[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510087692.9

[43] 公开日 2006 年 2 月 1 日

[11] 公开号 CN 1728038A

[22] 申请日 2005.7.29
[21] 申请号 200510087692.9
[30] 优先权
[32] 2004. 7.30 [33] EP [31] 04103696.3
[71] 申请人 耶德托存取公司
地址 荷兰霍夫多普
[72] 发明人 安德鲁·A.·瓦基斯

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 李春晖

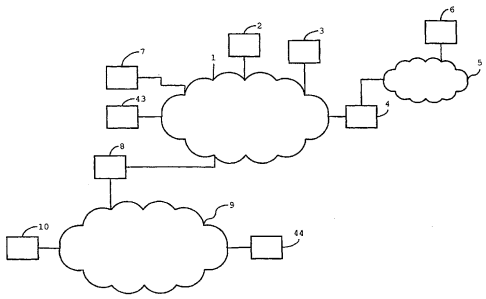
权利要求书 4 页 说明书 24 页 附图 2 页

[54] 发明名称

提供权限数据对象的方法

[57] 摘要

本发明公开了一种方法，用于提供权限数据对象以发布到下述设备，所述设备能访问与位置指示和事件信息一起提供的属于多个事件中的一个的加密内容，所述位置指示指示从其可以请求到权限数据对象的位置，所述事件信息与该事件唯一地关联，所述设备包括代理功能，用于向从所指示的位置发布权限数据对象的设备(24)提供请求和代表该事件信息的数据，包括：接收请求和代表事件信息的数据；生成权限数据对象，该权限数据对象包括使得能够对属于唯一地关联到该事件信息的事件的内容数据进行解密的事件密钥信息，并且其特征在于使用对至少部分事件信息进行运算的密码函数来生成该事件密钥信息。



1. 一种提供权限数据对象以发布到设备（2－4，6）的方法，所述设备能访问属于多个事件中的一个并与位置指示和事件信息一起提供的加密内容，所述位置指示指示从其可以请求到所述权限数据对象的位置，所述事件信息与所述事件唯一地关联，所述设备包括代理功能，用于提供到从所指示的位置发布权限数据对象的设备（24）的请求和代表所述事件信息的数据，所述方法包括:

接收所述请求和代表所述事件信息的数据;

生成权限数据对象，所述权限数据对象包括使得能够对属于唯一地关联到所述事件信息的事件的所述内容数据进行解密的事件密钥信息，并且其特征在于

使用对至少部分所述事件信息进行运算的密码函数来生成所述事件密钥信息。

2. 如权利要求 1 所述的方法，包括从所述加密内容的提供者（7、10）加载密钥信息，并且使用将至少部分所加载的密钥信息与至少部分所述事件信息组合的密码函数来生成所述事件密钥信息。

3. 如权利要求 1 或 2 所述的方法，包括将标识所述事件信息唯一地关联到的所述事件的数据存储到日志中。

4. 如权利要求 3 所述的方法，包括接收来自关联到内容数据的提供者的系统（7、10、43、44）的消息，并且返回至少一个消息，所述至少一个消息包括代表存储在所述日志中的至少部分所述数据的信息。

5. 如权利要求 1 所述的方法，包括将代表实体的信用等级的数据加载并存储到存储器设备（27）中，并且如果所生成的权限数据对象被提供给包括所述代理功能的设备，则修改所存储的数据来反映降低的信用等级。

6. 如权利要求 5 所述的方法，其中，所述代理功能允许包括了所述代理功能的所述设备从与所述加密内容数据一起提供的数据导出证

书，所述方法包括：

接收来自提供所述请求的所述设备（2－4、6）的包括了反映所述事件费用的数据的证书，以及

修改所存储的数据来反映降低了等于所述事件费用的数量的信用等级。

7. 如权利要求 6 所述的方法，包括接收包括了加密形式的所述数据的证书，并且对反映所述事件费用的所述数据进行解密，所述解密优选使用与已用其对所述数据加密的密钥形成公钥/密钥对的密钥。

8. 如权利要求 6 或 7 所述的方法，包括从所接收到的代表所述事件信息的数据提取所述证书。

9. 如权利要求 1 所述的方法，其中，包括所述代理功能的所述设备（2－4、6）被配置以在执行所述代理功能时只根据包括在由所述设备接收到的权限数据对象中的访问权限来提供对加密内容的访问，所述方法包括：

生成还包括至少一个访问权限的权限数据对象。

10. 如权利要求 9 所述的方法，其中，包括所述代理功能的所述设备（2－4、6）被配置以在执行所述代理功能时从与所述加密内容一起提供的数据导出确定许可条件的数据，所述方法包括：

接收来自提供所述请求的所述设备的确定许可条件的导出数据，以及

根据所接收到的导出数据，选择包括在所述权限数据对象中的一个或多个访问权限。

11. 如权利要求 10 所述的方法，包括从所接收到的代表所述事件信息的数据抽取确定所述许可条件的数据。

12. 一种用于向设备（2－4，6）提供权限数据对象的系统，所述设备能访问属于多个事件中的一个并与位置指示和事件信息一起提供的加密内容，所述位置指示指示从其可以请求到所述权限数据对象的位置，所述事件信息与所述事件唯一地关联，所述设备包括代理功能，用于提供到从所指示的位置发布权限数据对象的设备（24）的请求和

代表所述事件信息的数据，其中，所述系统包括:

在安全环境中运行的处理器，和

接口，该接口用于将所述请求和代表所述事件信息的数据传递到所述处理器，其中所述处理器被配置来生成权限数据对象，所述权限数据对象包括使得能够对属于唯一地关联到所述事件信息的事件的所述内容数据进行解密的事件密钥信息，其特征在于

所述处理器还被配置来使用对至少部分所述事件信息进行运算的密码函数来生成所述事件密钥信息。

13. 如权利要求 12 所述的系统，其被配置来执行根据权利要求 1 的方法。

14. 一种计算机程序，其被安排来在被加载到可编程处理设备中时使得所述可编程处理设备执行根据权利要求 1 的方法。

15. 一种方法，用于向属于多个事件中的一个的内容数据附加受限访问权限，以允许至少下述用户系统的组件使用所述内容数据，所述用户系统包括具有代理功能的设备（2－4、6），所述方法包括:

以加密的形式提供至少部分所述内容数据，以使得能够使用事件密钥信息来进行解密，

与其一起提供事件信息，所述事件信息唯一地关联到所述内容数据所属的所述事件中的具体一个，

与其一起提供位置指示，所述位置指示指示从其可以请求到包括至少部分所述事件密钥信息的权限数据对象的位置，

所述代理功能允许其中提供有所述代理功能的设备提供到从所指示的位置发布权限数据对象的设备（24）的请求和代表所述事件信息的数据，其特征在于

所述内容数据的所述加密部分以下述方式被提供，所述方式允许使用作为所提供的事件信息的至少一部分的密码函数的事件密钥信息进行解密，并且其中所指示的位置是被安排来执行根据权利要求 1 的方法的服务器（24）被配置来从其发布权限数据对象的位置。

16. 如权利要求 15 所述的方法，包括生成链接两个可标识数据字

段的结构，将包括事件编码的事件标识信息安置在第一字段中，并且将至少部分所述加密内容数据安置在第二字段中，包括所述代理功能的所述设备被配置来在所述请求中至少包括所述事件编码。

17. 如权利要求 15 或 16 所述的方法，包括与所述加密内容一起提供确定许可条件的数据，其中所指示的位置是被安排来执行根据权利要求 9 或 10 的方法的服务器从其发布权限数据对象的位置。

18. 如权利要求 16 所述的方法，其中，至少某些所述许可条件通过所述事件编码被传输到所述服务器。

19. 一种系统，用于向属于多个事件中的一个的内容数据附加受限访问权限，以允许至少下述用户系统的组件使用所述内容数据，所述用户系统包括具有代理功能的设备（2－4、6），所述系统被配置来执行根据权利要求 15 的方法。

20. 一种计算机程序，其被安排来在被加载到可编程处理设备中时使得所述可编程处理设备执行根据权利要求 15 的方法。

提供权限数据对象的方法

技术领域

本发明涉及提供权限数据对象的方法。

背景技术

本发明涉及一种提供权限数据对象以发布到下述设备的方法，所述设备能访问与位置指示和事件信息一起提供的属于多个事件中的一个的加密内容，该位置指示指示从其可以请求到权限数据对象的位置，该事件信息与该事件唯一地关联，所述设备包括代理功能，用于向从所指示的位置发布权限数据对象的设备提供请求和代表该事件信息的数据，所述方法包括：接收请求和代表事件信息的数据；生成权限数据对象，该权限数据对象包括使得能够对属于唯一地关联到该事件信息的事件的内容数据进行解密的事件密钥信息。

本发明还涉及用于向下述设备提供权限数据对象的系统，所述设备能访问与位置指示和事件信息一起提供的属于多个事件中的一个的加密内容，该位置指示指示从其可以请求到所述权限数据对象的位置，该事件信息与所述事件唯一地关联，所述设备包括代理功能，用于向从所指示的位置发布权限数据对象的设备提供请求和代表事件信息的数据，其中，该系统包括：在安全环境中工作的处理器；和用于将请求和代表事件信息的数据传递到该处理器的接口，其中该处理器被配置来生成权限数据对象，该权限数据对象包括使得能够对属于唯一地关联到事件信息的事件的内容数据进行解密的事件密钥信息。

本发明还涉及计算机程序。

本发明还涉及向属于多个事件中的一个的内容数据附加受限访问权限的方法，以允许至少下述用户系统的组件使用该内容数据，所述用户系统包括具有代理功能的设备，该方法包括：以加密的形式提供

至少部分内容数据，以使得能够使用事件密钥信息来进行解密；与其一起提供事件信息，该事件信息唯一地关联到该内容数据属于的事件中的具体一个；以及与其一起提供位置指示，该位置指示指示从其可以请求到包括至少部分事件密钥信息的权限数据对象的位置；代理功能允许其中提供有该代理功能的设备向从所指示的位置发布权限数据对象的设备提供请求和代表事件信息的数据。

本发明还涉及用于向属于多个事件中的一个的内容数据附加受限访问权限的系统，以允许至少包括具有代理功能的设备的用户系统的组件使用该内容数据。

本发明还涉及其他计算机程序。

这些方法和系统的示例是已知的，例如从“OMA DRM Architecture, Draft Version 2.0”，Open Mobile Alliance Ltd.，2004年3月15日可知。该文件描述用于下述工作的机制：受信DRM（数字权限管理）代理的安全认证，安全打包和将使用权限和DRM内容传送到受信DRM代理。内容被打包到安全内容容器（DCF）中。DRM内容被用对称内容加密密钥（CEK）加密。DRM代理包括受信环境，在该受信环境中，可以安全地使用DRM内容。其角色是强制执行许可和约束，并且控制对DRM内容的访问。所有的DRM代理都具有唯一的私钥/公钥对和证书。权限对象是表达与内容相关联的许可和约束的文档。权限对象也包含CEK。在发送权限对象之前，敏感部分被加密，然后，该权限对象被加密地绑定到目标DRM代理。然后，可以使用任何传输机制（例如，HTTP/WSP、WAP Push、MMS）来发送权限对象和DCF。用于内容分发的一个模型是使用空中（Over-The-Air）下载机制。客户发起到内容门户（Content Portal）的浏览会话。然后，客户将DRM内容从内容门户下载到本地存储。客户在该DRM内容头部中查找权限发布者URL（统一资源定位符），然后发起到权限发布者门户的连接。该过程采用权限对象获取协议。在成功完成该协议的情况下，客户获得与DRM内容相关联的权限对象。

当权限发布者门户从该内容门户物理地移动时，问题就发生了。在这种情形中，需要提供一种机制，以允许生成权限数据对象的实体生成事件密钥信息。在存在许多事件的情况下，权限发布者门户需要用大量的事件密钥信息不断地更新。在替换中，许多事件可以共享相同的事件密钥信息，但是这种替换对于强力攻击来获取事件密钥信息来说是脆弱的。

发明内容

本发明的一个目的是提供在前面的段落中定义的类型的方法和系统，这些方法和系统允许发布权限数据对象的设备在针对许多不同的事件发布权限数据对象时相对独立于内容提供者工作，同时维持足够多的密钥。

利用根据本发明提供数字权限数据对象的方法实现了这个目的，其特征在于使用对至少部分事件信息进行运算的密码函数来生成事件密钥信息。

这样，因为事件密钥信息是至少部分事件信息的函数，并且事件信息对于具体的事件唯一，所以确保了足够多的事件密钥。因为代表事件信息的数据与请求权限数据对象的请求一起被提供，所以不需要引用内容提供者，这允许发布权限数据对象的设备极大地限制与内容提供者的系统的通信量。从而其可以独立地工作。

优选地，该方法包括从加密内容的提供者加载密钥信息，并且使用将至少部分所加载的密钥信息与至少部分事件信息组合的密码函数来生成事件密钥信息。

来自该提供者的密钥信息可以以较大的间隔被发送，并且可以用来生成事件组的事件信息。从而，到加密内容提供者的通信量仍旧相对被限制。本实施方式的优点在于加密内容的提供者保留对对事件的访问的全面控制。此外，该实施方式允许针对具体事件的事件密钥信息循环，而不必将新的唯一事件信息与其相关联。

一种实施方式包括将标识事件信息唯一地关联到的事件的数据存

储到日志中。

这样，该日志可以用于开帐单的目的。优点在于可以针对每次使用属于事件的内容数据来给关联到包括代理功能的设备（通常是诸如视频点播或广播事件的订户）的实体开帐单。

一种有利的变化包括接收来自关联到内容数据的提供者的系统的消息，并且返回至少一个消息，该消息包括代表存储在日志中的至少部分数据的信息。

这样，代表内容提供者收集许可费的实体可以查询发布权限数据对象的设备。这允许使开帐单和订户管理集中，而发布权限数据对象分散。

一种实施方式包括将下述数据加载并存储到存储器设备中，所述数据代表关联到包括有代理功能的设备的实体的信用等级，并且如果所生成的权限数据对象被提供给包括代理功能的设备，则修改所存储的数据来反映降低信用等级。

这使得能够使用每次支付定购模式来独立提供权限数据对象。发布权限数据对象的设备不需要回去参考订户管理系统来确定其是否应提供权限数据对象，而是将独立地检查信用等级，并且如果发现该等级足以生成所请求的权限数据对象，则扣除适当的数量。

在优选实施方式中，代理功能允许包括了该代理功能的设备从与加密内容数据一起提供的数据导出证书，该方法包括接收来自提供请求的设备的包括了反映事件费用的数据的证书，并且修改所存储的数据来反映降低了等于该事件费用的数量的信用等级。

这样，实现了每次支付模式，在该模式中，加密内容的提供者设置每个事件的费用。在不影响发布权限数据对象的设备的独立工作的情况下，可以实现价格差别，这是由于该费用并不直接从内容提供者被传输到那个设备。

一种优选实施方式包括接收包括了加密形式的数据的证书，并且对反映事件费用的数据进行解密，所述解密优选使用与已用其对该数据加密的密钥形成公钥/密钥对的密钥。

这排除了由用户进行的加密内容操作，例如，设置较低的价格。

一种优选实施方式包括从所接收到的代表事件信息的数据提取证书。

这样，事件信息能够标识事件，生成事件密钥信息，并且确定可以在其中提供权限数据对象的条件。从而充分使用单个通信。

在优选实施方式中，包括代理功能的设备被配置以在执行该代理功能时只根据包括在由该设备接收到的权限数据对象中的访问权限来提供对加密内容的访问，该方法包括生成还包括至少一个访问权限的权限数据对象。

这样，例如取决于订购的类别，可以授予不同类型的访问。

在一种优选实施方式中，包括代理功能的设备被配置以在执行该代理功能时从与加密内容一起提供的数据导出确定许可条件的数据，该方法包括接收来自提供请求的设备的确定许可条件的导出数据，并且根据所接收到的导出数据，选择包括在权限数据对象中的一个或多个访问权限。

这样，发布权限数据对象的设备可以以独立的方式提供访问权限的差别。没必要为了获得适于该事件的许可条件而针对每个所请求的权限数据对象回去参考内容提供者。

一种优选的实施方式包括从所接收到的代表事件信息的数据抽取确定许可条件的数据。

这样，事件信息被内容提供者用来将许可条件传输到发布权限数据对象的设备。这是一种相对高效的通信方式。

根据本发明的另一个方面，用于提供数字权限数据对象的系统特征在于处理器还被配置来使用对至少部分事件信息进行运算的密码函数来生成事件密钥信息。

根据本发明的另一个方面，本发明提供了一种计算机程序，其被安排来在被加载到可编程处理设备中时使得所述可编程处理设备执行根据本发明提供权限数据对象的方法。

根据本发明的另一个方面，向属于多个事件中的一个的内容数据

附加受限访问权限的方法，其特征在于，内容数据的加密部分以下述方式被提供，所述方式允许使用作为所提供的事件信息的至少一部分的密码函数的事件密钥信息进行解密，并且其中所指示的位置是安排来执行根据本发明提供权限数据对象的方法的服务器被配置来从其发布权限数据对象的位置。

这样，内容提供者可以将内容数据划分为大量的事件，每个都用其自己的密钥加密，而不必向生成权限数据对象的设备传输大量的事件密钥信息。

一种优选实施方式包括生成链接两个可标识数据字段的结构，将包括事件编码的事件标识信息安置在第一字段中，并且将至少部分所述加密内容数据安置在第二字段中，包括代理功能的设备被配置来在请求中至少包括该事件编码。

这样，使得包括有代理功能的设备能够检索回对于其试图提供访问的事件唯一的相关事件信息。

根据本发明另一个方面，本发明提供了一种系统，用于向属于多个事件中的一个的内容数据附加受限访问权限的系统，以允许至少包括具有代理功能的设备的用户系统的组件使用内容数据，该系统配置来执行根据本发明向内容数据附加受限访问权限的方法。

根据另一个方面，本发明提供了一种计算机程序，其被安排来在被加载到可编程处理设备中时使得该可编程处理设备执行根据本发明向内容数据附加受限访问权限的方法。

附图说明

现在参考附图更加详细地描述本发明，其中：

图 1 以示意形式示出了用于向多个用户系统提供安全内容包和权限数据对象的系统，其中权限数据对象提供对这些安全内容包的访问；

图 2 以示意形式示出了包括有加密内容数据的第一类安全内容包；

图 3 以示意形式示出了包括有加密内容数据的第二类安全内容

包;

图 4 示出了一个或多个用户系统中的蜂窝电话手机的示意性概况图。

具体实施方式

在图 1 中，加密内容经由蜂窝网络 1 被提供给用户系统。蜂窝网络例如可以是 CDMA、GSM、GPRS 或者 UMTS 网络。因此，第一用户系统由第一蜂窝电话 2 形成，并且第二用户系统由第二蜂窝电话 3 形成。第三用户系统由第三蜂窝电话 4、归属网络 5 和个人计算机 6 的组合形成。

作为经由蜂窝网络 1 向第三用户系统提供加密内容的替换，可以经由到个人计算机 6 的电缆或卫星网络（未示出）以广播、多播或单播模式提供加密内容，或者在数据载体上（例如，CD 或 DVD）提供加密内容。用户系统被定义为能够获得加密内容这一事实并不排除下述方案：在该方案中，加密内容被预加载到第一、第二和第三蜂窝电话 2－4 中的一个或多个，但是尚不能访问。

内容的示例包括振铃音、屏保或背景主题，以及在蜂窝电话 2－4 中玩的游戏。取决于蜂窝网络 1 的类型，内容可以包括压缩的音频或视频文件。MP3 文件是前一类的示例；MPEG－2、H.264/AVC 是定义后一类的示例的标准。

至少包括一段加密内容的安全内容包是从第一内容服务器 7 提供的，其中该内容服务器是经由将蜂窝网络 1 连接到（至少部分）因特网 9 的网关 8 可访问的。或者，诸如振铃音之类的内容可以直接经由蜂窝网络 1 从第二内容服务器 10 下载。

在下面将详细描述这样的实现：在该实现中，对于用户系统可用的安全内容包基本遵守开放移动联盟规范，尤其是属于该规范的数字权限管理（DRM）版本 2。也可以使用用于实现数字权限管理的其他标准。

“OMA DRM Content Format V2.0, Draft Version 2.0”，Open

Mobile Alliance Ltd.，2004 年 4 月 20 日定义了两种优选使用的文件结构。具体细节请参考该公开。

图 2 示出了离散媒体概况（Discrete Media Profile，DCF）文件 11 的格式。该文件包括文件头部 12，其标识文件 11 的类型和版本。文件头部 12 之后跟随着第一数据结构，称作第一 DRM 容器 13。在本示例中，该文件还包括第二 DRM 容器 14。第一 DRM 容器 13 包括公共头部框 15 和内容对象容器 16。内容对象容器 16 包括第一段加密内容数据。第二 DRM 容器 14 中的类似结构携带第二段加密内容数据，其前面有第二公共头部框（未示出）。从而，第一 DRM 容器 13 将公共头部框 15 链接至内容对象容器 16。

公共头部框 15 至少包括包含有全局唯一标识符的字段。其值对于包括在内容对象容器 16 中的内容数据的加密段是唯一的。在这里称作 event_ID。

公共头部框 15 还包括统一资源定位符（URL），统一资源定位符指示从其请求权限数据对象的位置，权限数据对象包括内容密钥信息，用于对第一 DRM 容器 13 中的内容数据的加密段的至少一部分进行解密。从而，作为由多个用户系统之一使用的提供包括有加密内容数据的安全内容数据包的方法的一部分，资源指示符数据与加密内容数据一起被提供。所提供的资源数据指示这样的位置：充当权限发布者的设备从该位置发布权限数据对象。因此，第一和第二内容服务器 7、10 配置来与提供加密内容数据一起向一个用户系统提供资源指示符数据。

图 3 示出了连续分组化概况（PDCF）文件 17 的格式，其目标是音频和视频之类的媒体内容。这是一种这样的文件结构，其是要帮助安全内容包流动到蜂窝电话 2－4 之一。PDCF 文件 17 开始于文件头部 18，该文件头部标识 PDCF 文件 17 的类型和版本。PDCF 文件 17 还包括影片框 19，影片框包括第一轨迹框 20 和至少一个额外轨迹框 21。第一轨迹框 20 包括保护方案框 22。在本示例中，一段第一轨迹内容数是加密的，并且作为分组被包括在媒体数据框 23 中。属于至少

一个额外轨迹内容数据的一段的分组未加密地（in the clear）被包括在相同的媒体数据框 23 中。每个分组中的头部标识出该分组所属的轨迹，并且将该分组链接到第一轨迹框 20 和额外轨迹框 21。在影片框 19 中包括至少一个公共头部框（未示出）。或者存在一个可适用于所有轨迹，或者在第一轨迹框 20 中存在一个只可适用于第一轨迹内容的加密段。从而，PDCF 文件 17 构建为具有包含 event_ID 的头部，该 event_ID 对于内容数据的加密段是唯一的。

可以以某些其他方式（例如，作为一段 MPEG－2 分组化基本流）对该段加密内容进行打包，并且利用基本流标识符、或者承载分组化基本流的 MPEG－2 传输流的包标识符，将其链接到类似于公共头部框 15 的结构。在每种情形中，一起提供内容数据的加密段和对于该内容数据的加密段唯一的 event_ID。

图 4 是示出了第三蜂窝电话 4 的相关组件的示意图。蜂窝电话形成包括手机和便携式安全数据处理器件的终端，该安全数据处理器件采用用户识别模块（SIM）卡 24 的形式。SIM 卡包括嵌入在 SIM 卡 24 中集成电路（IC）25，该集成电路优选采用数据篡改验证（tamper-proof）方式封装。以此方式封装 IC 25 的机制在本领域中是公知的。IC 25 包括处理器 26、电可擦可编程只读存储器（EEROM）27、主存储器 28 和到手机的接口部分 29，该接口还包括与手机中的触点协作的接触盘。使 SIM 卡 24 安全的其他安全特性包括加密技术和/或密码混淆技术，这些本质上也是公知的。从而，IC 25 提供了一种受保护的环境，用于运行对于 DRM 方案整体的安全至关重要的应用。

手机包括手机控制器 30，其被链接到到 SIM 卡 24 的接口 31，该接口被设置来与 SIM 卡到手机的接口 29 相互作用。对于语音电话，手机包括音频输入级 32 和音频输出级 33，前者将用户的话音数字化，后者向扬声器提供输出。调制器 34、解调器 35 和第一天线 36 形成到蜂窝网络 1 的接口。无线通信控制器 37 和第二天线 38 形成到归属网络 5 的接口。手机还包括手机只读存储器（RAM）39、手机 EEPROM

40、以及键盘 41 和显示驱动器 42。

存储在手机 EEPROM 40 中的软件代码向其提供代理功能，这使得其能够使用权限数据对象中的信息访问加密内容数据。手机还具有唯一的私钥/公钥对和证书，这使得能够对该手机进行认证。

在一种实施方式中，手机包含来自第一内容服务器 7 的内容数据包，例如 MMS 消息。在另一种实施方式中，手机包括用于浏览因特网 9 的浏览器，并且获得来自第二内容服务器 10 的安全内容包。在另一种实施方式中，该安全内容包在工厂就被安装到 SIM 卡 24 的 EEPROM 27 中或者手机 EEPROM 40 中。安全内容包也可以通过到归属网络 5 的接口获得。

在充当代理时，一旦被触发来访问加密内容数据，手机就检索回与该加密内容数据一起接收到的 event_ID 和 URL。其构造到安装有权限发布者模块的设备的请求消息。该 URL 被解析来获得要将该请求发送到的地址。请求自身也可以是 URL 的形式，这在本领域中是公知的。请求至少包括链接到期望访问的该段加密内容数据的 event_ID。

响应于并遵守用于完成授予访问的标准，手机从安装有权限发布者模块的设备接收到权限数据对象。该权限数据对象包括密钥，用于对唯一地关联到 event_ID 的加密内容数据部分进行解密。

权限数据对象优选还包括代表访问权限的数据，该数据的形式为一组许可和约束。许可定义所准许的访问的类型，例如复制、与其他设备通信、提交等。约束限定许可，例如，通过定义可以提供的访问所定义的类型的次数。每个具有代理功能的设备被认为是受信实体。向手机提供代理功能的程序代码配置该手机，以只根据在权限数据对象中定义的访问权限来提供对加密内容的访问。这根据通用条件访问方案阐明了这里介绍的 DRM 方案，使其尤其适用于到包括有归属网络 5 的用户系统的广播内容，下面将对此进行解释。为了确保访问权限的执行，向手机提供代理功能的程序代码优选也是数据篡改防止的，这是结合 SIM 卡 24 中的 IC 25，使用上述一种或多种技术实现的。代

理功能中的某些或全部可以在 SIM 卡 24 中。

权限发布者模块被这样配置，以使得所发布的权限数据对象至少加密地绑定到具有代理功能的手机。优选地，至少权限数据对象中的密钥信息被用公钥加密，其中该公钥与手机的私钥形成一密钥对。注意，权限数据对象可以加密地绑定到这样的多个具有代理功能的设备，这多个设备形成一个用户系统内的限定域，以使得可以将权限数据对象传送到个人计算机 6，并且由该计算机用来提供对加密数据的访问，所提供的个人计算机也包括代理功能，并且具有正确的证书和/或加密密钥。某些或全部代理功能可以在与计算机协作的智能卡中。

在第一实施方式中，在 SIM 卡被安装到第三蜂窝电话 4 之前，权限发布者模块已被传送到 SIM 卡 24 的 EEPROM 27。在工作时，权限发布者模块（优选是可由处理器 26 执行的计算机程序模块）使得 SIM 卡 24 能够生成权限数据对象，该权限数据对象加密地绑定到该手机，或者加密地绑定到作为归属网络 5 中的节点的具有代理功能的任何其他设备。

在第二实施方式中，在 SIM 卡安装到第三蜂窝电话 4 之后，权限发布者模块被传送到该 SIM 卡 24。例如，第一 DRM 服务器 43 被安排来传送权限发布者模块，该权限发布者模块用于发布与从第一内容源 7 提供的加密内容相关的权限数据对象。第二 DRM 服务器 44 被安排来传送下述权限发布者模块：该权限发布者模块用于发布与从第二内容源 10 提供的加密内容相关的权限数据对象。

在包括第三蜂窝电话 4 的用户系统中，第三实施方式是可以想象到的，其中，权限发布者模块被预装或者传送到智能卡（未示出）中，以通过将智能卡插入到附接到个人计算机 6 的智能卡读卡器（未示出）中，从而安装到用户系统中。另一种替换是将权限发布者模块下载到固定安装在手机或者个人计算机 6 中的受信平台模块。

优选地，其他各个权限发布者模块被传送到第一和第二蜂窝电话 2、3 中的 SIM 卡。他们每个都使各自的 SIM 卡能够生成加密地绑定到该 SIM 卡安装在其中的手机的权限数据对象。这样的效果是不需要

使用蜂窝网络 1 来获得权限数据对象。当加密内容数据是广播的时，这种效果最显著，这是因为由于避免了无数的蜂窝电话试图同时获得权限数据对象，所以就带宽利用来说广播相对更高效。

如上所述，权限发布者模块配置来发布至少包括一个访问权限的权限数据对象。优选地，提供权限发布者模块的实体接收一组适于该用户系统或者每个用户系统的访问条件。其以这样的方式配置传送到了第三蜂窝电话 4 中的 SIM 卡 24 的权限发布者模块：包括在向手机、个人计算机 6 和附接到归属网络 5 的具有代理功能的任何其他设备发布的所有权限数据对象中的访问权限的组合符合该组适于由这些设备形成的一个用户系统的条件。从而，例如加密的内容可以具有这样的访问条件：每个用户系统只可以复制 5 次。然后，SIM 卡 24 中的权限发布者模块被配置来发布 5 个权限数据对象，每个定义复制一次的权限。

在第一变化中，这组适于用户系统的访问条件被编码到传送到了 SIM 卡 24 中的权限发布者模块中。在另一种实施方式中，依靠通过蜂窝网络 1 到先前安装有权限发布者模块的 SIM 卡 24 的分离的通信来配置权限发布者模块，从而有效地重配置那个权限发布者模块。

注意，生成 DCF 文件 11 或 PDCF 文件 17 的实体在其中提供 URL，该 URL 指向接收安全内容数据包的用户系统中的位置。另外，从第一和/或第二内容服务器 7、10 提供的信号包括数据资源指示符数据，其指向内容数据被提供给的一个用户系统内的位置。该 URL 可以采用通用形式，即，代表到用户系统内的位置的数据路径，而没必要是仅仅在一个具体的用户系统的上下文才有意义。就是说，可以采用这样的指令形式：指示接收手机从任何安装有 SIM 卡 24，而不必是具有具体的序列号的手机请求权限数据对象。

现在将集中描述代理功能和权限发布者模块的优选功能的细节，并且深入描述具体类型的安全内容包。

尤其是在要提供的内容数据包括要按需提供的广播程序或视频时，最好将要传送的整组内容数据划分为多个段，在本说明中这些段

也将被称作事件。通过分离地对每段加密，以使每段可以只用其自己的内容密钥而被解密，从而实现了密钥循环方案（key cycling scheme）。通过将整组内容数据划分为较小的分离事件，从而获得更高程度的保护。

因为权限发布者模块安排来针对事件发布至少包括内容解密密钥（或者事件密钥）部分的权限数据对象，所以其必须能访问密钥信息。为了避免必须从第一和第二内容服务器 7、10 向 SIM 卡 24 传送大量的密钥信息，事件的密钥是唯一与该事件关联的事件信息的函数，并且由第一和第二内容服务器 7、10 提供。

在第一变化中，event_ID 用来携带唯一与事件关联的事件信息，并且用作到权限发布者模块执行来再生成事件密钥的加密函数的输入。

在第二变化中，代理功能使得手机能够从属于事件的内容数据导出证书。优选地，该证书是加密的形式。SIM 卡 24 接收该证书，对其进行解密，从而获得对于该事件唯一的事件信息。至少部分被用来生成密钥信息，该密钥信息在可能进一步处理之后使得手机能够对该事件进行解密。在本实施方式中，用 SIM 卡 24 的公钥加密该证书是优选的。这样，内容提供者可以将访问权限捆绑到具体的 SIM 卡 24，从而捆绑到具体的用户，而不是具体的手机。

证书也可以包括在 event_ID 中，就此而言，必须对至少部分 event_ID 执行解密运算来获得事件信息，该事件信息可用作最终提供事件密钥信息的加密操作的输入。

为了提供安全性来抵御对用于生成事件密钥信息的加密函数进行的任何分析，使用这样的加密函数来生成事件密钥信息：该加密函数将由具有至少部分密钥信息的权限发布者模块加载的至少部分密钥信息组合。优选地，这种组密钥信息从第一和第二内容服务器 7、10 或者第一和第二 DRM 服务器 43、44 之一被上传到 SIM 卡 24。另外，SIM 卡 24 可以预加载有这些组密钥。一个或多个组密钥可以是传送到 SIM 卡 24 权限发布者模块的一部分。注意，这些组密钥几乎不需

要更新，这是由于这样的事实：这些组密钥和对于事件唯一的事件信息都被用作提供该事件的事件密钥信息的加密函数的输入。

组密钥优选适用于多个事件，例如，所有的事件，即，诸如影片之类的大内容数据单元已被划分为多段内容数据。在用户系统的所有成员被数次划分而成为多组的情形中，组密钥也可以（或者替代地）适用于一组一个或多个用户系统。一旦确定发布权限数据对象的设备中的具体一个损坏了，就不再使用适于包括那个设备的组的组密钥。这样，就可以撤消损坏了的 SIM 卡 24。

在一种实施方式中，可以实现组密钥层次，其中高层的每个组密钥关联到多组事件和/或用户系统中的一组，并且每个低层的组密钥管理到这些组中的一组的多个子组。在这种情形中，不同层次的组密钥优选按照不同的频率改变。

这里所述的方案允许实现数种支付模型。

在一种实施方式中，权限发布者模块配置 SIM 卡 24，以在 EEPROM 27 中的日志中存储这样的数据，该数据标识出由手机提供给其的事件信息唯一地关联到的事件。优选但不是必须地，该数据与下述数据一起存储：代表与包括代理功能的设备相关联的实体的数据，例如，其拥有者。存储事件标识符数据允许根据对由提供者提供的内容数据的使用数量来向内容数据提供者公平地分发所收集的许可费。

SIM 卡 24 接收来自与内容数据的提供者相关联的系统的消息，并且返回至少一个消息，该消息代表存储在日志中的至少部分数据。当然，这优选是响应于来自第一和第二内容服务器 7、10 或第一和第二 DRM 服务器 43、44 之一的查询，通过手机作为中介来实现的。

当在 SIM 卡 24 中工作时，权限发布者模块将代表实体的信用等级的数据加载并存储到 EEPROM 27 中。该实体本质上优选是 SIM 卡 24 的用户，即，包括蜂窝电话 2－4 之一的用户系统的用户。每次权限数据对象被提供给具有代理功能的设备时，存储的数据被修改来反映降低的信用等级。

在第一变化中，每发布一个权限数据对象，信用等级就被降低某

一标准量。这样，请求发布权限数据对象的每个请求代表存储在 SIM 卡 24 中的存储位置（purse）的单个信用单元。

在第二变化中，代理功能允许在其上提供代理功能的设备从与形成事件的加密内容数据一起提供的数据导出证书。SIM 卡 24 中的权限发布者模块接收来自下述设备的证书，该设备提供了对权限数据对象的请求。该证书包括反映事件费用的数据。将受限访问权限或许可条件关联到事件的实体或内容提供者根据其希望对访问事件收费的数量来生成证书。可以以与提供事件信息的证书类似的方式来包括该证书，其中事件信息用来生成对事件进行解密的密钥。实际上，其可以是相同的证书。代表唯一的事件信息的数据（更具体地说是 event_ID 自身）可以允许提取这样的证书。从而，event_ID 的具体值或者值的集合提供了事件费用的指示。

已经提到数字权限管理方案的优点在于权限发布者模块能够根据下述许可条件生成至少包括一个访问权限的权限数据对象：所述许可条件可以从具有加密内容的数据导出，并且被手机转发到 SIM 卡 24。SIM 卡 24 接收来自具有提供请求权限数据对象的请求的代理功能的设备的导出数据，其中该导出数据确定许可条件。其根据接收到的导出数据，选择要包括到权限数据对象中的访问权限。

有利地是，许可条件也包括在证书中，例如反映事件费用的证书。许可条件自身也可以包括反映事件费用的数据。在那种情形中，SIM 卡 24 存储将每类许可条件链接到某一事件费用的数据。这样，允许 5 次复制的许可条件导致 5 次扣减，每次扣减与存储的复制费用相等的量。证书可以携带可用许可类型的定义，每种类型与不同的费用相关联。SIM 卡 24 一旦接收到证书并可选地对其进行了解密，就利用手机控制器 30、键盘 41 和显示驱动器 42 与用户交互，以选择可用许可类型之一，并且授权适当地确定存储在 EEPROM 27 中的信用等级。

如上对事件费用的描述，确定许可条件的数据可以被包括在 event_ID 中。具体组件、event_ID 的值和值的范围确定许可条件和/或支付模型。例如，“重放一次”可能在值的第一范围中，而“不限

次重放”可能在值的第二范围中。这样，内容提供者利用 event_ID 把至少某些许可条件传输给了服务器，即 SIM 卡 24。

上面已提到，在要提供的内容数据包括要按需提供的广播程序或视频的情况中，尤其希望密钥循环方案。为了避免使对用不同密钥加密、从而利用不同的 event_ID 标识出的内容数据部分的连续解密中断，优选在所考虑的事件之前，使解密密钥信息对具有代理功能的设备可用。这样，通过蜂窝网络 1 提供的至少内容数据的某些加密部分具有两个 event_ID: 一个标识事件自身，另一个标识随后提供的事件。

第二 event_ID 可以在 DCF 文件 11 或 PDCF 文件 17 中的携带有第一 event_ID 的公共头部框的文本头部字段中。因此，第一和第二 event_ID 几乎同时被提供。这是因为当流动内容到蜂窝电话 2－4 之一时，第一和第二内容服务器 7、10 会基于这样一个文件来创建串行数据流。在这种数据流中，第一 event_ID 之后紧随着第二 event_ID，其前没有在任何事件。在 DCF 文件 11 中，第一 DRM 容器 13 将公共头部框 15 链接到承载有第一事件的内容对象容器 16。如果在第二 DRM 容器 14 中承载第二 event_ID 被关联到的事件，则第二 event_ID 第二次被提供到第二 DRM 容器 14 的公共头部框 15 中。

类似地，在 PDCF 文件 17 形成使内容数据流动到蜂窝电话 2－4 的基础时的情形中，媒体数据框 23 中的访问单元或分组将被提供有将其链接到下述数据结构的包装器（即，由包括头部和/或尾部的数据封装的），以使得他们类似地基本同时被提供，其中所述数据结构具有用于第一 event_ID 的字段和用于第二 event_ID 的字段。当提供了属于第二 event_ID 被唯一地关联到的事件的加密数据时，在第二时间提供第二 event_ID。

加载到手机中的软件向手机提供了执行适合的解密方法的能力。手机与接收第一 event_ID 和第二 event_ID 二者一起从第一或第二内容提供者 7、10 接收第一事件。在接收到内容数据的第二部分之前，其提供请求，以请求具有第二 event_ID 的权限数据对象。从而，它就可以提前获得紧随第一事件之后的至少一个事件的事件密钥信息。为

了最小化通过接口 29、31 的通信，在到具有权限发布者模块的 SIM 卡 24 的单个请求中提供第一 event_ID 和第二 event_ID。

手机控制器 30 接收到来自 SIM 卡 24 的一个或多个权限数据对象中的两个解密密钥。这些密钥中的第一个用来对第一事件进行解密，并可选地对在接收第一事件后的有限数目个事件进行解密。第二解密密钥存储在主存储器 28 或 EEPROM 27 中，用于随后使用。

如上所述，第二次接收到第二 event_ID。响应于第二次接收到第二 event_ID，手机检索回存储的第二内容解密密钥，并且用那个密钥对至少第二事件进行解密。

这样，event_ID 用来触发密钥循环方案中的密钥改变。一般来说，触发密钥改变的 event_ID 没必要是唯一地关联到第二事件的 event_ID。手机可以配置来对不同的 event_ID 或者不同类型的 event_ID 作出反应。例如，event_ID 中的一个数字或者位可以以在传统的条件访问方案中公知的方式发出从奇数密钥到偶数密钥的改变的信号。从而，可以在第二事件之前提供第三事件。唯一地关联到该第三事件的 event_ID 触发手机，使其改变密钥，但是该改变对第三事件之后的预定数目个事件生效。

本发明不受限于上述实施方式，而是可以在权利要求的范围内变化。例如，归属网络 5 可以是根据蓝牙、IEEE 802.11 或 UWB 标准之一的无线网络，该网络可以使用光链路，例如根据 IrDA 标准的链路，或者其可以包括有线 USB 或以太网连接。数字权限发布者模块可以置于智能卡中，或者作为 SIM 卡 24 的替换的安全硬件中。

另外，不是将数字权限发布者模块传送到每个用户系统中的设备（即，蜂窝电话 2－4 中的一个），而是将其安装到第一或第二 DRM 服务器 43、44。从而，第一或第二 DRM 服务器将被配置来使用这里所概述的方法向蜂窝电话 2－4 中的一个或数个发布数字权限发布者模块。在更高级的实现中，数字权限发布者模块优选被传送到位于服务网里 1 的边缘的多个代理 DRM 服务器（未示出），但是这并不是必须的。优选地，每个都将配置来向多个用户系统中选择出的子集发

布权限数据对象。这样的效果在于用户系统能够比可能只使用单个中央 DRM 服务器更快地获得权限数据对象。在这种实施方式中，每个代理 DRM 服务器将加载来自该中央 DRM 服务器的组密钥。

这样，上面的描述已公开了用于数字权限管理的各种技术，可以以任何方式对这些技术进行自由组合，以实现优选的方案。下面将扼要概括所公开的技术。

本发明已公开了一种方法，用于提供对到多个用户系统中的一个的加密内容的访问。每个用户系统能够获得安全内容包，其包括加密内容和对从其请求权限数据对象的位置的指示，并且每个用户系统还包括至少一个设备，该设备能访问这样获得的安全内容包，并且具有代理功能，使得其能够从所指示的位置从发布权限数据对象的设备检索回权限数据对象，并且用于提供对至少部分加密内容的访问。权限数据对象至少包括使得能够对至少部分加密内容进行解密的内容密钥信息，并且至少被加密地绑定到该权限数据对象被发布到的设备，以使得只有该权限数据对象已被绑定到的具有代理功能的设备才能够获得该内容密钥信息。权限发布者模块被传送到设备的受保护环境，以安装到一个用户系统中，当在该用户系统中工作时，使得该设备能够生成至少一个权限数据对象，其中该权限数据对象加密地绑定到具有代理功能的用户系统中的设备中发出请求的一个设备。

在一种实施方式中，一个用户系统包括到外部通信网络的接口，并且其中该用户系统被安排来通过接口将接收到的数据传送到具有受保护环境的设备，其中权限发布者模块经由该通信网络而被传送。

可选地，权限发布者模块被传送到具有到用户系统中的设备的接口的便携式安全数据处理设备。

可选地，权限发布者模块被传送到具有到蜂窝电话手机的接口的便携式安全设备，优选是用户识别模块卡。

该方法包括将其他各个权限发布者模块传送到其他设备的受保护环境，以安装到其他各个用户系统中，当在其他用户系统中的一个中工作时，每个权限发布者模块使得该权限发布者模块被传送到的设备

能够生成至少一个权限数据对象，其中该权限数据对象加密地绑定到具有代理功能的用户系统中的设备中发出请求的一个设备。

每个具有代理功能的设备配置来在执行代理功能时只根据包括在权限数据对象中的访问权限来提供对加密内容的访问。该方法包括传送权限发布者模块，使得具有受保护环境的设备在用户系统中工作时，能够生成至少一个权限数据对象，该权限数据对象加密地绑定到具有代理功能的用户系统中的设备中发出请求的一个设备，并且包括至少一个访问权限。

该方法包括：接收适于一个用户系统的一组访问条件；以下述方式配置权限发布者模块，所述方式为包括在一组一个或多个权限数据对象中的访问权限的组合符合可适用于这一个用户系统的一组访问条件，这一组一个或多个权限数据对象是向具有代理功能的一个用户系统中的发出请求的设备发布的。

本发明还公开了一种用于安装到多个用户系统中的一个中的数据处理设备，其中，每个用户系统能够获得安全内容包，其包括加密内容和对从其请求权限数据对象的位置的指示，并且每个用户系统还包括至少一个设备，该设备能访问这样获得的安全内容包，并且具有代理功能，使得其能够从所指示的位置从发布权限数据对象的设备检索回权限数据对象，并且用于提供对至少部分加密内容的访问，该权限数据对象至少包括使得能够对至少部分加密内容进行解密的内容密钥信息，并且至少被加密地绑定到该权限数据对象被发布到的设备，以使得只有该权限数据对象已被绑定到的具有代理功能的设备才能够获得该内容密钥信息，数据处理设备包括受保护环境，其特征在于：该数据处理设备还包括权限发布者模块，其配置来在受保护环境中运行，使得该数据处理设备被安装在用户系统中并在其中工作时，能够生成至少一个权限数据对象，其中该权限数据对象加密地绑定到具有代理功能的用户系统中的设备中发出请求的一个设备。

数据处理设备是通过执行前述提供对到多个用户系统中的一个的加密内容的访问的方法可获得的。

本发明还公开了一种计算机程序，其被安排以在被加载到包括受保护环境的数据处理设备中时使得该数据处理设备能够充当前述数据处理设备。

在提供用于由多个用户系统中的一个使用的包括加密内容数据的安全内容数据包的方法中，每个用户系统包括至少一个接口，用于获得来自外部源的安全内容数据包，并且还包括至少一个设备，该设备能访问这样获得的安全内容包，并且具有代理功能，使得其能够从所指示的位置从发布权限数据对象的设备检索回权限数据对象，并且用于提供对至少部分加密内容的访问，该权限数据对象至少包括使得能够对至少部分加密内容进行解密的内容密钥信息，并且至少被加密地绑定到该权限数据对象被发布到的设备，以使得只有该权限数据对象已被绑定到的具有代理功能的设备才能够获得该内容密钥信息，其中资源标识符数据与加密内容数据一起被提供，该资源标识数据指示充当权限发布者的设备从其发布权限数据对象的位置。该方法的特征在于：提供指向一个用户系统中的位置的资源指示符数据。

本发明公开了一种服务器，用于提供用于由多个用户系统中的一个使用的包括安全内容数据的安全内容数据包的服务器，其中该服务器包括到通信网络的网络接口。每个用户系统包括至少一个接口，用于经由通信网络获得安全内容数据，并且还包括至少一个设备，该设备能访问这样获得的安全内容包，并且具有代理功能，使得其能够从所指示的位置从发布权限数据对象的设备检索回权限数据对象，用于提供对至少部分加密内容的访问，该权限数据对象至少包括使得能够对至少部分加密内容进行解密的内容密钥信息，并且至少被加密地绑定到该权限数据对象被发布到的设备，以使得只有该权限数据对象已被绑定到的具有代理功能的设备才能够获得该内容密钥信息。该服务器配置来与提供加密内容一起向一个用户系统提供资源标识符数据，该资源标识数据指示充当权限发布者的设备从其发布权限数据对象的位置。该服务器配置来与提供加密内容数据一起提供指向一个用户系统中的位置的资源指示符数据。

本发明公开了一种信号，其承载用于由用户系统使用的包括加密内容数据的安全内容数据包，该用户系统包括至少一个接口，用于获得来自外部源的安全内容数据包，并且还包括至少一个设备，该设备能访问这样获得的安全内容包，并且具有代理功能，使得其能够从所指示的位置从发布权限数据对象的设备检索回权限数据对象，用于提供对至少部分加密内容的访问，该权限数据对象至少包括使得能够对至少部分加密内容进行解密的内容密钥信息，并且至少被加密地绑定到该权限数据对象被发布到的设备，以使得只有该权限数据对象已被绑定到的具有代理功能的设备才能够获得该内容密钥信息，其中安全内容数据包包括资源标识符数据，该资源标识数据指示充当权限发布者的设备从其发布权限数据对象的位置，其特征在于，安全内容数据包还包括资源指示数据，其代表到用户系统中的位置的数据路径。

本发明还公开了一种计算机程序，其被安排以在被加载到数据处理设备中时使得该数据处理设备能够执行如上所述提供安全内容数据包的方法。

另外，本发明已公开了一种向内容数据附加受限访问权限的方法，以允许至少下述用户系统的组件使用该内容数据，其中所述用户系统包括具有代理功能的设备，该方法包括：以加密的形式提供第一段内容数据，这允许使用第一段解密密钥来解密；以加密的形式提供第二段内容数据，这允许使用第二段解密密钥来解密，其中第二段内容数据是在第一段内容数据之后提供的，其中第一段内容数据与第一事件标识数据一起被提供，该标识数据唯一标识一段内容数据，并且至少第一段内容数据与位置指示一起被提供，该位置指示指示从其可以请求到权限数据对象的位置，代理功能允许其中提供有该代理功能的设备向下述设备提供包括这样数据的请求，其中该数据代表与内容数据部分一起提供的事件信息，所述设备从所指示出的位置发布权限数据对象，该数据对象包括至少部分内容解密密钥，用于对由代表请求中的事件信息的数据所标识出的内容数据部分进行解密。

该方法可选包括提供第二事件标识数据，该数据唯一标识与第一

段内容数据一起的第二段内容数据。

在该方法中，基本同时提供第一和第二事件标识。

可选地，对应于第二事件标识数据的数据在第二时间与第二段内容数据一起可选地被提供。

可选地，在链接两个可标识数据字段的数据结构中提供内容数据的每段，其中第一和第二事件标识数据安置在第一字段中，并且至少部分第一段内容数据被安置在第二字段中。

该方法可选包括对至少第二段内容数据进行加密，使得允许使用这样的密钥进行解密，该密钥是至少部分第二事件标识数据的加密函数。

一种计算机程序，被安排来在该程序被加载到可编程处理设备中时使得该可编程处理设备能够执行上述向内容数据附加受限访问权限的方法。

一种承载具有多个段的串行数据的信号，其中第一段包括第一段内容数据，该串行数据的第一段后的第二段包括第二段内容数据，其中第一段内容数据是允许使用第一内容解密密钥进行解密的加密形式的，第二段内容数据是允许使用第二内容解密密钥进行解密的加密形式的。串行数据流的第一段还包括第一事件标识数据，该数据唯一标识一段内容数据和位置指示，该位置指示指示具有代理功能的设备可以从其请求到权限数据对象的位置，这允许该设备向下述设备提供包括这样数据的请求，其中该数据代表与内容数据部分一起提供的事件信息，所述设备从所指示出的位置发布权限数据对象，该权限数据对象包括至少部分内容解密密钥，用于对由代表请求中的事件信息的数据所标识出的该段内容数据进行解密。串行数据的第一段还包括第二事件标识数据，该数据唯一标识第二段内容数据，并且由来自串行数据的第二段的其他数据分离开。

在信号中，每段可选包括至少一个头部和一个体，其中每段内容数据被包括在体中，并且与该段内容数据一起提供的事件标识数据通过该头部链接到该部分内容数据。

可选地，串行数据的第二段还包括代表第二标识数据的事件。

向至少一个用户系统提供内容数据的服务器被配置来实现上述向内容数据附加受限访问权限的方法，并且/或者提供上面定义的信号。

访问与受限访问权限相关联的内容数据的方法，包括：与第一事件标识数据和位置指示一起接收第一段内容数据，其中第一段内容数据是允许使用第一内容解密密钥来进行解密的加密形式的，第一事件标识数据唯一标识第一段内容数据，位置指示指示从其可以请求到权限数据对象的位置；向下述设备提供包括这样数据的请求，其中该数据代表与第一段内容数据一起提供的事件信息，所述设备从所指示出的位置发布权限数据对象，该权限数据对象包括至少部分内容解密密钥，用于对由代表请求中的事件信息的数据所标识出的该段内容数据进行解密；以及接收第二段内容数据，其中第二段内容数据是允许使用第二内容解密密钥来进行解密的加密形式的，并且是在第一段内容数据之后提供的；以及与第一段内容数据一起接收唯一标识第二段内容数据的第二事件标识数据；在接收第二段内容数据之前向发布权限数据对象的设备提供请求，其中该请求包括代表第二事件标识的数据。

在本发明中，代表第一和第二事件标识的数据可选地在单个请求中被提供给发布权限数据对象的设备。

该方法可选地包括在至少一个权限数据对象中接收第一和第二内容解密密钥，其中第一内容解密密钥用来对至少第一段内容数据进行解密，而第二内容解密密钥存储来随后使用。

该方法可选地包括与接收唯一标识一段内容数据的事件标识数据一起接收该段内容数据，响应于接收该事件标识数据而检索回所存储的第二内容解密密钥，并且随后使用第二内容解密密钥来对至少第二段内容数据进行解密。

一种用于访问与受限访问权限相关联的内容数据的系统，包括：用于与接收第一事件标识数据和位置指示一起接收第一段内容数据，并且接收第二段内容数据的接口，其中第一段内容数据是允许使用第一内容解密密钥来进行解密的加密形式的，第一事件标识数据唯一标

识第一段内容数据，位置指示指示从其可以请求到权限数据对象的位置，其中第二段内容数据是允许使用第二内容解密密钥来进行解密的加密形式的，并且是在第一段内容数据之后提供的；处理器，其被安排来生成这样的请求，该请求包括代表与第一段内容数据一起提供的第一事件信息的数据；和用于向下述设备提供请求的接口，该设备从所指示出的位置发布权限数据对象，这些权限数据对象包括至少部分内容解密密钥，用于对由代表该请求中的事件信息的数据标识出的该部分内容数据进行解密。一旦与第一段内容数据一起接收到唯一标识第二段内容数据的第二事件标识数据，该系统就被配置来在接收第二段内容数据之前向发布权限数据对象的设备提供这样的请求，其中该请求包括代表第二事件标识的数据。

该系统可选地被配置来执行上面定义的访问与受限访问权限相关联的内容数据的方法。

一种计算机程序，被安排来在该程序被加载到可编程处理设备中时使得该可编程处理设备能够执行访问关联到受限访问权限的内容数据的方法。

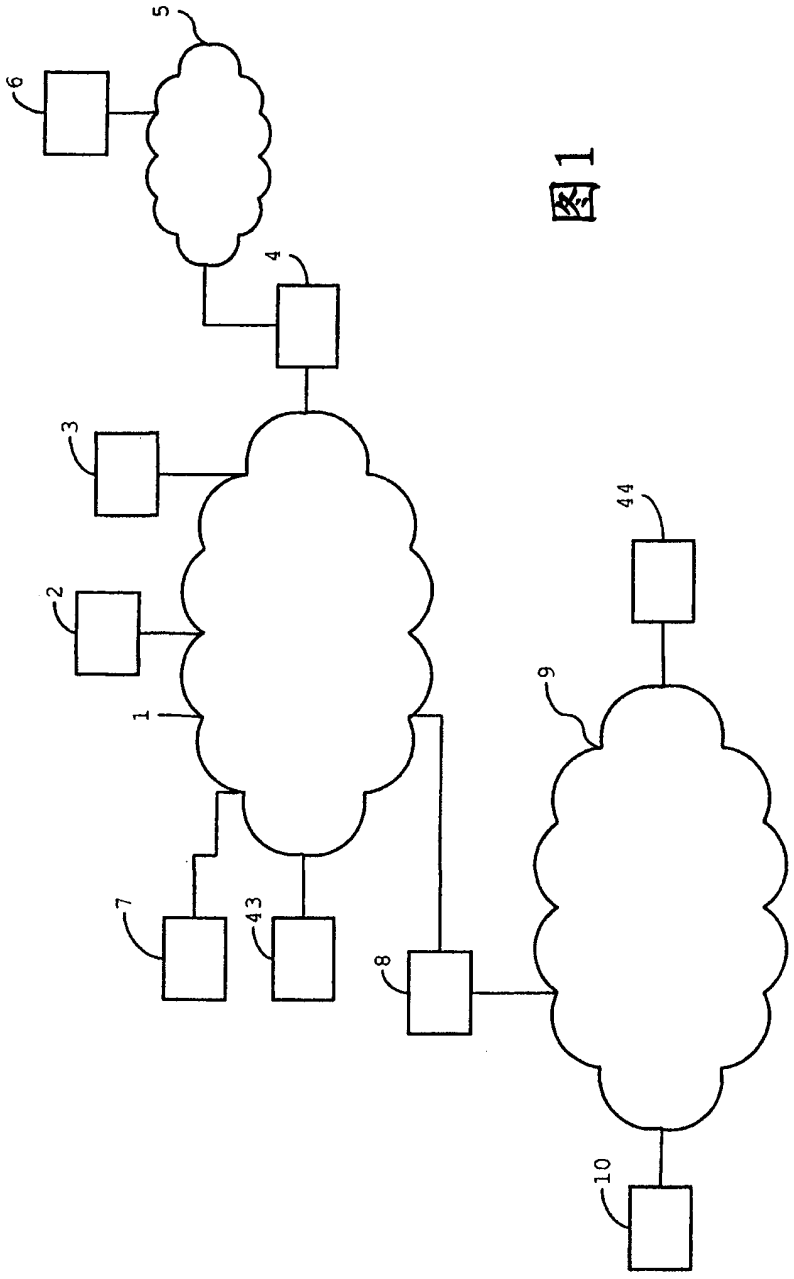


图1

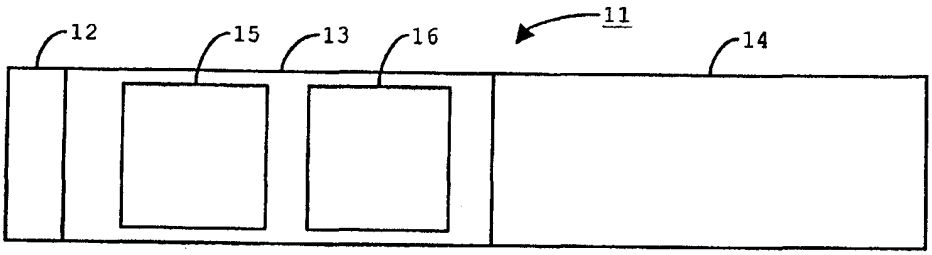

12
15
13
16
11
14

图2

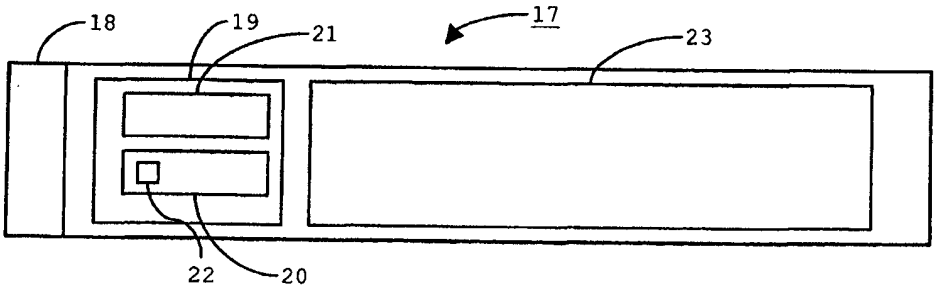

18
19
21
17
23
22
20

图3

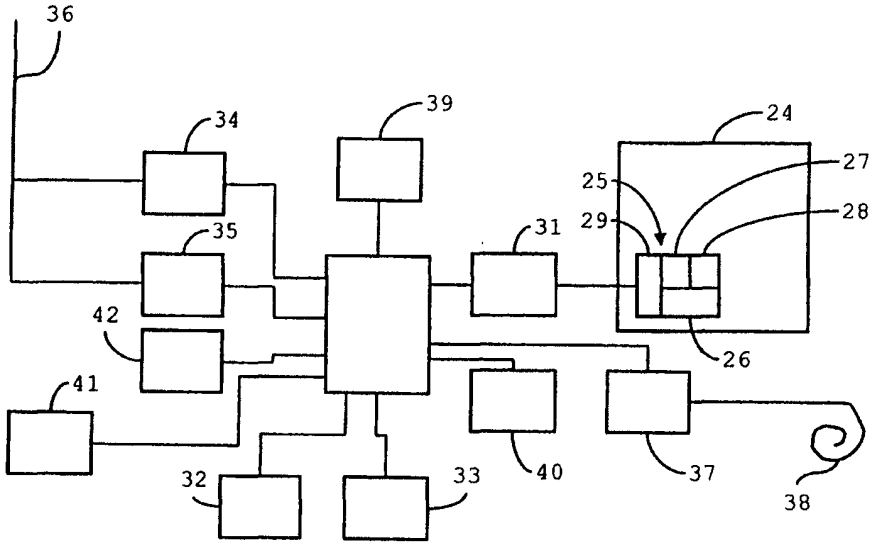

36
34
39
24
27
25
29
28
35
31
42
26
41
40
37
32
33
38

图4