



# (12) 发明专利

(10) 授权公告号 CN 101305545 B

(45) 授权公告日 2013. 04. 03

(21) 申请号 200680041859. 0

(22) 申请日 2006. 11. 10

(30) 优先权数据

10-2005-0108263 2005. 11. 11 KR

(85) PCT申请进入国家阶段日

2008. 05. 09

(86) PCT申请的申请数据

PCT/KR2006/004717 2006. 11. 10

(87) PCT申请的公布数据

W02007/055539 EN 2007. 05. 18

(73) 专利权人 LG 电子株式会社

地址 韩国首尔

(72) 发明人 金兑炫 李承帝

(74) 专利代理机构 北京三友知识产权代理有限公司

11127

代理人 李辉

(51) Int. Cl.

H04L 9/32(2006. 01)

(56) 对比文件

US 2005/0216739 A1, 2005. 09. 29, 说明书第 003-004 段、0012 段、0017 段、0054-0091 段, 附图 1-4.

WO 2005/091551 A1, 2005. 09. 29, 全文.

WO 2005/091162 A1, 2005. 09. 29, 全文.

WO 2005/101258 A1, 2005. 10. 27, 全文.

WO 2005/093558 A1, 2005. 10. 06, 全文.

审查员 杨瑞丽

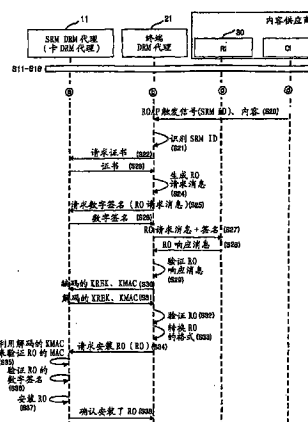
权利要求书 2 页 说明书 8 页 附图 4 页

## (54) 发明名称

用于管理安全可移除介质的数字版权的方法和装置

## (57) 摘要

公开了一种在数字版权管理系统中管理 SRM 的版权对象的方法和装置。用于管理绑定到 SRM 的版权对象的方法包括以下步骤: 从授权中心向终端发送 ROAP 触发信号; 从终端向授权中心发送 RO 请求消息, 并且从授权中心向终端发送对于 RO 请求消息的响应消息; 以及将包括在响应消息中的版权对象从终端的 DRM 代理发送给 SRM 的 DRM 代理并在 SRM 中安装版权对象。因此, SRM 可通过终端从授权中心接收其自己的版权对象。



1. 一种用于管理安全可移除介质 SRM 的版权对象的方法,该方法由终端执行并且包括以下步骤:

所述终端从授权服务器接收触发消息;

所述终端检查在所述触发消息中包括的设备参数;

如果所述设备参数表示所述 SRM,所述终端生成用于从所述授权服务器请求针对所述 SRM 的版权对象的版权对象请求消息,所述版权对象绑定到所述 SRM,并且所述版权对象请求消息包括用于标识所述 SRM 的 SRM ID;

所述终端向所述 SRM 发送包括所生成的用于请求针对所述 SRM 的版权对象的版权对象请求消息的签名请求;

所述终端从所述 SRM 接收包括所述 SRM 的签名的签名响应;

所述终端向所述授权服务器发送所生成的用于请求针对所述 SRM 的版权对象的版权对象请求消息,其中在所生成的版权对象请求消息中插入有所接收到的所述 SRM 的签名;

所述终端从所述授权服务器接收版权对象响应消息,该版权对象响应消息包括所述 SRM ID 以及受保护的版权对象,其中所述版权对象被加密地绑定到所述 SRM;

所述终端将所述受保护的版权对象转换为用于与所接收到的版权对象的相关信息格式;以及

所述终端将与要被安装在所述 SRM 内的所述受保护的版权对象相关的信息发送给该 SRM。

2. 根据权利要求 1 所述的方法,其中所述触发消息是版权对象获取协议 ROAP 触发消息。

3. 根据权利要求 1 所述的方法,其中所述转换步骤包括将与所述受保护的版权对象相关的信息格式化,以使得该与所述受保护的版权对象有关的信息能够被安装在所述 SRM 内。

4. 根据权利要求 1 所述的方法,其中所述版权对象响应消息包括第二签名,并且所述方法还包括以下步骤:

验证所述第二签名。

5. 根据权利要求 1 所述的方法,其中,

所述受保护的版权对象包括版权加密密钥 KREK 和消息认证码 MAC 算法密钥 KMAC,并且利用所述 SRM 的公钥加密所述版权对象响应消息中的所述 SRMID、所述受保护的版权对象的 KREK 以及 KMAC 中的任意一个。

6. 根据权利要求 5 所述的方法,其中所述方法进一步包括以下步骤:

所述终端将包括在所述版权对象中的加密后的 KREK 和 KMAC 发送给所述 SRM;

所述终端从所述 SRM 接收解密后的 KMAC 密钥;以及

所述终端利用所述解密后的 KMAC 验证所述受保护的版权对象中的 MAC 值。

7. 根据权利要求 1 所述的方法,其中所述设备参数是 SRM ID。

8. 一种用于管理安全可移除介质 SRM 的版权对象的终端,所述终端包括:

用于从授权服务器接收触发消息的模块;

用于检查在所述触发消息中包括的设备参数的模块;

用于如果所述设备参数表示所述 SRM,则生成用于从所述授权服务器请求针对所述

SRM 的版权对象的版权对象请求消息的模块,所述版权对象绑定到所述 SRM,并且所述版权对象请求消息包括用于标识所述 SRM 的 SRM ID;

用于向所述 SRM 发送包括所生成的版权对象请求消息的签名请求的模块;

用于从所述 SRM 接收包括所述 SRM 的签名的签名响应的模块;

用于向所述授权服务器发送所生成的版权对象请求消息的模块,其中在所述版权对象请求消息中插入有接收到的所述 SRM 的签名;

用于从所述授权服务器接收版权对象响应消息的模块,该版权对象响应消息包括所述 SRM ID 以及受保护的版权对象,其中所述版权对象被加密地绑定到所述 SRM;

用于将所述受保护的版权对象转换为用于与所述受保护的版权对象相关的信息的格式的模块;以及

用于将与要被安装在所述 SRM 内的受保护的版权对象相关的信息发送给该 SRM 的模块。

9. 根据权利要求 8 所述的终端,其中所述触发消息是版权对象获取协议 ROAP 触发消息。

10. 根据权利要求 8 所述的终端,其中所述版权对象响应消息包括签名,并且其中所述 DRM 代理还被配置为验证所述签名。

11. 根据权利要求 8 所述的终端,其中所述受保护的版权对象包括版权加密密钥 KREK 和消息认证码 MAC 算法密钥 KMAC,并且

所述 SRM ID、所述版权对象中的 KREK 以及 KMAC 中的任意一个被所述 SRM 的公钥加密。

## 用于管理安全可移除介质的数字版权的方法和装置

### 技术领域

[0001] 本发明涉及数字版权管理 (DRM) 系统,更具体地涉及一种用于发布、下载和存储安全可移除介质 (SRM) 中的 DRM 数字内容的数字版权的方法和系统。

### 背景技术

[0002] 通常来讲,DRM 是这样一种技术,其用于安全地保护和系统地管理数字内容的版权对象 (rights object),并且提供相与数字内容的非法复制、获得使用数字内容的权限,以及使用数字内容的过程有关的一系列保护和管理系统。

[0003] 图 1 示出了通常的 DRM 系统。

[0004] 通常的 DRM 系统对从内容供应商向用户提供的数字内容进行控制,以允许用户使用与授权给该用户的版权对象 (RO) 一样多的数字内容。这里,内容供应商是对应于内容中心 (CI) 和 / 或授权中心 (RI) 的实体。

[0005] 内容中心使用特定的编码密钥来发布受保护的内容 (以下称为 DRM 内容 (或数字内容)),以防止对它们没有访问权限的用户进行访问,并且发布使用这些 DRM 内容所需的版权对象。

[0006] 终端中设置的 DRM 代理从内容中心和授权中心接收 DRM 内容和版权对象,并且通过分析版权对象中包括的许可和 / 或约束来控制相应终端中对 DRM 内容的使用。

### 发明内容

[0007] 通常,因为版权对象是经过特定终端的公有密钥 (public key) 编码的,所以除了拥有与该公有密钥相对应的私有密钥 (private key) 的终端之外的终端不能解码和使用与该版权对象有关的 DRM 内容。

[0008] 因此,该通常 DRM 系统中出现了这样的问题,如果将版权对象和与该版权对象有关的 DRM 内容存储在便携式存储卡 (SRM),例如的多媒体卡中,那么除了已被发布了该版权对象的特定终端之外的终端不能从该存储卡 (即,可称为 SRM) 读出 DRM 内容。

[0009] 而且,因为在通常 DRM 系统中版权对象已经被发布到特定终端,所以如果将版权对象和与该版权对象有关的 DRM 内容存储在存储卡中,则只有已经被发布了该版权对象的特定终端才能从 SRM 读出这些 DRM 内容和该版权对象。因此,出现了 SRM 效用降低的问题。

[0010] 此外,还出现了这样的问题,因为在通常 DRM 系统中内容供应商不能将 DRM 内容的版权对象发布到 SRM,所以 SRM 不能拥有其自己的版权对象。

[0011] 因此,本发明的目的是提供一种用于管理存储卡的数字版权的方法和装置,其中存储卡可以有其自己的版权对象。

[0012] 本发明的另一个目的是提供一种对存储卡中的 DRM 内容的版权对象进行发布、下载和存储的方法和装置。

[0013] 本发明的另一个目的是提供一种用于管理 SRM 的版权对象的方法和装置,其中连接到 SRM 的终端获得绑定到 SRM 的版权对象并且将版权对象发送给 SRM。

[0014] 为了实现这些和其它优点并且根据这里实施和广泛描述的本发明的目的,提供了一种安全可移除介质 (SRM) 的版权对象管理系统,其包括从服务器接收绑定到 SRM 的版权对象的终端;以及通过该终端来接收该版权对象的 SRM。

[0015] 本发明的另一个方面提供了一种用于管理 SRM 的版权对象的方法,该方法包括以下步骤:一设备向授权中心请求绑定到该 SRM 的版权对象;该设备从授权中心接收绑定到该 SRM 的版权对象;以及该设备将绑定到该 SRM 的版权对象发送给该 SRM。

[0016] 本发明的另一个方面提供了一种用于管理 SRM 的版权对象的方法,该方法包括以下步骤:授权中心向终端发送触发信号 (trigger),该触发信号用于通告可以从授权中心向该终端发布绑定到 SRM 的版权对象;授权中心通过该终端来接收对绑定到 SRM 的版权对象的请求;以及授权中心通过该终端将绑定到 SRM 的版权对象发布给 SRM。

[0017] 本发明的另一个方面提供了一种用于管理 SRM 的数字版权的终端,该终端包括:用于接收绑定到 SRM 的版权对象的 DRM 代理。

[0018] 该 DRM 代理将接收到的版权对象发送给 SRM。

[0019] 本发明的另一个方面提供了一种用于管理数字版权的 SRM,该 SRM 包括:用于通过与其相连的终端从授权中心接收绑定到该 SRM 的版权对象的 DRM 代理。

[0020] 本发明的另一个方面提供了一种针对 SRM 的版权对象管理方法,该方法包括以下步骤:从终端向授权中心发送请求绑定到 SRM 的版权对象的 RO 请求消息;接收从授权中心到该终端的响应消息;通过允许该终端验证该版权对象而将该响应消息中包括的版权对象从该终端发送给该 SRM;以及该 SRM 对所发送的版权对象进行验证并安装该版权对象。

[0021] 本发明的另一个方面提供了一种用于管理存储卡的版权对象的方法,该方法包括以下步骤:使终端结合存储卡来验证从服务器接收的版权对象的响应消息中所包括的版权对象;以及使该终端将版权对象转换为可由该存储卡分析的特定格式并将特定格式发送给该存储卡。

[0022] 本发明的另一个方面提供了一种用于管理存储卡的版权对象的方法,该方法包括以下步骤:使终端结合存储卡来验证从服务器接收的版权对象的响应消息中所包括的版权对象;以及在对该版权对象的验证失败的情况下使该终端通告安装版权对象的失败。

[0023] 本发明的另一个方面提供了一种用于对绑定到 SRM 的版权对象进行管理的方法,该方法包括以下步骤:从授权中心向主机设备发送 ROAP 触发信号;从该主机设备向授权中心发送 RO 请求消息并且接收从授权中心到该主机设备的对于该请求消息的响应消息;以及将该响应消息中包括的版权对象从该主机设备的 DRM 代理发送到 SRM 中的 DRM 代理,并将该版权对象安装于其中。

[0024] 通过结合附图来阅读以下对于本发明的详细描述,本发明的前述和其它目的、特征、方面和优点将变得更加清楚。

## 附图说明

[0025] 所包括的用于提供对本发明的进一步理解且并入而构成本说明书的一部分的附图示出了本发明的实施方式并与说明书一起用于说明本发明的原理。

[0026] 附图中:

[0027] 图 1 示出了通常的 DRM 系统;

- [0028] 图 2 示出了根据本发明的 SRM 的数字版权管理系统 ;而
- [0029] 图 3 和 4 示出了根据本发明的用于对 SRM 的数字版权进行管理的方法 ;
- [0030] 图 5 示出了用于对图 3 和 4 中示出的 SRM 的数字版权进行管理的方法。

### 具体实施方式

- [0031] 现在将详细参照本发明的优选实施方式,在附图中示出了这些实施方式的示例。
- [0032] 在本发明中,通过连接到存储卡的终端来发布绑定到存储卡的版权对象 (RO)。终端接收 RO 获取触发信号 (ROAP 触发信号),该出发信号向该终端表明:在内容供应商,即授权中心 (RI) 处准备好了绑定到存储卡的版权对象 (RO),并且绑定到存储卡的版权对象安装在存储卡中。而且,终端生成至少包括存储卡的设备 ID 及其数字签名值的 RO 请求消息,并且将生成的 RO 请求消息发送到授权中心 (RI)。授权中心发送至少包括绑定到该存储卡的版权对象和该 RO 请求消息中包括的存储卡的设备 ID 的响应消息 (RO 响应)。终端将该响应消息中包括的版权对象发送到存储卡,存储卡验证并且安装版权对象。
- [0033] ROAP 触发信号包括存储卡的设备 ID。RO 请求消息包括存储卡的设备 ID、存储卡的数字签名值以及存储卡的证书链。响应消息包括存储卡的设备 ID 和绑定到存储卡的版权对象。
- [0034] 下面将参照附图来描述本发明的优选实施方式。
- [0035] 图 2 示出了根据本发明的存储卡的版权对象管理系统。
- [0036] 如图 2 中所示,根据本发明的存储卡的数字版权管理系统包括:终端 20,用于利用存储卡 ID 来接收版权对象并将版权对象发送到存储卡 10;以及存储卡 10,用于利用存储卡 10 的 ID 通过终端 20 来接收版权对象。
- [0037] 该数字版权管理系统还包括根据终端 20 的请求来发布 DRM 内容和 / 或绑定到存储卡的版权对象的内容供应商。内容供应商包括发布数字内容的版权对象的授权中心 (RI) 30。
- [0038] 终端 20 包括 DRM 代理 21,该 DRM 代理 21 用于生成并发送 RO 请求消息以请求绑定到存储卡的版权对象,并将从授权中心 30 发布的绑定到存储卡的版权对象发送给存储卡 10。
- [0039] 存储卡 10 被称为安全可移除介质 (SRM)。SRM10 包括 DRM 代理 11,该 DRM 代理 11 用于执行与终端 20 的相互认证,并根据终端 20 的请求将 SRM 的数字签名值发送给终端 20,以及通过终端 20 来接收 DRM 内容和 / 或绑定到 SRM 的版权对象。
- [0040] 终端 20 还包括与授权中心 30 进行通信的通信模块 22、在 DRM 代理 21 的控制下访问授权中心 30 以接收 DRM 内容和 / 或版权对象的 web/WAP 浏览器 23,以及在 DRM 代理 21 的控制下与用户进行交互的用户界面 26。
- [0041] 终端 20 还包括用于存储 DRM 内容的元数据和 / 或版权对象的元数据的媒体库 (media library) 24,以及用于存储 DRM 内容和 DRM 代理 21 的应用程序和数据的存储器 25。
- [0042] 内容供应商可以包括用于发布 DRM 内容的内容中心和 / 或用于发布绑定到 SRM 的版权对象的授权中心 30。
- [0043] SRM10 可以是包括用于执行简单计算 (或处理) 的处理器和存储器的便携式存储卡。

[0044] SRM10 还包括存储器 12, 该存储器 12 用于存储包括通过终端 20 而接收到的 DRM 内容和 / 或版权对象的 SRM DRM 代理信息。

[0045] SRM DRM 代理信息包括 DRM 内容、DRM 内容的元数据、DRM 内容的版权对象、版权对象的元数据、授权中心的 RI 上下文以及用于接收版权对象的域的域上下文。

[0046] SRM 代理 11 将要包括在请求绑定到 SRM 的版权对象的 RO 请求消息中的 SRM 签名值发送给终端 20 的 DRM 代理 21, 并验证通过 DRM 代理 21 发送的版权对象。SRM 代理 11 可以建立与终端 20 的安全链路。安全链路表示安全的通信信道。

[0047] SRM10 包括安全数字 (SD) 卡、多媒体卡 (MMC)、智能媒体卡 (SMC)、用户标识模块 (SIM) 卡以及各种可存储多媒体的存储卡。

[0048] 用户界面 26 包括小键盘、jog-shuttle 旋钮、开关、功能键、软键和菜单中的至少一种。

[0049] 下面将参照附图来描述前述根据本发明的 SRM 的数字版权管理系统的操作。

[0050] 因为 SRM10 没有通信模块, 所以它希望通过终端 20 来接收 DRM 内容的版权对象。

[0051] 图 3 和 4 示出了根据本发明的用于对 SRM 的数字版权进行管理的方法。

[0052] 首先, 将描述根据本发明的用于对 SRM 的数字版权进行管理的方法的第一实施方式。

[0053] 如果在 SRM10 插入终端 20 之后施加了电源, 则终端 20 识别 SRM10 (S11), 并执行与 SRM10 的 DRM 代理 11 的相互认证 (S12) (下文中, SRM10 的 DRM 代理 11 可表示为 SRM DRM 代理 11)。此时, 终端 DRM 代理 21 和 SRM DRM 代理 11 相互识别终端 ID (终端 10 的设备 ID) 和 SRM ID (SRM10 的设备 ID)。

[0054] 如果成功地完成了相互认证, 终端 DRM 代理 21 和 SRM DRM 代理 11 就建立安全通信信道。此时, 可选择性地建立终端 DRM 代理 21 和 SRMDRM 代理 11 之间的安全通信信道 (S13)。

[0055] 终端 DRM 代理 21 向 SRM DRM 代理 11 请求 SRM11 的 DRM 代理信息 (下文中, SRM 的 DRM 代理信息可表示为 SRM DRM 代理信息) (S14)。SRM DRM 代理 11 将所请求的 SRM DRM 代理信息提供给终端 DRM 代理 21 (S15)。可在安全通信信道中执行 S14 和 S15 这两个步骤。SRM DRM 代理信息存储在 SRM10 的存储器 12 中。SRM DRM 代理信息包括 DRM 内容、DRM 内容的元数据、DRM 内容的版权对象、版权对象的元数据、授权中心的 RI 上下文, 以及用于接收版权对象的域的域上下文。

[0056] 如果 SRM10 提供了 SRM DRM 代理信息, 终端 20 就基于该 SRMDRM 代理信息和存储在媒体库 24 中的信息来识别要发布的 DRM 内容和版权对象。

[0057] 如果特定 DRM 内容已经存储在 SRM10 和终端 20 的至少一个中, 终端 20 就可以不下载这些特定 DRM 内容。终端 20 可以向内容供应商的内容中心 (CI) 发送内容购买请求, 以接收用于再现这些特定 DRM 内容的版权对象。

[0058] 如果这些特定 DRM 内容既未存储在 SRM10 中也未存储在终端 20 中, 终端 20 就可以向内容供应商的内容中心 (CI) 发送内容购买请求, 以请求 DRM 内容和用于再现这些 DRM 内容的版权对象。

[0059] 终端 20 通过 web/WAP 浏览器 23 来访问内容中心的预定域, 以请求这些特定 DRM 内容 (S16)。在请求这些特定 DRM 内容的情况下, 终端 20 可以向内容中心发送设备参数。设

备参数表示了版权对象所属设备的标识符。例如,版权对象属于 SRM,设备参数就表示 SRM ID。

[0060] 接收到这些特定 DRM 内容的购买请求的内容中心请求授权中心 30 生成这些特定 DRM 内容的版权对象 (S17)。此时,内容中心将从终端 20 发送来的设备参数发送给授权中心 30。而且,内容中心还可将 DRM 内容的 ID 的元数据发送给授权中心 30。

[0061] 然后,授权中心 30 基于设备参数来生成 DRM 内容的版权对象 (S18)。如果设备参数表现为 SRM10 的设备 ID,授权中心 30 就生成绑定到 SRM10 的版权对象。

[0062] 授权中心 30 向内容中心发送包括该设备参数的 RO 生成确认消息,以通知已经生成了针对 SRM10 的版权对象 (S19)。

[0063] 内容中心向终端 20 发送 RO 下载触发信号,即 RO 获取触发信号 (ROAP 触发信号),以通知终端 20 接收 DRM 内容的版权对象 (S20)。ROAP 触发信号包括设备参数 (即 SRM ID) 和授权中心 30 的信息。而且,内容中心还可将 ROAP 触发信号连同 DRM 内容一起发送给终端 20。DRM 内容可存储在终端 20 或 SRM10 中。终端 20 设置有使用户能够确定所下载特定 DRM 内容的存储区的界面 (例如,图形用户界面 (GUI))。

[0064] 可以不执行步骤 S16 到 S19。

[0065] 同时,在执行了步骤 S11 到 S15 之后,终端 20 可以接收来自授权中心 30 的 ROAP 触发信号以接收版权对象 (S20)。

[0066] 从授权中心 30 接收到 ROAP 触发信号的终端 20 识别包含在 ROAP 触发信号中的设备参数 (SRM ID)。

[0067] 如果设备参数表现为 SRM ID,终端 20 就请求 SRM10 的 SRM 代理 11 提供证书链 (S22) 并接收证书链 (S23)。接收到的 SRM 证书链包括 SRM10 的公有密钥。如果终端 20 未与 SRM10 接触,终端 20 就立即停止对于绑定到 SRM10 的版权对象的接收过程 (即,ROAP 事务)。

[0068] 终端 20 利用 SRM ID 来生成包括在步骤 S23 中接收的 SRM 证书链的 RO 请求消息,以请求绑定到 SRM 的版权对象 (S24)。

[0069] 如果生成了用于请求绑定到 SRM10 的版权对象的 RO 请求消息,终端 20 就将该 RO 请求消息发送给 SRM10 的 DRM 代理 11 并且向 DRM 代理 11 请求数字签名 (S25)。

[0070] SRM10 的 DRM 代理 11 利用其私有密钥来生成数字签名然后将所生成的数字签名发送给终端 20 的 DRM 代理 21 (S26)。

[0071] 终端 20 的 DRM 代理 21 将包括从 DRM 代理 11 接收到的 SRM 数字签名的 RO 请求消息发送给授权中心 30 (S27)。

[0072] 授权中心 30 将包括 SRM ID 和版权对象的版权对象响应消息 (RO 响应) 发送给终端 20。在组合发送数字内容和版权对象的情况下,当版权对象被发送给终端 20 时,可将具有版权对象的内容发送给终端 20。

[0073] 终端 20 的 DRM 代理 21 对响应消息进行分析并验证该响应消息的数字签名 (S29)。

[0074] 这样,如果成功地完成了消息验证,终端 20 的 DRM 代理 21 就将包括在版权对象响应消息中的版权对象的元数据登记在媒体库 24 中。如果连同版权对象一起发送了内容,那么终端还将这些内容的元数据登记在媒体库 24 中。如果用户希望的话,可以将内容存储在终端 20 中。



[0075] 如果必要的话,终端 20 可将从授权中心 30 发送来的版权对象转换为可由 SRM10 的 DRM 代理 11 分析的格式 (S33)。终端 20 将版权对象发送给 SRM10 的 DRM 代理 11,以指示安装该版权对象 (S34)。此时,可连同版权对象一起向 SRM10 发送内容。SRM10 的 DRM 代理 11 可将版权对象的安装结果通知给终端 DRM 代理 21 (S38)。

[0076] 接下来,将描述根据本发明的用于对 SRM 的数字版权进行管理的方法的第二实施方式。

[0077] 第二实施方式以这样的方式执行,即,将图 4 中示出的步骤 S30 到 S32 以及 S35 到 S36 添加到第一实施方式中。

[0078] 因为第二实施方式的步骤 S11 到 S29 与第一实施方式中的相同,所以下面将描述步骤 S30 到 S36。

[0079] 如果终端 20 的 DRM 代理 21 从授权中心 (RI)30 接收到了对于 R0 请求消息的响应消息,DRM 代理 21 就通过与 SRM10 的 DRM 代理 11 互相作用 (interwork) 来验证包括在该响应消息中的版权对象。即,终端 20 的 DRM 代理 21 请求 SRM10 的 DRM 代理 11 提供验证信息,来验证包括在响应消息中的版权对象。换言之,终端 20 的 DRM 代理 21 请求对编码的 (或加密的) KPEK (版权加密密钥) 或编码的 (或加密的) KMAC (验证版权对象完整性的 MAC 算法中使用的密钥) 进行解码 (S30)。

[0080] SRM10 的 DRM 代理 11 利用其私有密钥或域密钥来对 KREK 或 KMAC 进行解码,并将解码后的 (或解密后的) KREK 或 KMAC 发送给终端 20 的 DRM 代理 21 (S31)。

[0081] 终端 20 的 DRM 代理 21 利用所发送的 KPEK 或 KMAC 来验证包括在响应消息中的版权对象的 MAC 值 (S32)。

[0082] 如果成功地完成了对该消息的验证,终端 20 的 DRM 代理 21 就将包括在响应消息中的版权对象的元数据登记在媒体库 24 中。如果连同版权对象一起发送了内容,终端 20 就将这些内容的元数据登记在媒体库 24 中。如果用户希望的话,终端 20 可将这些内容存储于其中。

[0083] 如果必要的话,终端 20 可将从授权中心 30 发送来的版权对象转换为可由 SRM10 的 DRM 代理 11 分析的格式 (S33)。终端 20 在将版权对象发送给 SRM 的 DRM 代理之后请求安装该版权对象 (S34)。

[0084] SRM10 的 DRM 代理 11 利用其私有密钥或域密钥解码了的 KMAC 来验证从 DRM 代理 21 发送来的版权对象的 MAC 值 (S35)。结果,如果 MAC 值有效,SRM10 的 DRM 代理 11 就安装所发送的版权对象 (S37)。如果 MAC 值无效,SRM10 的 DRM 代理 11 就不安装所发送的版权对象并丢弃所发送的版权对象。

[0085] 同时,如果在步骤 (S35) 中验证的 MAC 值有效,DRM 代理 11 就可验证包括在所发送的版权对象中的数字签名值 (S36)。如果数字签名值有效,SRM10 的 DRM 代理 11 就安装所发送的版权对象 (S37)。

[0086] 如果 MAC 值或数字签名值无效,SRM10 的 DRM 代理 11 就不安装所发送的版权对象并丢弃所发送的版权对象。

[0087] 在安装了版权对象之后,SRM10 可向终端 20 发送与版权对象的安装有关的确认消息 (S38)。

[0088] 现在来描述根据本发明的第三实施方式的用于获取 SRM 的数字版权的方法。

[0089] 首先,用户连接到授权中心,然后授权中心向终端的 DRM 代理发送 ROAP 触发信号,以表示版权对象应当安装在 SRM 中。

[0090] 终端的 DRM 代理向 SRM 的 DRM 代理请求证书并接收来自 SRM 的 DRM 代理的证书。

[0091] 终端的 DRM 代理生成包括 SRM 的证书的请求消息 (RO 请求消息) 并通过 SRM 的 DRM 代理获得针对所生成的 RO 请求消息的数字签名值 (其中, SRM 的 DRM 代理利用其私有密钥来计算数字签名值并将数字签名值发送给终端)。终端将从 SRM 的 DRM 代理获得的数字签名值附在原始 RO 请求消息商,然后将 RO 请求消息发送给授权中心。此时, RO 请求消息至少包括 SRM ID、SRM 证书链和 SRM 信息。SRM 证书链表示了终端与 SRM 相连接。如果终端未与 SRM 相连接,那么终端立即放弃用于接收绑定到 SRM 的版权对象的进一步过程。

[0092] 授权中心向终端发送 RO 响应消息 (响应消息),该 RO 响应消息包括经 SRM 的公有密钥编码 (或加密) 的 RO、SRM ID 和数字签名值。数字签名值等于通过 RO 请求消息而接收的数字签名值。执行响应消息的后续步骤与图 4 中示出的步骤 S29 到 S38 相同。

[0093] 接下来,将基于成功情况和失败情况来描述根据本发明另一实施方式的用于获取 SRM 的版权对象的方法。

[0094] 当发送 RO 请求消息并由此从授权中心 (授权服务器) 接收到 RO 响应消息时,终端的 DRM 代理请求 SRM 的证书并接收它。终端的 DRM 代理结合 SRM 的 DRM 代理经历对包括在 RO 响应消息中的版权对象 (RO) 的验证。换言之,为了验证包括在 RO 响应消息中的 RO,终端的 DRM 代理请求 SRM 的 DRM 代理来解码 KREK 和 KMAC。

[0095] SRM 的 DRM 代理利用 SRM 的私有密钥来解码 KMAC 和 KPEK 并将解码后的 KMAC 发送给终端的 DRM 代理。

[0096] 终端的 DRM 代理利用所接收的 KMAC 来识别 RO 的完整性。

[0097] 终端的 DRM 代理将 RO 中包括的成对的编码 CEK 和内容 ID 连同 RO ID 一起发送给 SRM 的 DRM 代理,并请求 SRM 的 DRM 代理来解码该 CEK。

[0098] SRM 的 DRM 代理利用解码后的 KPEK 来解码从终端的 DRM 代理发送来的编码 CEK,通过绑定到内容 ID 来存储每个 CEK,并向终端的 DRM 代理发送是否已成功解码 CEK 的消息。

[0099] 如果成功地解码了 CEK, SRM 的 DRM 代理就向终端的 DRM 代理通知已成功解码了 CEK。然后,SRM 的 DRM 代理根据来自终端的 DRM 代理的请求、利用 RO ID 和内容 ID 来搜索 CEK,并将 CEK 发送给终端的 DRM 代理。终端的 DRM 代理将 RO 转换为可由 SRM 识别的格式 (例如,针对版权对象的安全可移除介质格式 (SRMF)),并将 RO 发送给 SRM 的 DRM 代理,以指示安装 RO。SRM 的 DRM 代理向终端的 DRM 代理发送是否已成功安装了 RO 的消息。

[0100] 然而,如果对编码 CEK 的解码失败了,SRM 的 DRM 代理就向终端的 DRM 代理通知对编码 CEK 的解码失败。

[0101] 如果在从授权中心接收的 ROAP 触发信号中设置了表示是否已成功安装 RO 的标记,终端的 DRM 代理就向授权中心发送 RO ID 和是否已成功地在 SRM 中安装了 RO 的消息。如果已成功地在 SRM 中安装了 RO,终端的 DRM 代理就向授权中心发送 RO ID 和是否已成功地在 SRM 中安装了 RO 的消息。如果未在 SRM 中成功地安装 RO,终端的 DRM 代理就向授权中心发送 RO ID 和是否已成功地在 SRM 中安装了 RO 的消息。终端的 DRM 代理可向用户通知是否已成功地在 SRM 中安装了 RO。

[0102] 如上所述,在本发明中,SRM 可通过具有通信模块的终端来接收 DRM 内容和 / 或版

权对象。

[0103] 图 5 示出了用于管理图 3 和 4 中示出的 SRM 的版权对象的方法。

[0104] 如图 5 中所示,通过主机设备从授权中心发布绑定到 SRM 的版权对象。接收绑定到 SRM 的版权对象的过程包括 (A) 从授权中心向主机设备发送 ROAP 触发信号, (B) 从主机设备向授权中心发送 RO 请求消息并且接收对于 RO 请求消息的 RO 响应消息,以及 (C) 将来自主机设备的 DRM 代理的 RO 响应消息中所包括的版权对象发送给 SRM 的 DRM 代理,并且安装该版权对象。

[0105] 主机设备 (例如,终端) 从授权中心接收 ROAP 触发信号。ROAP 触发信号至少包括 SRM ID。

[0106] 主机设备向授权中心发送用于请求绑定到 SRM 的版权对象的 RO 请求消息,用于请求绑定到 SRM 的版权对象。RO 请求消息至少包括 SRMID、SRM 的证书链和 SRM 信息,其中 SRM ID 等于 ROAP 触发信号中所包括的 SRM ID。SRM 信息包括 SRM 的数字签名值。SRM 的公有密钥通过 SRM 的证书链将 SRM 的公有密钥发送给授权中心,并且授权中心通过使用利用 SRM 的公有密钥来验证 SRM 的签名值。如果 SRM 未与连接到主机设备相连接,主机设备就立即放弃用于接收绑定到 SRM 的 RO 的过程 (即,放弃 ROAP 事务)。

[0107] 主机设备从授权中心接收对于 RO 请求消息的 RO 响应消息。RO 响应消息至少包括 SRM ID、数字签名值和受保护的 RO。

[0108] 主机设备通知 SRM 安装包括在 RO 响应消息中的 RO,并且 SRM 通过验证包括在 RO 响应消息中的 RO 来安装 RO。SRM 通过使用利用其私有密钥或域密钥来解码 MAC 密钥并且通过使用利用解码后的 MAC 密钥来验证包括在 RO 响应消息中的 RO 的 MAC 值。如果 RO 的 MAC 值有效,SRM 就安装 RO。而且,SRM 验证包括在 RO 响应消息中的 RO 的 MAC 值和 RO 响应消息的数字签名值,并且如果 MAC 值和数字签名值都有效,SRM 就可安装 RO。

[0109] 如上所述,用于管理存储卡的数字版权的方法和装置具有下面的优点。

[0110] 具有 SRM 的终端通过和与 SRM 的 DRM 代理互相作用而生成用于请求绑定到 SRM 的版权对象的 RO 请求消息,用于请求绑定到 SRM 的版权对象,并且将该 RO 请求消息发送给授权中心,使得由授权中心发布的绑定到 SRM 的版权对象可安装在 SRM 中。

[0111] 因为连接 SRM 的终端通过和与 SRM 相互作用而生成用于请求绑定到 SRM 的版权对象的 RO 请求消息,用于请求绑定到 SRM 的版权对象,所以授权中心可发布绑定到 SRM 的版权对象。

[0112] 当特定 DRM 内容存储在 SRM 和具有 SRM 的终端的至少一个中时,可通过终端将这些特定 DRM 内容的版权对象发布给 SRM,并且然后可在 SRM 中安装该版权对象。

[0113] 可通过组合递送或分开递送,而从授权中心发布这些 DRM 内容和绑定到 SRM 的版权对象。

[0114] 最后,SRM 可存储这些 DRM 内容和 / 或安装绑定到 SRM 的版权对象。

[0115] 因为本发明可具体化实施为若干形式,而不偏离脱离其精神或本质特征,所以还应当理解的是,除非另外指定,上述实施例实施方式不受限于之前描述的任何细节,而是应当在如在所附权利要求中定义的本发明的精神和范围内被广义地解释,并且因此落入权利要求的边界和范围,或这种边界和范围的等效物形式内的所有改变和修改旨在由所附权利要求所包含。

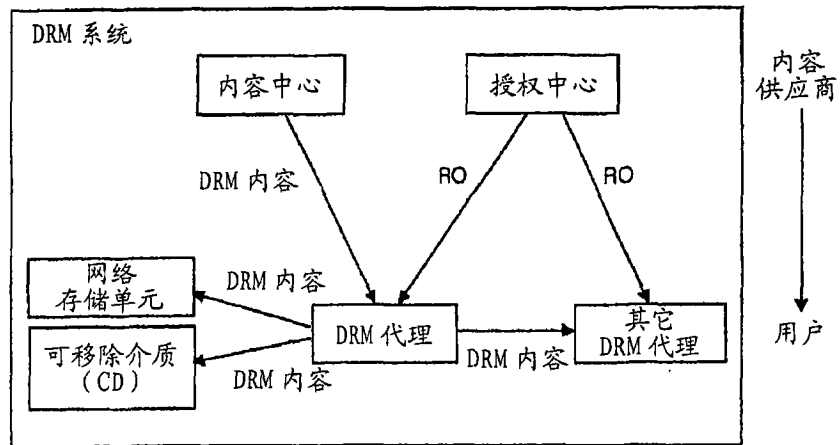


图 1

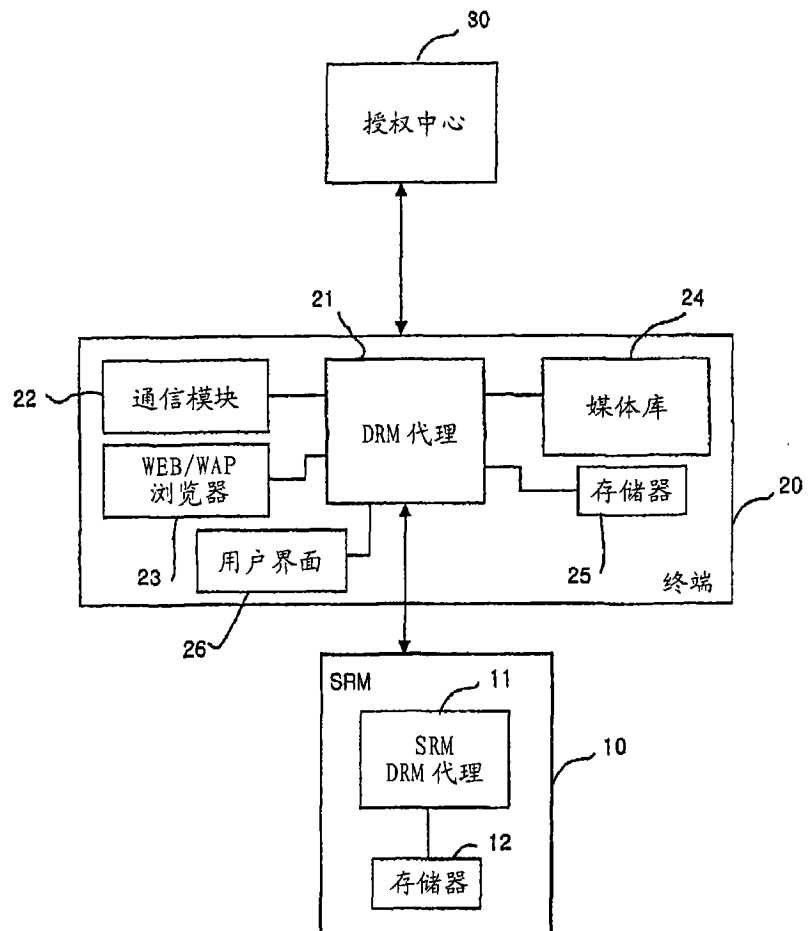


图 2

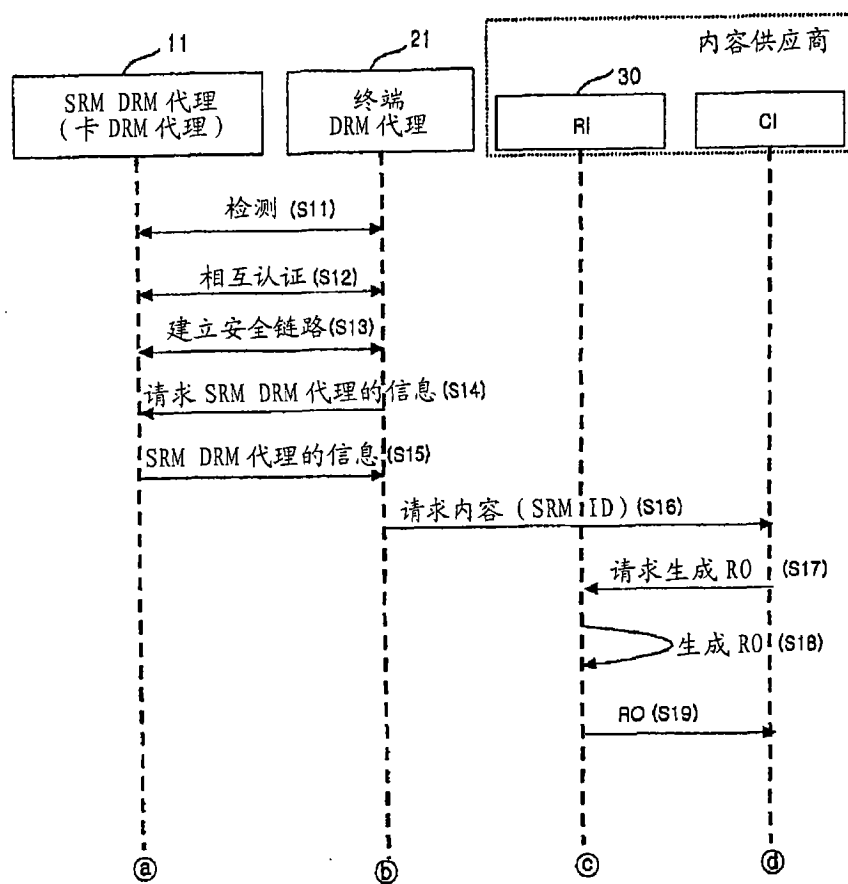


图 3

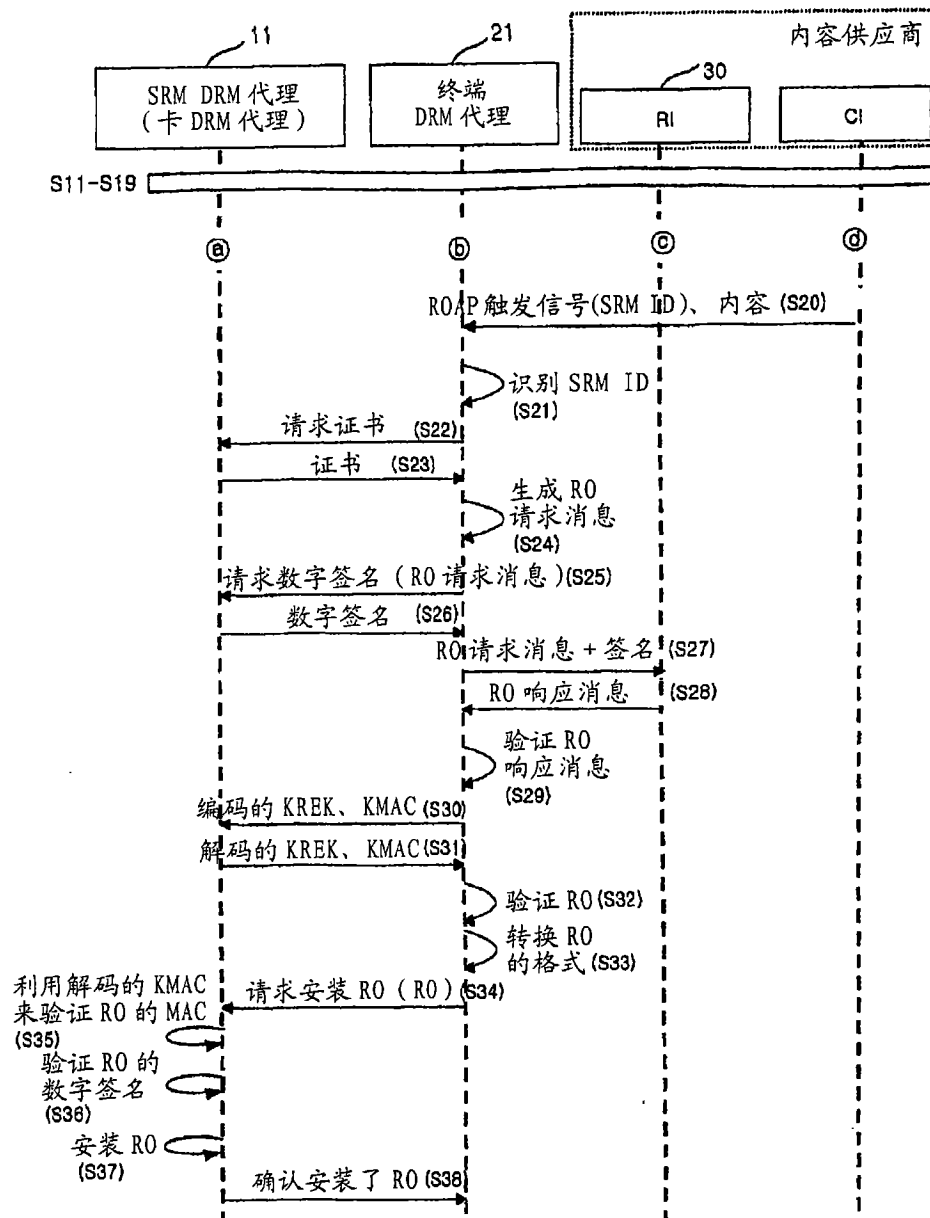


图 4

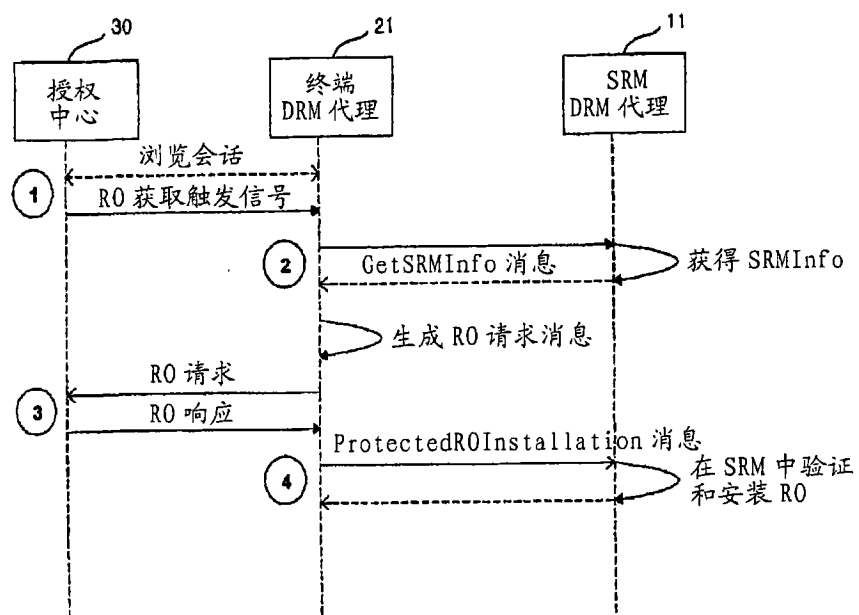


图 5