(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101073239 B
(45)授权公告日 2012.08.01

(21)申请号 200580037425.9
(22)申请日 2005.09.07
(30)优先权数据
0411625 2004.10.29 FR
(85)PCT申请进入国家阶段日
2007.04.29
(86)PCT申请的申请数据
PCT/FR2005/002233 2005.09.07
(87)PCT申请的公布数据
WO2006/048515 FR 2006.05.11
(73)专利权人 法国电信公司
地址 法国巴黎
(72)发明人 琼-皮埃尔·勒罗滋克
吉勒斯·玛卡瑞欧-拉奇
西瑞·莱克尔克 文森特·巴纳德
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 杜娟
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/22(2006.01)
(56)对比文件
CN 1304101 A,2001.07.18, 说明书第2、3、6-8页.
US 4849614 A,1989.07.18, 全文.
审查员 高菲

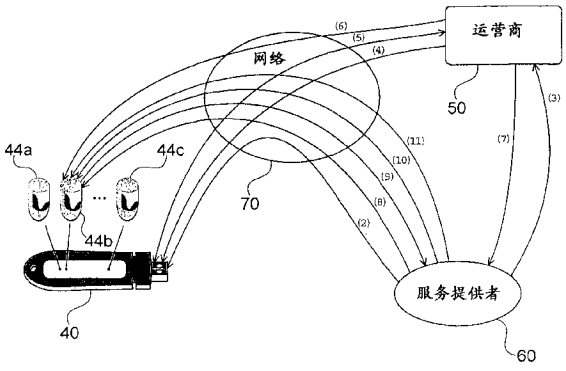
权利要求书 3 页 说明书 10 页 附图 2 页

(54)发明名称

安全信息存储装置与至少一个第三方之间的通信方法和系统、相应实体、装置和第三方

(57)摘要

本发明涉及一种安全信息存储装置(40)和与起交换所述信息的至少一个第三方(60)之间的通信方法。实体(50)执行对于所述装置所属的多个安全信息存储装置的管理。本发明的方法包括下述步骤:实体在设置在装置中并特定于特定第三方的安全容器(44b)中放置(6)安全容器和特定第三方之间的通信授权;实体向特定第三方发送(7)装置标识符、装置地址、安全容器标识符和通信授权;特定第三方尝试使用装置地址、装置标识符、安全容器标识符和通信授权建立(8)与安全容器的通信;以及在接受所述通信之前,装置根据实体先前置于安全容器中的通信授权,检查(9)第三方所传送的通信授权是可以接受的。



CN 101073239 B

1. 一种在多个安全信息存储装置中的安全信息存储装置 (40) 和至少一个与其交换信息的第三方 (60) 之间的通信方法，其中实体 (50) 执行对所述安全信息存储装置所属的多个安全信息存储装置的管理，所述方法包括下述步骤：

- 所述实体在包括在所述安全信息存储装置中并特定于特定第三方的安全容器 (44b) 中直接放置 (6) 所述安全容器和所述特定第三方之间的通信授权；

- 所述实体向所述特定第三方发送 (7)：

(a) 所述安全信息存储装置的标识符；

(b) 所述安全信息存储装置在通信网络中的地址；

(c) 安全容器的标识符；和

(d) 所述通信授权；

- 所述特定第三方尝试只使用以下单元建立 (8) 与所述安全容器的通信：

(a) 所述安全信息存储装置的地址；

(b) 所述安全信息存储装置的标识符；

(c) 所述安全容器的标识符；和

(d) 所述通信授权；

- 在接受所述特定第三方和所述安全容器之间的通信之前，根据所述实体先前放置于所述安全容器中的通信授权，所述安全信息存储装置检查 (9) 所述第三方所传送的通信授权是可接受的。

2. 如权利请求 1 所述的方法，其中还包括在已经接受所述安全容器和所述特定第三方之间的通信之后执行的以下步骤 (10)：

- 所述特定第三方向所述安全容器发送所述安全容器的特定于所述特定第三方的第一访问授权；

- 所述安全容器存储所述第一访问授权，从而随后与所述实体无关地，所述安全容器只授权具有所述第一访问授权的所述特定第三方使用和修改包含在所述安全容器中的信息。

3. 如权利请求 2 所述的方法，其中还包括下述步骤：

- 所述实体向所述安全信息存储装置发送 (31) 请求，请求撤销所述安全容器的特定于所述特定第三方的所述第一访问授权；

- 所述安全信息存储装置撤销 (33) 所述安全容器的特定于所述特定第三方的所述第一访问授权。

4. 如权利请求 3 所述的方法，其中所述撤消第一访问授权的步骤在以下步骤之后执行：

- 在同意撤销所述安全容器的特定于所述特定第三方的第一访问授权之前，所述安全信息存储装置用所述实体先前授予并由所述安全信息存储装置放置的第二访问授权鉴权 (32) 所述实体。

5. 如权利请求 1-4 中任一项所述的方法，其中所述将通信授权放置于安全容器中的步骤在下述步骤之后进行：

- 所述实体向所述安全信息存储装置发送 (4) 将所述通信授权放置于所述安全容器中的请求；

- 在接受将所述通信授权放置在所述安全容器中之前，所述安全信息存储装置用所述

实体先前授予并被放置于所述安全信息存储装置中的访问授权鉴权 (5) 所述实体。

6. 如权利请求 1 所述的方法，其中所述将通信授权放置于安全容器中的步骤在下述步骤之后执行：

- 所述特定第三方 (3) 请求所述实体将所述特定第三方与所述安全容器之间的通信授权放置于所述安全容器中，其中所述特定第三方向所述实体提供所述安全信息存储装置的标识符。

7. 如权利请求 1 所述的方法，其中在已经接受所述安全容器和所述特定第三方之间的通信之后，所述特定第三方将信息发送 (11) 到所述安全容器，从而所述安全容器存储所述信息。

8. 如权利请求 1 所述的方法，其中存储在所述安全容器中的信息属于包含数据和程序的组。

9. 如权利请求 1 所述的方法，其中存储在所述安全容器中的信息被用于实现属于包括以下内容的组的功能：

- 所述特定第三方鉴权所述安全信息存储装置的持有者；
- 电子钱包；
- 授权使用与所述安全信息存储装置协作的设备；
- 维护与所述安全信息存储装置协作的设备；
- 管理与所述安全信息存储装置协作的设备的功能。

10. 如权利请求 1 所述的方法，其中所述特定第三方 (60) 是服务提供者。

11. 如权利请求 1 所述的方法，其中支持所述安全信息存储装置与至少两个第三方之间的通信，其中特定于每个第三方的至少一个容器被包括在所述安全信息存储装置中。

12. 一种在多个安全信息存储装置中的安全信息存储装置和与其交换信息的至少一个第三方之间的通信系统，其中实体执行对所述安全信息存储装置所属于的多个安全信息存储装置的管理，其中：

- 所述实体包括放置单元，用于在包括在所述安全信息存储装置中并特定于特定第三方的安全容器中直接放置所述安全容器和所述特定第三方之间的通信授权；
- 所述实体包括发送单元，用于将所述安全信息存储装置的标识符、所述安全信息存储装置在通信网络中的地址、所述安全容器的标识符和所述通信授权发送到所述特定第三方；
- 所述特定第三方包括尝试单元，用于尝试利用所述安全信息存储装置的地址、所述安全信息存储装置的标识符、所述安全容器的标识符和所述通信授权建立与所述安全容器的通信；
- 所述安全信息存储装置包括检查单元，用于根据所述实体先前放置于所述安全容器中的通信授权，检查所述特定第三方所传送的通信授权是可接受的，从而仅在所述检查单元确定所述第三方所传送的通信授权是可接受的情况下，所述安全信息存储装置才接受所述特定第三方和所述安全容器之间的通信。

13. 一种执行对多个安全信息存储装置的管理的实体，所述实体包括：

- 放置单元，用于在包括在特定装置中并特定于特定第三方的安全容器中直接放置所述安全容器与所述特定第三方之间的通信授权；

- 发送单元，用于向所述特定第三方发送所述特定装置的标识符、所述安全信息存储装置在通信网络中的地址、所述安全容器的标识符和所述通信授权；

从而所述特定第三方尝试只使用所述特定装置的地址、所述特定装置的标识符、所述安全容器的标识符和所述通信授权建立与所述安全容器的通信，并且在接受所述特定第三方和所述安全容器之间的通信之前，所述安全信息存储装置根据实体先前放置于所述安全容器中的通信授权，检查所述第三方所传送的通信授权是可接受的。

14. 一种包括和与其交换信息的至少一个第三方通信的单元的类型的安全信息存储装置，所述安全信息存储装置包括：

- 存储单元，用于在包括在所述安全信息存储装置中并特定于特定第三方的安全容器中存储所述安全容器和所述特定第三方之间的通信授权，所述通信授权由用于管理所述安全信息存储装置所属于的多个安全信息存储装置的实体放置；

- 检查单元，用于根据所述实体先前直接放置于所述安全容器中的通信授权，检查所述特定第三方所传送的通信授权是可接受的，从而仅仅在所述检查单元确定所述第三方所传送的通信授权是可接受的情况下，所述安全信息存储装置才接受所述特定第三方和所述安全容器之间的通信。

15. 一种包括与安全信息存储装置通信的单元的类型的服务器，所述服务器包括：

- 接收单元，用于从执行对所述安全信息存储装置所属的多个安全信息存储装置的管理的实体接收所述安全信息存储装置的标识符、所述安全信息存储装置在通信网络中的地址、所述安全容器的标识符和所述安全容器与所述服务器之间的通信授权；

- 尝试单元，用于只利用所述安全信息存储装置的地址、所述安全信息存储装置的标识符、所述安全容器的标识符和所述通信授权，尝试建立与所述安全容器的通信；

使得在接受所述服务器与所述容器之间的通信之前，所述安全信息存储装置根据所述实体先前直接放置在所述安全容器中的通信授权，检查所述通信授权是可接受的。

安全信息存储装置与至少一个第三方之间的通信方法和系统、相应实体、装置和第三方

技术领域

[0001] 本发明属于安全信息存储装置领域，该装置由管理这些装置的实体（也被称为装置运营商）置于个体（也被称为持有者）的支配之下。

[0002] 更具体地，本发明涉及一种信息安全存储装置（以下称为安全信息存储装置）和至少一个第三方之间的通信方法和系统。

[0003] 例如，安全信息存储装置以智能卡、硬件钥匙(dongles)(例如USB棒:USB stick)或其他任何硬件或软件装置的形式制造。其通常包括至少一个存储信息（数据和/或程序）的安全容器，其中当该容器与装置通信时该容器由第三方加以使用以提供一种或多种功能。

[0004] 为了简化起见，在以下的描述中，术语“实体”被理解为适于该主体在系统中发挥作用的任何部件（硬件和/或软件）。类似地，术语“第三方”被理解为适于该第三方在系统中发挥作用的任何部件（硬件和/或软件）。

[0005] 实体、第三方和安全信息存储装置通过一个或多个通信网络连接在一起。

[0006] 传统地，每个装置可以以不同方式连接到网络，例如直接连接（例如在IP网络的情况下其拥有SOAP服务器）、通过硬件元件连接（诸如手机接口）、软件媒介（在ISO 7816或PKCS驱动器的情况下）。

[0007] 例如，第三方是业务提供者，诸如银行、权力机构、企业等等。

[0008] 可以想到很多功能，其中尤其是下述内容但不局限于下述内容：

[0009] -第三方对持有者的鉴权功能（例如执行半永久性密码类型的强鉴权、一次性密码或OTP、秘密密钥质询或CS或者再次区别地使用密钥对(PKI)的两个密钥）；

[0010] -电子钱包功能；

[0011] -等等。

背景技术

[0012] 现在在具体情形下讨论现有技术及其缺陷，在该情形中，安全信息存储装置是第三方用以鉴权这些装置的持有者的鉴权装置。然而，正如上面已经描述的，与用以向第三方提供包含在安全信息存储装置中的信息的一种或多种功能无关地，可以应用本发明。

[0013] 使用安全访问的应用可以分为两类：

[0014] -使用在线（同步）安全的应用，诸如例如银行卡应用和移动电话(SIM)应用；

[0015] -使用延迟或离线控制安全的应用，诸如例如安全电子邮件应用或电子提交纳税申报单。

[0016] 在这两种情况下所实现的鉴权架构不同，并且相互完全不兼容。在前一种情况下（在线安全），鉴权架构是集中式的。在后一种情况下（离线控制安全），鉴权架构是分布式的。因为本质上只是一个执行该鉴权的集中式部件，所以集中式架构较差地处理来自不同服务提供者的应用的互助性。

[0017] 强鉴权装置（例如具有双鉴权：“我知道什么”PIN码和“我拥有什么”鉴权，智能卡或硬件钥匙）已经在这两类架构下得以实现。然而，不存在这样的情况，即其中一个装置很好地同时参与不同类别的强鉴权（OTP、CS、PKI）并且能够在集中式架构和分布式架构中同等好的作为鉴权部件。相反，因为不可能涵盖所有类型的强鉴权以及所有类型的架构，所以鉴权装置通常被特定化为强类型的鉴权并被特定化为给定架构。

[0018] 换句话说，每个第三方实现适于该第三方并且特定于鉴权方法（OTP、CS、PKI 等）和鉴权基础设施（集中式架构或者分布式架构）的鉴权装置。因此，在不同的第三方之间，投资开发的成本不会互利。因为存在硬件装置并且每个实例需要具有特定学习成本以及因缺少互利而产生的成本的特定记录基础设施，所以鉴权装置的管理是棘手的。

[0019] 为了克服这个问题，已经提出了一些技术解决方案，诸如例如被称为“全球开放平台（Global Open Platform）”（“Global PlatformSmart Card Management System Functional requirements，version4.0”）的技术方案，以便使多个第三方（服务提供者）能够在不链接到管理卡（尤其是它们的供应和发行）的实体（也被称为运营商）的情况下使用同一智能卡类型鉴权装置。

[0020] 然而，因为在预定制阶段末使用可信赖的第三方以使第三方服务提供者独立于运营商，因此该现有技术不是最优的。

[0021] 另外，因为如果可能的话，卡发行者必须提前已知将置于卡中的应用，所以该现有技术是极其苛刻的。在卡的服务寿命期间可以下载新的应用。然而，卡的整个映像必须被重载。

发明内容

[0022] 本发明的目的尤其是克服现有技术的这些不同缺点。

[0023] 更具体地，本发明的一个目的是，在至少一个实施例中提供安全信息存储装置和至少一个第三方之间的通信的技术，使得第三方能够在包括在装置中的安全容器中并且特定于该第三方的装置的服务寿命期间安全地存放和/或减少和/或修改信息。

[0024] 因此，本发明的目的尤其在于但是并不局限于，在装置的服务寿命期间支持第三方对包括在装置中并分配给第三方的安全容器执行第一定制操作（其代替传统的工厂内（in-plant）预定制操作）或后定制操作（如果传统的工厂内预定制操作或根据本发明的第一定制操作已经被执行）。

[0025] 在至少一个实施例中，本发明的目的还在于提供一种该类型的技术，使得多个第三方分别具有包括在同一装置（装置的互助性）的特定安全容器；并且每个第三方可以与其他第三方无关地存放和/或使用和/或修改特定于其的安全容器中信息。尤其但不局限于，每个第三方应该能够与其他第三方无关地定制其安全容器的内容以及包括在同一装置中的其他安全容器的内容。

[0026] 在至少一个实施例中，本发明的目标也在于提供一种该类型的技术，以由装置管理实体以及由其他第三方（如果装置包括分配给不同第三方的多个安全容器）禁止对安全容器的访问。

[0027] 在至少一个实施例中，本发明的另一个目标在于提供一种该类型的技术，其中装置管理实体（运营商）作为装置持有者在其装置有问题的情况（停止支付、替换等等）下

可以求助于的负责执行者、以及作为持有者的权利和隐私的保证者（保护持有者的数据不受到第三方的非授权访问或甚至非法访问）。

[0028] 本发明的另一个目标在于，如果存储在安全容器中的信息被第三方用于对装置持有者鉴权，则提供一种该类型的技术，该技术与鉴权方法无关并且不指示集中式或者分布式架构模型。

[0029] 根据本发明，通过安全信息存储装置和与其交换所述信息的至少一个第三方之间的通信方法实现这些不同目标以及以下将看出的目标，其中实体对所述装置所属的多个安全信息存储装置执行管理。根据本发明，该方法包括下述步骤：

[0030] - 实体将安全容器和特定第三方之间通信的授权置于包括在所述装置中并且特定于该特定第三方的安全容器中；

[0031] - 实体向该特定第三方发送装置标识符、装置在通信网络中的地址、安全容器标识符和所述通信授权；

[0032] - 该特定第三方尝试使用装置地址、装置标识符、安全容器标识符和通信授权与安全容器建立通信；

[0033] - 在接受该特定第三方与安全容器之间的通信之前，装置根据实体先前放置于安全容器中的通信授权，检查该第三方所传送的通信授权是否可以接受。

[0034] 因此，本发明的一般原则包括，在装置已经移交给持有者之后，将安全容器与第三方之间的通信授权放置在包含在该装置中的安全容器中，该通信授权决定装置后续是否接受该安全容器和该第三方之间的通信。

[0035] 安全容器和第三方之间的通信旨在使第三方能够放置、使用或修 改安全容器中的信息。因此，本发明使得第三方能够在装置已经被转交给持有者（例如通过下载）之后执行包含在装置中的安全容器的第一定制操作或后定制操作。

[0036] 注意下述内容是重要的，即实体在将通信授权放置到安全容器中以确保安全容器仅由已经将其分配给的第三方使用的机制中具有关键作用。

[0037] 在本发明的一个优选实施例中，该方法进一步包括下述步骤，该步骤在已经接受安全容器和特定第三方之间的通信之后被执行：

[0038] - 特定第三方向安全容器发送对于安全容器的特定于该特定第三方的第一访问授权；

[0039] - 安全容器存储所述第一访问授权，使得只有具有第一访问授权的特定第三方随后被安全容器授权与实体无关地使用和修改安全容器中所包含的信息。

[0040] 因此，在安全容器已经存储对特定第三方的第一特定访问授权之后，包含在安全容器中的信息只处于该第三方的控制之下，并且对于实体和其他第三方（如果该装置在多个第三方中是互利的）是不可访问的。于是，该特定第三方可以直接访问其安全容器，而不受到实体干预，并且因此不重新执行上述机制（基于安全容器中实体存放第三方和安全容器之间的通信授权）。

[0041] 换句话说，在本发明的这个优选实施例中，装置的与管理相关的方面（并且尤其是该装置的发行）和关于通过包含在安全容器中的信息执行的功能的方面分离。实际上，是实体（运营商）执行装置的管理，是第三方执行上述功能。

[0042] 该分离使得实体对装置的鉴权架构独立于第三方为了对装置持有者鉴权所执行

的鉴权方法。换句话说，在这种情况下，本发明的解决方案不指定架构模型（集中式或分布式），并且不与对于所有第三方公共的鉴权方法（OTP、CS、PKI.....）相关。

[0043] 有利地，该方法进一步包括下述步骤：

[0044] -实体向装置发送请求，请求撤销安全容器的特定于该特定第三 方的所述第一访问授权；

[0045] -装置撤销安全容器的特定于该特定第三方的第一访问授权。

[0046] 因此，实体不知道特定于第三方的第一访问授权，但能够撤销它，例如基于装置持有者的请求（在丢失、被盗等情况下）或者基于第三方的请求（在装置持有者撤销的情况下或者在实体和第三方之间的合同没有续定的情况下）。

[0047] 有利地，第一访问鉴权的撤销步骤在以下步骤之后：在同意撤销安全容器的特定于该特定第三方的第一访问授权之前，装置用预先由实体授予并且由装置放置的第二访问授权鉴权实体。

[0048] 根据一个有利特性，将通信授权放置于安全容器的步骤在下述步骤之后：

[0049] -实体向装置发送将所述通信授权放置于安全容器中的请求；

[0050] -在接受将通信授权放置在安全装置中之前，装置用预先由实体授予并且放置被置于装置中的第三访问鉴权鉴权实体。

[0051] 必须注意，特定于实体的第二和第三访问授权可以是同一或相同的。

[0052] 在本发明的一个有利实施例中，将通信授权放置于安全容器中的步骤在下述步骤之后执行：特定第三方请求实体将该特定第三方和安全容器之间的通信授权置于安全容器中，该特定第三方将装置标识符提供给实体。

[0053] 有利地，在已经接受安全容器和特定第三方之间的通信之后，该特定第三方将信息发送到安全容器，以便安全容器存储该信息。

[0054] 优选地，存储在安全容器中的信息属于包括数据和程序的组。

[0055] 有利地，存储在安全容器中的信息可以被用于完成属于包括以下内容的组的功能：

[0056] -特定第三方对装置持有者的鉴权；

[0057] -电子钱包；

[0058] -授权使用装置与其协作的设备；

[0059] -装置与其协作的设备的维护；

[0060] -装置与其协作的设备的功能管理。

[0061] 该列表决不是穷举的。

[0062] 有利地，特定第三方是服务提供者。

[0063] 在本发明的一个特定实施例中，本发明实现了装置和至少两个第三方之间的通信，特定于每个第三方的至少一个容器被包括在该装置中。

[0064] 因此，在该特定实施例中，装置包括多个被分配给不同第三方的安全容器，其中每个第三方至少一个容器（装置的互助性）。每个第三方可以存放和/或使用和/或修改特定于其的安全容器中的信息，而与其他第三方无关（并且在优选情况下，即该第三方已经将特定于其的第一访问授权放置于它的容器中，甚至与实体无关）。

[0065] 本发明还涉及安全信息存储装置和与其交换所述信息的至少一个第三方之间的

通信系统，其中实体执行对于所述装置所属于的多个安全信息存储装置的管理，其特征在于：

[0066] －实体包括放置单元，用于将安全容器和特定第三方之间的通信授权放置于包括在所述装置中并且特定于给所述特定第三方的安全容器中；

[0067] －实体包括发送单元，用于向该特定第三方发送装置标识符、装置在通信网络中的地址、安全容器标识符和所述通信授权；

[0068] －特定第三方包括尝试单元，用于尝试利用装置地址、装置标识符、安全容器标识符和通信授权建立与安全容器的通信；

[0069] －装置包括检查单元，用于根据由实体预先放置于安全容器中的通信授权，检查该特定第三方所传送的通信授权是可接受的，从而仅在检查单元确定第三方所传送的通信授权是可接受的情况下，装置才接受该特定第三方和安全容器之间的通信。

[0070] 本发明还涉及执行对所述装置所属于的多个安全信息存储装置的管理的实体，该实体包括：

[0071] －放置单元，用于将安全容器和特定第三方之间的通信授权放置于包括在特定装置中并且特定于所述特定第三方的安全容器中；

[0072] －发送单元，用于向该特定第三方发送该特定装置的标识符、该装置在通信网络中的地址、安全容器的标识符和所述通信授权；

[0073] 从而该特定第三方可以利用该特定装置的地址、该特定装置的标识符、安全容器的标识符和通信授权建立与安全容器的通信，并且在接受该特定第三方和安全容器之间的通信之前，该装置根据实体先前放置于安全容器中的通信授权，检查第三方所传送的通信授权是可接受的。

[0074] 本发明还涉及该类型的安全信息存储装置，包括用于与与其交换所述信息的至少一个第三方通信的单元，该装置包括：

[0075] －存储单元，用于将安全容器和特定第三方之间的通信授权存储在包括在所述装置中并且特定于所述特定第三方的安全容器中，所述通信授权由用于管理所述装置所属于的多个安全信息存储装置的实体放置；

[0076] －检查单元，用于根据实体先前放置于安全容器中的通信授权，检查该特定第三方所传送的通信授权是可接受的，从而仅在检查单元确定该第三方所传送的通信授权是可接受的情况下，该装置才接受该特定第三方和安全容器之间的通信。

[0077] 本发明还涉及该类型的第三方，包括用于与安全信息存储装置通信的单元，该第三方包括：

[0078] －接收单元，用于从对所述装置所属的多个安全信息存储装置执行管理的实体接收装置标识符、装置在通信网络中的地址、安全容器标识符和安全容器与所述第三方之间的通信授权；

[0079] －尝试单元，用于尝试利用装置地址、装置标识符、安全容器标识符和通信授权建立与安全容器的通信。

[0080] 从而，在接受第三方和安全容器之间的通信之前，装置可以根据实体先前放置于安全容器中的通信授权，检查通信授权是可接受的。

附图说明

[0081] 本发明的其他特征和优点在以下以非限制性的指示所提供的对 本发明的优选实施例的描述和附图中得以显现，其中：

[0082] - 附图 1 和 3 分别示出根据本发明一个特定实施例的在安全信息存储装置和第三方之间的通信的不同阶段，即：

[0083] ✧附图 1 显示了第三方访问包括在装置中的安全容器的初始化阶段；

[0084] ✧附图 2 显示了第三方访问该安全容器的阶段；

[0085] ✧附图 3 显示了先前分配给第三方的特定访问授权的撤销阶段；以及

[0086] - 附图 4 示出了本发明的安全存储装置的一个特定实施例的功能性模块图。

具体实施方式

[0087] 在这里以下所描述的本发明的特定实施例中，本发明的系统包括：

[0088] - 多个安全信息存储装置，例如硬件钥匙，其中每个安全装置包括一个或多个安全容器；

[0089] - 这些安全信息存储装置被委托给的多个持有者；

[0090] - 实体，这里以下被称为运营商，其执行安全信息存储装置的管理（包括分配）；

[0091] - 一个或多个第三方，例如服务提供者（诸如银行、管理机关、企业等等）；

[0092] - 一个或多个标识提供者或 IDP，其可能与运营商是相同的；

[0093] - 一个或多个通信网络，用于连接实体（运营商）、第三方（服务提供者）、安全信息存储装置（硬件钥匙）和标识提供者 (IDP)。

[0094] 运营商是配置本发明系统并装备持有者的行动者。因为每个装置最开始由适于它的鉴权单元分别特性化，所以运营商能够识别和鉴权该装置。运营商向这些服务提供者出租或销售其安全容器（包含在其委托给持有者的装置中）。例如，运营商连接到不同的通过持有者鉴权委托的标识提供者 (IDP)，例如偏差标识提供者 (offset identity provider)。

[0095] 正如这里以下详细阐释的，运营商具有特定于其的访问授权（例如密码意义上的秘密），并使其能够管理委托给持有者的装置的安全内容。利用特定于其的访问授权，运营商可以尤其授权特定安全容器接受另一特定于特定访问提供者的访问授权。其也可以在不需要知道访问提供者的情况下撤销特定于该提供者的访问授权。总之，运营商对于持有者和服务提供者保留整个系统的安全度、密封质量 (sealedquality) 和可靠度的保证人。

[0096] 持有者是具有运营商所委托的装置的个体。持有者使用该装置和包括在其中的每个安全容器，就像它们是许多单独装置。例如，可通过应用程序编程接口 API、诸如 ISO 7816、PKCS 或其他类型接口访问安全容器。

[0097] 包括在装置中的安全容器拥有只能由有权访问安全容器的主体读取或利用。在持有者的控制下，这些权利由运营商委派。包含在安全容器中的信息例如是数据和程序，例如在多应用环境中的非专用文档、证书或小程序或小型应用程序 (applet)，尤其包括但不局限于鉴权。

[0098] 服务提供者是与运营商订立合同以能够使用由运营商所部署的装置的行动者。运营商使服务提供者能够计划：持有者在其装置上（并且更具体地在该装置的一个安全容器中）接收支持服务提供者和持有者之间直接关系的信息（数据和 / 或程序）。在特定于鉴

权的应用中，装置因此对于一个或多个服务提供者保证“签名承载(signaturebearing)”功能。

[0099] 正如这里以下详细解释的，每个服务提供者本身有资格生成特定于其的访问授权（例如以秘密的形式），这在其已经被运营商鉴权之后为其提供对安全容器的直接访问（即独立于运营商的访问）。

[0100] 服务提供者必须实现其自己的记录作为分配给该服务提供者的安全容器的使用者的持有者的机制。该机制尤其保证持有者同意服务提供者使用其装置的安全容器。

[0101] 服务提供者由委托给持有者的装置中的标识符标识。当服务提供者已经获得被标识提供者（IDP）鉴权的装置的网络标识时，服务提供者可以访问该装置。

[0102] 标识提供者能够鉴权给定网络地址上的安全信息存储装置。鉴权方法对于装置是无关紧要的。标识提供者响应于鉴权请求提供对于服务提供者可以是匿名的也可以不是匿名的指针（pointer）。

[0103] 在这里以下的描述中，以示例的方式假设安全信息存储装置是硬件钥匙（例如USB棒）。然而显然，本发明也可以以该装置的任何其他类型的实施例、硬件或软件中（例如以智能卡的形式）被应用。

[0104] 参考附图1，提供根据本发明的用于安全信息存储装置（硬件钥匙）和第三方（服务提供者）之间通信的方法的一个特定实施例的第一阶段。该第一阶段是服务提供者访问包括在装置中的安全容器的初始化阶段。

[0105] 在第一步骤中（未示出），最终用户（终端）具有包括几个安全容器（在所示示例中为三个）44a、44b 和 44c 的硬件钥匙 40。该硬件钥匙 40 使标识符成为必要，可能与该硬件钥匙在通信网络 70 中的地址相同。

[0106] 在第二步骤 (2) 中，试图与一个安全容器（例如 44b）通信的服务提供者 60 识别硬件钥匙 40。此处假设硬件钥匙的持有者是该服务提供者的顾客。

[0107] 在第三步骤 (3) 中，服务提供者 60 寻址管理硬件钥匙的运营商 50 和包含在硬件钥匙中的安全容器，以请求运营商 50 放置与特定安全容器（例如标记为 44b 的安全容器）的通信授权。服务提供者向运营商至少发送硬件钥匙的标识符（例如印刷在顾客的硬件钥匙上的序列号，或者标识提供者 (IDP) 的匿名“句柄 (handle)”，或者如果选择由PCI证书或匿名鉴权证书执行硬件钥匙的识别，则诸如可以在硬件钥匙的标识证书中读取的标识号）。

[0108] 在可选步骤中（未示出）（选项a），服务提供者 60 向运营商 50 询问对于该顾客被分配给服务提供者的安全内容 44b 的标识符。因 为在另一实现（选项B）中，只要建立绑定运营商和服务提供者的合同，运营商就将该信息提供给服务提供者，因此该步骤是可选的。

[0109] 在第四步骤 (4) 中，运营商 50 向硬件钥匙 44 请求将信息放置于有关安全容器 44b 中。

[0110] 在第五步骤 (5) 中，硬件钥匙 40 借助于在硬件钥匙被商业销售之前定制硬件钥匙时已经被放置的特定于运营商的访问（秘密）授权鉴权运营商 50。

[0111] 在第六步骤中，运营商 50 在安全容器 44b 中放置该安全容器与服务提供者 60 之间的通信授权。

[0112] 在第七步骤 (7) 中，运营商 50 在网络 70 上至少发送下述内容给服务提供者 60：相关硬件钥匙 40 的标识符，该硬件钥匙的网络地址、安全容器 44b 的标识符和上述通信授

权。

[0113] 在第八步骤 (8) 中，因为服务提供者知道硬件钥匙的标识符和网络地址以及安全容器 44b 的标识符，并且给出上述通信授权，所以服务提供者 60 直接寻址硬件钥匙 40 的安全容器 44b。

[0114] 在第九步骤 (9) 中，硬件钥匙 40 在接受安全容器 44b 和服务提供者 60 之间的通信之前执行对上述通信授权的先校验。更具体地，例如由硬件钥匙的操作系统执行该验证，并且在肯定结果的情况下，该硬件钥匙请求安全容器的操作系统接受服务提供者将通过上述通信为其提供的秘密（参见附图 4 的描述）。

[0115] 在第十步骤 (10) 中，服务提供者 60 向安全容器 44b 发送其自身的对该安全容器的访问授权，以便其可以被存储在其中以便随后使用（即，在服务提供者期望与安全容器 44b 再次通信的任意时候，参见附图 2 的描述）。以这种方式，访问提供者变得独立于运营商。运营商不知道这个特定于服务提供者的授权。因此，在不知道服务提供者的情况下，运营商不能使用该授权。相反，其能够撤销授权（参见附图 3 的描述）。

[0116] 在第十一步骤 (11) 中，服务提供者 60 现在可以将数据和程序放置在安全容器 44b 中，安全容器将处于该服务提供者的唯一控制之 下并且对于其他服务提供者以及运营商 50 是不可访问的。

[0117] 因此，运营商确保了安全容器的密封质量。只有将信息放置在安全容器中的服务提供者能够访问该信息，并且不知道使用同一硬件钥匙的其他安全容器的服务提供者的标识和置于其中的信息的属性。

[0118] 现在参考附图 4，提出本发明的安全存储装置的一个特定实施例。

[0119] 在该实施例中，装置 40 包括操作系统 (OS)41、存储区域 42 和三个安全容器 44a、44b 和 44c。本发明当然不局限于安全容器的该特定数量。

[0120] 存储区域 42 尤其存储特定于运营商的访问授权 43（参见上述有关附图 1 所示初始化阶段的第五步骤 (5) 的讨论）。

[0121] 每个安全容器 44a、44b 或 44c 包括操作系统 (OS)441a、441b 或 441c，以及存储区域 442a、442b 或者 442c。每个安全容器的操作系统 (OS) 也可以被看作信息处理堆栈的较低层。每个存储区域 442a、442b 或 442c 尤其存储特定于服务提供者的访问授权 443a、443b 或 443c（参见上述有关附图 1 所示初始化阶段的第十步骤 (10) 的讨论）。

[0122] 更具体地，装置 40 的操作系统（本地程序 (OS)）41 例如具有类似于操作系统本身的作为诸如 CP/CMS（也被称为 VM/370）的虚拟操作系统的介质的功能或还类似于应用服务器的功能的功能。因此，其可以在完全虚拟的、分离的并且隔离的存储空间和最终系统中根据不同安全容器进行不同虚拟机的操作。换句话说，每个虚拟机是“安全容器”功能的支持。其例如借助于 API ISO7816 或 PKCS 标准控制对永久性或易失性数据的访问以及程序的执行。

[0123] 装置 40 的操作系统 41 还负责与服务提供者、运营商和标识提供者 (IDP) 之间的关系。每个安全容器知晓与服务提供者共享的秘密。在装置 40 的操作系统 41 的控制下下载秘密。该操作系统 41 可以允许安全容器接受与服务提供者共享的新的秘密，而不需要因此知晓位于虚拟机中的该秘密，并且通过装置 40 的构建，不知道该装置的操作系统 41。

[0124] 每个安全容器的工作存储空间对于另一安全容器是完全可访问 的。每个虚拟机

因此不知道其他虚拟机的存在，并且期望装置的所有潜在优点。如该情况可以如此的，可能保存仅仅将由一个安全容器使用的存储资源。

[0125] 每个安全容器可以安全地从 / 向外部接受或提供数据（“空中 (overthe air)”数据），因为在该容器和该容器的受托者（服务提供者）之间存在共享秘密。根据安全容器的受托者（服务提供者）的进度，在装置的操作系统的控制下，该秘密可以由运营商改变。例如在装置中存在数据库，以具有有关被授权使用安全容器的服务提供者的标识的信息。对于每个安全容器，该数据库包括包含服务提供者标识符和与服务提供者共享的秘密的数据对 (doublet)。为了能够更新用于访问安全容器的秘密，还存在借助于另一共享秘密的运营商平台的鉴权。该秘密在制造时被植入受保护区域。为了安全容器的受托者可以与该容器通信，应当存在可以通过运营商鉴权系统获得的装置标识符。

[0126] 现在参考附图 2，提出本发明方法的该特定实施例的第二阶段，即服务提供者 60 访问已经分配给它的安全容器 44b 的阶段。

[0127] 假设此处上面参考附图 1 所描述的第一阶段已经实现，并且因此安全容器 44b 尤其存储特定于服务提供者 60 的访问授权。

[0128] 在第一步骤 (21) 中，服务提供者 60 请求硬件钥匙 40 的持有者用标识提供者 (IDP)80 标识自己，以便得知硬件钥匙的网络地址和持有者标识符之间的对应关系。

[0129] 必须注意，存在两种服务提供者 60 访问硬件钥匙 40 的方法：服务提供者能够与硬件钥匙直接在线对话，或者服务提供者请求运营商（其自己或者借助于 IDP) 鉴权硬件钥匙。第二方法（其是上面描述并在附图 2 中阐释的方法）的效果是其通过发送使其总是能够从特定硬件钥匙获得相同响应的随机常量、或者通过获得对在读取模式下自由发现其中循环信息 (recurrent information) 的安全容器的读取访问，防止与运营商无关的服务提供者获得硬件钥匙的鉴权形式并因此获得持有者的鉴权形式。这里，目标在于保护与运营商达成协议的服务提供者的商业利益。

[0130] 在第二步骤 (22) 中，如果服务提供者 60 具有与标识提供者 (IDP)80 的关系，则该标识提供者建立鉴权。

[0131] 在第三步骤 (23) 中，如果鉴权是有效的，则标识提供者 (IDP) 通知服务提供者在该网络地址上存在被标识的持有者。无论采用什么鉴权方法 (PKI、OTP、秘密密钥质询等等），都是这样。向服务提供者传输该信息可以直接由“偏带通道 (off-channel)”实现，或者由浏览器上的 cookie 完成，即对（持有者的标识符，硬件钥匙的网络地址）。服务提供者因此通过标识符得知硬件钥匙，并且通过网络地址知道如何对其寻址。

[0132] 在第四步骤 (24)，服务提供者 60 因此可以直接寻址硬件钥匙的安全容器 404B，以请求其运行，例如借助于 API ISO 7816 或 PKCS 标准。该请求由硬件钥匙 40 的操作系统 (OS) 接收，其中操作系统将进行查询以找出哪个安全容器是请求的目的容器。

[0133] 以下介绍第五步骤 (25)。硬件钥匙 40 侧的问题在于获得保护以阻止对安全容器的非法访问企图。安全容器的操作系统被委托以该控制。为此，其必须知道服务提供者 60 的标识。如果该标识是一个被授权访问该安全容器 40b 的服务提供者，则操作系统或安全容器还必须知道该服务提供者 60 具有对安全容器 44b 的合法访问（该信息由运营商通过硬件钥匙的操作系统给出），并且知道其鉴权服务提供者。这例如通过秘密密钥质查实现。为了能够进行该质询，硬件钥匙应当能够通过网络向服务提供者发送请求。正如可能的情

况，硬件钥匙可以具有其自己的网络接口或者可以调用外部接口。根据该鉴权成功还是失败，服务提供者 60 可以与安全容器 44b 通信或者不可以与安全容器 44b 通信。

[0134] 在第六步骤 (26) 中，如果通信是可能的，则其他交换可以借助于经典协议完成，诸如 ISO 7816、PKCS 或其他协议。安全容器 44b 的操作系统通过硬件钥匙 40 的操作系统支持该协议，以向服务提供者 60 提供具有作为其选中协议中行动者的单元的经验。

[0135] 现在参考附图 3，提出本发明方法的该特定实施例的第三阶段，即撤销硬件钥匙 40 的特定安全容器 44b 的先前分配给服务提供者 60（第三方）的访问授权。

[0136] 假设，这里上面参考附图 1 所描述的第一阶段已经被执行，并且因此安全容器 44b 尤其存储特定于服务提供者 60 的访问授权。

[0137] 在第一步骤 (31)，运营商 50 向硬件钥匙 40 请求撤销该安全容器 44b 的特定于该服务提供者 60 的该访问授权。

[0138] 在第二步骤 (32)，硬件钥匙 40 借助于特定于运营商并且在其被商业分售之前在定制硬件钥匙时已经被放置的访问（秘密）授权鉴权运营商 50。

[0139] 在第三步骤 (33)，硬件钥匙的操作系统 (OS) 将该请求转发到相关安全容器 44b，该安全容器执行所请求的撤销。

[0140] 尽管这里以上已经参考有限数目的实施例描述了本发明，但是本领域技术人员通过阅读说明书将理解，可以想到其他实施例，而不偏离本发明范围。因此，本发明的范围仅仅由权利请求书进行限制。

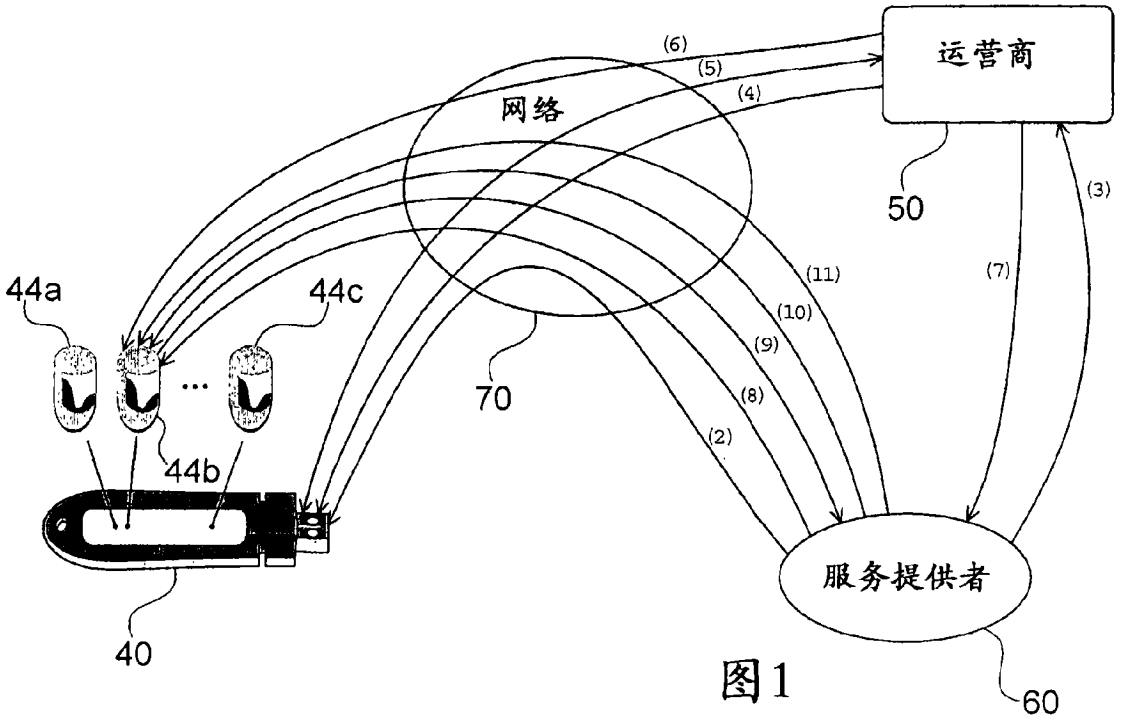

运营商
网络
(6)
(5)
(4)
(3)
50
(11)
(10)
(9)
(8)
(2)
(7)
44a
44c
44b
70
服务提供者
40
60

图1

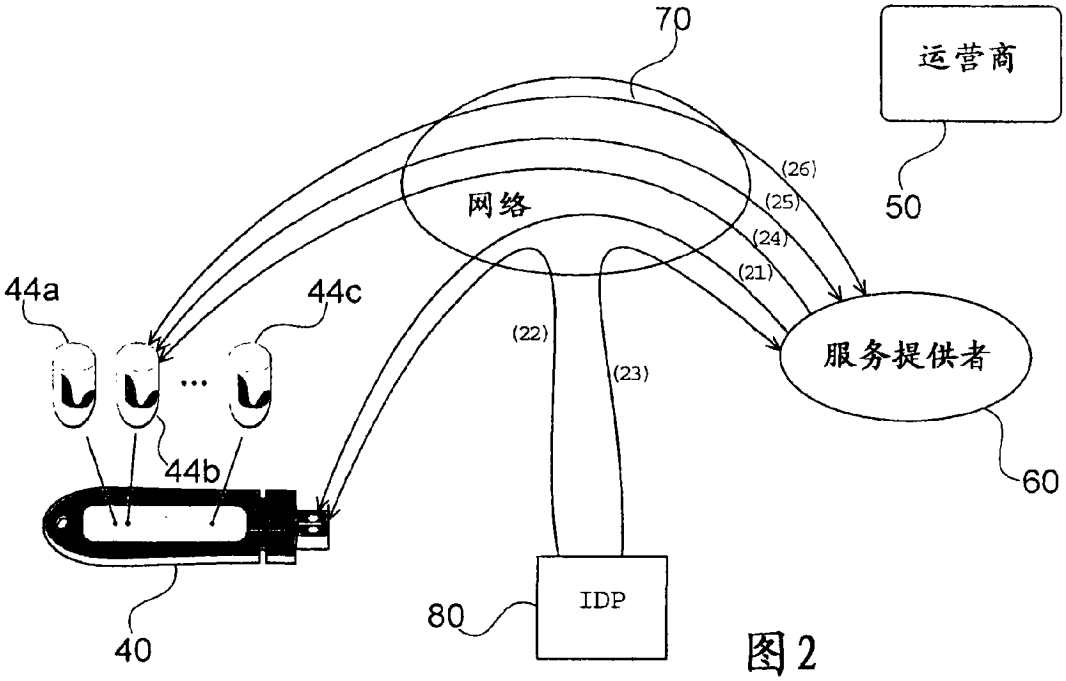

70
运营商
网络
(26)
(25)
(24)
(21)
50
44a
44c
(22)
(23)
服务提供者
44b
60
IDP
80
40

图2

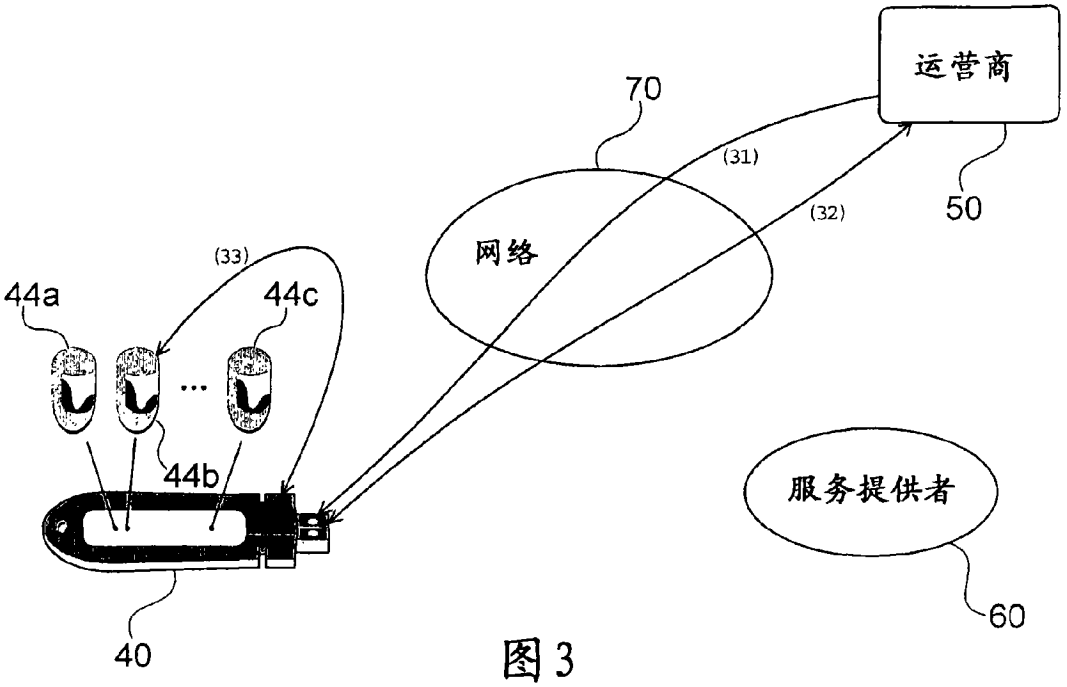

运营商
70
(31)
50
(32)
网络
(33)
44a
44c
44b
服务提供者
60
40

图 3

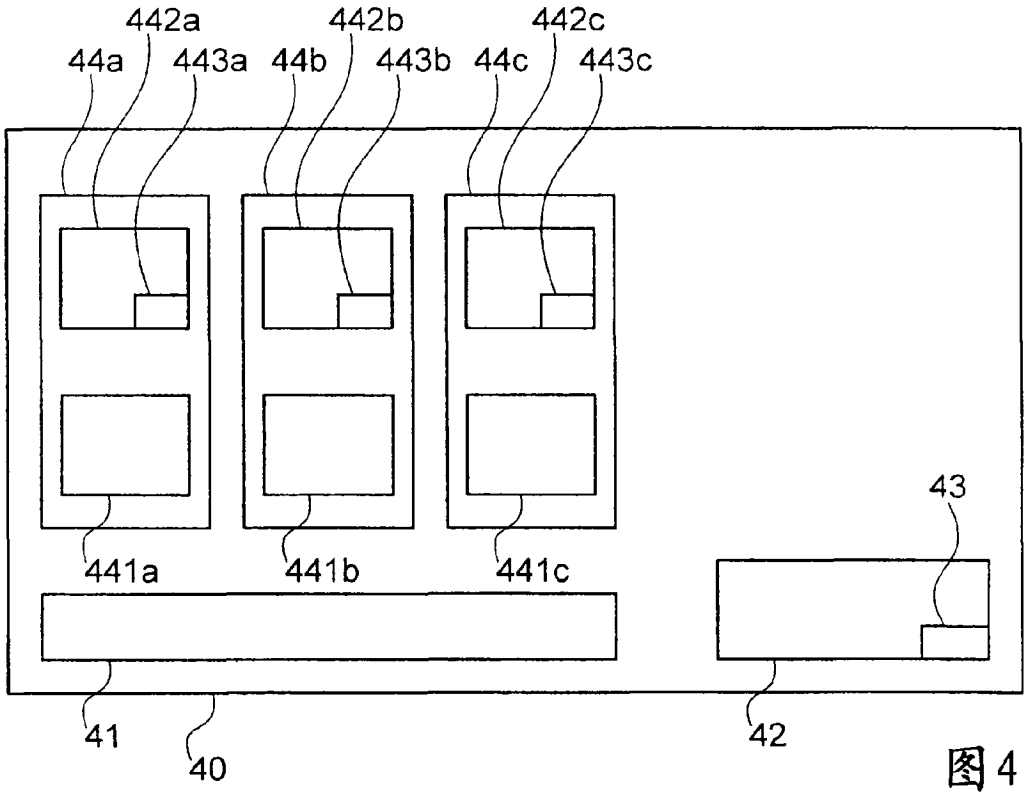

442a
442b
442c
44a
443a
44b
443b
44c
443c
43
441a
441b
441c
41
40
42

图 4