[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G07F 7/10 (2006.01)

[12] 发明专利说明书

专利号 ZL 200480008830.3

[45] 授权公告日 2008 年 9 月 10 日

[11] 授权公告号 CN 100418110C

[22] 申请日 2004.3.30
[21] 申请号 200480008830.3
[30] 优先权
[32] 2003. 3.31 [33] EP [31] 03100837.8
[86] 国际申请 PCT/IB2004/050358 2004.3.30
[87] 国际公布 WO2004/088603 英 2004.10.14
[85] 进入国家阶段日期 2005.9.29
[73] 专利权人 NXP 股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 H·普日比拉
[56] 参考文献
EP0935214A2 1999.8.11
US6233683B1 2001.5.15
WO98/09257A1 1998.3.5
US2002/89890A1 2002.7.11
US2002/40438A1 2002.4.4
US6317832B1 2001.11.13
EP1004992A2 2000.5.31
US6385723B1 2002.5.7
审查员 高 磊
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 王波波

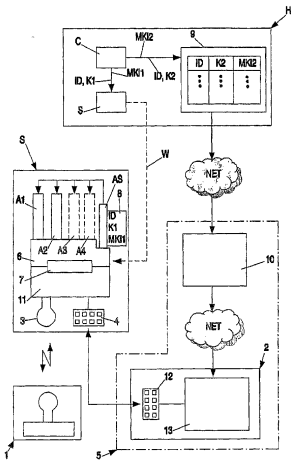
权利要求书 4 页 说明书 11 页 附图 2 页

[54] 发明名称

授予智能卡修改权利的方法

[57] 摘要

修改设备(5)被设计成修改由数据载体(S)运行的应用程序(A1，A2，A3，A4)，其中第一密钥信息项(K1)被存储在数据载体(S)中，并且关联的第二密钥信息项(K2)被存储在修改设备中。



1. 一种授权方法（E），用于授予修改设备（5）修改数据载体（S）中的应用程序的修改权利，其中执行以下步骤:

在数据载体（S）制造过程中，为每个数据载体（S）生成第一密钥信息项（K1）和关联的第二密钥信息项（K2），所述数据载体（S）由数据载体识别信息项（ID）识别;

通过输出数据载体识别信息项（ID）和关联的第二密钥信息项（K2）到修改设备（5）来授予对由数据载体识别信息项（ID）识别的数据载体（S）的修改权利;

检查存储在数据载体（S）中的第一密钥信息项（K1）和在数据载体（S）中被修改设备（5）输出到数据载体（S）的第二密钥信息项（K2）的关联，并且如果检查结果是肯定的:

允许修改设备（5）去修改数据载体（S）中的应用程序（A1，A2，A3，A4）。

2. 如权利要求 1 所述的授权方法（E），其中修改权利给予安装和／或更新和／或删除数据载体（S）中的应用程序（A1，A2，A3，A4）的权利。

3. 如权利要求 1 所述的授权方法（E），其中修改权利只给予修改数据载体（S）中的特定的应用程序（A1，A2，A3，A4）的权利。

4. 如权利要求 1 所述的授权方法（E），其中修改权利只给予安装数据载体（S）中要求预定最大量存储空间的应用程序（A1，A2，A3，A4）的权利。

5. 如权利要求 1 所述的授权方法（E），其中数据载体识别信息项（ID）识别一组数据载体（S）。

6. 如权利要求 1 所述的授权方法（E），其中修改权利还确定在数据载体（S）中待修改的应用程序（A1，A2，A3，A4）对存储区域和数据载体（S）的接口（3，4，11）的访问权利。

7. 如权利要求 1 所述的授权方法（E），其中执行以下进一步的步骤:

为由数据载体识别信息项（ID）识别的一个或多个数据载体（S）生成第一主密钥信息项（MKI1）和关联的第二主密钥信息项（MKI2），其中修改数据载体（S）中的访问权利和／或在数据载体（S）和修改设备（5）中生成另外的密钥信息项只可能利用存储在数据载体（S）中的第一主密钥信息项（MKI1）和存储在修改设备（5）中的第二主密钥信息项（MKI2）。

8. 如权利要求 7 所述的授权方法（E），其中第一主密钥信息项（MKI1）和关联的第二主密钥信息项（MKI2）只可能修改数据载体（S）中的特定应用程序（A1，A2，A3，A4）的访问权利和／或在数据载体（S）和修改设备（5）中生成另外的密钥信息项，以便修改特定的应用程序（A1，A2，A3，A4）。

9. 如权利要求 1 所述的授权方法（E），其中仅当确定待修改的应用程序（A1，A2，A3，A4）的特定属性时，才允许数据载体（S）的修改设备（5）修改数据载体（S）中的应用程序（A1，A2，A3，A4）。

10. 用于运行至少一个应用程序（A1，A2，A3，A4）的数据载体（S），具有

至少一个接口（3，4，11），用于无接触和／或接触传送信息项，并具有

计算机装置（6），用于运行至少一个应用程序（A1，A2，A3，A4），其中处理经由接口（3，4，11）传递的信息项或存储在数据载体（S）中的信息项，并具有

存储装置（8），用于存储第一密钥信息项和识别数据载体（S）的关联的数据载体识别信息项（ID），并具有

检查装置（6，AS），用于检查修改设备（5）经由接口（3，4，11）修改数据载体（S）中的应用程序（A1，A2，A3，A4）的修改权利，其中将检查装置（6，AS）设计来检查存储在存储装置（8）中的第一密钥信息项（K1）和被修改设备（5）输出到数据载体（S）的第二密钥信息项（K2）的关联，并具有

修改装置（6），在检查装置（6，AS）确认修改设备（5）的修改权利之后，被设计成使修改设备（5）能够修改数据载体（S）中的应用

程序（A1，A2，A3，A4）。

11. 如权利要求 10 所述的数据载体（S），其中检查装置（6，AS）被设计成确认限制的修改权利，该限制的修改权利只给予安装和／或更新和／或删除数据载体（S）中的应用程序（A1，A2，A3，A4）的权利。

12. 如权利要求 10 所述的数据载体（S），其中检查装置（6，AS）被设计成确认限制的修改权利，该限制的修改权利只给予修改数据载体（S）中的特定的应用程序（A1，A2，A3，A4）的权利。

13. 如权利要求 10 所述的数据载体（S），其中检查装置（6，AS）被设计成确认限制的修改权利，该限制的修改权利只给予安装数据载体（S）中要求预定最大量存储空间的应用程序（A1，A2，A3，A4）的权利。

14. 如权利要求 10 所述的数据载体（S），其中检查装置（6，AS）被设计成确认一个修改权利，该修改权利确定在数据载体（S）中待修改的应用程序（A1，A2，A3，A4）对存储装置（7）的存储区域和数据载体（S）的接口（3，4，11）的访问权利。

15. 如权利要求 10 所述的数据载体（S），其中计算机装置（6）被设计成运行由 Java 小应用程序形成的应用程序（A1，A2，A3，A4）。

16. 用于修改数据载体（S）中的应用程序（A1，A2，A3，A4）的修改设备（5），具有

至少一个接口（12），用于无接触和／或接触地将信息项传送到由数据载体识别信息项（ID）识别的数据载体（S），并具有

存储装置，用于存储识别数据载体（S）的至少一个数据载体识别信息项（ID），以及关联的第二密钥信息项（K2），并具有

计算机装置（13），用于经由接口（12）修改数据载体（S）中的应用程序（A1，A2，A3，A4），其中在与由存储的数据载体识别信息项（ID）识别的数据载体（S）通信的过程中，通过传递与这个数据载体识别信息项（ID）关联的第二密钥信息项（K2），将修改设备（5）的修改权利输出到数据载体（S），因此在数据载体（S）确认修改权利之后，修改设备（5）被授权并被设计来修改数据载体（S）中的应用程序（A1，A2，A3，A4）。

17. 如权利要求 16 所述的修改设备（5），其中修改设备（5）由包含所述存储装置的操作者计算机（10）和通过数据网络（NET）与操作者计算机（10）连接的读取设备（2）形成，读取设备（2）包括所述至少一个接口（12）和修改设备（5）的计算机装置（13）的至少一部分。

授予智能卡修改权利的方法

技术领域

本发明涉及授予修改设备修改权利的授权方法，以便修改数据载体中的应用程序。

本发明还涉及用于运行至少一个应用程序的数据载体。

本发明还涉及用于修改数据载体中的应用程序的修改设备。

背景技术

在文献 EP0935214A 中公开这样的数据载体，在这种情况下，由智能卡形成数据载体。将数据载体的计算机装置设计来运行多个应用程序或软件程序。已知的数据载体可例如运行金融应用程序，运行该金融应用程序可能使得货币数目被加载到提款机上的数据载体并用于在商店里支付。另外，已知的数据载体能运行病人应用程序、运行病人应用程序可能使得病人数据被医生或医药保险公司读取和修正。许多其它的应用对于本领域技术人员来说是已知的，比如信用卡应用或停车场票单应用。

当使用运行信用卡应用程序的这种类型的数据载体，在信用卡终端处进行支付时，那么为了验证数据载体的有效性，已知为信任中心的信用卡终端电子地发送识别数据载体的数据载体识别信息项。信任中心检查数据载体识别信息项的有效性，并且如果检查的结果是肯定的，将有效信息项电子地输出到信用卡终端。

在已知的数据载体中，应用程序在制造数据载体的时候或在它们在被发布给数据载体的用户之前的任何情况下就被安装或存储在数据载体的存储装置中。如果多个应用程序已经安装在数据载体上，必须保证应用程序以明显相互分离的形式运行，并且保证防止对可能是保密或安全有关的数据（例如货币数目、病人数据）的不期望的可逆访问。在 EP0935214A 中公开了适当的预防措施。然而，当修改在数据载体中运

行或将要运行的应用程序时，还必须保证由数据载体运行的其他应用程序不受到不利影响。另外，必须保证只有授权修改应用程序的人或设备才获得对数据载体的存储装置的访问。另外，在安装应用程序之前，必须毫无疑问地验证数据载体的身份，以便应用程序不存储在由第三方使用的不同数据载体上。

发明内容

本发明的一个目的是提供第一段中提到的类型的授权方法，第二段中提到的类型的数据载体和第三段中提到的类型的修改设备，其中已经采取了上述的预防措施。为了实现本目的，在这样一种授权方法中提供下列的方法步骤:

在数据载体制造过程中，为每个数据载体生成第一密钥信息项和关联的第二密钥信息项，数据载体由数据载体识别信息项识别;

通过输出数据载体识别信息项和关联的第二密钥信息项到修改设备来授予对由数据载体识别信息项识别的数据载体的修改权利;

检查存储在数据载体中的第一密钥信息项和在数据载体中被修改设备输出到数据载体的第二密钥信息项的关联，并且如果检查结果是肯定的;

允许修改设备去修改数据载体中的应用程序.

为实现以上目的，这种数据载体的特征在于下列特征：用于运行至少一个应用程序的计算机装置，在其中处理经由接口通信的信息项或存储在数据载体中的信息项，并具有

存储装置，用于存储第一密钥信息项和识别数据载体的关联的数据载体识别信息项，并具有

检查装置，用于检查修改设备经由接口修改数据载体中的应用程序的修改权利，其中将检查装置设计来检查存储在存储装置中的第一密钥信息项和被修改设备输出到数据载体的第二密钥信息项的关联，并具有

修改装置，在检查装置确认修改设备的修改权利之后，被设计成使修改设备能够修改数据载体中的应用程序。

为了实现以上目的，这种修改设备的特征在于以下特征：至少一个

接口，用于无接触和／或接触地将信息项传送到由数据载体识别信息项识别的数据载体，并具有

存储装置，用于存储识别数据载体的至少一个数据载体识别信息项，以及关联的第二密钥信息项，并具有

计算机装置，用于经由接口修改数据载体中的应用程序，其中在与由存储的数据载体识别信息项识别的数据载体通信的过程中，通过传递与这个数据载体识别信息项关联的第二密钥信息项，将修改设备的修改权利输出到数据载体，因此在数据载体确认修改权利之后，修改设备被授权并被设计来修改数据载体中的应用程序。

借助本发明的这些特征，实现了下列情形，即为由数据载体识别信息项识别的数据载体，生成分别关联的第一和第二密钥信息项。第一密钥信息项和数据载体识别信息项被存储在数据载体中，并且第二密钥信息项和数据载体识别信息项被输出到修改设备。结果，修改设备获得修改权利来修改由数据载体识别信息项识别的数据载体或多个数据载体的一个或多个应用程序。在这种情况下，修改数据载体的应用程序意味着在数据载体上初始化安装应用程序，更新已经安装在数据载体上的应用程序（例如新版本），以及从数据载体删除应用程序。

修改设备可因此有利地在数据载体已经被发布给用户时修改数据载体的应用程序，对于该数据载体需要通过获得数据载体识别信息项和关联的第二密钥信息项获取修改权利。获取修改权利可与为支付修改权利的费用联系在一起，由此获得一个有趣的商业方法。在该情况下尤其有利的是，修改数据载体的应用程序能发生在数据载体与修改设备进行通信的过程中，而不是必须与信任中心联系以确认修改权利。

根据权利要求 2 和 11 的方法，获得的优点在于，修改权利可例如授权修改设备只安装新的应用程序，却不能更新或删除应用程序。同样，修改权利可授权修改设备只删除应用程序，而与此同时适合于在数据载体中的存储装置的存储区域中安装新的应用程序，作为删除的结果该存储区域变为空闲。如果新版本的应用程序将被安装以替换所有数据载体上已经发布给用户的旧版本的应用程序，那么可由应用程序（金融应用程序）的操作者将对应的修改权利发布给修改设备（取款机）的操作者。

有可能得到大量这样的有益用途，同时反过来可能获取在各种情况下与服务器连接的修改权利，由此获得了一种有趣的商业方法。

根据权利要求 3 和 12 的方法，获得的优点在于，借助修改权利，也就是说借助数据载体识别信息项和关联的第二密钥信息项，识别可修改的应用程序。对于运行两个应用程序的数据载体，为两个应用程序的每一个授予上述不同的修改权利（安装、更新、删除）因此可能是有利的。

根据权利要求 4 和 13 的方法，获得的优点在于，可授予修改权利来修改在数据载体中安装新的应用程序，而该新的应用程序不要求大于在存储装置中最大量的存储空间（例如 1 千比特）。结果，获得了一种十分有趣的商业模型，其中可以在已经发布给用户的数据载体中出售存储空间。因此，信用卡制造商可以在他的信用卡的存储装置中为将来的应用程序保留存储空间，并且当大量信用卡已经被发布给用户时，以对应的修改权利的方式将该存储空间出售给一个或多个公司，以便也能运行它们的使用信用卡的应用程序（例如，客户忠诚卡、电子停车场票）。

根据权利要求 5 的方法，获得的优点在于，使用由仅仅一个数据载体识别信息项和仅仅一个第二密钥信息项形成的仅仅一个修改权利，可在一组数据载体中修改应用程序，其中数据载体都由相同的数据载体识别信息项识别。

根据权利要求 6 和 14 的方法，获得的优点在于，修改权利识别待修改的应用程序的特定访问权利。例如，修改权利可被授予给信用卡，该修改权利授权安装只能使用接触接口而不能使用非接触接口的应用程序并排他地允许读取特定存储区域中的权利，该特定存储区域对信用卡的所有应用程序来说是公共的。

根据权利要求 7 的方法，获得的优点在于，借助存储在数据载体的与第一主密钥信息项关联的第二主密钥信息项，修改权利可为由数据载体运行的一些或所有应用程序修改访问接口或存储区域的访问权利。同样，通过使用主密钥信息项，可生成新的第一密钥信息项，并将其存储在数据载体中，并且可生成新的第二密钥信息项，并将其存储在修改设备中，以便能够修改另一个应用程序。

根据权利要求 8 的方法，获得的优点在于，通过使用主密钥信息项，

能将修改访问权利和／或生成密钥信息项限制在仅一个特定应用程序。

根据权利要求 9 的方法，获得的优点在于，除了由数据载体检查密钥信息，在允许修改应用程序之前，检查待被修改的应用程序的特定属性。在该情况下，例如应用程序操作者能在应用程序中存储第三密钥信息项，在数据载体修改应用程序之前检查其正确性。

根据权利要求 15 的方法，获得的优点在于，特别有利地由数据载体运行所知的 Java 小应用程序。

根据权利要求 16 的方法，获得的优点在于，可由通过网络（例如互联网、公司网络、电话网络等）相互连接的应用程序的操作者的操作者计算机和读取设备（例如取款机）形成修改设备。通过这种方式，可能得到大量的有利用途。

附图说明

参考附图中所示的实施例的实例来进一步描述本发明，但本发明不限于此。

图 1 显示了一个数据载体，其中修改设备安装另一个应用程序。

图 2 显示了用于在图 1 所示的数据载体中修改应用程序的修改方法。

具体实施方式

图 1 示意地显示了用于智能卡 S 的制造过程 H，智能卡 S 形成数据载体，并在完成制造过程 H 之后被设计用于与终端 1 无接触通信并用于与读取设备 2 进行接触通信。在制造过程 H 期间，集成电路被合并到塑料卡中并与天线 3 连接，以便进行无接触通信，并连接到接点排 4，以便进行接触通信。这样的制造过程 H 早已被得知并且因此不在这里做详细讨论。

图 2 显示了授权方法 E，用于授予修改设备 5 修改权利以便修改智能卡 S 中的应用程序。在这种情况下，应用程序被理解为表示智能卡 S 的用途（例如，信用卡、博物馆门票等）的性质，因此智能卡 S 的计算机装置 6 被理解为表示运行软件程序以便使该用途可能的计算机装置。

在智能卡 S 的制造过程 H 期间，一个或多个应用或对应的软件程序被存储在智能卡 S 的存储装置 7 中。另外，在制造过程 H 期间，每个智能卡 S 被给予一个数据载体识别信息项，根据本实施例的实例即是一个递增的序列号 ID，其被存储在智能卡 S 的安全存储装置 8 中并用于明确地识别每个智能卡 S。在该情况下，由具有 64 位数的二进制比特组合形成序列号 ID，并且由防止黑客攻击特别有效的存储装置 7 的区域形成安全存储装置 8。

根据授权方法 E 的方框 B1，在制造过程 H 期间，计算机 C 为由每个智能卡的序列号 ID 识别的智能卡 S 生成第一密钥信息项 K1 和关联的第二密钥信息项 K2。另外，对于由序列号 ID 识别的一些或所有智能卡 S，生成第一主密钥信息项 MKI1 和第二主密钥信息项 MKI2，如下面详细描述的那样。密钥信息项 K1 和 K2 以及主密钥信息项 MKI1 和 MKI2 在该情况下可由被称为对称二进制密钥和称为不对称二进制密钥形成，这对于本领域的技术人员长期以来已经得知。本领域的技术人员还知道在每个情况下具有两个密钥信息项的其他加密方法，可同样地用在这一点。

由计算机 C 生成的第一密钥信息项 K1，和也已经生成的第一主密钥信息项 MKI1 以与智能卡 S 的序列号 ID 关联的方式被存储在智能卡 S 的安全存储装置 8 中，并且被由智能卡 S 运行的安全应用程序朋处理，如下面详细描述的那样。可能计算机生成的所有信息项，但无论如何有序列号 ID、第二密钥信息项 K2 和也已经生成的第二主密钥信息项 MKI2 被存储在智能卡 S 的制造商的安全存储装置 9 中．存储在安全存储装置 9 中的信息项可随后被用于授予修改权利，以便修改智能卡 S 中的应用程序，如下面参考实施例的示例所详细描述的那样。

根据本申请的第一个实施例，假设智能卡 S 的制造商为信用卡公司制造一百万个智能卡 S。为此目的，在智能卡 S 的制造期间，智能卡软件的项被存储在存储装置 7 中并作为第一应用程序 A1 由计算机装置 6 运行。在制造期间，序列号 ID=“123…84”、第一密钥信息项 K1=“2…4”、和第一主密钥信息项 MKI1=“88…3”被存储在智能卡 S 的安全存储装置 8 中。序列号 ID=“123…84”、与第一密钥信息项 K1 关联的第

二密钥信息项 K2=“3…5”、和与第一主密钥信息项 MKI1 关联的第二主密钥信息项 MKI2=“99…4”以关联的方式被存储在制造商的安全存储装置 9 中。一个有效连接 W 指示生成的所有智能卡 S 都被发布给信用卡公司的客户。因此，智能卡 S 如通常所知那样用于支付商店里的交易。

当制造智能卡 S 时，需要注意即使在写入信用卡软件之后，也要保证存储装置 7 仍然具有足够的附加存储空间。例如，信用卡软件可占据 3 千比特的存储装置 7 的存储空间，并且安全存储装置 8 可占据 4 千比特，存储装置 7 的 17 千比特仍然保持空闲，所述存储装置 7 总共有 24 千比特并由 EEPROM 形成。另外，计算机装置 6 的尺寸是依照它们的计算能力而定，使得多达四个应用程序 A1、A2、A3 和 A4 可并行地或者以根据时间的偏移的方式运行。

根据本申请的实例，现在假设大的百货公司链想发布客户的忠诚度卡给其客户，以便为这些客户提供专门的廉销或返款条件。因为大量百货公司链的客户使用信用卡公司的智能卡 S 来支付它们的购买，并且对于客户来说更方便的是他不需要携带其他的信用卡作为客户忠诚度卡，百货公司链从信用卡公司获得修改权利以便在智能卡 S 上安装客户忠诚度卡软件作为第二应用程序 A2。

在授权方法 E 的方框 B2 处，百货公司链作为应用程序 A2 的未来操作者向信用卡公司或者智能卡 S 的制造商要求修改权利并且为此支付需要的购买价格。在该情况下，百货公司链实质上是购买已经发布给客户的所有信用卡 S 的存储装置 7 中的存储空间，以便在存储装置 7 中存储客户忠诚度软件。在该情况下，购买价格取决于存储空间要求和发布给客户的智能卡 S 的数量。另外，购买价格还取决于第二应用程序 A2 要求的接口（要么只有无接触接口要么只有接触接口或两种接口）和运行第二应用程序 A2 所需的计算能力。另外，购买价格取决于是否已经为智能卡 S 生成了主密钥信息项并取决于是否在同时正在购买第二主密钥信息项 MKI2。因此，通过购买修改权利获得一种有趣的商业模型。

一旦信用卡公司或智能卡 S 的制造商已经与第二应用程序 A2 的操作者达成一致，也就是说与百货公司链达成一致，在方框 B3，修改权利，也就是序列号 ID 以及每个智能卡 S 的关联的第二密钥信息项 K2 和也占

用第二主密钥信息项 MKI2 之处被传送到第二应用程序 A2 的操作者的操作者计算机 10。如图 1 所示，这个传送可发生在数据网络 NET 上，在此必须例如通过接触信任中心，采取最严格的安全防范措施，以便防止未授权的人获得修改权利。但是，通过移交具有在其上存储了对应信息的 CD-ROM、硬盘或 DVD 给应用程序 A2 的操作者，修改权利还可以被手动传送。该修改权利然后在操作者计算机 10 中是可得的.

根据本申请的实例，假设为了安全的原因，只有智能卡 S 的接触接口用于安装第二应用程序的目的。为此目的，由操作者计算机 10 和通过数据网络 NET 连接到操作者计算机 10 的大量读取设备 2 形成用于安装第二应用程序的修改设备 5。一旦客户想使用智能卡 S 的信用卡应用程序来支付他的货物并且售货员将智能卡 S 插入到读取设备 2 中，在智能卡 S 上安装第二应用程序的过程就在方框 B4 上开始了。

在安装过程开始时，智能卡 S 经由接口装置 11、读取设备 2 的接点排 4 和接点排 12 来传送它的序列号 ID。读取设备 2 的计算机级 13 将该序列号 ID 传送到操作者计算机 10，操作者计算机 10 接着检查智能卡 S 是否是有效的智能卡 S，当需要时，智能卡 S 能使用它的第一密钥信息项 K1 加密一个代码字，并经由读取设备 2 将其传送到操作者计算机 10，在操作者计算机 10 中可仅仅借助关联的第二密钥信息项 K2 解密加密的代码字. 这种检查智能卡 S 的有效性用来防止第二应用程序 A2 被安装在无效的智能卡 S 上。

一旦已经在方框 B4 中确定了智能卡 S 的有效性，那么在方框 B5 上继续第二应用程序 A2 的安装，否则结束第二应用程序 A2 的安装. 在方框 B5，与操作者计算机 10 中的智能卡 S 的序列号 ID 关联的第二密钥信息项 K2 被确定并经由读取设备 2 被输出到智能卡 S 的安全应用程序 AS。 当需要时，为了安全的原因还可加密第二密钥信息项 K2. 在方框 B6，安全应用程序 AS 接着检查存储在安全存储装置 8 中的第一密钥信息项 K1 是否与由修改设备 5 输出的第二密钥信息项 K2 关联，确定修改设备 5 是否具有修改或安装第二应用程序 A2 的修改权利.

如果在方框 B6 的检查结果显示出修改设备 5 被授权安装第二应用程序 A2，那么在方框 B7 将第二应用程序 A2 存储在智能卡 S 的存储装

置 7 中。为了实现此，操作者计算机 10 经由读取设备 2 传送第二应用程序 A2 并且智能卡 S 允许读取设备 2 在特定范围内访问存储装置 7. 在该情况下，修改设备 5 对第二应用程序 A2 的修改范围或性质是由修改权利的性质确定的，即是由第二密钥信息项 K2 确定的，并且由智能卡 S 中的安全应用程序 AS 确定。

修改权利可授权第二应用程序 A2 的操作者在存储装置 7 的一个由它的存储空间（例如 5 千比特的最大值）限制的部分中安装第二应用程序 A2。这保证了对于 4 个应用程序 A1 到 A4 在存储装置 7 中存在实际上足够的存储空间.

另外，修改权利可确定第二应用程序 A2 访问存储装置 7 的对于应用程序公共的区域以及访问智能卡 S 的接口的访问权利。在该情况下，客户忠诚度卡应用程序可例如只使用无接触接口，以便传递客户数据和返款。

另外，修改权利可确定应用程序哪种类型的修改可由修改设备 5 执行。在该情况下，修改设备 5 可被授权仅用新版本的客户忠诚度卡应用程序来代替第二应用程序 A2 或用完全不同的第二应用程序 A2 来代替它。同样，修改权利可排他地允许第二应用程序的删除. 同样，这些可能性的组合或所有这些可能性可只与第二密钥信息项 K2 一起.

另外，修改权利可以或必须还识别可修改的应用程序，以便例如防止从智能卡 S 的存储装置 7 删除错误的应用程序. 但是，修改权利还可只识别存储装置 7 中的特定存储区域，在该存储区域中，可执行任何修改或规定的修改。

如果已经在智能卡 S 中存储了第一主密钥信息项 MKI1 并且如果对于智能卡 S 已经把关联的第二主密钥信息项 MKI2 输出到修改设备 5，那么修改设备 5 可修改智能卡 S 中的访问权利和／或在智能卡 S 中生成另外的第一密钥信息项 K1 并在操作者计算机 10 中生成另外的第二密钥信息项 K2。假设百货公司链不再期望仅使用进行无接触通信来传递客户数据的终端 1，而还想使用以要求接触的方式通信的读取设备 2. 但是，因为在安装时第二应用程序 A2 只被给予访问无接触接口（接口 11 和天线 3）的访问权利，因此这是不可能的。修改设备 5 可通过加密使用第

二主密钥信息项 MKI2 的访问权利修改命令并将加密的代码传送到智能卡 S 来接触，以得到这样的效果，即安全应用程序 AS 通过使用存储在安全存储装置 8 中的第一主密钥信息项 MKI1 解密接收的代码来确定修改设备 5 的修改权利，并且执行访问权利修改命令。结果，第二应用程序 A2 获得对智能卡 S 中的无接触接口和接触接口的访问。因此可能有利的是，即使在由智能卡 S 运行的应用程序已经被发布给客户的情况下，可修改对接口以及同样对存储装置 7 的存储区域的访问权利。

另外，该情况可出现在存储在安全存储装置 8 中的第一密钥信息项 K1 已经被用于修改应用程序或已经被黑客发现并因此也许不能再被使用的情况。在该情况下，新的第一和第二密钥信息项可由操作者计算机 10 生成，其中新的第一密钥信息项可作为代码以使用第一主密钥信息项 MKI1 加密的方式被传送到智能卡 S。智能卡 S 的安全应用程序 AS 可接着使用第二主密钥信息项 MKI2 解密接收的代码，因此新的第一密钥信息项可被有利地存储在智能卡 S 的安全存储装置 8 中，以修改其他的应用程序。

还可生成第一主密钥信息项 MKI1 和第二主密钥信息项 MKI2，使得进行与将智能卡 S 作为整体有关的修改是不可能的，但是可能作出与仅仅一个应用程序有关的访问权利的修改，或者可能仅为该一个应用程序生成新的密钥信息项。在此可以保证特定的关键应用程序（例如信用卡应用程序、金融应用程序等）不可能被修改，也就是说即使借助主密钥信息项也不能，因为主密钥信息项的权利可被限制到其他应用程序。

作为进一步的安全防范措施，可以定义在确定应用程序待被修改的特定属性时才允许通过智能卡 S 的修改设备 5 修改智能卡 S 中的应用程序。例如，应用程序的操作者可能将可能甚至对于智能卡的制造商都不知道的其他密钥信息项插入到应用程序中，应用程序隐藏的另外的密钥信息项形成应用程序的属性。那么，仅当修改设备 5 向智能卡 S 传送与另外的密钥信息项关联的密钥信息项时，智能卡 S 允许修改（例如删除）由修改设备 5 存储在智能卡 S 中的该应用程序。由此获得的优点在于，应用程序的操作者可为它的应用程序作出进一步的安全防范措施。

根据在图中没有示出的实施例的第二个实例，智能卡 S 的用户可拥

有计算机以及连接的无接触通信终端，在该情况下，无接触通信终端形成修改设备。根据实施例的第二实例，计算机经由互联网连接到消息发射器的服务器，通过该服务器，可呼叫消息并提供消息预定。用户电子地填写用于消息预定的注册表格并输入他的信用卡号以便支付消息预定（方框 B2）。接着，经由互联网在用户的计算机上存储修改权利（ID 和 K1），借助修改权利，消息应用程序可被安装在智能卡上。根据上述的安装过程，接着消息应用程序作为第三应用程序被存储在智能卡上。用户接着可以使用智能卡在任何计算机上用无接触通信终端呼叫消息预定的当前消息。另外，造访电影院的电影票也包括在消息预定中。用户因此可在电影院售票处的终端出示他的智能卡，由此在无接触通信的过程中，智能卡的消息应用程序只确认电影票一次。该服务是可能的，因为电影院的操作者与消息发射器的操作者合作。

应答器、个人数字助理、移动电话或其他类似设备可用作为数据载体。无接触通信可例如依照公布的标准 IS014.443、IS015.693、IS018.000、ECMA340 的其中一个进行或根据电话标准 GSM 或 UMTS 其中一个进行。

借助根据本发明的授权方法、根据本发明的数据载体和根据本发明的修改设备，除了上述优点外，还获得了实质上的优点，即可在已经发布给客户的数据载体中修改应用程序，因此数据载体能进行其他业务而不需要涉及为此目的的信任中心。通过避免对信用中心的需要，还可由操作“离线”的修改设备来修改应用程序并且也节省了信用中心的成本。通过出售修改权利还获得一种有趣的商业方法。

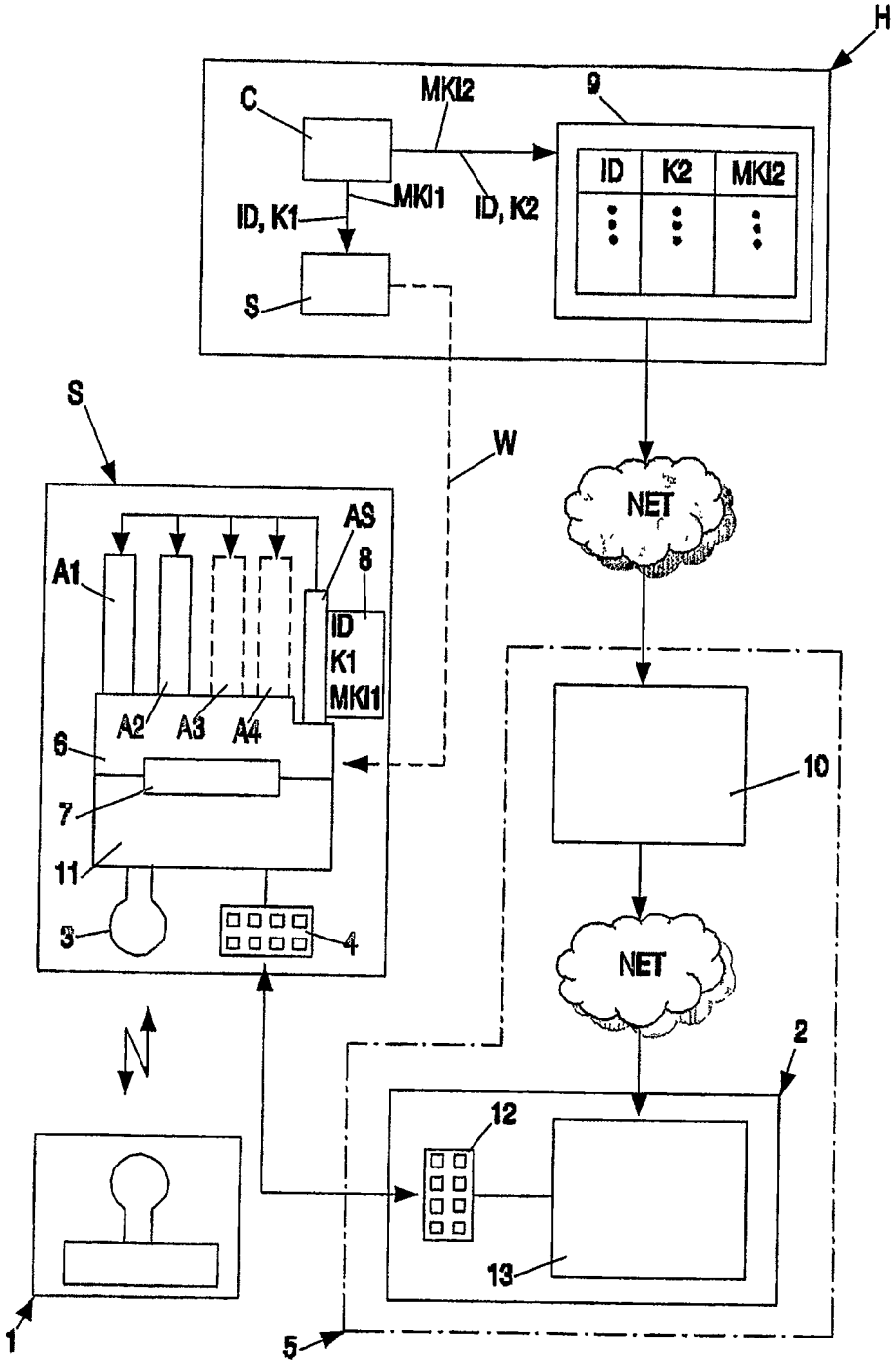

H
C
MKI2
9
ID
K2
MKI2
ID, K1
MKI1
ID, K2
S
W
NET
AS
8
A1
ID
K1
MKI1
A2
A3
A4
6
7
11
3
4
10
NET
2
12
13
1
5

图 1

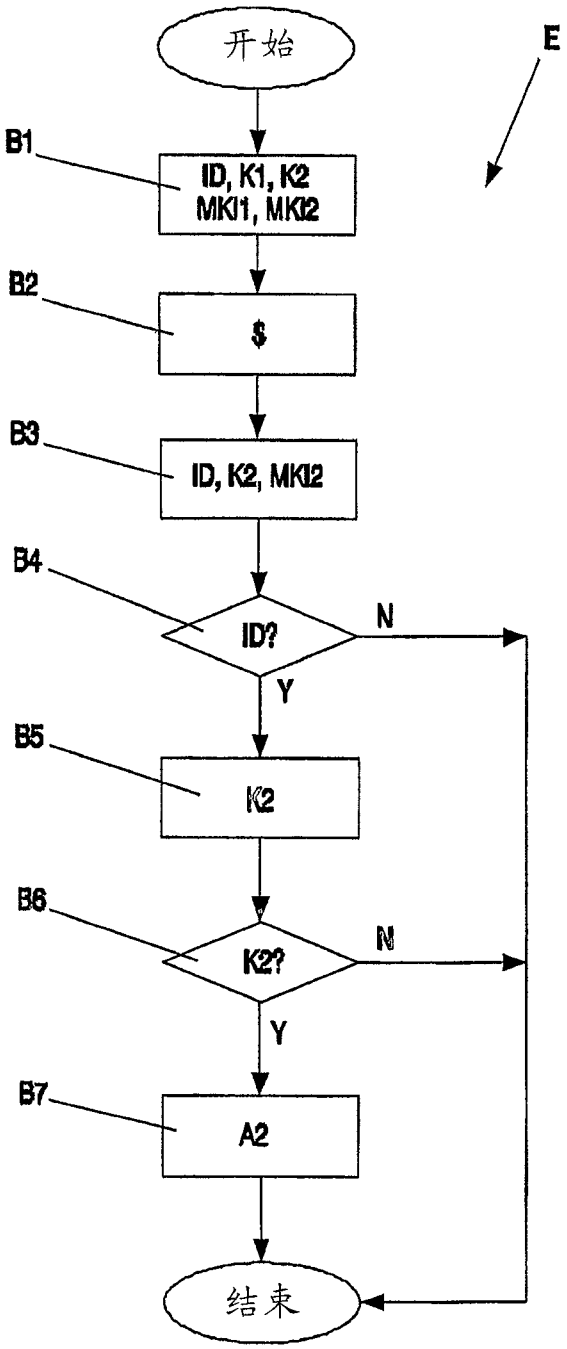

开始
E
B1
ID, K1, K2
MKI1, MKI2
B2
$
B3
ID, K2, MKI2
B4
ID?
N
Y
B5
K2
B6
K2?
N
Y
B7
A2
结束

图 2