[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)
G06Q 20/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 03800349.X

[45] 授权公告日 2007 年 1 月 31 日

[11] 授权公告号 CN 1297911C

[22] 申请日 2003.3.28 [21] 申请号 03800349.X

[30] 优先权

[32] 2002.3.29 [33] JP [31] 097846/2002

[86] 国际申请 PCT/JP2003/003930 2003.3.28

[87] 国际公布 WO2003/083746 日 2003.10.9

[85] 进入国家阶段日期 2003.11.28

[73] 专利权人 松下电器产业株式会社

地址 日本大阪府

[72] 发明人 高桥荣治 古山纯子 峰村淳 杉浦雅贵

[56] 参考文献

JP2002-73421A 2002.3.12 G06F12/14

JP2000-324098A 2000.11.24 H04L9/32

CN1250286A 2000.4.12 H04L9/14

JP2000-83233A 2000.3.21 H04N7/16

WO01/16821A2 2001.3.8 G06F17/60

JP2002-9763A 2002.1.11 H04L9/32

WO01/43342A1 2001.6.14 H04L9/32

审查员 高琛颢

[74] 专利代理机构 北京市柳沈律师事务所

代理人 邸万奎 黄小临

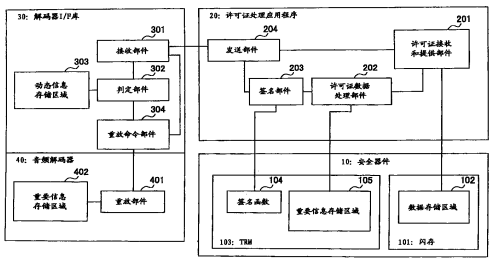
权利要求书 1 页 说明书 25 页 附图 19 页

[54] 发明名称

内容重放设备和内容重放控制方法

[57] 摘要

一种能在通用终端中使用和控制具有可扩展性的安全内容的内容重放设备。在该设备中，在许可证处理应用程序(20)，许可证数据处理部件(202)更新许可证数据、创建使用授权信息、和经由许可证接收/发送部件(201)将已更新的许可证存入数据存储区域(102)。签名部件(203)在使用授权信息上进行通过使用安全器件(10)的签名函数(104)所创建的签名，从而创建使用授权证明。发送部件(204)将加密的内容解密密钥连同使用授权证明发送到解码器 I/F 库(30)的接收部件(301)。在解码器 I/F 库(30)，判定部件(302)通过利用使用授权信息中包含的动态信息来判定签名的真实性和使用授权信息的真实性。



1. 一种内容重放设备，包括:

获取部件，用于获取其中描述了内容使用条件的许可证数据;

创建部件，用于在符合使用条件的情况下基于许可证数据创建包含重放命令的使用授权信息;

判定部件，用于判定使用授权信息的真实性；和

重放部件，用于在所述判定部件证明使用授权信息是真的情况下，根据重放命令重放内容，

其中，所述使用授权信息包含每次创建使用授权信息时的值不同的动态性信息。

2. 根据权利要求 1 的内容重放设备，其中所述创建部件创建还包括用于执行符合使用条件的重放控制的控制信息的使用授权信息，并且所述重放部件根据重放命令和控制信息来重放该内容。

3. 根据权利要求 2 的内容重放设备，其中所述创建部件将用于指示将要通知的内容重放结果或进程的通知命令作为控制信息合并入使用授权信息，并且所述设备还包括通知部件，用于根据通知命令通知内容重放的结果或进程。

4. 根据权利要求 3 的内容重放设备，还包括更新部件，用于根据来自所述通知部件的通知更新许可证数据。

5. 一种内容重放控制方法，包括:

获取步骤，获取描述内容使用条件的许可证数据;

创建步骤，在符合使用条件的情况下，基于许可证数据创建包含重放命令的使用授权信息;

判定步骤，判定使用授权信息的真实性；和

重放步骤，在所述判定步骤中证明使用授权信息是真的情况下，根据重放命令重放内容，

其中，所述使用授权信息包含每次创建使用授权信息时的值不同的动态性信息。

内容重放设备和内容重放控制方法

技术领域

本发明涉及内容重放设备和内容重放控制方法。

背景技术

近来，随着因特网的普遍使用，诸如通过因特网向 PC 用户销售内容或许可证、或通过移动电话网络向移动电话用户销售内容或许可证的新商业模式正在市场中出现，并且这些新商业模式显示了将来其数目进一步增长的趋势。所分发的内容在 PC、移动电话、或专用重放终端等上重放。

内容意指以电子形式形成的字符、音频、视频、图等的数据、或游戏或软件、及其组合等。内容重放意指例如在显示器上展示字符或可视图像、或从扬声器输出声音。

许可证意指为了保护内容的版权而给予内容重放、分发或存储的授权的信息，并且该信息可包括使用条件和内容解密密钥。使用条件意指控制内容重放的信息，例如限制内容重放次数的信息、或限制内容重放周期的信息、或限制其重放累积时间的信息。内容解密密钥意指在内容以加密形式分发和存储的情况下，用来解密加密内容的密钥。

根据任一传统内容分发系统，由服务器将加密内容和包含以对用户唯一的密钥加密的内容解密密钥的许可证分发到终端，并将所分发的内容和许可证存储在该终端的存储介质中。另外，终端具有传统执行的处理，用于认证内容的许可证、更新许可证、以及解密内容解密密钥以解码和重放该内容。而且，为了达到许可证的认证及更新等中内容的安全使用控制，传统上给终端提供安全 LSI 或抗篡改模块等。而且，在许多传统情况下，为每一内容分发系统专门提供用于内容重放的终端。

顺便说一句，现在，日益需要对于由诸如移动电话和其它手持小型装置(handset)(PDA)等通用手持终端提供的内容使用的安全和可扩充控制。

在内容重放时，由执行内容的许可证相关处理的应用程序(许可证处理应用程序)进行许可证认证和更新。然后，将内容数据发送到解码器，在那里解

密该内容。例如，假设该内容数据是AAC-格式音乐数据，则使用AAC解码器解密该内容数据，并从与解码器相连的扬声器输出所解密的声音。

这里，有一种方法，其中在解码器外进行内容的解密和许可证的认证，并将纯文本格式的内容数据提供给解码器以供重放。然而，在这样的方法中，在将纯文本内容数据提供给解码器时可能发生窃听。所以，为了防止窃听的发生，另一种方法在解码器外执行许可证认证，并向解码器提供加密内容数据和纯文本格式的内容解密密钥，以在解码器内进行内容解密和重放。但是，即使在这样的方法中，在将纯文本内容解密密钥提供给解码器时仍可能发生窃听。所以，为了防止窃听的发生，另一种方法在解码器外执行许可证认证，并向解码器提供加密内容数据和用解码器的公开密钥加密的内容解密密钥，其中用解码器内持有的解码器的私密密钥来解密所加密的内容解密密钥，并用所解密的内容解密密钥来解密加密内容数据以在这里重放。然而，即使在这样的方法中，当在将用解码器的公开密钥加密的内容解密密钥提供给解码器时用解码器的公开密钥加密的内容解密密钥被窃听，且随后窃听的密钥被重新使用时，有可能发生对许可证处理应用程序的所谓冒名的行为。另外，还有一种方法，其中将加密的内容数据和许可证提供给解码器，并在解码器内进行许可证的认证和内容的解密。然而，在普通情况下，许可证依赖于内容分发/重放服务，另外，与大多数情况下的软件不同，配置为硬件的解码器不能提供其处理内容的可重写性；这意味着为了在解码器内进行许可证认证，解码器自身必须依赖于内容分发/重放服务，其结果是，用户需要多于一个终端，每一个专门为特定内容分发/重放服务而提供。

而且，在作为使用条件描述了允许重放总时间时，一旦已达到总时间，则必须自动停止内容重放。出于这个目的，必须测量重放花费的实际时间长度，并通过重写使用条件来更新许可证，即必须从作为使用条件描述的允许重放总时间长度中减去重放花费的实际时间长度。而且，在作为使用条件描述了允许重放次数，此外，描述了视为执行一次重放的重放时间长度的情况下，仅当重放被执行视为执行一次重放的重放时间长度时，才必须通过重写使用条件来更新许可证，即必须将描述为使用条件的重放次数递减1。

为了达到这些，一些方法在解码器内执行重放时间测量和许可证更新。然而，在一般情况下，许可证依赖于内容分发/重放服务，另外，与大多数情况下的软件不同，配置为硬件的解码器不能提供其处理内容的可重写性；这

意味着为了在解码器内实现许可证更新，解码器自身必须依赖于内容分发/重放服务，其结果是，用户需要多于一个终端，每一个专门为特定内容分发/重放服务而提供。

可替换地，存在其它一些方法，其中在解码器外执行重放时间测量和许可证更新。然而，很难在解码器外精确测量内容重放时间。内容重放时间意指内容已重放的实际时间长度；这里，由于实际开始重放前所花费的归因于解码器的内容数据装载时间的时间间隔或其它时间间隔，所以仅测量从用户按下“重放按钮”的时间点到用户按下“停止按钮”的时间点之间的时间长度，不能提供任何正确测量值，而且由于不能保证数据大小与实际重放时间成比例，所以仅测量发送到解码器的内容数据的数据大小也不能提供任何正确测量值；因此，很难在解码器外精确测量重放时间。

发明内容

本发明的目的在于提供一种内容重放设备和一种内容重放控制方法，利用所述设备和方法，可在通用终端中实现安全、可扩展的内容使用控制。

根据本发明的一个方面，一种内容重放设备包括：获取部件，用于获取其中描述了内容使用条件的许可证数据；创建部件，用于在符合使用条件的情况下基于许可证数据创建包含重放命令的使用授权信息；判定部件，用于判定使用授权信息的真实性；和重放部件，用于在判定部件证明使用授权信息是真的情况下，根据重放命令重放内容。其中，所述使用授权信息包含每次创建使用授权信息时的值不同的动态性信息。

一种内容重放控制方法包括：获取步骤，获取描述内容使用条件的许可证数据；创建步骤，在符合使用条件的情况下，基于许可证数据创建包含重放命令的使用授权信息；判定步骤，判定使用授权信息的真实性；重放步骤，在判定步骤证明使用授权信息是真的情况下，根据重放命令重放内容。其中，所述使用授权信息包含每次创建使用授权信息时的值不同的动态性信息。

附图说明

图 1 是示出了根据本发明实施例 1 的内容重放设备的配置的方框图；

图 2 是示出了根据本发明实施例 1 的内容重放设备的处理过程的示意图；

图 3 是示出了根据本发明实施例 1 的许可证数据的配置的示意图；

图 4 是示出了根据本发明实施例 1 的使用授权证明的配置的示意图；

图 5 是示出了根据本发明实施例 1 的许可证数据的内容的示意图；

图 6 是示出了根据本发明实施例 1 的使用授权信息的内容的示意图；

图 7 是示出了根据本发明实施例 1 的许可证数据的内容的示意图；

图 8 是示出了根据本发明实施例 1 的使用授权信息的内容的示意图；

图 9 是示出了根据本发明实施例 2 的内容重放设备的配置的方框图；

图 10 是示出了根据本发明实施例 2 的内容重放设备的处理过程的示意图；

图 11 是示出了根据本发明实施例 2 的使用授权信息的内容的示意图；

图 12 是示出了根据本发明实施例 2 的许可证数据的内容的示意图；

图 13 是示出了根据本发明实施例 2 的使用授权信息的内容的示意图；

图 14 是示出了根据本发明实施例 2 的使用授权信息的内容的示意图；

图 15 是示出了根据本发明实施例 2 的许可证数据的内容的示意图；

图 16 是示出了根据本发明实施例 2 的使用授权信息的内容的示意图；

图 17 是示出了根据本发明实施例 3 的内容的数据结构的示意图；

图 18 是示出了根据本发明实施例 3 的指纹的数据结构的示意图；

图 19 是示出了根据本发明实施例 3 的内容获取处理过程的示意图；

图 20 是示出了根据本发明实施例 4 的许可证购买处理过程的示意图；

图 21 是示出了根据本发明实施例 4 的内容重放处理过程的示意图；

图 22 是示出了根据本发明实施例 5 的许可证购买处理过程的示意图；

图 23 是示出了根据本发明实施例 5 的内容重放处理过程的示意图；

图 24 是示出了根据本发明实施例 5 的许可证购买处理过程的示意图；

图 25 是示出了根据本发明实施例 5 的内容重放处理过程的示意图；

图 26 是示出了根据本发明实施例 6 的许可证购买处理过程的示意图；

图 27 是示出了根据本发明实施例 6 的内容重放处理过程的示意图；

图 28 是示出了根据本发明实施例 7 的许可证上载处理过程的示意图；和

图 29 是示出了根据本发明实施例 7 的许可证上载处理过程的示意图。

具体实施方式

在本发明的内容重放设备和内容重放控制方法中，结合使用了具有抗篡改模块(TRM)的安全器件、许可证处理应用程序和解码器。具体说来，许可证处理应用程序执行与安全器件的交互认证，然后创建附有安全器件的签名

的使用授权信息。在下面说明中，将附有安全器件的签名的使用授权信息称为使用授权证明。解码器 I/F 库判定使用授权信息和签名的真实性。这防止了对许可证处理应用程序的所谓冒名行为。

另外，仅在既接收了内容解密密钥又接收了正当使用授权信息的情况下，解码器才重放内容。例如，假设是音频解码器，则其与扬声器相连。仅内容重放设备中的一个解码器能接受发布到解码器自身的重放命令，或接受内容数据的传输以便重放。使用授权信息设计为包含诸如时间和日期的每次与其它不同的数据，并且该数据存储在解码器或解码器 I/F 库中。

另外，使用授权信息包含诸如“当实际已执行重放时通知实际重放时间”的信息和关于重放次数及重放时间的信息。然后，解码器 I/F 库将重放时间通知给许可证处理应用程序，并向解码器发布重放停止命令。许可证处理应用程序一旦接收到来自解码器 I/F 库的通知或命令，就执行许可证数据的更新。这确保了内容重放的正确控制。

下面将参考附图详细说明本发明的实施例。

(实施例 1)

图 1 是示出了根据本发明实施例 1 的内容重放设备的配置的方框图。许可证处理应用程序 20 存储在内容重放设备中预安装的存储器中。许可证处理应用程序 20 作为例如 Java 库增强而执行。另外，内容重放设备包括解码器 I/F 库 30 和音频解码器 40。将解码器 I/F 库 30 和音频解码器 40 配置为硬件。而且，将作为可卸式存储介质的安全器件 10 插入内容重放设备。

在安全器件 10 中，闪存 101 包括数据存储区域 102，其中存储了从内容服务器获取的内容和该内容的许可证。另外，TRM 103 包括诸如由 WAP 论坛定义的 WIM 函数的签名函数 104 和重要信息存储区域 105。诸如指纹等的重要信息存储在重要信息存储区域 105。

在许可证处理应用程序 20 中，许可证接收和提供部件 201 从安全器件 10 接收加密的内容解密密钥和许可证数据，并将加密的内容解密密钥和许可证数据提供给许可证处理应用程序 20。许可证数据处理部件 202 执行指纹的认证、许可证数据的更新、使用授权信息的创建、重要信息存储区域 105 中指纹的登记、以及在许可证接收和提供部件 201 的中间媒介作用下将已更新的许可证存储在数据存储区域 102 中。签名部件 203 从许可证数据处理部件 202 接收使用授权信息以创建摘要(digest)，并通过将使用安全器件 10 的签名

函数 104 所得到的签名附于使用授权信息上来创建使用授权证明。发送部件 204 分别从许可证接收和提供部件 201 接收加密的内容解密密钥，从签名部件 203 接收使用授权证明，并将使用授权证明附于加密的内容解密密钥上，以将加密的内容解密密钥和附于其上的证明发送到解码器 I/F 库 30 中的接收部件 301。

在解码器 I/F 库 30 中，接收部件 301 接收从许可证处理应用程序 20 中的发送部件 204 发送的内容解密密钥和使用授权证明，然后将加密的内容解密密钥传输到重放命令部件 304，将使用授权证明传输到判定部件 302。判定部件 302 从接收部件 301 接收使用授权证明，并通过使用使用授权信息中包含的动态信息来判定签名的真实性和使用授权信息的真实性。判定之后，判定部件 302 将动态信息存入动态信息存储区域 303，同时部件 302 将使用授权信息中包含的重放命令发送到重放命令部件 304。将先前的动态信息存入动态信息存储区域 303。重放命令部件 304 将重放命令和加密的内容解密密钥发送到音频解码器 40。

在音频解码器 40 中，重放部件 401 通过使用在重要信息存储区域 402 中存储的解码器私密密钥来解密加密的内容解密密钥，然后根据重放命令解密和重放内容。

接下来，参考图 2 描述根据本实施例的内容重放设备中的处理过程。

将用内容解密密钥适当加密的内容存入安全器件中的闪存中。内容解密密钥自身利用解码器公开密钥而被加密，并与许可证数据一起被存入闪存。许可证数据是描述诸如允许内容重放次数、允许内容重放时间长度等的内容使用条件的数据。许可证由加密的内容解密密钥和许可证数据组成。下面描述许可证数据的配置。

由许可证处理应用程序执行的处理过程如下：(1)首先，从闪存中读取许可证，并获取许可证。(2)接下来，对许可证数据执行指纹认证。(3)然后，执行许可证认证和许可证数据更新。下面将具体描述如何更新。(4)然后，在符合许可证数据指示的使用条件的情况下，基于许可证数据创建使用授权信息。在解码器 I/F 库判定该使用授权信息的真实性。该使用授权信息包含重放命令。下面将具体描述如何创建使用授权信息。(5)接下来，基于已更新的许可证数据创建指纹，并在安全器件中的 TRM 中登记所创建的指纹。(6)接下来，将包含已更新的许可证数据的许可证存入安全器件中的闪存中。(7)然后，利

用安全器件的签名函数，将签名附于使用授权信息。在附加签名之后，使用授权信息变为使用授权证明。利用安全器件私密密钥实现安全器件的签名函数。仅允许已与安全器件交互认证的正确许可证处理应用程序来将签名附于使用授权信息。(8)然后，将从许可证中取出的附有使用授权证明的内容解密密钥被发送到解码器 I/F 库。由许可证处理应用程序进行上述处理过程。这里，可在(7)或(8)的处理之后、或下述(9)的处理之后立即执行(6)的处理。

(9)接下来，在解码器 I/F 库，判定附于内容解密密钥的使用授权证明的真实性。也就是说，判定签名的真实性和使用授权信息的真实性，以进一步判定是否允许使用该内容。然后，在判定签名可信且使用授权信息正当的情况下，授权重放该内容。通过使用安全器件证明来判定签名的真实性。安全器件证明在上述处理(8)中与内容解密密钥和使用授权证明一起获取。可替换地，可与这里的步骤分离地预先获取安全器件证明。基于使用授权信息中包含的动态信息而判定使用授权信息的真实性。(10)然后，在音频解码器，仅在解码器 I/F 库核实了其真实性的情况下，根据重放命令重放该内容。也就是说，在音频解码器，在用解码器私密密钥解密内容解密密钥之后，通过用内容解密密钥正确解密该内容，来重放该内容。

接下来，参考图 3 说明许可证数据的配置。如图 3 所示，许可证数据连同用解码器公开密钥加密的内容解密密钥组成许可证。许可证数据由许可证 ID、内容 ID、内容相关信息、和使用规则(Usage Rule)组成。使用规则由静态特性(Static Property)和可变特性(Variable Property)组成。

在内容是音乐的情况下，内容相关信息包含音乐标题名和艺术家名。

使用规则描述内容使用条件，静态特性包括不由许可证处理应用程序更新的信息，例如内容重放的时间限制等，而可变特性包括在每次内容重放时都要更新的信息，例如允许重放次数、允许重放时间长度等。

接下来，参考图 4 说明使用授权证明的配置。如上所述，使用授权证明是附加了由安全器件制作的签名的使用授权信息。换言之，使用授权证明证明已在许可证处理应用程序中核实了许可证。

使用授权信息由动态信息、诸如重放命令的命令、和重放控制信息组成。在符合许可证数据所指示的使用条件的情况下，主要基于许可证数据的使用规则来创建使用授权信息。

动态信息是在每次创建使用授权信息时，具有不同于其它值的值的信息。

例如，其是指示创建使用授权信息的时间和日期、随机号、序列号等的信息。通过比较先前动态信息与当前动态信息，解码器 I/F 库判定使用授权信息的真实性，以进一步判定是否允许使用该内容。具体说，如下所述进行判定。

在动态信息是时间和日期信息或随机号的情况下，存储到此为止的所有动态信息。然后，在包含与先前任一动态信息相同的当前动态信息的任意使用授权信息被再次输入到解码器 I/F 库时，便发生许可证处理应用程序的所谓冒名行为，并且否认该使用授权信息的真实性，从而不重放该内容。相反地，在包含与先前任意动态信息不同的当前动态信息的任意使用授权信息被输入到解码器 I/F 库时，便肯定该使用授权信息的真实性以重放该内容。

在动态信息采用序列号形式的情况下，存储上一个动态信息(序列号 n)。然后，仅在当前输入到解码器 I/F 库的使用授权信息中包含的当前动态信息是“n+1”的情况下，才肯定使用授权信息的真实性以重放该内容。另外，上一个动态信息和当前动态信息之间的关系规则可为减“-1”或乘“×2”；在这样的情况下，仅在使用授权信息具有符合这些规则中所安排的规则的当前动态信息，且输入这些信息的情况下，才肯定某一使用授权信息的真实性。可替换地，在规定当前动态信息必须小于/大于先前动态信息的规则的情况下，仅在当前动态信息小于/大于先前动态信息时，才肯定使用授权信息的真实性。

规定当前动态信息必须大于任一先前动态信息的规则也可能应用于时间和日期信息。例如，假设根据使用授权信息的最早创建日期为 2002 年 3 月 4 日，根据另一使用授权信息的第二早创建日期为 2002 年 3 月 7 日，且根据另一使用授权信息的第三早创建日期为 2002 年 3 月 9 日。在将包含这些时间和日期信息的使用授权信息按最早→第二早→第三早的顺序输入到解码器 I/F 库中的情况下，这些时间和日期信息的比较显示了较晚输入的信息具有较大值，因此在该情况下，肯定最早、第二早、和第三早输入的每一个的使用授权信息的真实性，并从而重放该内容。相反，在具有第二早时间和日期信息的使用授权信息比具有第三早时间和日期信息的另一使用授权信息晚输入解码器 I/F 库中的情况下，这些时间和日期信息的比较显示第二早时间和日期信息具有比第三早时间和日期信息较小的值，这导致具有第二早时间和日期信息的使用授权信息的真实性被否认，并从而不重放该内容。

以这种方式，通过将在每次创建使用授权信息时具有不同于其它值的值的动态信息合并入使用授权信息，有可能防止内容解密密钥的未授权使用，

即许可证处理应用程序的所谓冒名行为。

接下来，解释如何设置使用授权信息命令和重放控制信息。

首先，如图 5 所示，解释使用规则的静态特性为 “Null(空)”，而使用规则的可变特性为 “Count(允许的重放次数)” 的情况。在这种情况下，根据重放次数进行重放控制。也就是说，在许可证数据更新处理中，当 “Count≥1” 时，Count 递减 1(Count-1)，从而更新许可证数据。另外，在 “Count≥1”的情况下，其与使用条件不冲突，所以创建如图 6 所示的使用授权信息。换言之，创建具有命令 “REPLAY(重放)” 和重放控制信息 “NULL” 的使用授权信息。由许可证处理应用程序进行许可证的认证和更新以及使用授权信息的创建。根据使用授权信息中包含的重放命令，将该内容重放仅一次。因此，有可能使该内容重放不多于原始 “Count” 中所述的次数。相反，在 “Count = 0”的情况下，其不符合使用条件，所以不创建使用授权信息。因此，在 “Count = 0”的情况下，不重放该内容。

接下来，如图 7 所示，解释使用规则的静态特性为 “Limit(重放时间限制)”，而使用规则的可变特性为 “NULL” 的情况。在这种情况下，根据重放周期进行重放控制。换言之，在创建使用授权信息的时间和日期在 “Limit” 之前的情况下，重放与使用条件不冲突，所以创建如图 8 所示的具有命令 “REPLAY” 和重放控制信息 “NULL” 的使用授权信息。由许可证处理应用程序进行许可证的认证和更新以及使用授权信息的创建。根据使用授权信息中包含的重放命令，将该内容重放仅一次。因此，有可能使该内容重放直到 “Limit” 中所述的时间点。相反，在创建使用授权信息的时间和日期不在 “Limit” 之前的情况下，重放与使用条件冲突，所以不创建使用授权信息。因此，在创建使用授权信息的时间和日期不在 “Limit” 之前的情况下，不重放该内容。

这里，关于 “Limit(重放时间限制)” 的设置，可以想到下列三种模式；即(1)从内容服务器售出描述重放时间限制的许可证。(2)从内容服务器售出描述允许重放周期的许可证，其中在将许可证存入其闪存中时，终端根据允许重放周期设置重放时间限制。例如，在从内容服务器向终端发送的许可证数据中描述允许重放周期(例如 2 星期)的情况下，在将许可证存入其闪存中时，在终端侧设置 “Limit(重放时间限制)” 为 “存储许可证数据的时间和日期 + 许可证数据中所述的允许重放周期” 的时间点。(3)从内容服务器售出描述允

许重放周期的许可证，其中在内容的初次重放时，终端根据允许重放周期设置重放时间限制。例如，在从内容服务器向终端发送的许可证数据中描述允许重放周期(例如 2 星期)的情况下，在内容初次重放时，在终端侧设置“Limit(重放时间限制)”为“初次重放的时间和日期+许可证数据中所述的允许重放周期”的时间点。

这里，多个许可证处理应用程序可驻留在内容重放设备中。例如，多个许可证处理应用程序可驻留在单个相同内容重放设备中，每个许可证处理应用程序彼此不同，且专门为特定的内容分发/重放服务而提供。

另外，可在解码器 I/F 库而不是解码器中提供用于存储解码器私密密钥的重要信息存储区域，在这种情况下，在解码器 I/F 库中执行内容解密。

另外，在许可证数据的数据尺寸小的情况下，许可证数据可被存储在安全器件的 TRM 中，而不是安全器件的闪存中。

而且，尽管许可证数据中的使用规则的可变特性是经历更新的信息，仍可将其分为两部分，即不经历更新的缺省值部分和经历更新的当前值部分，在这种情况下，仅更新了当前值部分。

而且，解码器和解码器 I/F 库也支持不存在对应许可证的纯文本内容，即不受版权保护的普通内容。在将纯文本内容数据提供给解码器 I/F 库的情况下，即使在没有附加使用授权信息时，仍有可能重放内容数据。

而且，在内容和许可证的格式从内容重放设备获取时的最初格式转换时，可将该内容和许可证存入闪存。更具体的说，内容保护格式和许可证保护格式可从分发时的格式转换为用于 java 库增强或安全器件应用程序的指定格式。

而且，尽管在每次内容重放时，许可证的可变特性经历更新，但动态信息可保持在许可证之外，而不是许可证的可变特性之内，其中当保持许可证和外面的动态信息之间的链接时，许可证自身不经历更新。

而且，在内容重放时，为了仅在内容重放处理设备重放该内容的情况下对许可证执行实际处理，可在对许可证执行处理之前检查内容类型。这使得有可能防止在不能重放任何内容时许可证被消耗。

以这种方式，根据本实施例，仅在肯定使用授权信息的真实性的情况下，授权内容重放，其中基于描述内容使用条件的许可证数据创建使用授权信息，有可能防止对内容数据的窃听或许可证处理应用程序的所谓冒名行为，从而

进一步防止对内容的未授权使用。另外，由于使用在每次创建使用授权信息时具有不同于其它值的值的动态信息来判定使用授权信息的真实性，所以有可能正确判定使用授权信息的真实性，并有可能防止已创建一次的使用授权信息的未授权重新使用，这进一步使得正确判定是否允许使用该内容成为可能。而且，由于安全器件的签名被附于使用授权信息，所以有可能防止使用授权信息被篡改。

(实施例 2)

根据本实施例的内容重放设备将用于执行精确重放控制的重放控制信息合并入使用授权信息，而不损失其通用性。另外，许可证处理应用程序将用于通知内容重放的结果或进程的通知命令合并入使用授权信息作为控制信息，并且解码器 I/F 库根据通知命令将内容重放的结果或进程通知给许可证处理应用程序。另外，许可证处理应用程序根据内容重放的结果或进程的通知更新许可证数据。

图 9 是示出了根据本发明实施例 2 的内容重放设备的配置的方框图。将图 9 中与实施例 1(图 1)中相同的部件分配相同的附图标记，并省略对其的进一步说明。

在许可证处理应用程序 20 中，许可证数据处理部件 205 执行指纹的认证和使用授权信息的创建。在从解码器 I/F 库 30 接收通知之后，部件 205 进一步执行许可证数据的更新、重要信息存储区域 105 中指纹的登记、和在许可证接收和提供部件 201 的中间媒介作用下将已更新的许可证存入数据存储区域 102。也就是说，在创建使用授权信息之后，部件 205 备用直至从解码器 I/F 库 30 接收通知。如上所述，该实施例和实施例 1 的区别在于：在该实施例中，许可证数据处理部件 205 根据来自解码器 I/F 库 30 的通知来更新许可证数据。

在解码器 I/F 库 30 中，重放控制部件 305 根据从判定部件 302 发送的重放控制信息，而将重放命令和加密的内容解密密钥发送到音频解码器 40。另外，部件 305 基于重放控制信息执行内容重放控制(测量重放持续时间、计数重放次数、停止重放等)，并随后创建用于通知按重放控制信息命令的重放结果或进程的数据(指示重放实际持续时间、实际重放次数、重放完成等的数据)，以将所创建的数据发送到通知部件 306。通知部件 306 将重放控制部件 305 所创建的数据通知给许可证处理应用程序 20 中的许可证数据处理部件 205。

在音频解码器 40 中，重放部件 403 通过使用在重要信息存储区域 402 中存储的解码器私密密钥来解密加密的内容解密密钥，然后根据重放命令解密和重放该内容。另外，根据来自重放控制部件 305 的重放停止命令而停止内容重放。

接下来，将参考图 10 说明根据该实施例的内容重放设备的处理过程。

(1)首先，从闪存中读出许可证，并在许可证处理应用程序中获取许可证。(2)接下来，对许可证数据执行指纹认证。(3)然后，执行许可证认证，并在符合许可证数据所指示的使用条件的情况下，基于许可证数据创建使用授权信息。使用授权信息包括用于依据内容使用条件执行重放控制的重放控制信息。另外，使用授权信息包括用于通知内容重放的结果或进程的通知命令。(4)然后，利用安全器件的签名函数，签名被附于使用授权信息。在附加签名之后，使用授权信息变为使用授权证明。(5)然后，将从许可证中取出的附有使用授权证明的内容解密密钥发送到解码器 I/F 库。(6)接下来，在解码器 I/F 库，判定附于内容解密密钥的使用授权证明的真实性。也就是说，判定签名的真实性和使用授权信息的真实性，以进一步判定是否允许使用该内容。然后，在判定签名可信且使用授权信息正当的情况下，授权重放该内容。(7)然后，在授权内容重放的情况下，根据使用授权信息中包含的重放控制信息执行诸如重放次数控制、重放持续时间控制、重放质量控制等的重放控制。(8)然后，在音频解码器，仅在解码器 I/F 库核实了其真实性的情况下，根据重放命令重放该内容。也就是说，在音频解码器，在用解码器私密密钥解密内容解密密钥自身之后，通过用内容解密密钥正确解密该内容，来重放该内容。此时根据来自解码器 I/F 库的重放控制而执行内容重放。(9)接下来，解码器 I/F 库根据使用授权信息中包含的通知命令将内容重放的结果或进程通知给许可证处理应用程序。(10)一旦接收了重放的结果或进程的通知，许可证处理应用程序根据这一通知更新许可证数据。(11)接下来，基于所更新的许可证数据而创建指纹，并在安全器件的 TRM 中登记所创建的指纹。(12)接下来，将包含已更新的许可证数据的许可证存入安全器件的闪存中。可替换地，可在(3)的处理之后将许可证暂时存入安全器件的闪存中，并在(11)的处理之前再次从安全器件的闪存中读出。

可替换地，解码器 I/F 库可在非易失性存储器中存储重放控制信息和内容重放的结果或进程，然后在将重放的结果或进程通知给许可证处理应用程

序之后，可擦除所存储的信息。在启动内容重放设备时，任意重放控制信息、或重放的结果或进程不被擦除而保持在解码器 I/F 库的非易失性存储器中的情况下，其表示在进行许可证数据的更新之前，该处理已在不期望的反常状态终止。在这种情况下，处理可在以上(9)重新开始。以这种方式，即使在许可证更新之前，由于例如电源切断等，异常中断该处理的情况下，仍有可能保持重放的结果或进程的信息，这使得正确更新许可证进一步成为可能。

接下来，解释如何设置使用授权信息命令和重放控制信息。

首先，如图 5 所示，解释使用规则的静态特性为 “Null”，而使用规则的可变特性为 “Count(允许的重放次数)”，并且用户命令连续重放的情况。在这种情况下，根据重放次数进行重放控制。换言之，当 “Count≥1”时，重放与使用条件不冲突，所以创建图 11 所示的具有命令 “REPLAY” 和重放控制信息 “执行重放比 Count 所述次数少的多次，并且一旦完成重放，就通知实际重放次数” 的使用授权信息。根据该使用授权信息中包含的重放命令和重放控制信息，该内容被重放多次 “C_play”(限制：该数值小于 Count)。在重放该内容多次之后，将重放结果，特别是重放次数 “C_play”从解码器 I/F 库通知给许可证处理应用程序。一旦接收了重放结果的这一通知，许可证处理应用程序通过将图 5 所示许可证数据的 “Count”(允许重放的次数)减少 “C_play” 来更新许可证数据。以这种方式，有可能执行多次连续重放。

可替换地，作为另一种控制重放次数的方法，可创建由用户命令的授权重放少于期望次数的重放命令，此后可重复使用授权信息的创建和许可证数据的更新，直至实际重放次数达到用户命令的期望次数。

具体说，例如，在使用规则的静态特性为 “Null”，而使用规则的可变特性为 “Count(允许的重放次数)”，并且用户命令连续重放时，可如下所述根据所述重放次数进行重放控制。换言之，当 “Count≥1”时，重放与使用条件不冲突，所以创建具有命令 “REPLAY” 和重放控制信息 “将重放的完成通知给许可证处理应用程序” 的使用授权信息。然后根据该使用授权信息中包含的重放命令和重放控制信息，重放该内容一次，并将重放完成从解码器 I/F 库通知给许可证处理应用程序。每次接收了重放结果的通知，许可证处理应用程序通过将许可证数据的 “Count”(允许重放的次数)减少 1 来更新许可证数据。然后，每次许可证更新时，进行验证以检查是否 “Count≥1”，并且当 “Count≥1”时，创建具有命令 “REPLAY” 和重放控制信息 “将重放的完成

通知给许可证处理应用程序”的使用授权信息。通过重复以上处理也能执行多次连续重放。这减轻了解码器 I/F 库管理重放次数的负担，降低了解码器 I/F 库的处理负荷。这里，重放次数(使用条件减少的单元数)可是多个，而不是一个，还可是每次执行时变化的可变数。

而且这里，可以下列方式执行在解码器 I/F 库中的重放次数的计数；例如，将通过其末尾的内容重放计数为一次执行，将在重放中途的内容倒退也计数为一次执行，将在内容重放中途的终止也计数为一次执行。

另外关于通知，可将通知既发到许可证处理应用程序又发到内容重放设备的用户。例如，在完成重放之后，可在液晶显示器等上显示已更新的重放次数。同样，在下列描述中，也可将通知发到内容重放设备的用户。

接下来，如图 12 中的许可证数据所述，解释使用规则的静态特性为“T_min(视为执行一次重放的重放持续时间)”，而使用规则的可变特性为“Count(允许的重放次数)”的情况。如图 13 所述，当“Count≥1”时，重放与使用条件不冲突，所以创建具有命令“REPLAY”和重放控制信息“在完成 T_min 长度重放的中途的时间点，执行一次重放并将重放的完成通知给许可证处理应用程序”的使用授权信息。然后根据使用授权信息中包含的重放命令和重放控制信息，重放该内容仅一次。然后，在重放中途经过“T_min”的时间点，将重放的进程，特别是经过“T_min”从解码器 I/F 库通知给许可证处理应用程序。此时继续内容重放。一旦接收了重放进程的通知，许可证处理应用程序通过将图 12 所示的许可证数据的“Count”(允许重放的次数)减少 1 来更新许可证数据。同时，在经过了“T_min”时才进行重放的情况下，将不完整执行的通知从解码器 I/F 库发送到许可证处理应用程序。在经过了“T_min”时才进行重放的情况下，不更新许可证数据。这使得能够忽略不能计数为一次重放执行的短持续时间的重放来实现控制。

这里，在解码器 I/F 库的重放经过时间的测量中，当测量重放时间时，不测量例如临时重放暂停周期的时间。

另外，在图 12 所示许可证数据的情况下，可创建具有命令“REPLAY”和重放控制信息“执行一次重放，并在每次完成 T_min 长度重放时，发送通知到许可证处理应用程序”的使用授权信息。在创建这样的使用授权信息的情况下，在内容重放期间，每次经过了“T_min”时，从解码器 I/F 库发送经过“T_min”的通知到许可证处理应用程序作为重放进程通知。此时，继续内

容重放。每次接收重放进程的通知时，许可证处理应用程序通过将图 12 所示的许可证数据的 “Count(允许重放的次数)”减少 1 来更新许可证数据。

接下来，如图 7 的许可证数据中所示，解释使用规则的静态特性为 “Limit(重放时间限制)”，而使用规则的可变特性为 “NULL” 的情况。在这种情况下，根据重放周期进行重放控制。也就是说，在创建使用授权信息的时间和日期在 “Limit”之前的情况下，重放与使用条件不冲突，所以创建如图 14 所示的具有命令 “REPLAY” 和重放控制信息 “在指定持续时间(Limit-当前时间和日期)内重放” 的使用授权信息。根据这一使用授权信息中包含的重放命令和重放控制信息，在指定持续时间内重放该内容。换言之，在执行了指定持续时间的重放的时间点，停止重放。以这种方式，有可能获得基于时间周期的精确重放控制。

接下来，如图 15 的许可证数据中所示，解释使用规则的静态特性为 “NULL”，而使用规则的可变特性为 “T_all(允许的重放时间长度)” 的情况。如图 16 所示，当 “T_all>0” 时，重放与使用条件不冲突，所以创建具有命令 “REPLAY” 和重放控制信息 “执行持续时间 T_all 内的重放，并且一旦完成重放，将实际重放时间 T_play 通知给许可证处理应用程序” 的使用授权信息。根据使用授权信息中包含的重放命令和重放控制信息，在 “T_all” 内重放该内容。换言之，在执行了 “T_all” 的重放的时间点，停止重放。重放之后，将实际重放时间长度 “T_play” 从解码器 I/F 库通知给许可证处理应用程序。一旦接收了该通知，许可证处理应用程序通过将图 15 所示的许可证数据的 “T_all(允许的重放时间长度)”减少 “T_play” 来更新许可证数据。

可替换地，在根据允许重放次数或允许重放时间长度的重放控制方法中，可以下列步骤停止重放：当重放被执行指定时间长度或指定次数时，将执行重放的通知发送到许可证处理应用程序，然后许可证处理应用程序创建具有命令 “STOP” 的使用授权信息，并将所创建的信息以与重放时相同的方式发送到解码器 I/F 库，解码器 I/F 库发送停止命令到音频解码器以停止重放。

除了与此类似的重放次数或重放时间长度之外，可在重放控制信息中设置各种信息来执行重放控制。作为一个例子，有可能设置其中的诸如声音质量或图像质量的重放质量。例如，当在重放控制信息中设置声音质量时，音频解码器以设置的声音质量重放音乐内容。

在该实施例中，为了执行与许可证使用条件相符的重放，当在解码器 I/F

库中认证使用认证信息时，在许可证处理应用程序中进行许可证的认证。在许可证处理应用程序中，很难精确测量和控制实际重放时间、重放质量、或重放范围等。另外，当假设解码器 I/F 库负责所有控制时，那么解码器 I/F 库必须依赖于许可证格式等，结果可得出结论，依赖于内容分发/重放服务的解码器 I/F 库将成为必须。因此，将测量和控制实际重放时间、重放质量、或重放范围等的任务分配给解码器 I/F 库，并将依赖于内容分发/重放服务的其它控制分配给许可证处理应用程序。

如上所述，根据该实施例，由于用于执行重放控制的重放控制信息被合并入使用授权信息中，所以可保证精确重放控制而不损失内容重放设备的一般通用性。

也就是说，在允许重放次数被描述为许可证使用条件的情况下，有可能测量内容重放次数，这使得又有可能限制允许重放次数而不损失内容重放设备的一般通用性。可替换地，在允许重放时间长度被描述为许可证使用条件的情况下，有可能测量内容重放的精确时间长度，这使得又有可能限制允许重放时间长度而不损失内容重放设备的一般通用性。另外，在重放质量被描述为许可证使用条件的情况下，有可能指定内容重放质量，这使得又有可能限制重放质量而不损失内容重放设备的一般通用性。而且，例如重放允许次数和在视为执行一次重放的最小重放时间长度被描述为许可证使用条件的情况下，有可能测量内容重放时间，这使得又有可能限制允许重放次数而不损失内容重放设备的一般通用性。

另外，在例如允许重放时间长度被描述为许可证的使用条件的情况下，有可能测量精确的内容重放时间长度，并通过基于测量时间重写在许可证使用条件中所述的允许重放时间长度，来更新许可证。另外，在例如允许重放次数和视为执行一次重放的最小重放时间长度被描述为许可证使用条件的情况下，有可能测量精确的内容重放时间长度，并通过基于测量时间重写在许可证使用条件中所述的允许重放次数，来更新许可证。因此有可能限制重放次数或重放时间长度而不损失内容重放设备的一般通用性。

(实施例 3)

在该实施例中，描述内容的数据结构、指纹的数据结构、和从内容服务器获取内容的获取方法。

内容的数据结构如图 17 所示。具体说，它由内容 ID、内容相关信息、

许可证 ID、许可证获取 URL、和用内容解密密钥适当加密的内容组成。内容相关信息是与内容相关的信息，例如在内容是音乐的情况下，内容相关信息是例如音乐标题名和作曲家名。许可证 ID 是与内容对应的许可证的 ID，并在某些情况下，多个许可证可对应单个内容。例如可为单个内容提供对重放次数无限制的许可证和仅允许重放 10 次的“试用”许可证，并且可以以彼此不同的价格售出每一许可证。许可证获取 URL 是在许可证获取(购买)时访问的 URL。合适的内容包括但不限于音乐数据、视频数据、图像数据、文档数据、和程序数据。有时合适的内容包含诸如音乐、其封套图像、及其歌词数据的多种类型数据，这种情况下可用彼此不同的内容解密密钥加密每一类型数据。

指纹的数据结构如图 18 所示。具体地说，其由许可证 ID 和许可证摘要组成。许可证摘要是许可证数据的散列(hashed)数据。

接下来，参考图 19 说明从内容服务器获取内容的方法。内容获取的处理过程如下: 即(1)内容重放设备中的内容获取应用程序从内容服务器下载内容，并将该内容传输到 java 库增强。(2)将所下载的内容通过 java 库增强存储到安全器件中的闪存中。

这里，只要重放时内容和许可证都在手边，就可先进行内容获取和许可证购买的任一个，这将在下面描述。

(实施例 4)

在该实施例中，解释用解码器公开密钥加密内容解密密钥，并用安全器件公开密钥进一步加密内容解密密钥的情况。另外，该实施例描述了由下载服务器对所下载许可证签名的情况。在这些情况下，如下进行许可证购买处理和内容重放处理。

图 20 示出了根据本实施例的许可证购买处理过程的示意图。(1)首先，内容重放设备中的内容购买应用程序从内容服务器下载(购买)许可证，并将许可证提供到 java 库增强。由下载服务器将签名附于许可证(签名 1)。(2)然后，利用安全器件中 TRM 的签名函数，由 java 库增强执行签名 1 的认证，以判定签名的真实性。(3)然后，将许可证的指纹存入 TRM。(4)接下来，利用安全器件私密密钥，TRM 重新附加签名(签名 2)。也就是说，用签名 2 替代签名 1。重新附加签名的原因在于在内容重放时，许可证数据经历了更新。(5)将重新附加签名后的许可证存入安全器件的闪存中。如上所述，将购买的许

可证通过java库增强存入安全器件的闪存中。

图 21 是示出了根据本实施例的内容重放处理过程的示意图。(1)首先，从闪存中读出许可证到java库增强。(2)然后，利用安全器件中的签名函数，执行签名2的认证，以判定签名2的真实性。(3)接下来，对许可证数据执行指纹认证。(4)接下来，对许可证数据的使用规则执行认证。(5)接下来，更新许可证数据的可变特性。(6)接下来，基于已更新的许可证数据创建指纹，并在安全器件的 TRM 中登记所创建的指纹。(7)然后，利用安全器件的签名函数，重新附加签名。(8)然后，在符合该内容数据所指示的使用条件的情况下，基于许可证数据创建使用授权信息。(9)然后，利用安全器件的签名函数，将签名附于使用授权信息。在附加签名之后，使用授权信息成为使用授权证明。(10)接下来，利用安全器件私密密钥解密内容解密密钥。在这一步，仍用解码器公开密钥加密内容解密密钥。(11)接下来，将包含已更新的许可证数据的许可证存入安全器件的闪存中。(12)然后，将从许可证中取出的附有使用授权证明的内容解密密钥发送到解码器 I/F 库。(13)接下来，在解码器 I/F 库，判定附于内容解密密钥的使用授权证明的真实性。然后，在音频解码器，仅在解码器 I/F 库核实了其真实性的情况下，根据重放命令重放该内容。也就是说，在音频解码器，在用解码器私密密钥解密内容解密密钥自身之后，通过用内容解密密钥适当解密该内容来重放该内容。

(实施例 5)

在该实施例中，解释用安全器件公开密钥加密内容解密密钥的情况。另外，解释在安全器件的 TRM 中对所购买的许可证进行的一系列处理的情况。在这些情况下，如下进行许可证购买处理和内容重放处理。

图 22 是示出了根据本实施例的许可证购买处理过程的示意图。(1)首先，内容重放设备中的内容购买应用程序从内容服务器下载(购买)许可证，并将许可证通过java库增强传输到安全器件中的 TRM。由下载服务器将签名附于许可证(签名 1)。(2)然后，由安全器件中的 TRM 执行签名 1 的认证，以判定签名的真实性。(3)然后，在 TRM 中登记许可证的指纹。(4)接下来，利用安全器件私密密钥，TRM 重新附加签名(签名 2)。也就是说，用签名 2 替代签名 1。(5)将重新附加签名后的许可证通过java库增强存入安全器件的闪存中。

图 23 是示出了根据该实施例的内容重放处理过程的示意图。(1)首先，通过java库增强从闪存中读出许可证到 TRM。(2)然后，在 TRM 执行签名 2

的认证，以判定签名 2 的真实性。(3)接下来，对许可证数据执行指纹认证。(4)接下来，对许可证数据的使用规则执行认证。(5)接下来，更新许可证数据的可变特性。(6)接下来，基于已更新的许可证数据创建指纹，并在 TRM 中登记所创建的指纹。(7)然后，重新附加安全器件的签名。(8)然后，在用安全器件私密密钥解密内容解密密钥之后，TRM 用解码器公开密钥重新加密内容解密密钥。也就是说，执行密钥替换。(9)然后，在符合该内容数据所指示的使用条件的情况下，基于许可证数据创建使用授权信息。(10)然后，将签名附于使用授权信息。在附加签名之后，使用授权信息成为使用授权证明。(11)接下来，将包含已更新的许可证数据的许可证通过 java 库增强存入安全器件的闪存中。(12)然后，从许可证中取出的附有使用授权证明的内容解密密钥发送到解码器 I/F 库。(13)接下来，在解码器 I/F 库，判定附于内容解密密钥的使用授权证明的真实性。然后，在音频解码器，仅在解码器 I/F 库核实了其真实性的情况下，根据重放命令重放该内容。也就是说，在音频解码器，在用解码器私密密钥解密内容解密密钥自身之后，通过用内容解密密钥适当解密该内容来重放该内容。

可替换地，也可以图 24 所示的方式执行上述许可证购买处理中的步骤(5)。也就是说，(5)通过绕开 java 库增强而将重新附加签名之后的许可证直接从安全器件内的 TRM 存入闪存中。

另外，也有可能用安全器件公开密钥加密内容解密密钥。在这种情况下，通过在多个终端中可互换地共享单个可移动安全器件，有可能使得内容仅在多个终端中插入了安全器件的终端有限地可重放。也就是说，能实现与安全器件捆绑的许可证。

可替换地，有可能通过以图 25 所示的方式绕开 java 库增强，来执行上述 TRM 中内容重放处理的全部步骤(1)-(12)。

可替换地，也有可能通过有限制地允许已仅与安全器件交互认证的重放设备读出安全器件中存储的许可证处理应用程序，来执行许可证处理。

可替换地，也有可能通过将许可证处理应用程序配置为在安全器件的 TRM 中执行许可证处理的插入卡型器件应用程序，来执行安全器件的 TRM 内的许可证处理。而且，当这类应用程序成为必须时，也有可能从内容服务器下载许可证处理应用程序以供使用。

(实施例 6)

在该实施例中，解释用安全器件公开密钥加密内容解密密钥，并且进一步用 SIM 卡唯一密钥加密内容解密密钥的情况。在这种情况下，将许可证捆绑于 SIM 卡，或更具体地说，是 SIM 卡的所有者-用户，因此仅当将 SIM 卡插入终端时，才可能重放内容。

SIM 卡是在符合 GSM(全球数字移动通信系统)系统的移动电话中使用的 IC 芯片，需要插入 SIM 卡以操作 GSM 格式移动电话，因为这类电话不能单独工作。在 SIM 卡内部，存储了诸如移动电话号码、电话号簿等的信息。

图 26 是示出了根据该实施例的许可证购买处理过程的示意图。与图 24 的许可证购买处理的过程相比，这里描述的过程的区别在于(3)存在附加的，从插入终端的 SIM 卡中读出 SIM 卡唯一密钥，并利用 SIM 卡唯一密钥加密内容解密密钥的处理。

图 27 是示出了根据该实施例的内容重放处理过程的示意图。与图 25 的内容重放处理的过程相比，这里描述的过程的区别在于(8)当利用解码器公开密钥执行重新加密时，从插入终端的 SIM 卡中读出 SIM 卡唯一密钥，并利用 SIM 卡唯一密钥解密内容解密密钥，然后用安全器件私密密钥进一步解密内容解密密钥，此后，用解码器公开密钥重新加密内容解密密钥。

在该实施例中，有可能仅在通过既用 SIM 卡唯一密钥又用安全器件公开密钥加密内容解密密钥，来组合使用特定 SIM 卡和特定安全器件的情况下，在有限地允许内容重放。

此外，有可能如图 2 和图 10 所示通过用解码器公开密钥加密内容解密密钥来将许可证捆绑于特定终端，或如图 23 和图 25 所示通过用安全器件公开密钥加密内容解密密钥来将许可证捆绑于特定安全器件，或如图 21 所示通过既用解码器公开密钥又用安全器件公开密钥加密内容解密密钥来将许可证捆绑于特定终端和特定安全器件。可替换地，有可能通过用对于多个器件或用户而设置的共享唯一密钥加密内容解密密钥来将许可证捆绑于器件或用户的特定组。

(实施例 7)

在该实施例中，解释从内容重放设备向外输出(上载)许可证以免除版权备份的情况。在这种情况下，如下进行许可证上载和重新下载的处理。

图 28 是示出了根据该实施例的许可证上载和重新下载处理的过程的示意图。(1)首先，拷贝内容重放设备 1 的许可证，并将所拷贝的许可证上载到

网络上的备份服务器。(2)当随着执行重放，诸如允许重放次数的许可证状态改变时(剩余重放次数减少)，网络上的备份服务器上的许可证状态与内容重放设备 1 的许可证状态同步。(3)由于崩溃或损耗，内容重放设备 1 自身或与安全器件一同变得不可用。(4)在备份服务器上，用代替插入内容重放设备 1 的安全器件的公开密钥的插入内容重放设备 2 的安全器件的公开密钥重新加密内容解密密钥。(5)许可证被重新下载到内容重放设备 2。

在该实施例中，通过保持网络服务器上许可证的备份拷贝，有可能处理内容重放设备自身或和安全器件一起的崩溃或损耗，也有可能处理当重放的执行改变允许重放次数时改变其状态的许可证。

可替换地，取代从内容重放设备上载拷贝的许可证，可在购买时在服务器端输入许可证的购买记录，用作上载许可证的替代品。

可替换地，如图 29 所示，也有可能通过无需保存许可证拷贝而上载许可证并通过将重新下载目的设备限定为上载源内容重放设备，来临时增加安全器件中闪存的自由容量。

如上所述，根据本发明，有可能达到通用终端的安全和可扩展的内容使用控制。

也就是说，根据本发明的内容重放设备包括：获取部件，用于获取其中描述了内容使用条件的许可证数据；创建部件，用于在符合使用条件的情况下基于许可证数据创建包含重放命令的使用授权信息；判定部件，用于判定使用授权信息的真实性；和重放部件，用于在判定部件证明使用授权信息是真的情况下，根据重放命令重放内容。

根据该配置，仅在肯定使用授权信息的真实性的情况下，允许内容重放，其中基于描述内容使用条件的许可证数据创建使用授权信息，有可能防止对内容数据的窃听或对许可证处理应用程序的所谓冒名行为，从而防止内容的未授权使用。

在该认证中，例如，创建部件将在每次创建使用授权信息时具有不同于其它值的值的动态信息合并入使用授权信息，并且判定部件基于动态信息判定使用授权信息的真实性。

根据该配置，由于使用在每次创建使用授权信息时具有不同于其它值的值的动态信息，来判定使用授权信息的真实性，所以有可能正确判定使用授权信息的真实性，并有可能防止已创建一次的使用授权信息的未授权重新使

用，这进一步使得正确判定是否允许使用该内容成为可能。

另外，例如，创建部件创建还包括用于执行符合使用条件的重放控制的控制信息的使用授权信息，并且重放部件根据重放命令和控制信息重放内容。

根据该配置，由于将用于执行重放控制的控制信息合并入使用授权信息，所以可保证精确重放控制而不损失内容重放设备的一般通用性。

另外，例如，创建部件将指示内容重放次数的次数信息作为控制信息合并入使用授权信息，并且重放部件重放该内容一直到所指示的次数。

根据该配置，在将允许重放次数描述为许可证使用条件的情况下，有可能测量内容重放次数，这使得又有可能限制允许重放次数而不损失内容重放设备的一般通用性。

另外，例如，创建部件将指示内容重放时间长度的时间长度信息作为控制信息合并入使用授权信息，并且重放部件重放该内容的时间长度最多到所指示的时间长度。

根据该配置，在将允许重放时间长度描述为许可证使用条件的情况下，有可能测量内容重放的精确时间长度，这使得又有可能限制允许重放时间长度而不损失内容重放设备的一般通用性。

另外，例如，创建部件将指示内容重放质量的质量信息作为控制信息合并入使用授权信息，并且重放部件以所指示的重放质量重放该内容。

根据该配置，在将重放质量描述为许可证使用条件的情况下，有可能指定内容重放质量，这使得又有可能限制重放质量而不损失内容重放设备的一般通用性。

另外，例如，创建部件将用于指示将要通知的内容重放结果的通知命令作为控制信息合并入使用授权信息，而内容重放设备还包括通知部件，用于根据通知命令通知内容重放的结果。

根据该配置，例如在将允许重放时间长度描述为许可证使用条件的情况下，有可能测量内容重放的精确时间长度，这使得又有可能限制允许重放时间长度而不损失内容重放设备的一般通用性。

另外，例如，创建部件将用于指示将要通知的内容重放进程的通知命令作为控制信息合并入使用授权信息，并且内容重放设备还包括通知部件，用于根据通知命令通知内容重放的进程。

根据该配置，在将重放允许次数和视为执行一次重放的最小重放时间长

度描述为许可证使用条件的情况下，有可能测量内容重放时间，这使得又有可能限制允许重放次数而不损失内容重放设备的一般通用性。

另外，例如，以上内容重放设备还具有更新部件，用于根据来自通知部件的通知更新许可证数据。

根据该配置，例如在将允许重放时间长度描述为许可证使用条件的情况下，有可能测量内容重放的精确时间长度，并有可能基于所测量的时间通过重写在许可证使用条件中所述的允许重放时间长度，来更新许可证。另外，例如在将允许重放次数和视为执行一次重放的最小重放时间长度描述为许可证使用条件的情况下，有可能测量内容重放精确时间长度，并基于所测量的时间通过重写在许可证使用条件中所述的允许重放次数，来更新许可证。因此有可能限制重放次数或重放时间长度而不损失内容重放设备的一般通用性。

而且，例如上述内容重放设备还包括签名部件，用于将签名附于使用授权信息，其中判定部件判定签名的真实性。

根据该配置，由于将通过使用例如安全器件等所做的签名附于使用授权信息，所以有可能能防止使用授权信息被篡改。

而且，例如，将上述内容重放设备配置为获取与唯一 ID(特定器件、用户、存储介质、或特定类型器件等)捆绑的许可证，例如经历了与唯一 ID 相关地加密的许可证。

根据该配置，有可能将许可证的使用限制到特定器件(例如许可证所分发到的终端)、特定用户(例如购买许可证的用户)、或特定类型器件。

另外，例如，将上述内容重放设备配置为进一步包括将许可证输出到外部的许可证输出器件，并将由内容重放设备所持有的许可证上载/备份到服务器或网络上的 PC 上。

根据该配置，有可能从服务器或网络上的 PC 重新下载备份许可证，其中在终端崩溃/损坏、或正常迁移到新模式等的情况下，上载备份许可证。而且，有可能临时释放存储器空间。

另外，例如，将上述内容重放设备配置为进一步包括用于获取与外部许可证的同步的许可证同步器件，其中在内容重放设备将许可证既保持在网络上的服务器或网络上的 PC 又保持在内容重放设备自身上时，可保持网络上的服务器或网络上的 PC 上的许可证和内容重放设备自身上的许可证之间的

同步。

根据该配置，即使在执行重放时，诸如允许重放次数的许可证状态改变的情况下(例如剩余重放次数减少)，仍有可能备份反映这样的改变状态的版权。

根据本发明的许可证管理设备包括获取部件，用于获取其中描述了内容使用条件的许可证数据；创建部件，用于在符合使用条件的情况下基于许可证数据创建包含重放命令的使用授权信息；和发送部件，用于向外发送使用授权信息。

而且，根据本发明的内容重放设备包括获取部件，用于获取基于其中描述了内容使用条件的许可证数据而创建的使用授权信息，其中使用授权信息包含重放命令；判定部件，用于判定使用授权信息的真实性；和重放部件，用于在判定部件证明使用授权信息是真的情况下，根据重放命令重放内容。

根据这些配置，仅在肯定使用授权信息的真实性的情况下，允许内容重放，其中基于其中描述了内容使用条件的许可证数据创建使用授权信息，有可能防止对内容数据的窃听或对许可证处理应用程序的所谓冒名行为，从而进一步防止内容的未授权使用。

根据本发明的内容重放控制方法包括：获取步骤，获取声明内容使用条件的许可证数据；创建步骤，在符合使用条件的情况下基于许可证数据创建包含重放命令的使用授权信息；判定步骤，判定使用授权信息的真实性；和重放步骤，在判定步骤证明使用授权信息是真的情况下，根据重放命令重放内容。

根据该方法，仅在肯定使用授权信息的真实性的情况下，允许内容重放，其中基于描述了内容使用条件的许可证数据创建使用授权信息，有可能防止对内容数据的窃听或对许可证处理应用程序的所谓冒名行为，从而进一步防止内容的未授权使用。

根据本发明的许可证管理程序包括：获取步骤，获取声明了内容使用条件的许可证数据；创建步骤，在符合使用条件的情况下基于许可证数据创建包含重放命令的使用授权信息；和发送步骤，向外发送使用授权信息。

而且，根据本发明的内容重放程序包括：获取步骤，获取基于声明内容使用条件的许可证数据创建的使用授权信息，其中使用授权信息包含重放命令；判定步骤，判定使用授权信息的真实性；和重放步骤，在判定步骤证明

使用授权信息是真的情况下，根据重放命令重放内容。

根据这些程序，仅在肯定使用授权信息的真实性的情况下，允许内容重放，其中基于描述内容使用条件的许可证数据创建使用授权信息，有可能防止对内容数据的窃听或对许可证处理应用程序的所谓冒名行为，从而进一步防止内容的未授权使用。

本说明书基于2002年3月29日提交的日本专利申请第2002-097846号，在此全文引用，以供参考。

工业实用性

本发明适用于内容分发系统中的内容重放设备和许可证管理设备。

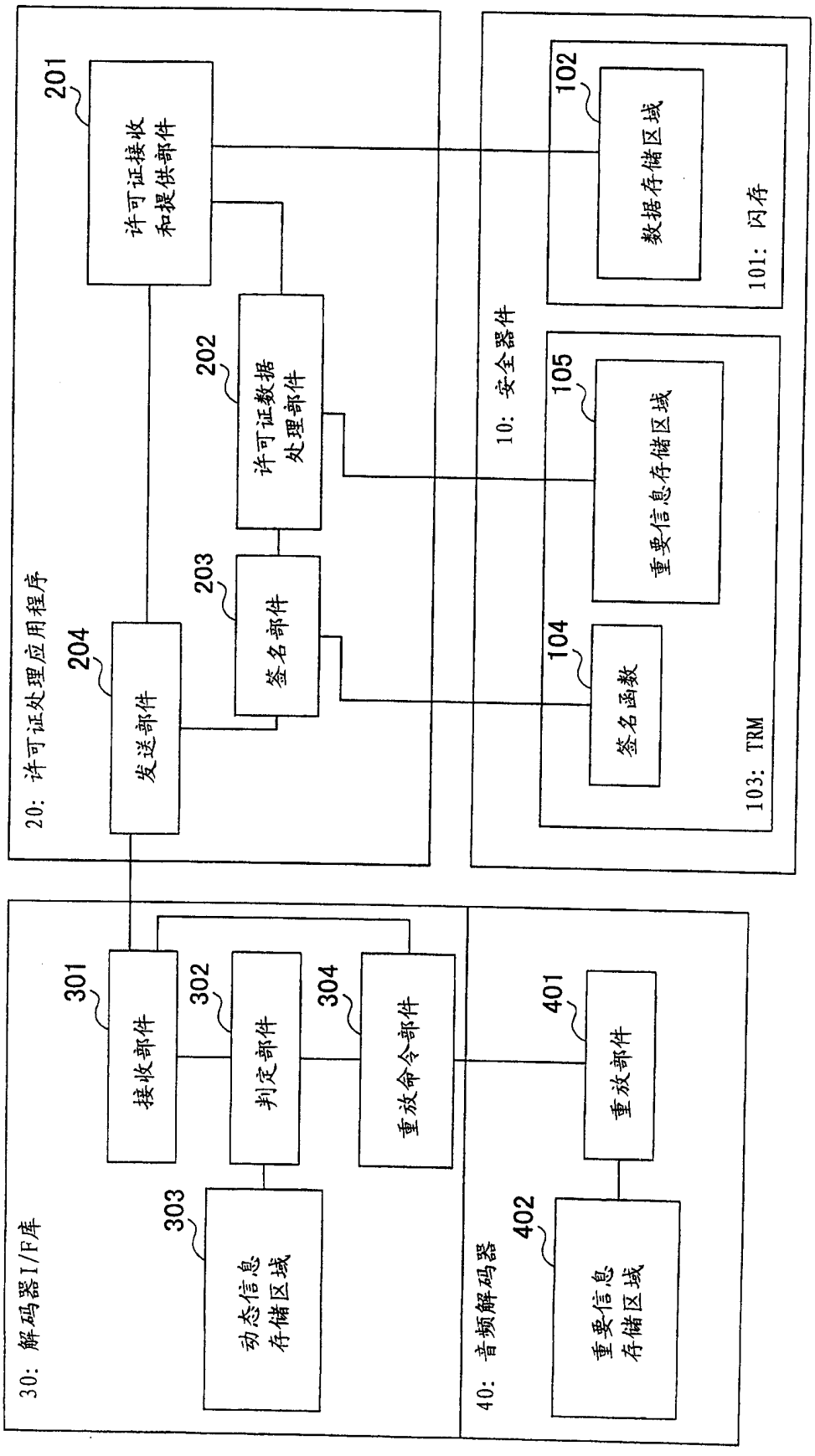

20：许可证处理应用程序
201
许可证接收和提供部件
202
许可证数据处理部件
203
签名部件
204
发送部件
10：安全器件
101：闪存
102
数据存储区域
103：TRM
104
签名函数
105
重要信息存储区域
30：解码器I/F库
301
接收部件
302
判定部件
303
动态信息存储区域
304
重放命令部件
40：音频解码器
401
重放部件
402
重要信息存储区域

图 1

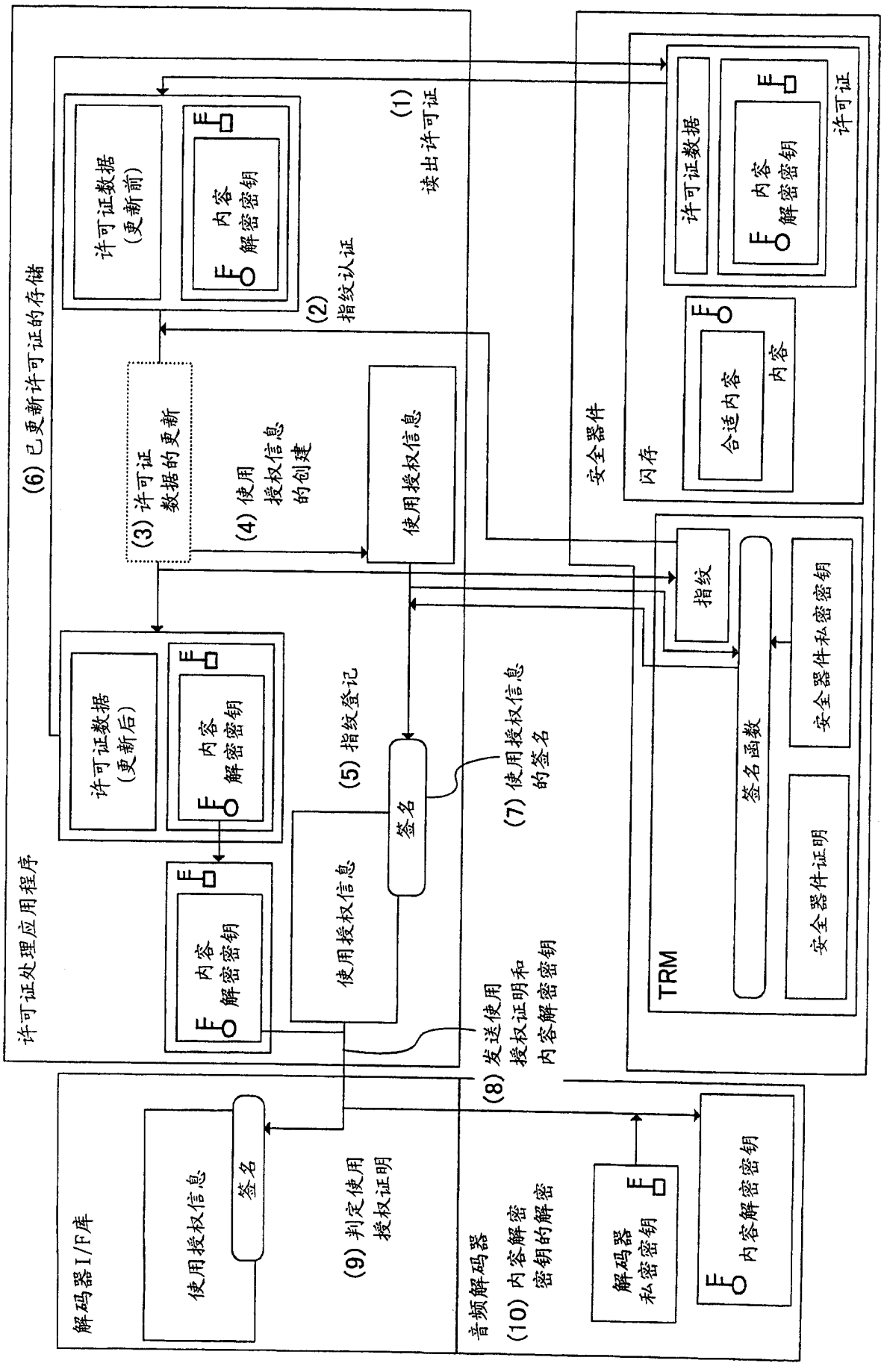

许可证处理应用程序
(6) 已更新许可证的存储
许可证数据
(更新前)
内容
解密密钥
(1)
读出许可证
(2)
指纹认证
(3) 许可证
数据的更新
(4) 使用
授权信息
的创建
使用授权信息
安全器件
闪存
许可证数据
内容
解密密钥
许可证
合适内容
内容
指纹
签名函数
安全器件私密密钥
安全器件证明
TRM
许可证数据
(更新后)
内容
解密密钥
(5) 指纹登记
使用授权信息
签名
(7) 使用授权信息
的签名
内容
解密密钥
使用授权信息
签名
(8) 发送使用
授权证明和
内容解密密钥
(9) 判定使用
授权证明
(10) 内容解密
密钥的解密
解码器
私密密钥
内容解密密钥
解码器I/F库
音频解码器

图 2

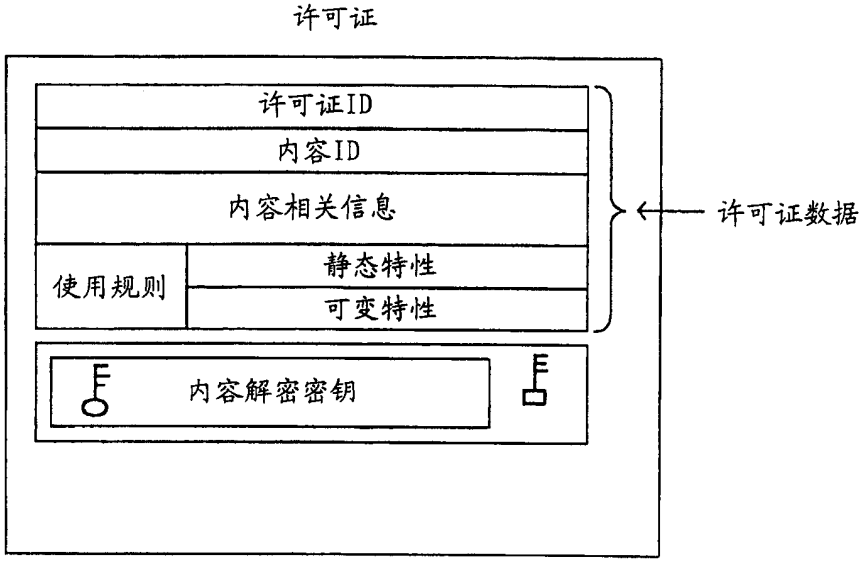

许可证
许可证ID
内容ID
内容相关信息
使用规则
静态特性
可变特性
内容解密密钥
许可证数据

图 3

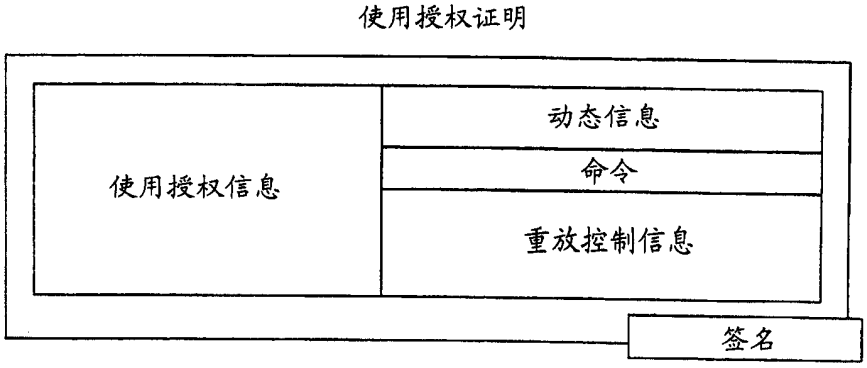

使用授权证明
使用授权信息
动态信息
命令
重放控制信息
签名

图 4

<table>
<tr><td colspan="2">许可证ID</td></tr>
<tr><td colspan="2">内容ID</td></tr>
<tr><td rowspan="2">使用规则</td><td>空</td></tr>
<tr><td>COUNT(允许重放次数)</td></tr>
</table>

图 5

<table>
<tr><td rowspan="3">使用授权信息</td><td>动态信息</td></tr>
<tr><td>重放</td></tr>
<tr><td>空</td></tr>
</table>

图 6

<table>
<tr><td colspan="2">许可证ID</td></tr>
<tr><td colspan="2">内容ID</td></tr>
<tr><td rowspan="2">使用规则</td><td>LIMIT(重放时间限制)</td></tr>
<tr><td>空</td></tr>
</table>

图 7

<table>
<tr><td rowspan="3">使用授权信息</td><td>动态信息</td></tr>
<tr><td>重放</td></tr>
<tr><td>空</td></tr>
</table>

图 8

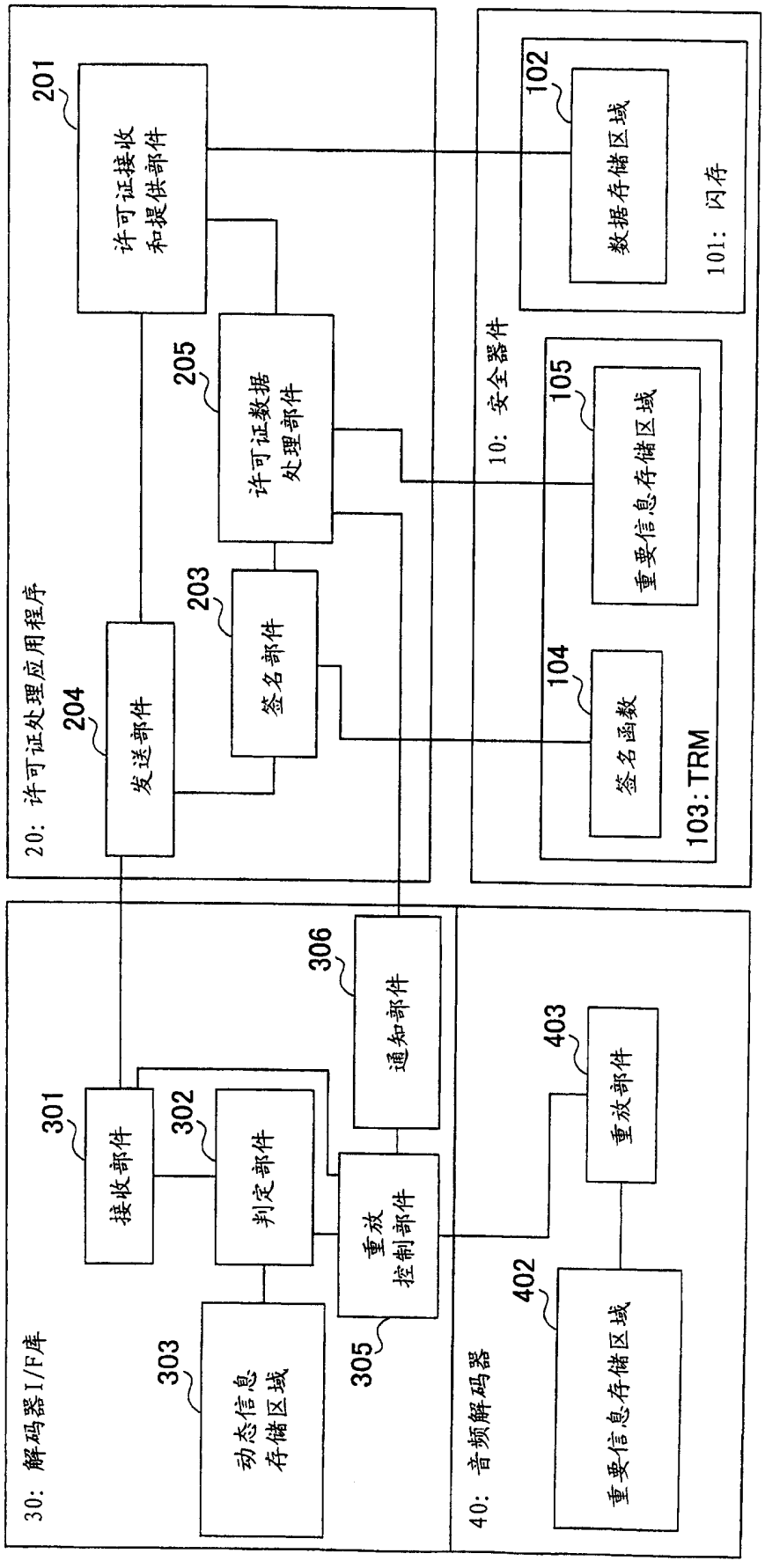

20：许可证处理应用程序
201
许可证接收和提供部件
205
许可证数据处理部件
203
签名部件
204
发送部件
10：安全器件
102
数据存储区域
101：闪存
105
重要信息存储区域
104
签名函数
103:TRM
30：解码器I/F库
306
通知部件
301
接收部件
302
判定部件
重放控制部件
303
动态信息存储区域
305
40：音频解码器
403
重放部件
402
重要信息存储区域

图 9

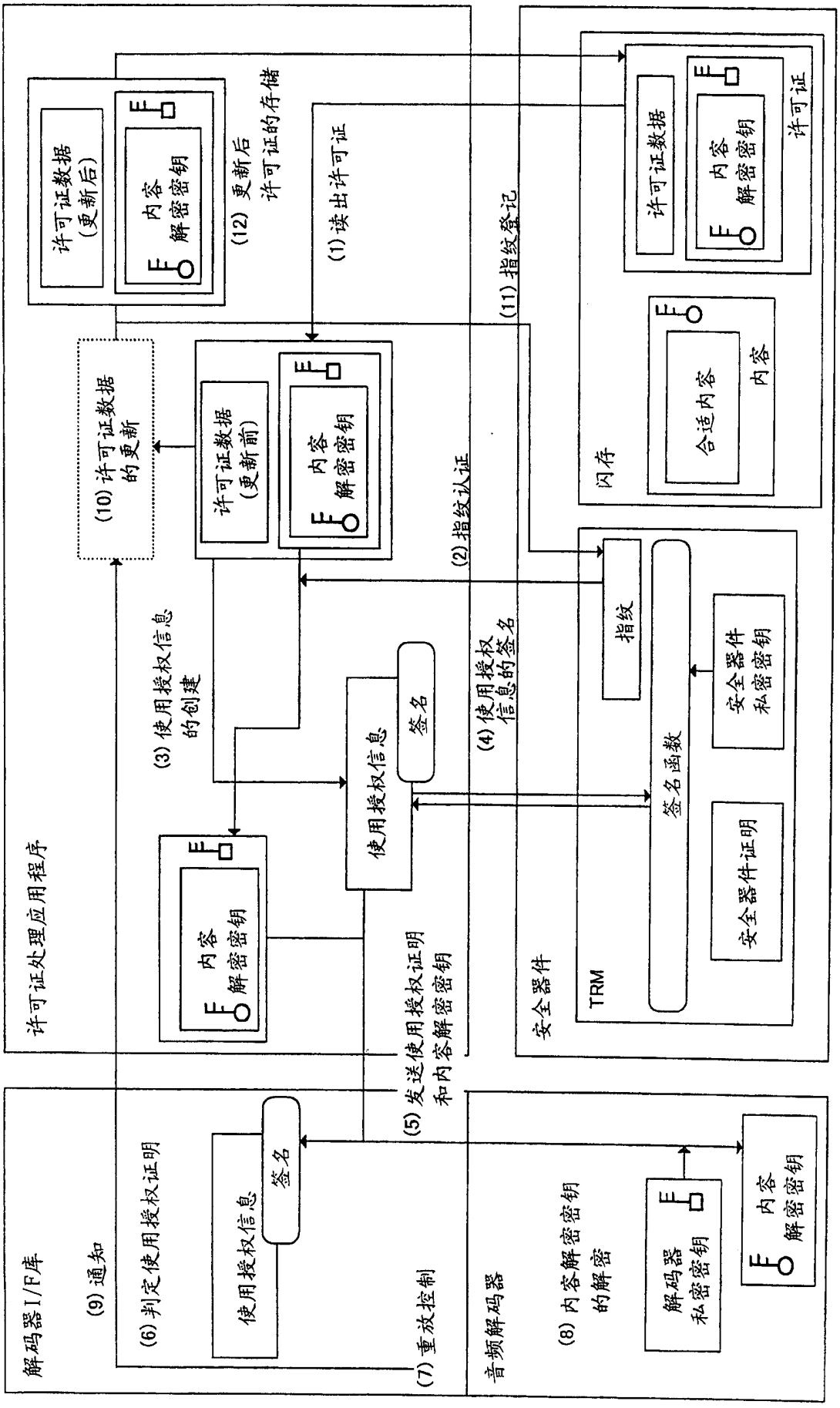

解码器I/F库
(9) 通知
(6) 判定使用授权证明
使用授权信息
签名
(7) 重放控制
(5) 发送使用授权证明和内容解密密钥
音频解码器
(8) 内容解密密钥的解密
解码器私密密钥
内容解密密钥
许可证处理应用程序
(3) 使用授权信息的创建
内容解密密钥
使用授权信息
签名
(4) 使用授权信息的签名
(10) 许可证数据的更新
许可证数据(更新前)
内容解密密钥
(2) 指纹认证
(1) 读出许可证
(12) 更新后许可证的存储
许可证数据(更新后)
内容解密密钥
(11) 指纹登记
安全器件
TRM
指纹
签名函数
安全器件私密密钥
安全器件证明
闪存
合适内容
内容
许可证
许可证数据
内容解密密钥

图 10

使用授权信息	动态信息
	重放
	在完成最多Count的多次重放后通知重放次数

图 11

许可证ID	
内容ID	
使用规则	T_min(视作一次执行的重放时间长度)
	Count(允许重放次数)

图 12

使用授权信息	动态信息
	重放
	如果已执行重放T_min则通知

图 13

使用授权信息	动态信息
	重放
	如果已执行指定时间长度则停止重放

图 14

<table>
<tr><td colspan="2">许可证ID</td></tr>
<tr><td colspan="2">内容ID</td></tr>
<tr><td rowspan="2">使用规则</td><td>空</td></tr>
<tr><td>T_all(允许重放时间长度)</td></tr>
</table>

图 15

<table>
<tr><td rowspan="3">使用授权信息</td><td>动态信息</td></tr>
<tr><td>重放</td></tr>
<tr><td>如果已执行指定时间长度则停止
重放，并通知执行重放的时间长度</td></tr>
</table>

图 16

<table>
<tr><td>内容ID</td></tr>
<tr><td>内容相关信息</td></tr>
<tr><td>许可证ID</td></tr>
<tr><td>许可证获取URL</td></tr>
<tr><td>合适的内容</td></tr>
</table>

图 17

<table>
<tr><td>许可证ID</td></tr>
<tr><td>许可证摘要</td></tr>
</table>

图 18

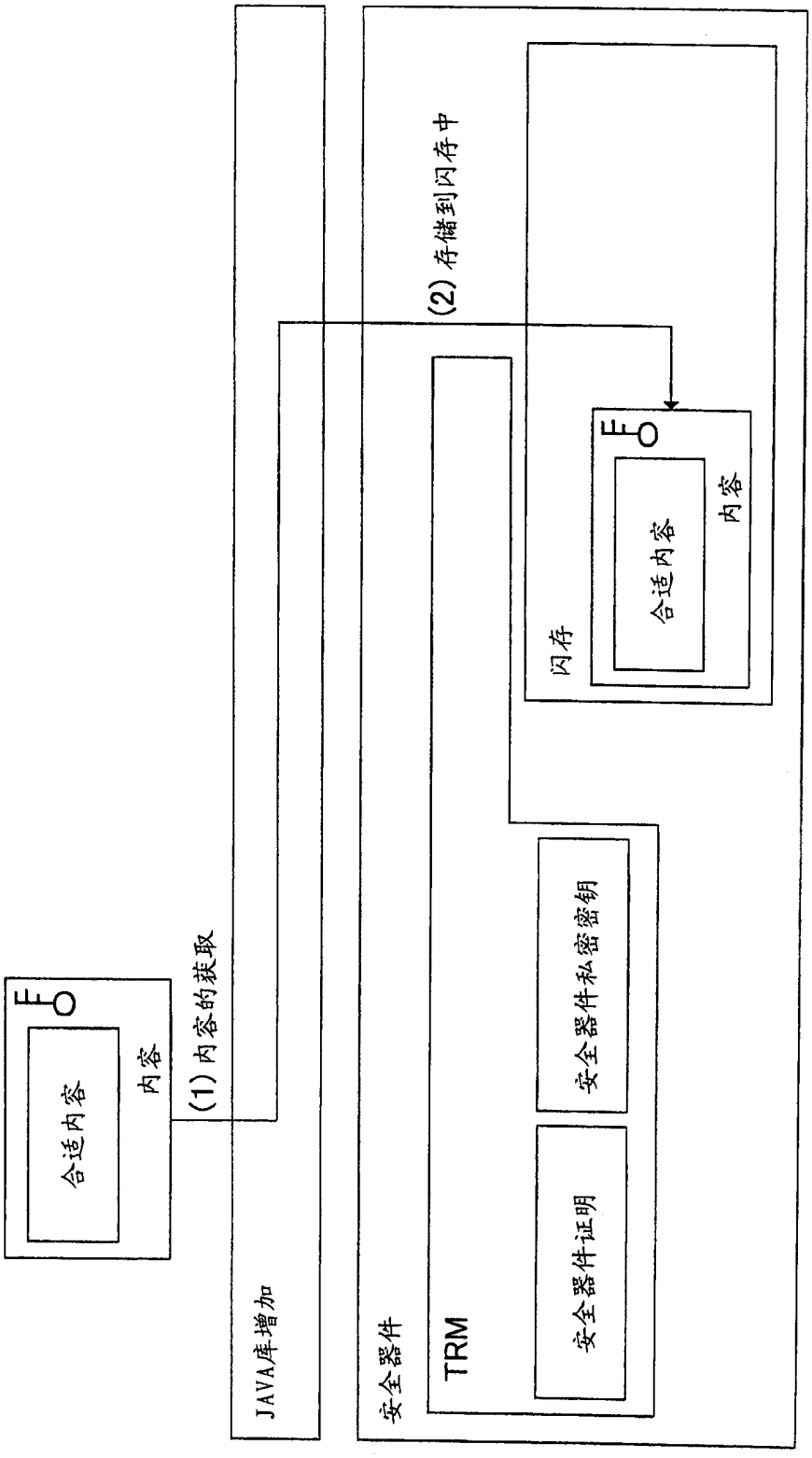

合适内容
内容
(1) 内容的获取
JAVA库增加
安全器件
(2) 存储到闪存中
TRM
安全器件证明
安全器件私密密钥
闪存
合适内容
内容

图 19

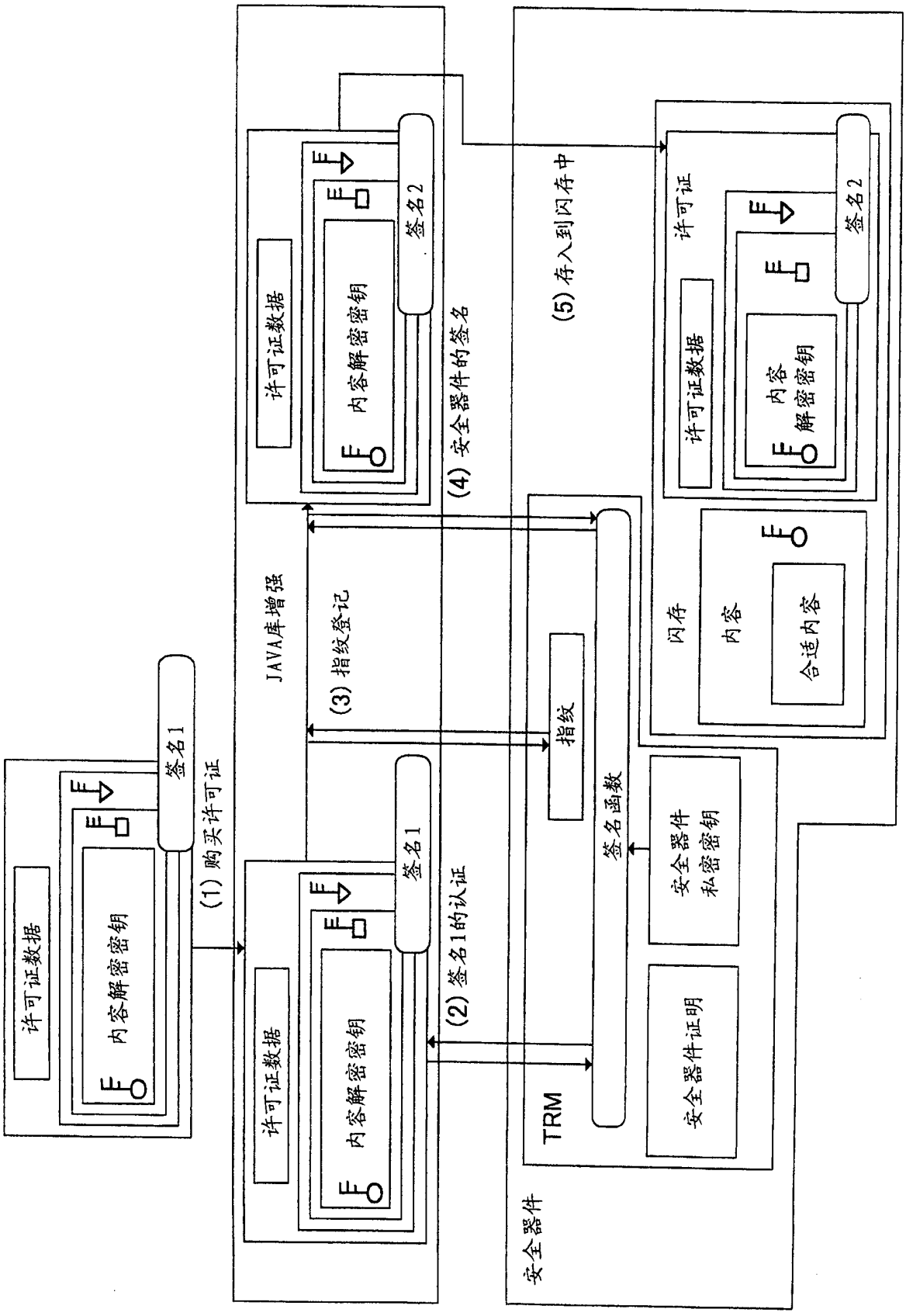

许可证数据
内容解密密钥
签名1
(1) 购买许可证
JAVA库增强
(3) 指纹登记
(4) 安全器件的签名
(5) 存入到闪存中
(2) 签名1的认证
指纹
签名函数
TRM
安全器件证明
安全器件私密密钥
闪存
内容
合适内容
许可证
签名2
安全器件

图 20

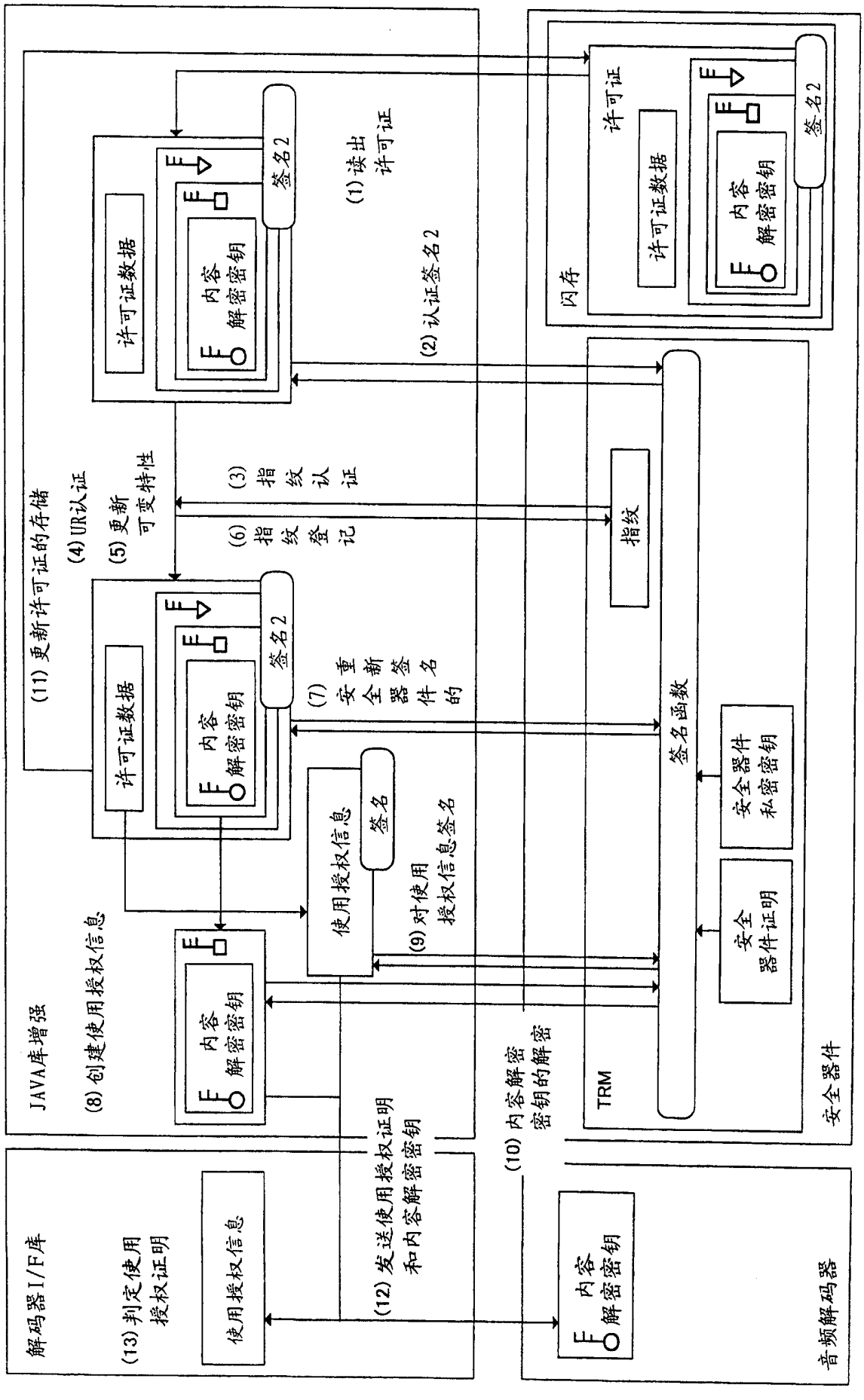

解码器I/F库
使用授权信息
(13) 判定使用授权证明
JAVA库增强
(8) 创建使用授权信息
(11) 更新许可证的存储
(4) UR认证
(5) 更新可变特性
(6) 指纹登记
(3) 指纹认证
(1) 读出许可证
(2) 认证签名2
许可证数据
内容解密密钥
签名2
(7) 安全重新签名器件的
使用授权信息
签名
(9) 对使用授权信息签名
(12) 发送使用授权证明和内容解密密钥
(10) 内容解密密钥的解密
闪存
许可证
许可证数据
内容解密密钥
签名2
指纹
TRM
签名函数
安全器件私密密钥
安全器件证明
安全器件
内容解密密钥
音频解码器

图 21

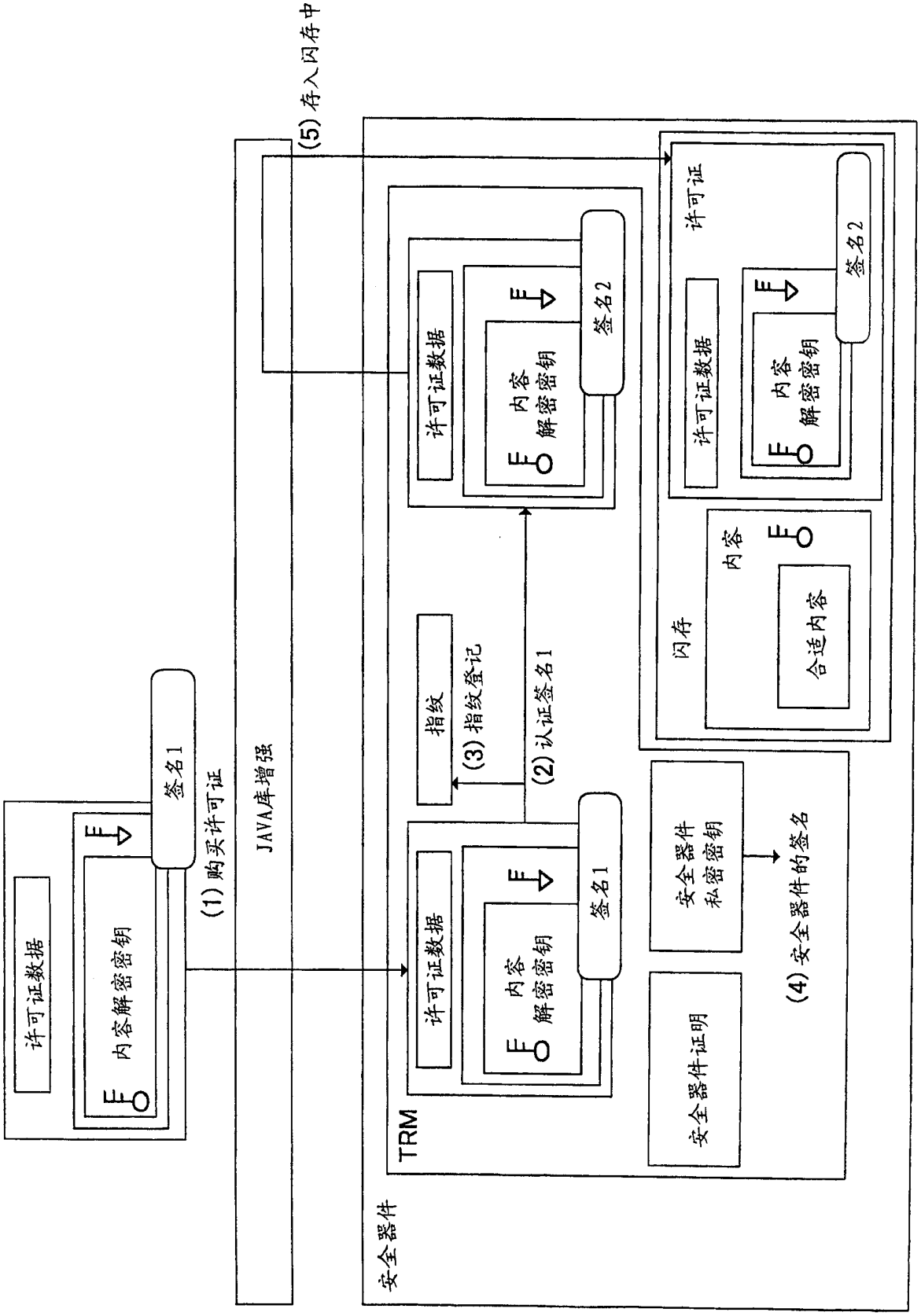

许可证数据
内容解密密钥
签名1
(1) 购买许可证
JAVA库增强
(5) 存入闪存中
安全器件
TRM
许可证数据
内容解密密钥
签名1
指纹
(3) 指纹登记
(2) 认证签名1
许可证数据
内容解密密钥
签名2
安全器件证明
安全器件私密密钥
(4) 安全器件的签名
闪存
内容
合适内容
许可证
许可证数据
内容解密密钥
签名2

图 22

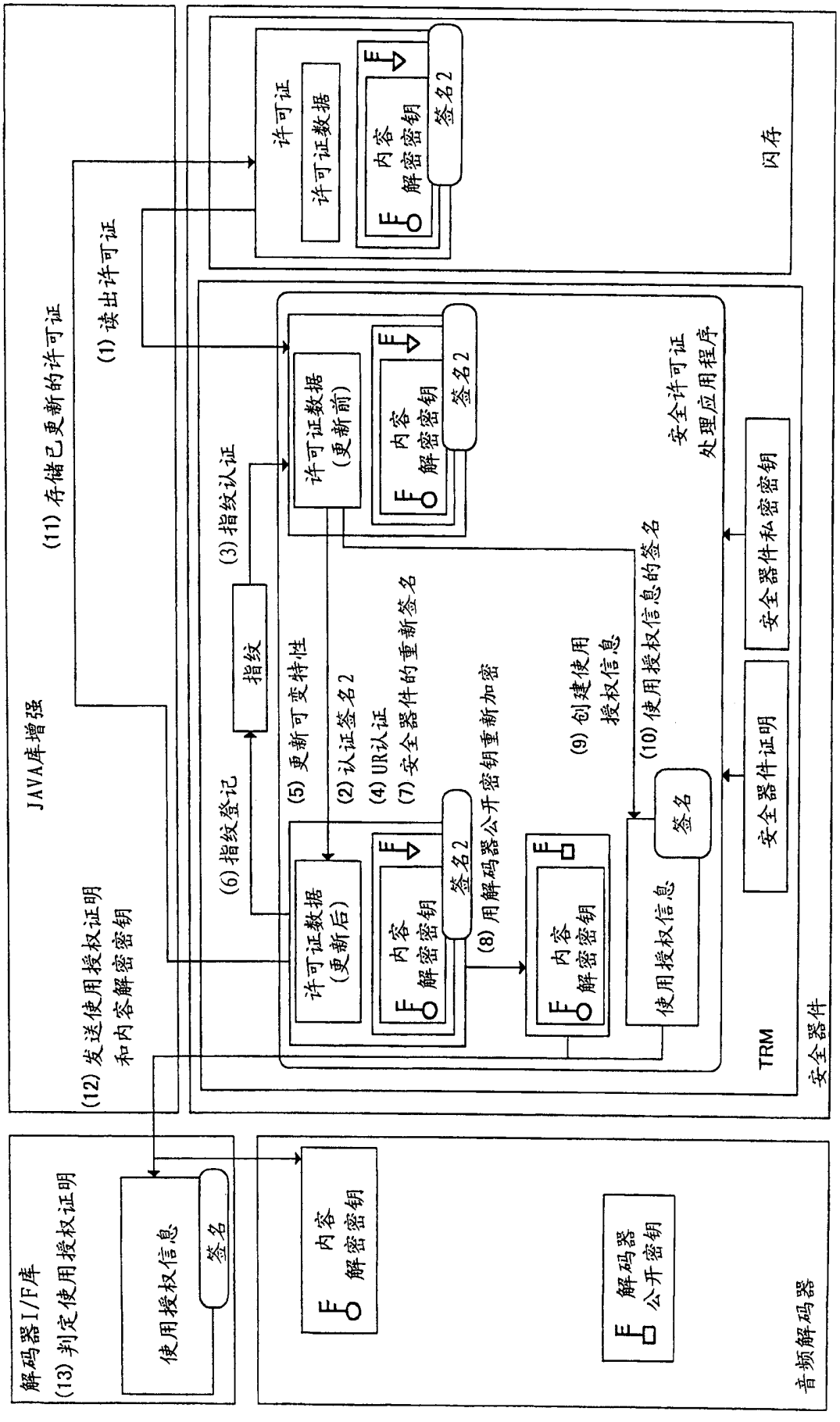

解码器I/F库
(13) 判定使用授权证明
使用授权信息
签名
内容
解密密钥
解码器
公开密钥
音频解码器
JAVA库增强
(12) 发送使用授权证明
和内容解密密钥
(11) 存储已更新的许可证
(1) 读出许可证
(6) 指纹登记
指纹
(3) 指纹认证
(5) 更新可变特性
(2) 认证签名2
(4) UR认证
(7) 安全器件的重新签名
(8) 用解码器公开密钥重新加密
(9) 创建使用
授权信息
(10) 使用授权信息的签名
许可证数据
(更新后)
内容
解密密钥
签名2
使用授权信息
签名
安全器件证明
TRM
安全器件
许可证数据
(更新前)
内容
解密密钥
签名2
安全许可证
处理应用程序
安全器件私密密钥
许可证
许可证数据
内容
解密密钥
签名2
闪存

图 23

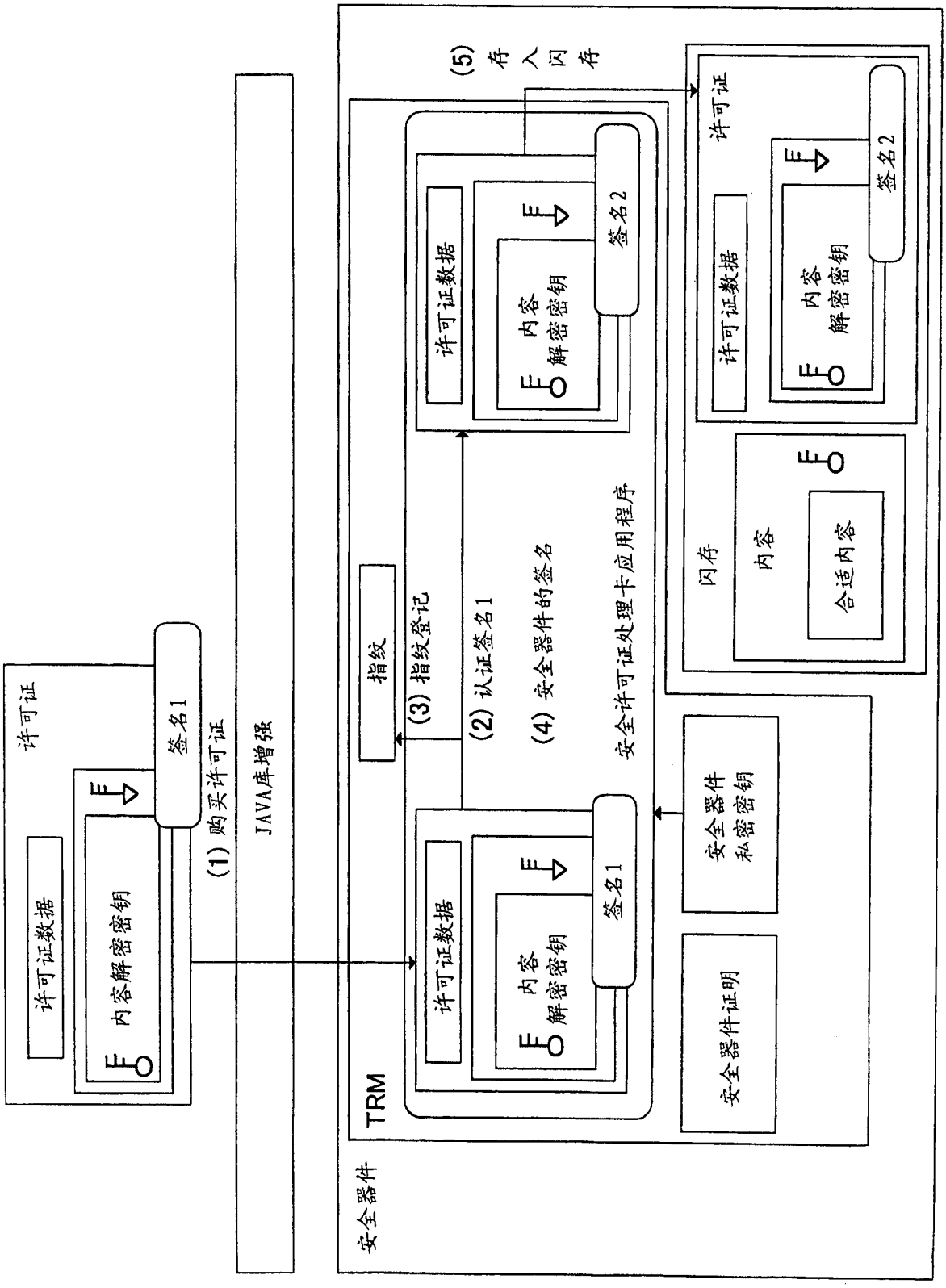

许可证
许可证数据
内容解密密钥
签名1
(1) 购买许可证
JAVA库增强
安全器件
TRM
指纹
(3) 指纹登记
(2) 认证签名1
(4) 安全器件的签名
安全许可证处理卡应用程序
许可证数据
内容解密密钥
签名1
安全器件私密密钥
安全器件证明
(5) 存入闪存
许可证数据
内容解密密钥
签名2
闪存
内容
合适内容
许可证
许可证数据
内容解密密钥
签名2

图 24

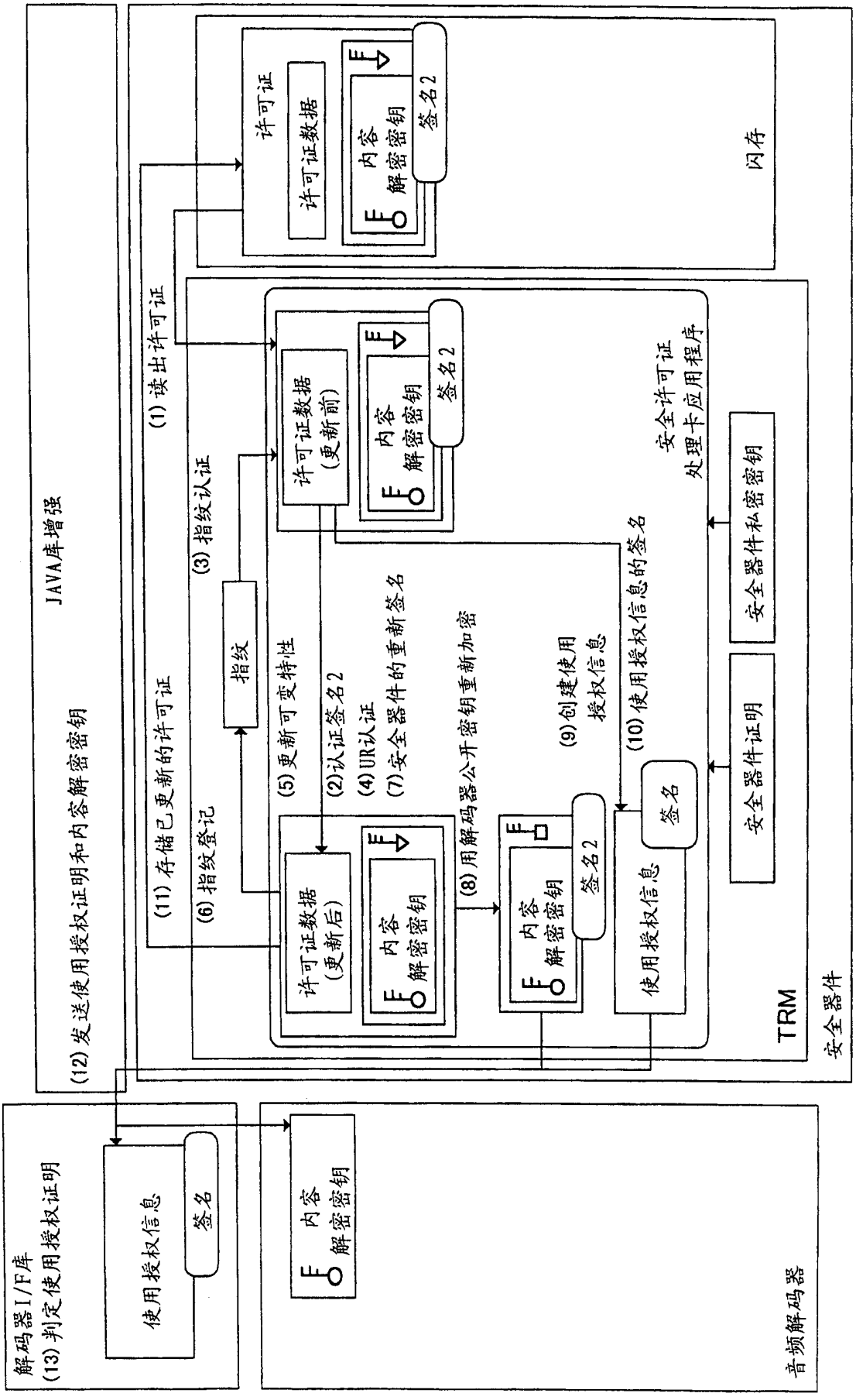

解码器I/F库
(13) 判定使用授权证明
使用授权信息
签名
音频解码器
内容
解密密钥
JAVA库增强
(12) 发送使用授权证明和内容解密密钥
安全器件
TRM
(11) 存储已更新的许可证
(1) 读出许可证
(3) 指纹认证
(6) 指纹登记
指纹
(5) 更新可变特性
(2)认证签名2
(4) UR认证
(7)安全器件的重新签名
(8) 用解码器公开密钥重新加密
(9)创建使用
授权信息
(10) 使用授权信息的签名
安全许可证
处理卡应用程序
许可证数据
(更新后)
内容
解密密钥
签名2
使用授权信息
签名
安全器件证明
安全器件私密密钥
许可证
许可证数据
内容
解密密钥
签名2
闪存

图 25

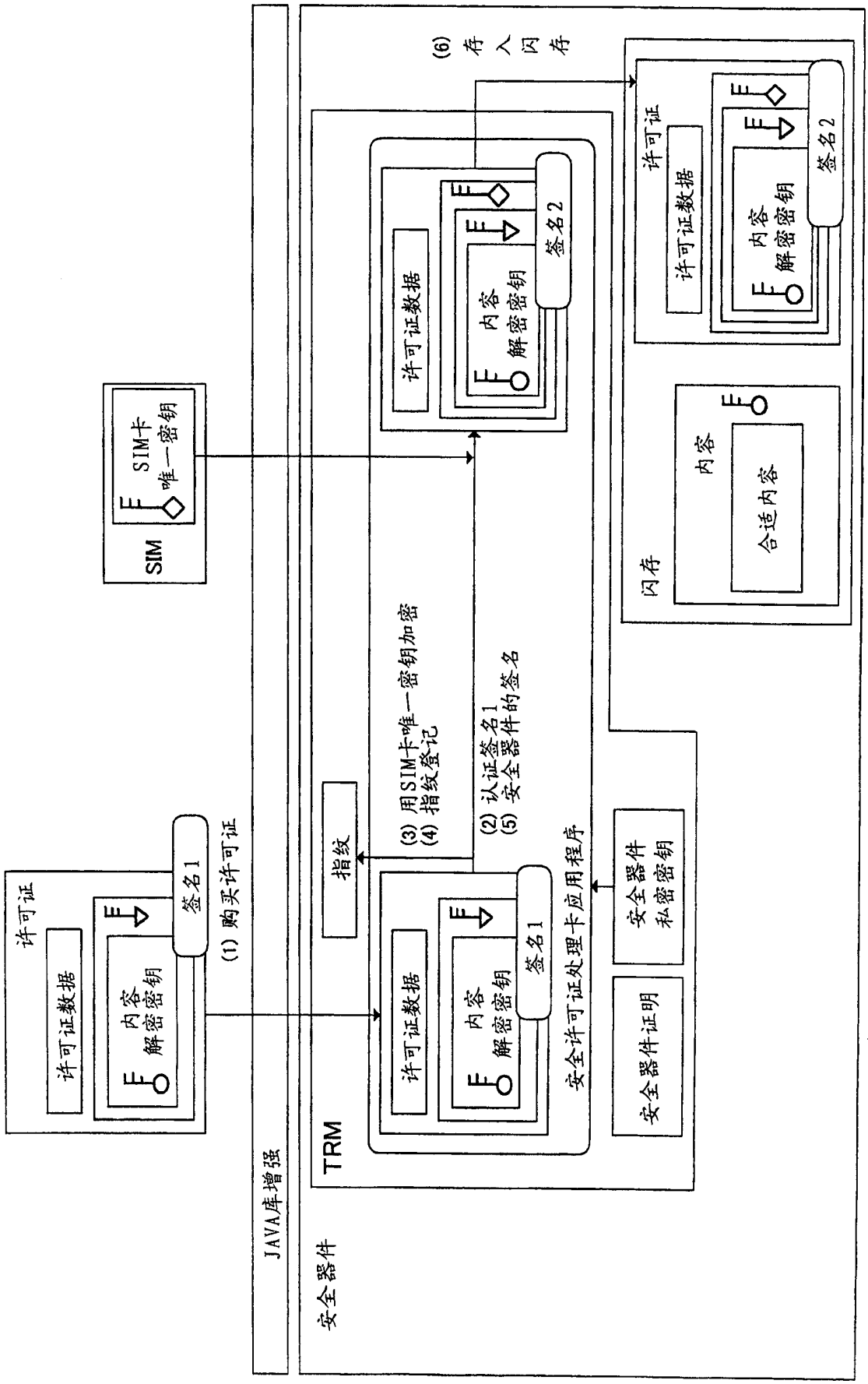

许可证
许可证数据
内容
解密密钥
签名1
(1) 购买许可证
JAVA库增强
安全器件
SIM
SIM卡
唯一密钥
TRM
指纹
(3) 用SIM卡唯一密钥加密
(4) 指纹登记
(2) 认证签名1
(5) 安全器件的签名
安全许可证处理卡应用程序
安全器件证明
安全器件
私密密钥
(6) 存入闪存
闪存
内容
合适内容

图 26

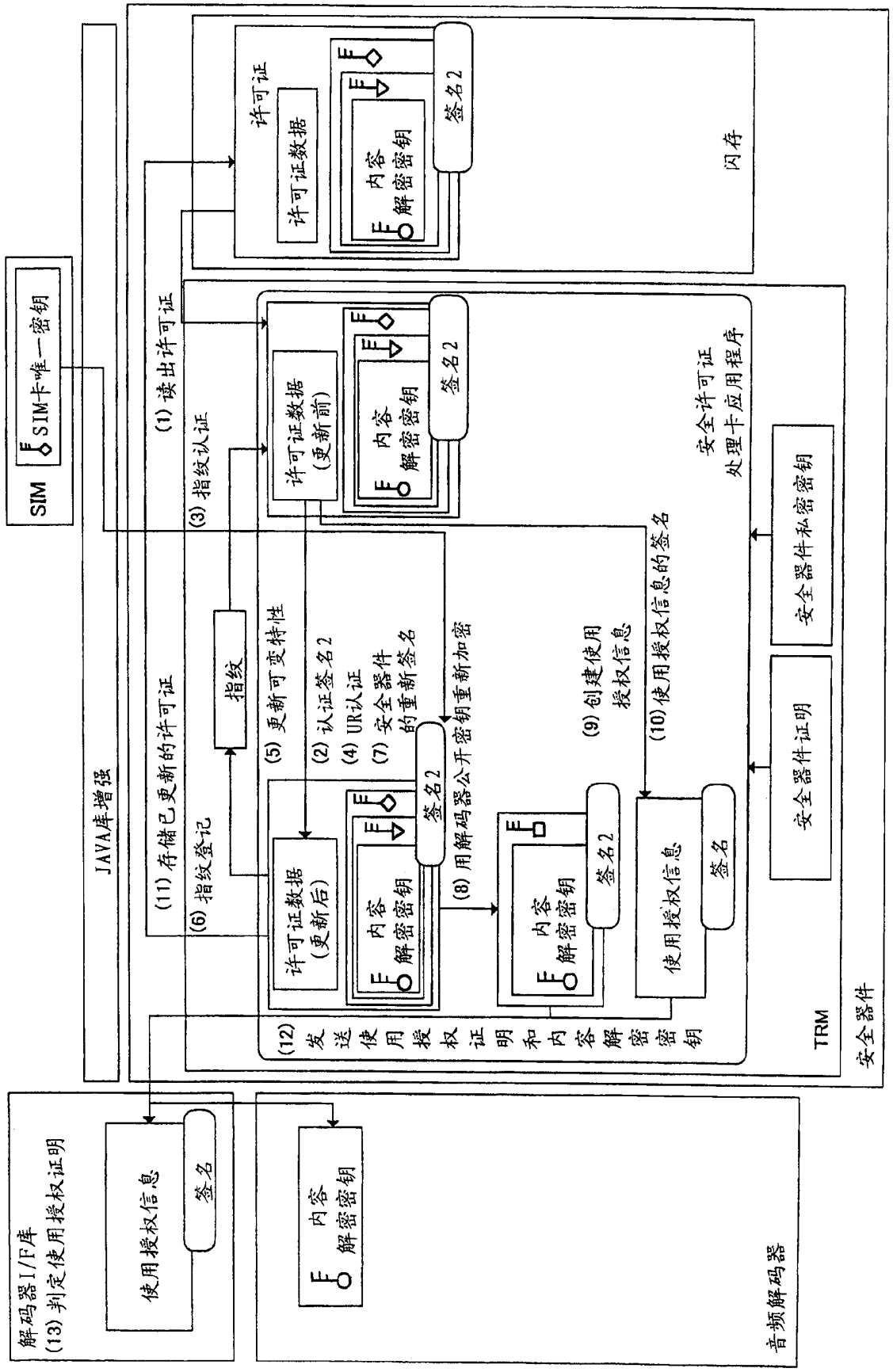

解码器I/F库
(13) 判定使用授权证明
使用授权信息
签名
内容解密密钥
音频解码器
JAVA库增强
SIM
SIM卡唯一密钥
安全器件
TRM
闪存
(1) 读出许可证
(3) 指纹认证
(11) 存储已更新的许可证
(6) 指纹登记
指纹
(5) 更新可变特性
(2) 认证签名2
(4) UR认证
(7) 安全器件的重新签名
(8) 用解码器公开密钥重新加密
(9) 创建使用授权信息
(10)使用授权信息的签名
(12)发送使用授权证明和内容解密密钥
许可证数据(更新后)
许可证数据(更新前)
许可证
许可证数据
内容解密密钥
签名2
使用授权信息
签名
安全器件证明
安全器件私密密钥
安全许可证处理卡应用程序

图 27

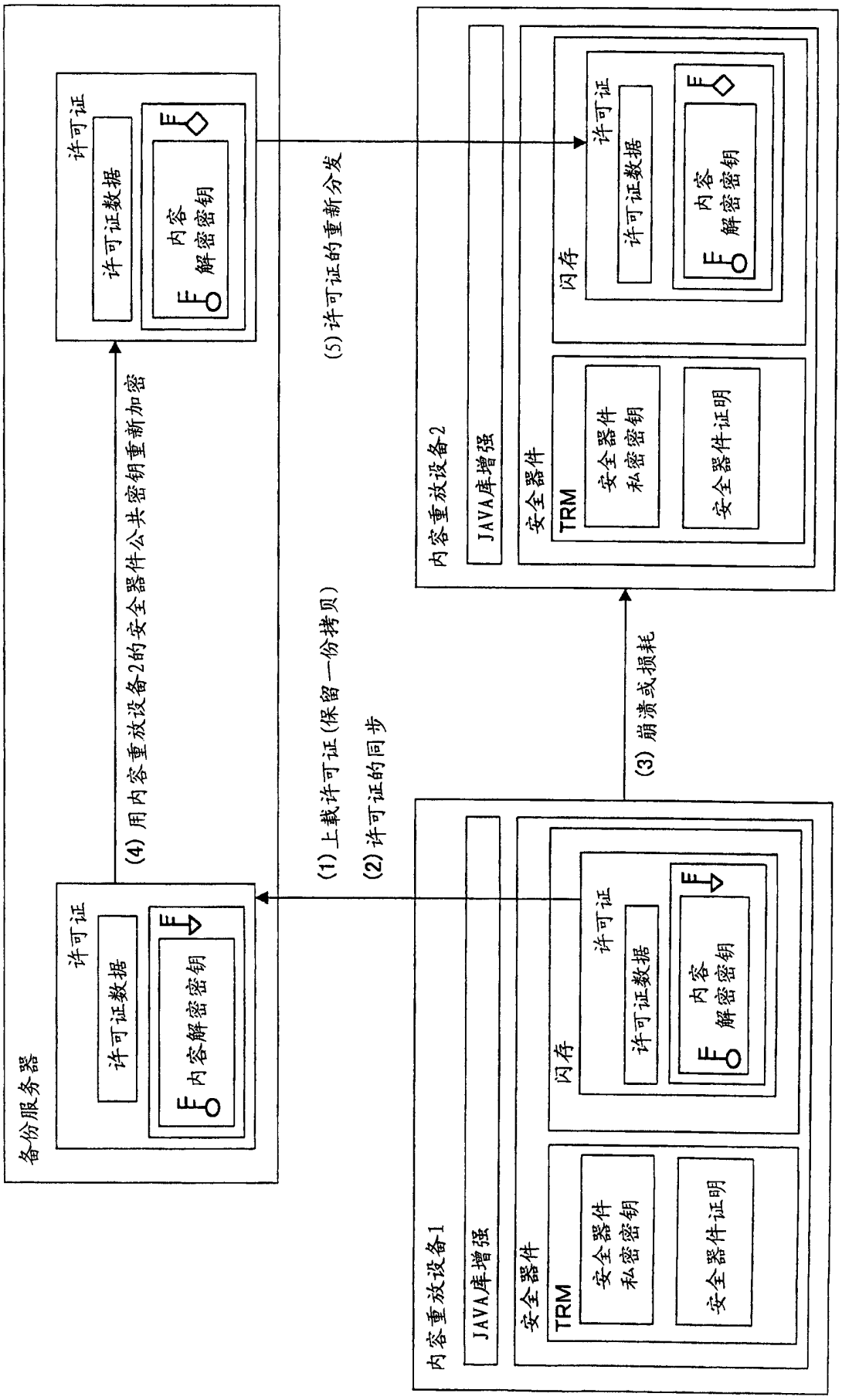

备份服务器
许可证
许可证数据
内容解密密钥
(4) 用内容重放设备2的安全器件公共密钥重新加密
(5) 许可证的重新分发
(1) 上载许可证(保留一份拷贝)
(2) 许可证的同步
(3) 崩溃或损耗
内容重放设备2
JAVA库增强
安全器件
TRM
安全器件私密密钥
安全器件证明
闪存
许可证
许可证数据
内容解密密钥
内容重放设备1

图 28

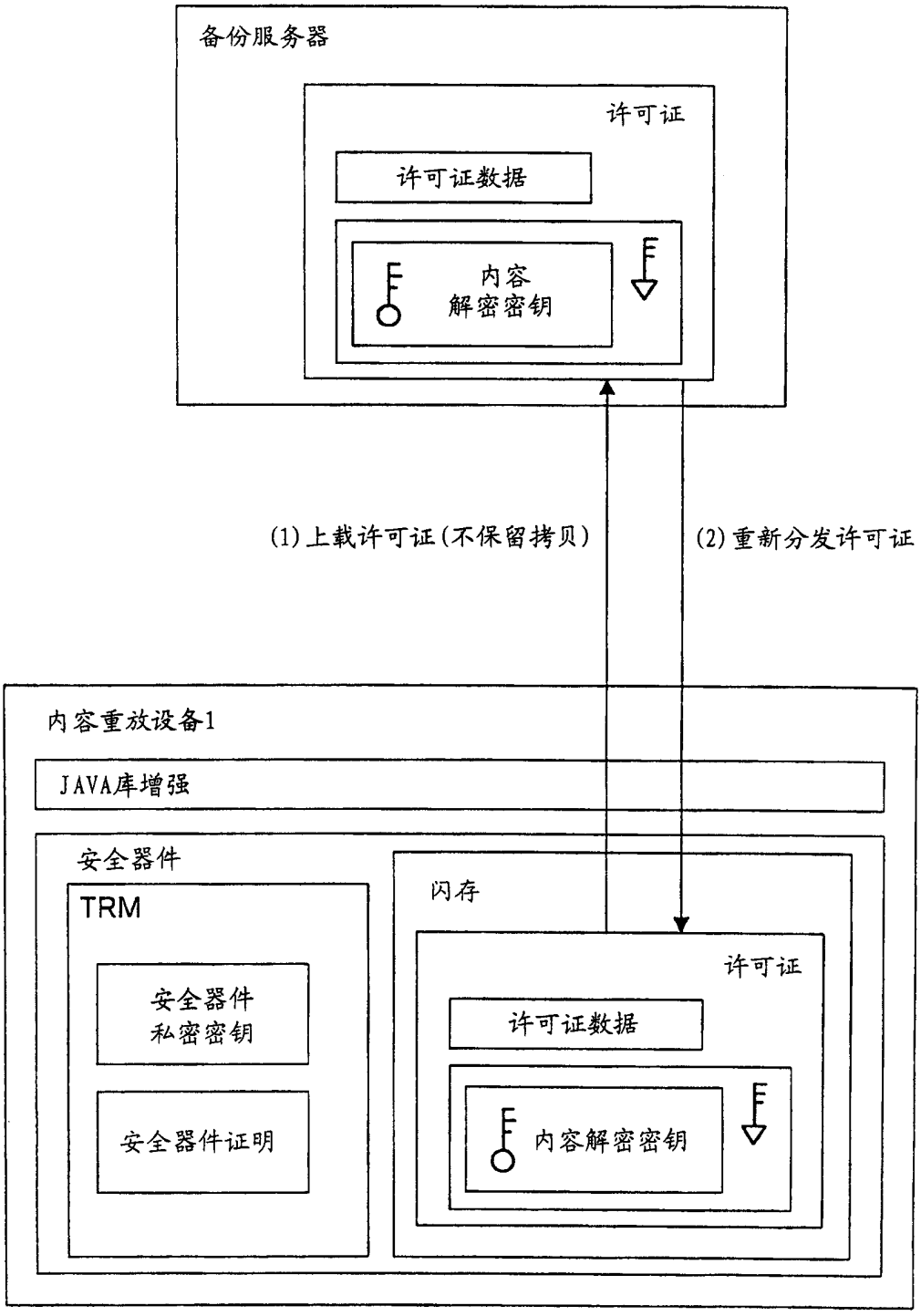

备份服务器
许可证
许可证数据
内容
解密密钥
(1)上载许可证(不保留拷贝)
(2)重新分发许可证
内容重放设备1
JAVA库增强
安全器件
TRM
安全器件
私密密钥
安全器件证明
闪存
许可证
许可证数据
内容解密密钥

图 29