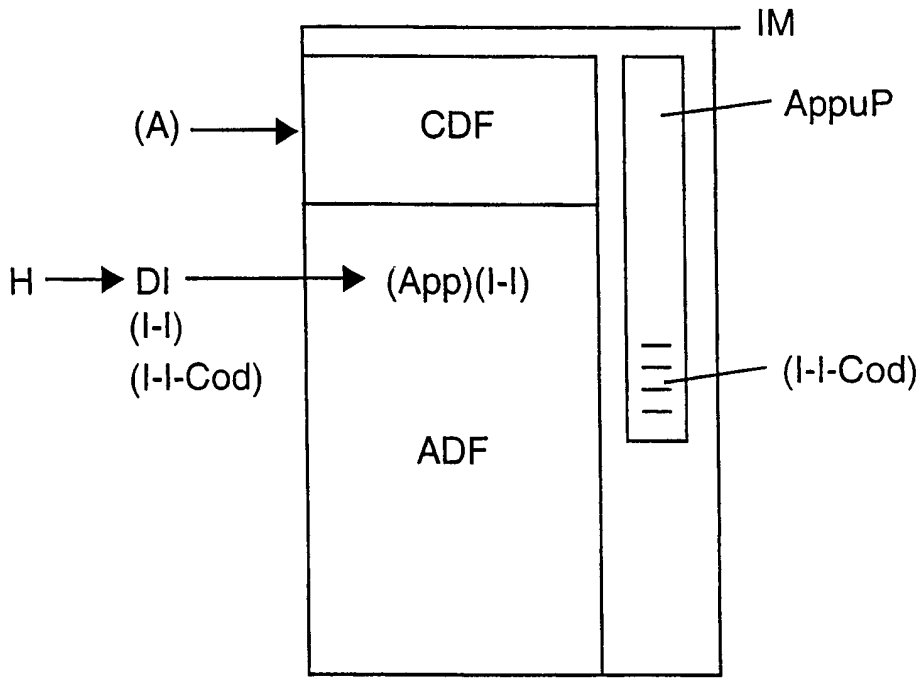

IM
(A)
CDF
AppuP
H
DI
(I-I)
(I-I-Cod)
(App)(I-I)
(I-I-Cod)
ADF

图 12

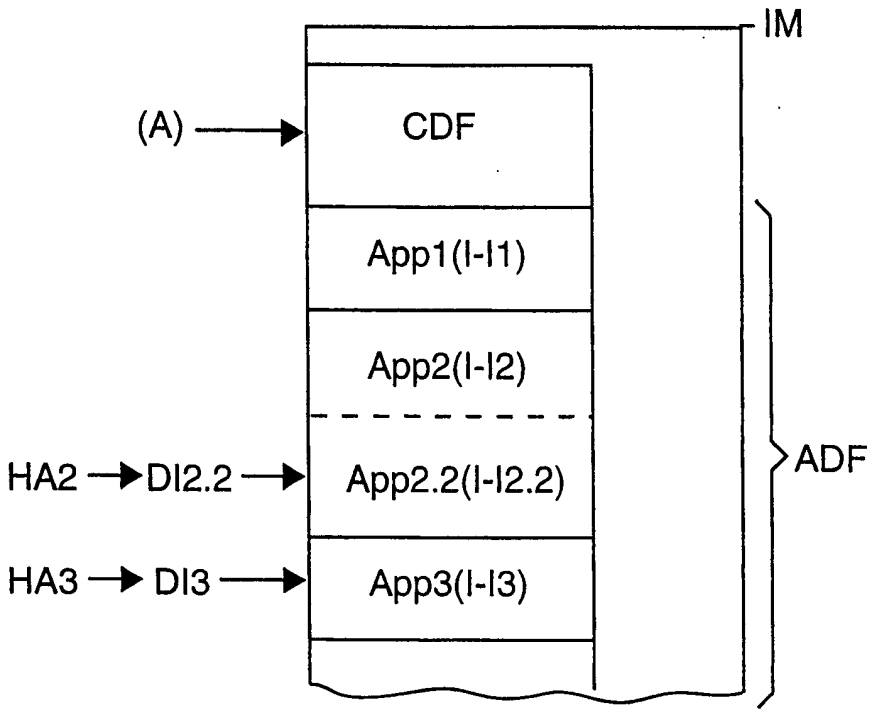

IM
(A)
CDF
App1(I-I1)
App2(I-I2)
HA2
DI2.2
App2.2(I-I2.2)
HA3
DI3
App3(I-I3)
ADF

图 13

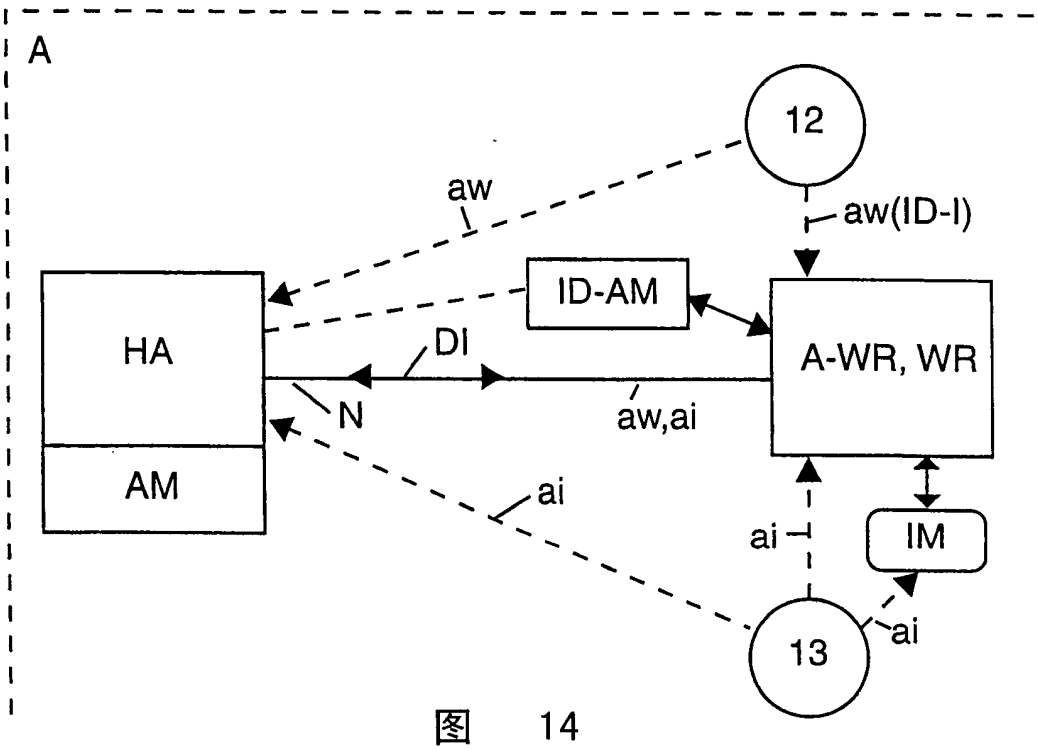

A
12
aw
aw(ID-I)
ID-AM
HA
DI
A-WR, WR
N
aw,ai
AM
ai
ai
IM
13
ai

图 14