



[12] 发明专利申请公开说明书

[21] 申请号 200410005381.9

[43] 公开日 2004 年 8 月 18 日

[11] 公开号 CN 1521980A

[22] 申请日 2004. 2. 11

[21] 申请号 200410005381.9

[30] 优先权

[32] 2003. 2. 11 [33] US [31] 10/364, 627

[71] 申请人 微软公司

地址 美国华盛顿州

[72] 发明人 A · 纳林 C · 文卡特施
F · D · 比鲁姆 M · A · 德米罗
P · D · 瓦科斯曼 P · 马里克
R · U · 马拉维亚拉奇切
S · 包尔尼 V · 科里什纳斯瓦米
Y · (E) 罗森菲尔德

[74] 专利代理机构 上海专利商标事务所

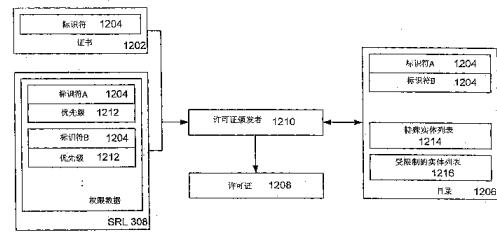
代理人 李家麟

权利要求书 5 页 说明书 37 页 附图 16 页

[54] 发明名称 按照数据权限管理(DRM)系统在一个定义域诸如—组织内发行数字内容

[57] 摘要

许可证颁发者从请求者接收一个请求，包括标识请求者的标识符和与数字内容关联的权限数据，在其中权限数据列出至少一个标识符和与其关联的权限。之后许可证颁发者在一目录中找到请求者的标识符，且在此基础上，在目录中找到请求者是其成员的每个组的标识符。将找到的请求者标识符的每一个和每个找到的组标识符与在权限数据中的每个标识符比较，以找到一个匹配，以及向请求者发布带有与匹配标识符关联的权限的许可证以再现内容。



1. 一种方法，用于许可证颁发者向一个请求者发布数字许可证，以允许请求者再现相应的数字内容，许可证颁发者可以访问一个包括用于请求者的列表的目录，列表包括请求者的标识符和请求者是其成员的每个组的标识符，所述方法包括：

从请求者接收请求，请求包括标识请求者的标识符和与内容关联的权限数据，权限数据列出至少一个标识符和与其关联的权限；

在目录中找到请求者的标识符；

根据在目录中找到的请求者标识符，在目录中找到请求者是其成员的每个组的标识符；

将找到的请求者标识符的每一个和每个找到的组标识符与在权限数据中的每个标识符比较，以找到一个匹配；以及

向请求者发布带有与匹配标识符关联的权限的许可证。

2. 如权利要求 1 所述的方法包括，从请求者接收一个请求包括，带有识别请求者的标识符的数字证书。

3. 如权利要求 1 所述的方法包括，从请求者接收一个请求包括，带有基于以上的数字签名的权限数据。

4. 如权利要求 3 所述的方法，还包括，验证数字签名。

5. 如权利要求 1 所述的方法包括：

对于每个找到的请求者标识符和每个找到的组标识符：

将这样的标识符与在权限数据中列出的每个标识符比较；以及

注意被比较的标识符是否是一个匹配标识符；

产生至少两个匹配标识符；

选择匹配标识符中的一个；以及

向请求者发布带有与选择的匹配标识符关联的权限的许可证。

6. 如权利要求 5 所述的方法包括，选择向请求者传送最大量权限的匹配标识符。

7. 如权利要求 5 所述的方法，其特征在于，在权限数据中的每个标识符具有一相应的优先级标记，所述方法包括，选择具有最高优先级标记的匹配标识符。

8. 一个具有存储在其上的计算机可执行指令的计算机可读媒体，所述指令用于执行一种方法，用于许可证颁发者向请求者发布数字许可证，以允许请求者再现相应的数字内容，许可证颁发者可以访问包括用于请求者的列表的目录，列表包括请求者的标识符和请求者是其成员的每个组的标识符，所述方法包括：

从请求者接收请求，请求包括标识请求者的标识符和与内容关联的权限数据，权限数据列出至少一个标识符和与其关联的权限；

在目录中找到请求者的标识符；

根据在目录中找到的请求者标识符，在目录中找到请求者是其成员的每个组的标识符；

将找到的请求者标识符的每一个和每个找到的组标识符与在权限数据中的每个标识符比较，以找到一个匹配；以及

向请求者发布带有与匹配标识符关联的权限的许可证。

9. 如权利要求 8 所述的媒体，其特征在于，所述方法包括，从请求者接收一个请求包括，一个带有识别请求者的标识符的数字证书。

10. 如权利要求 8 所述的媒体，其特征在于，所述方法包括，从请求者接收一个请求包括，带有一个基于以上的数字签名的权限数据。

11. 如权利要求 10 所述的媒体，其特征在于，所述方法包括，验证数字签名。

12. 如权利要求 8 所述的媒体，所述方法包括：

对于每个找到的请求者标识符和每个找到的组标识符：

将这样的标识符与在权限数据中列出的每个标识符比较；以及

注意被比较的标识符是否是一个匹配标识符；

产生至少两个匹配标识符；

选择匹配标识符中的一个；以及

向请求者发布带有与选择的匹配标识符关联的权限的许可证。

13. 如权利要求 12 所述的媒体，其特征在于，所述方法包括，选择向请求者传送最大量权限的匹配标识符。

14. 如权利要求 12 所述的媒体，其特征在于，在权限数据中的每个标识符具有相应的优先级标记，所述方法包括，选择具有最高优先级标记的匹配标识符。

15. 一种方法，用于许可证颁发者向请求者发布数字许可证，以允许请求者再现相应的数字内容，请求者是一个组的成员，所述方法包括：

从请求者接收一个请求，请求包括一标识组的标识符和与内容关联的权限数据，权限数据列出至少一个标识符和与其关联的权限；

将来自请求者的组标识符与在权限数据中的每个标识符比较，以找到一个匹配；以及

向请求者发布带有与匹配的组标识符关联的权限的许可证，发布的许可证包括相应于按照组的公用密钥加密的内容的内容密钥，由此请求者用相应于组的公用密钥的组的私有密钥能够获得内容密钥。

16. 如权利要求 15 所述的方法包括，从请求者接收一个请求包括，一个带有识别组的标识符的数字证书。

17. 如权利要求 15 所述的方法包括，从请求者接收一个请求包括，带有一基于以上的数字签名的权限数据。

18. 如权利要求 17 所述的方法包括，验证数字签名。

19. 如权利要求 15 所述的方法，其特征在于，许可证颁发者可以访问一个包括用于组的列表的目录，列表包括组的标识符和组的每个成员的标识符，所述方法还包括：

从每个请求者接收其标识符；

在目录中基于组的标识符找到用于组的列表；以及

验证在目录找到的用于组的列表包括请求者的标识符。

20. 一个具有存储在其上的计算机可执行指令的计算机可读媒体，所述指令用于执行一种方法，用于许可证颁发者向请求者发布数字许可证，以允许请求者再现相应的数字内容，请求者是一个组的成员，所述方法包括：

从请求者接收一个请求，请求包括一标识组的标识符和与内容关联的权限数据，权限数据列出至少一个标识符和与其关联的权限；

将来自请求者的组标识符与在权限数据中的每个标识符比较，以找到一个匹配；以及

向请求者发布带有与匹配的组标识符关联的权限的许可证，发布的许可证包括一相应于按照组的公用密钥加密的内容的内容密钥，由此请求者用相应于组的公用密钥的组的私有密钥能够获得内容密钥。

21. 如权利要求 20 所述的媒体，所述方法包括，从请求者接收一个请求包

括，一个带有识别组的标识符的数字证书。

22. 如权利要求 20 所述的媒体，其特征在于，所述方法包括，从请求者接收一个请求包括，带有一个基于以上的数字签名的权限数据。

23. 如权利要求 22 所述的媒体，其特征在于，所述方法包括，验证数字签名。

24. 如权利要求 20 所述的媒体，其特征在于，许可证颁发者可以访问一个包括用于组的列表的目录，列表包括组的标识符和组的每个成员的标识符，所述方法还包括：

从请求者接收其标识符；

在目录中基于组的标识符找到用于组的列表；以及

验证在目录找到的用于组的列表包括请求者的标识符。

25. 一种方法，用于许可证颁发者向请求者发布数字许可证，以允许请求者再现相应的数字内容，请求者是一组的成员，许可证颁发者可以访问一个包括用于组的列表的目录，列表包括组的每个成员的标识符，所述方法包括：

从请求者接收一个请求，所述请求包括标识所述组的标识符，标识请求者的标识符，和关联于内容的权限数据，权限数据列出至少一个标识符及其关联的权限；

将来自请求者的组标识符与在权限数据中的每个标识符比较，以找到一个匹配；

在目录中基于组的标识符找到用于组的列表；

从找到的列表中验证其中包括请求者的标识符；以及

向请求者发布带有与匹配的组标识符关联的权限的许可证，发布的许可证包括一个相应于按照请求者的公用密钥加密的内容的内容密钥，由此请求者用相应于请求者的公用密钥的组的私有密钥能够获得内容密钥。

26. 如权利要求 25 所述的方法包括，从请求者接收一个请求包括，一个带有识别组的标识符的数字证书。

27. 如权利要求 25 所述的方法包括，从请求者接收一个请求包括，一个带有识别请求者的标识符的数字证书。

28. 如权利要求 27 所述的方法，还包括，从数字证书中获得请求者的公用密钥。

29. 如权利要求 25 所述的方法包括，从请求者接收一个请求包括，带有一

个基于以上的数字签名的权限数据。

30. 如权利要求 29 所述的方法还包括，验证数字签名。

31. 如权利要求 25 所述的方法，还包括，从一文件上的数字证书获得请求者的公用密钥，所述数字证书包括请求者的标识符。

32. 一个具有存储在其上的计算机可执行指令的计算机可读媒体，所述指令用于执行一种方法，用于许可证颁发者向请求者发布数字许可证，以允许请求者再现相应的数字内容，请求者是一个组的成员，许可证颁发者可以访问一个包括用于组的列表的目录，列表包括组的每个成员的标识符，所述方法包括：

从请求者接收一请求，所述请求包括标识所述组的标识符，一标识请求者的标识符，和关联于内容的权限数据，权限数据列出至少一个标识符及其关联的权限；

将来自请求者的组标识符与在权限数据中的每个标识符比较，以找到一个匹配；

在目录中基于组的标识符找到用于组的列表；

从找到的列表中验证在其中包括请求者的标识符；以及

向请求者发布带有与匹配的组标识符关联的权限的许可证，发布的许可证包括一个相应于按照请求者的公用密钥加密的内容的内容密钥，由此请求者用相应于请求者的公用密钥的组的私有密钥能够获得内容密钥。

33. 如权利要求 32 所述的媒体，其特征在于，所述方法包括，从请求者接收一个请求包括，一个带有识别组的标识符的数字证书。

34. 如权利要求 32 所述的媒体，其特征在于，所述方法包括，从请求者接收一个请求包括，一个带有识别请求者的标识符的数字证书。

35. 如权利要求 34 所述的媒体，其特征在于，所述方法还包括，从数字证书中获得请求者的公用密钥。

36. 如权利要求 32 所述的媒体，其特征在于，所述方法包括，从请求者接收一个请求包括，带有一个基于以上的数字签名的权限数据。

37. 如权利要求 36 所述的媒体，其特征在于，所述方法还包括，验证数字签名。

38. 如权利要求 32 所述的媒体，其特征在于，所述方法还包括，从一个文件上的数字证书获得请求者的公用密钥，所述数字证书包括请求者的标识符。

按照数据权限管理(DRM)系统在一个
定义域诸如一组织内发行数字内容

对相关申请的交叉参考

下面的美国专利申请揭示涉及本申请的主题的主题，并因此通过引用将它们整体包括在此：

美国专利申请 No. ___, 与本发明同时在代理人摘要编号(attorney docket number) MSFT-1569 下申请的，且标题为“Publishing Digital Content Within a Defined Universe Such As an Organization in Accordance with a Digital Rights Management (DRM) System”；

美国专利申请 No. 10/185, 527, 在代理人摘要编号 MSFT-1330 下于 2002 年 6 月 28 日申请的，且标题为“Obtaining a Signed Rights Label (SRL) for Digital Content and Obtaining a Digital License Corresponding to the Content Based on the SRL in a Digital Rights Mangement System”；

美国专利申请 No. 10/185, 278, 在代理人摘要编号 MSFT-1333 下于 2002 年 6 月 28 日申请的，且标题为“Using a Rights Template to Obtain a Signed Rights Label (SRL) for Digital Content in a Digtial Rights Management System”；以及

美国专利申请 No. 10/185, 511, 在代理人摘要编号 MSFT-1343 下于 2002 年 6 月 28 日申请的，且标题为“Systems And Methods For Issuing Usage Licenses For Digital Content And Services”。

技术领域

本发明涉及数据权限管理(DRM)系统。更具体地说，本发明涉及使用 DRM 系统在诸如组织、办公室、公司等等定义域内发行数字内容，因此在这个域内可按照相应的使用或许可条款约束内容的再现和使用。

背景技术

在数字内容诸如数字音频、数字视频、数字文本、数字数据、数字多媒体

等方面，在其中这样的数字内容要被分发至一或多个用户，数据权限管理和实施是非常需要的。数字内容可能是静态的，诸如文本文档，或者它可能是被流化的，诸如流化的实况转播事件的音频/视频。典型的分发模式包括有形的设备诸如磁(软)盘、磁带、光(激光)盘(CD)等，和无形的媒体诸如电子公告板、电子网络、因特网等。在由用户接收时，这样的用户在适当的再现设备诸如个人计算机等等上的媒体播放器再现或‘播放’数字内容。

在一个情景中，内容所有者或权限所有者诸如作者、发行人、广播员等，想要将这样的数字内容分发给许多用户或接受者的每一个以交换许可费或一些其它的费用。那么，在这样的情景中，内容可能是歌曲、歌曲集、电影等，而分发的目的是产生许可费。如果让这样的内容所有者选择，很可能想要对用户能够对这样被分发的数字内容能做什么进行限制。例如，内容所有者意欲限制用户复制和重新分发这样的内容至第二个用户，至少是在这样的第二个用户向拒绝内容所有者许可费时。

另外，内容所有者可能想要为用户提供以不同许可费购买不同类型的用户许可的灵活性，而同时使用户遵守实际购买的无论什么类型的许可的条款。例如，内容所有者可能想要允许被分发的数字内容只被播放有限的次数，只被播放某个总的时间，只在某种类型的机器上播放，只在某种类型的媒体播放器上播放，只由某种类型的用户播放。

在另一个情景中，诸如在一组织内的职工或组织的成员想要将这样的数字内容分发给组织内的其它职工或成员或者分发给组织外的其它个人，但内容开发者，往往欲阻止其它人再现这个内容。这里，内容的分发与以机密的或限制的方式共享基于组织的内容非常相似，而与以交换许可费或一些其它报酬的无限的(broad-based)分发相反。

在这样的情景中，内容可能是文档报告、电子表格、数据库、电子邮件等等，诸如在办公室环境内可被交流的，以及内容开发者可能想要确保内容保持在组织或办公室环境内并且不被未经授权的个人诸如例如竞争者或对手再现。再一次，这样内容开发者想要对接受者能够对这样被分发的数字内容所做的事进行限制。例如，内容所有者意欲限制用户，复制和重新分发这样的内容至第二个用户，至少是在被允许再现内容的个人范围之外暴露内容时。

此外，内容开发者可能想要为各种接受者提供不同级别的再现权限。例如，内容开发者可能想要允许受保护的数字内容相对于一类个人可被观看而不可

被打印，并且相对于另一类个人可被观看且可被打印。

不过，在任一情景中，在分发已经发生后，这样的内容所有者/开发者即使对数字内容有控制也只具有很少的控制。实际上任何个人计算机包括制作这样的数字内容的准确的数字拷贝所需的软件和硬件，和将这样准确的数字拷贝下载至可写的磁或光盘所需的软件和硬件，以及通过网络诸如因特网将这样准确的数字拷贝送到任何目的地所需的软件和硬件，所以这特别成问题。

当然，作为分发内容的交易的一部分，内容所有者/开发者可能要求数字内容的用户/接受者承诺不以讨厌的方式重新分发这样的数字内容。然而，这样的承诺很容易作出也很容易打破。内容所有者/开发者可能试图通过几种已知的通常包括加密和解密的安全设备阻止这样的重新分发。但是，要阻止适当地被确定的用户不解密被加密的数字内容，以非加密的形式保存这样的数字内容，然后重新分发同一数字内容，其存在的可能性非常小。

于是，存在一种需求，用于提供数据权限管理(DRM)和实施结构和方法，允许受控制地再现或播放任意形式的数字内容，在其中该控制是灵活的且可由这样的数字内容的内容所有者/开发者定义的。更明确地说，存在对这样一种结构的需求，该结构允许和促进这样的受控制的再现，特别是在办公室或组织环境等等中，在其中文档要在规定的一组个人或一类个人中共享。

概述

至少部分地由本发明满足上述需求，在本发明中，许可证颁发者向请求者发布允许请求者再现相应的数字内容的数字许可证。在本发明中，许可证颁发者可以使用一个包括请求者的列表的目录，在其中这个列表包括请求者的标识符和请求者是其成员的每个组的标识符。

许可证颁发者从请求者接收一个请求，在其中该请求包括一标识请求者的标识符以及与内容关联的权限数据，且在其中权限数据列出至少一标识符和与其关联的权限。许可证颁发者之后在目录中找到请求者的标识符，以及由在目录中被找到的请求者标识符，在目录中找到请求者是其成员的每个组的标识符。将每个被找到的请求者标识符和每个被找到的组标识符，与在权限数据中列出的每个标识符比较，以找到一个匹配，以及向请求者发布带有与匹配的标识符关联的权限的许可证。

附图说明

结合附图阅读时将更好地理解前面的概述，以及后面本发明实施例的详细说明。为了例示本发明，在附图中所示的实施例目前是较佳的。不过，如应该理解的，本发明不受限于所示的精确安排和工具。在附图中：

图 1 是一表示典型的非限制的计算环境的方框图，在该环境中可实现本发明；

图 2 是一表示具有各种计算设备的典型网络环境的方框图，在该环境中可实现本发明；

图 3 是按照本发明的系统和方法的一个实施例的功能方框图，用于发行数字内容；

图 4 是按照本发明的方法的一个实施例的流程图，用于发行权限管理的数字内容；

图 4A 是一方框图，示出如由图 4 的方法产生的签署的权限标签的结构；

图 5 是按照本发明的系统和方法的一个实施例的方框图，用于许可权限管理的数字内容；

图 6A 和 6B 是按照本发明的方法的一个实施例的流程图，用于许可权限管理的数字内容；

图 7 是一流程图，示出按照本发明的一个实施例在重新发行一权限标签时所执行的关键步骤；

图 8 是一方框图，示出按照本发明的一个实施例的一证书，它由一 DRM 服务器发布，以允许用户执行离线发行；

图 9 是一方框图，示出按照本发明的一个实施例的一权限模板，指定要被结合到一权限标签中的信息；

图 10 是一流程图，示出按照本发明的一个实施例，在创建图 9 的权限模板和基于权限模板创建图 4A 的签署的权限标签的时候所执行的关键步骤；

图 11 是一方框图，示出基于信任的系统的实例的实施结构；

图 12 是一方框图，示出按照本发明的一个实施例的处理对一许可证的请求的许可证颁发者；

图 13 是一流程图，示出由图 12 的许可证颁发者在发布许可证时所执行的与一目录有关的步骤；以及

图 14 是一流程图，示出由图 12 的许可证颁发者在将政策插入一要被发行

的许可证中时所执行的步骤。

详细说明

图 1 和下面的讨论旨在提供一合适的计算环境的简要概括的说明，在该环境中可实现本发明。不过，应该理解，手持的、便携的和其它所有种类的计算设备被预期结合于本发明使用。尽管下面描述是通用计算机，但是这只是一个实例，并且本发明只要求具有网络服务器互操作性和交互性的瘦客户机。因而，可在一网络化主机化服务的环境中实现本发明，在该环境中，包含非常少或最小程度的客户机资源，例如，一个在其中客户机设备只用作为对于万维网的浏览器或接口的网络化环境。

尽管不要求，但可通过由开发者使用的应用编程接口 (API) 实现本发明，和/或将本发明包括在网络浏览软件内，将在计算机可执行指令诸如程序模块的一般背景中描述网络浏览软件，由一或多个计算机诸如客户工作站、服务器或其它设备执行。通常，程序模块包括执行特定任务或实现特定的抽象数据类型的例程、程序、对象、组件、数据结构等等。一般地，可将程序模块的功能按要求结合或分发到各种实施例中。而且，本领域熟练技术人员将意识到，可用其它计算机系统配置实施本发明。其它可能适合于本发明使用的知名的计算系统、环境和/或配置包括，但不限于，个人计算机 (PC)、自动出纳机 (automated teller machine)、服务器计算机、手持或膝上型设备、多处理器系统、基于微处理器的系统、可编程消费电子产品、网络 PC、小型机、大型机等等。还可分布式计算环境中实施本发明，在该环境中，由通过通信网络或其它数据传输媒体连接的远程处理设备执行任务。在一分布式环境中，可将程序模块放在包括存储器设备的本地或远程计算机存储媒体两者之中。

图 1 这样示出一合适的计算系统环境 100 的实例，在该环境中可实现本发明，尽管如上面清楚地说明的，计算系统环境 100 只是合适的计算系统环境的一个实例，而非意指关于本发明的使用或功能的范围的任何限制。也不应该将计算环境 100 解释为具有与在典型操作环境 100 中所示的组件的任何一个或组合有关的任何依赖性或要求。

参考图 1，用于实现本发明的典型系统包括一以计算机 110 形式的通用计算设备。计算机 110 的组件可包括，但不限于，处理单元 120，系统存储器 130，和将各种系统组件包括系统存储器在内连接至处理单元 120 的系统总线 121。

系统总线 121 可以是几种类型总线结构的任何一种，包括使用各种总线结构的存储器总线或存储控制器，外部设备总线，和局部总线。作为实例，但不限制，这样结构包括工业标准结构 (ISA) 总线、微通道结构 (MCA) 总线、增强 ISA (EISA) 总线、视频电子标准协会 (VESA) 局部总线、以及周边元件互连 (PCI) 总线（也被称为夹层 (Mezzanine) 总线）。

计算机 110 一般包括多种多样的计算机可读媒体。计算机可读媒体可以是能够由计算机 110 存取的任何可用媒体，并包括易失的或非易失的媒体，可移动的和不可移动的媒体。作为例子，不是限制，计算机可读媒体可包括计算机存储媒体和通信媒体。计算机存储媒体包括易失的和非易失的、可移动的和不可移动的媒体两者，它们是以任何用于存储信息诸如计算机可读指令、数据结构、程序模块或其它数据的方法和技术实现的。计算机存储媒体的实例包括，但不限于，RAM(随机存取存储器)、ROM(只读存储器)、EEPROM(电可擦除可编程只读存储器)、闪存或其它存储技术、CD-ROM(光盘)、数字通用盘(DVD)或其它光盘存储器、磁盒、磁带、磁盘存储器或其它磁存储设备，或者可能被用于存储想要的信息和能由计算机 110 存取的任何其它媒体。通信媒体一般包括计算机可读指令、数据结构、程序模块或其它数据，它们在调制的数据信号诸如载波或其它传输机制中，还包括任何信息传送媒体。术语“调制的数据信号”指具有以将信息编码在信号中的方式设置或改变的一或多个特征的信号。作为实例，但不是限制，通信媒体包括有线的媒体，诸如有线的网络或直接线连接，以及无线的媒体，诸如耦合器、RF(射频)和其它无线媒体。任何上述各项的组合应该也包括在计算机可读媒体的范围之内。

系统存储器 130 包括以易失的和/或非易失的存储器形式的计算机存储媒体，诸如只读存储器 (ROM) 131 和随机存取存储器 (RAM) 132。基本输入/输出系统 133 (BIOS)，包含帮助计算机 110 内部件之间传送信息的基本例程，诸如在起动期间，它一般被存储在 ROM 131 中。RAM 132 一般包含由处理单元 120 可直接存取和/或目前操作的数据和/或程序模块。作为例子，不是限制，图 1 示出操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137。

计算机 110 还可包括其它可移动的/不可移动的、易失的/非易失计算机存储媒体。只是作为例子，图 1 示出读写不可移动的、非易失的磁媒体的硬盘驱动器 141，读写可移动的、非易失的磁盘 152 的磁盘驱动器 151，和读写可移动的、非易失的光盘 156 诸如 CD ROM 或其它光媒体的光盘驱动器 155。能用于

典型操作环境的其它可移动的/不可移动的、易失的/非易失的计算机存储媒体包括，但不限于，磁带盒、闪存卡、数字通用盘、数字视频带、固态 ROM(solid state ROM)等等。硬盘驱动器 141 一般通过一不可移动的存储器接口诸如接口 140 连接至系统总线 121，以及磁盘驱动器 151 和光盘驱动器 155 一般由可移动的存储器接口诸如接口 150 连接至系统总线 121。

上面所述和在图 1 中所示的驱动器及其关联的计算机存储媒体，为计算机 110 提供计算机可读指令、数据结构、程序模块和其它数据的存储。在图 1 中，例如，硬盘驱动器 141 被示为存储操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147。注意这些组件可以与操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137 或者相同，或者不同。操作系统 144、应用程序 145、其它应用模块 146 和程序数据 147 在这里给出不同的编号，以说明在最低程度上它们是不同的拷贝。用户可通过输入设备，诸如键盘 162 和普通被称为鼠标的定点设备 161、轨迹球或触摸垫，将命令和信息输入到计算机 110 中。其它输入设备(未示出)可包括话筒、游戏杆、游戏垫、卫星天线等等。这些和其它输入设备常常通过连接到系统总线的用户输入接口 160 连接至处理单元 120，但是也可以通过其它接口和总线结构连接，诸如并行端口、游戏端口或通用串行总线(USB)。

显示器 191 或其它类型的显示设备也通过一个接口诸如视频接口 190 连接至系统总线 121。图形接口 182，诸如北桥(Northbridge)，也可连接至系统总线 121。北桥是一芯片组，与 CPU 或主机处理单元 120 通信，并承担加速图形接口(AGP)的通信职责。一或多个图形处理单元(GPU)184 可与图形接口 182 通信。在这点上，GPU184 一般包括芯片内的存储器，诸如寄存存储，且 GPU184 与视频存储器 186 通信。不过，GPU184 只是协处理器的一个实例，且因而多种多样的协处理器可包括在计算机 110 之内。显示器 191 或其它类型的显示设备也通过一个接口诸如视频接口 190 连接至系统总线 121。除显示器之外，计算机还可包括其它外部输出设备诸如扬声器 197 和打印机 196，它们可通过输出外部接口 195 连接。

计算机 110 可在一个使用逻辑连接至一或多个计算机诸如远程计算机 180 的网络化环境中运行。远程计算机 180 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其它普通网络节点，并且一般包括上面相对于计算机 110 所述的组件的许多或全部，尽管在图 1 中只示出存储器设备 181。图 1 中所示

的逻辑连接包括局域网 (LAN) 171 和广域网 (WAN) 173，还可包括其它网络。这样的网络环境在办公室、企业级计算机网络、企业内部互联网和因特网中是普通的。

当在 LAN 网络环境中使用时，计算机 110 通过网络接口或适配器 170 连接至 LAN171。当在 WAN 网络环境中使用时，计算机 110 一般包括调制解调器 172 或用于建立在 WAN173 诸如因特网上的通信的其它工具。调制解调器 172，可以是内置的或外置的，可通过用户输入接口 160 或其它适当的机制连接至系统总线 121。在网络化环境中，相对于计算机 110 所述的程序模块，或其一部分，可存储在远程存储器设备中。作为例子，不是限制，图 1 示出远程应用程序 185 为驻留在存储设备 181 上。将意识到所示的网络连接是典型的，并且可使用用于在计算机之间建立通信链路的其它方法。

本领域的一个普通熟练技术人员能意识到，计算机 100 或其它客户机设备能作为计算机网络配置的一部分。在这点上，本发明适合于任何具有出现在任意数量存储单元或卷上的任意数量应用程序和过程的计算机系统。本发明可应用于带有配置在一网络环境中的、具有远程或地存储的服务器计算机和客户计算机的环境。本发明也可应用于具有编程语言功能、解释和执行能力的独立的计算设备。

分布式计算促进通过计算设备和系统之间的直接交流共享计算机资源和服务。这些资源和服务包括信息交换、高速缓冲和用于文件的磁盘存储。分布式计算利用网络连接，允许客户机平衡其集体的能力以有利于整个企业。在这点上，多种多样的设备可具有应用程序、对象和资源，它们可交互以包含用于可信的图形流水线 (trusted graphics pipeline) 的本发明的认证技术。

图 2 提供一典型的网络化或分布式计算环境的示意图。这个分布式计算环境包括计算对象 10a、10b 等，以及计算对象或设备 110a、110b、110c 等。这些对象可包括程序、方法、数据存储、可编程逻辑等。这些对象可包括同一或不同设备诸如 PDA、电视、MP3 播放器、电视、个人计算机等的部分。每个对象经由通信网络 14 能与另一个对象通信。这个网络可自包含其它计算对象和计算设备，它们为图 2 的系统提供服务。按照本发明的一个方面，每个对象 10 或 110 可包含一个可请求用于可信的图形流水线的本发明的认证技术的应用程序。

还能意识到，一个对象诸如 110c 可以另一个计算设备 10 或 110 为主机。

这样，尽管所示的物理环境可将连接的设备示为计算机，这样的例示只是示范性，且可以可替换地包括各种数字设备诸如 PDA，电视，MP3 播放器等，软件对象如接口，COM 对象等来图示或描述这个物理环境。

存在各种各样支持分布式计算环境的系统、组件和网络配置。例如，计算系统可通过有线的或无线的系统、通过本地网络或广泛分布的网络连接在一起。目前，许多网络被连接到因特网，它提供广泛的分布式计算基础设施和包含许多不同的网络。

在家庭网络环境中，存在至少四个全异的网络传输媒体，它们每个可支持一唯一的协议，诸如电源线、数据(无线的或有线的两者)、语音(例如电话)和娱乐媒体(entertainment media)。大多数家庭控制设备诸如电灯开关和器具可使用电源线用于连接。数据服务可作为宽带(例如或者 DSL 或者线缆调制解调器)进入家庭，且在家庭中使用或者无线的(例如家用射频(HomeRF) 802.1.b)或者有线的(例如家用 PNA(Home PNA)、5 类线(Cat 5)甚至电源线)连接，数据服务是可访问的。语音业务可作为或者有线的(例如 3 类线(Cat 3))或者无线的(例如蜂窝电话)进入家庭，且可在家庭内使用 3 类配线分布语音业务。娱乐媒体可或者通过卫星或线缆进入家庭，且一般在家庭中使用同轴电缆分布娱乐媒体。IEEE1394 和 DVI 也可作为用于媒体设备群的数字互连出现。所有这些网络环境和可作为协议标准出现的其它环境，可互联以构成一内部互联网，它可经由因特网连接到外部世界。简而言之，多种多样全异的源存在，用于存储和传输数据，并且因此，在前进中，计算设备将要求在数据处理流水的所有部分保护内容的方法。

‘因特网(Internet)’一般指利用 TCP/IP 协议组的网络和网关的集合，在计算机网络领域中是众所周知的。TCP/IP 是“Transport Control Protocol/Interface Program(传输控制协议/接口程序)”的首字母缩写。因特网可被描述为在地理上分布式的由执行允许用户通过网络交互和共享信息的网络协议的计算机互连的远程计算机网络的系统。因为这样广泛的信息共享，远程网络诸如因特网因而已经很一般地卷入到开放系统中，对于这个系统开发者能在基本上没有限制的情况下，设计用于执行特殊的操作或服务的软件应用程序。

这样，网络基础设施启用网络布局的主机诸如客户机/服务器、对等网络或混合结构。“客户机(client)”是一类或组的成员，使用与其无关的另一类或

组的服务。这样，在计算中，客户是一过程，也就是说，约略地为一组指令或任务，它们请求由另一个程序提供的服务。客户过程在不必“了解”有关其它程序或服务本身任何运行细节的情况下，使用所请求的服务。在客户机/服务器结构中，特别是一个网络化的系统，客户通常是访问由另一个计算机例如服务器提供的共享网络资源的计算机。在图 2 的实例中，计算机 110a、110b 等可被认为是客户机，而计算机 10a、10b 等可被认为是服务器，其中服务器 10a、10b 等维护在然后被复制到客户计算机 110a、110b 等中的数据。

服务器一般是可通过远程网络诸如因特网访问的远程计算机。客户机过程可在第一计算机系统中激活，而服务器过程可在第二计算机系统中激活，通过通信媒体彼此通信，因而提供分布式功能且允许多个客户机利用服务器的信息收集能力。

客户机和服务器使用由协议层提供的功能彼此通信。例如，超文本传输协议 (HTTP) 是一个和万维网 (WWW) 一起使用的普通协议。一般地，计算机网络地址诸如通用资源定位符 (Universal Resource Locator) (URL) 或互联网协议 (IP) 地址，被用于互相识别服务器或客户计算机。网络地址可被称为通用资源定位符地址。例如，可通过通信媒体提供通信。更具体地说，客户机和服务器可通过 TCP/IP 连接互相耦合用于高性能通信。

这样，图 2 示出一典型的网络化的或分布式的环境，带有通过网络/总线与客户计算机通信的服务器，在其中可使用本发明。更详细地说，按照本发明，许多服务器 10a、10b 等可通过通信网络/总线 14 互相连接，网络/总线 14 可以是 LAN、WAN、内部互联网、因特网等，带有许多客户机或远程计算设备 110a、110b、110c、110d、110e 等，诸如便携式计算机、手持计算机、瘦客户机、网络化的器具或其它设备，诸如 VCR(录像机)、TV(电视机)、微波炉、电灯、取暖器等等。因而这是预期的，即本发明可应用任何计算设备，想要结合这些设备处理、存储或再现来自一受托源 (trusted source) 的安全内容。

在通信网络/总线 14 为因特网的网络环境中，例如，服务器 10 可以是网络服务器，客户机 110a、110b、110c、110d、110e 等通过许多已知的协议诸如 HTTP 与其通信。服务器 10 也可用作为客户机 110，可作为是分布式计算环境的特性。通信可以是有线的或无线的，只要适当。客户机设备 110 可通过或可不通过通信网络/总线 14 通信，且可具有与其关联的独立的通信。例如，在 TV 或 VCR 的情况下，可能存在或不存在网络化的方面以控制它们。每个客户计

算机 110 和服务器计算机 10 可配备各种应用程序模块或对象 135，并连接或访问各种类型的存储部件或对象，通过它们可存储文件或将文件的部分下载或移动到它们中。这样，本发明能够被用在具有能够用计算机网络/总线 14 访问和交互的客户计算机 110a、110b 等，以及可与客户计算机 110a、110b 等和其他设备 111 及数据库 20 交互服务器计算机 10a、10b 等。

数据权限管理 (DRM) 概述

如已知的，且现在参考图 11，在数字内容 12 方面，诸如数字音频、数字视频、数字文本、数字数据、数字多媒体等，在这样的数字内容要被分发至用户时，数据权限管理 (DRM) 和实施是可取的。在由用户接收时，这样的用户在合适的再现设备诸如在个人计算机 14 上的媒体播放器等等的帮助下再现或‘播放’数字内容。

一般地，分发这样的数字内容 12 的内容所有者或开发者(在下文中‘所有者’)想要对用户能用这样被分发的数字内容 12 所做的进行限制。例如，内容所有者可能想要限制用户将这样的内容 12 复制和重新分发至第二个用户，或者可能想要允许被分发的数字内容 12 只被播放有限的次数、只播放某个总的时间、只在某种类型的机器上播放、只在某种类型的媒体播放器上播放、只由某种类型的用户播放等等。

不过，在分发已经发生后，这样的内容所有者即使对数字内容 12 有控制，也只有非常少的控制。DRM 系统 10 则允许任意形式的数字内容 12 的受控制的再现或播放，在其中这样的控制是灵活的且可由该数字内容的内容所有者定义。一般地，内容 12 以包 13 的形式经由任何合适的分发通道被分发到用户。如分发的数字内容包 13 可包括用对称加密/解密密钥 (KD)(即 (KD(内容)) 加密的数字内容 12，以及标识内容的其它信息，如何获得用于这样的内容的许可证等等。

基于信任的 DRM 系统 10 允许数字内容 12 的所有者指定许可规则，在这样的数字内容 12 被允许在用户的计算设备 14 上再现之前必须满足这些许可规则。这样的许可规则可包括前述时间要求，以及可被包含在数字许可证或者使用文档(在下文中‘许可证’)16 内，用户/用户的计算设备 14(在下文中，这样的术语是可互换的，除了在环境要求另外的情况下)必须从内容所有者或其代理人获得许可证。这样的许可证 16 还包括解密密钥 (KD) 用于解密数字内容，它

可能是按照可由用户的计算设备解密的密钥加密的。

一件数字内容 12 的内容所有者必须信任用户的计算设备 14 将遵守由这样的内容所有者在许可证 16 中所指定的规则和要求，即数字内容 12 将不会被再现，除非在满足许可证 16 内的规则和要求。然后最好，为用户的计算设备 14 提供可信的组件 (trusted component) 和机制 18，它将不再现数字内容 12，除了按照包含在与数字内容 12 关联的且由用户获得的许可证 16 中的许可规则之外。

可信的组件 18 一般具有一许可证鉴别器 (license evaluator) 20，它确定许可证 16 是否是有效的，检查在这样的有效许可证 16 中的许可规则和要求，并基于所检查的许可规则和要求，确定请求的用户是否具有其中以寻找的方式再现所请求的数字内容 12 的权限。应该理解，许可证鉴别器 20 在 DRM 系统 10 中是可信的，以按照在许可证 16 中的规则和要求完成数字内容 12 的所有者的愿望，且用户应该不能够容易地为了任何不法的或其它的目的而改变这样的可信的单元。

如应该理解的，在许可证 16 中的规则和要求能指定用户是否具有基于几个因素的任何因素再现数字内容 12 的权限，这些因素包括用户是谁，用户在什么地方，用户使用的是什么类型的计算设备，什么再现应用程序在调用 DRM 系统，日期，时间等等。此外，许可证 16 的规则和要求可限制许可证 16 为，例如，预定次数的播放，或预定的播放时间。

可按照任何合适的语言和语法在许可证 16 中指定规则和要求。例如，该语言可简单地指定必须满足的属性和值(例如，日期必须比 X 晚)，或者可要求按照一指定的脚本执行功能(例如，如果日期大于 X，那么做...)。

在许可证鉴别器 20 确定许可证 16 是有效的且用户满足在其中的规则和要求时，于是可再现数字内容 12。更具体地说，要再现内容 12，从许可证 16 获得解密密钥 (KD)，并将它应用于来自内容包 13 的 (KD(内容))，以产生实际内容 12，然后实际上再现实际内容 12。

发行数字内容

图 3 是按照本发明的系统和方法的一实施例的功能方框图，用于发行数字内容。在这里所使用的术语“发行 (publishing)”，指应用程序或服务依从的一个过程，以对于可信的实体 (trusted entity) 建立一组权限和条件，该实体能

为那个内容发布这组权限和条件，以及那些权限和条件能对谁发布。按照本发明，发行过程包括加密数字内容和将它关联于一永久可实施的权限列表，永久可实施的权限是内容的作者想要用于内容的所有可能的用户的权限。这个过程可以安全的方法执行，以阻止对任何权限或对内容的访问，除非内容的作者想要。

在本发明的一个实施例中，具体地说，可使用三个实体发行安全的数字内容：一个内容准备应用程序(content preparation application)302，在客户机300上执行并用于准备发行的内容，一个数据权限管理(DRM)应用编程接口(API)306，也驻留在客户机设备300上，以及一个DRM服务器320，以通信方式通过通信网络330连接到客户机300。在本发明的一个实施例中，通信网络330包括因特网，尽管应该理解，通信网络330可能是任何局域或广域网，例如一私有的内部互联网。

内容准备应用程序302可以是任何产生数字内容的应用程序。例如，应用程序302可以是一个字处理器或其它发行物，它产生数字文本文件、数字音乐、视频或其它这样的内容。内容也可能包括流化的内容，诸如例如流化的实况或录制的事件的音频/视频。按照本发明，内容准备应用程序请求其用户使用用户提供的密钥加密内容。应用程序302使用这个密钥加密数字内容，因而形成加密的数字内容文件304。客户机应用程序也请求用户为数字内容文件304提供权限数据。权限数据包括用于每个具有数字内容中的权限的实体的相应的身份。

这样的实体可以是，例如，个人、一类个人或设备。对于每个这样的实体，权限数据还包括一个那个实体在内容中具有的权限的列表，以及可被强加于那些权限的任何或全部的任何条件。这样的权限可包括对数字内容读、编辑、复制、打印等的权限。另外，权限可以是内含的或除外的。内含的权限表示一指定的用户具有在内容中指定的权限(例如，用户能够编辑数字内容)。除外的权限表示一指定的用户具有在内容中的全部权限，除了那些指定的(例如，用户能对数字内容做任何事，除复制它之外)。

按照本发明的一个实施例，客户机API306可将加密的数字内容和权限数据传递至DRM服务器320。使用下面详细说明的过程，DRM服务器320确定它是否能够实施用户已经分配的权限，如果是，则DRM320签署权限数据以形成一签署的权限标签(signed rights label)(SRL)308。不过，一般而言，任何

可信的实体能够签署权限数据，最好使用由 DRM 服务器 320 信任的密钥。例如，客户机能够使用由 DRM 服务器 320 为它提供的密钥签署权限数据。

权限标签 308 可包括代表权限描述的数据、加密的内容密钥和在权限描述和加密的内容密钥上的数字签名。如果 DRM 服务器正在签署权限标签，则它将签署的权限标签 308 通过客户机 API306 传递回到客户机，API306 将签署的权限标签 308 存储在客户机设备 300 上。内容准备应用程序 302 然后将签署的权限标签 308 与加密的数字内容文件 304 关联。例如，SRL308 与加密的数字内容文件集中在一起以形成权限管理的内容文件 310。

不过，一般而言，权限数据不需要与数字内容结合。例如，权限数据可能被存储在一个已知的位置，而被存储的权限数据的参考可能与加密的数字内容结合。这个参考可能包括指示存储权限数据的位置（例如，包含这个权限数据的数据存储）的标识符，以及相应于那个特定的权限数据在那个特定的存储位置的标识符（例如，标识包含感兴趣的特定的权限数据的文件）。权限管理的内容 310 然后可被传送到任何人任何地方，且只有那些具有恢复内容的权限的实体能够恢复内容，且只按照它们被分配的权限。

图 4 是按照本发明的典型方法 400 的流程图，用于发行权限管理的数字内容，在其中由 DRM 服务器签署权限标签。不过应该理解，这个实施例仅仅是示范的，且一般而言，可由任何可信的实体签署权限标签。一般而言，按照本发明用于发行数字内容的方法可包括：使用一内容密钥（CK）加密数字内容，生成与数字内容关联的权限描述，按照用于 DRM 服务器的公用密钥（PU-DRM）以产生（PU-DRM(CK)），并基于一相应于（PU-DRM）的私有密钥（PR-DRM）在权限描述和（PU-DRM(CK)）上创建一数字签名。

在步骤 402，应用程序 302 生成一个被用于加密数字内容的内容密钥（CK）。最好，内容密钥（CK）是一个对称密钥，尽管一般而言，任何密钥可被用于加密数字内容。对称密钥算法，有时被称为“秘密关键码（secret key）”算法，在它们要加密一消息时使用同一密钥加密该消息。为了那个原因，最好将那个（CK）保密。在发送者与接收者之间的共用（CK）应该做得非常小心，以避免未经授权的窃听这样的（CK）。因为（CK）是在加密者和解密者之间共用的，（CK）最好在传输任何加密的消息之前被传送。

在本领域中几个对称密钥生成算法是众所周知的。在一个实施例中，使用数据加密标准（Data Encryption Standard）（DES），尽管应该理解可使用任何

对称算法。这样的对称密钥算法的实例包括，但不是限制，AES、Triple-DES(三重数据加密标准)、国际数据加密算法(International Data Encryption Algorithm)(IDEA)、Cast、Cast-128、RC4、RC5 和 SkipJack。

在步骤 404，应用程序 302 用对称内容密钥(CK)加密数字内容形成加密的数字内容 304，它可使用符号(CK(content))书写。使用应用程序 302 的作者也可生成与数字内容关联的权限数据。这个权限数据可包括一个将授权恢复内容的实体列表，以及每个实体相对于内容所拥有的专用权限，连同可被强加于那些权限的任何条件。这样的权限例如可包括观看内容、打印内容等。应用程序 302 为 API306 提供权限数据。以 XML/XrML 格式的权限数据的实例作为附 1 附在这里。

在步骤 406，API306 生成第二加密密钥(DES1)，它可被用于加密内容密钥(CK)。最好(DES1)也是一个对称密钥。在步骤 408，API306 用(DES1)加密(CK)以产生(DES1(CK))。在步骤 410，API306 丢弃(CK)，因为现在只能通过解密的(DES1(CK))得到(CK)的结果。要确保(CK(content))受中央 DRM 服务器 320 保护和在中央按照权限数据完成所有用于内容的“许可请求”，API306 在步骤 412，与所提供的 DRM 服务器 320 联系并取回它的公用密钥(PU-DRM)。在步骤 414，API306 用(PU-DRM)加密(DES1)以产生(PU-DRM(DES1))。这样，(CK)可受(PU-DRM)保护，以确保 DRM 服务器 320 是将来能够取得对(CK)访问的唯一的实体，如解密(CK(content))所要求的。在步骤 416，API306 用(DES1)加密权限数据(即，授权的实体列表和与在这个列表中每个授权的实体关联的相应的权限和条件)，以产生(DES1(权限数据))。

在一个可替换的实施例中，(CK)可被用于直接加密权限数据以产生(CK(权限数据))，且(PU-DRM)可被用于直接加密(CK)以产生(PU-DRM(CK))，因此完成前述的(DES1)的使用。不过，使用(DES1)加密权限数据和(CK)允许这样的(DES1)遵守可能服从 DRM 服务器的任何特定的算法，然而(CK)可能由一个与 DRM 服务器独立的实体指定且可能不服从 DRM 服务器。

在步骤 418，内容准备应用程序 302 可将(PU-DRM(DES1))和(DES1(权限数据))作为用于签署的权限标签提交给 DRM 服务器 320。可替换地，客户机本身可签署权限数据。如果正在将权限数据提交至服务器用于签署，那么在步骤 420，DRM 服务器 320 访问权限数据并验证它能够实施在所提交的权限标签中的权限和条件。要验证它能够实施权限数据，DRM 服务器 320 将(PR-DRM)应用于

(PU-DRM(DES1))以产生(DES1)，然后将(DES1)应用于(DES1(权限数据))以产生不用密码的权限数据。服务器320然后可进行任何政策检查以验证在权限数据中指定的用户、权限和条件是在由服务器320所实施的任何政策之内的。服务器320原来提交的包括(PU-DRM(DES1))和(DES1(权限数据))的权限标签，以产生签署的权限标签(SRL)308，在其中签字是基于DRM服务器320的私有密钥(PR-DRM)的，并将SRL308返回至API306，API306然后将返回的SRL308提供给客户机应用程序302。

SRL308是以数字方式签署的文档，使它防篡改。另外，SRL308独立于用于加密内容的实际的密钥类型和算法，但与它正在保护的内容保持1-1关系。现在参考图4A，在本发明的一个实施例中，SRL308可包括关于内容的信息，它是SRL308的基础，有可能包括一个内容的ID(标识符)；关于签署这个SRL308的DRM服务器的信息，包括(PU-DRM(DES1))和参考信息(referral information)诸如用于在网络上定位DRM服务器的URL及这个URL失败时的退回信息；描述SRL308本身的信息；(DES1(权限数据))；(DES1(CK))；和其中的S(PR-DRM)。用XML/XrML的实例SRL308作为附录2附在这里。

通过确保可信的实体签署权限数据以创建签署的权限标签308，按照由发行人在权限标签308中的权限数据中所述的条款，DRM服务器声称它将发布用于内容的许可证。如应该意识到的，要求用户获得许可证以再现内容，尤其是因为许可证包含内容密钥(CK)。当用户想要获得用于加密内容的许可证时，用户可向DRM服务器320或其它许可证发布实体license issuing entity提供许可证请求，该请求包括用于内容的签署的权限标签308和验证用户的凭证的证书。许可证发布实体然后可解密(PU-DRM(DES1))和(DES1(权限数据))以产生权限数据，向许可证请求实体license requesting entity列出由作者准予的所有权限(如果有的话)，并构造一个只具有那些特定权限的许可证。

最好，在应用程序302接收SRL308时，这样的应用程序302将签署的权限标签308与相应的(CK(内容))304集中以构成权限管理的数字内容。可替换地，可将权限数据存储在一个已知的位置中，带有为加密的数字内容提供的那个位置的参考。这样，DRM允许的再现应用程序能够通过再现应用程序从正在试图再现的这件内容发现签署的权限标签308。这个发现触发再现应用程序发起一个对于DRM许可服务器320的许可证请求。发行应用程序302可存储一个指向DRM许可服务器320的URL，例如，或者DRM许可服务器320可将它自己

的 URL，在以数字方式签署权限标签之前作为一件元数据嵌入到权限标签中，因此由再现应用程序调用的 DRM 客户机 API306 能够识别正确的 DRM 许可服务器 320。最好，在签署权限标签之前，将一个唯一的标识符，诸如全球唯一标识符(globally unique identifier) (GUID) 放入权限标签中。

在本发明的一个实施例中，简单对象访问协议(simple object access protocol) (SOAP) 可用于内容准备应用程序 302 或再现应用程序和 DRM 服务器 320 之间的通信。另外，可提供 API 库诸如 API306，因此不要求应用程序诸如应用程序 302 实现 DRM 协议的客户端，而是能够只进行本地 API 调用。最好，使用 XrML，一种 XML 语言，描述用于数字内容的权限描述、许可证和权限标签，尽管应该理解，任何合适的格式能够被用于权限描述和其它数据。

获得用于发行的内容的许可证

图 5 是按照本发明的系统和方法的一个实施例的功能方框图，用于许可权限管理的数字内容。“许可(licensing)”，作为在此所使用的术语，指应用程序或服务遵守的请求和接收许可证的过程，许可证将使一个在许可证中指定的实体能够按照在许可证中所指定的条款恢复内容。许可过程的输入可包括与正在请求的许可证所用于的内容关联的签署的权限标签(SRL)308，和正在请求的许可证所用于的实体的公用密钥证书。注意，请求许可证的实体不需要必须是正在请求的许可证所用于的实体。一般地，许可证包括来自 SRL308 的权限描述，能够解密加密的内容的加密的密钥，和在权限描述和加密的密钥上的数字签名。数字签名断言所指定的实体和权限是合法的。

一种用于应用程序 302 恢复权限管理的内容 310 的方法是，客户机 API306 将权限管理的内容 310 签署的权限标签 308 通过通信网络 330 传送到 DRM 服务器 320。DRM 服务器 320 的位置，例如可在 SRL308 中的参考信息中找到。在这样一个实施例中，DRM 许可服务器 320，通过下面详细描述的过程，可使用权限标签中的权限描述确定它是否能够发布许可证，如果能，则导出权限描述以包括许可证。

如上所述，权限标签 308 包含按照 DRM 服务器 320 的公用密钥(PU-DRM) 加密的内容密钥(CK)(即(PU-DRM(CK)))。在发布许可证的过程中，DRM 服务器 320 安全地解密这个值以获得(CK)。然后它使用公用密钥证书中的公用密钥(PU-ENTITY)以重新加密(CK)(即(PU-ENTITY(CK))), 公用密钥证书是在许可证请求

中被向上传递的。重新被加密的(PU-ENTITY(CK))是服务器 320 放在许可证中的内容。这样，可在没有暴露(CK)的危险的情况下，将许可证返回给调用者，因为只有关联于私有密钥(PR-ENTITY)的持有者能够从(PU-ENTITY(CK))恢复(CK)。客户 API306 然后使用(CK)解密加密的内容以构成解密的数字内容 312。客户应用程序 302 然后能够使用按照在许可证中所提供的权限的解密的数字内容 312。

可替换地，例如，诸如发行客户机的客户机，能够发布它自己的许可证以恢复内容。在这样一个实施例中，受保护的过程可在客户计算机上运行，为客户机提供在合适的环境下解密数字内容所需要的密钥。

图 6A 和 6B 提供按照本发明的方法 600 的一个实施例的流程图，用于许可权限管理的数字内容。按照本发明，请求实体可提交一个代表一或多个可能的许可证持有人的许可证请求。请求实体可以是/可以不是可能的许可证持有人之一。可能的许可证持有人可以是一个人、一个组、一个设备或任何能够以任何方式恢复内容的其它实体。现在将参考一个实施例描述方法 600，在这个实施例中，DRM 服务器处理许可证请求，尽管应该理解，可在客户机上执行许可证请求处理，以及由客户机直接发布许可证。

在步骤 602，许可证发布实体诸如 DRM 服务器，例如，接收一个许可证请求。最好，许可证请求包括用于一或多个被请求的许可证持有人的每一个的公用密钥证书或者身份。

在步骤 604，认证请求实体(即产生许可证请求的实体)。按照本发明的一个实施例，许可证发布实体可被配置为使用协议(例如质询-应答(challenge-response))认证以确定请求实体的身份，或者它可被配置为不要求认证请求实体(也被称为“允许匿名认证(allowing anonymous authentication)”)。当要求认证时，可使用任何类型的认证方案(例如，上面提到的质询-应答方案，用户标识符和口令(user-id-and-password)方案诸如 MICROSOFT.NET、PASSPORT、WINDOWS 授权、x509 等)。最好，既允许匿名认证，又支持由集成信息系统支持的任何协议认证方案。认证步骤的结果将是一个身份，诸如例如，一个“匿名”身份(对于匿名认证)，或者一个个人帐户身份。如果因任何原因不能认证许可证请求，则返回一个错误并不准予许可证。

在步骤 606，授权认证的实体--即，确定在步骤 608 被认证的实体是否被允许请求许可证(或者为它自己或者代表另一个实体)。最好，许可证发布实体

存储一个被允许(或者不被允许)请求许可证的实体列表。在一个实施例中，在身份列表中的一个身份是产生请求的实体的身份，而不是正在请求的许可证所用于的实体的身份，尽管它可能是任一个。例如，可允许个人帐户身份直接产生许可证请求，但是可信的服务器过程可代表这样一个实体产生许可证请求。

按照本发明，许可证请求能够包括用于每个可能的许可证持有人的公用密钥证书或者身份。如果只为一个许可证持有人请求许可证，则只指定一个证书或身份。如果为多个许可证持有人请求许可证，则可为每个可能的许可证持有人指定证书或身份。

最好，许可证发布实体具有用于每个有效许可证持有人的公用密钥证书。不过，应用程序 302 可能想要为给定用户生成许可证，但是应用程序 302 不能访问用于那个用户的公用密钥证书。在这样一种情况下，应用程序 302 可在许可证请求中指定用户的身份，并且结果，许可证发布实体可调用已注册的证书插件模块，该模块在目录服务中执行查找并返回合适的公用密钥证书。

如果在步骤 608，发布实体确定公用密钥证书没有被包括在许可证请求中，那么发布实体使用指定的身份在目录服务或数据库中查找合适的公用密钥证书。如果在步骤 610，发布实体确定证书在目录中，那么在步骤 612，取回证书。在一个实施例中，使用证书插件经由目录访问协议从目录服务取回公用密钥证书。如果或者在请求中或者在目录中，都不能为一给定的可能的许可证持有人找到证书，那么许可证服务器不为那个可能的许可证持有人生成许可证，且在步骤 614，返回一个错误至请求实体。

假定许可证发布实体具有用于至少一个可能的许可证持有人的公用密钥证书，那么在步骤 616，发布实体验证许可证持有人证书的可信性。最好，用一组可信的证书发布者证书(trusted certificate issuer certificate)配置发布实体，并确定许可证持有人证书的发布者是否在可信的发布者列表中。如果在步骤 616，发布实体确定许可证持有人证书的发布者不在可信的发布者列表中，那么对于那个许可证持有人的请求失败，且在步骤 614 产生一个错误。这样，可信的发布者没有发布其证书的任何可能的许可证持有人，将接收不到许可证。

另外，发布实体最好对证书链中所有的数字签名执行数字签名验证，该证书链从可信的发布者证书到个人许可证持有人公用密钥证书。在一个链中验证数字签名的过程是一个众所周知的算法。如果没有证实用于一给定的可能的许

可证持有人的公用密钥证书，或者没有证实在链中的一个证书，则可能的许可证持有人是不可信的，且因此不为那个可能的许可证持有人发布证书。否则，在步骤 618，可发布证书。这个过程在步骤 620 重复，直到已经处理所有已经请求许可证的实体为止。

如在图 6B 中所示，许可证发布实体进行至验证在许可证请求中所接收的签署的权限标签 308。在一个实施例中，发布实体可使用权限标签插件和后端数据库，该数据库在服务器上存储由发布实体签署的每个权限标签的主拷贝。权限标签是由在发行时放入它们中的 GUID 标识的。在许可时间(在步骤 622)，发布实体解析在许可证请求中的权限标签输入并取回其 GUID。然后它将这个 GUID 传递至权限标签插件，该插件向数据库发布一个查询以取回主权限标签的一个拷贝。这个主权限标签直到现在可能比在许可证请求中发送的权限标签的拷贝更多，并且它将是在下面的步骤中在请求中所使用的权限标签。如果基于 GUID 在数据库中找不到权限标签，发布实体在步骤 624 检查其政策，以基于在请求中的权限标签确定它是否还允许发布许可证。如果政策不允许这个，则许可证请求将在步骤 626 失败，且在步骤 628 将向 API306 返回一个错误。

在步骤 630，许可证发布实体验证权限标签 308。验证在权限标签上的数字签名，且如果许可证发布实体不是权限标签的发布者(签署它的实体)，那么许可证发布实体确定权限标签的发布者是否是另一个可信的实体(例如，一个使许可证发布实体能够与其共用密钥材料的实体)。如果权限标签没有证实，或者它不是由可信的实体发布的，那么在步骤 626 许可证请求失败，且在步骤 628 将向 API306 返回一个错误。

在所有的验证已经发生后，许可证发布实体将权限标签 308 译成用于每个被批准的许可证持有人的许可证。在步骤 632，许可证发布实体为要向每个许可证持有人发布的许可证生成一个相应的权限描述。对于每个许可证，发布实体对照权限标签中的权限描述所指定的身份，鉴定在那个许可证持有人的公用密钥证书中指定的身份。权限描述将一组身份分配给每个权限或权限组，该组身份能够行使在一许可证中的那个权限或那组权限。对于与这个许可证持有人的身份相关联的每个权限或权限组，那个权限或那组权限被复制到一个用于这个许可证的新数据结构中。最后得到的数据结构是在用于特定的许可证持有人的许可证中的权限描述。作为这个过程的一部分，许可证发布实体鉴定任何先决条件，它们可能与在权限标签的权限描述中的任何权限或权限组关联。例如，

一个权限可具有与其关联的时间先决条件，它限制许可证发布实体在一指定的时间之后发布许可证。在这种情况下，发布实体将需要检查当前时间，且如果过了在先决条件中所指定的时间，那么发布实体将不能够向许可证持有人发布那个权限，即使那个许可证持有人的身份与那个权限关联。

在步骤 636，发布实体从权限标签 308 获得 (PU-DRM(DES1)) 和 (DES1(CK)) 并应用 (PR-DRM) 以获得 (CK)。发布实体然后使用 (PU-ENTITY) 许可证持有人的公用密钥证书重新加密 (CK) 以产生 (PU-ENTITY(CK))。在步骤 638，发布实体将所生成的权限描述与 (PU-ENTITY(CK)) 集中，并使用 (PR-DRM) 以数字方式签署最后得到的数据结构。这个签署的数据结构是用于这个特定的许可证持有人的许可证。

当在步骤 640 发布实体确定没有更多的许可证要为特定的请求生成时，它将已经生成零或多个许可证。在步骤 642 将所生成的许可证返回至请求实体，连同与那些许可证关联的证书链一起(例如，服务器自己的公用密钥证书和发布其证书的证书等等)。

在按照本发明的系统的一个实施例中，可使用多个许可证颁发者密钥。在这样一个实施例中，加密地通过权限标签 308 传播并到许可证持有人的内容密钥 (CK)，实际上可以是任何任意的数据。一个特别有用的变化是使用一组独立的、加密的、分别与权限描述中不同的权限或不同的原则关联的内容密钥 (CK)。例如，在一首集中歌曲的数据版本可全部用不同的密钥 (CK) 加密。可将这些密钥 (CK) 包括在同一权限标签中，但一个原则可具有播放歌曲中的一首的权限(例如，他可能只具有在他的许可证中取得一个密钥的权限)，而第二个原则可能具有播放所有歌曲的权限(她可能具有在她的许可证中取得所有密钥的权限)。

最好，按照本发明的系统使发行应用程序/用户能够在权限标签 308 中指定许可证持有人的组或类。在这样一个实施例中，许可证发布实体将鉴定在权限标签中指定的任何组/类，以确定当前的许可证持有人身份是否是那些组类的成员。如果在指定的组/类中找到成员资格，则发布实体可将与组/类关联的权限或权限组添加到用于许可证持有人的权限描述数据结构。

在本发明的一个实施例中，在 DRM 服务器中的发行和许可协议接口 (publish and license protocol interface) 支持调用应用程序或用户的认证和授权，以及用于 DRM 服务器的管理控制台 (administrative console) 允许管

理者为许可和发行接口两者生成一个访问控制列表。这使服务器的客户能够应用政策，通过政策允许用户/应用程序或者发行或者许可，或者两者。

修改或重新发行签署的权限标签 308

在本发明的一个实施例中，可“再发行(republish)”SRL308，如果已经准予内容的用户有足够的许可这么做。也就是说，如果允许，则用户可改变在 SRL308 内的权限数据。注意，应该谨慎地和深思远虑地准予改变权限数据这样的许可，特别是因为具有改变权限数据的许可的用户基本上能够准予它自己关于所关联的内容的宽广的权限。想象得到的，这样一个用户甚至能够准予它自己暴露内容和向世界传送同一内容的权限。

这里，改变的许可是通过在 SRL308 中权限数据内包括一个一个标志表示的，这个标志表示特定的用户或用户类能够实际上改变或‘再发行’权限数据和权限标签 308。当 DRM 服务器 320 接收带有与对许可证的请求有关的这样的许可的 SRL308 时，DRM 服务器 320 在用户所请求的许可证内包括按照用户的公用密钥(即 PU-ENTITY)加密的对称密钥(DES1)，以产生(PU-ENTITY(DES1))。

这样，要在 SRL308 内编辑权限数据，以及现在转到图 7，用户从许可证取回(PU-ENTITY(DES1))(步骤 701)，对它应用(PR-ENTITY)以产生(DES1)(步骤 703)，从 SRL308 取回(DES1(权限数据))(步骤 705)，并对它应用(DES1)以产生权限数据(步骤 707)。之后，用户按需要改变权限数据(步骤 709)，并以结合图 4 阐述的方式将改变的权限数据提交给 DRM 服务器 320，以获得签署的权限标签 308(步骤 711)。当然，这里，签署的权限标签 308 实际上是一个再发行的 SRL308，且因此一旦接收到 SRL308(步骤 713)，用户剥去集中在关联的内容中的原来的 SRL308(步骤 715)，并然后将再发行的 SRL308 集中到这样的内容中(步骤 717)。

这样，以及可意识到的，再发行 SRL308 使用户能够在不必改变所关联的内容的情况下，更新 SRL308 中的权限数据，包括权限、条件或用户。具体地说，再发行不要求用新的(CK)重新加密所关联的内容。而且，再发行不要求从零开始生成新的 SRL，特别是因为原来的 SRL308 在其中具有许多条款，可将它们复制到新的 SRL308。

自发行签署的权限标签 308

在本发明的一个实施例中，可通过请求用户本身签署 SRL308。因此，用户不需要联系 DRM 服务器 320 以获得用于一件关联的内容的 SRL308。结果，自发行也可指离线发行。在这样的实施例中，可要求用户与 DRM 服务器 320 联系以请求一个基于这样一个自发行的 SRL308 的许可证。应该理解，可使发行实体能够发布它自己的许可证。

具体地说，以及现在参考图 8，在实施例中，首先通过从 DRM 服务器 320 接收一 DRM 证书为用户提供自发行，DRM 证书包括一公用密钥 (PU-CERT) 和按照用户的公用密钥 (PU-ENTITY) 加密的相应的私有密钥以产生 (PU-ENTITY (PR-CERT))。这个证书应该由 DRM 服务器 320 的私有密钥 (PR-DRM) 签署，因此 DRM 服务器 320 可验证完全一致，在下面将更详细地讨论。如可意识到的，DRM 证书 810 授权用户自发行。如也可意识到的，密钥对 (PU-CERT, PR-CERT) 是与 (PU-ENTITY, PR-ENTITY) 分开的，且专门为自发行使用。注意，没有密钥对 (PU-CERT, PR-CERT) 也行，在这个情况下 DRM 证书 810 只包括用户的公用密钥 (PU-ENTITY)，并由 DRM 服务器的私有密钥 (PR-DRM) 签署，这样的 DRM 服务器 320 也可验证完全一致。

自发行与如在图 4 中所示的发行不同，在于用户基本上取代 DRM 服务器 320 相关的在那里执行的步骤。值得注意，用户用如由 DRM 证书 810 获得的 (PR-CERT) 签署所提交的包括 (PU-DRM (DES1)) 和 (DES1 (权限数据)) 的权限标签，以产生签署的权限标签 (SRL) 308。如应该意识到的，用户通过从这样的 DRM 证书 810 获得 (PU-ENTITY (PR-CERT)) 并将 (PR-ENTITY) 应用于它，并从 DRM 证书 810 获得 (PR-CERT)。注意，尽管用户不能验证 DRM 服务器 320 能够实施在所提交的权限标签中的权限，特别是因为用户不具有要应用于 (PU-DRM (DES1)) 的 (PR-DRM)。因此，在基于自发行的 SRL308 请求许可证的时候，DRM 服务器 320 本身应该执行验证。

一旦用户自发行 SRL308，用户将这样自发行的 SRL308 与使用的 DRM 证书 810 集中以产生与该内容相同的内容，以及将带有 SRL308 和 DRM 证书 810 的这样的内容分发至另一个用户。其后，其它用户实质上以如在图 6A 和 6B 中所示的相同的方式，从 DRM 服务器 320 请求和获得用于内容的许可证。这里，然而，许可证请求用户向 DRM 服务器提交作为集中于内容中的自发行 SRL308 和 DRM 证书 810 两者。DRM 服务器 320 然后基于相应的 (PU-DRM) 验证在 DRM 证书 810 中的 S (PR-DRM)，且从 DRM 证书 810 获得 (PU-CERT)。DRM 服务器 320 然后基于

获得的(PU-CERT)验证 SRL308 中的 S(PR-CERT)，且象以前一样继续。然而注意，由于用户没有验证 DRM 服务器 320 能够实施在 SRL308 中的权限，以如上面所阐述的，DRM 服务器 320 本身应该在这时执行这个验证。

权限模板

如上所述，通过定义用户或用户类，定义用于每个被定义的用户或用户类的权限，且然后定义任何使用条件，在权限标签中为用户提供创建大多数任何种类的权限数据的自由。不过，值得注意，反复地为多个权限标签定义权限数据是讨厌的和重复的，特别是当为不同件内容反复地定义同一用户或用户类、权限和条件的时候。这样一个情况例如能发生在公司或办公室环境中，在用户反复地发行要由特定定义的用户团队共享的不同件内容的时候。于是，在这样一个情况下，且在本发明的一个实施例中，创建权限模板，在权限模板是已经包括预定义的用户组或用户类、用于每个定义的用户或用户类的预定义的权限和预定义的使用条件的时候，用户可在创建权限标签时反复地使用权限模板。

在本发明的一个实施例中，且现在转到图 9，权限模板 900 实质上具有与将在权限标签中的相同的权限数据。不过，由于(DES1)是不知道的，直到发行内容为止，权限数据不能按照这样的(DES1)加密，如在权限标签中的情况。在本发明的一个实施例中，然后，在图 4 的步骤 416 的用(DES1)加密权限数据的期间，提交带有未加密的权限数据的权限模板 900，以产生(DES1(权限数据))。当然，在这样加密之前，从所提交的权限模板 900 取回权限数据。

可以是或可以不是这个情况，即在构建权限模板的时候，DRM 服务器 320 和它的公用密钥(PU-DRM)是已知的。另外，即使知道，可以是或可以不是这个情况，即存在多于一个 DRM 服务器 320，每个具有其自己的(PU-DRM)。然而，在构建权限模板的时候 DRM 服务器 320 和其公用密钥(PU-DRM)是已知的情况下，以及在只使用一个 DRM 服务器 320，或者只有一个 DRM 服务器 320 要结合权限模板 900 使用的情况下，这样的权限模板也可在其中包括关于 DRM 服务器的信息，该 DRM 服务器是要签署从权限模板 900 得到的权限标签，包括其公用密钥(PU-DRM)。尽管这样的(PU-DRM)出现在 SRL308 用作加密(DES1)以产生(PU-DRM(DES1))，要再次意识到(DES1)是不知道的，直到发行内容为止，并因此在权限模板 900 中的(PU-DRM)不能加密这样的(DES1)，如在权限标签中的情况。然后，在本发明的一个实施例中，在图 4 的步骤 414 的用(PU-DRM)加密(DES1)

期间，提交带有未加密的(PU-DRM)的权限模板900，以产生(PU-DRM(DES1))。

当然，在使用之前，从所提交的权限模板900取回(PU-DRM)。

还是在上述情况下，可被包括在权限模板中的关于DRM服务器的其它信息也可包括参考信息，诸如用于在网络上定位DRM服务器的URL，和如果URL失败时退回的信息。在任何情况下，权限模板还可在其中包括描述权限模板900本身的信息。注意，权限模板900也可为与被发行的内容相关的信息提供空间，诸如出现在与内容和/或加密的密钥(CK)和(DES1)有关的权限标签中的信息，尽管如果将权限模板的实例化实际地转换到权限标签中，这样的空间是不必要的。

尽管如到现在为止所揭示的权限模板900主要是为了方便用户，也要意识到在某些环境中，用户不应该具有无限制的自由以在权限标签中定义权限数据，并且可使用权限模板900限制能创建的权限标签的范围或类型。例如，且特别是在公司或办公室环境的情况下，它可被预定义为一特定用户应该始终只向一类特定的用户发行内容或者该用户应该从不向一类特定的用户发行内容的政策。在任何情况下，以及在本发明的一个实施例中，这样的政策被作为权限数据包含在一或多个权限模板900中，且可在发行内容时限制用户使用这样的权限模板以创建权限标签。值得注意，使可用于用户为该用户指定发行政策的一个权限模板900或一组权限模板900，可在不脱离本发明的精神和范围的情况下，指定任何特殊类型的发行政策。

要为受限制的用户等等指定权限模板900，以及现在转到图10，管理者等等实际上通过预定义的权限数据(步骤1001)，以及定义可能是必需的和适当的任何其它数据，诸如相关与特定的DRM服务器320相关的信息(步骤1003)，构建权限模板900。值得注意，要完成由受限制的用户等等使用的权限模板，必须使权限模板900为正式的。也就是说，权限模板900必须可被识别为一个受限制的用户等等可使用的权限模板。因此，在本发明的一个实施例中，如由管理者等等构建的权限模板被提交至DRM服务器320用于由其签署，在这里这样的签署使权限模板为正式的(步骤1005)。

注意，如果这样的信息实际上真的存在于权限模板900中，签署的DRM服务器320是其信息在权限模板900中的DRM服务器320。还注意，DRM服务器320可只在进行任何必要的检查时，签署权限模板900，或者在根本没有任何检查的情况下可签署权限模板900。最后注意，来自DRM服务器320的模板签

名 S(PR-DRM-T) (在这时-T 表示用于 ORT(正式的权限模板)900 的签名)，应该基于至少在权限模板 900 中预定义的权限数据，但在不脱离本发明的精神和范围的情况下，还可以基于其它信息。如下面所述，将签名 S(PR-DRM-T)合并到权限标签中，并且结合权限标签验证这个签名，且因此无论签名基于什么，应该将它以非改变的形式合并到权限标签中。

在 DRM 服务器 320 签署权限模板 900 和将它返回至管理者等等的时候，管理者接收带有 S(PR-DRM-T) 的签署的和现在正式的权限模板 900(步骤 1007)，并将正式的权限模板(ORT)900 传送至使用它的一或多个用户(步骤 1009)。因此，对于一个基于 ORT900 发行内容的用户，该用户取回 ORT900(步骤 1011)，并通过提供任何需要的信息，诸如关于内容的信息；合适的密钥信息；由 (DES1) 加密以产生 (DES1(权限数据)) 的来自 ORT900 的权限数据；以及任何来自 ORT900 的其它信息，基于 ORT900 来构建权限标签(步骤 1013)。值得注意地，用户还用权限标签包括来自 ORT900 的签名 S(PR-DRM-T)。

其后，以及象以前一样，用户将权限标签提交至 DRM 服务器 320 用于签署(步骤 1015)。这里，然而，DRM 服务器 320 将不签署所提交的权限标签，除非在其中的 S(PR-DRM-T) 证实。也就是说，DRM 服务器 320 通过拒绝签署所提交的权限标签，除非所提交的权限标签包括签名 S(PR-DRM-T)，实施用户必须将所提交的权限标签以 ORT900 为基础。具体地说，DRM 服务器 320 从所提交的权限标签中，取回该 S(PR-DRM-T) 和该签名所基于的无论什么信息，然后基于 (PU-DRM) 验证这样的签名。注意，在所提交的权限标签中权限数据是按照 (DES1) 加密的(即 (DES1(权限数据)))。因此，DRM 服务器 320 必须首先获得 (DES1) 并用它解密 (DES1(权限数据))，如结合图 7 所述的，要能够验证基于在所提交的权限标签中的权限数据的签名。

一旦被验证，DRM 服务器 320 用 S(PR-DRM-L) 签署所提交的权限标签以产生 SRL308，如前面一样(在这里-L 表示签名是用于 SRL308 的)。这里，S(PR-DRM-L) 可代替 S(PR-DRM-T)，或可以是附加于 S(PR-DRM-T)。如果附加，则 S(PR-DRM-L) 可部分地基于 S(PR-DRM-T)。注意，可使用 (PR-DRM) 产生 S(PR-DRM-T) 和 S(PR-DRM-L) 两者，或者可使用不同的 (PR-DRM) 用于 S(PR-DRM-T) 和 S(PR-DRM-L) 的每一个。在 DRM 服务器 320 签署权限标签和将 SRL308 返回至用户时，用户接收带有 S(PR-DRM-L) 的 SRL308(步骤 1017) 并进行将前者集中到正在发行的内容上，如前面一样。

如果 ORT900 的签名 S(PR-DRM-T) 是至少部分地基于在 ORT900 中预定义的权限数据的，那么这样的权限数据如出现在 SRL308 中时(在 DES1(权限数据)中)不能被修改或改变。否则，S(PR-DRM-T)将不能证实。然而，在本发明的一个实施例中，在 ORT900 中的权限数据能够在也被包括在 ORT900 中的规定的规则内变化。例如，这些规则可指定要被包括在 SRL308 中的两个权限数据组中的一个，或者可允许从一组选择对象中选择。如可意识到的，在不脱离本发明的精神和范围的情况下，这些规则可以是以任何合适的语法阐述的任何特定的规则。这里，在创建权限标签的时候，由合适的规则解释器为用户解释规则。尽管权限数据可变化，但是规则不同样变化，且因此用于 ORT900 的模板签名 S(PR-DRM-T)是至少部分地基于规则且不基于权限数据本身。结果，用 ORT900 包括的规则也必须用 SRL308 包括。

在本发明的一个实施例中，在 ORT900 中预定义的权限数据是部分地固定的和不变的，以及是部分地可变的和规则驱动的，如上所述。这里，用于 ORT900 的模板签名 S(PR-DRM-T)是至少部分地基于规则的固定的部分和基于用于权限数据的可变部分的规则。

如可意识到的，如由用户拥有的 ORT900 可变成过时的或失效的。也就是说，ORT900 通过其中的权限数据可反映已经变成过时的、不相关的或简单地不可再应用的政策。例如，在 ORT900 的权限数据中指定的一或多个用户或用户类在政策环境内可能不再存在，或者在 ORT900 的权限数据中指定的一特定的用户或用户类在政策环境内可能不再具有同样的权限。在这样的情况下，可能是管理者已经发布一个修改的 ORT900，但用户还使用先前的、失效的版本的 ORT900。

在这样的情况下，且在本发明的一个实施例中，然后，DRM 服务器 320 在签署提交的权限模板 900 以创建一个 ORT900 时保留 ORT900 的一个拷贝，每个 ORT900 具有唯一的辨识标记，且基于一个在其中包括这样的 ORT900 的辨识标记的 ORT900 构建每个权限标签。因此，在诸如结合图 10 接收所提交的权限标签时，DRM 服务器 320 找出在权限标签中 ORT900 的辨识标记，基于所找到的辨识标记取回这样的 ORT900 的最新的拷贝，从所提交的权限标签中删除权限数据，然后至少部分地基于所插入的权限数据签署权限标签。当然，DRM 服务器还执行在如所述的过程中必需的和有义务的任何必需的加密和解密步骤，包括解密或重新加密(DES1(权限数据))。注意，如果 DRM 服务器自适应地替换所提

交的权限标签中的权限数据，这样的权限标签和由其构建这样的权限标签的 ORT900 就不必要在其中包括权限数据。改为，权限数据只需要驻留在 DRM 服务器 320 上。不过，用权限标签和由其构建这样的权限标签的 ORT900 包括权限数据，对于用户可能是有用的，并因此在某些情况下是有用的。

经由目录许可

当为受保护的内容发布许可证时，许可证发布实体(在下文中‘许可证颁发者(licensor)’)从内容查阅所发送的 SRL308，以确定要为哪个用户/group)/群(cluster)/部门(division)/平台(platform)/等(在下文中‘实体(entity)’)提供权限，以及查阅所发送的证书以识别许可证请求者。基于上面的，许可证颁发者确定要将在 SRL308 中所列出那些中哪些权限发布给请求者。概念地，许可证颁发者检查在 SRL308 中所列出的实体并将这样的实体与请求者比较。这样，如果 SRL308 指定一特定的组要接收许可证且请求者是这样的组的成员，则请求者被准予带有如在 SRL308 中为这个组所述的权限的许可证。同样，如果 SRL308 指定一特定的用户要接收许可证且请求者是这样的用户，则请求者被准予带有在 SRL308 中为这样的用户所述的权限的许可证。如可意识到的，特定的 SRL308 可列出用于它的几个实体和权限，且一特定的请求者可被准予基于是一或多个实体的成员的许可证。

在本发明的一个实施例中，且如在图 12 中所看到的，在所发送的证书 1202 中经由标识符 1204 识别请求者，在这里标识符 1204 例如可以是一个别名，通过别名在一组织的目录 1206 中识别请求者。因此，SRL308 在其中按照这样一个标识符 1204 列出每个被授权的实体。这样，且作为处理对许可证 1208 的请求的部分，许可证颁发者 1210 从证书 1202 获得请求者的标识符 1204，并将所获得的标识符 1204 与如在所发送 SRL308 中所列出的所有标识符 1204 比较。如果找到一个匹配，则许可证颁发者 1210 向请求者发布带有在 SRL308 中为这样的请求者的标识符 1204 指定的权限的许可证。

而且，在目录 1206 有效的情况下，许可证颁发者 1210 也可确定请求者是否是在 SRL308 中所列出的任何其它实体，假定目录 1206 包含适当的交叉引用信息，它能够反映在每个这样的其它实体中请求者的成员资格状态。一般地，目录 1206 为每个请求者不只是列出其标识符 1204，还列出请求者其成员的每个组/群/部门/平台/其它实体/等的标识符 1208。注意，目录 1206 可包括标识

符 1208，诸如邮件地址、可替换的邮件地址、ID(标识符)、可替换的 ID、组成员资格、历史标识符和/或等等。

有了从请求者接收的在其中带有其标识符 1204 的证书 1202，以及有了来自请求者接收的 SRL308 的权限数据，然后，以及现在参考图 13，许可证颁发者 1210 以下列方式为请求者发布许可证 1208。最初，许可证颁发者 1210 从所接收的证书 1202 获得标识符 1204(步骤 1301)，并在目录 1206 中找到所获得的标识符 1204(步骤 1303)。之后，许可证颁发者 1210 基于被找到的标识符 1204，在目录 1206 中找到请求者 1204 是其成员的每个成员的标识符 1204(步骤 1305)。这样，对于每个被找到的请求者标识符 1204 和所有被找到的实体标识符 1204，许可证颁发者 1210 将这样的标识符 1204 与如在所发送的 SRL308 中列出的所有标识符 1204 比较(步骤 1307)。再一次，如果找到匹配，许可证颁发者 1210 为请求者发布带有在 SRL308 中为所匹配的标识符 1204 指定的权限的许可证(步骤 1309a)。

注意，由于将多个标识符 1204 与 SRL308 的比较，可能的情况是，在 SRL308 中找到多个匹配的标识符 1204。如果这样，许可证颁发者 1210 在 SRL308 中选择一个合适的匹配的标识符 1204，并向请求者发布带有在 SRL308 中为所选择的匹配的标识符 1204 指定的权限的许可证(步骤 1309b)。例如，许可证颁发者可选择向请求者传送最多权限的匹配标识符 1204(步骤 1309b-1)。注意，许可证颁发者可能能够确定哪个匹配的标识符 1204 传送最多的权限，或者可能必须依赖于在 SRL308 中的某种类型的优先标记。在后一种情况下，在 SRL308 中的每个匹配的标识符(用户)1204 具有一相应的优先级标记 1212，且较高标记 1212 例如表示较大范围的准予的权限。这样，如果许可证颁发者 1210 在 SRL308 中找到多个匹配的标识符 1204，这样的许可证颁发者 1210 选择具有最高优先级标记 1212 的匹配标识符 1204(步骤 1309b-2)。

注意，在参考目录 1206 以生成另外的相关于请求者的标识符 1204 时，许可证颁发者 1210 将增加找到匹配的可能性，即使在这样的情况下，例如，请求者的邮件地址或 ID 从创建 SRL308 时起已经改变。一般而言，目录 1206 提供从一个请求者的标识符 1204 映射到其它可能的请求者的标识符 1204，由此就可使用所有的标识符 1204 试图找到一个与在 SRL308 中的标识符 1204 的匹配。

对组的许可

在本发明的一个实施例中，所发送的证书 1202，如由请求者所提交的，可代表一组或群或一些其它的个人的集合（在下文中‘组’），在这里这样的组在目录 1206 中被适当地代表。这样的组可包括邮件激活的组诸如一分发列表或邮件别名，或一安全组诸如可结合网络操作系统等等定义的。因此，许可证颁发者 1210 在接收所发送的‘组’证书 1202 时，实际上如前面一样地进行。注意，然而，因为所发送的证书 1202 代表一特定的组，它可以是，明确地说，来自许可证颁发者 1210 所发布的许可证 1208 是用于在证书 1202 中识别的组而不是请求者。可替换地，许可证颁发者 1210 可从目录 1206 确定请求者是在证书 1202 中识别的组的部分，且如果是则所发布的 1210 是用于请求者的。

在前一种情况下，所发布的许可证 1208 可包括按照组的公用密钥加密的内容密钥，且请求者因而需要获得相应的组的私有密钥。因此，请求者可具有带有这样的私有密钥的组成员资格证书，它有可能是按照请求者的公用密钥加密的且可按照请求者的私有密钥解密的。

在后一种情况下，要将按照请求者的公用密钥加密的内容密钥包括在所发布的许可证 1208 中，许可证颁发者 1210 可附加地从请求者接收带有这样的公用密钥的证书。可替换地，许可证颁发者 1210 可以在文件上具有这样一个证书（见图 6A 和 6B 的步骤 608-612），且在从目录 1206 确定请求者是在所发送的组证书 1202 中识别的组的一部分时，使用在证书中的公用密钥。

值得注意，在 SRL 308 中指定权限和按照组发布许可证 1208 在企业或组织环境中完成数据权限管理。例如，文档或电子邮件可以是受 DRM 保护的，因此一给定部门的所有成员具有读文档或电子邮件的权限。假定用这样一个部门的组（例如电子邮件别名）存在于组织的目录 1206 中，这是最经常的情况，文档或电子邮件的作者将基于组而不是个人准予权限。如可意识到的，这样的组级权限准予的好处包括对于作者在指定具有权限的个人的类时易于使用。另外，通过按照组指定权限，在新的个人加入组和老的个人离开组的时候所指定的权限不会变成‘失效的’。改为，组的所有当前的成员能够行使这些权限，只要直到现在这样的组的成员资格被保持在组织的目录 1206 中。

在许可期间插入政策

在本发明的一个实施例中，且如上面结合图 9 的 ORT900 间接提到的，当

基于这样的 SRL308 发布许可证 1208 时，DRM 服务器/许可证颁发者 1210 能自适应地修改或代替来自所提交的 SRL308 的权限数据。具体地说，在明确地忽略在所提交的 SRL308 中的权限数据时几种情况会发生，且当基于这样的 SRL308 创建许可证 1208 时，许可证颁发者 1210 改为代替或‘插入 (inject)’一可替换的政策。注意，尽管在此所揭示的几个许可证颁发者 1210 将政策插入许可证 1208 的特定的情况，但是许可证颁发者 1210 在不脱离本发明的精神和范围的情况下，也可将政策插入在任何其它类型的情况中的许可证颁发者 1208。

在第一种情况中，且现在参考图 14，许可证颁发者 1208 保存一个被授予特殊权限的特殊实体(用户、组等)的列表(图 12)。例如，特殊的实体可包括在组织中某些高级别的个人，某些管理的个人，某些应该能够再现所有内容的个人，和前述的个人的组。这样的列表 1214 实际上被包含在组织的目录 1206 内，作为在目录中为每个特殊实体列出的辨识信息，或更简单地通过创建一或多个这样的特殊实体的组。这样，这样的特殊实体能再现内容，即使用于它们的 SRL308 相反将阻止这样的再现。

在一实体提交 SRL308 作为对许可证 1208 的请求的部分时，然后，现在参考图 14，许可证颁发者 1210 用目录 1206 以合适的方式检查，以确定所提交的实体是否被鉴定为一特殊实体(步骤 1401)，且如果是，则许可证颁发者 1210 为这个特殊实体创建带有不同于在所提交的 SRL308 中提供的权限数据的特殊权限的许可证 1208(步骤 1403)。注意，特殊权限可能是在不脱离本发明的精神和范围的情况下任何权限。例如，特殊权限可以是来自一特定组的所有特殊实体能够完全访问和再现内容，一个特定的特殊实体接收增强的权限诸如更高的播放次数或在许可证 1208 期满前更长的时间等。注意，如果特殊权限对于个人或组是特定的，在目录 1206 中可在用于这个个人或组的目录项中指定这样的权限，这样的目录项可具有对一位置的合适的参考，该位置放置特殊的权限，许可证颁发者 1210 可基于这个个人或组的标识符 1204 在数据库找到这个特殊的权限，等等。

在第二种情况中，现在转到图 15，许可证颁发者 1208 保存一个对其要限制或拒绝权限的受限制的实体(用户、组等)的列表 1216(图 12)。例如，受限制的实体可包括已经离开组织的个人，在组织中不应该正常地具有对于任何内容的任何权限的个人，诸如维修和建筑人员，在组织中只具有有限的地位的个人，诸如接线员和临时职工，以及上述个人的组。象上述‘特殊的’列表 1214，

受限制的列表 1216 也可被包含在组织的目录 1206 中，作为在目录中为每个受限制的实体列出的辨识信息，或更简单地通过创建一或多个这样的受限制的组。这样，这样的受限制的实体被限制再现内容，即使用于它们的 SRL308 相反将允许这样的再现。

在一实体提交 SRL308 作为对许可证 1208 的请求的部分，然后，仍参考图 14，许可证颁发者 1210 用目录 1206 以合适的方式检查，以确定所提交的实体是否被鉴定为受限制的实体(步骤 1405)，且如果是，则许可证颁发者 1210 为受限制的实体创建带有与在所提交的 SRL308 中提供的权限不同的受限制的权限的许可证 1208(步骤 1407)。注意，受限制的权限可以是在不脱离本发明的精神和范围的情况下任何权限。例如，受限制的权限可以是所有受限制的实体不能以任何方式访问和再现相应的内容，所有来自一特定组的受限制的实体只能以短暂的形式再现内容，一特定的受限制的实体只能打印一件内容的单一拷贝，等等。另外，受限制的权限可以是无论什么权限也不准予受限制的实体。如关于特殊权限一样，如果受限制的权限是特定于一个个人或组，则可在目录 1206 中为这个个人或组在一目录项指定这样的权限，这样的目录项可具有对于一位置的合适的参考，该位置放置受限制的权限，许可证颁发者 1210 可基于这个个人或组的标识符 1204 在数据库中找到受限制的权限，等等。

在第三种情况中，许可证颁发者 1208 可将政策插入许可证 1208 中以指定最低程度的系统要求，这些要求是在计算设备 14(图 11)上要再现相应的内容所必需的(步骤 1409)。这样的最低程度的系统要求一般涉及计算设备 14 的确实性和安全性，尽管在不脱离本发明的精神和范围的情况下，这样的要求可涉及任何其它内容。

将关系到许可证颁发者 1210 的确实性和安全性的基本的实例是，计算设备 14 的可信的组件 18 或其安全部分是否是当前的。如可意识到的，这样的当前性可通过版本编号、建立日期等等代表，并反映可信的组件 18 或其部分的使用时间。如也可意识到的，随着这样的可信的组件 18 或其部分的使用时间，可信的组件 18 或其部分更易受到不法的实体的安全性攻击。因此，许可证颁发者 1210 可决定超过某个使用时间的可信的组件 18 或其部分应该是不可信的，且可将政策插入由它发布的许可证 1208，要求在允许再现相应的内容之前，先更新这样的不可信的可信的组件 18 或其部分。

关系到许可证颁发者 1210 的确实性和安全性的另一个实例是，要再现内

容的应用程序事实上应该是可信的。如可意识到的，可以是这个情况，即一个应用程序可以是可信的，以通过不允许以不受保护的形式保存内容，在许可证颁发者 1208 的限制内再现内容，而另一个应用程序不能同样是可信的。因此，许可证颁发者 1210 可决定只有某个应用程序能够被使用，以再现相应的内容，并可将政策插入由它发布的许可证 1208 中，要求只使用这样的应用程序再现这样的内容。

当然，其它政策插入情况是大量的。一般而言，可执行政策插入以增加附加的权限至 SRL308 的权限数据中，或者从 SRL308 的权限数据中删除权限，有可能基于请求者(步骤 1411)；且同样将条件添加到这样的权限数据中，或者从这样的权限数据中删除条件，再一次有可能基于请求者(步骤 1413)。

结论

完成结合本发明执行的过程所需要的编程是相对直接的且对于相关的编程人员是显而易见的。因此，没有将这样的编程附在这里。于是，可使用任何特定的编程，在不脱离本发明的精神和范围的情况下，以完成本发明。

应该意识到，在不脱离其发明的概念的情况下，可对所述的实施例进行修改。值得注意地，尽管按照规定的领域诸如组织来描述本发明，但是还可以在为组织的子集或者包含多个组织的规定领域内使用本发明，所有在不脱离本发明的精神和范围的情况下。因此，应该理解，这个发明不是受限于所揭示的特定实施例，而是旨在覆盖在如由所附的权利要求书所定义的本发明精神和范围内的修改方案。

附录 1

取样权利数据

Sample Rights Data

```
<?xml version="1.0" ?>
<XrML version="1.2">
  <BODY type="Rights Template">
    <DESCRIPTOR>
      <OBJECT>
        <ID type="GUID">c43...</ID>
        <NAME>$411$411name$411desc</NAME>
      </OBJECT>
    </DESCRIPTOR>
    <WORK>
      <OBJECT>
        <ID />
      </OBJECT>
      <RIGHTSGROUP name="MAIN RIGHTS">
        <RIGHTSLIST>
          <VIEW>
            <CONDITIONLIST>
              <ACCESS>
                <PRINCIPAL>
                  <OBJECT>
                    <ID />
                    <NAME>test@company.com</NAME>
                  </OBJECT>
                </PRINCIPAL>
              </ACCESS>
            </CONDITIONLIST>
          </VIEW>
          <RIGHT name="generic">
            <CONDITIONLIST>
              <ACCESS>
                <PRINCIPAL>
                  <OBJECT>
                    <ID />
                    <NAME>test@company.com</NAME>
                  </OBJECT>
                </PRINCIPAL>
              </ACCESS>
            </CONDITIONLIST>
          </RIGHT>
        <RIGHTSLIST>
      </RIGHTSGROUP>
    </WORK>
  </BODY>
</XrML>
```

```
        </CONDITIONLIST>
        </RIGHT>
    </RIGHTSLIST>
    </RIGHTSGROUP>
</WORK>
</BODY>
<SIGNATURE>
    <ALGORITHM>RSA PKCS#1-V1.5</ALGORITHM>
    <DIGEST>
        <ALGORITHM>SHA1</ALGORITHM>
        <PARAMETER name="codingtype">
            <VALUE encoding="string">surface-coding</VALUE>
        </PARAMETER>
        <VALUE encoding="base64" size="160">Mwl...=</VALUE>
    </DIGEST>
    <VALUE encoding="base64" size="1024">Ms...=</VALUE>
</SIGNATURE>
</XrML>
```

附录 2

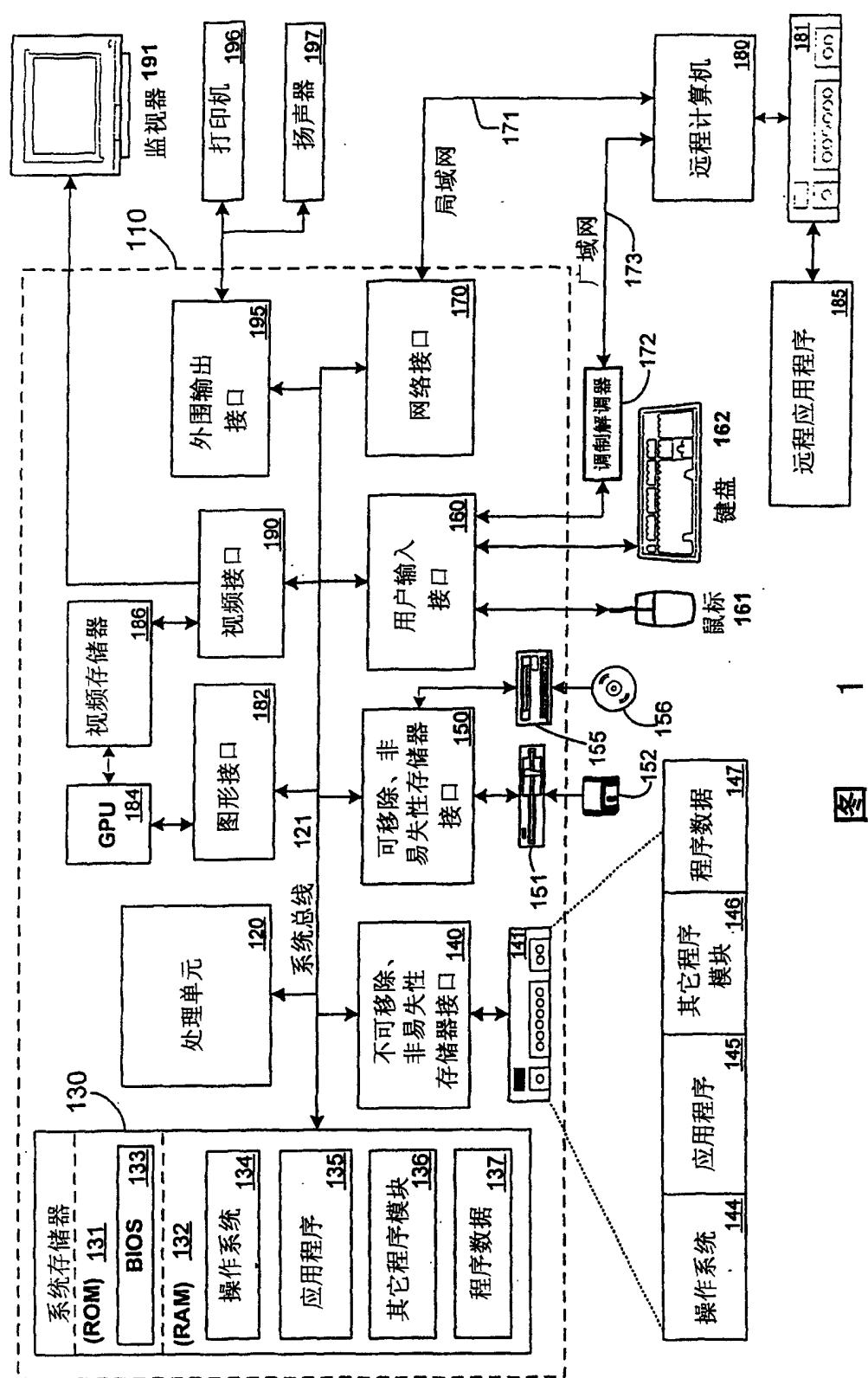
经签名的取样权利标签(SRL) 308

Sample Signed Rights Label (SRL) 308

```
<?xml version="1.0" ?>
<XrML version="1.2">
<BODY type="Rights Label" version="3.0">
  <ISSUEDTIME>2002-01-01_12:00:00</ISSUEDTIME>
  <DESCRIPTOR>
    <OBJECT>
      <ID />
      <NAME>$$409$...</NAME>
    </OBJECT>
  </DESCRIPTOR>
  <ISSUER>
    <OBJECT type="DRM-Server">
      <ID type="GUID">{d81...}</ID>
      <NAME>Test DRM Server</NAME>
      <ADDRESS type="URL">http://licensing.dev.com</ADDRESS>
    </OBJECT>
    <PUBLICKEY>
      <ALGORITHM>RSA</ALGORITHM>
      <PARAMETER name="public-exponent">
        <VALUE encoding="integer32">65537</VALUE>
      </PARAMETER>
      <PARAMETER name="modulus">
        <VALUE encoding="base64" size="1024">NcO...=</VALUE>
      </PARAMETER>
    </PUBLICKEY>
    <ENABLINGSBITS type="sealed-key">
      <VALUE encoding="base64" size="1024">tFg...=</VALUE>
    </ENABLINGSBITS>
    <SECURITYLEVEL name="Server-Version" value="2.0" />
    <SECURITYLEVEL name="Server-SKU" value="22222-3333" />
  </ISSUER>
  <DISTRIBUTIONPOINT>
    <OBJECT type="LICENSE ACQUISITION URL">
      <ID type="GUID">{0F4...}</ID>
      <NAME>DRM Server Cluster</NAME>
      <ADDRESS type="URL">http://localhost/Licensing</ADDRESS>
    </OBJECT>
```

```
</DISTRIBUTIONPOINT>
<WORK>
  <OBJECT type="TEST-FORMAT">
    <ID type="MYID">FDB-1</ID>
  </OBJECT>
  <METADATA>
    <SKU type="PIDTYPE">PID</SKU>
  </METADATA>
  <PRECONDITIONLIST>
    <TIME />
  </PRECONDITIONLIST>
</WORK>
<AUDITDATA name="Encrypted Rights data">PAB... </AUDITDATA>
</BODY>
<SIGNATURE>
  <ALGORITHM>RSA PKCS#1-V1.5</ALGORITHM>
  <DIGEST>
    <ALGORITHM>SHA1</ALGORITHM>
    <PARAMETER name="codingtype">
      <VALUE encoding="string">surface-coding</VALUE>
    </PARAMETER>
    <VALUE encoding="base64" size="160">Prc...=</VALUE>
  </DIGEST>
  <VALUE encoding="base64" size="1024">EHd...=</VALUE>
</SIGNATURE>
</XrML>
```

计算环境 100



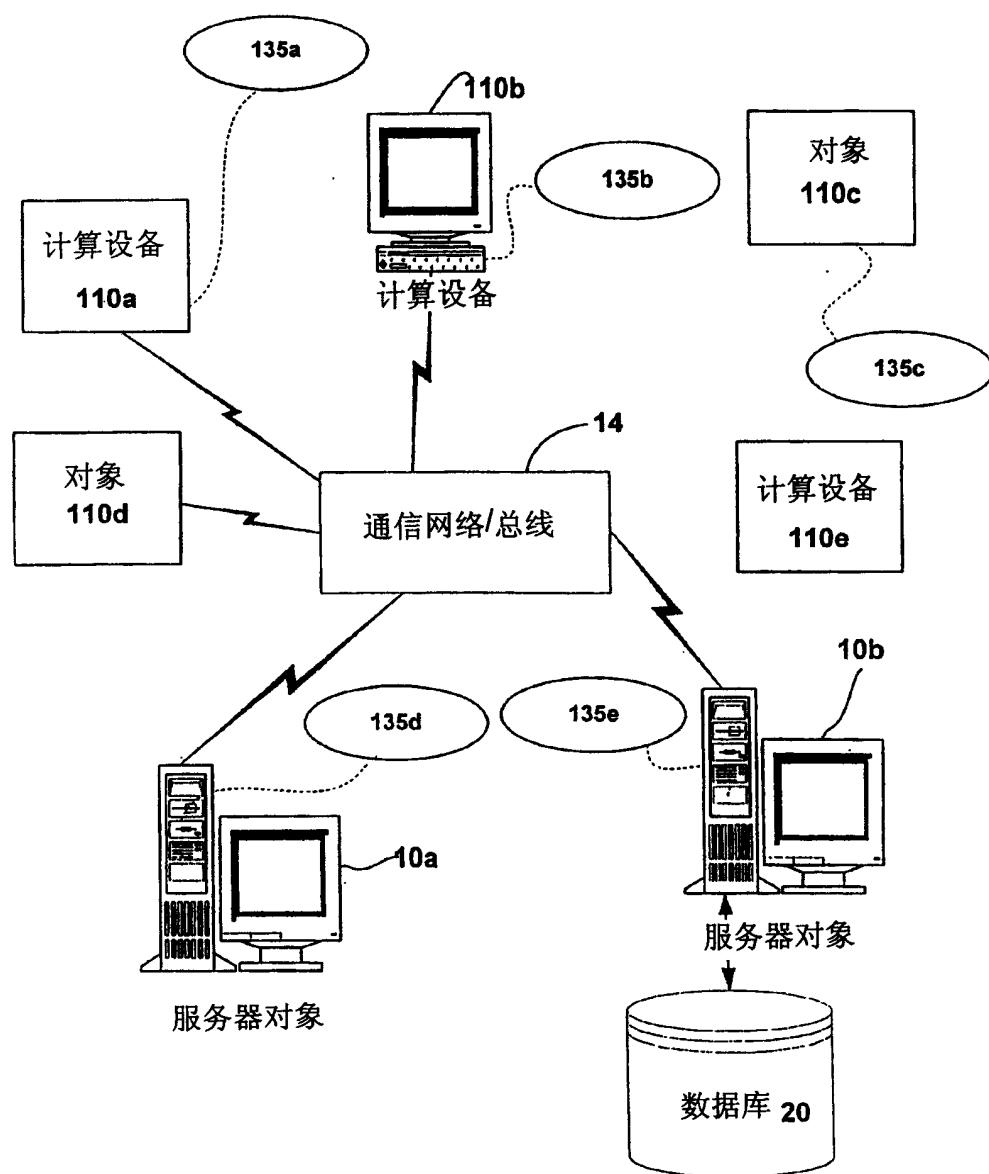
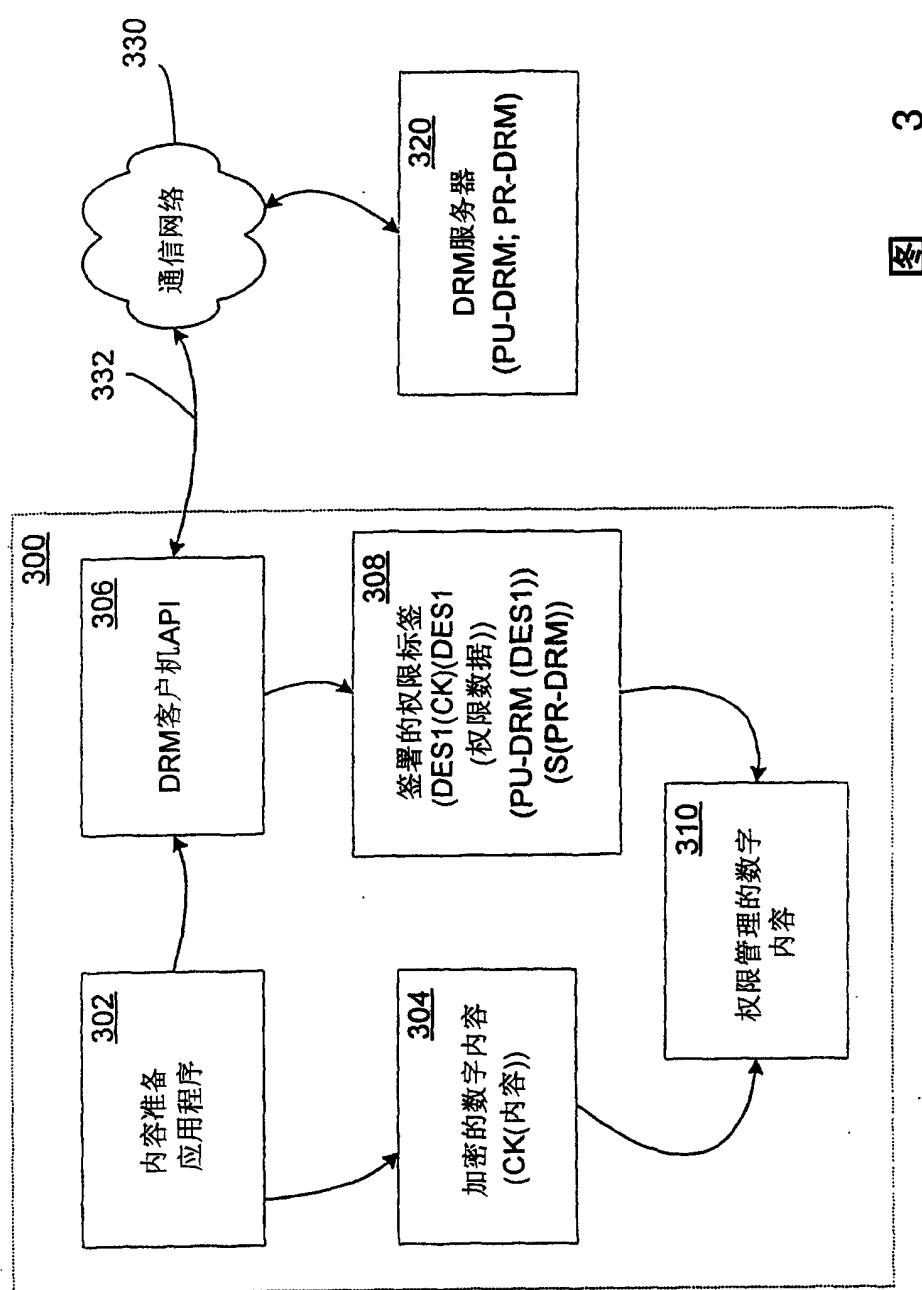
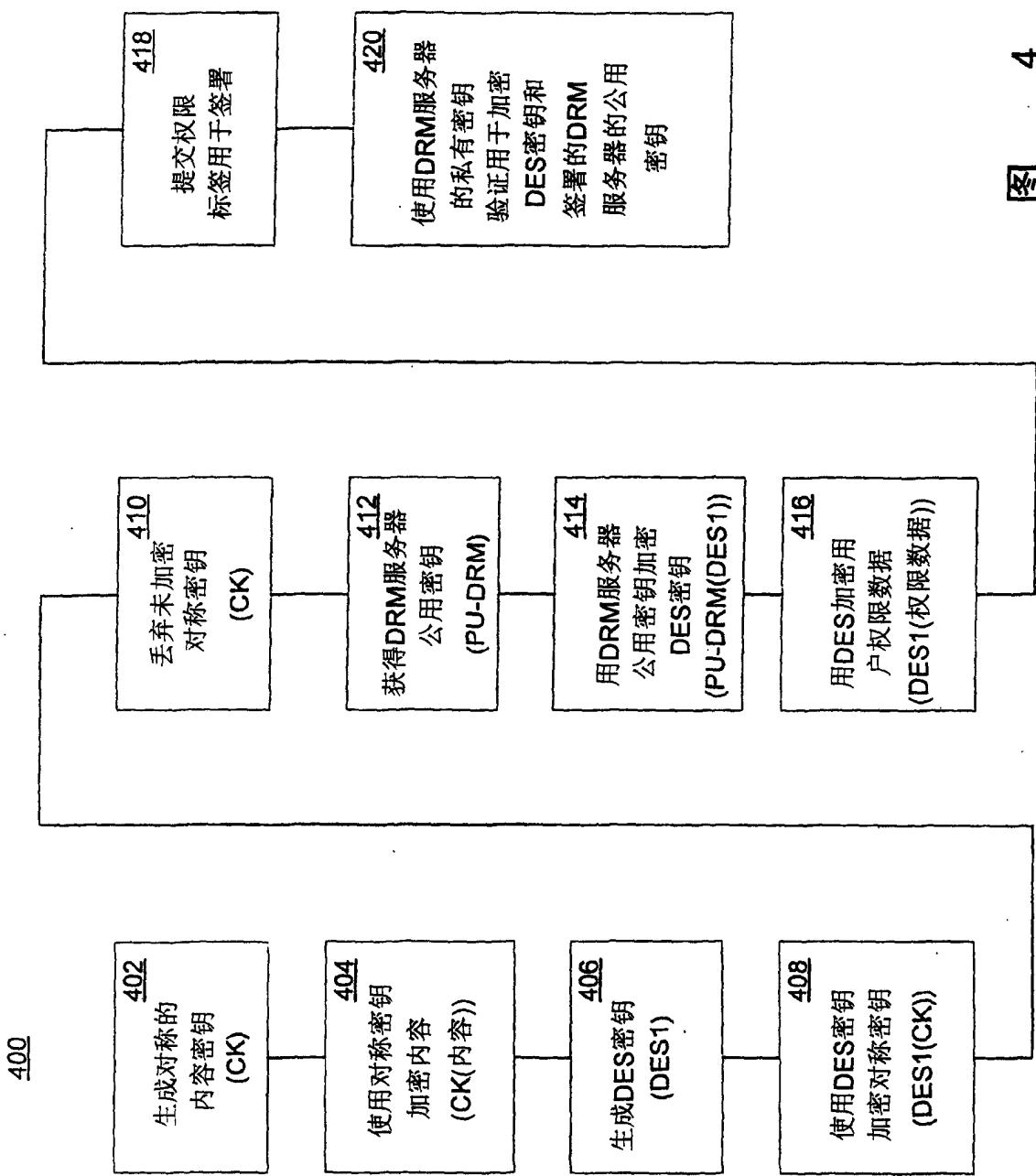


图 2



3

图



4

图

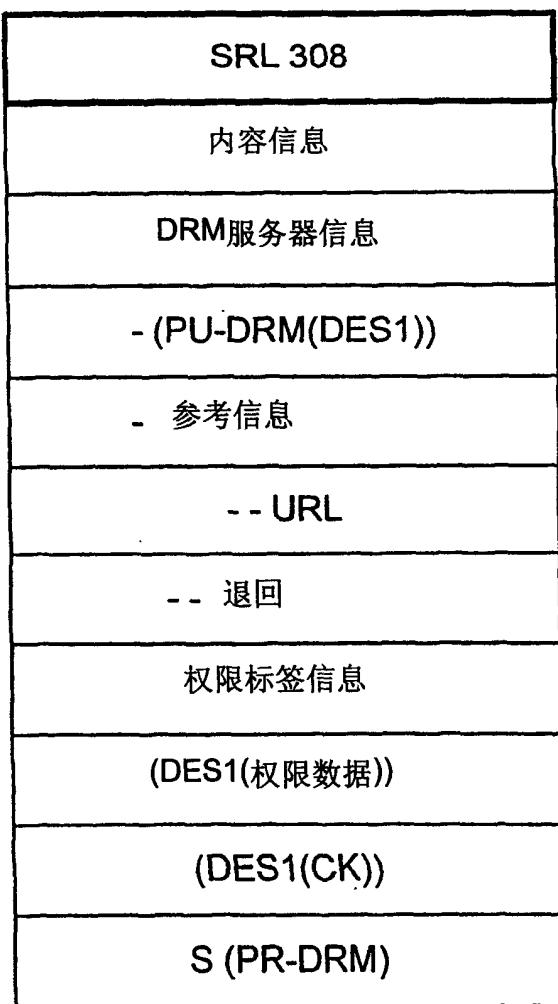


图 4A

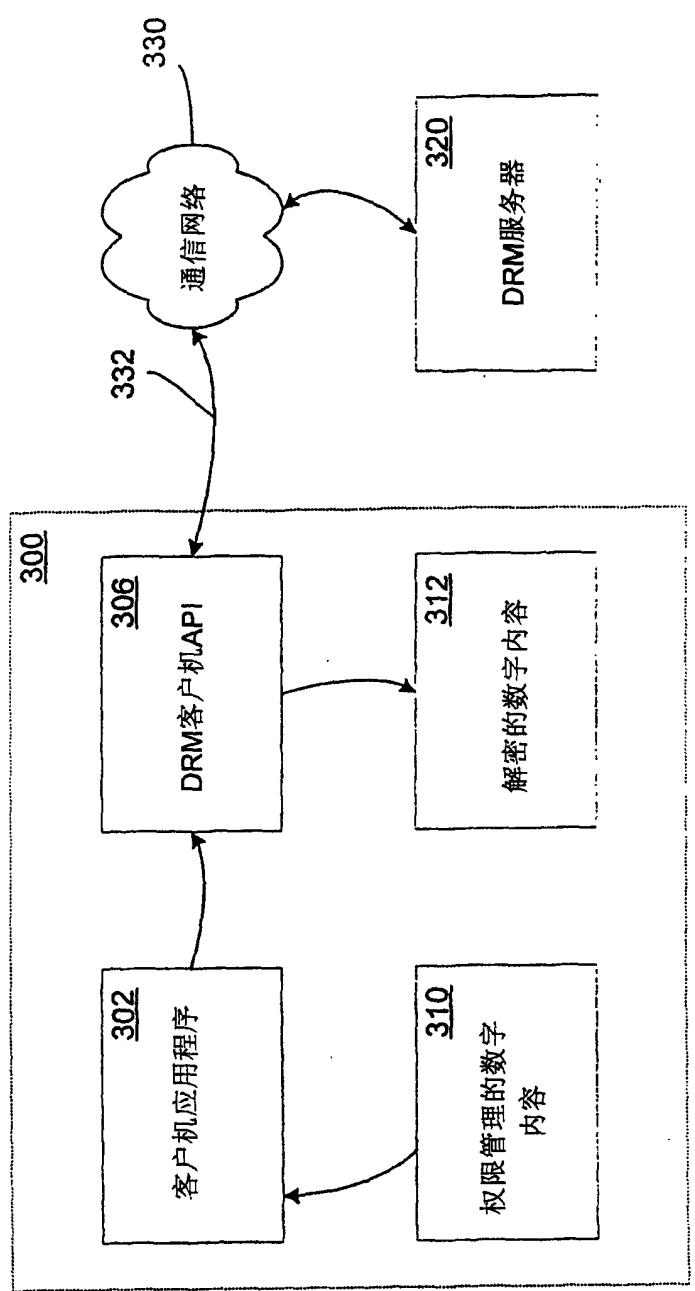
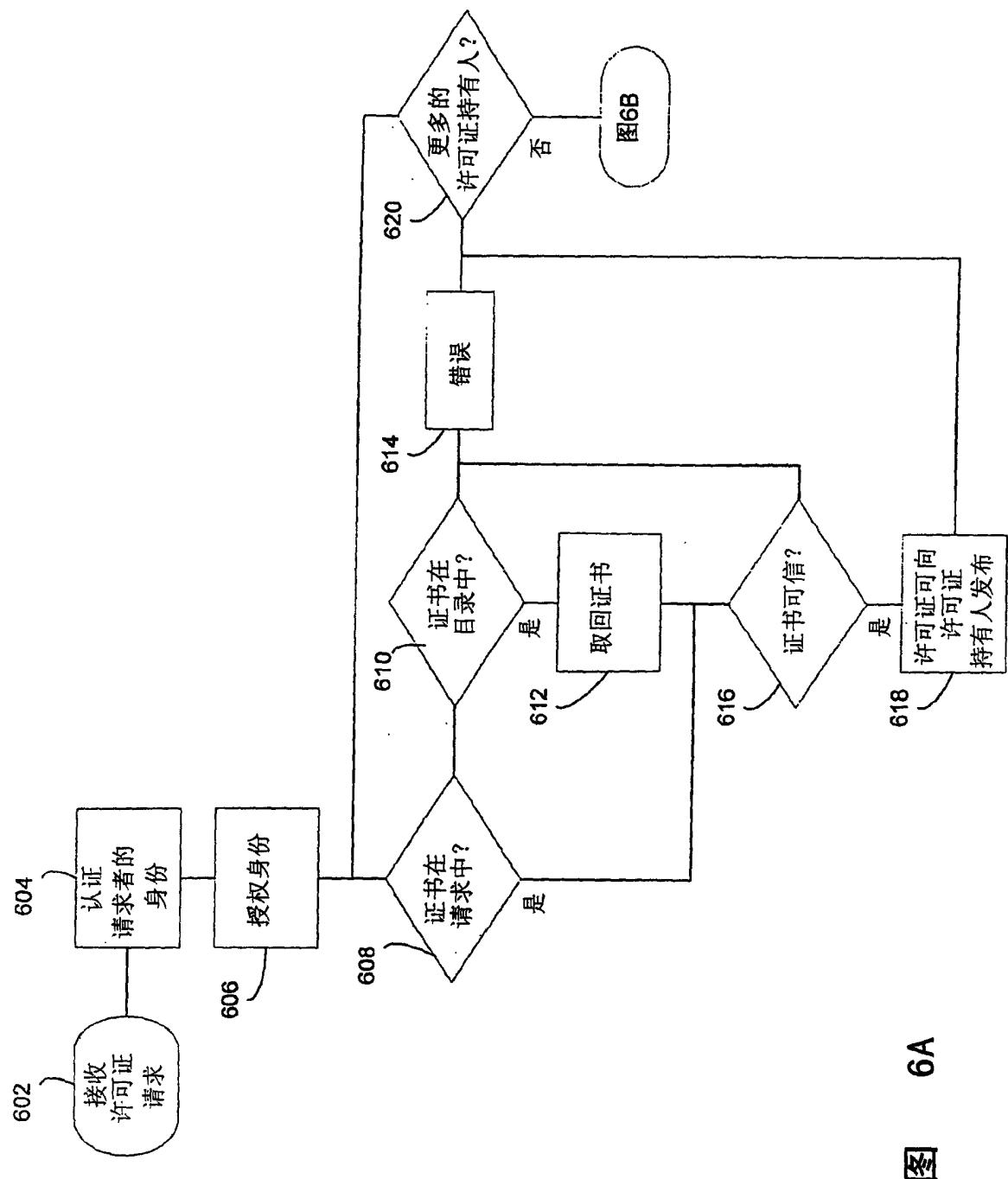
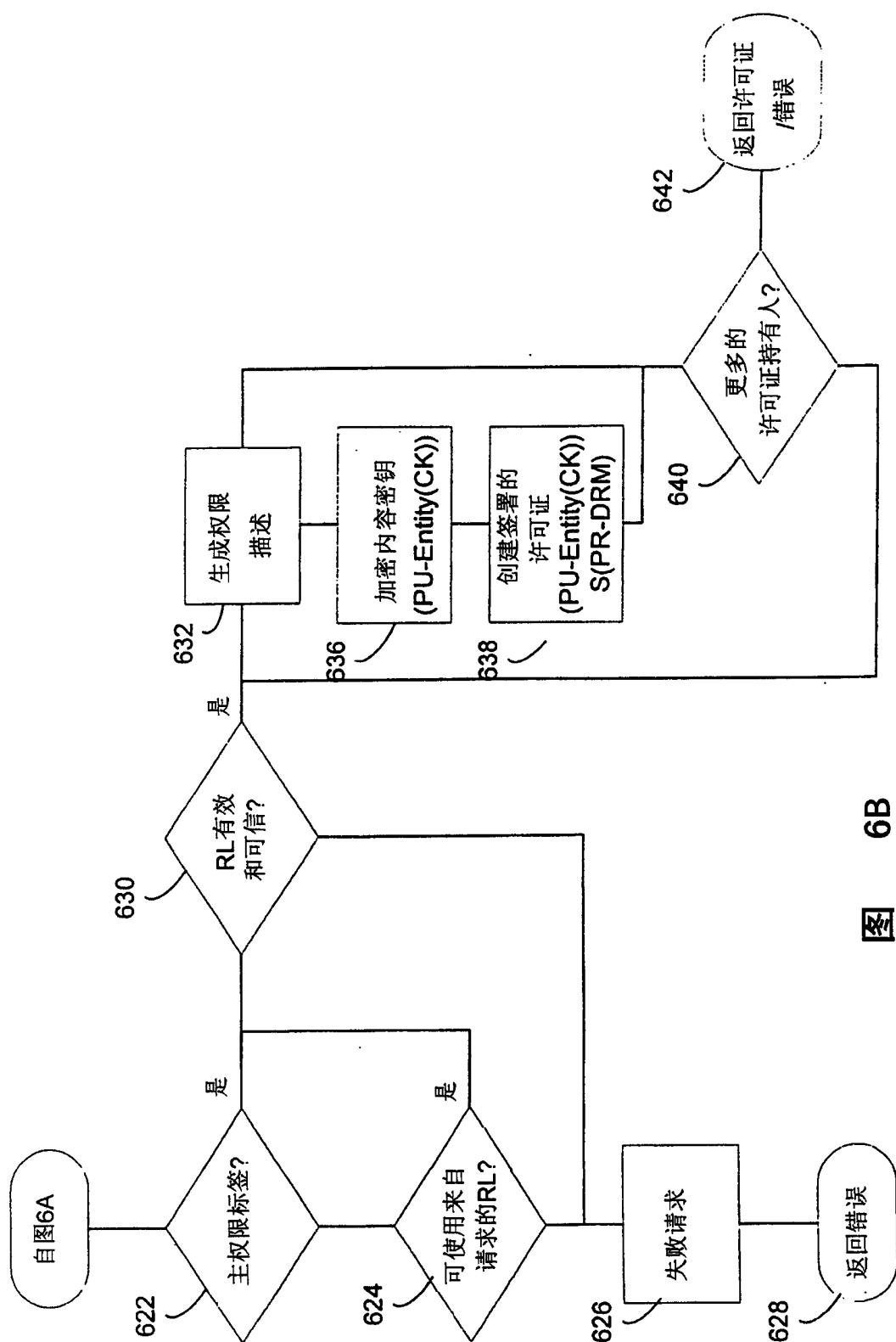


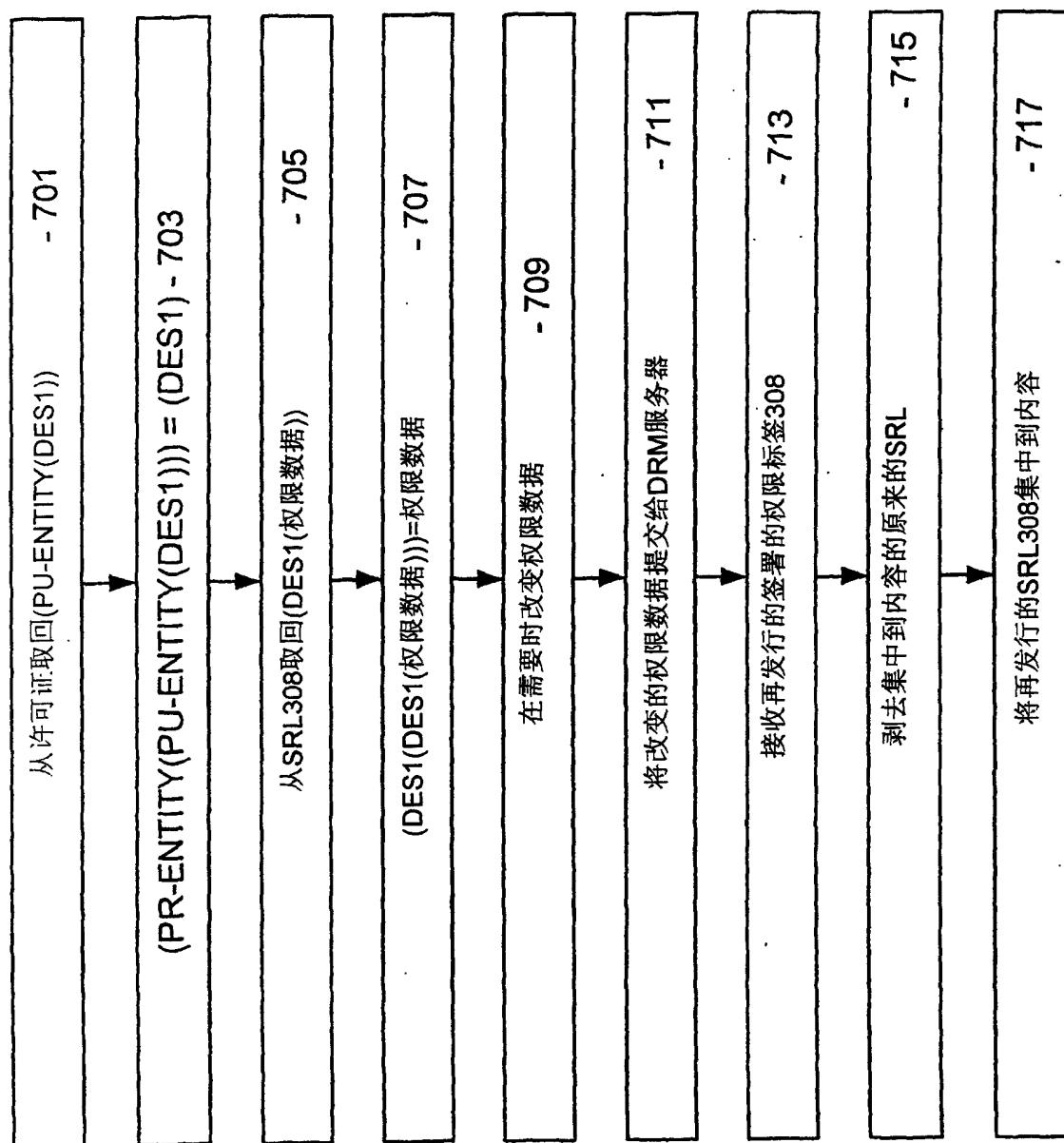
图 5





6B

图



7

图

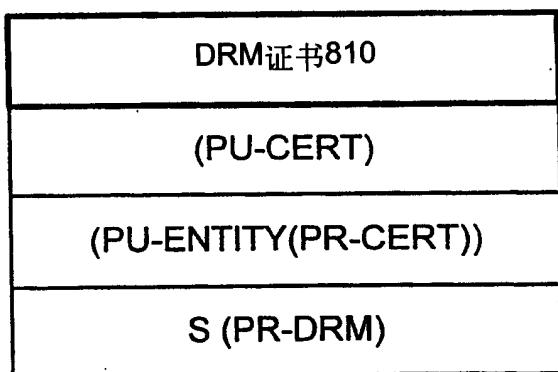


图 8

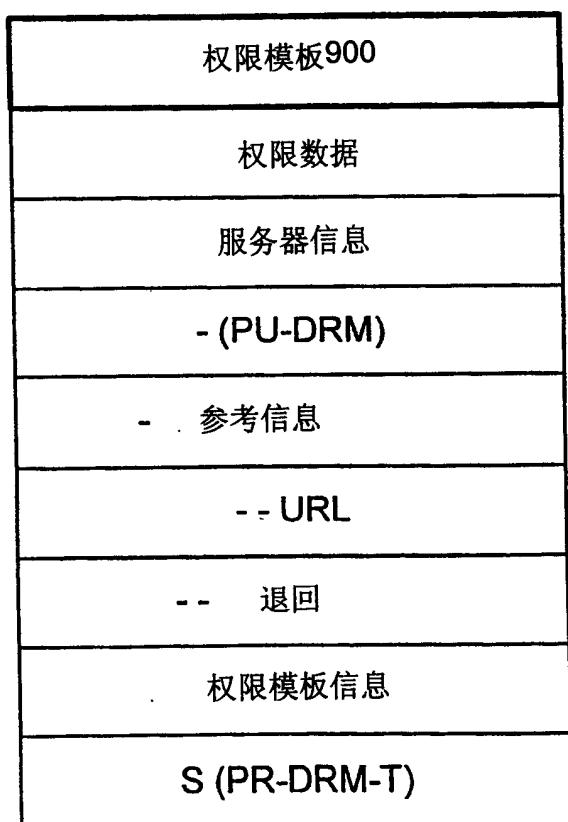


图 9

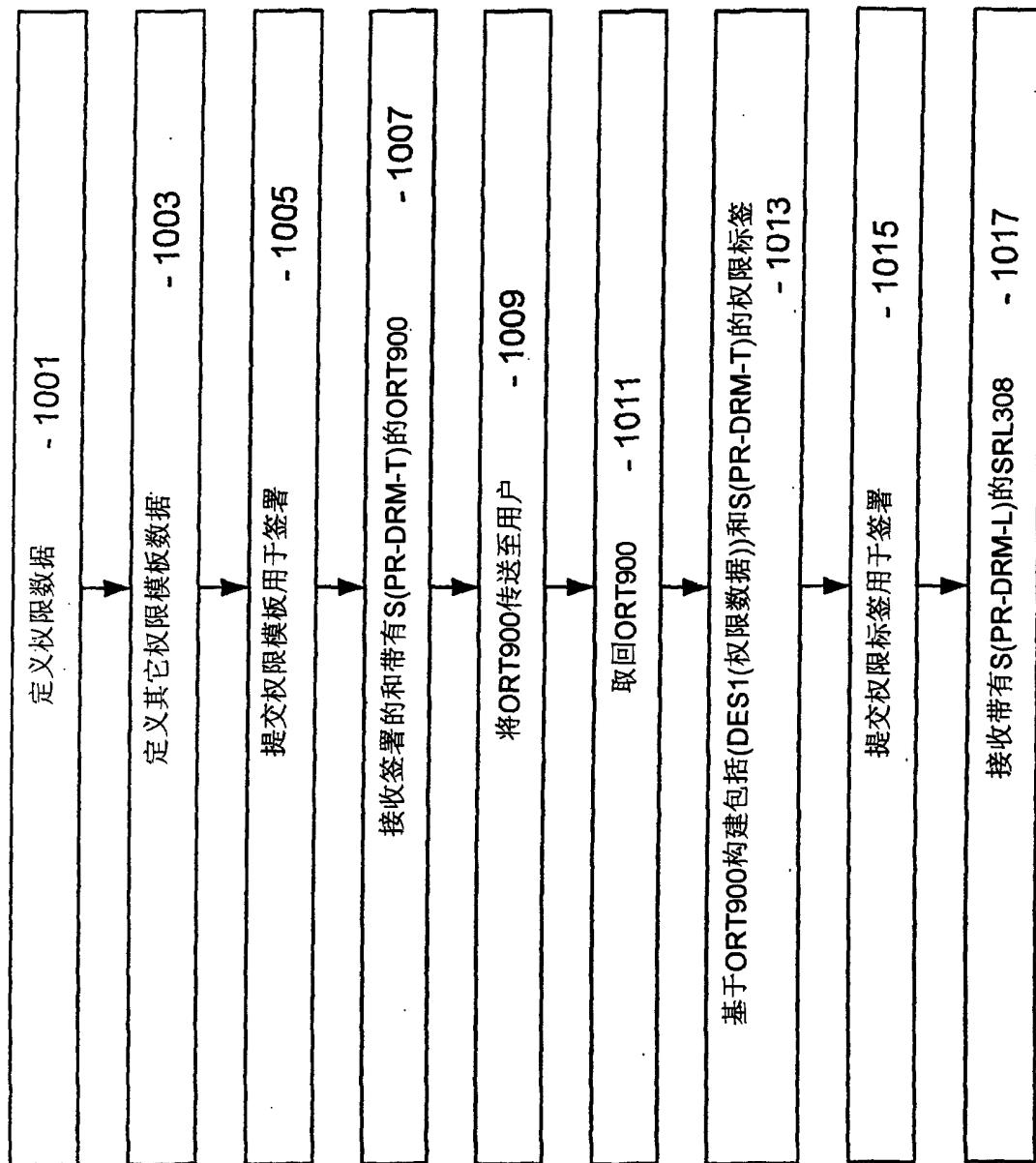
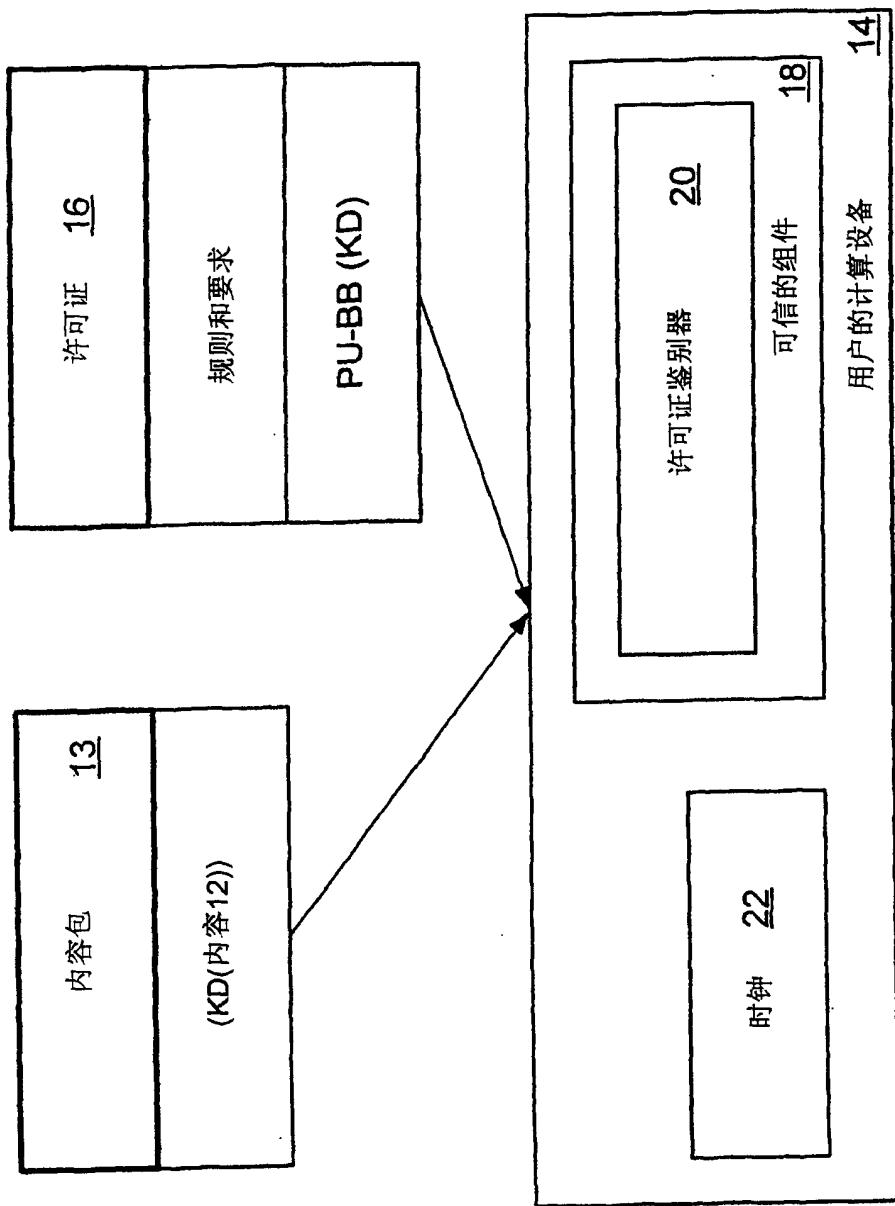


图 10

DRM系统 10



11

图

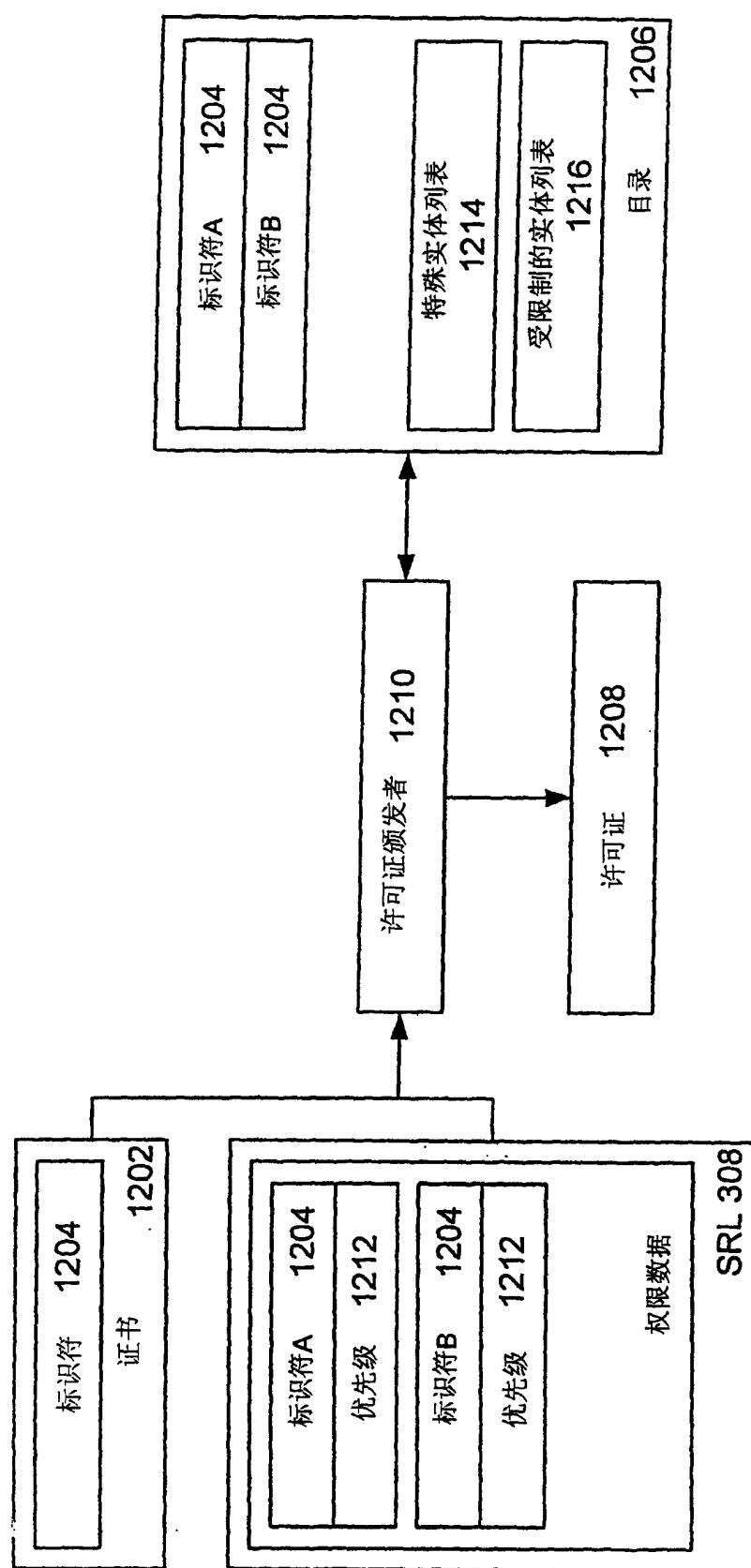


图 12

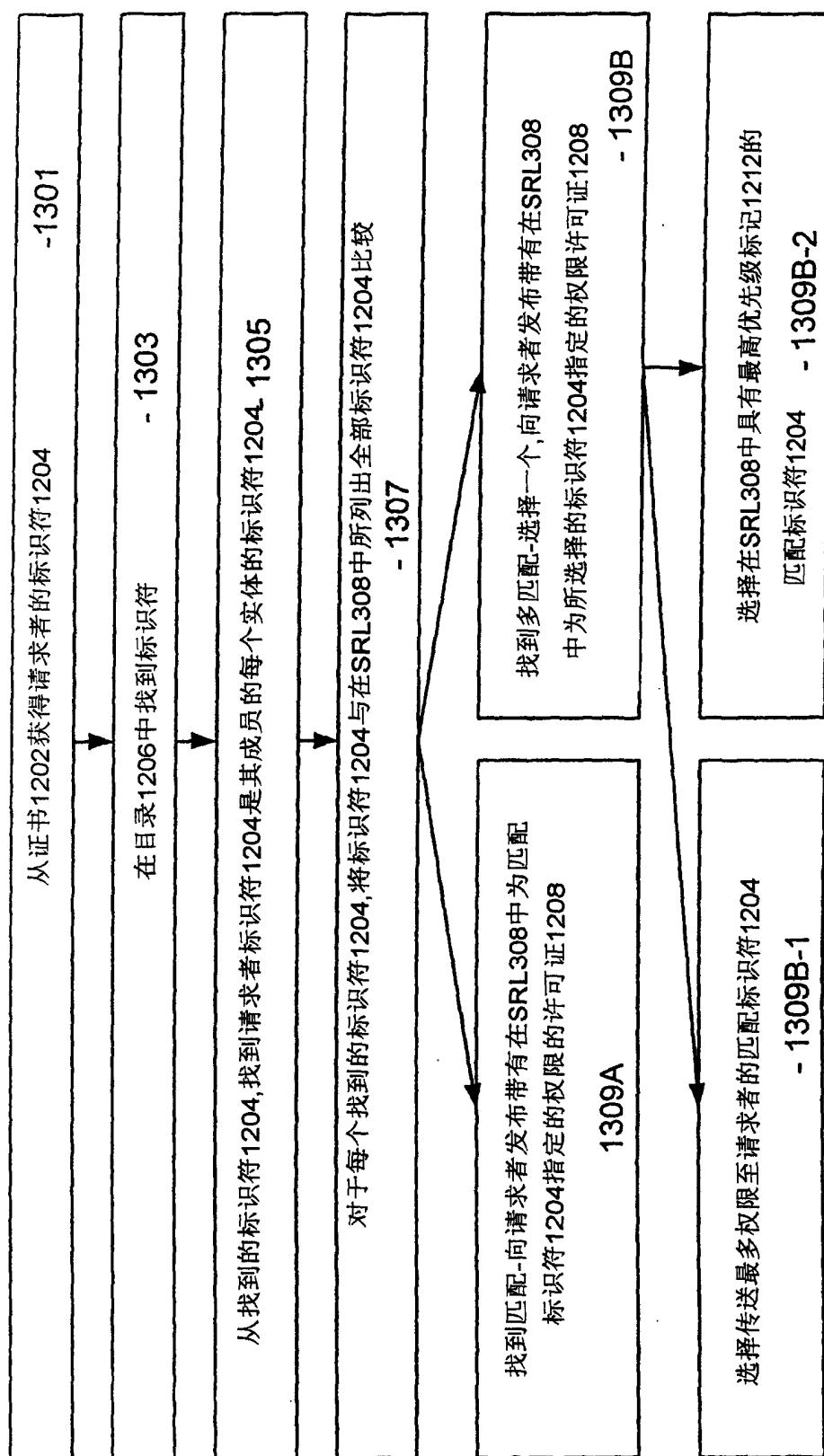


图 13

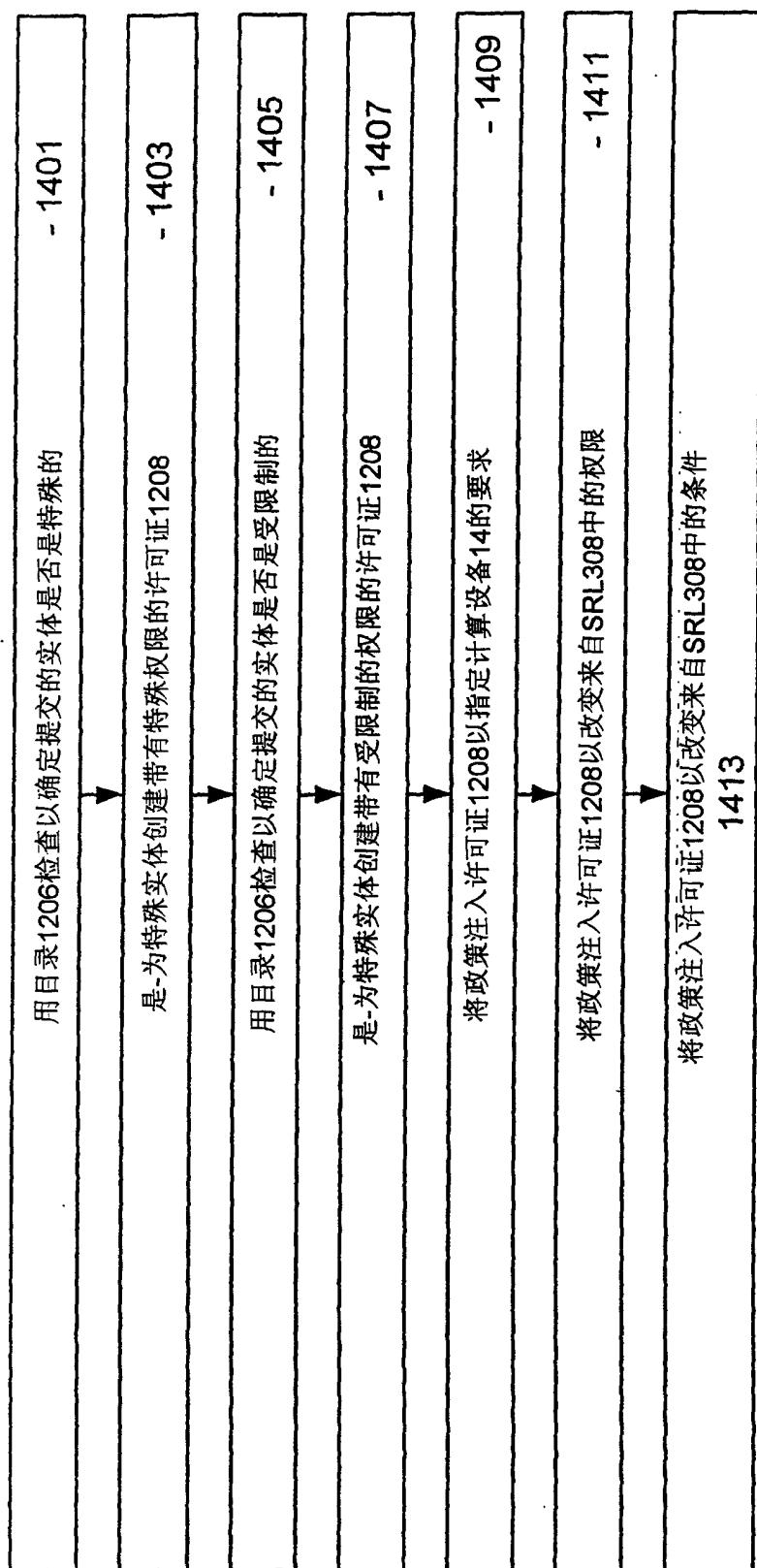


图 14