[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 1/00

[12] 发明专利申请公开说明书

[21] 申请号 200380101942.9

[43] 公开日 2005 年 12 月 14 日

[11] 公开号 CN 1708740A

[22] 申请日 2003.10.15
[21] 申请号 200380101942.9
[30] 优先权
[32] 2002.10.22 [33] EP [31] 02079390.7
[86] 国际申请 PCT/IB2003/004538 2003.10.15
[87] 国际公布 WO2004/038568 英 2004.5.6
[85] 进入国家阶段日期 2005.4.22
[71] 申请人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 F·L·A·J·坎佩曼
G·J·施里詹

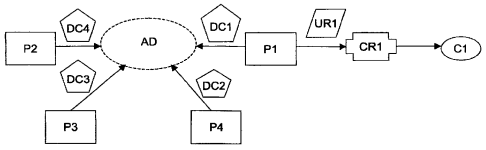
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 李亚非 刘 杰

权利要求书 3 页 说明书 20 页 附图 2 页

[54] 发明名称 用于授权内容操作的方法与装置

[57] 摘要

本发明提供了方法和装置(D1)，用于根据一个用户权力(UR1)授权由第一用户(P2)请求的对于一个信息内容选项(C1)的操作。 该用户权力可以标识第一用户或第二用户(P1)并且授权当事的用户来执行对于该信息内容选项的请求的操作。 如果用户权力标识该第二用户，则在收到链接该第一用户的用户权力和第二用户的用户权力的信息之时授权该操作。 该信息最好包括标识同一个授权与域(AD)的作为成员的第一和第二用户的一个或多个域鉴证(DC1、DC2)。 最好使用实现该操作的一个信息内容权力(CR1)，从而该用户权力将授权该第二用户采用该信息内容权力。



ISSN1008-4274

1. 一种授权方法，根据标识一个第二用户的用户权力授权由一个第一用户对于一个信息内容选项请求的操作，并且授权该第二用户对于该信息内容选项执行该请求的操作，其中该操作是依据链接该第一用户的用户权力和第二用户的用户权力的信息的接收而被授权的。

2. 权利要求 1 的方法，其中该信息包括把该第一和第二用户标识为同一个授权域的成员的一个或多个域鉴证。

3. 权利要求 2 的方法，其中该一个或多个域鉴证包括把该第一用户标识作为一授权域的一个成员的第一域鉴证和把该第二用户标识作为该授权域的一个成员的第二域鉴证。

4. 权利要求 2 的方法，其中该一个或者多个域鉴证包括把该第一和第二用户标识为该授权域的成员的单一鉴证。

5. 权利要求 1 的方法，其中该操作至少包括下列步骤之一：提供信息内容选项、记录信息内容选项、转移信息内容选项以及创建该信息内容选项的一个拷贝。

6. 权利要求 1 或 2 的方法，包括接收一个信息内容权力的步骤，该信息内容权力包含用于对该信息内容选项执行请求的操作、授权该第二用户采用该信息内容权力的该第二用户的用户权力的必要信息。

7. 从属于权利要求 2 的权利要求 6 的方法，其中，如果该信息内容权力不标识该授权的域，则将不授权该操作。

8. 用于根据标识一个第二用户的用户权力，执行由一个第一用户请求的对于一个信息内容选项的操作的装置，并且授权该第二用户对于该信息内容选项执行该请求的操作，被用于在接收链接该第一用户的用户权力和该第二用户的用户权力的信息之时授权该操作。

9. 权利要求 8 的装置，其中信息包括一个或多个将第一和第二用户标识作为同一个授权域的成员的域鉴证。

10. 权利要求 9 的装置，其中该一个或多个域鉴证包括把该第一用户标识作为一授权域的一个成员的第一域鉴证和把该第二用户标识作为该授权域的一个成员的第二域鉴证。

11. 权利要求 9 的装置，其中该一个或者多个域鉴证包括把该第一和第二用户标识为该授权域的成员的单一鉴证。

12. 权利要求 8 的装置，被用于从一个标识装置接收用于该第一用户的一个标识符，并且如果该接收的标识符与在该第一用户的用户权力中的该第一用户的标识匹配的话，则执行该操作。

13. 权利要求 8 或 9 的装置，被用于接收一个信息内容权力，该信息内容权力包含用于对该信息内容选项执行请求的操作、授权该第二用户采用该信息内容权力的该第二用户的用户权力的必要信息。

14. 权利要求 11 的装置，其中该信息内容权力的至少一部分被使用一个加密密钥所加密，对于该加密密钥来说，该装置可得到对应的解密密钥。

15. 权利要求 13 的装置，其中，该信息内容权力具有一个实现该信息内容权力的真实性的验证的数字签名。

16. 权利要求 15 的装置，如果该数字签名能够被使用与一个授权信息内容提供者相关的一个数字鉴证成功地验证，则被用于执行该操作。

17. 权利要求 15 的装置，如果该数字签名能够被使用与一个具体装置相关的一个数字鉴证成功地验证，则被用于执行该操作。

18. 权利要求 15 的装置，如果不能使用与授权的信息内容供应商相关的一个数字鉴证成功地验证该数字签名、并且与该授权的信息内容供应商相关的一个数字水印存在于该信息内容选项中，则该装置被用于拒绝执行该操作。

19. 权利要求 13 或 15 的装置，被用于从该信息内容权力中提取一公共密钥，并且在进行该操作是否被授权的确定中使用该提取的公共密钥。

20. 权利要求 13 的装置，该装置被用于确定针对该信息内容选项的一个可靠指纹，并且如果一个确定的可靠指纹不与该信息内容权力中包括的一个可靠指纹匹配，则用于拒绝执行该操作。

21. 从属于权利要求 9 的权利要求 13 的装置，如果该授权域未被该信息内容权力所标识，则被用于拒绝执行该操作。

22. 一种方法，根据包含用于对该信息内容选项执行请求的操作的必要信息的一个信息内容权力和标识一个第一用户并且授权该第

一用户采用该信息内容权力的一个用户权力，授权由该第一用户请求的对于一个信息内容选项的操作。

23. 一种装置，用于根据一个信息内容权力执行由第一用户请求的对于一个信息内容选项的一个操作，该信息内容权力包含用于对该信息内容选项执行请求的操作的必要信息以及标识该第一用户和授权该第一用户来采用该信息内容权力的一个用户权力。

24. 权利要求 23 的装置，其中该信息内容权力的至少一部分被使用一个加密密钥所加密，对于该加密密钥来说，该装置可得到对应的解密密钥。

25. 权利要求 23 的装置，其中，该信息内容权力具有一个实现该信息内容权力的真实性的验证的数字签名。

26. 权利要求 25 的装置，如果该数字签名能够被使用与一个授权信息内容提供者相关的一个数字鉴证成功地验证，则被用于执行该操作。

27. 权利要求 25 的装置，如果该数字签名能够被使用与一个具体装置相关的一个数字鉴证成功地验证，则被用于执行该操作。

28. 权利要求 25 的装置，如果不能使用与授权的信息内容供应商相关的一个数字鉴证成功地验证该数字签名、并且与该授权的信息内容供应商相关的一个数字水印存在于该信息内容选项中，则该装置被用于拒绝执行该操作。

29. 权利要求 23 的装置，该装置被用于确定针对该信息内容选项的一个可靠指纹，并且如果一个确定的可靠指纹不与该信息内容权力中包括的一个可靠指纹匹配，则用于拒绝执行该操作。

30. 权利要求 23 的装置，被用于从一个标识装置接收用于该第一用户的一个标识符，并且如果该接收的标识符与在该第一用户的用户权力中的该第一用户的标识匹配的话，则执行该操作。

用于授权内容操作的方法与装置

本发明涉及授权由一个第一用户请求的对于一个信息内容项的操作。本发明进一步涉及用于执行由一个第一用户对于一个信息内容项请求的操作的装置。

近年来，信息内容保护系统的数量快速增加。某些系统仅保护信息内容抵抗非法复制，而其它一些系统还禁止用户接入该信息内容。第一类系统被称之为防复制(CP)系统。CP 系统传统地被主要集中用于消费电子(CE)装置，因为此类信息内容保护被认为低价实现并且不需要与内容的供应商双方向相互作用。例如内容加扰系统(CSS)是 DVD ROM 磁盘和 DTCP 保护系统，该保护系统用于 IEEE 1394 连接。

第二类系统已知有几种叫法。在广播领域中，这类系统一般称之为条件接入(CA)系统，而在互联网络领域中，这类系统一般称之为数字权管理(DRM)系统。

近来，已经采用了新的信息内容保护系统，其中能够通过一个双向连接在一组设备中彼此鉴证。基于这种鉴证，这些装置将彼此信任并且将实现它们彼此交换保护的信息内容。在伴随该信息内容的许可协议中，描述该用户具有哪些权力以及用户被允许对于该内容执行的操作。利用某些通用网秘密保护该许可协议，该秘密仅在一个确定的家用装置之间交换，或一般地说仅在一个确定的范围之内的装置之间交换。这种装置的网络被因此称为授权域(AD)。

授权域的概念试图寻找一种既服务于内容拥有者的利益(需要的版权保护)又服务信息内容消费者(即想要无限制使用信息内容)的解决方案。该基本原则是，具有一个控制网络环境，其中只要不越界该授权域，就能相当自由地使用该信息内容。通常，授权域是围绕该家庭环境为中心的，也称作家庭网络。当然其它方案也是可能的。用户能够在旅行中使用一个便携式电视机，并且在旅馆房间使用便携式电视机接入在其家里个人录像机上储存的信息内容。尽管该便携式电视机是在该家庭网络的外部，它仍将是授权域的用户的一部分。

这种用于装置之间的安全内部通信的必要信任是基于某些秘

密，这些秘密仅有被测试和鉴证具有安全方案的装置才知道。该秘密的了解是使用一种认证协议测试的。当前已知用于这些协议的最佳方案采用的是"公共密钥"加密技术，使用两个不同密钥的对儿。这种将被测试的秘密则是该成对的保密密钥，而该公用密钥可用于该测试的结果的验证。为确保该公用密钥的正确性和检验该密钥对儿是否为一个被鉴证装置的一个合法密钥对儿，该公用密钥伴随有由一个鉴证权限数字签名的一个鉴定，该鉴证权限管理着全部装置的公用/专用密钥对儿的分配。在一个简单的实施方案中，该鉴证权限的公用密钥被硬编码到该装置的实施方案中。

已知有若干 AD 形式的 DRM 系统的实施方案。但是，这些方案通常受若干限制和问题的影响，这些限制和问题使得其难于配置和为市场的所接受。具体地说，一种没有被充分解决的重要问题是如何管理和保持一个授权的域结构，允许消费者在其选择的任何时间和任何位置来运用其权力。当前的 AD 解决方案通常把消费者限制到一个特定和局限的系统设置，并且不提供期望的灵活性。

一个通用的方法是为购买一个信息内容权力(需要接入一个信息内容选项的权力，通常包含必需的解密密钥)的人提供一个安全的像智能卡的个人装置。在重放过程中，该智能卡与一个顺应性的重放装置共享此解密密钥。只要这个人随身带有他的智能卡，就能够立刻接入信息内容。这种解决方案的缺点是，一个智能卡具有的存储器数量有限，这意味着不能在该卡上存储全部权力。

一种对于该系统的改进是利用该智能卡的公用密钥加密该信息内容的权力并且把该权力存储在某处，例如与信息内容选项一起存储在多个位置。但是，现在还不完全清楚这种信息内容权力如何能够与人员的家庭共享的方式。目前的可能是对于购买(一个权力)一个信息内容选项，例如在一个激光唱盘上存储的歌曲的一个家庭成员来说，该歌曲能够被该家庭的其它成员所共享。消费者习惯于这种共享，并且也期待来自基于 AD 系统的这种共享。只要把这种权力保持固在一个特定家庭之内，版权法一般允许这种活动。DRM 系统努力防止任何第三方的复制，所以无意中也阻断了允许这种类型的活动。

这种信息内容的权力能够以该家庭成员的各个智能卡的分别的公共密钥重新加密。这要花费许多时间和处理能力，因为全部权力都

必须单独处理。为了检验是否为一个家庭成员，拥有重新加密的信息内容权力的特定智能卡人将被提供一个能够被添加到该智能卡的家庭标识符。但是，这不是一个灵便的解决方案，事实上目前很难删除或撤销在一个家庭成员的智能卡上的信息内容权力。

本发明的一个目的是提供实现允许基于人员而不是装置的权力管理的授权方法。

此目的是根据本发明的一种方法实现的，根据包含用于对该信息内容选项执行请求的操作的必要信息的一个信息内容权力和标识一个第一用户并且授权该第一用户采用该信息内容权力的一个用户权力，该方法授权由该第一用户请求的对于一个信息内容选项的操作。该用户权力是在一个用户和一个信息内容权力之间的一种单一连接。

例如，因为信息内容权力包括一个必要的解密密钥，所以为了接入一段信息内容而要求该信息内容权力。通过给出更多的用户权力授权人采用该信息内容权力而实现基于人员的权力管理。

此目的是根据本发明的一种授权方法实现的，根据标识一个第二用户的用户权力授权由一个第一用户对于一个信息内容选项请求的操作，并且授权该第二用户对于该信息内容选项执行该请求的操作，其中该操作是依据链接该第一用户的用户权力和第二用户的用户权力的信息的接收而授权的。通过用户权力，人员能够被授权执行操作而与他们希望使用哪些装置无关。该链接信息使得用户互相分享权力，而与信息内容所驻留的装置或例如可能需要来对于那信息内容执行操作的信息内容权力的任何信息无关。因此，权力管理是基于人员而不是基于装置。

该链接信息最好包括把该第一和第二用户标识为同一个授权域的成员的一个或多个域鉴证。期望的是能够以一个特定家庭的成员、或一般地说一种特定的域共享对于该信息内容选项的接入。为此目的，由一个信任的第三方发行域鉴证(指示一个组或域的鉴证)，以便限定哪些人员是一个特定域的成员。如果该第一用户目前未被授权执行该操作，但在同一域中确实有第二用户具有这样的权力，则该第一用户仍然被允许执行该操作。用户权力最好能够在系统的任意位置。

现在有可能:

个人购买接入信息内容(确定的片段)的权力，

在家庭/住户中分享这样的权力，

能够象个人在家庭中那样在任何装置和(在世界)任意位置运用这样的权力，

能够把这样的权力转移到其它人(在家庭内部和外部)，

如果有必要，能够撤销和/或更新权力，

应对家庭结构的变化，

应付权力秘密的公开和非法行为(例如装置的黑客)。

在一个实施例中，本方法包括接收一个信息内容的权力的步骤，该信息内容权力包含用于对该信息内容选项执行请求的操作、授权该第二用户采用该信息内容权力的该第二用户的用户权力的必要信息。现在任何人都能够获得一个用户权力并且因此独立于其他人可能拥有的任何其它用户权力而运用该信息内容权力。该信息内容权力有可能使得一个装置能够执行该操作，因为该信息内容权力包含用于接入该信息内容所需要的解密密钥。一个用户权力授权一个具体用户在该装置上采用该信息内容权力。此装置必须检测该权力是否有效以及该用户否有效。如果一个正确的域鉴证也是有效的，则将授权一个第二用户，该正确的域鉴证连接了这两个用户。

在另外一个实施例中，如果该信息内容权力不标识该授权的域，则将不授权该操作。此方法能够把信息内容权力限制到具体的授权域。这不仅实现更加细化（fine-grained）的权力管理，而且还通过把一个装置折衷在一个具体授权域中而限制试图获得解密密钥(由信息内容权力提供的)的一个黑客所能做的破坏。为了进一步扩展本实施例，能够有选择地使用一种加密密钥局部地加密该信息内容权力，在该域中的装置可得到该对应的解密密钥。此方法的信息内容权力不可在该域之外使用。

本发明的一个另外目的是提供实现允许基于人员的权力管理的授权装置。

此目的是根据本发明的一个装置实现的，此装置用于根据一个信息内容权力执行由第一用户请求的对于一个信息内容选项的一个操作，该信息内容权力包含用于对该信息内容选项执行请求的操作的必要信息以及标识该第一用户和授权该第一用户来采用该信息内容权

力的一个用户权力。

此目的是以根据本发明的一个装置实现的，该装置用于根据一个用户权力执行由一个第一用户请求的对于一个信息内容选项的操作，该用户权力标识一个第二用户并且授权该第二用户对于该信息内容选项执行该请求的操作，被用于在接收链接该第一用户的用户权力和该第二用户的用户权力的信息之时授权该操作。

该链接信息最好包括一个或多个标识作为同一个授权域的成员的第一和第二用户的域鉴证。期望的是能够以一个具体家庭的成员、或一般地说一个具体的域共享对于该信息内容选项的接入。

在一个实施例中，该装置被用于接收一个信息内容的权力，该信息内容权力包含用于对该信息内容选项执行请求的操作、授权该第二用户采用该信息内容权力的该第二用户的用户权力的必要信息。该信息内容权力的至少一部分最好被使用一个加密密钥所加密，对于该加密密钥来说，该装置可得到对应的解密密钥。以此方式，只有在一个具体授权域中的装置才能够使用该信息内容权力，从而有效地把该信息内容权力限制到该具体域。

在一个进一步的实施例中的，该信息内容权力具有一个实现该信息内容权力的真实性的验证的数字签名。如果该数字签名能够被使用与一个授权信息内容提供者相关的一个数字鉴证成功地验证，则该装置最好被用于执行该操作。以此方式，只有该信息内容供应商自己才能够产生"正式的"信息内容权力。

在一个进一步实施例中，如果能够使用与一个具体装置相关的数字鉴证成功地核对该数字签名，则该装置才被用于执行该操作。以此方式，个人信息内容(根据该具体装置产生的)还可以被重放或另外使用，无需涉及第三方。

在本实施例的一改进中，如果不能使用与授权的信息内容供应商相关的一个数字鉴证成功地验证该数字签名并且与该授权的信息内容供应商相关的一个数字水印存在于该信息内容选项中，则该装置被用于拒绝执行该操作。此方法中，即使当恶意的用户试图传送该"正式"内容作为个人信息内容，例如通过从一个电视屏幕创建一个模拟记录，该恶意的用户也无法产生针对"正式"信息内容的信息内容权力。

在一个进一步的实施例中，该装置被用于确定针对该信息内容选项的一个可靠指纹，并且如果一个确定的可靠指纹不与该信息内容权力中包括的一个可靠指纹匹配，则用于拒绝执行该操作。此方法中，恶意的用户无法产生针对个人信息内容的信息内容权力并且随后试图使用针对"官方"信息内容的那些信息内容权力。

本发明这些以及其它方面将从如图所示的示例实施例中变得明显，并且参考这些实施例而被阐明，附图中：

图 1 示出根据人员、权力和信息内容的一个授权域(AD)的模式；

图 2 示出一个装置的实例，该装置由想对于信息内容选项执行一个操作的携带智能卡的一个用户所操作；和

图 3 示出一种方式，其中如果有两个人都属于同一个 AD，则一个人能够采用另一人的用户权力来运用一个信息内容权力。

在各个图中，相同的参考数字指示类似的或相应的特征。附图中指示的一些特征通常以软件的形式实现，并且如此表示软件实体，比如软件模块或物体。

图 1 示出根据人员、权力和信息内容的一个授权域(AD)的模式。该授权域 AD 包含信息内容 C1、C2、C3、...Ck，权力 R1、R2、R3、...Rm 和人员 P1、P2、P3、...Pn。该模式还显示内容选项，例如信息内容选项 Ci 可被导入该域或从该域输出，还显示人员，例如人员 Pj，可以注册到该域或从该域消除注册。有关授权域结构和实现选项的更多的信息可以参考国际专利申请 WO03/047204(代理卷号 PHNL010880)或国际专利申请序列号 PCT/IB03/01940(代理卷号 PHNL020455)。

可被用于图 1 模式的给出的域中的某些实例功能是：

AD 人员会员资格管理：

人员识别(一个人员属于哪一个 AD)

人员注册到一个 AD

人员从一个 AD 消除注册

AD 人员-权力链接管理：

人员-权力链接识别(哪些人员可以使用一个全力)

把一个权力链接到一个人员

断开一个人员-权力链接

必须指出，实际上的信息内容只能被操作一个装置的用户接入/

使用。在下面描述中假设该系统中使用的装置是顺应性和"公用"装置。这意味着，一个装置将遵守确定的操作规则(例如将不在一数字接口上非法输出信息内容)而装置的所有权是不重要的(公用)。装置的顺应性管理，即顺应性装置标识、装置的更新能力以及装置的撤销将被认为是适当的(使用已知技术)，在此将不再考虑。该信息内容权力可用于完成装置顺从管理。

该用户权力是在用户和信息内容权力之间的单一连接(该信息内容权力是解密一个信息内容字段所需要的)。通过引入这种用户权力，系统中现具有五个主要实体，能够工作如下:

信息内容: 信息内容选项被加密(有许多选项，例如每一信息内容标题具有唯一密钥)并且能够在系统中的任意位置。

信息内容权力: 包含为了接入一确定的信息内容选项的规则(例如限制观众为18岁或大于18岁，或仅限欧洲市场)和密钥。从内容权力能够被产生为每一信息内容标题是唯一的甚至信息内容的每一样本(复制)是唯一的方面看来，系统是灵活的。信息内容权力应当仅传输到顺应性的装置。一个更安全的规则是，强迫信息内容权力只可被传输到由授权用户操作的顺应性装置(即被利用其用户权力授权而可以使用该具体信息内容权力的用户)。信息内容权力也可以与信息内容一起存储在例如一个光盘上。

用户权力: 由内容供应商发放的一个鉴证，授权一个人使用某一信息内容权力(属于信息内容的一个确定的字段)。原则上，用户权力能够在系统的任意位置。SPKI授权鉴证(被实施顺应性于例如X.509)可用于实现这样的一个用户权力。

装置: 一个(顺应性)装置，能够利用个性化标识装置(例如一个智能卡)或例如生物测量(或两者)识别一个用户并且收集证明该用户被允许使用一个确定的内容权力的鉴证(例如从该智能卡或从其它装置)。从其中储存了信息内容权力的智能卡(如果该权力储存在其中)获得此信息内容权力或从网络上的另一装置(在示出正确鉴证链路之后)获得该信息内容权力。

用户:一个用户由某些生物测量或最好由用户携带的个性化标识装置(例如智能卡)所标识。后者最好是个性化装置，因为个性化装置允许用户随身携带(在离线装置上接入信息内容)并且产生签字，以便

发出他们自己的鉴证(用户权力)。该标识装置本身可以由一种生物测量鉴别机制保护,以使除合法拥有者以外的任何人都不能使用该标识装置。

图 2 示出装置 D1 的一个实例,由携带智能卡 ID 的想对于信息内容选项 C1 执行操作的用户操作,例如信息内容选项的提供、信息内容选项的记录、信息内容的转移或创建该信息内容选项的一个拷贝。设备 D1 从在互联网络上的远程数据库获得一个用户权力,最好具体化为一个数字鉴证,并且将其储存在本地存储介质 UR 中。

从一个第二装置 D2 获得为了对于该信息内容选项 C1 执行操作所需的该信息内容权力,也最好具体化为数字鉴证,并且存储在本地存储介质 CR 中。在开始该信息内容权力的传送之前,装置 D2 核查用户的用户权力(根据如以前所说的用于传送信息内容权力的规则)并且核查该装置 D1 是否为顺应性装置。为这目的,装置 D1 和 D2 分别具有鉴证模块 AUTH。这些模块例如能够包括来自一个公用/专用密钥对儿的分别的专用密钥和用于相关公共密钥的鉴证,实现基于公共密钥授权认证。

如果有包含用于对信息内容选项 C1 执行请求的操作的必要信息的一个信息内容权力以及标识该第一用户并授权该第一用户使用该信息内容权力的一个用户权力,则授权对于该信息内容选项 C1 的操作。在其它系统中,可能不需要使用一个单独的内容权力,例如假设全部对于该系统中的信息内容的操作总是被授权的。

如果没有授权该用户执行该操作的用户权力,或没有授权该第一用户采用该信息内容权力的用户权力,则一般说来不执行该操作。但是,如果接收了链接第一用户的用户权力和第二用户的用户权力的信息,则仍然可以授权该操作。这样的信息可以是任何类型的信息,例如标识用户或关于指示该用户权力被链接的一个 Web 服务器的一个列表的一个鉴证。该信息还能够被包括在该用户权力本身之一(或两个)中。如下讨论的那样,该信息最好以一个或者多个域的鉴证的形式提供。

提供的解决方案假设可得到一种公共密钥基础结构,其中的用户,信息内容持有人和其它信任的第三方保持他们自己的唯一的专用/公用密钥对儿,并且能够通过利用其专用密钥签名发布鉴证。一个

可能性是按照该 SPKI/SDSI 结构中的限定来使用鉴证。

为了引起授权域的概念，建议把另一类型的鉴证采用到该系统中。一种叫作域鉴证的鉴证由一个(信任的)第三方给出，该第三方限定属于一个确定域的人员/实体。这样的一个鉴证包含该目标(一个人)的标识符(例如生物测量，公共密钥)和该目标申明属于是其一部分的该授权域的标识符(例如名字，公共密钥)。该鉴证以该发布信任方的专用密钥签名。而且该鉴证必须包括普通的字段，象对应一个适当的撤销系统的"发行日期"和"有效日期"。该 SPKI"姓名鉴证"可用于实施这种域鉴证。

例如，一个人可以把一个住户域定义到每一用户，这将定义一个人住在其中住所。这能够通过让该当局(或其一个代表)发布申明该登记的街道和用户地址的鉴证来实现。这样的一个鉴证创建在一个人(用户)和其家庭之间的单一连接。

能够以多种方法实现该域鉴证。在一个实施例中，每一用户被发布一个单独的域鉴证，标识其作为一个具体授权域的成员。在两个不同域鉴证中的相应的 AD 标识符的比较将确定两个用户是否为同一个域的成员。此方法的每个域鉴证都能够被单独管理并且在另一人加入或离开该授权域时，一个人员的域鉴证不受影响。

在另一个实施例中，用于单一授权域的成员的标识符被以单个域鉴证列举。此方法更为容易地核查是否两个人属于单个授权域。而且，每人都自动具有其可用域的全部其它成员的 AD 会员资格信息，无需要求检取一个单独的鉴证。然而，当一个新人员加入该 AD 时，全部人员都必须被发给新的域鉴证。

能够以如下所述方式实现把对于信息内容的接入授权给居住在同一个授权域中的人们。如果住在授权域(住户)AD 中的一个人 P1 例如具有用户权力来运用该信息内容权力 CR1 重放信息内容选项 C1，则如果一个第二人 P2 属于同一个家庭 AD，将也可以通过把下面的鉴证提供到一个顺应性装置 D1 而运用该权力 CR1:

由显示 P1 有权运用 CR1 的内容提供者签名的用户权力 UR1

由显示 P1 是 AD 成员的当局签名的域鉴证 DC1

由显示 P2 是 AD 成员的当局签名的域鉴证 DC2

图 3 描述了这种情形。注意，假设装置 D1 已知一个确定的根公

共密钥，以便核查一个鉴证是由真实授权的发行人签名的。

可选地，该信息内容供应商可以仅允许在该域中的其他人员在某种情况下播放该信息内容。在此情况中，应该利用某些额外比特在该用户权力中说明。除说明涉及在该域中使用的许可之外，能够把其它标记或比特加到用户权力鉴证。例如涉及第一代复制许可的比特或针对一次重放的比特能够被添加在该鉴证中。这种比特还可以被加到该信息内容权力 CR1，然后与被用于运用该信息内容权力的用户权力无关地应用。

该系统还允许所谓的跨越授权域权力。这些权力是允许信息内容越界该授权域的权力。这能够通过把附加字段添加在指示该被允许的顺应性装置必须遵从的跨域行为的用户权力中来实现。该用户权力中的一个字段能够包括例如一个像"XAD=否"的语句，意指将没有用户权力鉴证被授予在该家庭授权域之外的用户。在 SPKI 授权鉴证中的代表标记能被用于这一目的。用这种方法，能够实现可以把复制限制到一代的串行复制管理。还可以期望实现"一次复制"限制。

为了实现系统的良好管理和协调，装置需要知道几个根公共密钥。为了核查在该系统中存在的鉴证(以及鉴证链路)，这是必要的。下面列出装置必须已知的在该系统中的信任的第三方面的一些根/主密钥:

信息内容持有者或代表的根密钥: 用于查验用户权力(用户权力管理)。

装置顺应性管理器根密钥: 用于查验该系统中的其它装置是否为(仍然)顺应性的(装置顺应性管理)。

命名权限的根密钥(例如发行家庭-域鉴证的政府): 用于检验在一个授权的家庭域中的关系(域管理)。

用户管理的根密钥: 用于检验单独用户(智能卡)的密钥对儿是否真实以及是否尚未被危害(用户管理)。

权力的所有和一个家庭的组成(或其他域)可能会随着时间改变。此外，装置可能被黑客攻击或保密密钥可以变成公知。因此必须针对下列情况考虑动态特性:

域(家庭成员)管理: 一个家庭的组成可能改变。

用户权力管理: 用户权力可能改变; 用户可能放弃该权力给其

他人。

用户管理：一个 ID 装置可能被黑客攻击，或一人例如可能去世。

装置顺应性管理：装置可能被黑客攻击，然后必须被撤销/更新。

一个家庭的组成以一个鉴证表示，即该鉴证列出该家庭的成员。该系统通过使用域鉴证、列出家庭成员、利用限制有效日期来处理该家庭组成中的变化。在有效日期已经到期之后，该家庭必须以某一信任的第三方申请新的鉴证。该社区管理例如能够起到这样一个信任的第三方的作用，并且考虑在该家庭组成中的变化。

注意，日期/时间能够通过把日期/时间包括在信息内容或用户权力中而容易、可靠和安全地把日期/时间传输到设备。这将实现该机制，即如果其日期迟于在用户权力或内容权力中的日期，则一个装置可以仅接受一个域鉴证。该装置也可以储存该日期/时间作为该"当前"时间的下边界供将来使用。而且某些编号机制的某些种类可被使用在用途和信息内容权力中，来实现类似的用于接受该域鉴证的效果。

一个用户权力还可以被用于把新的域鉴证分配给一个家庭。这甚至似乎是更可取的。如果一个家庭成员想使用和检取该用户权力，则其将自动地接收该新的域鉴证。该方法意味着该用途鉴证分配器还分配该域鉴证(这当然可以通过另一方实现)。

用于家庭鉴证的一个撤销机制似乎不是很有用，因为这样的撤销鉴证能够被阻断并且不能担保其分配。可以利用用户权力(或利用局部信息内容权力)分配撤销信息。

用户权力还将涉及使用有效日期。这样的一个有效日期还可能被设置为不定的。然而，仍然需要处理用户权力的转移(即一个移动操作)。对于一个用户权力来说最困难的情况是一个不定的有效日期。一些可能的解决方案是：

不提供这一选项。

使用服务供应商实现转移，给定新用户权力，撤销旧的权力：

把一个撤销信息发送到用户 ID 装置(如果可用)并且存储该撤销信息。当用户想访问信息内容时，用于接入信息内容的装置，将查阅在该用户 ID 装置中的撤销列表，并且

把一个撤销消息放在该域鉴证中(该鉴证可能变成非常大，不是

很可取的解决方案)并且要求在接入信息内容时，除提供该用途鉴证之外，还必须提供域鉴证。

利用用户 ID 装置帮助传送用户权力(具有自己专用密钥的新的签字)，在 ID 装置中添加撤销数据，并且把撤销数据发送到其它家庭成员。

发布带有有效日期的用户鉴证,这一有效日期在某时间需要被更新。

在使用一个用户权力之前，要求查阅一个外部撤销数据库。

如前所述，可以根据一个人的生物测量数据或根据属于此人的 ID 装置(例如一个无线智能卡、移动电话等)标识此人。生物测量数据将跟随着人，并且"自动"管理这些数据。然而 ID 装置则能够被黑客攻击和复制、丢失等。为了处理这种"事件"，要求注意 ID 装置的管理。

假定一个 ID 装置以使用一个公用/专用密钥对儿的某些公开密钥算法操作。其中最好还有用于 ID 装置的有效日期(或在某一个时，要求用于新信息内容的一个新的 ID 装置)。在一个专用密钥变成公知的情况下，首先应当撤销装置 ID。这样的一个撤销信息可被包括在新信息内容权力或新用户权力中。而且应该从家庭鉴证中消除这个人。这将为黑客给出一个附加的障碍，使之不能接入家庭成员拥有的信息内容。

应该指出，当一个人购买信息内容，即获得一个使用鉴证时，能够自动地更新该 ID 装置。

能够根据信息内容权力的分配来完成装置顺应性管理。只允许顺应性装置获得信息内容权力。可用不同的技术执行装置管理并且保证信息内容权力分配，例如使用安全鉴证信道(SAC)和鉴证，以及例如使用MKB结构,如在CPPM和CPRM(参见http://www.4centity.com/)中使用的那样。

使用两种类型的信息内容权力的一个具体解决方案：全球权力(能遍及全世界使用)和个人/家庭权力(将局部地保持在购买它的用户并且不能被分配)。该理由是，这将实现权力的计算机制的使用，这对于由一个服务供应商签名的用户权力是不可能的。

在特定的/计算权力的情况下，该信息内容权力将被实现个人/

家庭权力。用户权力应指明一个全球或该个人/家庭信息内容权力是否必须被使用。为了使得其更一般化：允许针对一个具体信息内容字段的不同信息内容权力。用户权力将指示将被使用何种具体信息内容权力。

信息内容权力能够包含用于用户权力和人员 ID 装置的撤销数据或在信息内容被重放之前，联系一确定的撤销数据库的一个指令。能够通过要求一个雄鹿跳动机制（hart beat mechanism）获得时间而实现基于时间的权力(参见例如国际专利申请 WO 03/058948，代理卷号 PHNL020010)。

一个关键的假定是，该信息内容权力只被传输到顺应性装置，并且由具有适当用户权力的用户操作。这种假定可能不总是真实的，因为实际不可能保持一个保密密钥(需要来解密某些信息内容字段)不被泄露。如果发生这种泄露，黑客能够产生针对相同信息内容字段的一个新的信息内容权力，而且具有比原始信息内容权力少的限制。通常，该信息内容供应商可能不喜爱任何人都能够创建信息内容权力的构思，因为这种构思使得任何信息内容都有可能进入该系统。

解决上述问题的最佳方式是，信息内容供应商数字地签名信息内容权力。而且必须确保(顺应性)装置核查关于信息内容权力的签字并且仅接受由该内容供应商正确签名的信息内容权力。因此，装置必须知道该信息内容供应商的(根)公共密钥。当然不强制信息内容权力被签名。

此方法的一个附加优点是，该顺应性装置必须知道的公共密钥（根）很少。在其它内容当中，一个顺应性装置必须知道用户权力的发行人的公共密钥(根)、设备顺从管理器和命名权限。这些值将必须按照某些方式存储在该装置中。但是，如果内容权力由该信息内容供应商签名，这些公共密钥则能够被简单地添加到该信息内容权力。装置必须知道的只是该信息内容供应商的(根)公共密钥。以此方式，该信息内容供应商能够确定谁被授权来发放用户权力、一致鉴证和命名鉴证。

而且，能够把关于何处检测鉴证撤销信息的信息添加到信息内容权力。黑客不能改变全部在该内容权力中的附加信息，因为一个有效的信息内容权力必须由该信息内容供应商数字签名。

只允许用正式信息内容供应商的专用密钥签名的信息内容权力表示为 CP 作品，用于安全地把信息内容引入到来自 CP 的系统。但是，如果用户想把个人信息内容(如个人照片或最后假期的家庭图像记录)引入到该系统中，则应该首先包括 CP，以便创建该要求的信息内容权力。这是一个不期望的情形，因为 CP 不应该具有控制个人内容的能力。因此为了允许个人内容在该系统中的第一步骤是允许信息内容权力由除该 CP 之外的其他人签名。

引入的第一个规则是，不是由 CP 发放的该信息内容权力必须由一个顺应性装置签名。如果情况不是这样，则该内容权力将被想使用这些权力的任何(顺应性)装置拒绝。这意味着该个人信息内容只能通过一个顺应性装置进入该系统。这样的一个顺应性装置将进一步核查在该信息内容中不存在水印。加水印的内容是原始来自 CP，因此不允许用户创建他们自己的针对这种内容的信息内容权力。

该解决方案迄今为止表现还不是十分安全的，由于它允许一个通常的攻击。假设一个用户已经针对自制的信息内容的确定字段创建了一个信息内容权力。一个恶意的用户能够在实现该信息内容权力之后，(并且因此在顺应性装置对其签名之后)利用信息内容的另一字段替代该信息内容！ 因此他不得不以在核准的信息内容权力中的该信息内容密钥(重新)加密该(非法)信息内容，并且给予这一信息内容与被实现信息内容权力的自制的信息内容相同的标识符。如果用相同的(泄漏的)信息内容密钥加密，则有大量非法内容进入该系统。

为了解决这一问题，必须在一个信息内容权力和信息内容的实际字段之间有一种安全的链接。信息内容的指纹用途能够提供这种链接。一个信息内容选项的指纹是相关的信息信号的一种表示形式，在该信息内容选项稍加修改时不改变。这种指纹有时也称之为"(强壮)散列"（robust hashes）。强壮散列是指一个散列函数，在一定程度上相对于例如由于压缩/解压缩、编码、AD/DA 转换等数据处理和信号恶化是强壮的。强壮散列有时也称为强壮概要、强壮签名或感觉散列。产生一个指纹的方法的示例在国际专利申请 WO02/065782(代理人卷号 PHNL010110)中公开。

一个信息内容权力将包括某些额外信息，说明在该信息内容的什么确切部分能够找到什么指纹。所以，不添加全部信息内容(将是大

量的数据)的字段的指纹信息，就能够添加在确定的具体时间点的指纹信息(连同这些时间值)。在签名该信息内容权力之前，该顺应性装置把这一指纹信息添加到信息内容权力中。当使用一个内容权力时(例如播放信息内容)，该顺应性装置必须核查包含在该信息内容权力中的该指纹数据是否还可以在该实际信息内容(在指示的时间点)发现。如果不能找到，则该信息内容权力必须被拒绝。

总结，本实施例包括如下内容:

来自"官方"内容供应商 CP 的信息内容必须被加水印，并且信息内容权力必须包括有关他们链接的该信息内容的指纹信息。

当针对个人信息内容的信息内容权力被建立时，顺应性装置(或信息内容/业务供应商)必须核查没有水印出现的情况。

顺应性装置必须在签名一个新的信息内容权力之前，把指纹信息添加到一个新信息内容权力(用于个人信息内容)。

想使用信息内容权力的顺应性装置必须核查在该信息内容权力中的指纹信息是否与该实际信息内容匹配。

象在原始系统中一样，一个信息内容权力的创建者确定什么用户权力发行人的公共密钥(根)、命名权限和装置顺从管理器必须被查验，以便接入该信息内容。所以一个用户能授权任何当事人(包括自己或他自己的装置)来发放针对他个人信息内容的伴随用户权力。

具有信息内容的输入装置签名指纹信息的构思与国际专利申请序列号 PCT/IB03/00803(代理人卷号 PHNL020246)中的构思紧密匹配。但是，本发明的技术方案更具体，并且在官方信息内容与内容供应商(加水印的)和个人信息内容之间作出一个清楚的区别。

在信息内容被加水印的情况中，如果一个顺应性装置具有由该官方内容提供者签名的适当的信息内容(其中该公用密钥已知)，则该顺应性装置将仅播放该信息内容。如果没有水印被检测，则该信息内容被分类为"个人信息内容"并且可由任何顺应性装置签名该伴随信息内容权力。

作为进一步的可选扩展，有可能在该域等级上"个性化或域化"信息内容权。如果该授权域未被在该信息内容权力中标识，则一般能够通过安排顺应性装置拒绝执行该操作来实现这种"个性化或域化"。这样，如果该信息内容权力标识"错误的"域(或根本没有域)，则

来自该授权域的人员将不能运用该信息内容权力。然而这种方案具有某些风险，给出该可能的巨量(有可能是数千万)的未来的顺应性装置：当一个装置被黑客攻击(并且未被十分快速撤销)，这将可能是在整个系统中的全部信息内容权力的泄露。

最好通过使用在授权域中的装置可用的一个对应解密密钥的一个加密密钥来加密该信息内容权力来实现这种个性化/域化。该解密密钥通常将可在标识装置中得到。该信息内容供应商利用如下的一个附加关键码 CREK(信息内容权力加密密钥)来加密信息内容权力：

E {CREK} [信息内容权力].

随后这一密钥将由全部域成员可用的公众域密钥(PDK)在其 ID 卡中加密(本信息内容供应商已经在从 ID 卡购买业务过程中获得这一密钥，因此能够使用该密钥)。该加密的 CREK 将与该信息内容权力连接：

E{PDK} [CREK]||E {CREK} [信息内容权力]

然后连同该信息内容一起送到用户(是否需要的话)。

如果假设全部标识装置(例如智能卡)都已经装载了该 SDK(私人(秘密)域密钥)，则在用户标识之后，该用于重放的协议可操作如下：

重放装置送到用户 ID 装置：

E{PDK} [CREK]||PK_Playback_device

用户 ID 装置通过利用 SDK 解密来检取 CREK，随后利用重放装置 PK_Playback_device 的公用密钥加密 CREK。

随后该用户 ID 装置发送到该重放装置：

E{PK_Playback_device} [CREK]

该重放装置现在可以检取该 CREK 并且随后解密该信息内容权力并且解密该信息内容。

总结而言，下列两表格列出不同的数据成分以及它们的功能。这些表格仅用于说明的目的而不是详尽的说明的。表格 1 列出系统功能以及对应的数据成分。

数据成分	管理功能	机制
内容权力	装置顺从强制	仅分配内容权力到顺从装置
用户权力	权力管理	仅分配用户权力到

		付费用户
域鉴证	(授权)域管理	确定谁属于一个域
用户 ID	用户标识	标识用户的安全方式

表格 2 列出数据成分、它们的功能和信息内容。这些功能的多个当然是可选的。

	位置	功能	管理	管理
内容权力	- 用于全球接入的全球 - 在更新内容 权力情况下的个人 - 用于附加安全的域化	指示接入内容的规则并包含接入内容的密钥	- 包含签字的日期字段。用于分配“最新的”日期到装置和 ID 卡 - 可以包含用于用户权利的白清单	- 可以包含用于用户 ID 的撤销管理
使用鉴证	全球	表明可以“使用”一个/哪个内容权力的用户(全球或个人)>在内容权力中的哪个日期	- 可以包含签名的新日期 - 可以包含更新的域鉴证(将自动地分配)	- 可以包含针对用户鉴证的撤销 - 可以包含针对域鉴证的撤销
域鉴证	全球	指示家庭成员	具有有效的日期:过期之后必须被更新	- 可以包含针对用户鉴证的撤销
用户鉴证	在 ID 卡的用户中	指示一个用户;	具有有效的日期:	- 可以包含针对使

（生物数据）		可以附加地存储其它数据	过期之后必须被更新	用鉴证的撤销

现将讨论发明人目前考虑的实现本发明的最佳方式的一个实例。该系统的实现使用这SPKI/SDSI结构。参见SPKI Certificate Theory(Internet RFC 2693)和Carl Ellison的文章"Improvements on Conventional PKI wisdom"(2002年4月第一届年度PKI研究研讨会)。在X.509框架之内实施也被认为是可能的。

假定每一实体都保持其自己的公用/专用密钥对儿。公用和专用密钥将以符号PK和SK分别指示。

一个SPKI命名鉴证被表示为一个4元组(K，A，S，V)：

K = 发行人的公共密钥

A = 本地名称被定义

S = 鉴证的目标

V = 有效规定

一个SPKI授权鉴证被表示为一个5元组(K，S，D，T，V)：

K= 发行人的公共密钥

S = 鉴证的目标

D = 代表群组比特

T = 规定被授权的权限的标记

V = 有效规定

如果该代表群组比特被设置为真实，则目标可以进一步代表对于其它密钥和命名的许可(在该标记中规定)。

能够通过让某些中心权限发布SPKI命名鉴证来形成一个授权域，该SPKI命名鉴证把人员的公共密钥束联到一个官方唯一标识符(例如名称和地址信息)。这种其中"寻址权限"AA是提供接入到人"P1"的一个鉴证(SPKI形式)的一个实例：Cert1=SK_AA{(K，A，S，V)}指的是由SKAA(即寻址权限的专用密钥)签名的一个4元组，其中：

K=PK_AA

A = 街道地址和号码

S =PK_P1

注意，为了简化起见，这里省去了有效性规定。它们应该被选择与撤销和再更新能力系统一致。

一种可选方案是仅按照单一域鉴证分组在授权域中的所有的人的 PK。这样做具有的附加优点是只需要一个域鉴证。这样的一个鉴证的示例是 Cert1b=SK_AA{(K，A，S，V)}，指的是由 SKAA 签名的一个 4 元组(即域权限的专用密钥)，其中:

K = PK_AA

A = 家庭鉴证

S = PK_P1，PK_P2，PK_P3，...

其中假设一个信息内容权力 CR1 控制了为了播放信息内容的一个确定字段所需的规则和密钥。一个信息内容持有者 CO1 能够通过发放下列鉴证来授权个人 P1: Cert2 =SK_CO1 {(K，S，D，T，V)} 具有:

K = PK_CO1

S = PK_P1

D = 伪

T = CR1

在鉴证 Cert2 中的代表比特 D 被设置为"伪"，这表明不允许该用户代表对于另一用户的用户权力(信息内容权力 CR1 的用户权力)。如果该代表比特被设置为"真"，则人员 P1 被允许代表该权限。整个系统能够被设计成使得顺应性装置仍然容许在同一个系统中的其它用户(被授权)使用 CR1 并且播放该信息内容选项。在此情况中的代表比特防止权力对授权域之外部的散布。

用户可以通过一个装置来使用信息内容。如果用户拥有鉴证的正确设置，则一个顺应性装置将仅提供接入(利用在内容权力中的密钥解密该信息内容)。注意，如果没有授权用户，则可能该装置将甚至不能获得一个信息内容权力!

能够从网络上的任意位置检取属于一个用户的鉴证，或储存在用户的智能卡上。信息内容权力也可以存储在该智能卡上。这是在脱机装置上播放信息内容所需要的。允许信息内容权力存储在可通过网络

接入的用户的信任代理上将可能是有益的。用这种方法，用户仍然能够检取没有储存在其智能卡并且不能在网络其它地方得到的信息内容权力。

下面列出在实施该解决方案时可能需要(或有用)的一个鉴证中的某些字段。该列表只显示除以前提到的标准 SPKI 鉴证字段以外的一些字段：签名日期

其上被签署了鉴定的装置标识符(有助于装置的名誉信息的收集，该名誉信息能够导致在装置顺从子系统中的撤销)

复制一次/从不复制/不进一步复制以及类似的标志

撤销系统的位置/服务器

应当指出，上述实施例说明了而不是限制了本发明并且本领域技术人员将能够设计许多替换实施例而不偏离附加权利要求的范围。

在权利要求中，位于括弧之间的任何附图标记不应该被解释为限制该权利要求。单词 "包括 "不排除除了在权利要求中列出的那些之外的元件或步骤的存在。在一个元件前面使用冠词 "一个 "不排除多个这种元件的存在。依靠包括一些分离元件的硬件，以及依靠一个适当编程的计算机，都能够实现本发明。

在列举一些装置的设备权利要求中，这些装置的一些可以被具体化为完全一样硬件零件。在相互不同的从属权利要求中叙述的某些措施的起码事实不表示这些措施的组合不能被用来优化。

总之，本发明提供了方法和装置(D1)，用于根据一个用户权力(UR1)授权由第一用户(P2)请求的对于一个信息内容选项(C1)的操作。该用户权力可以标识第一用户或第二用户(P1)并且授权当事的用户来执行对于该信息内容选项的请求的操作。如果用户权力标识该第二用户，则在收到链接该第一用户的用户权力和第二用户的用户权力的信息之时授权该操作。该信息最好包括标识同一个授权与域(AD)的作为成员的第一和第二用户的一个或多个域鉴证(DC1、DC2)。最好使用实现该操作的一个信息内容权力(CR1)，从而该用户权力将授权该第二用户采用该信息内容权力。

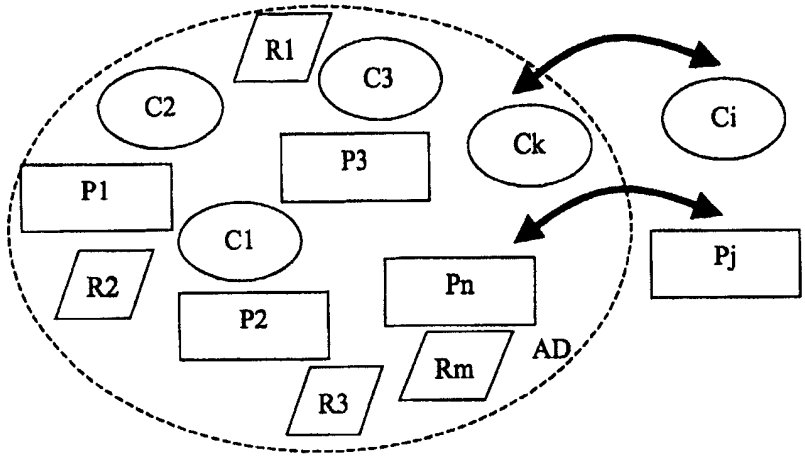

R1
C3
C2
Ci
Ck
P3
P1
C1
Pj
R2
Pn
P2
AD
Rm
R3

图 1

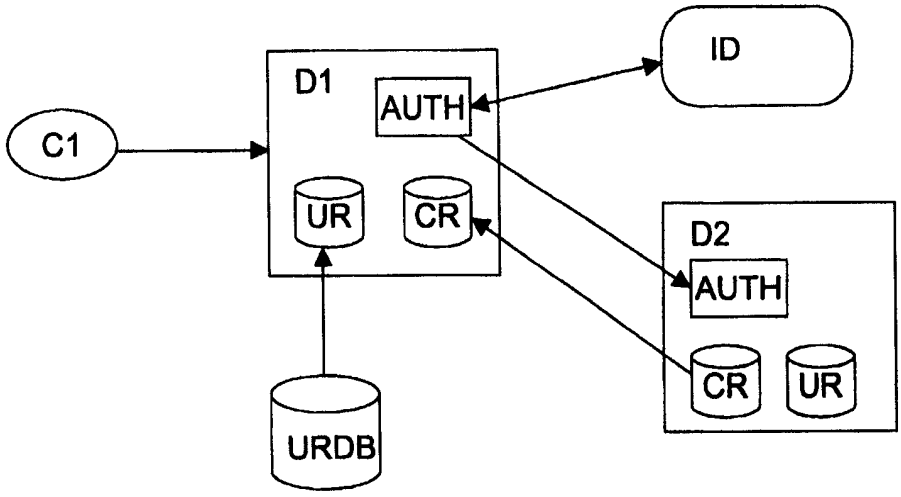

ID
D1
AUTH
C1
UR
CR
D2
AUTH
CR
UR
URDB

图 2

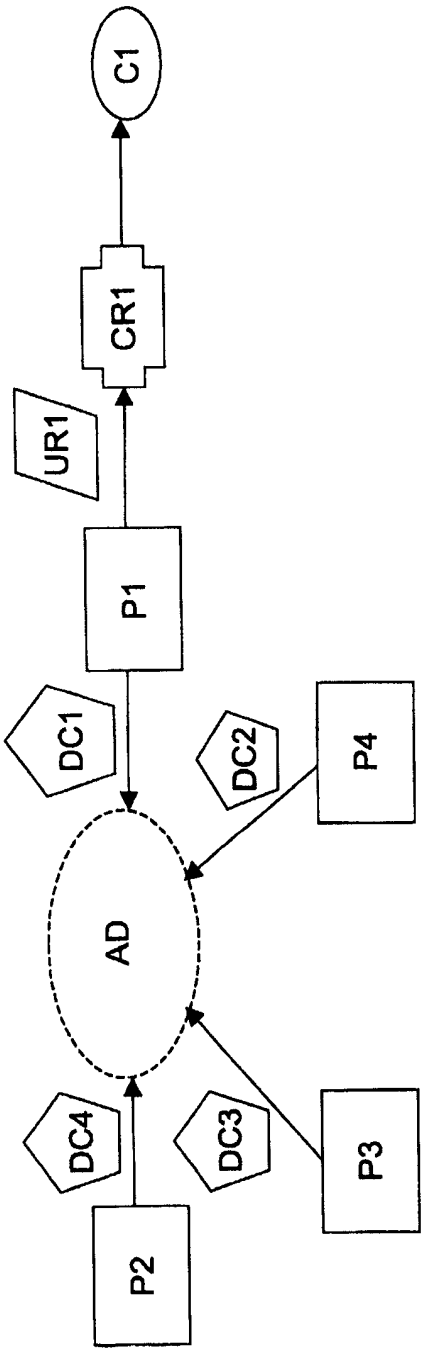


图 3