[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/00

[12] 发明专利申请公开说明书

[21] 申请号 02815592.0

[43] 公开日 2004 年 10 月 20 日

[11] 公开号 CN 1539217A

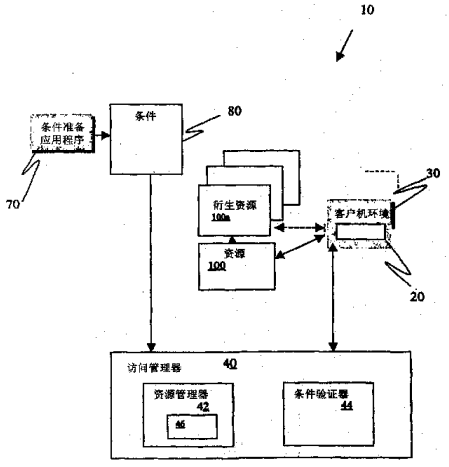
[22] 申请日 2002.6.7 [21] 申请号 02815592.0
[30] 优先权
[32] 2001. 6. 7 [33] US [31] 60/296,113
[32] 2001. 6. 7 [33] US [31] 60/296,117
[32] 2001. 6. 7 [33] US [31] 60/296,118
[32] 2001.11.20 [33] US [31] 60/331,623
[32] 2001.11.20 [33] US [31] 60/331,624
[32] 2001.11.20 [33] US [31] 60/331,625
[32] 2001.11.20 [33] US [31] 60/331,621
[86] 国际申请 PCT/US2002/017753 2002.6.7
[87] 国际公布 WO2002/101975 英 2002.12.19
[85] 进入国家阶段日期 2004.2.9
[71] 申请人 康坦夹德控股股份有限公司
地址 美国特拉华州
[72] 发明人 T·塔 T·德马蒂尼 J·Z·丰
G·劳 M·纽耶恩 B·塔达阳
V·迪由 D·特兰 X·王
[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 3 页 说明书 13 页 附图 5 页

[54] 发明名称 通过校验条件管理资源访问和使用的方法及相应使用条件

[57] 摘要

一种方法和装置，用于管理对资源的访问，所述方法和装置集成了对大范围资源的授权和保护。访问受保护资源(100)的权利是基于条件的。 条件和资源及资源的状态关联，从而在其生命周期中的不同阶段保护资源。 和受保护资源的整个生命周期关联的条件可以通过使用包括数据结构、成组的规则或语言(44)的语法来表示。



ISSN1008-4274

知识产权出版社出版

1. 一种方法，用于管理受保护资源在资源系统中的使用，其特征在于，所述方法包括：

当满足和受保护资源及该主体关联的先决条件时，授权主体对该受保护资源的访问；

当满足和该受保护资源及该主体关联的访问中条件时，允许该主体继续访问该受保护资源，所述访问中条件和所述先决条件不同；及

当终止事件发生时，终止该主体对该受保护资源的访问，所述终止事件包括满足不同于所述访问中条件的访问后条件或不能继续满足所述访问中条件。

2. 如权利要求 1 所述的方法，其特征在于，其中，所述先决条件和使用权关联；且其中，所述受保护资源包括和使用权关联的主资源及用于连同该主资源执行该使用权的衍生资源。

3. 如权利要求 2 所述的方法，其特征在于，其中，所述主资源是数字内容，且所述衍生资源是用于呈现所述受保护内容的资源。

4. 如权利要求 1 所述的方法，其特征在于，其中，所述访问中条件指定表示该受保护资源的状态的状态变量；且其中，根据所述访问中条件评估所述状态变量的值，以确定是否满足所述访问中条件。

5. 如权利要求 2 所述的方法，其特征在于，其中，所述访问中条件应用于所述主资源和所述衍生资源。

6. 如权利要求 1 所述的方法，其特征在于，其中，所述访问中条件包括其中该受保护资源被访问的系统的状态的条件。

7. 如权利要求 1 所述的方法，其特征在于，其中，所述访问中条件包括其中驻留该受保护资源的设备的条件。

8. 如权利要求 1 所述的方法，其特征在于，其中，所述受保护资源是数字内容。

9. 一种方法，用于管理受保护资源在资源系统中的使用，其特征在于，所述方法包括：

准备必须满足才能获取对受保护资源的访问的先决条件；

准备必须满足才能继续访问所述受保护资源的访问中条件；

当所述受保护资源待用时，实施所述先决条件，直到满足所述先决条件；及

当满足所述先决条件时，使所述受保护资源可用并实施所述访问中条件。

10. 如权利要求 9 所述的方法，其特征在于，进一步包括这个步骤：当终止事件发生时，终止该主体对该受保护资源的访问；所述终止事件包括满足不同于所述访问中条件的访问后条件或不能继续满足所述访问中条件。

11. 如权利要求 10 所述的方法，其特征在于，其中，所述先决条件和使用权关联；且其中，所述受保护资源包括和该使用权关联的主资源及用于连同该主资源执行该使用权的衍生资源。

12. 如权利要求 11 所述的方法，其特征在于，其中，所述主资源是数字内容，且所述衍生资源是用于呈现所述受保护内容的资源。

13. 如权利要求 10 所述的方法，其特征在于，其中，所述访问中条件指定表示该受保护资源的状态的状态变量；且其中，根据所述访问中条件评估所述状态变量的值，以确定是否满足所述访问中条件。

14. 如权利要求 11 所述的方法，其特征在于，其中，所述访问中条件应用于所述主资源和所述衍生资源。

15. 如权利要求 10 所述的方法，其特征在于，其中，所述访问中条件包括其中该受保护资源被访问的系统的状态的条件。

16. 如权利要求 10 所述的方法，其特征在于，其中，所述访问中条件包括其中驻留该受保护资源的设备的条件。

17. 如权利要求 8 所述的方法，其特征在于，其中，所述受保护资源是数字内容。

18. 一种条件说明，用以在管理受保护资源的系统中将条件和受保护资源关联，以控制该受保护资源，其特征在于，所述说明包括：

表示和该条件关联的该受保护资源的资源标志；

表示与该条件有关的该资源的状态的状态变量；及

表示可从设备获取该状态变量的值的方式的方法说明。

19. 如权利要求 18 所述的条件说明，其特征在于，其中，所述方法说明包括其上存储该状态变量的值的设备的位置。

20. 如权利要求 18 所述的条件说明，其特征在于，其中，所述方法说明包括获取该状态变量的值的通信协议。

21. 如权利要求 18 所述的条件说明，其特征在于，进一步包括在满足该条件时将要执行的使用权。

22. 如权利要求 18 所述的条件说明，其特征在于，其中，所述条件是在对资源的访问得到授权之后必须满足才能继续使用该资源的访问中条件。

通过校验条件管理资源访问和使用的方法及相应使用条件

版权声明

背景技术

阻止数字著作（即计算机可读形式的文档或其他内容）通过电子方法，特别是因特网，广泛发布的最重要的事项之一是目前在数字著作的发布和使用中缺乏保障内容所有者的知识产权的能力。为解决这个问题所付出的努力被称为“知识产权管理”（“IPRM”）、“数字产权管理”（“DPRM”）、“知识产权管理”（“IPM”）、“权利管理”（“RM”）和“电子版权管理”（“ECM”），在此统称为“数字权利管理（DRM）”。在实现 DRM 系统时有很多事项需要考虑。例如，验证、授权、账目管理、支付和财务清算、权利说明、权利校验、权利实施及文档保护的事项都应该考虑。美国专利 5,530,235，5,634,012，5,715,403，5,638,443 和 5,629,940，其内容被包含在此引用，揭示了处理这些事项的 DRM 系统。

例如，美国专利 5,634,012 揭示了控制数字文档发布的系统。每个呈现设备都有与其关联的存储库。预定的一组使用处理步骤定义了由存储库使用的协议，用于实施和文档关联的使用权。使用权坚持该文档内容。使用权说明该内容的各种使用方式，如只读、使用一次、发布等等。先决条件，如费用的支付、身份的证明或其他条件可以在允许访问该内容之前根据使用权来获取。一旦满足先决条件，对内容的访问即被授权。有条件的访问的概念在访问控制应用中也是众所周知的。例如，大家知道可以基于输入登录名和密码来授权对网络资源的访问。

有条件访问的概念是访问控制和 DRM 系统的基础。典型的先决条件，即授权访问的条件，定义授权用户的列表和一组对给定资源的访问权利和条件。

和给定资源关联的先决条件可以被定义为和特定用户关联的资源。这被称为“基于角色的”访问控制。在被称为“基于规则的”访问控制的处理中，先决条件也可以由规则定义。两种类型的先决条件都可以表示为访问控制列表，访问控制列表是一组以某种语言或数据结构定义的资源或规则。

有条件的访问通常由多数系统作为授权过程来实现，其中，在满足和/或校验特定条件后，允许主体(如，人、系统或过程)对受保护资源进行访问。

发明概要

本发明的第一个方面是在资源系统中管理受保护资源的使用的方法。该方法包括：当满足和受保护资源及主体关联的先决条件时，授权由主体对受保护资源的访问；当满足和受保护资源及主体关联的访问中条件时，允许主体继续访问受保护资源；以及，当发生终止事件时，终止由主体对受保护资源的访问。终止事件可以是满足不同于访问中条件的访问后条件或未能继续满足访问中条件。

本发明的第二个方面是在资源系统中管理受保护资源的使用的方法。该方法包括：准备获得对受保护资源的访问所必须满足的先决条件；以及，准备继续访问所述受保护资源所必须满足的访问中条件。当所述受保护资源待用时，实施所述先决条件，直到满足所述先决条件；且当满足所述先决条件时，使所述受保护资源可用并实施所述访问中条件。

本发明的第三个方面是条件说明，该条件说明适用于关联条件和受保护资源，以便在管理受保护资源的系统中控制受保护资源。该说明包括指示和条件关联的受保护资源的资源标志、根据条件来指示资源状态的状态变量，及指示可从设备获取该状态变量的值的方式的方法说明。

附图说明

本发明通过较佳实施例和附图来加以说明，附图包括：

图 1 为框图，展示较佳实施例的计算机结构；

图 2 为示意图，展示常规的访问控制模型的状态；

图 3 为示意图，展示较佳实施例的状态；

图 4 为流程图，展示较佳实施例的授权过程；

图 5 为示意图，展示较佳实施例的条件；及

图 6 为示意图，展示较佳实施例的条件状态。

详细说明

不同类型的资源要求不同类型的条件和不同的机制来保护它们以防非授权的使用。申请人扩展了常规的先决条件，以包括保护及承诺的条件，从而获取灵活的机制来表示和实施这样的条件。

在较佳实施例中，条件是受保护资源整个生命周期的一部分。这意味着不仅在允许访问之前评估条件，而且在资源的实际消耗过程中也评估条件。另外，条件和受保护资源及受保护资源的状态两者关联。通过将条件和受保护资源的不同状态关联，为内容所有者或服务提供者提供灵活的方式来保护不同类型的资源。资源可以是数字内容、硬件、软件程序、存储空间、货物、服务(包括 web 服务)、时间、费用、使用权或许可证。

使用权指定使用的方式。例如，使用方式可以包括以指定的方法在指定的时期内使用项目的能力。进一步来说，使用权可以指定转让权，如发布权，并可以允许授权使用权给他人或授权使用权的衍生物。

较佳实施例在受保护资源的使用或消耗之前、之中和之后校验并验证条件。条件可以表示为条件状态，以便每个条件的当前状态和历史可以被记录并在以后使用。“状态变量”跟踪潜在动态的条件。状态变量是具有表示资源状态或其他动态条件的值的变量。状态变量可以被跟踪，且状态变量的值可以用在条件中。例如，使用权，作为资源，可以是查看内容的权利，且条件可以是：当执行使用权时，没有其他用户登录到网络。在这例子中，当合适状态的值表明其他用户已登录时，该条件不再被满足，且内容不能被查看，或者查看终止。

图 1 展示较佳实施例的计算机结构 10。条件 80 在下面详细说明，且可以用和项目的发布者、内容服务提供者、企业管理者或希望控制对资源(如数字内容)的访问的任何其他一方关联的准备应用程序 70 来准备。可以用如 XrMLTM 这样的语法来说明条件 80。然而，条件 80 可以用任何方式说明。用户在客户机环境 30(包括计算机或其他和该用户关联的设备)中操作。软件应用程序 20，如呈现引擎或其他应用程序，可以安装在客户机环境 30 中。访问管理器 40 用以下所陈述的方式来控制对受保护资源 100 和衍生资源 100a 的访问。

访问管理器 40——较佳实施例中的计算机设备，处理对资源 100 和衍生资

源 100a 的访问的安全方面。特别是，访问管理器 40 可以通过校验和验证签名(如加密签名)或消息的其他标识字符，用已知的方式验证该消息。访问管理器 40 包括两个主要部件——资源管理器 42 和条件验证器 44。资源管理器 42 负责资源注册、资源转换和资源终止。“转换”指从资源 100 得到衍生资源 100a。例如，在资源是表示图像或类似物的加密文件的情况下，衍生资源 100a 可以包括原始图像自身和保存该图像的存储器的地址。在资源注册的过程中，保存该图像的存储地址由资源管理器 42 的资源存储库 46 记录，以便对该存储器(即衍生资源 100a)的任何访问都可以被跟踪。另外，跟踪标志(如水印)可以插入图像，使其能在任何时间被跟踪。

条件验证器 44 监控设置的条件并管理系统的当前状态。如下面的详细说明，条件验证器 44 和资源管理器 46 交互作用，来控制衍生资源 100a。在当前系统状态不再有效时，条件验证器 44 请求资源管理器 42 删除(或禁用)所有的衍生资源 100a 或通知应用程序 20：不再允许使用衍生资源 100a(如下面的详细说明)。

对受保护资源 100 的访问是基于条件 80 的。这种类型的条件被称为访问条件或“先决条件”。然而，通过将条件和资源 100 及资源 100 的状态两者关联，可能在其生命周期中的不同阶段保护资源 100。资源 100 可以在用户被授权访问之前、在授权访问时、在资源 100 的实际使用中和在使用资源 100 之后受到保护。和受保护资源的整个生命周期关联的条件 80 可以通过使用包括数据结构、成组的规则或如 XrMLTM 这样的语言的语法来表示。较佳实施例使用 XrMLTM，作为表示条件的语言。

为了保护资源 100，条件 80 可以被强加于资源 100 自身或其他任何资源——无论是有形的还是无形的——包括那些构成任何执行环境的资源(如客户机环境 30 的应用程序 20)，通过其访问和使用受保护资源 100。

条件 80 可以是作为主体被授权访问并使用受保护资源 100 的用户或用户组的身份。条件 80 的例子在下面以 XrMLTM 语言的表示来阐述。例子 A 表示和被授权“查看”受保护数字内容“XrML Book”的主体“Edgar”关联的条件。例子 B 表示和一组主体关联的条件，一组主体即属于被授权打印受保护数字著作“XrML Book”的“ContentGuard employee”种类的所有人。

实例 A

```
<license>
        <inventory>
                <digitalWork licensePartID="XrMLBook"/>
                <keyHolder licensePartID="Edgar"/>
        </inventory>
        <grant>
                <keyHolder licensePartIDRef="Edgar"/>
                <view/>
                <digitalWork licensePartIDRef="XrMLBook"/>
        </grant>
</license>
```

实例 B

```
<license>
        <inventory>
                <digitalWork licensePartID="XrMLBook"/>
        </inventory>
        <grant>
                <forAll varName="ContentGuard Employee"/>
                <principal varRef=" ContentGuard Employee"/>
                <print/>
                <digitalWork licensePartIDRef="XrMLBook"/>
        </grant>
</license>
```

条件 80 可以是主体必需拥有特定属性(如特定头衔，或权利，如安全许可)的条件。例子 C 表示主体必需拥有管理者身份的条件。

实例 C

```
<license>
        <inventory>
                <digitalWork licensePartID="XrMLBook"/>
                <keyHolder licensePartID="Edgar"/>
        </inventory>
        <grant>
                <forAll varName="anyone"/>
                <principal varRef="anyone"/>
                <possessProperty/>
                <badge>
                <title>Manager</title>
                </badge>
                <view/>
                <digitalWork licensePartIDRef="XrMLBook"/>
        </grant>
</license>
```

条件 80 可以是对受保护项目访问的时间间隔的条件。下面的例子 D 表示作为主体的密钥持有者“Edgar”在 2002 年 5 月 29 日到 2003 年 5 月 29 日期

间可以查看内容“XrML book”的条件。

实例 D

```
<license>
    <inventory>
        <digitalWork licensePartID="XrMLBook"/>
        <keyHolder licensePartID="Edgar"/>
    </inventory>
    <grant>
        <keyHolder licensePartIDRef="Edgar"/>
        <view/>
        <digitalWork licensePartIDRef="XrMLBook"/>
        <validityInterval>
            <notBefore>2002-05-29T00:00:00</notBefore>
            <notAfter>2003-05-29T00:00:00</notAfter>
        </validityInterval>
    </grant>
</license>
```

条件 80 可以和被用来访问内容的主体或资源的物理位置相关。下面的例子 E 表示目前在美国的任何人都可以打印内容“XrML Book”的条件。

实例 E

```
<license>
    <inventory>
        <digitalWork licensePartID="XrMLBook"/>
    </inventory>
    <grant>
        <forAll varName="anyone"/>
        <principal varRef="anyone"/>
        <print/>
        <digitalWork licensePartId="XrMLBook"/>
        <territory>
            <country>US</country>
        </territory>
    </grant>
</license>
```

条件 80 可以指定主体必须为访问支付的费用。下面的例子 F 表示任何人在支付 $3.10 的费用之后都可以打印内容“XrML book”的条件。下面的例子 G 表示任何人在为每次打印支付 $3.10 的费用之后都可以打印内容“XrML book”的条件。下面的例子 H 表示任何人在为每小时的查看时间支付 $10.00 的费用之后都可以查看内容“XrML book”的条件。

实例 F

```
<license>
        <inventory>
                <digitalWork licensePartID="XrMLBook"/>
        </inventory>
        <grant>
                <forAll varName="anyone"/>
                <principal varRef="anyone"/>
                <print/>
                <digitalWork licensePartId="XrMLBook"/>
                <fee>
                        <paymentFlat>
                        <rate currency="USD">3.10</rate>
                        </paymmentFlat>
                        <to>
                        <aba>
                        <institution>123456789></institution>
                        <account>987654321</account>
                        </aba>
                           </to>
                   </fee>
            </grant>
     </license>
```

实例 G

```
  <license>
          <inventory>
                  <digitalWork licensePartID="XrMLBook"/>
          </inventory>
          <grant>
                  <forAll varName="anyone"/>
                  <principal varRef="anyone"/>
                  <print/>
                  <digitalWork licensePartIDRef="XrMLBook"/>
                  <fee>
                          <paymentPerUse>
                          <rate currency="USD">3.10</rate>
                          </paymentPerUse>
                  </fee>
           </grant>
    </license>
```

实例 H

```
<license>
       <inventory>
              <digitalWork licensePartID="XrMLBook"/>
              </inventory>
```

```
<grant>
<forAll varName="anyone"/>
<principal varRef="anyone"/>
<view/>
<digitalWork licensePartIDRef="XrMLBook"/>
        <fee>
                <paymentMetered>
                <rate currency="USD">10.00</rate>
                <per>PT1H</per>
                <phase>PT10M</phase>
                </paymementMetered>
                <to>
                <aba>
                <institution>123456789></institution>
                <account>987654321</account>
                </aba>
                </to>
        </fee>
</grant>
</license>
```

下面的例子 I 表示的条件是：任何人都可以打印内容，但打印权的执行将由跟踪服务在打印前跟踪。

实例 I

```
<license>
        <inventory>
                <digitalWork licensePartID="XrMLBook"/>
                <keyHolder licensePartID="Edgar"/>
        </inventory>
        <grant>
                <forAll varName="anyone"/>
                <principal varRef="anyone"/>
                <print/>
                <digitalWork licensePartIDRef="XrMLBook"/>
                <trackReport>
                        <stateReference>
                                <uddi>
                                <serviceKey>
                                <uuid>...</uuid>
                                </serviceKey>
                                </uddi>
                                <serviceParam>
                                </serviceParam>
                        </stateReference>
                </trackReport>
        </grant>
</license>
```

条件 80 也可以是对在其中消耗资源 100 的系统的条件。例如，条件 80 可以要求：系统有授权的安全机制或其他特定硬件或软件，或仅有特定最大数量的用户可以登录。

条件 80 可以指定其中驻留资源 100(如内容)的存储库或其他设备。条件 80 可以和主体必须在使用受保护资源 100 之前获取的批准通知相关。条件 80 可以在使用资源 100 之前或之后要求通知。条件 80 可以指定和受保护资源 100 或其他资源相关的原先的权利。条件 80 也可以被强加于其他条件 80(如怎样校验条件)。

当然，条件 80 并不局限于上述例子，而可以是作为先决条件、访问中条件和访问后条件的任何和受保护资源 100 关联的限制、义务或要求。同样，即使上述例子是使用 XrMLTM 表示的，条件也并不局限于 XrML 或被 XrML 限制，且能够以任何方式表示。

图 5 根据较佳实施例示意性地展示条件 80。条件 80 包括可以隐含或明确表示的资源标志 42。例如，在上述的例子 A 中，资源标志 42 由“digitalWork”元素的“licensePartID”属性表示。条件 80 也包括状态变量 44，及表示如何可以获取状态变量 44 的值的方法说明 46。方法说明 46 可以包括存储状态变量 44 的值的位置(如管理条件的远程服务器)、用来和管理该条件的服务器进行通信的通信协议，及获取该值所需的任何参数(如服务参数等)。替换地，该方法可以被硬编码在系统中，且方法说明 46 可以被略去。

如上所述，状态变量 44 表示条件 80 的状态。关于给定权利的所有状态变量 44 的集合在此称为“权利状态”。每个状态变量 44 在任何时间对主体、权利和资源都有对应的值。条件 80 的所有状态变量 44 的集合在此只被称为“条件状态”。图 6 展示包括条件 80 的条件状态 50，及条件 80 的状态变量 44 的当前值 52。方法说明 56 表示用来获取状态变量 44 的当前值 52 的方法，潜在地包括获取该值的来源、凭证的数字签名、请求的会话 ID 及其他任何适当的信息。注意，方法说明 56 可以被视为和方法说明 46 冗余，且可以仅为它的重复。然而，在一些情况下，被用于实际获取值 52 的方法说明 56 可以不同于建议在条件 80 中使用的方法说明 46。

通过使用条件状态 50 来表示关于权利的条件 80，可简化校验条件 80 的过程，因为校验条件 80 所需的所有信息是容易获得的。无论何时评估和校验对应的条件 80，都构建并(然后)使用条件状态 50。每个条件状态 50 可以包含校

验状态变量 44 的值 52 所需的所有信息。和已验证的主体及受保护资源 100 关联的给定权利的条件状态 50 的集合在此称为“系统状态”。

已验证的主体是已由验证用户可靠性的系统处理的那个用户，例如当用户成功地用用户名和密码登录时，该用户成为已验证的主体或只是“主体”。使用“系统状态”概念，给定组的权利的条件 80 被定义为一组在其下允许主体访问受保护资源 100 的所需系统状态。当已验证的主体希望访问受保护资源 100 时，系统状态从“初始状态”变成 “特许状态”。

一旦系统处于特许状态，主体就能够访问受保护资源 100，以进行授权操作。在很多情况下，并不是已验证的主体自身实际访问受保护资源 100。例如，该访问可以委托给另一已验证的主体，如呈现应用程序、服务等等。虽然受保护资源 100 被访问和消耗，但授权初始访问的那组访问前条件 80 对授权继续的访问可能不再适用。同样，消耗受保护资源 100 可以将该资源转换为一组临时的(即衍生的)资源 100a ，而从中，施于初始资源的访问条件 80 也不适用。为了在访问资源 100 和它的衍生资源 100a 时对其进行保护，较佳实施例使用被称为“访问中条件”的授权和保护的概念，下面对其进行详细说明。

在常规系统中，资源处于两种状态之一。如图 2 所示，当资源 100 待用时，系统处于初始状态 102，直到满足先决条件。在那时，资源 100 变得可用，且系统进入特许或可用状态 104。为了增强对资源的控制，除“初始状态”和“特许状态”外，较佳实施例还定义两种附加的状态。如图 3 所示，在受保护资源 100 的使用或访问中，系统状态将经下述状态改变：初始状态 102、特许状态 104、使用状态 106 和终止状态 108。可以为每种状态定义条件 80，必须满足该条件，才能转移到下一状态或继续保持同一状态。如上述引用图 1， 可以使用包括任何必要的用户界面和编辑能力的准备应用程序 70 来定义和准备条件 80。需要被满足才能进入“特许状态”的条件 80 被成为“先决条件”。在使用资源 100 的过程中需要满足的条件 80 被称为“访问中条件”，在使用终止时需要的条件 80 被称为“访问后条件”。条件验证器 44 可以调用每种状态的必需条件。

访问中条件是条件 80，当它们由已验证的主体访问和消耗时，条件 80 从初始资源 100 转换到其自身和任何衍生资源 100a。例如，如果资源 100 是在授权操作“查看”的过程中被显示在客户机环境 30 的屏幕上的文档，然后，衍生资源 100a 可以各自包括包含来自文档的数据的存储器、文档的呈现格式，

及显示窗口。衍生资源 100a 全部将由该组访问中条件保护。换句话说，只要满足访问中条件，主体就将只访问衍生资源 100a。访问中条件可以用和其他条件 80 相同的方式定义。

在另一例子中，应用程序(如应用程序 20)或其他用户请求是受保护资源 100 的服务。一旦该请求被授权，执行该服务的应用程序可以被看作衍生资源并在执行该服务时受访问中条件的约束。访问中条件不断地更改系统状态，直到衍生资源不再被使用或系统状态变为未授权。一旦请求的操作完成(或者强制地，或者自发地)，所有由访问中条件保护的衍生资源 100a 被删除(或禁用)，然后，系统状态由那组访问后条件转换到最终状态。

条件 80 在资源的使用或访问之后或之中可以或可以不改变。有未改变状态的那些条件称为“无状态条件”，而在使用资源之后或之中改变的条件称为“有状态条件”。先决条件 80 通常是无状态条件 80，且被用来控制对受保护文档的访问。访问中条件和访问后条件通常是有状态条件 80。它们被用来控制受保护资源 100 的生命期。(例如，一旦登录到网络的用户超过指定数量，就不能再访问受保护资源 100。)用这些和不同阶段的受保护资源 100 关联的扩展类型的条件 80，较佳实施例提供一种机制，该机制用于授权使用受保护资源 100，并且在使用资源 100 时保护并跟踪它。

如图 3 所示并参照图 1 中的元素，根据较佳实施例的系统经历三个阶段。在“访问授权”阶段 302 中，访问管理器 40 通过校验满足先决条件来授权已验证的主体访问受保护资源 100，以进行授权操作。在资源保护阶段 304 中，访问管理器 40 通过校验仍然被满足的访问中条件，在它们被使用的时候保护资源 100 及其衍生资源 100a。在操作终止阶段 306 中，访问管理器 40 在满足访问后条件或停止满足访问中条件时，终止受保护资源 100 和衍生资源 100a 对给定操作的使用。

在递归情况下，其中对同一资源 100 有多个访问，访问后条件可以和下一个循环的先决条件相同。在这样的情况下，可以使用非静态参数，以防止无限循环的情况。例如依赖于时间的条件或由外部实体(如人为干预)更改或强加的条件。

访问授权将访问受保护资源 100 以便进行授权操作的权利授权给已验证的主体。图 4 展示根据较佳实施例的访问授权程序，它包括：在步骤 400 中，基于和已验证的主体、操作，及受保护资源 100 关联的条件 80 的列表，来收集

当前系统状态。每个状态条件 50 可以由访问管理器 40 从本地系统或远程系统，从设备、应用程序、存储库或服务来获取。步骤 400 的结果是初始状态。在步骤 402 中，先决条件中的每个状态变量 44 的当前值 52 由访问管理器 40 收集。当前值 52 可以汇编成记录(例如，XML 文档)。可以验证用来构建该记录的信息(例如，验证资源 100 的主体)。在步骤 404 中，根据该记录来评估(即实施)先决条件。例如，存储在该记录中的信息(该信息包含先决条件的每个状态变量 44 的当前值 52)可以被接受并/或进行不同的处理(如校验该记录的签名或重新评估所有的先决条件值)。如果成功实施，则在步骤 406 中，资源 100 和任何衍生资源 100a 进入特许状态。

根据条件验证器 42 在验证该组访问前条件时所使用的方法，授权过程可以分类为“自发的”或“强制的”。接受存储在上述记录中的状态变量 44 的值的过程被称为“自发的”过程，而质询那些值的系统被称为“强制的”过程。在强制的过程中，一旦任何条件 80(包括先决条件、访问中条件或访问后条件)不能被满足时，受保护资源 100 及其所有的衍生资源 100a 就被禁用。当资源 100 或衍生资源 100a 被禁用(或变得无效)时，应用程序 20 不能再访问受保护资源 100。在自发的过程中，如果任何条件 80 不能被满足且变得无效，应用程序 20 会收到通知。然后，应用 20 程序负责禁用受保护资源 100 和衍生资源 100a。是否禁用的决定可以自动作出或在人的干预下作出。实施步骤 404 将把系统从它的初始状态改变到特许状态(步骤 406)或拒绝状态(步骤 404)。在特许状态中，受保护资源 100 被释放给所请求的主体或其委托的主体，并开始实施访问中条件。注意，访问中条件可以不同于先决条件，以提供对资源 100 的灵活的控制。

如上所述，资源保护通过实施该组访问中条件，来保护初始受保护资源 100 和它的衍生资源 100a。从访问授权状态返回的特许状态包含将要在已授权操作中实施的访问中条件的列表。在强制的系统中，当产生和使用衍生资源 100a 时，所有的衍生资源 100a 可以注册资源管理器 42 的资源存储库 46。如果任何访问中条件变得无效，资源管理器 42 将禁用由应用程序 20 对受保护资源 100 及衍生资源 100a 的访问。

在其他类型的系统(例如，“跟踪系统”)中，跟踪对象(如特殊标志或 ID)在资源注册和转换的过程中被插入衍生资源 100a。这使得能够用资源保护部件跟踪资源。插入标志可以采用对处理衍生资源 100a 的应用程序而言透明的格

式。跟踪系统可以是强制的系统或自发的系统。

授权操作的终止执行那组访问后条件(如果有的话)。执行访问后条件永久地改变系统状态并影响访问资源 100 的下一次请求。例如，如果访问后条件是在执行限制达到之后移除对资源 100 的访问；当达到限制时，资源 100 被删除或采取其他禁用或防止访问的动作。操作终止可以包括资源终止。无论操作是被迫终止，还是应用程序自发地终止该操作，当操作被终止时，资源管理器 42 都可以删除(禁用)衍生资源 100a。删除(或禁用)衍生资源 100a 在保护资源 100 的过程中很重要。条件验证器 44 保证受保护资源 100 的使用，并实施那组访问后条件。作为系统状态改变的结果，如果资源 100 变得无效，条件验证器 44 将使受保护资源 100 无效(禁用)。

较佳实施例可利用不同的设备，如个人计算机、服务器、工作站、PDA、瘦客户等。例如，客户机环境可以是手持设备(如移动电话或 PDA)。可以使用不同的通信通道。进一步来说，不同的功能可以集成在一个设备中。为清楚起见，所揭示的功能设备及模块由功能来划分。然而，不同的功能可以用任何方式合并或划分为硬件和/或软件模块和设备。不同的功能模块和设备有单独或合并的效用。

其不同的记录、消息、元件和部分可以被存储在同一设备或不同设备上。不同的连接、引用、说明及类似物可以用来关联元件。对任何类型的资源的访问都可以被控制。可以使用用于跟踪状态变量的值的任何机制。

已通过较佳实施例和例子对本发明进行了说明。然而，可以做出不同的修改，而不偏离由后附的权利要求和法律相等物定义的本发明的范围。

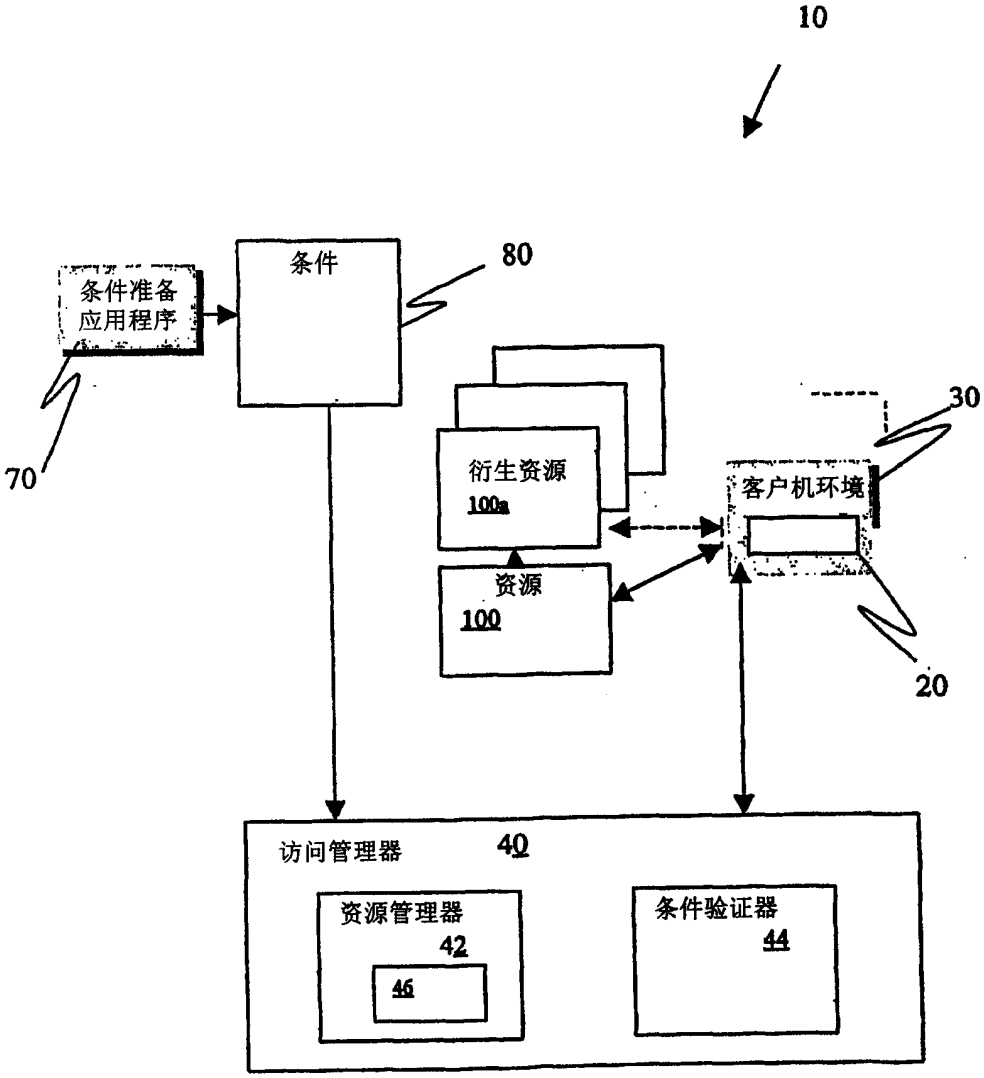

10
条件准备
应用程序
条件
80
70
衍生资源
100a
资源
100
客户机环境
30
20
访问管理器
40
资源管理器
42
46
条件验证器
44

图 1

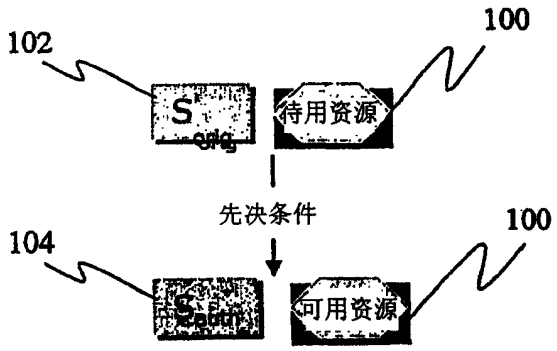

102
100
待用资源
先决条件
104
100
可用资源

图 2

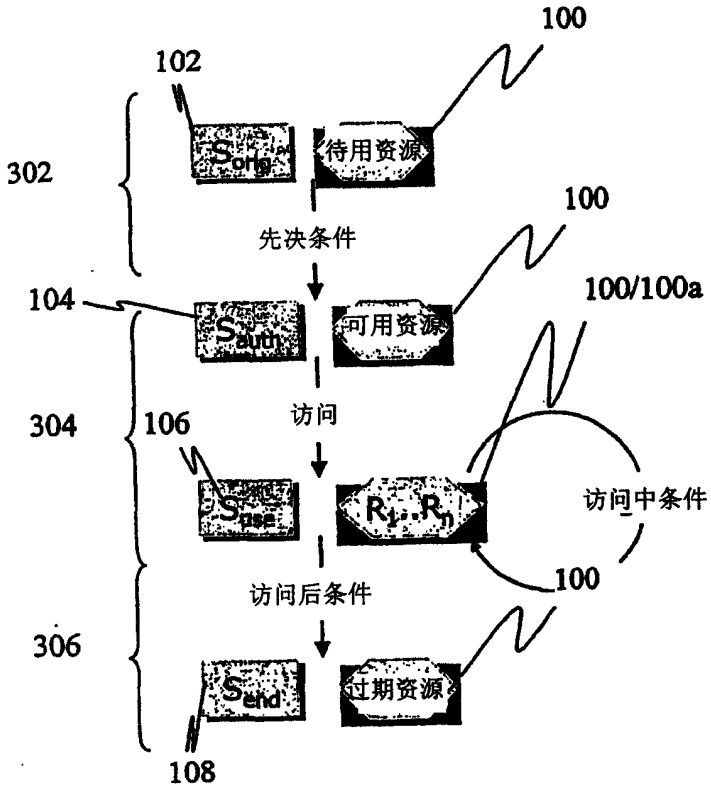

100
102
302
待用资源
100
先决条件
104
100/100a
可用资源
访问
304
106
访问中条件
100
访问后条件
306
过期资源
108

图 3

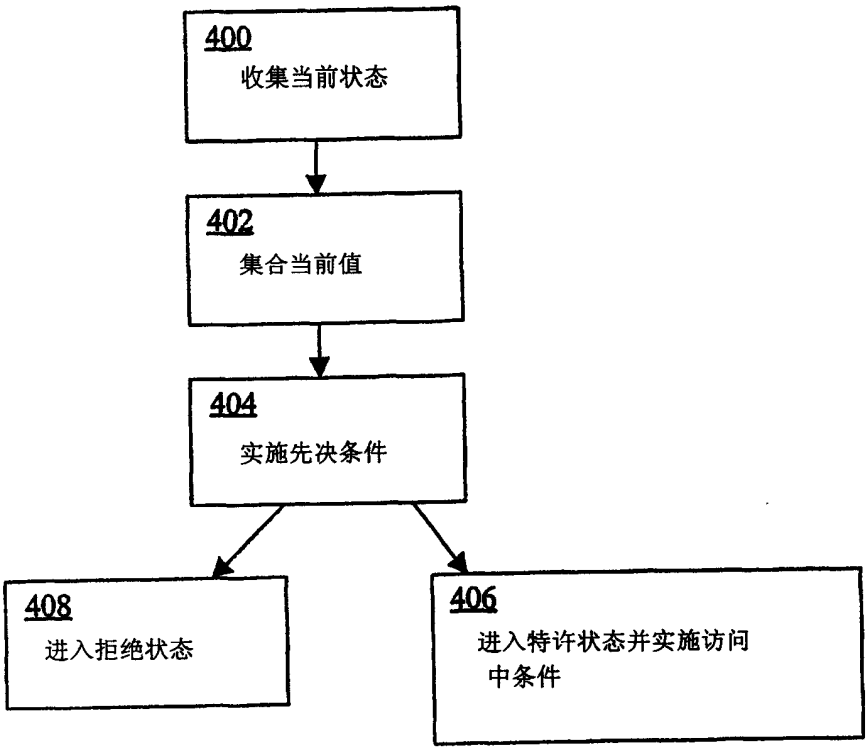

400
收集当前状态
402
集合当前值
404
实施先决条件
408
进入拒绝状态
406
进入特许状态并实施访问中条件

图 4

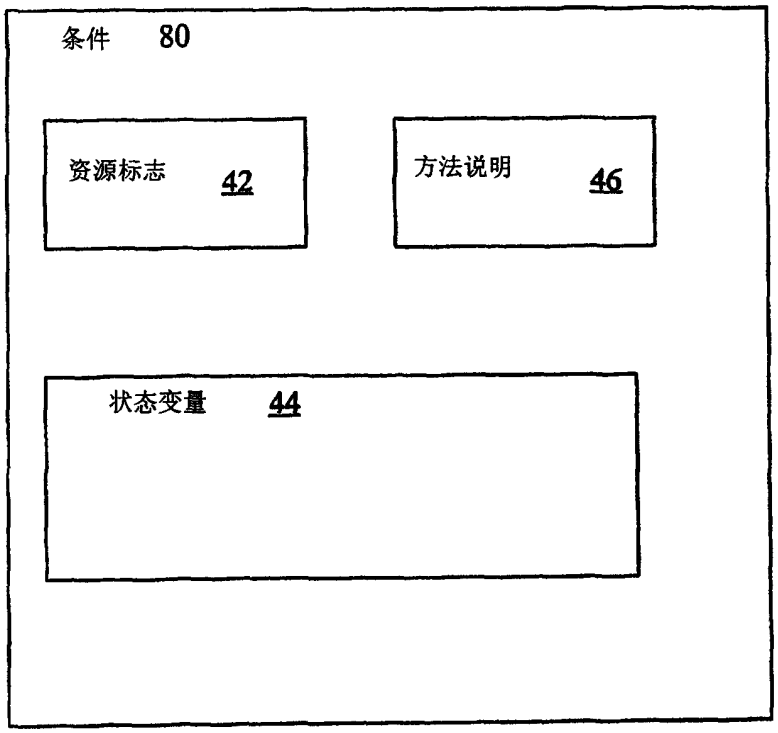


图 5

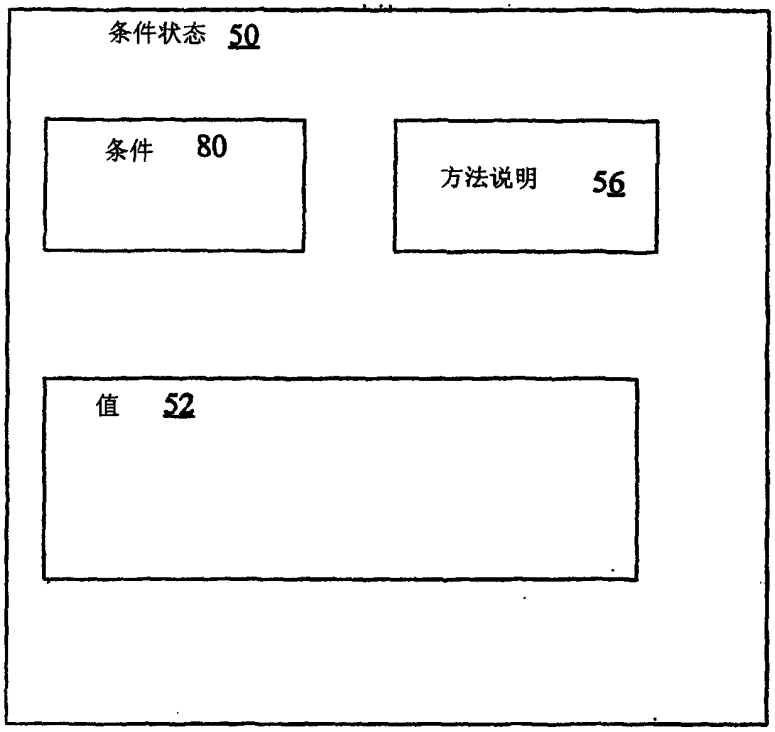


图 6