(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102498493 B
(45)授权公告日 2015.04.01

(21)申请号 201080041436.5
(22)申请日 2010.07.16
(30)优先权数据
61/244,873 2009.09.22 US
61/251,280 2009.10.13 US
61/260,371 2009.11.11 US
10-2010-0011216 2010.02.05 KR
(85)PCT国际申请进入国家阶段日
2012.03.16
(86)PCT国际申请的申请数据
PCT/KR2010/004650 2010.07.16
(87)PCT国际申请的公布数据
WO2011/037318 EN 2011.03.31
(73)专利权人 LG电子株式会社
地址 韩国首尔
(72)发明人 秋渊成 李承帝
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 刘敏 夏凯
(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/82(2013.01)

(56)对比文件
US 2004179691 A1,2004.09.16, 说明书第[0005]段,[0011]段,[0033]段,[0074]段,[0094]段,[0100]段,[0020]段,[0151]段,[0182]段和说明书摘要, 图1-14.
US 2006010498 A1,2006.01.12, 说明书第[0082]-[0086]段, 图1-7.
US 2006129814 A1,2006.06.15, 说明书第[0014]段,[0037]段, 图1-7.
CN 101206696 A,2008.06.25, 全文.
CN 101094062 A,2007.12.26, 全文.

审查员 赵洋

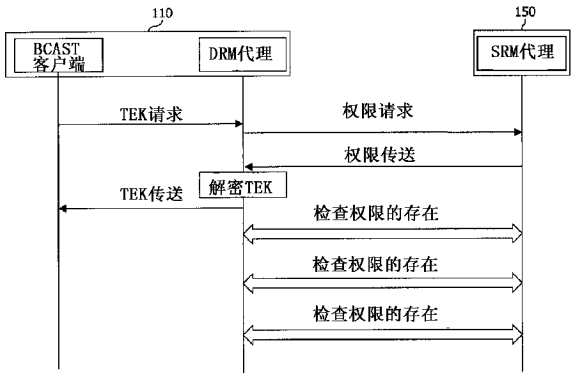
权利要求书2页 说明书21页 附图8页

(54)发明名称

使用对内容的权限的方法

(57)摘要

本发明公开了一种在使用内容的过程期间检查包括有对内容的权限的存储卡是否被安装在终端中的方法。检查操作可以与终端内的BCAST客户端向DRM代理请求业务加密密钥(TEK)的定时同步地执行。另外,在此公开了一种检查存储卡是否被安装在其中以及存储卡中是否实际存在对内容的权限的方法。



CN 102498493 B

1. 一种在终端中使用与广播内容相对应的权限的方法，所述终端具有与其附连的存储卡，所述方法包括：

由所述终端检查与广播内容相对应的权限是否包括用于验证存储卡的存在和在存储卡中的权限的存在的约束；

其中，所述约束包括下述中的至少一个：

同步元素，所述同步元素指示对所述权限的存在的验证应当与业务加密密钥 TEK 请求同步执行，

同步阈值元素，所述同步阈值元素指示导致 TEK 请求的短期密钥消息的数目，使得在其达到所述数目之后，应当执行对所述权限的存在的验证，

检查间隔元素，所述检查间隔元素指定在两个连续执行之间的时间间隔，使得应当重复地执行对所述权限的存在的验证；

如果与广播内容相对应的权限包括所述约束，则从所述终端向所述存储卡传送用于验证在存储卡中的所述权限的存在或不存在的请求消息；

由所述终端从所述存储卡接收响应消息；

检查所述响应消息；以及

如果所述响应消息包括指示失败的状态，则停止或不启动对与广播内容相对应的权限的消费。

2. 根据权利要求 1 所述的方法，其中，根据对业务加密密钥 TEK 的请求来传送所述请求消息。

3. 根据权利要求 1 所述的方法，其中，所述约束是安全可移除介质 Ping SPMPing 元素。

4. 根据权利要求 1 所述的方法，其中，所述请求消息的传送步骤包括：

由所述终端内的数字版权管理 DRM 代理从所述终端内的广播 BCAST 客户端接收业务加密密钥 TEK 请求消息；以及

响应于由所述 DRM 代理接收的 TEK 请求消息的接收来传送所述请求消息。

5. 根据权利要求 1 所述的方法，其中，所述请求消息的传送步骤包括：

由所述终端内的数字版权管理 DRM 代理检查所述约束内的同步阈值元素所指示的数目；以及

根据所述检查步骤来传送所述请求消息。

6. 根据权利要求 1 所述的方法，其中，所述请求消息的传送步骤包括：

检查所述约束中的检查间隔元素所指示的时间间隔；以及

根据所述检查步骤来传送所述请求消息。

7. 根据权利要求 1 所述的方法，其中，如果在所述约束中不存在与是否应当在每个预定持续时间中执行有关的信息，

则对存在的验证应当与业务加密密钥 TEK 请求同步执行。

8. 根据权利要求 1 所述的方法，其中，所述权限内的信息是权限对象加密密钥 REK。

9. 根据权利要求 1 所述的方法，其中，所述请求消息包括权限标识信息和随机值。

10. 根据权利要求 9 所述的方法，所述权限标识信息是句柄。

11. 根据权利要求 9 所述的方法，其中，所述响应消息包括为所述权限内的预定信息和所述随机值中的至少一个获得的散列值。

12. 根据权利要求 11 所述的方法，确定与广播内容相对应的权限是否存在的步骤包括：

为所述权限内的预定信息和所述随机值中的至少一个从所述终端中的存储装置获得散列值；以及

将获得的散列值与所述响应消息内的散列值作比较。

13. 根据权利要求 12 所述的方法，其中，如果散列值彼此相同，则确定在所述存储卡内存在所述权限，并且如果散列值彼此不同，或者权限存在检查响应消息内不存在散列值，则确定所述存储卡内不存在所述权限。

14. 一种将用于广播内容的权限从存储卡提供到终端的方法，所述方法包括：

由所述存储卡将与所述广播内容相对应的权限提供到所述终端，其中，权限信息包括用于验证所述权限的存在和在存储卡中的权限的存在的约束；

其中，所述约束包括下述中的至少一个：

同步元素，所述同步元素指示对所述权限的存在的验证应当与业务加密密钥 TEK 请求同步执行，

同步阈值元素，所述同步阈值元素指示导致 TEK 请求的短期密钥消息的数目，使得在其达到所述数目之后，应当执行对所述权限的存在的验证，

检查间隔元素，所述检查间隔元素指定在两个连续执行之间的时间间隔，使得应当重复地执行对所述权限的存在的验证；

由所述存储卡去激活所述权限；

由所述存储卡从所述终端接收用于验证在存储卡中的所述权限的存在的请求消息，其中，所述请求消息包括用于所述权限的标识信息和随机值；

由所述存储卡检查是否存在所述权限；

如果确定存在所述权限，则由所述存储卡为所述权限内的预定信息和所述随机值中的至少一个生成散列值；以及

将包括所述散列值的响应消息传送到所述终端。

15. 根据权利要求 14 所述的方法，其中，所述约束是安全可移除介质 Ping SRMPing 元素。

使用对内容的权限的方法

技术领域

[0001] 本发明涉及数字版权管理方法，并且更具体地，涉及用于在数字版权管理 (DRM) 中将权限对象安全地发布给存储卡的方法。

背景技术

[0002] 数字版权管理 (DRM)，作为用于安全地保护和系统地管理数字内容的权限的系统技术，提供了用于防止内容的非法复制、获得 DRM 内容的权限对象 (RO)、以及生产、分配和使用 DRM 内容的过程的一系列保护和管理系统。

[0003] 图 1 是图示 DRM 系统的一般配置的视图。

[0004] 典型的 DRM 系统管理数字内容，该数字内容被从内容提供者传送到用户，以被仅按照对用户允许的权限对象来进行使用。此时，内容提供者是与内容发布者 (content issuer)(CI)30 和 / 或权限发布者 (right issuer)(RI)40 相对应的实体。

[0005] 内容发布者 (CI)30 发布通过使用特定的加密密钥（以下称为“DRM 内容”或“数字内容”）来保护内容不受不具有访问授权的用户访问的内容，并且权限发布者 (RI)40 发布使用 DRM 内容所需要的权限对象。

[0006] 终端 10 包括 DRM 代理 (agent)，并且 DRM 代理接收来自内容发布者 (CI)30 的 DRM 内容，并且接收来自权限发布者 (RI)40 的用于内容的权限对象，并且解释包括在权限对象 (RO) 中的许可和 / 或约束，从而管理相关终端中的 DRM 内容的使用。

[0007] 通常，权限对象通过特定终端的公共密钥来加密，并且因此，除了具有与公共密钥配对的私密密钥的终端之外，其他终端都不能解密或使用与该权限对象相关的 DRM 内容。

[0008] 图 2 图示了将现有技术中的 DRM 技术应用于广播服务的示例。

[0009] 参考图 2，图示了将现有技术中的 DRM 技术应用于广播服务（即，BCAST 服务）的示例。

[0010] 广播服务器 50 向权限发布者 (RI)40 传送用服务加密密钥 (SEK) 或节目加密密钥 (PEK) 进行加密的业务加密密钥 (traffic encryption key)(TEK)，并且向第一终端 11 传送用 TEK 加密的广播内容。

[0011] 权限发布者 (RI)40 向第一终端 11 提供包括 SEK 或 PEK 以及加密的 TEK 的权限。

[0012] 终端 11 将从权限发布者 (RI)40 接收到的权限存储在可拆卸存储器 15 中。而且，终端 11 将存储器 15 中的权限复制到终端 11 中，并且然后对包括在权限中的 TEK 进行解密。而且，终端 11 使用解密的 TEK 来消费 (consume) 从广播服务器 50 传送的内容。

[0013] 在上述现有技术中，第二终端 12 还能够接收广播内容；然而，如果第二终端 12 不具有包括 TEK 的权限，则不允许第二终端 12 消费广播内容，从而对该内容进行保护。

[0014] 然而，在上述现有技术中，存储器 15 中的权限被复制到终端 11 中，并且然后通过使用权限来消费内容。因此，如果存储器中已经存在的权限被复制到终端 11 中，并且然后将该存储器 15 安装到第二终端 12 中，则可能导致可以通过第二终端 12 来使用广播内容的问题。

[0015] 如果是诸如电影或戏剧的具有长播放时间的广播内容，则这样的问题可能更加严重。换句话说，存储器 15 可以在没有责任感的情况下被多个终端共享，从而导致广播内容可能在没有许可的情况下被消费的问题。

发明内容

[0016] 对问题的解决方案

[0017] 因此，本发明的目的在于解决上述问题。

[0018] 具体地，本发明的目的在于，只有当包括权限的存储卡被安装在终端中时才允许终端使用内容。另外，本发明的另一个目的在于，当终端使用内容时，检查存储卡内是否存在内容的权限。

[0019] 为了实现以上目标，在此公开了一种在使用内容的过程期间检查包括有对内容的权限的存储卡是否被安装在终端中的方法。可以与终端内的 BCAST 客户端向 DRM 代理请求业务加密密钥 (TEK) 的定时同步地执行检查操作。

[0020] 另外，在此公开了一种检查存储卡是否安装在其中、以及存储卡中是否实际存在内容的权限的方法。

[0021] 具体地，为了实现上述目的，根据本发明，提供了一种在终端中使用对广播内容的权限的方法。在终端中使用对广播内容的权限的方法可以包括 ：检查与广播内容相对应的权限是否包括用于验证存储卡的存在的约束 ；如果权限包括约束，则将用于验证权限（或权限信息）的存在的请求消息传送到存储卡 ；从存储卡接收响应消息 ；响应于该响应消息来确定在存储卡内是否存在权限（或权限信息）；以及根据权限（或权限信息）的存在或不存在来停止或不启动对与广播内容相对应的权限的消费。

[0022] 可以根据对业务加密密钥 (TEK) 的请求来传送请求消息。

[0023] 约束（或限制）可以是 SRMPing 元素。约束（或限制）可以包括同步元素、同步阈值元素和间隔元素中的至少一个，同步元素指示对权限（或权限信息）的存在的验证应当与 TEK 请求同步执行，同步阈值元素指示对权限（或权限信息）的存在的验证应当在 TEK 请求的接收超过预定阈值时执行，间隔元素指示对权限（或权限信息）的存在的验证应当在每个预定持续时间中执行。

[0024] 请求消息的传送步骤可以包括 ：由终端内的 DRM 代理从终端内的 BCAST 客户端接收 TEK 请求消息 ；以及响应于 TEK 请求消息的接收来传送请求消息。

[0025] 请求消息的传送步骤可以包括 ：由终端内的 DRM 代理确定从 BCAST 客户端接收的 TEK 请求消息的数目是否超过约束（或限制）内所指示的阈值 ；以及当超过阈值时，传送请求消息。

[0026] 请求消息的传送步骤可以包括 ：检查是否达到约束（或限制）中所指示的预定持续时间 ；以及当达到持续时间时，传送请求消息。

[0027] 如果不存在与是否应当在约束（或限制）中的每个预定持续时间中执行有关的信息，则对存在的验证应当与 TEK 请求同步执行。

[0028] 权限内的信息可以是权限对象加密密钥 (REK)。

[0029] 请求消息可以包括对权限的标识信息和随机值。

[0030] 响应消息可以包括散列值 (hash value)，并且可以为权限内的预定信息和随机值

中的至少一个获得该散列值。

[0031] 确定步骤包括：为存储在终端中的权限内的信息和随机值中的至少一个获得散列值；以及将获得的散列值与响应消息内的散列值进行比较。

[0032] 如果散列值彼此相同，则可以确定在存储卡内存在权限（或权限信息），而如果散列值彼此不同或者权限存在检查响应消息中不存在散列值，则确定存储卡内不存在权限（或权限信息）。标识信息可以是句柄。

[0033] 另一方面，为了实现上述目标，根据本发明，提供了一种将用于广播内容的权限从存储卡提供到终端的方法。提供权限的方法可以包括：由存储卡将与广播内容相对应的权限提供给终端，其中，权限信息包括用于验证存在权限（或权限信息）的存在的约束；由存储卡去激活该权限；由存储卡从终端接收用于验证权限（或权限信息）的存在的请求消息，其中，请求消息包括对权限（或权限信息）的标识信息和随机值；由存储卡检查是否存在权限（或权限信息）；如果存在权限（或权限信息），则由存储卡为权限（或权限信息）内的预定信息和随机值中的至少一个生成散列值；以及将包括散列值的响应消息传送到终端。

[0034] 本发明被提供以解决上述问题。换句话说，本发明被提供以防止权限在没有责任的情况下被复制，从而允许内容被安全地使用。

[0035] 另外，根据本发明，能够检查存储卡是否被安装在其中，以及在使用广播内容的同时存储卡内是否存在权限，从而防止内容在没有允许的情况下被使用。

附图说明

[0036] 附图被包括进来以提供对本发明进一步理解，并且并入本说明书中，并且构成本说明书的一部分，附图图示了本发明的实施例，并且与说明书一起用于解释本发明的原理。

[0037] 在附图中：

[0038] 图 1 是图示 DRM 系统的一般配置的视图；

[0039] 图 2 图示了现有技术中的 DRM 技术应用于广播服务的示例。

[0040] 图 3 图示了根据本发明的内容和权限对象被发布到存储卡的原理；

[0041] 图 4 是图示根据本发明的原理的示例性流程图；

[0042] 图 5 是图示本发明的第一实施例的流程图；

[0043] 图 6 是图示本发明的第二实施例的流程图；

[0044] 图 7 是图示本发明的第三实施例的流程图；

[0045] 图 8 是图示本发明的第四实施例的流程图；

[0046] 图 9 是从 DRM 代理和 SRM 代理之间的协议的观点图示本发明优选实施例的示例性视图；

[0047] 图 10 是图示根据本发明的终端的操作的流程图；以及

[0048] 图 11 是图示根据本发明的终端 100 和 SRM 150 的配置框图。

具体实施方式

[0049] 本发明将适用于数字版权管理 (DRM) 系统。然而，本发明不限于上述系统，而可以适用于本发明的技术精神所应用于的所有通信系统和方法、以及其他数字版权管理相关系统和方法。

[0050] 应当注意，在此使用的技术术语仅用于描述特定实施例，而不限制本发明。而且，除非另外特别限定，在此使用的技术术语应当被解释为本发明所属的技术领域中的普通技术人员通常理解的意义，并且应该不被过宽或过窄地解释。而且，如果在此使用的技术术语是不能正确表达本发明的精神的错误术语，则应该用本领域技术人员所适当理解的技术术语来代替。另外，在本发明中使用的通用术语应该基于词典的定义或上下文来进行解释，并且应该不被过宽或过窄地解释。

[0051] 顺便提及，除非另外明确使用，单数的表达包括复数意义。在本申请中，术语“包括”不应该被解释为必须包括在此公开的所有元件或步骤，并且应该被解释为不包括其元素或步骤中的一些，或者应该被解释为进一步包括另外的元件或步骤。

[0052] 而且，包括诸如第一、第二等的序号的在此使用的术语可以用于描述多种元件，但是元件不应该受到那些术语的限制。术语仅用于将一个元件与另一个元件进行区分的目的。例如，在不脱离本发明的范围的情况下，第一元件可以被命名为第二元件，并且类似地，第二元件可以被命名为第一元件。

[0053] 在将一个元件“连接”或“链接”到另一个元件的情况下，可以直接地连接或链接至另一个元件，而另一个元件可以存在于其间。相反，在元件被“直接连接”或“直接链接”至另一个元件的情况下，应该理解任何其他元件都不存在于其间。

[0054] 此后，将参考附图来详细地描述本发明的优选实施例，并且不论附图中的附图标记如何，都用相同的附图标记来指示相同或类似元件，并且其冗余的描述将被省略。而且，在描述本发明中，当本发明所属的公知技术的特定描述被判定为混淆了本发明的主旨时，将省略详细描述。而且，应该注意，图示附图仅用于易于解释本发明的精神，并且因此，应该不被解释为通过附图限制本发明的精神。本发明的精神应该被解释为甚至扩展到所有的改变、等价物以及替换，而不是附图。

[0055] 此后，如图 3 至图 7 所示，使用术语“设备”，但是设备还可以被称为用户设备 (UE)、移动设备 (ME) 以及移动站 (MS)。而且，设备可以是便携式设备，诸如便携式电话、PDA、智能电话以及笔记本，或非便携式设备，诸如 PC 和车载设备。

[0056] 术语的定义

[0057] 此后，在参考附图进行描述之前，将简单地定义在本说明书中使用的术语。

[0058] 1)DRM 代理 :当在终端内存在实体时，DRM 代理管理对媒体对象的许可。

[0059] 2) 媒体对象 :表示数字工作 (或操作)，例如，对电话铃声、屏幕保护程序、Java 游戏或其结合的操作。

[0060] 3)DRM 内容 :表示根据权限对象内的许可所消费的媒体对象。

[0061] 4) 广播权限 :还被称为 BCAST 权限。用于 BCAST 服务。

[0062] 5) 权限发布者 (RI) :表示用于对 DRM 内容发布权限对象的实体。

[0063] 6) 许可 :权限发布者 (RI) 允许的实际使用 DRM 内容的许可。

[0064] 权限 :表示给予 DRM 内容的许可 (permission) 和约束 (constraint)(或限制 (restriction))。权限及关于其相关状态的信息和其他信息一起被包括在权限对象中。

[0065] 权限＝权限信息 + 权限对象加密密钥 (REK)

[0066] 8) 权限对象

[0067] 权限对象还被称为权限，包括对 DRM 内容的许可 (或约束 (或限制)) 和与该内容

相关的其他属性。

[0068] 根据本发明的实施例，权限对象通常可以被存储在终端中，而且还可以被存储在存储卡中，例如，DRM。此时，可以以权限对象容器 (rights object container) 的形式存储权限对象。

[0069] SRM 的代理将权限对象容器作为不透明对象进行管理。换句话说，SRM 代理不解析权限对象容器。

[0070] 权限＝权限信息的一部分（不包括状态信息，但是包括所有其他值）+ 权限对象加密密钥 (REK)

[0071] 9) 权限信息

[0072] 权限信息包括权限元数据、权限对象容器以及状态信息。

[0073] 权限信息＝（权限对象 - 权限对象加密密钥 (REK)+ 状态信息 + 状态信息＝权限 - 权限对象加密密钥 (REK)）

[0074] 10) 权限元数据

[0075] 权限元数据包括权限对象版本、权限对象 (RO) 别名 (alias)、权限发布者 (RI) 标识符、权限发布者 (RI)URL、权限发布者 (RI) 别名以及权限发布者 (RI) 时间戳。

[0076] 11) 状态信息

[0077] 状态信息表示有状态使用权 (stateful use rights)（例如，保持计数、间隔开始日期等）内的每个有状态许可 (stateful permission) 的当前状态。如果使用权是有状态使用权，则将状态信息包括在权限中。

[0078] 12) 资产 ID(Asset ID)

[0079] 作为“资产标识符”的缩写，被包括在权限对象 (RO) 中，并且用于标识 DRM 内容。

[0080] 13)REK

[0081] REK 是权限对象加密密钥，具有二进制形式，没有 base64 编码。

[0082] 14) 句柄 (Handle)

[0083] 作为由 DRM 代理生成的随机数，句柄用于允许 DRM 代理识别存储在例如 SRM 的存储卡中的使用权（或权限对象 (RO) 或权限信息）。当由 DRM 代理访问以使用或移动在 SRM 内的使用权时，句柄用于标识使用权（或权限对象 (RO)）。句柄被存储在 SRM 中，或者被存储在终端的操作日志中。

[0084] DRM 代理生成句柄，并且当传送用于使用或移动使用权（或权限对象 (RO)）的消息时，将所生成的句柄传送到 SRM。

[0085] 15) 安全认证信道 (Secure Authenticated channel)(SAC)：表示用于确保所传送或接收到的消息的完整性和可靠性的逻辑信道。

[0086] 16)MAKE：是“Mutual Authentication and Key Exchange（相互认证和密钥交换）”的缩写。配置 SAC 所需要的 SAC 上下文 (SAC context) 可以通过 MAKE 过程来生成。

[0087] 具体地，在 DRM 代理和 SRM 代理之间针对信任模型、实体 ID、安全算法等来执行协商，并且在 MAKE 过程中执行相互识别过程。在 MAKE 过程中交换要在 SAC 中使用的加密密钥（会话密钥、MAC 密钥）的信息。稍后将参考图 5 来详细描述 MAKE 过程。

[0088] 17)MAC 密钥：表示用于确保在 DRM 代理和 SRM 代理之间的 SAC 会话的完整性的密钥。

[0089] 18) 会话密钥：表示用于确保在 DRM 代理和 SRM 代理之间的 SAC 会话的可靠性的加密密钥。

[0090] 19) 实体 ID：是用于终端的 SRM ID 以及用于 SRM 的终端的 ID。

[0091] 20) SAC 上下文

[0092] SAC 上下文包括如表 1 中所示的配置 SAC 所需要的信息。在 DRM 代理和 SRM 代理之间生成新的 SAC 之前一直保持 SAC 上下文。

[0093] 表 1

[0094] [表 1]

[0095]

名称	描述
MAC 密钥	用于确保在 DRM 代理和 SRM 代理之间的 SAC 会话中的完整性的密钥。
会话密钥	用于确保在 DRM 代理和 SRM 代理之间的 SAC 会话中的可靠性的加密密钥。
选择的算法	通过 MAKE 过程协商的算法。
信任锚（trust anchor）	在 SAC 中配置的信任锚。
实体 ID	指示用于 DRM 代理的 SRM 的 ID，并且指示用于 SRM 代理的 DRM 的 ID。

[0096] 21) 受保护的权限对象 (RO)

[0097] 受保护的权限对象 (RO) 是基于 DRM 版本 2.0 的形式。受保护的 RO 是在从 RI 提供到终端时所使用的格式。而且，受保护的 RO 是在从终端的 DRM 代理传送到存储卡（例如 SRM 的 SRM 代理）时所使用的格式。

[0098] 受保护的权限对象 (RO) 包括一系列权限对象，即，<RO> 元素和包括 MAC 值的 <mac> 元素，如以下表中所示。<mac> 元素用于检查 <ro> 元素和密钥的完整性。

[0099] 表 2

[0100] [表 2]

[0101]

```
<element name="protectedRO" type="roap:ProtectedRO" form="qualified"/>
<complexType name="ProtectedRO">
  <sequence>
    <element name="ro" type="roap:ROPayload" form="qualified"/>
    <element name="mac" type="ds:SignatureType"/>
  </sequence>
</complexType>
```

[0102] 如以上表中所示，<ro> 元素包括 ROPayload 项。ROPayload 项包括受保护的权限和包裹密钥 (wrapped key)。包裹密钥用于对权限内加密的部分进行解密。ROPayload 项包括如以下表中所示的内容。

[0103] 表 3

[0104] [表 3]

[0105]

```
<!--      权限对象定义      -->
<complexType name="ROPayload">
  <sequence>
    <element name="riID" type="roap:Identifier"/>
    <element name="rights" type="o-ex:rightsType"/>
    <element name="signature" type="ds:SignatureType" minOccurs="0"/>
    <element name="timeStamp" type="dateTime" minOccurs="0"/>
    <element name="encKey" type="xenc:EncryptedKeyType"/>
    <element ref="roap:roPayloadAliases" minOccurs="0"/>
    <any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="version" type="roap:Version" use="required" />
  <attribute name="Id" type="ID" use="required" />
  <attribute name="stateful" type="boolean"/>
  <attribute name="domainRO" type="boolean"/>
  <attribute name="riURL" type="anyURI"/>
</complexType>
```

[0106] <riID> 元素包括用于标识权限对象发布者的标识符。

[0107] <timestamp>(< 时间戳 >) 元素的值被给定为用于防止通过重传进行攻击或破解的国际协调时间 (UTC)。

[0108] <Signature>(< 签名 >) 元素包括权限对象发布者的签名。

[0109] <encKey>(< 加密密钥 >) 元素包括 MAC 密钥、KMAC、REK(RO 加密密钥) 以及 KREK。

[0110] 另一方面,下表中所示的 <roPayloadAliases>(< 权限对象净荷别名 >) 元素被包括在 ROPayload 中。

[0111] 表 4

[0112] [表 4]

[0113]

```
<element name="roPayloadAliases">
  <complexType>
    <sequence>
      <element name="roAlias" type="roap:String80" minOccurs="0"/>
      <element name="domainAlias" type="roap:String80" minOccurs="0"/>
      <element name="riAlias" type="roap:String80"/>
      <any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </sequence>
  </complexType>
</element>
```

[0114] 另一方面，Nonce 项包括 ROAP 协议消息内的随机值。仅当通过名称指示时，应当使用 Nonce 项。换句话说，每当生成 ROAP 消息时，就生成 Nonce 的随机值。

[0115] 表 5

[0116] [表 5]

[0117]

```
<simpleType name="Nonce">
  <restriction base="base64Binary">
    <minLength value="14"/>
  </restriction>
</simpleType>
```

[0118] 对于本说明书中提出的方法的原理的描述

[0119] 在本发明中，在使用内容的过程期间，检查包括内容的权限的存储卡（即，安全可移除介质 (Secure Removable Media)(SRM)）是否被安装在终端中。另外，根据本发明，在使用内容的过程期间，检查 SRM 内是否实际存在内容的权限、以及 SRM 是否被安装在其中。

[0120] 为了检查，根据本发明，在此公开了权限存在检查协议。权限存在检查协议可以示意性地是 SRM Ping 协议。

[0121] 此后，将参考附图来详细描述根据本发明的实施例。

[0122] 图 3 图示了对存储卡发布根据本发明的内容和权限对象的概念。

[0123] 第一和第二终端 110、120 分别包括 DRM 代理。而且，SRM 150 包括 SRM 代理。

[0124] 参考图 3，内容发布者 (CI)300 将内容发布到第一终端 110。

[0125] 然后，广播服务器 500 将用服务加密密钥 (SEK) 或节目加密密钥 (PEK) 加密的业务加密密钥 (TEK) 传送到权限发布者 (RI)400，并且将用 TEK 加密的广播内容传送到终端 110。

[0126] 权限发布者 (RI)400 将包括 SEK 或 PEK 以及加密的 TEK 的权限提供给第一终端 110。此时，以存储卡（即，SRM 150）的名义发布权限（或 RO）。

[0127] 第一终端 110 将从权限发布者 (RI)400 接收到的权限存储在存储器（即，SRM 150）中。而且，终端 110 将存储器 150 内的权限复制到终端 110 中，并且然后对包括在权限中的 TEK 进行解密。而且，终端 110 使用解密的 TEK 来消费从广播服务器 500 传送的内容。

[0128] 在第一终端 110 使用广播内容的情况下，在 SRM 150 和 SRM 代理之间检查存储有权限的存储卡（即，安全可移除介质 (SRM)）是否被安装在其中。另外，根据本发明，在使用内容的过程期间，检查在 SRM 内是否实际存在内容的权限、以及 SRM 是否安装在其中。

[0129] 此后，将参考图 4 至图 8 来描述本发明的优选实施例。

[0130] 图 4 是图示根据本发明的原理的示意性流程图。

[0131] 参考图 4，第一终端 110 包括广播客户端 (BCAST 客户端）和 DRM 代理。第一终端 110 安装有存储卡，即，SRM 150。SRM 150 包括 SRM 代理。

[0132] 如果应该根据第一终端 110 的用户的请求或其他应用的请求来使用广播内容，则 BCAST 客户端向 DRM 代理请求 TEK。

[0133] 然后，DRM 代理向 SRM 代理 150 请求权限（或 RO) 以获得 TEK。SRM 代理将 SRM 内的权限提供给 DRM 代理。

[0134] DRM 代理临时地存储接收到的权限，并且对权限内的 TEK 进行解密。然后，DRM 代理将 TEK 传送到 BCAST 客户端。

[0135] BCAST 客户端使用 TEK 来消费从广播服务器 500 广播的内容。

[0136] 在消费广播内容的同时，在 DRM 代理和 SRM 代理之间检查存储有权限的存储卡（即，安全可移除介质 (SRM)）是否被安装在其中。换句话说，如附图中所示，执行权限存在检查协议。

[0137] 此时，如果仅检查 SRM 是否被安装在终端中，则造成如下的安全问题。例如，即使在 SRM 代理由于任何原因而不包括用于 BCAST 服务的权限的情况下，SRM 仍然被安装在终端中，并且因此，DRM 代理使用临时存储的权限内的 SEK 和 PEK 来解密 TEK，以提供到 BCAST 客户端。因此，其具有严重的安全错误 :BCAST 客户端消费广播消息。对于另一个实例，在安装在终端内的另一个应用程序向 DRM 代理通知 SRM 被正确地安装在其中的情况下，存在 DRM 代理确定没有错误发生并且解密 TEK 以提供给 BCAST 客户端的问题。因此，甚至在终端中不安装存储卡（即，SRM) 的情况下，能够连续地进行 BCAST 服务的观看。

[0138] 因此，根据本发明的权限存在检查协议允许 SRM 检查实际上在 SRM 内是否实际存在内容的权限、以及 SRM 是否被安装在终端中。

[0139] 权限存在检查协议可以示意性地包括 SRM Ping 请求消息和 SRM Ping 响应消息。

[0140] SRM Ping 请求消息是从 DRM 代理传送到 SRM 代理的消息。SRM Ping 请求消息包括用于存储在 SRM 内的权限的句柄。SRM Ping 请求消息可以包括特定值，例如，随机值，以防止重放攻击 (replay attack)。重放攻击指通过向 DRM 代理传送先前处理的 SRM Ping 响应消息来欺骗 DRM 代理以使其相信在 SRM 内存在权限的行为。

[0141] 如果 SRM 代理接收到 SRM Ping 请求消息，则检查在其中是否存储了与包括在 SRM Ping 请求消息内的句柄相对应的权限。然后，如果存在权限，则 SRM 代理生成与句柄相对应的权限内的 REK 以及随机值的散列值 (hash)，允许散列值被包括在 SRM Ping 响应消息中，以传送到 DRM 代理。DRM 代理可以检查在 SRM 内是否存在权限、以及 SRM 是否被安装在其中。因此，能够防止通过将空的 SRM(vacant SRM) 安装在终端中而非法地使用内容。

[0142] 另一方面，根据本发明，SRM Ping 请求消息可以通过 BCAST 客户端或以预定持续时间与 TEK 的请求同步地被传送到 SRM。而且，每当超过预定阈值时，SRM Ping 请求消息就可以被传送。可以针对用于 TEK 的请求来规定预定阈值。

[0143] 可以在权限中包括关于执行存在检查协议的信息。换句话说，可以在权限中包括与执行 SRM Ping 协议相关的约束（或限制）。与 SRMPing 协议的约束（或限制）可以是包括在权限中的 <srmPing> 元素。<srmPing> 元素可以位于 <constraint>(< 约束 >) 元素的较低层处，<constraint>(< 约束 >) 元素位于权限对象内的 <right>(< 权限 >) 元素的较低层处。

[0144] <srmPing> 元素可以如下所示。

[0145] 表 6

[0146] [表 6]

[0147]

```
<xsd:element name="srmPing" substitutionGroup="o-ex:constraintElement">
  <xsd:complexType>
    <xsd:complexContent>
      <xsd:extension base="xsd:constraintType">
        <xsd:choice minOccurs="0">
          <xsd:element name="synchronised" type="xsd:boolean" default="true"/>
          <xsd:element name="syncThreshold" type="xsd:count "/>
          <xsd:element name="checkInterval" type="xsd:duration"/>
        </xsd:choice>
        <xsd:any minOccurs="0" maxOccurs="unbounded" processContents="lax"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>
</xsd:element>
```

[0148] 如果在权限中包括 <srmPing> 元素，则 DRM 代理应该执行 SRMPing 协议。<srmPing> 元素可以包括 < 同步 > 子元素 (<synchronized> 子元素)、< 同步阈值 > 子元素 (<syncThreshold> 子元素) 以及 < 检查间隔 > 子元素 (<CheckInterval> 子元素) 中的任何一个。SRM Ping 协议的调用 (call) 或不调用 (non-call) 通过子元素来确定。如果在 <srmPing> 元素的较低层处不存在子元素，则认为 DRM 代理包括 < 同步 > 子元素。换句话说，如果在 <srmPing> 元素内包括 < 检查间隔 > 子元素，则根据 < 检查间隔 > 子元素来进行操作。然而，如果其中不包括 < 检查间隔 > 子元素，则在执行短期密钥消息 (Short Term Key Message)(STKM) 过程之前，执行 SRM Ping 协议。例如，如果其中不包括 < 检查间隔 >，则可以与 TEK 的请求同步地执行。

[0149] < 同步 > 子元素指示 SRM Ping 协议与 BCAST 客户端同步。如果 < 同步 > 子元素为“真”则同步，而如果 < 同步 > 子元素为“假”则不同步。如果子元素的值被省略，则解释为“真”。

[0150] < 检查间隔 > 子元素包括执行 SRM Ping 协议的持续时间。换句话说，< 检查间隔

> 子元素指示后续 SRM Ping 协议之间的时间。如果达到在 < 检查间隔 > 子元素中指示的持续时间，则执行 SRM Ping 协议。

[0151] < 同步阈值 > 子元素指示当接收 TEK 请求的数目达到预定值（例如，阈值）时，执行 SRM Ping 协议。例如，如果 < 同步阈值 > 的值为 5，则只要从 BCAST 客户端接收到 TEK 请求多达五次，DRM 代理就与 SRM 代理执行 SRM Ping 协议。此时，DRM 代理具有内部计数器，并且每当接收到 TEK 请求，就使逐一计数器增加。然后，将增加的计数器与在 < 同步阈值 > 子元素中指示的值作比较。如果两个值彼此相同或者计数器的值大于其他值，则 DRM 代理执行 SRM Ping 协议，并且将计数器初始化为零。< 同步阈值 > 子元素执行减小负载同时安全地检查在 SRM 中是否存在 BCAST 权限的作用，由于 SRM Ping 协议而导致可以在 DRM 代理和 SRM 代理中生成该负载。

[0152] 可以如下描述检查约束（或限制）的过程。

[0153] 如果 SRM 被安装在终端中，则终端中的 DRM 代理通过与 SRM 代理的 SRM Hello 和 MAKE（相互认证 & 密钥交换）过程来执行针对通信的基本协商和认证，并且生成安全认证信道 (SAC)。

[0154] 另一方面，如果请求接收 OMA MCAST 广播，则 DRM 代理针对是否存在用于观看 BCAST 服务的 BCAST 权限来检查 SRM 代理，并且复制（即，接收和存储）来自 SRM 代理的权限信息和 REK。随后，DRM 代理检查在从 SRM 复制的权限内是否包括 <srmPing>。

[0155] 如果存在 <srmPing>，则 DRM 代理根据 <srmPing> 来执行 SRM Ping 协议。

[0156] 图 5 是图示本发明的第一实施例的流程图。

[0157] 参考图 5，根据本发明的第一实施例，与 BCAST 客户端的 TEK 请求同步执行用于检查权限（即，BCAST 权限）的存在或不存在的权限存在检查协议，即，SRM Ping 协议。

[0158] 如图 5 中所示的第一实施例包括下述过程 : 接收 TEK 请求 (S111)，当不存在权限时询问 (inquire) 句柄列表 (S120)，询问权限信息 (S130)，选择并检查权限并且询问 REK(S140)，解密和传送 TEK(S150)，与接收 TEK 请求同步检查权限的存在 (S170)，如果检查出存在权限则解密和传送 TEK(S180)，以及如果对内容的使用完成则将权限的状态恢复至原始状态 (S190)。

[0159] 具体地，将如下进行描述。

[0160] 1) 首先，以下将描述接收 TEK 请求的过程 (S111)。

[0161] 如果应当根据第一终端 110 的用户的请求或其他应用的请求来使用广播内容，则第一终端 110 内的 BCAST 客户端将例如附图中图示的 TEK 请求消息传送到 DRM 代理 (S111)。

[0162] TEK 请求消息是为了 BCAST 客户端观看 BCAST 服务 / 节目 / 内容而请求解密短期密钥消息 (STKM) 中所包括的 TEK 的消息。TEK 请求消息包括用 SEK（或 PEK）(即，附图中所示的 AES- 加密 (SEK)(TEK) 和 CID) 加密的 TEK。CID 是内容 ID 并且是用于区分 SEK 或 PEK 的唯一标识符。CID 可以指示节目 _CID 或服务 _CID。替代地，如果权限是广播权限（或 RO)，则可以指示节目 _BCI 或服务 _BCI。节目 _BCI 和服务 _BCI 将由本领域技术人员通过参考 OMA BCAST 1.0 标准规范来理解，并且因此，这里将不进行描述。

[0163] 2) 接下来，以下将描述当不存在权限 (S120) 时询问句柄列表的过程。

[0164] 如果 DRM 代理接收到 TEK 请求消息，则 DRM 代理验证是否存在与 CID 相对应的 BCAST 权限（即，是否具有先前接收到的 BCAST 权限的副本）。如果在 DRM 代理内存在权限，

则 DRM 代理紧接着使用 SEK 和 PEK 中的至少一个来解密 TEK，并且将包括解密的 TEK 的 TEK 响应消息传送到 BCAST 客户端。

[0165] 然而，如果不存在权限，则 DRM 代理向 SRM 代理传送例如句柄列表查询请求消息的列表查询请求消息发送至 SRM 代理，以在存储在 SRM 中的权限中搜索 BCAST 权限 (S121)。该列表查询请求消息包括与 CID 相对应的资产 ID 的散列值的列表和句柄列表的长度。

[0166] SRM 代理询问存储在 SRM 150 中的句柄的列表。换句话说，SRM 代理搜索是否存在与资产 ID 相对应的句柄。

[0167] 然后，SRM 代理将例如句柄列表查询响应消息的列表响应消息发送到 DRM 代理 (S123)。列表响应消息包括状态字段，并且如果存在句柄，则状态的值为“成功”。然而，如果不存在句柄，则状态的值为“失败”。而且，列表响应消息包括错误代码。

[0168] 3) 接下来，以下将描述询问权限信息的过程 (S130)。

[0169] 如果接收到来自 SRM 代理的句柄列表查询响应消息，则 DRM 代理检查包括在消息中的句柄值。

[0170] 然后，DRM 代理向 SRM 代理传送包括检查到的句柄值的权限信息请求消息，例如，权限信息查询请求消息 (S131)。

[0171] SRM 代理搜索是否存在与句柄相对应的权限，即，BCAST 权限 (S132)。

[0172] 随后，SRM 代理向 SRM 代理传送权限信息响应消息，例如，权限信息查询响应消息 (S133)。如果存在与句柄相对应的权限，则权限信息响应消息包括权限信息。在此，权限信息包括权限元数据、权限对象容器以及权限的状态信息。

[0173] 而且，权限信息响应消息包括状态字段。如果存在权限，则状态包括“成功”或与成功相对应的值，而如果不存在权限，则包括“错误”或与错误相对应的值。

[0174] 4) 接下来，以下将描述选择和检查权限并且询问 REK 的过程 (S140)。

[0175] 如果接收的权限信息响应消息被接收到，则 DRM 代理存储提供权限信息的 SRM 的 ID。

[0176] DRM 代理选择接收到的权限信息响应消息内的权限信息并对其进行检查 (S141)。具体地，DRM 代理检查权限信息内的 <rights> 元素。然后，DRM 代理检查在 <rights> 元素内是否存在用于检查是否存在权限的约束 (或限制)，即，<srmPing> 元素。如果存在 <srmPing> 元素，则 DRM 代理检查 <srmPing> 元素内的子元素。<srmPing> 元素可以包括 < 同步 > 子元素、< 同步阈值 > 子元素以及 < 检查间隔 > 子元素中的至少一个。此后，如图 5 中所示，通过假设 < 同步 > 子元素被包括在 <srmPing> 元素内来进行描述。

[0177] DRM 代理获得权限信息，但是不具有用于 BCAST 权限的 REK，并且因此，不允许访问内容加密密钥 (CEK)。CEK 包括服务加密密钥 (SEK) 或节目加密密钥 (PEK)。

[0178] 因此，DRM 代理将例如 REK 查询请求消息的 REK 请求消息传送到 SRM 代理，以便于获得 REK(S142)。REK 请求消息包括存储在 SRM 中的权限的句柄以及针对权限所生成的新句柄。只有 DRM 代理知道该新句柄，并且因此，其他 DRM 代理不能访问相关权限。而且，REK 获得请求消息包括用于请求在 SRM 内将权限改变为非活动状态或禁用状态的信息。

[0179] 当接收 REK 请求消息时，SRM 代理将句柄改变为用于与该句柄相对应的权限的新句柄，并且将权限改变为非活动状态或禁用状态 (S143)。可以仅通过知道新句柄的 DRM 代理来将非活动或禁用权限再次改变为活动状态或启用状态。

[0180] 随后，SRM 代理向 DRM 代理传送包括权限的 REK 的 REK 响应消息，例如，REK 查询响应消息 (S144)。REK 响应消息状态。该状态指示非活动或禁用的成功或失败，即，是否将新句柄改变为成功。REK 响应消息可以进一步包括散列值。为此，SRM 代理生成随机值，并且生成对 REK 和所生成的随机值的散列值。

[0181] 5) 接下来，以下将描述解密和传送 TEK 的过程 (S150)。

[0182] 当接收 REK 响应消息时，DRM 代理使用 REK 响应消息内的 REK 来对权限信息内的 <rights> 元素内的 CEK 进行解密，并且使用解密的 CEK(包括 SEK 或 PEK) 来解密 TEK(S151)。

[0183] 换句话说，AES- 加密 {REK}(CEK) →通过使用 REK 解密→ CEK = SEK 或 PEK

[0184] AES- 加密 {REK}(CEK) 或 AES- 加密 {PEK}(TEK) →通过使用 SEK 或 PEK 解密→ TEK

[0185] 在此，AES- 加密 {x}(y) 指示使用加密密钥 x 的明文 (plaintext)y 的 AES- 加密值。通过使用加密密钥 x 来执行对此的加密以获得解密结果 y。

[0186] 响应于处理 S111 的 TEK 请求，DRM 代理将 TEK 响应消息传送到 BCAST 客户端 (S152)。TEK 响应消息包括解密的 TEK。此时，TEK 响应消息可以进一步包括状态字段。如果解密成功，则状态包括“成功”或与成功相对应的值。相反，如果解密失败，则状态包括“失败”或与失败相对应的值。而且，TEK 响应消息可以进一步包括状态码。如果解密失败，则状态码被设置为“TEK 解密失败”。

[0187] BCAST 客户端使用 TEK 来消费从广播服务器 500 广播的内容。

[0188] 6) 接下来，以下将描述与 TEK 请求的接收 (S 161) 同步的检查权限的存在的过程 (S170)。如果在 BCAST 客户端使用 TEK 消费内容的同时达到预定持续时间或预置定时，则 BCAST 客户端将 TEK 请求消息重传到 DRM 客户端 (S171)。TEK 请求消息类似于以上描述，并且不再进行描述。

[0189] 当接收 TEK 请求消息时，DRM 代理根据 <srmPing> 元素内的 < 同步 > 子元素来执行 SRM Ping 协议。

[0190] 具体地，DRM 代理向 SRM 代理传送权限存在检查请求消息或 SRM Ping 请求消息，以便于检查 SRM 内是否存在权限 (S172)。此时，权限存在检查请求消息或 SRM Ping 请求消息包括与包括在 TEK 请求消息中的 CID 相对应的权限等同的新句柄。而且，权限存在检查请求消息或 SRM Ping 请求消息可以进一步包括随机值。为此，DRM 代理生成随机值。随机值可以被实现为通过使用例如伪随机算法来生成。随机值具有确保权限存在检查请求消息或 SRM Ping 请求消息的最新性 (latestness) 并且防止重放攻击的优点。另一方面，DRM 代理在接收到权限存在检查响应消息或 SRM Ping 响应消息之前一直保持存储随机值，并且在稍后接收到权限存在检查响应消息或 SRM Ping 响应消息时，确定其是否是重放攻击。

[0191] 权限存在检查请求消息或 SRM Ping 请求消息可以包括以下字段。

[0192] 表 7

[0193] [表 7]

[0194]

字段	说明
句柄	*句柄*是指示 BCAST 权限的值，要求检查该 BCAST 权限存在或不存在，以接收在将要存储在 SRM 中的权限中的 BCAST 服务。句柄是指示存储在 SRM 中的权限的值。
RAND	*RAND* 是由 DRM 代理生成的随机值。RAND 是用于防止用于通过在 SRM Ping 响应之后 DRM 代理检查 BCAST 权限的检查存在或不存在的散列数据的重放。

[0195] 如果接收到权限存在检查请求消息或 SRM Ping 请求消息，则 SRM 代理验证完整性。然后，SRM 代理寻找与 SRM 内的句柄相对应的权限 (S173)。

[0196] 如果找到了与句柄相对应的权限，则 SRM 代理生成包括在接收到的消息中的随机值以及与句柄相对应的权限的 REK 的散列值，并且然后将包括所生成的散列值的权限存在检查响应消息或 SRM Ping 响应消息传送到 DRM 代理 (S174)。此时，用于传送散列值的原因在于，通知其实际上拥有权限而不公开 REK。散列值可以通过使用 SHA-1 散列算法来生成。权限存在检查响应消息或 SRM Ping 响应消息可以进一步包括状态字段。如果权限存在检查请求消息或 SRM Ping 请求消息意义明确，并且 HMAC 值被成功验证，并且在 SRM 内存在权限，则将状态字段设置为“成功”。

[0197] 权限存在检查响应消息或 SIM Ping 响应消息可以包括如以下表中所示的字段。

[0198] 表 8

[0199] [表 8]

[0200]

字段	说明
状态	处理 SRMPing 请求消息的结果。在表 9 中限定了状态值。如果状态中包括任何错误，则 SrmPing 响应消息仅包括状态字段。
散列数据	H(RAND|REK)。RAND 是通过 SRM Ping 请求消息从 DRM 代理接收到的值，并且 REK 指示与 SRM Ping 请求的句柄相对应的权限的 REK。如果用于 BCAST 服务，则该值指示 BCAST 权限的 REK。H( )指示 SHA-1 散列算法。散列数据是以 RAND 和 REK 进行散列的值，并且 RAND 和 REK 彼此相关联。

[0201] 在以下表 9 中示出状态的值。

[0202] 表 9

[0203] [表 9]

[0204]

状态值	说明
成功	成功地执行 SRM Ping 请求消息的处理。
字段完整性验证失败	对 SRM Ping 请求消息的 HMAC 值的验证失败。换句话说，指示 SRM Ping 请求消息的 HMAC 值通过 SRM 代理生成，并且然后与包括在 SRM Ping 请求消息中的 MAC 值作比较，但是它们彼此不同。
未发现句柄	在 SRM 中不存在 DRM 代理请求和检查的权限。换句话说，不存在包括在 SRM Ping 请求中的句柄。
参数失败	SRM Ping 请求的字段具有不适当的长度和结构。
未知错误	其他错误。

[0205] 7) 接下来，以下将描述如果检查出存在权限则解密和传送 TEK 的过程 (S180)。

[0206] 如果 DRM 代理接收到权限存在检查响应消息或 SRM Ping 响应消息，则 DRM 代理通过验证 HMAC 字段来验证消息的完整性。

[0207] 如果 HMAC 验证失败，则状态不被设置为“成功”，或者 DRM 代理不能接收正确的 SRM Ping 响应，则 SRM Ping 协议被认为失败。然后，DRM 代理结束 SRM Ping 协议，并且暂缓 (suspend)BCAST 权限的使用。然后，DRM 代理将 TEK 响应消息的状态设置为“失败”，并且将错误码“权限存在验证失败”传送到 BCAST 客户端。

[0208] 相反，如果成功地完成完整性验证，则 DRM 代理验证包括在接收到的消息中的散列值。DRM 代理可以通过验证来检查 SRM 内是否存在权限。为了验证散列值，则 DRM 代理生成接收到的消息内的随机值以及通过 DRM 代理以 REK 进行散列的值，并且然后与接收到的消息内的散列值作比较。

[0209] 如果两个值相同，则 DRM 代理确定在 SRM 中存在权限。然后，如果确定了存在权限，则 DRM 代理解密 TEK(S181)。TEK 解密类似于以上描述，并且不再进行描述。

[0210] 8) 接下来，以下将描述如果对内容的使用完成 (S190) 则将权限的状态恢复至原始状态的过程。

[0211] 如果在 BCAST 客户端中结束了对广播内容的使用，则 DRM 代理向 SRM 代理传送例如权限启用请求消息 (Rights Enablement Request message) 的权限启用请求消息 (S191)。权限启用请求消息包括权限的句柄和权限的状态信息 (在有状态权限的情况下)。

[0212] 如果接收到权限启用请求消息，则 SRM 代理激活或启用在 SRM 内不活动的权限 (S192)。从此，如果 SRM 被安装在另一个终端中，则 SRM 内的权限将由另一个终端内的 DRM 代理来处理。

[0213] 如果激活或启用是成功的，则 SRM 代理生成包括指示“成功”的状态的权限启用响应消息，例如，权限启用响应消息 (Rights Enablement Response message)。然后，SRM 代理将所生成的消息传送到 DRM 代理 (S193)。

[0214] 如果接收到权限启用响应消息，则 DRM 代理检查消息内的状态。如果状态是成功的，则 DRM 代理删除与临时存储的权限相对应的权限信息和 REK(S194)。

[0215] 图 6 是图示本发明的第二实施例的流程图。

[0216] 如参考图 6 可以看到，根据本发明的第二实施例，在每个预定持续时间中执行权限存在检查协议，即，SRM Ping 协议。

[0217] 换句话说，根据第二实施例，如果 < 检查间隔 > 子元素被包括在权限内的

<srmPing>元素中，则DRM代理使用在S230和S240的过程中获得的权限信息和REK来对来自BCAST客户端的TEK请求进行响应，直到在<检查间隔>子元素内指示的持续时间的计时器终止。如果计时器终止，则DRM代理执行SRM Ping协议。

[0218] 图6中所示的第二实施例包括下述过程：接收TEK请求(S211)、当不存在权限时询问句柄列表(S220)、询问权限信息(S230)、选择和检查权限并且询问REK(S240)、驱动计时器并且在计时器完成之前一直解密和传送TEK(S260)、在计时器完成时检查权限的存在(S270)、重置计时器并且解密和传送TEK直到计时器完成(S280)、以及如果对内容的使用完成则将权限的状态恢复至原始状态(S290)。

[0219] 1-4)接收TEK请求(S211)、当不存在权限时询问句柄列表(S220)、询问权限信息(S230)以及选择和检查权限并且询问REK的过程(S240)类似于图5中图示的每个过程，并且对图5的描述加以必要的变更以进行应用。

[0220] 5)接下来，以下将描述驱动计时器并且解密和传送TEK直到计时器完成为止的过程(S260)。

[0221] 当接收到REK响应消息(S244)时，DRM代理使用REK响应消息内的REK来对权限信息内的<rights>元素内的CEK进行解密，并且使用解密的CEK(包括SEK或PEK)来解密TEK(S261)。

[0222] 换句话说，AES-加密{REK}(CEK)→通过使用REK解密→CEK＝SEK或PEK

[0223] AES-加密{SEK}(TEK)或AES-加密{PEK}(TEK)→通过使用SEK或PEK解密→TEK

[0224] 在此，AES-加密{x}(y)指示使用加密密钥x的明文y的AES-加密值。通过使用加密密钥x来执行对此的加密以获得解密结果y。

[0225] 如果TEK的解密完成，则DRM代理根据<检查间隔>子元素内指示的持续时间来驱动计时器，例如，Ping计时器(S262)。如果计时器完成，即，计时器达到在<检查间隔>子元素中指示的持续时间，则DRM代理实现SRM Ping协议，并且再次重置计时器，以重复地执行SRM Ping协议。

[0226] DRM代理将包括解密的TEK的TEK响应消息传送到BCAST客户端(S263)。

[0227] 如果在计时器完成之前，从BCAST客户端接收到TEK请求消息(S264)，则DRM代理使用在S230和S240的过程中获得的权限信息和REK来解密TEK(S265)，并且将包括解密的TEK的REK响应消息传送到BCAST客户端(S266)。TEK响应消息可以进一步包括状态字段。如果计时器未完成，则状态包括“成功”或与成功相对应的值。相反，如果计时器完成并且SRM Ping协议被执行但失败，则将状态设置为指示“失败”或与失败相对应的值。此时，如果该失败是由权限存在检查过程中的错误而导致的，则将状态码被设置为“权限存在验证失败”，而如果失败是由TEK解密中的错误而导致的，则将状态码被设置为“TEK解密失败”。

[0228] 6)接下来，以下将描述在计时器完成时检查权限的存在的过程(S270)。

[0229] 另一方面，如果计时器完成(S271)，则DRM代理执行与SRM代理的SRM Ping协议(S272-S274)。这些过程(S272-S274)分别类似于如图5中所示的过程(S172-S174)，并且对图5的说明加以必要的变更来进行应用。

[0230] 7)接下来，以下将描述重置计时器并且解密和传送TEK直到计时器完成为止的过程(S280)。

[0231] 如果SRM Ping协议被成功地执行并且确认了在SRM内存在权限(S281),则DRM代理重置计时器(S282)。

[0232] 如果在计时器完成之前从BCAST客户端接收TEK请求消息,则DRM代理使用在S230和S240的过程中获得的权限信息和REK来解密TEK,并且将包括解密的TEK的TEK响应消息传送到BCAST客户端。

[0233] 8)另一方面,如果在BCAST客户端中结束了对广播内容的使用,则DRM代理执行将权限的状态恢复至原始状态的过程(S290)。这类似于图5中所示的S190的过程,并且对图5的说明加以必要的变更来进行应用。

[0234] 另一方面,图5图示了在<同步>子元素被包括在<srmPing>元素中的情况下的操作,而图6图示了在<检查间隔>子元素被包括在权限内的<srmPing>元素内的情况下的操作。从图5和图6的描述中,本领域技术人员可以容易地理解在<同步阈值>子元素被包括在权限内的<srmPing>元素内的情况下的操作的描述,并且因此,省略其描述。应该理解,本发明还包括在<同步阈值>子元素被包括在权限内的<srmPing>元素内的情况下的操作。

[0235] 图7是图示本发明的第三实施例的流程图。

[0236] 与图5和图6中图示的第一和第二实施例不同,图7中所示的第三实施例执行在DRM代理使用从SRM代理获得的权限信息和REK来解密TEK时使权限的状态恢复至原始状态的过程(S390)。

[0237] 图7中所示的第三实施例包括下述过程:接收TEK请求(S311)、当不存在权限时询问句柄列表(S320)、询问权限信息(S330)、选择和检查权限并且询问REK(S340)、如果TEK的加密(S351)成功地完成则使SRM内的权限的状态恢复至原始状态(S390)、检查权限的存在(S370)、以及如果确认了存在权限则解密和传送TEK(S380)。以下将详细地描述以上过程。

[0238] 1-4)接收TEK请求(S311)、当不存在权限时询问句柄列表(S320)、询问权限信息(S330)以及选择和检查权限并且询问REK的过程(S340)类似于图5中所示的每个过程,并且对图5的说明加以必要的变更来进行应用。

[0239] 5)接下来,如果TEK的加密(S351)成功地完成,则将执行下述过程:选择和检查权限并且询问REK(S340)、使SRM内的权限的状态恢复至原始状态(S390)。

[0240] 当接收REK响应消息(S344)时,DRM代理使用REK响应消息内的REK来解密权限信息内的<rights>元素内的CEK,并且使用解密的CEK(包括SEK或PEK)来解密TEK(S351)。

[0241] 如果加密(S351)成功地完成,则DRM代理执行使SRM内的权限的状态恢复至原始状态的过程(S390)。换句话说,DRM代理将例如权限启用请求消息(Rights Enablement Request message)的权限启用请求消息传送到SRM代理(S391),并且SRM代理激活或启用在SRM内不活动的权限(S392)。然后,SRM代理向DRM代理传送例如权限启用响应消息(Rights Enablement Response message)的权限启用响应消息(S393)。

[0242] 然后,DRM代理将包括解密的TEK的TEK响应消息传送到BCAST客户端(S352)。

[0243] 6)接下来,将执行检查权限的存在的过程(S370)。检查权限的存在的过程(S370)可以与如图5的第一实施例所示的TEK请求消息同步地执行,或者可以在如图6的第二实施例所示的计时器完成时来执行。替代地,每当接收TEK请求的次数达到在<同步阈值>

子元素中指示的预定阈值时，就可以执行检查权限的存在的过程 (S370)。

[0244] 7) 接下来，如果检查出存在权限，则执行解密和传送 TEK 的过程 (S380)。过程 380 类似于如图 5 中所示的过程 S180，并且对过程 S180 的描述加以必要的变更来进行应用。

[0245] 8) 另一方面，如果对内容的使用完成，则 DRM 代理删除对与临时存储的权限相对应权限信息和 REK。

[0246] 图 8 是图示本发明的第四实施例的流程图。

[0247] 如图 8 中所示的第四实施例包括下述过程：请求准备 (S411)、询问句柄列表 (S420)、询问权限信息 (S430)、选择和检查权限并且询问 REK(S440)、传送准备完成响应 (S451)、检查权限的存在并且然后根据 TEK 请求传送 TEK(S460)、检查权限的存在并且传送 TEK(S470)、以及如果对内容的使用完成则使 SRM 内的权限的状态恢复至原始状态 (S490)。

[0248] 如图 8 中所示的本发明的第四实施例图示了修改在 BCAST 客户端和 DRM 代理之间的协议 (即，传送或接收到的消息) 的示例。

[0249] 因此，此后，将不详细描述下述过程：询问句柄列表 (S420)、询问权限信息 (S430)、选择和检查权限并且询问 REK(S440)、以及如果对内容的使用完成则使 SRM 内的权限的状态恢复至原始状态 (S490)。

[0250] 此后，将描述下述过程：请求在 BCAST 客户端和 DRM 代理之间执行准备 (S411)、传送准备完成响应 (S451)、以及检查权限的存在并且然后根据 TEK 请求传送 TEK(S460)。

[0251] 1) 首先，以下将描述请求准备的过程 (S411)。

[0252] 如果应该根据第一终端 110 的用户的请求或者其他应用的请求来使用广播内容，则第一终端 110 内的 BCAST 客户端向 DRM 代理传送准备请求消息，例如，附图中所示的 SEK 准备请求消息 (SEK Preparation Request message)(S411)。

[0253] 准备请求消息包括 CID。CID 是内容 ID、以及用于区分 SEK 或 PEK 的唯一标识符。CID 可以指示节目 CID 或服务 CID。替代地，如果权限是广播权限 (或 RO)，则可以指示节目 BCI 或服务 BCI。

[0254] 2-4) 询问句柄列表 (S420)、询问权限信息 (S430)、以及选择和检查权限并且询问 REK 的过程 (S440) 类似于图 5 中所示的每个过程，并且对图 5 的说明加以必要的变更来进行应用。

[0255] 5) 接下来，将执行传送准备完成响应的过程 (S451)。

[0256] 如果接收到 REK 响应消息 (S444)，则 DRM 代理使用 REK 响应消息内的 REK 来解密权限信息内的 <rights> 元素内的 CEK，以从解密的 CEK 获得 SEK 或 PEK。

[0257] 如果如上所述获得 SEK 或 PEK，则 DRM 代理向 BCAST 客户端传送准备完成响应消息，例如，SEK 准备响应消息 (SEK Preparation Response message)(S451)。

[0258] 6) 接下来，将执行根据 TEK 请求检查权限的存在并且然后传送 TEK 的过程 (S460)。

[0259] DRM 代理从 BCAST 客户端接收 TEK 请求消息，例如，TEK 描述请求消息 (TEK Description Request message)(S461)。TEK 描述请求消息包括如上所述的 CID。而且，TEK 描述请求消息包括用 SEK(或 PEK) 加密的 TEK，即 AES- 加密 (SEK)(TEK)。

[0260] 然后，DRM 代理将权限存在检查请求消息或 SRM Ping 请求消息传送到 SRM 代理 (S462)。此时，权限存在检查请求消息或 SRM Ping 请求消息包括与 CID 相对应的权限等同

的新句柄。而且，权限存在检查请求消息或 SRM Ping 请求消息可以进一步包括随机值。

[0261] 如果接收到权限存在检查请求消息或 SRM Ping 请求消息，则 SRM 代理验证完整性。然后，SRM 代理寻找与 SRM 内的句柄相对应的权限 (S463)。如果找到与句柄相对应的权限，则 SRM 代理生成包括在接收到的消息中的随机值以及与句柄相对应的权限的 REK 的散列值，并且然后向 DRM 代理传送包括生成的散列值的权限存在检查响应消息或 SRM Ping 响应消息 (S464)。

[0262] 如果接收到权限存在检查响应消息或 SRM Ping 响应消息，则 DRM 代理使用 SEK 或 PEK 来解密 TEK(S465)。

[0263] 然后，DRM 代理向 BCAST 客户端传送包括解密的 TEK 的 TEK 响应消息，例如，TEK 描述响应消息 (TEK Description Response message)(S466)。

[0264] 然后，BCAST 客户端使用 TEK 来消费广播内容。

[0265] 7) 接下来，将执行在使用广播内容的同时检查权限的存在并且传送 TEK 的过程 (S470)。

[0266] 检查权限的存在的过程 (S470) 可以与图 5 的第一实施例中所示的 TEK 请求消息同步地执行，或者可以在图 6 的第二实施例中所示的计时器完成时执行。替代地，每当接收 TEK 请求的次数达到在 <同步阈值> 子元素中指示的预定阈值时，就可以执行检查权限的存在的过程 (S470)。

[0267] 8) 接下来，如果在 BCAST 客户端中结束对广播内容的使用，则 DRM 代理执行使 SRM 内的权限的状态恢复至原始状态的过程 (S490)。这类似于图 5 中所示的过程 190，并且对图 5 的描述加以必要的变更来进行应用。

[0268] 9) 另一方面，DRM 代理向 BCAST 客户端传送完成请求消息，例如，SEK 完成请求消息 (SEK completion request message)(S495)。完成请求消息可以进一步包括与 SRM 内的权限被激活的结果以及终端中临时存储的权限被删除的结果有关的信息。

[0269] 图 9 是从 DRM 代理和 SRM 代理之间的协议的观点图示本发明优选实施例的示例性视图。

[0270] 如图 9 中所示的示例性视图示出当终端消费 BCAST 权限时根据约束（或限制）检查消息的存在（即，SRM)。具体地，以下将进行描述。

[0271] 1) 首先，从 SRM 重新得到权限。

[0272] 具体地，如果与广播内容的权限相对应的句柄未知，则通过使用列表查询过程（即，句柄列表查询处理）来获得相应句柄。

[0273] 随后，通过权限信息询问处理（即，句柄列表查询处理）来从 SRM 获得权限信息。此时，对提供权限信息的 SRM 的 ID 进行存储。

[0274] 随后，通过 REK 询问过程（即，REK 查询过程）来从 SRM 获得 REK。

[0275] 2) 接下来，权限被用于消费广播内容，并且执行检查权限的存在的过程。

[0276] 当使用权限来消费广播内容时，执行权限存在检查过程（即，SRM Ping 协议），以检查提供权限的 SRM 是否被安装在其中。

[0277] 如果 <srmPing> 约束（或限制）被包括在权限中，则应该执行 SRMPing 协议来使用权限。如果不支持 SRM Ping 协议，则不能使用包括 <srmPing> 约束（或限制）的权限。因此，DRM 代理应该支持 SRM Ping 协议。为此，DRM 代理应该支持 DRM 时间。SRM 代理还应

该支持 SRMPing 协议。

[0278] 在 DRM 代理和 SRM 代理之间执行 SRM Ping 协议。在 DRM 代理和 SRM 代理之间配置 SAC，以执行 SRM Ping 协议。

[0279] 通过将 SRM Ping 请求消息从 DRM 代理传送到 SRM 代理来开始 SRM Ping 协议。SRM 代理执行验证，并且然后将 SRM Ping 响应消息传送到 DRM 代理。

[0280] 如果在权限内的<检查间隔>子元素中所指示的两个连续执行 (two-consecutive executions) 之间的时间被指定，则 DRM 代理重复执行 SRM Ping 协议。如果不存在 <检查间隔 > 子元素，则仅在 BCASTSTKM 的每次调用之前执行 SRM Ping 协议。

[0281] 如果由于失败或不成功地执行而导致 SRM Ping 协议结束，则 DRM 代理暂缓对权限的使用。然后，DRM 代理删除与临时存储的权限相对应的 REK。

[0282] 3) 另一方面，如果对广播内容的消费结束，则完成对权限的使用。

[0283] 如果由于对广播内容的消费结束而完成了对权限的使用，则 DRM 代理暂缓 SRM Ping 协议的执行，并且使用例如权限启用协议 (Rights Enablement protocol) 来激活 SRM 内的权限。然后，SRM 代理删除与临时存储的权限相对应的 REK。

[0284] 图 10 是图示根据本发明的终端的操作的流程图。

[0285] DRM 代理检查是否存在用于检查在广播内容的权限内是否存在存储卡内的权限的约束 (或限制)(S510)。

[0286] 如果存在约束 (或限制)，则 DRM 代理将权限存在检查请求消息传送到存储卡 (S520)。此时，权限存在检查请求消息可以包括权限的识别信息和随机值。

[0287] DRM 代理从存储卡接收包括散列值的权限存在检查响应消息 (S530)。此时，散列值可以被获得用于权限内的预定信息和随机值中的至少一个。

[0288] 然后，DRM 代理检查在 SRM 内是否存在权限 (S540)。此时，可以通过使用散列值来进行检查。

[0289] 随后，根据权限的存在或不存在来确定是否使用广播内容 (S550)。

[0290] 如果不存在权限，则 DRM 代理不开始或暂缓使用权限 (S560)。

[0291] 然而，如果存在权限，则 DRM 代理开始或继续使用权限 (S570)。

[0292] 上述根据本发明的方法可以通过软件、硬件或其结合来实现。例如，根据本发明的方法可以被存储在存储介质 (例如，内部存储器、闪速存储器、硬盘等) 中，并且可以通过可以由诸如微处理器、控制器、微控制器、ASIC(专用集成电路) 等的处理器执行的软件程序中的代码或指令来实现。此后，将参考图 11 来进行描述。

[0293] 图 11 是图示根据本发明的终端 100 和 SRM 150 的配置框图。

[0294] 如图 11 所示，终端 100 可以包括存储单元、传送和接收单元、连接器以及控制器。而且，存储卡 (即，SRM) 可以包括存储单元、连接器和控制器。

[0295] 连接器彼此连接终端 100 和存储卡 (即，SRM)。

[0296] 存储单元存储实现如图 4 至图 8 中所示的前述方法的软件程序。而且，存储单元存储每个接收到的消息内的信息。

[0297] 控制器中的每一个分别控制存储单元和传送接收单元。具体地，控制器实现特别是存储在每个存储单元中上述方法，。

[0298] 虽然以上仅示意性地描述了本发明的优选实施例，但是本发明的范围不限于那些

特定实施例，并且因此可以在不脱离本发明的精神的情况下，并且在所附权利要求的范围内，在本发明中作出多种修改、改变和改进。

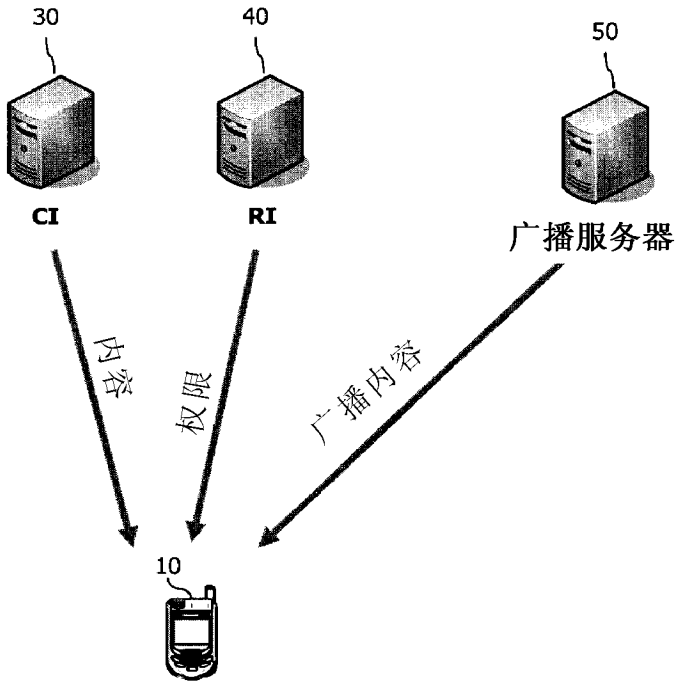

30
40
50
CI
RI
广播服务器
内容
权限
广播内容
10

图 1

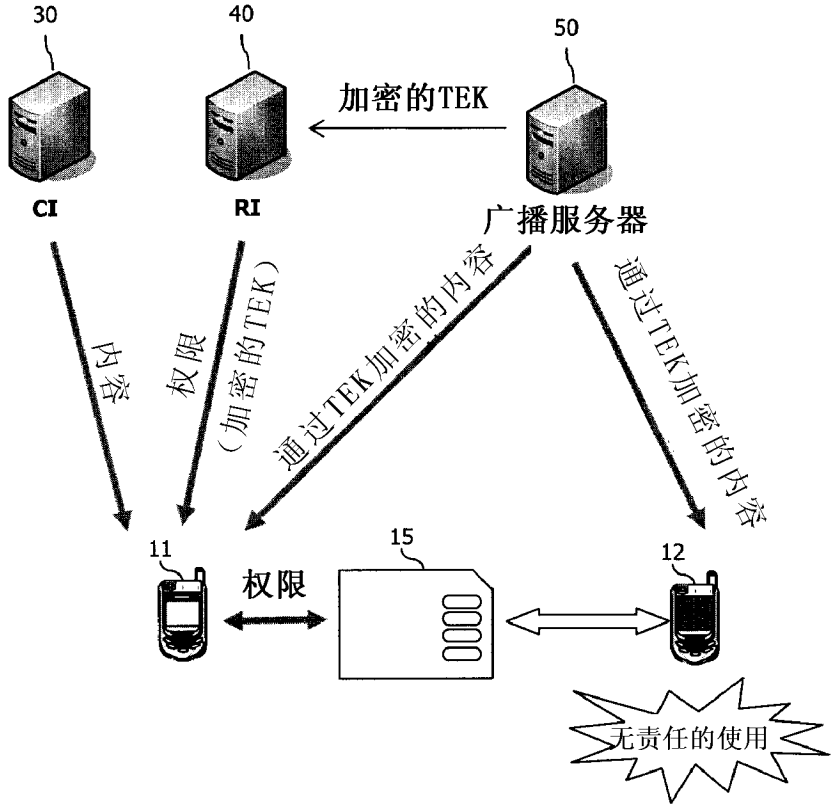

30
40
50
加密的TEK
CI
RI
广播服务器
内容
权限
(加密的TEK)
通过TEK加密的内容
通过TEK加密的内容
11
15
12
权限
无责任的使用

图 2

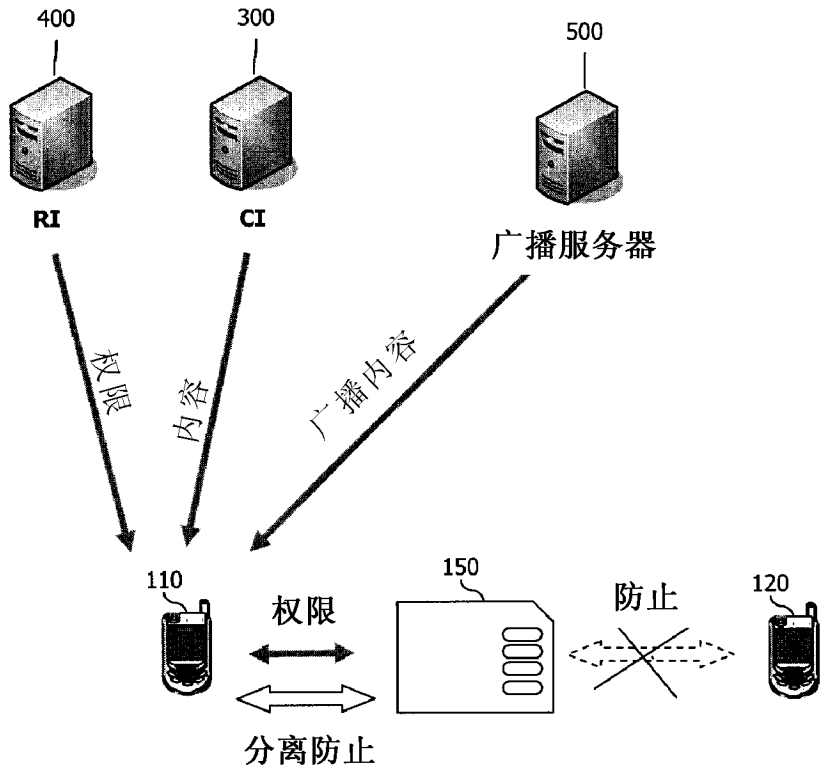

400
300
500
RI
CI
广播服务器
权限
内容
广播内容
110
150
120
权限
防止
分离防止

图 3

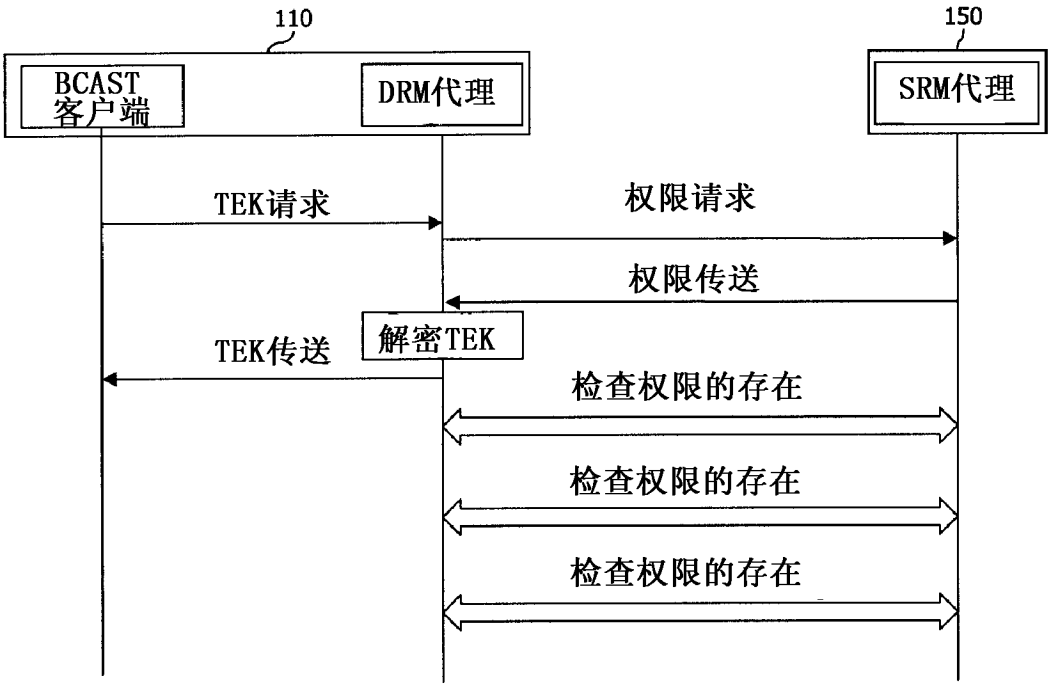

110
150
BCAST
客户端
DRM代理
SRM代理
TEK请求
权限请求
权限传送
解密TEK
TEK传送
检查权限的存在
检查权限的存在
检查权限的存在

图 4

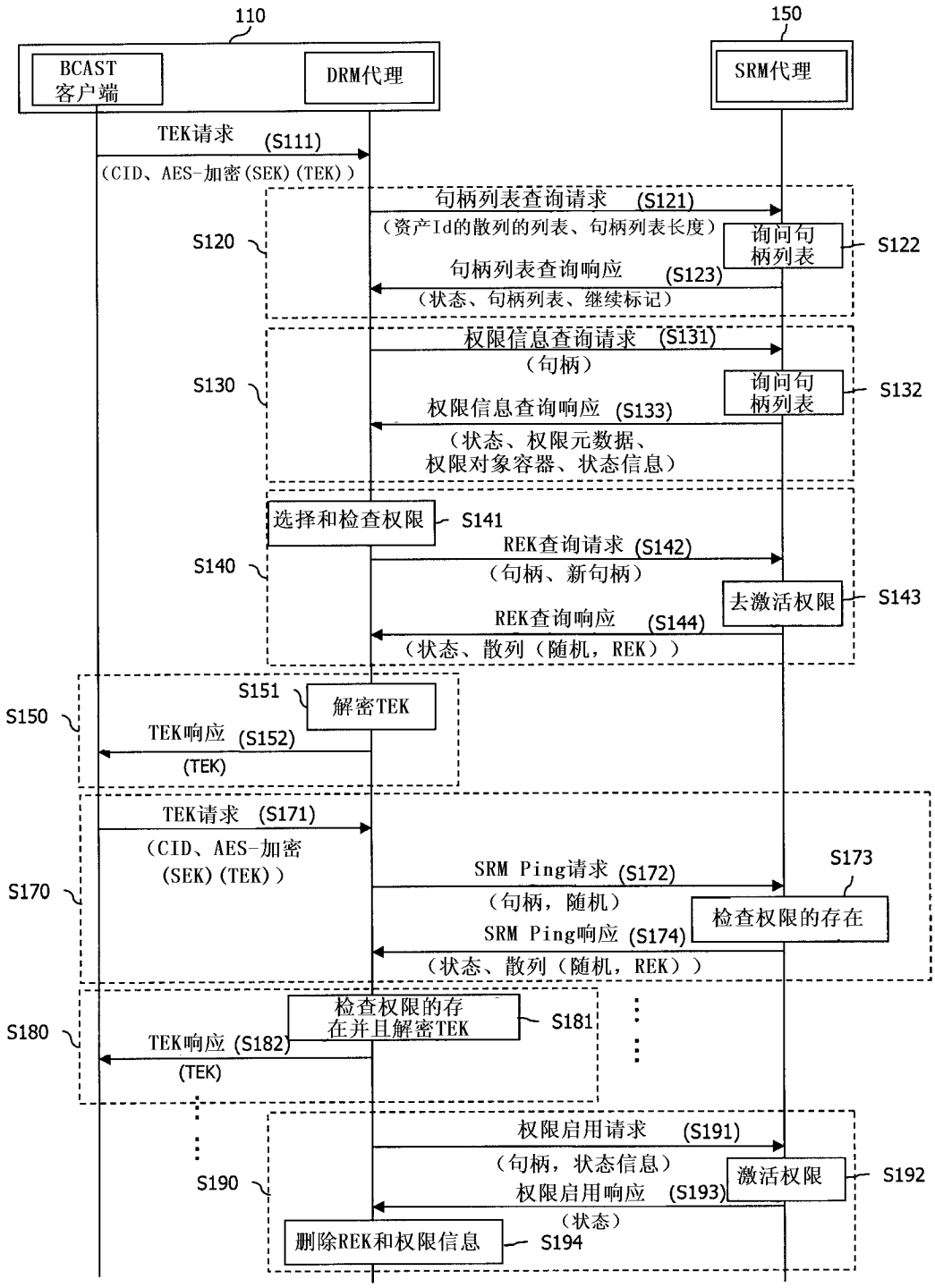

110
150
BCAST 客户端
DRM代理
SRM代理
TEK请求 (S111)
(CID、AES-加密(SEK)(TEK))
句柄列表查询请求 (S121)
(资产Id的散列的列表、句柄列表长度)
S120
询问句柄列表
S122
句柄列表查询响应 (S123)
(状态、句柄列表、继续标记)
权限信息查询请求 (S131)
(句柄)
S130
询问句柄列表
S132
权限信息查询响应 (S133)
(状态、权限元数据、权限对象容器、状态信息)
选择和检查权限
S141
REK查询请求 (S142)
(句柄、新句柄)
S140
去激活权限
S143
REK查询响应 (S144)
(状态、散列(随机,REK))
S151
解密TEK
S150
TEK响应 (S152)
(TEK)
TEK请求 (S171)
(CID、AES-加密(SEK)(TEK))
S173
SRM Ping请求 (S172)
(句柄,随机)
S170
检查权限的存在
SRM Ping响应 (S174)
(状态、散列(随机,REK))
检查权限的存在并且解密TEK
S181
S180
TEK响应 (S182)
(TEK)
权限启用请求 (S191)
(句柄,状态信息)
S190
激活权限
S192
权限启用响应 (S193)
(状态)
删除REK和权限信息
S194

图 5

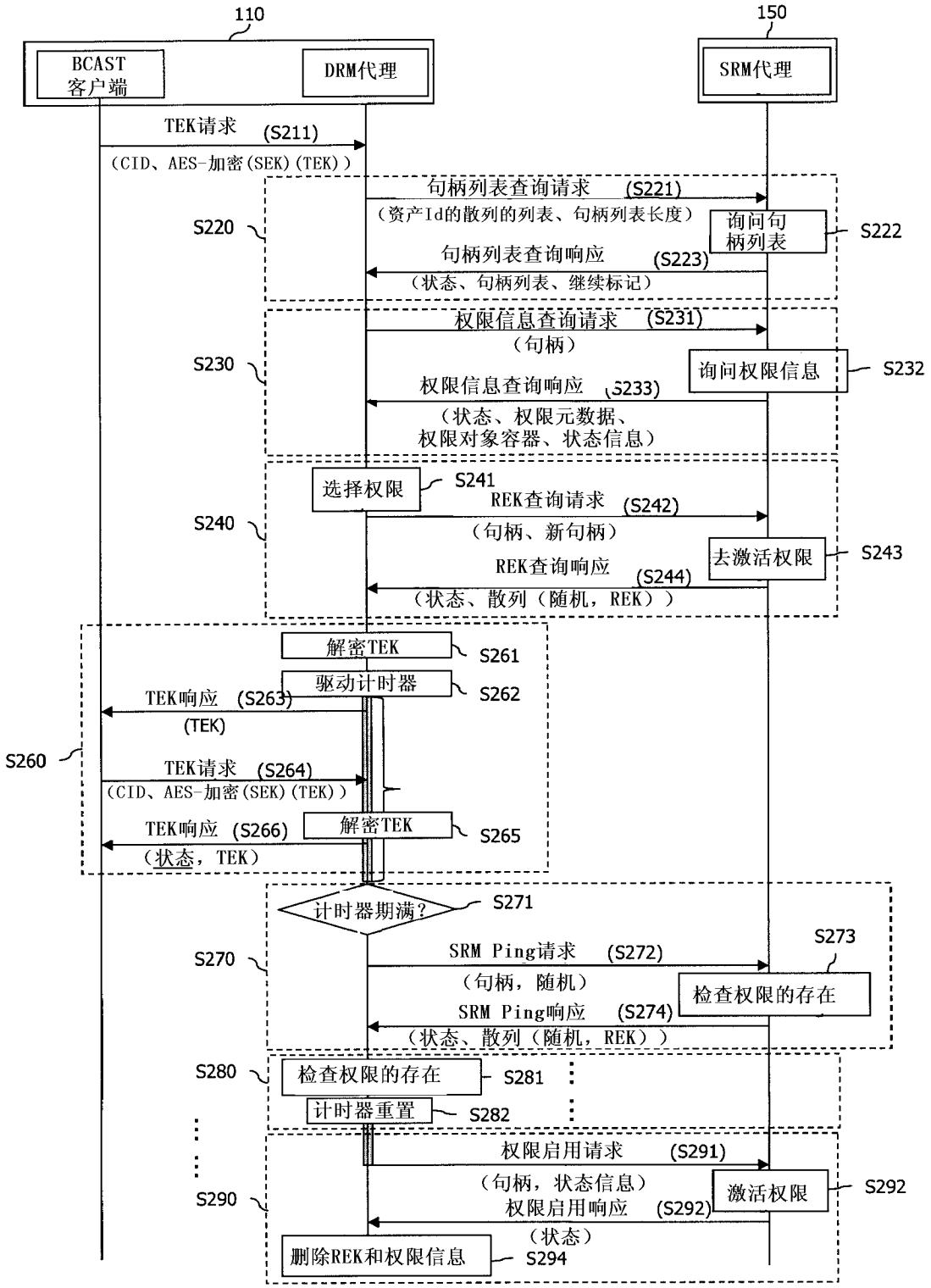

110
150
BCAST 客户端
DRM代理
SRM代理
TEK请求 (S211)
(CID、AES-加密(SEK)(TEK))
句柄列表查询请求 (S221)
(资产Id的散列的列表、句柄列表长度)
S220
询问句柄列表
S222
句柄列表查询响应 (S223)
(状态、句柄列表、继续标记)
权限信息查询请求 (S231)
(句柄)
S230
询问权限信息
S232
权限信息查询响应 (S233)
(状态、权限元数据、权限对象容器、状态信息)
选择权限
S241
REK查询请求 (S242)
(句柄、新句柄)
S240
去激活权限
S243
REK查询响应 (S244)
(状态、散列(随机，REK))
解密TEK
S261
驱动计时器
S262
TEK响应 (S263)
(TEK)
S260
TEK请求 (S264)
(CID、AES-加密(SEK)(TEK))
解密TEK
S265
TEK响应 (S266)
(状态，TEK)
计时器期满?
S271
S273
SRM Ping请求 (S272)
(句柄，随机)
S270
检查权限的存在
SRM Ping响应 (S274)
(状态、散列(随机，REK))
S280
检查权限的存在
S281
计时器重置
S282
权限启用请求 (S291)
(句柄，状态信息)
激活权限
S292
S290
权限启用响应 (S292)
(状态)
删除REK和权限信息
S294

图 6

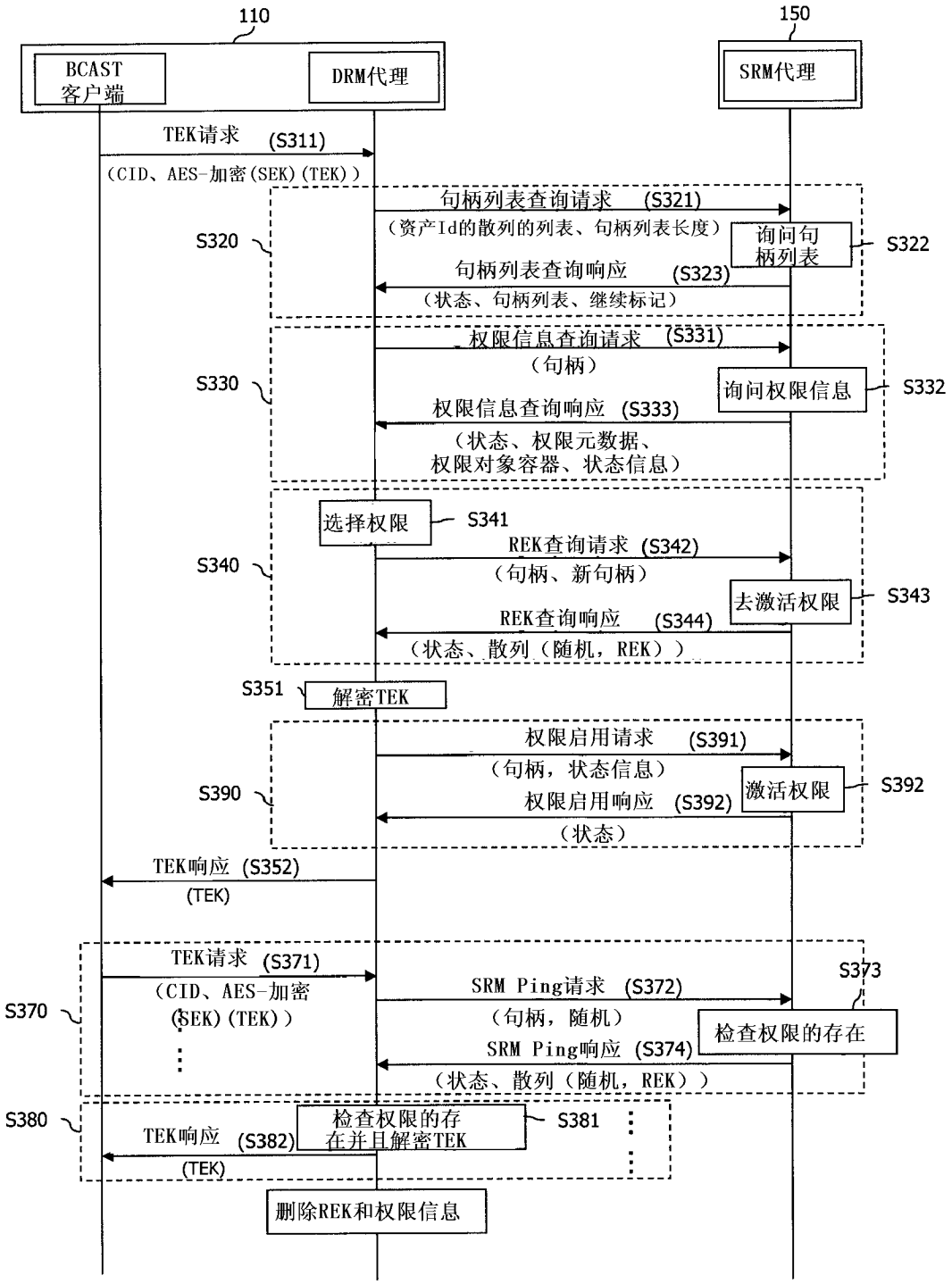

110
150
BCAST 客户端
DRM代理
SRM代理
TEK请求 (S311)
(CID、AES-加密(SEK)(TEK))
句柄列表查询请求 (S321)
(资产Id的散列的列表、句柄列表长度)
S320
询问句柄列表
S322
句柄列表查询响应 (S323)
(状态、句柄列表、继续标记)
权限信息查询请求 (S331)
(句柄)
S330
询问权限信息
S332
权限信息查询响应 (S333)
(状态、权限元数据、权限对象容器、状态信息)
选择权限
S341
REK查询请求 (S342)
(句柄、新句柄)
S340
去激活权限
S343
REK查询响应 (S344)
(状态、散列(随机，REK))
S351
解密TEK
权限启用请求 (S391)
(句柄，状态信息)
S390
激活权限
S392
权限启用响应 (S392)
(状态)
TEK响应 (S352)
(TEK)
TEK请求 (S371)
(CID、AES-加密(SEK)(TEK))
S370
SRM Ping请求 (S372)
(句柄，随机)
S373
检查权限的存在
SRM Ping响应 (S374)
(状态、散列(随机，REK))
S380
检查权限的存在并且解密TEK
S381
TEK响应 (S382)
(TEK)
删除REK和权限信息

图 7

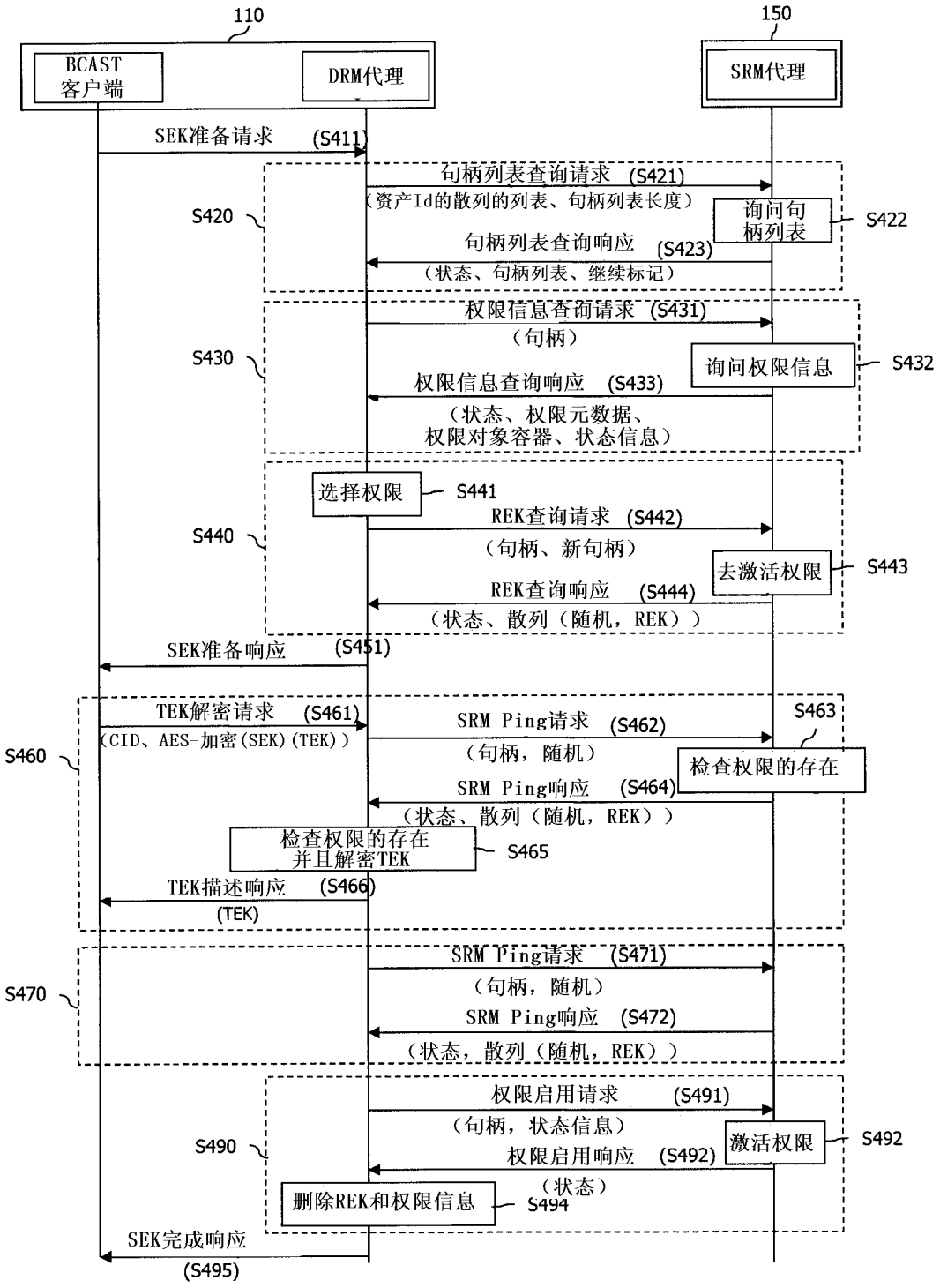

110
150
BCAST
客户端
DRM代理
SRM代理
SEK准备请求 (S411)
句柄列表查询请求 (S421)
(资产Id的散列的列表、句柄列表长度)
S420
询问句柄列表
S422
句柄列表查询响应 (S423)
(状态、句柄列表、继续标记)
权限信息查询请求 (S431)
(句柄)
S430
询问权限信息
S432
权限信息查询响应 (S433)
(状态、权限元数据、
权限对象容器、状态信息)
选择权限
S441
REK查询请求 (S442)
S440
(句柄、新句柄)
去激活权限
S443
REK查询响应 (S444)
(状态、散列(随机, REK))
SEK准备响应 (S451)
TEK解密请求 (S461)
(CID、AES-加密(SEK)(TEK))
SRM Ping请求 (S462)
S463
(句柄, 随机)
S460
检查权限的存在
SRM Ping响应 (S464)
(状态、散列(随机, REK))
检查权限的存在
并且解密TEK
S465
TEK描述响应 (S466)
(TEK)
SRM Ping请求 (S471)
(句柄, 随机)
S470
SRM Ping响应 (S472)
(状态, 散列(随机, REK))
权限启用请求 (S491)
(句柄, 状态信息)
S490
激活权限
S492
权限启用响应 (S492)
(状态)
删除REK和权限信息
S494
SEK完成响应
(S495)

图 8

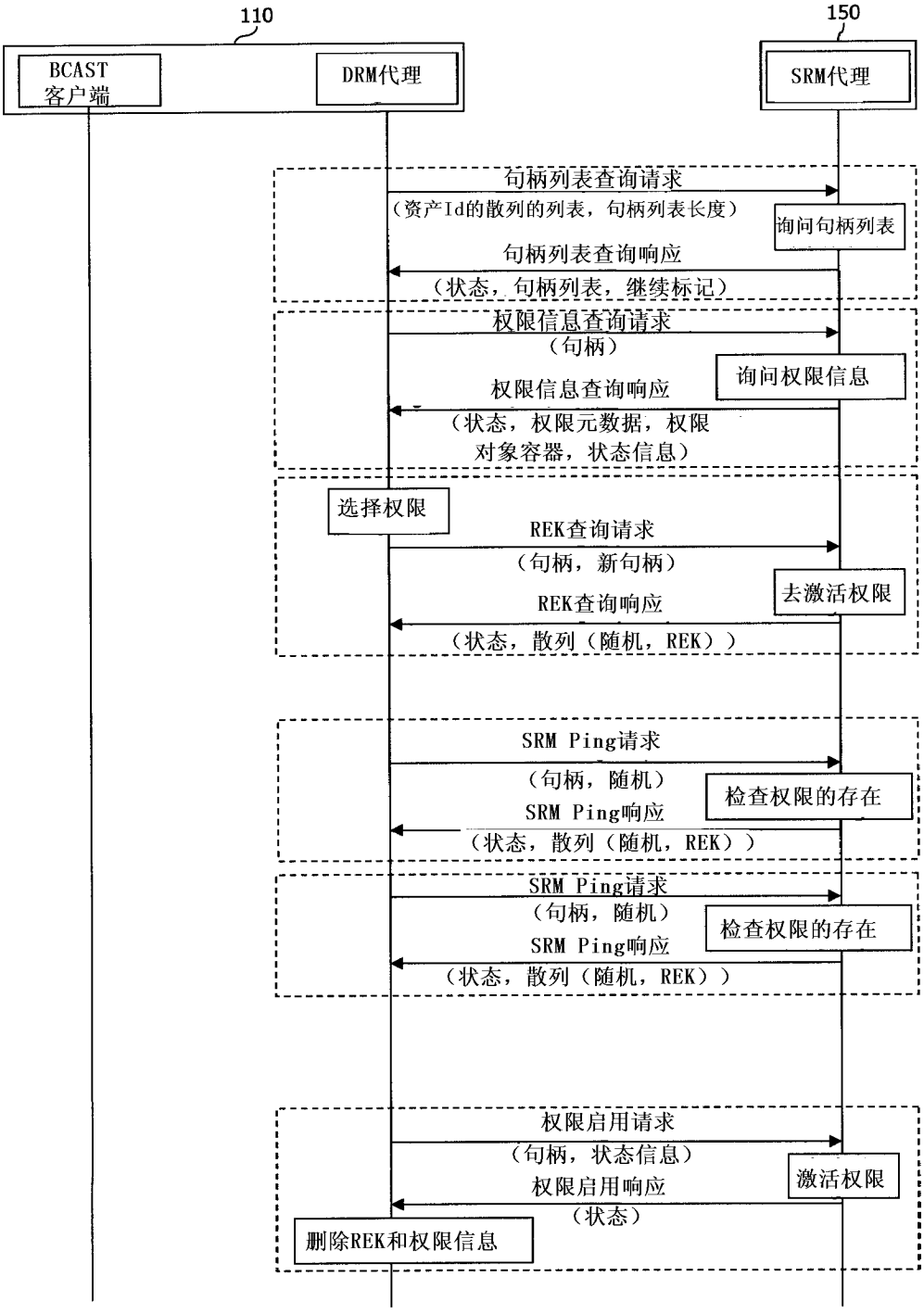

110
150
BCAST
客户端
DRM代理
SRM代理
句柄列表查询请求
（资产Id的散列的列表，句柄列表长度）
询问句柄列表
句柄列表查询响应
（状态，句柄列表，继续标记）
权限信息查询请求
（句柄）
询问权限信息
权限信息查询响应
（状态，权限元数据，权限
对象容器，状态信息）
选择权限
REK查询请求
（句柄，新句柄）
去激活权限
REK查询响应
（状态，散列（随机，REK））
SRM Ping请求
（句柄，随机）
检查权限的存在
SRM Ping响应
（状态，散列（随机，REK））
SRM Ping请求
（句柄，随机）
检查权限的存在
SRM Ping响应
（状态，散列（随机，REK））
权限启用请求
（句柄，状态信息）
激活权限
权限启用响应
（状态）
删除REK和权限信息

图 9

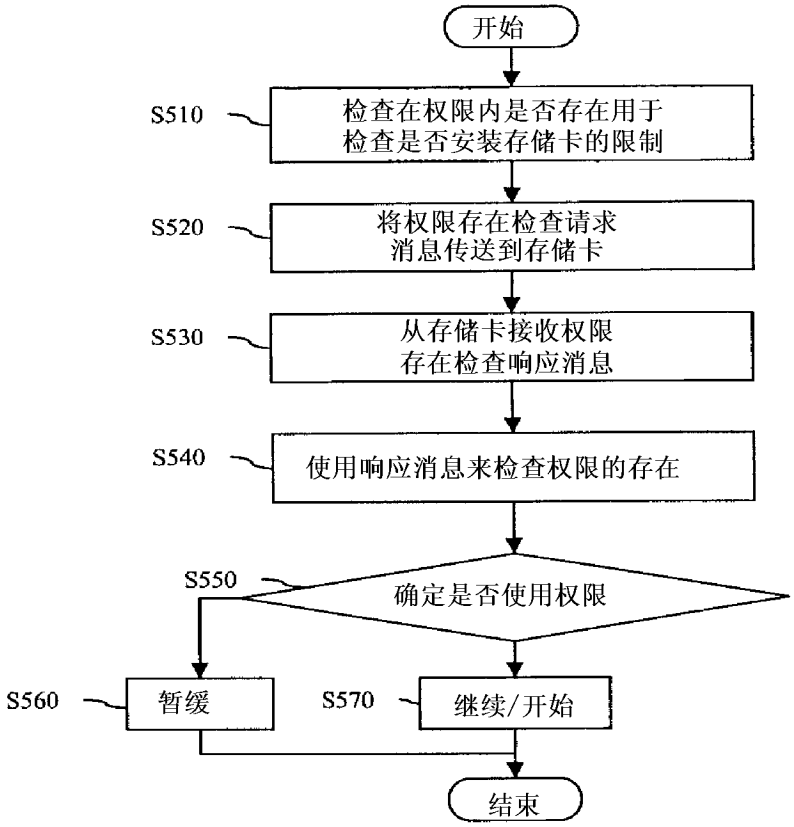

开始
S510
检查在权限内是否存在用于
检查是否安装存储卡的限制
S520
将权限存在检查请求
消息传送到存储卡
S530
从存储卡接收权限
存在检查响应消息
S540
使用响应消息来检查权限的存在
S550
确定是否使用权限
S560
暂缓
S570
继续/开始
结束

图 10

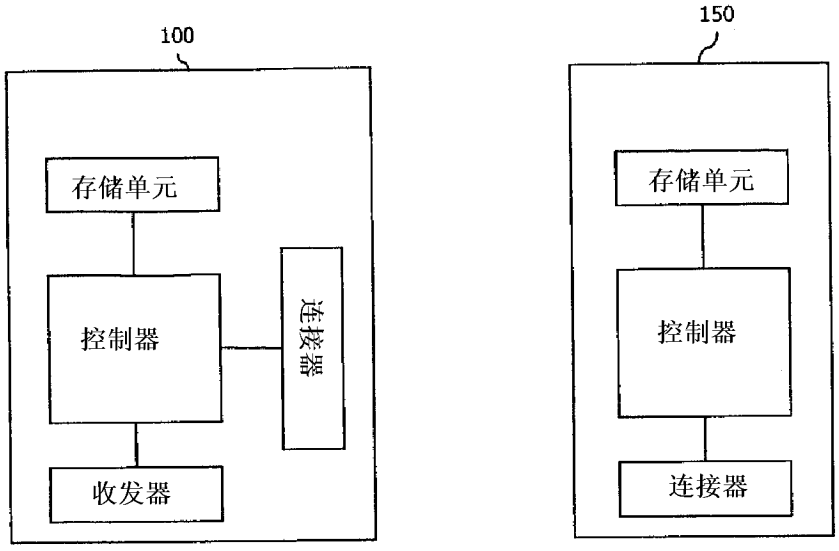

100
存储单元
控制器
连接器
收发器
150
存储单元
控制器
连接器

图 11