[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06K 9/18
G06F 17/60 G06F 9/30

[12]发明专利申请公开说明书

[21]申请号 00127012.5

[43]公开日 2001 年 3 月 28 日

[11]公开号 CN 1289100A

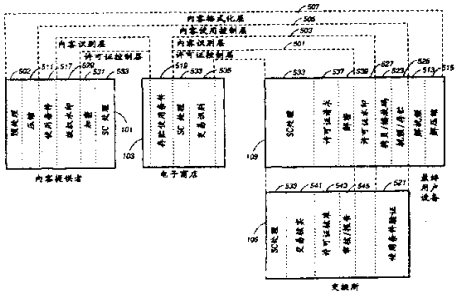
[22]申请日 2000.9.14 [21]申请号 00127012.5
[30]优先权
[32]1999.9.17 [33]US [31]09/397,419
[71]申请人 国际商业机器公司
地址 美国纽约
[72]发明人 小约翰·J·多拉克
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 酆 迅

权利要求书 4 页 说明书 136 页 附图页数 22 页

[54]发明名称 用于在电子销售系统中唯一识别顾客购买的方法及设备

[57]摘要

跟踪用户设备上数字内容使用的系统。内容站点用以通过计算机可读介质向用 户销售数字内容。内容站点把唯一的内容标识符同相关的内容结合起来。连到网络上的电子商店向用户销售许可证。许可证包括唯一的交易标识符。同时许 可证包括一唯一的项目标识符，以唯一地识别交易中的至少一个项目上。内容 播发器从网络上接收许可的内容数据，以便用来播放许可的内容数据。内容播 放器根据内容标识符、交易标识符、及项目标识符的数学组合产生一购买标识 符。



ISSN1008-4274

权 利 要 求 书

1. 一种唯一地识别数字内容播放器上数字内容的方法，包含下述步骤:

接收第一标识符，该标识符唯一地识别从内容提供器收到的内容;

接收第二标识符，该标识符唯一地识别内容已被交易接收的交易;

接收第三标识符，该标识符唯一地识别内容已被交易接收的交易中的项目; 及

根据第一标识符、第二标识符和第三标识符的数学组合产生第四个唯一的标识符。

2. 按照权利要求 1 的唯一识别数字内容的方法，其中生成步骤包括根据第一标识符、第二标识符和第三标识符级联生成第四个唯一的标识符。

3. 按照权利要求 1 的唯一识别数字内容的方法，其中接收第二标识符的步骤包括从销售内容的商店中接收一唯一标识符。

4. 按照权利要求 3 的唯一识别数字内容的方法，其中接收第三标识符的步骤包括从销售内容的商店中接收一唯一标识符，唯一地识别内容已被交易接收的交易。

5. 按照权利要求 1 的唯一识别数字内容的方法，还包括下述步骤:

把第四唯一的标识符同包含任何使用条件的内容相结合; 及

在播放内容之前，通过索引第四个唯一的标识符检查使用条件。

6. 按照权利要求 1 的唯一识别数字内容的方法，其中产生第四个唯一的标识符的步骤包括在反篡改环境中产生第四个唯一的标识符，以防止未授权地对其访问。

7. 一种对数字内容在用户设备上的使用进行跟踪的系统，所说的系统包括:

许多内容站点，用以通过计算机可读介质向用户销售数字内容，这里的内容包括与其相关的唯一内容标识符；

许多电子商店，用于向用户授予许可证以播放数字内容数据，每个电子商店连到一网络上，其中的许可证包括唯一交易标识符以唯一地识别交易，同时许可证包含唯一的项目标识符以唯一地识别交易中的至少一个项目；及

许多内容播放器，用于播放内容数据，每个数字内容播放器由用户之一从网络接收授权的数字内容数据，其中的内容播放器根据内容标识符，交易标识符及项目标识符的数学组合产生一购买标识符。

8. 按照权利要求 7 的对数字内容在用户设备上的使用进行跟踪的系统，其中的数学组合是一级联。

9. 按照权利要求 7 的对数字内容在用户设备上的使用进行跟踪的系统，其中的内容播放器包括一反篡改环境，以及在反篡改环境中产生的购买标识符，以防止未授权地对其访问。

10. 一种数字内容播放器，用以唯一地识别数字内容，它包括：

接收第一标识符的装置，该标识符唯一地识别从内容提供器收到的内容；

接收第二标识符的装置，该标识符唯一地识别内容已被交易接收的交易；

接收第三标识符的装置，该标识符唯一地识别内容已被交易接收的交易中的项目；及

根据第一标识符、第二标识符和第三标识符的数学组合产生第四个唯一的标识符的装置。

11. 按照权利要求 10 的唯一地识别数字内容的数字内容播放器，其中的产生装置包括根据第一标识符、第二标识符和第三标识符的级联产生第四个唯一的标识符的装置。

12. 按照权利要求 10 的唯一识别数字内容的数字内容播放器，其中接收第二标识符的装置包括从销售内容的商店接收一唯一标识符。

13. 按照权利要求 10 的唯一识别数字内容的数字内容播放器，其中接收第三标识符的装置包括从销售内容的商店接收一唯一标识符，唯一地识别内容已被交易接收的交易。

14. 按照权利要求 10 的唯一识别数字内容的数字内容播放器还包括：

用以把第四个唯一的标识符同包含任何使用条件的内容相关联的装置；及

在播放内容之前，通过索引第四个唯一的标识符检查使用条件的装置。

15. 一种计算机可读介质，包括在数字内容播放器上唯一地识别数字内容的程序指令，跟踪所包含的指令为：

接收第一标识符，该标识符唯一地识别从内容提供器收到的内容；

接收第二标识符，该标识符唯一地识别内容已被交易接收的交易；

接收第三标识符，该标识符唯一地识别内容已被交易接收的交易中的项目；及

根据第一标识符、第二标识符和第三标识符的数学组合产生第四个唯一的标识符。

16. 按照权利要求 15 的计算机可读介质，其中产生的程序指令包括根据第一标识符、第二标识符和第三标识符的级联产生第四个唯一的标识符。

17. 按照权利要求 15 的计算机可读介质，其中接收第二标识符的程序指令包括从销售内容的商店接收一唯一标识符。

18. 按照权利要求 17 的计算机可读介质，其中接收第三标识符的程序指令包括从销售内容的商店接收一唯一标识符，唯一地识别内容已被交易接收的交易。

19. 按照权利要求 15 的计算机可读介质，还包括的程序指令为：

把第四个唯一的标识符同包含任何用户条件的内容结合起来；及

在播放内容之前，通过索引第四个唯一的标识符检查使用条件。

20. 按照权利要求 15 的计算机可读介质，其中产生第四个唯一的标识符的程序指令包括在反篡改环境中产生第四个唯一的标识符，以防止未授权地对其访问。

说　　明　　书

用于在电子销售系统中
唯一识别顾客购买的方法及设备

本申请是一九九八年十月二十二日提交的第 09/177，097 号申请的部分继续申请，而那个申请又是一九九八年八月十三日提交的第 09/133，519 号申请的部分继续申请。因此，前面的第 09/177，097 号申请的全部公开内容，在此结合于本申请作为参照。

本发明广泛地涉及电子商务领域，尤其是涉及一种用于在 INTERNET 和 WWW 之类的全球通讯网络上面对如打印媒体，电影，游戏和音乐等数字财产进行安全送货和版权管理的系统以及相关工具。

使用诸如 INTERNET 等全球销售系统对如音乐，电影，计算机程序，图片，游戏和其它内容等数字财产的销售仍在持续增长。与此同时，基于以下几个原因，这些宝贵数字内容的所有人和出版商对于使用 INTERNET 销售数字财产却相对缓慢。一个原因是版权所有人对于这些数字内容的非法拷贝和侵权的恐惧。电子传送数字内容为侵权消除了几个障碍。用电子销售消除的一个障碍是它本身需要有形的可记录介质（如软盘或 CD ROM）。向有形介质上拷贝数字内容需要成本，尽管一个空白磁带或可写 CD 的成本通常不到一美元。然而在电子销售中不再需要有形介质。因数字内容是通过电子传送，有形介质的成本不再成为一个因素。另一种障碍是内容本身的形式，也就是以模拟形式存储还是以数字形式存储内容。当以模拟形式存储内容，如一幅打印的图片，通过复印而复制时，拷贝的质量较原件稍差。拷贝的每一个后续拷贝，有时被称为下一代，质量较原件更差。当图片是以数字存储时，这种质量的降级不复存在。每一份拷贝和每一代拷贝都会和原件一样清楚鲜明。完美的数字拷贝以及通过 INTERNET 广泛电子销售所需的极低成本相结合，使非法复制和销售未经授权的

拷贝相对容易。只需按几下键盘，一个侵权者就可以在 INTERNET 上传送成百上千的完美电子拷贝。因此需要对通过电子销售的数字财产的保护和安全有所保障。

数字内容的提供者希望为数字内容建立一个安全的全球性销售系统来保护内容所有者的权益。建立一个数字内容销售系统的问题包括建立用于电子销售数字内容，版权管理，以及财产保护的系统。通过电子销售的数字内容包括的内容如打印媒体，电影，游戏，程序，电视，多媒体和音乐。

建立一个电子销售系统不但可以为数字内容的提供者通过即时出售报告和电子核对提供快速结帐的能力，还通过再销售而增加了收入渠道。由于数字内容的电子销售系统不受实际上缺货和退货的影响，数字内容的提供者和零销商可以降低成本和增加利润。数字内容的提供者可以建立新的或增加现有销售渠道以便于更及时地发行存货。从电子销售系统得到的交易信息可用来获得关于顾客购买模式的信息，还可为电子销售程序和促销提供及时的反馈。为实现这些目标，数字内容的提供者需要使用一个电子销售模型使广大用户及企业获得数字内容，与此同时保证数字财产的保护和计量。

其它可大批供应的数字内容电子销售系统，如 AT&T 的 A 到 B 实时音频，Liquid Audio Pro Corp.的 Liquid Audio Pro, Audio Soft 的城市音乐网络等通过加密和不加密的电子网络提供数字数据的传送。使用加密电子网络大大的限制了数字内容提供者所能销售数字内容的用户。使用如 INTERNET 或 WEB 等不加密网络可以如通过加密使数字内容安全到达用户。然而，一旦加密的数字内容在最终用户的机器上被解码，最终用户可容易地对此数字内容进行未授权再销售。因此，需要一种不但能对数字财产进行保护，而且能在数字内容已被送到消费者或企业之后仍可对内容提供者的权益进行保护的安全的数字内容电子销售系统。因而需要版权管理以便进行安全传送，许可证、授权，以及对数字财产的使用控制。

另一个使数字内容所有人未迅速钟情于电子销售的原因是他们期

望保留并助长现有的销售渠道。大部分数字内容拥有人通过零售商销售。在音乐市场上的美国零售商包括 Tower Records, Peaches, Blockbuster, Circuit City 等。许多这些零售商都有网站，使 INTERNET 用户可以在 INTERNET 上作选择，并将其选择直接寄到最终用户。如音乐网站包括@tower, Music Boulevard 和 Columbia House 。使用电子销售，使零售商能消除自己将其自己与其他电子商区别，及自己和内容所有人区分开，尤其是在 Web 上。因此，在通过电子销售出售音乐时，需要为如图片，游戏，音乐，程序和录像等电子内容的零售商提供一种将其与其它零售店或数字内容所有人区分开的办法。

内容所有人通过如电子商店的销售点准备用于电子销售的数字内容。在 INTERNET 网络上或通过其它在线服务的电子商店，希望通过其商品报价及商品促销，将自己区分出来。一个传统的商店，即非电子，非在线电子商店，通过商品促销，商品削价，商品样品，宽松的退货政策和其它促销手段来使自己从其竞争者中脱颖而出。但是在在线世界上，内容所有者把使用条件放到数字内容上，电子商店区分自己的能力就受到严重限制。此外，即使使用条件可以被改变，电子商店仍面临着一个难题，即处理与来自内容提供者的数字内容相关的元数据以便用电子方法促销和出售商品。在处理元数据时，电子商店需要管理几个要求。首先，电子商店需要从内容提供者接收与数字内容相关的元数据。在很多时候，此元数据的部分必须被加密传送，因而内容提供者必须建立一种为加密内容解密的机制。第二点，电子商店可希望在其接收到来自内容提供者的内容之前或之后，对来自内容提供者的元数据进行预览，以便协助对内容的商品促销，商品定位以及其它促销考虑。第三，电子商店必须从用于促销的物资中提取出某些元数据，例如图形或艺术家的有关信息。通常，这些促销物资被电子商店直接用于其在线促销。第四，电子商店可能会希望通过改进某些允许的使用条件来创造数字内容的不同提供形式，以使自己展露头脚。第五，电子商店可能需要增加或改变元数据中的某些如 URL 的地址，以使购买者的付款调解直接到达一个帐号调解机构，而无需通

过电子商店结款。第六，电子商店将需要为符合使用条件的版权数字内容的合法使用提供许可证。例如，许可证可以允许对数字内容进行有限数量的拷贝。许可证需要反映出所给予的许可的条件和场合。

鉴于以上所有要求，在处理与数字内容相关的元数据时，许多电子商店编写用户化软件程序以解决这些需求。建立这些用户化软件程序往往需要相当的时间，成本和测试。因而需要对这些要求提供一个解决方法。

然而，另一个令数字内容的所有人未能迅速钟情于电子销售的原因是准备用于电子销售的内容的难度。当今，许多内容提供者在其业务中有成千上万的标题。以音乐为例，一个内容提供者往往会同时拥有同一原版录音的不同形式（如 CD，磁带和小形盘）。此外，同一形式的原版录音还有可能为某一特殊销售渠道而再版或重新混音。例如，为电台播放的音带混音就会与歌舞厅的音带混音有所不同，而这两者又可能与一般获得的用户 CD 不同。对这些不同混音进行盘点和编目录会很艰巨。此外，许多原版录音的所有人常重新发行旧的录音，如各种“精选”形式的后续集，为电影所编辑的音乐唱片以及其它收集和编辑形式。随着更多的内容被以数字形式提供，对电子销售的内容进行重新混音和编码的需求也随之增加。在很多场合，提供者需要以旧的录音形式为指导来选择正确的原版录音，并将这些录音重新处理和编码，以便于电子销售的发行。对于那些希望用其旧的录音形式来协助发行，用于电子销售的旧曲目的内容提供者，此问题尤为重要。提供者将要寻找其数据库匹配标题，艺术家和录音，并确定编码参数。这种人工寻找录音档案数据库的过程不无缺陷。一个缺陷是需要一个操作员手工寻找数据库并设置适当的处理参数。另一个缺陷是操作员在从数据库选择数据时有可能出现抄写错误。因此，内容提供者需要一种方法来自动查找与如音频内容相关的数字和原版录音。

内容所有人通过一种叫编码的过程准备其用于电子销售的数字内容。编码包括获得内容，将如果是以模拟形式存在的内容数字化，并将其压缩。压缩处理使通过网络传送并存储于可记录介质的数字内容

更加高效，因为所需传送和存储的数据量被减少。然而，压缩存在其缺陷。大多数压缩会导致部分信息的丢失，被称为有损压缩。内容提供者必须对使用何种算法以及所需的压缩程度作出决定。例如在音乐中，数字内容或歌曲可以随音乐的类型而截然不同。依据一种类型选择的压缩算法和压缩程度对于另一种类型就未必是最佳选择。内容提供者也许会发现某种压缩算法和压缩程度的组合对某类音乐效果甚佳，如古典音乐，但对如重金属的其它类型音乐则效果不佳。此外，音频工程师常需对音乐进行补偿，调节动态范围，并进行其它预处理和处理设置，以保证被编码的这类音乐能提供满意的效果。要求人工对每一数字内容进行编码参数设置，如补偿程度和动态范围的设定可能相当繁琐。再以音乐为例，一个拥有众多不同流派音乐的内容提供者将需要为每一首或每一组需要编码的乐曲人工选择理想的编码参数组合。与此相应，需要解决编码时人工选择处理参数的问题。

内容的压缩过程需要大量专门的计算资源，尤其是如电影全片一类的高容量项目。压缩算法提供者所提供的压缩技术各有其权衡和长处。权衡通常包括：压缩内容所需的时间和计算资源、从原件内容获得的压缩量、重放时的理想位率、被压缩内容的质量效果以及其它因素。使用那些接受输入的多媒体文件并产生编码后的输出文件却不对进度和状态进行任何中间指示的编码软件存在问题。此外，在很多情况下，被用来调用或管理编码程序的其它程序也无进度中间指示。这使调用运行无法测量已编码内容量所占的全部所选的需编码内容的百分比。这对于那些试图同时调度几个不同程序的调用程序是个问题。此外，在大量内容被选择进行编码而内容提供者希望确定编码过程的进度的情况下，这个问题尤为棘手。因此，这些问题需要得以解决。

另一个令数字内容的所有人未能迅速钟情于电子销售的原因是缺乏在最终用户设备上为电子传送内容建立数字播放器的标准。内容提供者，电子商店或其它电子销售链中的环节可能希望在如 PC，顶置盒，手持设备和其它一系列设备上提供用户化的播放器。这就需要一系列的工具以便在反篡改环境下，即一个阻止第三方在播放过程中非

法获得内容的环境，操作数字内容解密。此外，还需要一系列工具，使得在没提供最终用户可使用的未购买的内容时，最终用户能对本地数字内容库进行管理。

内容所有人面对的另一个关于销售电子内容的问题出现在购买同一份内容的多份拷贝的交易中。举例而言，假使一个顾客购买了一首歌或一部电影，并被授权制作一份拷贝。此外，此顾客还决定为一个朋友购买这首歌，但无制作拷贝的授权。对于这首歌的购买人，同一首歌的两份同样拷贝很容易被混淆。这是内容所有人不希望看到的，因为他们将希望搞清对歌曲的每种选择，尤其是对同一首歌。在必须对每首同样歌曲的使用条件进行监测时，就需要追踪歌曲，尤其是同一歌曲。此外，同一歌曲在不同选集或合集中被发行的情况时有发生。例如，同一首歌可以是单曲，一张唱盘或 CD 的一部分，精品集的一部分和合集的一部分。拥有同一歌曲的所有这些不同发行版本使其难以追踪。与此相应，需要一种独特的方法和系统来追踪数字内容，以克服这些问题。

关于保护数字内容的进一步背景信息可从以下三个来源获得。由位于 Florham Park, NJ 的 AT&T 实验室的 Jack Lacy, James Snyder, David Maher 所写的“Music on Internet and the Intellectual Property Protection Problem ”可由 URL 网点 http://www.a2bmusic.com/about/ papers/musicipp.htm 获得。由位于 Sunnyvale,CA 的 InterTrust Technologies Corp. 的 Olin Sibert, David Bernstein 和 David Van Wie 所写“Securing the Content,Not the Wire for information Commerce”一文中的被称为 DigiBox 的密码保护的容器可由 URL 网点 http://www.intertrust.com/architecture/stc.html 获得。另外，IBM 的白皮书“Cryptolope Container Technology”可从 URL 网点 http:///cyptolope.ibm.com/white.htm 获得。

本发明的目的是消除以上所提到的弱点，并提供一用于追踪内容数据使用的系统。本发明的一个实施例提供一个在用户设备上对数字内容的使用进行追踪的系统。通过计算机可读媒介向用户销售数字内

容的内容网站。将独特的内容标识符和与其相关的内容相联系的内容网站；电子商店与网络结合向用户出售播放数字内容数据的许可证。许可证包括一个用于独特鉴别交易的独特的交易标识符，还包括一个用于独特识别交易中至少一个项目的独特的对象标识符。内容播放器从网络接收经许可的内容数据，并被用于播放经许可的内容数据。内容播放器根据内容标识符，交易标识符和对象标识符的数学组合产生一个购买标识符。

图 1 是一方块图，概述了按照本发明的安全数字内容电子销售系统。

图 2 是一方块图，概述了按照本发明的安全容器（SC）的一个例子和与其相关的图示。

图 3 是一方块图，概述了按照本发明对安全容器（SC）进行的加密处理。

图 4 是一方块图，概述了按照本发明的为安全容器（SC）进行的解密处理。

图 5 是一方块图，概述了按照本发明的图 1 中安全数字内容销售系统的版权管理构造层次。

图 6 是一方块图，概述了按照本发明用于图 5 中许可证控制层的内容销售和许可证控制。

图 7 概述了按照本发明的图 1 的工作流程管理工具的一个用户界面的例子。

图 8 是按照本发明，对应于图 7 中用户界面的主要工具，部件和工作流程管理器的过程方块图。

图 9 是描述按照本发明的图 1 中一个电子数字内容商店的主要工具，部件和过程的方块图。

图 10 是描述按照本发明的图 1 中一个最终用户设备的主要元件和过程的方块图。

图 11 是按照本发明的一方法的流程图，以计算图 8 中的内容预处理和压缩工具的编码率因子。

图 12 是按照本发明的一方法的流程图，以自动地检索图 8 中的自动元数据获取工具的附加信息。

图 13 是按照本发明的一方法的流程图，以自动地设置图 8 中的预处理和预处理压缩参数及压缩工具。

图 14 是按照本发明的图 15 所描述的将内容下载到本地库的播放器应用程序的用户界面屏幕例子。

图 15 是一方块图，描述了按照本发明在图 9 的最终用户设备上运行的主要部件和播放器应用程序的过程。

图 16 是按照本发明的图 15 的播放器应用程序的用户界面屏幕例子。

图 17 是按照本发明的作为替代实施例的流程图，以自动检索图 8 中的自动元数据获取工具的附加信息。

图 18 是按照本发明为单独跟踪内容，在最终用户设备 9 上运行的过程流程图。

以下的目录有助于读者在本实施例中很快的寻找不同部分。

Ⅰ. 安全数字内容电子销售系统

A. 系统概述

1. 版权管理
2. 度量
3. 开放体系结构

B. 系统功能部件

1. 内容提供者
2. 电子数字内容商店
3. 中间贸易伙伴
4. 交换所
5. 最终用户设备
6. 传送基础设施

C. 系统的使用

Ⅱ.密码术概念及它们在安全数字内容电子销售系统中的应用

A. 对称算法

B. 公共密钥算法

C. 数字签名

D. 数字认证

E. 引导 SC 的图形表示

F. 安全容器加密例

Ⅲ 安全数字内容电子销售系统流程

Ⅳ 版权管理体系结构模式

A. 体系结构层次功能

B. 功能划分及流程

1. 内容格式层

2. 内容使用控制层

3. 内容标识层

4. 许可证控制层

C. 内容销售及许可证控制

Ⅴ 安全容器结构

A. 一般结构

B. 版权管理语言的语法和语义

C. 安全容器流性及处理的概述

D. 元数据安全容器 620 格式

E. 报价安全容器 641 格式

F. 交易安全容器 640 格式

G. 订单安全容器 650 格式

H. 许可证安全容器 660 格式

I. 内容安全容器格式

Ⅵ 安全容器的打包和解包

A. 概述

B. 物资（BOM）部分的帐单

C. 关键描述部分

Ⅶ 交换所

A. 概述

B. 版权管理处理

C. 国家指定的参数

D. 核查记录及跟踪

E. 结果报告

F. 帐单和支付核实

G. 再传输

Ⅷ 内容提供者

A. 概述

B. 工作流管理器

1. 产生等待动作/信息过程
2. 新内容请求过程
3. 自动元数据请求过程
4. 手工元数据输入过程
5. 用户条件过程
6. 监督发行工具
7. 元数据 SC 创建过程
8. 加水印过程
9. 预处理和压缩过程
10. 内容质量控制过程
11. 加密过程
12. 内容 SC 创建过程
13. 最终质量保证过程
14. 内容分散过程处理
15. 工作流规则

C. 元数据吸收和输入工具

1. 自动元数据获取工具
2. 手动元数据输入工具

3. 使用条件工具

4. 元数据 SC 的部件

5. 监督发行工具

D. 内容处理工具

1. 水印工具

2. 预处理和压缩工具

3. 内容质量控制工具

4. 加密工具

E. 内容 SC 创建工具

F. 最后质量保证工具

G. 内容分发工具

H. 内容促销 Web 站点

I. 内容托管

1. 内容托管站点

2. 由安全数字内容的电子销售系统提供的内容托管站点

IX 电子数字内容商点

A. 概述---支持多个电子数字内容商点

B. 点到点电子数字内容销售服务

1. 集成需求

2. 内容获取工具

3. 交易处理模块

4. 布告界面模块

5. 帐户调解工具

C. 广布电子数字内容销售服务

X 最终用户装置

A. 概述

B. 应用程序安装

C. 安全容器处理器

D. 播放器应用程序

1. 概述

2. 最终用户接口部件

3. 拷贝/播放管理部件

4. 解密 1505，解压缩 1506 及回放部件

5. 数据管理 1502 及库访问部件

6. 内部应用通信部件

7. 其他混合部件

8. 一般播放器

I.安全数字内容电子销售系统

A. 系统综述

安全数字内容电子销售系统是一个技术平台，它包括技术，规范，工具，将数字内容和与数字内容相关的内容安全发送到最终用户并管理版权所需的软件，以及用户设备。最终用户设备包括 PC，顶置盒（IRD）和网络设施。这些设备可将内容拷贝至经内容所有者允许的外部介质或可携带的顾客设备。术语“数字内容”或简单的“内容”是指包括图片，电影，录像，音乐，程序，多媒体和游戏在内的以数字形式存储的信息和数据。

技术平台详细说明如何准备数字内容，通过点对点和广播基础设施（如电缆，网络，卫星和无线设备）安全地将数字内容转送并授权给最终用户设备，且保护其不被非法拷贝或播放。此外，此技术平台的结构可集成和移植不断衍化过程中的多种技术，如加水印，压缩/编码，加密以及其它安全算法等。

安全数字内容电子销售系统的基本部分是:（1）版权管理以保护内容所有人的所有权;（2） 交易度量以迅速准确地进行偿付; 和（3）一个公开并详细引证的结构，使得内容提供者能准备内容，并允许内容通过多种网络基础设施安全发送，以便在任何标准兼容播放器上重播。

1. 版权管理

安全数字内容电子销售系统中版权管理的实现是通过分布于系统操作部件中的一系列功能。其主要功能包括：授予并控制许可证以使内容只能被已授权的中介或确有许可证的最终用户打开；依据购买条件或许可证条件对内容的使用进行控制和执行，如允许拷贝的数量，播放次数，以及许可证的有效期限或条件。版权管理的第二个功能是启用一种鉴别未经授权的内容拷贝来源的方法，以抗击盗版。

许可证的授权和控制是通过使用一个交换所实体和安全容器（SC）技术实现的。交换所使中介或最终用户在经过核实许可交易的顺利完成后能够打开内容，从而提供许可证授权。安全容器被用于在系统部件之间发送已加密的内容和信息。SC 是信息和内容的一个密码携带器，用于那些使用加密，数字签名，和数字证书以提供保护防止电子信息和内容受非法拦截或对其进行改动。SC 还允许对数字内容的真实性和完整性进行核实。这些版权管理功能的优点在于无需安全可信的电子数字内容销售的基础设施。因而可以通过如 WEB 和 INTERNET 的网络基础设施进行传送。这是由于内容是在安全容器内被加密的，而内容的存储和销售是与其打开和使用是被分开的。只有那些有解密密钥的用户才能够打开被加密的内容，而交换所只对经授权的适当使用要求授予解密密钥。交换所不会对来自不明或未经授权方或与内容所有人制定的使用条件不符的假冒要求予以放行。此外，如果 SC 在发送过程中被篡改，交换所中的软件就会确定 SC 中的内容已被破坏或伪造，并拒绝交易。

内容使用的控制是通过在最终用户设备上运行的最终用户播放器应用程序 195 来实行的。此应用程序在内容的每份拷贝中嵌入一个数字码以定义允许的二级拷贝数量和重播次数。数字水印技术被用来产生数字码，对其它最终用户播放器应用程序 195 为不可见，以使其能抵御篡改试图。在另一实施例中，数字码仅作为与内容 113 相应的使用条件的一部分而被保留。当数字内容 113 在一兼容的最终用户设备中被存取时，最终用户播放器应用程序 195 读水印以检查使用限制并根据需要更新水印。如果对内容的使用要求与使用条件不符，例如

允许的拷贝数已被用尽，最终用户设备则不执行要求。

数字水印还提供了用于鉴别已授权或未授权内容的来源的方法。内容的起始水印由内容所有人嵌入、以鉴别内容所有人、阐明版权信息、定义地理销售区域以及加入其它相关信息。二次水印在最终用户设备上被嵌入内容中，以识别内容的购买人（或被授权人）和最终用户设备，说明购买或授权条件和日期，并加入其它相关信息。

由于水印成为了内容的一组成部分，无论拷贝是否被授权，它们都被携带于拷贝中。因此，无论数字内容在何处或从何而来，它们永远包含关于其来源和其许可使用的信息。此信息可被用于抗击内容的非法使用。

2. 度量（METERING）

作为版权管理功能的一部分，交换所对通过交换所密钥交换理清的所有交易留有记录。此记录允许对许可证授权和使用的最初条件进行度量。交易记录可被即时或周期性的报告给负责人方，如内容所有人或内容提供者，零售商和其他，以协助交易付款的电子调解和其它用途。

3. 开放（OPEN）结构

安全数字内容电子销售系统是一具有已发表的规范和界面的开放结构，以在维持对内容所有人权益的保护同时促进此系统在市场上的广泛应用与认可。系统结构的灵活性和开放性还使系统能够随着各种技术，发送基础设施和设备发展被投入市场。

内容的性质和它的格式其结构是的开放的。音乐，程序，多媒体，录像或其它形式内容的销售受此结构所支持。内容可以是以原来形式，如数字音乐的线性 PCM，或是以经过附加的预处理或编码而得到的形式，如过滤，压缩，或预加重/去加重（PRE/DE-EMPHASIS）及其它。结构对于各种加密和水印技术开放。这样就可以选择特定技术以迎合不同的内容类型和形式，并可随着新技术的发展将之引入或采用。这种灵活性使得内容提供者能在安全数字内容电子销售系统内挑选和发展这些用于数据压缩，加密和格式化的技术。

结构还对不同的销售网络和销售模型开放。结构支持通过低速网络连接或高速卫星和电缆网络的内容销售，并可被用点对点或广播型式。此外，结构的设计使得最终用户设备的功能可以在一系列不同设备上使用，包括低成本顾客设备。这种灵活性使内容提供者和零售商能通过一系列不同服务选项向中介或最终用户提供内容，并使用户能购买或被许可内容，重新播放，并将其录于多种兼容播放器设备上。

B. 系统功能元素

翻到图 1，所示的是一描述依据本发明的安全数字内容电子销售系统 100 总体的框图。安全数字内容电子销售系统 100 包含由端到端解决方案构成的几个商业单元，包括：内容提供者 101 即数字内容的所有人，电子数字内容商店 103，中介市场伙伴（未显示），交换所 105，内容托管站 111，发送基础设施１０７和最终用户设备１０９。 这些商业元素中的每一个使用安全数字内容电子销售系统 100 中的不同部件。对这些商业单元和系统部件的高一级描述请见后，它们特别与电子内容１１３销售有关系。

１． 内容提供者１０１

内容提供者１０１或内容所有人是原始内容１１３的拥有者和／或被授权打包独立内容１１３的授权者，以便再出售的销售商。 内容提供者１０１可以直接使用其版权，或将内容１１３授权于电子数字内容商店１０３或中介市场伙伴（未显示），通常以获得与电子商业收入相关的内容使用付款。 内容提供者的例子包括 Sony, Time-Warner, MTV, IBM, Microsoft, Turner, Fox 及其它。

内容提供者１０１使用被作为安全数字内容电子销售系统 100 的一部分而提供的工具来准备他们的内容１１３和相关数据以便销售。工作流程管理工具１５４安排对内容１１３的处理，并跟踪内容１１３流经内容１１３准备和包装中各步时，以维持高质量的保证。术语“元数据”将在本文件全文中使用，用于指与内容１１３相关的数据，且在此实施例中不包括内容１１３本身。 举例而说，一首歌的元数据可以是一歌名或歌评（ＣＲＥＤＩＴ），但不是歌的声音录音。内

容113将包括声音录音。一个元数据吸收和输入工具161被用于从内容提供者数据库160或由内容提供者以一指定形式（对于音乐例内容113信息如CD标题，艺术家名字，歌曲题目，CD工艺品等）提供的数据中提取元数据，并将其包装以便电子销售。元数据吸收和输入工具 161 也被用于为内容 113 输入使用条件。使用条件中的数据包括拷贝限制规则、批发价格和任何被认为需要的商业规则。一个水印工具被用来隐藏内容 113 中用于鉴别内容所有人、处理日期和其它相关数据。对于一个内容 113 是音乐的实施例，一个音乐预处理器工具被用来调节动态和/或均衡内容 113 或其它音乐，以获得最佳压缩质量，将内容 113 压缩到理想的压缩级别，并对内容 113 加密。这些可适应如下数字内容压缩/编码、加密和格式化方法中的技术进步，从而使内容提供者 101 能在市场上，在工具发展的同时使用最佳工具。

加密的内容 113、数字内容相关的数据或元数据和已加密的密钥，由 SC 打包工具打包于 SC 中（描述见下），并被贮存于一内容托管网站和/或促销站点，以便于电子销售。内容托管站点可位于内容提供者 101 中或多个位置，包括电子数字内容商店 103 和中介市场伙伴（未显示）设施。由于内容 113 和密钥（描述见下）都是在 SC 中被加密和打包，电子数字内容商店 103 或其它托管代理不能在未经交换所许可和通知时向内容提供者 101 直接访问已解密的内容 113。

2. 电子数字内容商店 103

电子数字内容商店 103 是通过一系列广泛服务和应用，如内容 113 的主题设计或内容 113 的电子商品推销，来对内容 113 进行市场促销的实体。电子数字内容商店 103 管理其服务的设计，开发，业务操作，结算，商品推销，市场促销和销售。在线电子数字内容商店 103 的例子是提供软件电子下载的 Web 站点。

通过它们的服务，电子数字内容商店 103 执行安全数字内容电子销售系统 100 的某些功能。电子数字内容商店 103 从内容提供者 101 搜集信息，在附加的 SC 中打包内容和元数据，并将那些 SC 作为其服务或应用的一部分交付给顾客或企业。电子数字内容商店 103 运用

安全数字内容电子销售系统 100 所提供的工具来协助元数据提取、二级使用条件、SC 包装、以及对电子内容交易的跟踪。二级使用条件数据可包括零售企业的报价，如内容 113 的购买价格，每次播放的价格，拷贝授权和目标设备类型，或对可能的时间限制。

一旦电子数字内容商店 103 完成一个来自最终用户的对电子内容 113 的合法要求，电子数字内容商店 103 就负责授权交换所 105 向顾客发出内容 113 的解密密钥。电子数字内容商店还授权对包含内容 113 的 SC 的下载。电子数字内容商店可以选择在其本地站点托管含有数据内容的 SC，并/或利用另一个内容托管站点的托管和销售设施。

电子数字内容商店可使用安全数字内容电子销售系统 100 对最终用户有可能存在的任何提问和问题提供顾客服务或电子数字内容商店 103 也可将其顾客服务支持契约给交换所 105。

3. 中介市场伙伴（未显示）

在另一实施例中，安全数字内容电子销售系统 100 可被用来将内容 113 安全的提供给被称为中介市场伙伴的其它企业。这些伙伴可以包括销售内容 113 提供非电子服务的与数字内容有关的公司，如电视台或录像俱乐部，电台或唱片俱乐部。这些伙伴还可包括其它可信赖团体，它们管理在制作或促销音乐录音中物资，如唱片演播室、复制商或制作人。这些中介市场伙伴要获得交换所 105 的批准，以便对内容 113 解密。

4. 交换所 105

交换所 105 对所有涉及销售和/或对 SC 中加密的内容 113 的许可证使用的交易提供许可证授权的并备案。当交换所 105 从一中介或最终用户收到对内容 113 的解密密钥的要求时，交换所 105 对此要求中信息的完整性和真实性进行核实，确认此要求已由电子数字内容商店或内容提供者 101 授权，并确认所要求的使用与由内容提供者 101 所定义的内容使用条件相符合。一旦这些核实被满足，交换所 105 给提出要求的最终用户送去打包在一许可证 SC 中的内容 113 的解密密钥。此密钥以一种方式被加密，使得只有经授权的用户才能获得。如果最

终用户的要求未被核实、完成或授权，交换所 105 则拒绝对解密密钥的要求。

交换所 105 对所有交易留有记录，并可将记录瞬时、周期性或有限制地报告给负责人方，如电子数字内容商店 103 和内容提供者 101。通过这种报告方式，内容提供者 101 可以被通知到内容 113 的出售，且电子数字内容商店 103 可以获得电子发送至其顾客的核查踪迹。交换所 105 如果检测出 SC 中信息已危及安全或与内容的使用条件不符，还可通知内容提供者 101 和/或电子数字内容商店 103。交换所 105 数据库的交易记录和仓库容量是为数据挖掘和报告产生而构造的。

在另一实施例中，交换所 105 可为交易提供顾客支持和例外理，如退款、发送失败和购买纠纷。交换所 105 可被作为一个独立实体操作，为版权管理和计量提供一个可以信赖的管理角色。它还可根据需要提供帐单和结算。电子交换所的例子包括 Secure-Bank.com 和来自 Visa/Mastercard 的安全电子交易（SET）。在一个实施例中，交换所 105 是可以对最终用户设备 109 访问的 WEB 站点。在另一实施例中，交换所 105 是电子数字内容商店 103 的一部分。

5. 最终用户设备 109

最终用户设备 109 可以是含有一与安全数字内容电子销售系统 100 的指标相兼容的最终用户播放器应用程序 195（见后述）的任何播放器设备。这些设备可以包括 PC，顶置器（IRD）和网络设施。最终用户应用程序 195 可以软件和/或顾客电子硬件实现。除进行播放，录制和库管理功能外，最终用户播放器应用程序 195 还进行 SC 处理，以便于最终用户设备 109 中的版权管理。最终用户设备 109 管理对含有数字内容的 SC 的下载和存储；要求和管理来自交换所 105 的加密数字内容密钥的收据；每当数字内容被拷贝或播放时处理水印；根据数字内容的使用条件管理所制作（或删除）的拷贝数量；并在允许时向外部介质或可携带顾客设备进行拷贝。可携带顾客设备可以执行最终用户应用程序 195 功能中的一个子集，以便处理加在水印中的内容使用条件。术语“最终用户”和“最终用户播放器应用程序 195”将在

本文中被广泛使用，表示贯穿在一个最终用户设备 109 上的使用或运行。

6. 发送基础设施 107

安全数字内容电子销售系统100独立于连接电子数字内容商店103和最终用户设备 109 的发送网络。它同时支持例如 INTERNET 的点对点和例如数字广播电视的广播销售模式。

尽管通过不同发送基础设施 107 进行的对内容 113 的获取、打包和追踪是由同样的工具和应用程序完成的，将服务送至顾客所用的表示和方法可根据所选基础设施和销售模型而有所不同。所被发送的内容 113 的质量也可能有所不同，因为高带宽的基础设施比之较低带宽的基础设施能以更易被接受的响应时间发送高质量的数字内容。一个为点对点销售模式设计的服务应用程序也可被适应于支持一广播销售模式。

C. 系统使用

安全数字内容电子销售系统 100 使之能够将内容 113 的高质量电子拷贝安全发送到顾客或企业的最终用户设备 109，并对内容 113 的使用进行控制和追踪。

安全数字内容电子销售系统 100 可以使用新的和现有的销售渠道在各种顾客和企业对企业服务中展开。每一种特别服务都可使用由安全数字内容电子销售系统 100 的版权管理特色所推行的不同金融模型。例如批发或零售、每次都需付款的使用、订阅服务、拷贝/无拷贝限制或再销售等模型可以通过交换所 105 的版权管理和最终用户播放器应用程序 105 的拷贝保护特性得以实现。

安全数字内容电子销售系统 100 在建立用于出售内容 113 的服务方面给予了电子数字内容商店 103 和中介市场伙伴极大的灵活性。与此同时，它为内容提供者 101 提供了相当程度的保证，使他们的数字资产得到保护，从而使他们能对内容 113 的颁发许可证得到适当的补偿。

II. 密码系统的概念及其在安全数字内容电子销售系统中的应用

安全数字内容电子销售系统 100 中的许可证控制是基于密码系统的使用。此节介绍本发明的基本密码系统技术。公共密钥加密、对称密钥加密、数字签名、数字水印和数字证书的使用已为人所知。

A. 对称算法

在安全数字内容电子销售系统 100 中，内容提供者 101 使用对称算法对内容进行加密。它们被称为对称算法是因为同一密钥被用于加密和解密。数据的发送者和信息的接收者必须共享此密钥。此共享密钥在此被称为对称密钥。安全数字内容电子销售系统 100 的结构独立于为某一特定工具选择特定对称算法。

常见的对称算法有 DES，RC2 和 RC4。DES 和 RC2 都是块状密码（BLOCK CIPHER）。块状密码在加密数据时每次使用一位数据块。DES 是美国政府的官方密码标准，具有 64 位的块尺寸，并使用一 56 位的密钥。三重 DES 通常被使用，以获得比单重 DES 更高的安全程度。RSA 数据安全部设计了 RC2。RC2 使用一个可变密钥尺寸密码，并拥有 64 位的块尺寸。RC4 也是由 RSA 数据安全性设计的，是一个可变密钥尺寸的流密码。流密码每次对单个位数据操作。RSA 数据安全性宣称，每一个 RC4 输出字节需要 8 到 16 次机器操作。

IBM 设计了一种叫做 SEAL 的快速算法。SEAL 是一种流算法，它使用一个曾为 32 位处理器优化过的可变长度密钥。SEAL 对每字节需要大约五个基本机器指令。如果所使用的 160 位的密钥以被预处理到内部表中，50 兆赫的 486 计算机则可以每秒 7.2 兆字节的速度运行 SEAL 码。

微软公司在其 CryptoAPI 文件的综述中报告了加密操作的结果。这些结果是通过使用微软公司的 CryptoAPI 在一台配有 Windows NT4.0 的 120 兆赫奔腾机上应用而得到的。

密码	密钥尺寸	密钥启动时间	加密速度
DES	56	460	1,138,519
RC2	40	40	286,888
RC4	40	151	2,377,723

B. 公共密钥算法

在安全数字内容电子销售系统 100 中，对称密钥和其它小数据片段以公共密钥加密。公共密钥算法使用两个密钥。这两个密钥在数学上相关联，使得用其中一个密钥加密的数据只能以另一个密钥解密。密钥的所有者对一个密钥私人（PRIVATE）保存（私人密钥），而第二个密钥被公开销售（公共密钥）。

为保证使用公共密钥算法传送绝密消息的安全，必须使用接收人的公共密钥对此消息进行加密。只有拥有与之对应的私人密钥的接收人才可对消息解密。公共密钥还被用于产生数字签名。私人密钥被用于此目的。下一节将提供关于数字签名的信息。

最常用的公共密钥是 RSA 公共密钥密码。它已成为工业界中的事实上的公共密钥标准。其它对于加密和数字签名效果良好的算法有 ElGamal 和 Rabin。RSA 是一可变密钥长度密码。

对称密钥算法要比公共密钥算法快很多。以软件实现，DES 通常比 RSA 快至少一百倍。由于这个原因，RSA 不被用来加密海量数据。RSA 数据安全部报告说，在一般 90 兆赫的奔腾机上，RSA 数据安全部的工具箱 BSAFE 3.0 在 512 位模数时对私人密钥操作（使用私人密钥加密或解密）的吞吐量为 21.6 千位/秒，在 1024 位模数时吞吐量为 7.4 千位/秒。

C. 数字签名

在安全数字内容电子销售系统 100 中，SC 的发行者通过对 SC 数字签名来保护其完整性。一般来说，为了产生一个消息的数字签名，消息的所有者首先计算消息摘要（定义见下），然后用所有者的私人密钥对消息加密。消息被与其签名一起被销售。任何收到消息的人可以通过使用消息所有者的公共钥匙对签名解密以重现消息摘要来对数字签名先加以核实。之后，接收人计算所收到的消息摘要，并将其与重现的摘要相比较。如果消息在销售中未被篡改，计算出的摘要应与重现的摘要相同。

在安全数字内容电子销售系统 100 中，由于 SC 包含几个数据部分，对每一部分计算出一个摘要，并对级联的部分摘要计算出一个汇总摘要。汇总摘要以 SC 发行人的私人密钥被加密。被加密的汇总摘要就是发行人对 SC 的数字签名。部分摘要和数字签名被包含在 SC 的主体中。SC 的接收人可以通过接收到的数字签名和部分摘要来核实 SC 和其各部分的完整性。

一个单向散列算法被用来计算消息摘要。散列算法将一可变长度输入消息转换成一固定长度串，即消息摘要。单向散列算法只有一个操作方向。也就是说，很容易对输入的消息计算摘要，但很难（计算上不可能）由其摘要产生输入消息。由于单向散列函数的性质，可以认为消息摘要是一个消息的指纹。

更常见的单向散列 函数有来自 RSA 数据安全部的 MD5 和美国国家技术标准局（NITS）设计的 SHA。

D. 数字证书

数字证书被用于鉴别或核实一个发出经数字签名的消息的个人或实体的身份。证书是一由证书授权处发出的、将一公共密钥交与个人或实体的数字文件。证书包括公共密钥、个人或实体的名称、失效日期、证书授权处的名称以及其它信息。证书还包括证书授权处的电子签名。

当一个实体（或个人）发出一份经私人密钥签名并伴有其数字证书的消息时，消息的接收人利用来自证书的实体名称来决定是否接受此消息。

在安全数字内容电子销售系统 100 中，除了那些由最终用户设备 109 发行的 SC 外，每个 SC 都包括 SC 产生者的证书。最终用户设备 109 无需在其 SC 中加入证书，因为许多最终用户不愿费心获得证书或具有非善意证书授权处发行的证书。在安全数字内容电子销售系统 100 中，交换所 105 可以决定是否向电子数字内容商店 103 发证书。这使得最终用户设备 109 能够独立地核实电子数字内容商店是否已经过安全数字内容电子销售系统 100 的授权。

E. SC 图形表示指南

此文件使用绘制图形表示 SC，它显示加密部分、未加密部分、加密密钥和证书。现在，参见图 2，它是 SC200 的一幅代表图示。下面的符号被用于 SC 图中。密钥 201 可以是一私人或公共密钥。密钥的齿如交换所的 CLRNGH，指示密钥的所有者。PB 在把手内显示其为一公共密钥，因此密钥 201 是交换所的公共密钥。PV 在把手内则指示其为一私人密钥。菱型是一最终用户数字签名 202。缩写(initial)指示出哪一个私人密钥被用于产生签名，因而 EU 就是来自下表的最终用户数字签名。对称密钥 203 被用来给内容加密。一个经加密的对称密钥对象 204 包括一个以 CLRNGH 的 PB 来加密的对称密钥 203。在长方形上边界上的密钥是用于给对象加密的密钥。长方形中的符号或文字指示被加密的对象（在此例中是一对称密钥）。另一个被加密对象，在此例中显示的是一交易 ID 加密对象 205。还有用于下述的内容许可证管理的使用条件 206。SC200 包括使用条件 206、交易 ID 加密对象 205、应用 ID 加密对象 207 和加密的对称密钥对象 204，全都签有最终用户数字签名 202。

下面的表格显示了缩写以识别 SC 签名者身份的。

缩写	成分
CP	内容提供者 101
MS	电子数字内容商店 103
HS	内容托管站点 111
EU	最终用户设备 109
CH	票据交换所 105
CA	证书授权机关（未显示）

F. 安全容器加密的例子

下面的表格和图示提供了用于从 SC 建立和重现信息的加密和解密过程的综述。在此过程综述中被建立和解密的 SC 是一个一般性的 SC。它不代表安全数字内容电子销售系统 100 中用于版权管理的任何特定的 SC。此过程包括图 3 加密过程中描述的步骤。

图 3 的加密过程的过程流程

步骤过程

301 发送人产生一随机对称密钥并用其对内容加密。

302 发送人通过一散列 算法运行已加密内容以产生内容摘要。

303 发送人用接收人的公共密钥给对称密钥加密。PB RECPNT 指接收人的公共密钥。

304 发送人通过与第二步中使用的同一散列算法，运行被加密的对称密钥，以产生对称密钥摘要。

305 发送人通过与第二步中使用的同一散列算法运行内容摘要的级联和对称密钥摘要，以产生 SC 摘要。

306 发送人用发送人的私人密钥对 SC 的摘要加密，以便为 SC 产生数字签名。PV SENDER 指发送人的私人密钥。

307B 发送人产生一 SC 文件，它包括已加密的内容、已加密的对称密钥、内容摘要、对称密钥摘要、发送人的证书和 SC 签名。

307A 发送人必须在开始安全通信之前，从一证书授权处获得证书。证书授权处在其证书中包括发送人的公共密钥和发送人的名称，并对其签名。PV CAUTHR 指证书授权处的私人密钥。发送人将 SC 发给接收人。

图 4 的解密过程的过程流程

步骤过程

408 接收人收到 SC 并分离其各部分。

409 接收人通过使用证书授权处的公共密钥对其解密，以核实发送人证书中的数字签名。如果证书中的数字签名是合法的，接收人获得来自证书的发送人的公共密钥。

410 接收人用发送人的公共密钥对 SC 数字签名进行解密。此过程重现 SC 摘要。PB SENDER 指发送人的公共密钥。

411 接收人通过与发送人用于计算 SC 摘要的同一散列算法来运行所接收的内容摘要的级联和加密的密钥摘要。

412 接收人把计算出的 SC 摘要与从发送人的数字签名中重现的摘要相比较。如果它们相同，接受人确认收到的摘要从未被更改，并继续其解密过程。如果它们不同，接收人丢弃此 SC 并通知发送人。

413 接收人通过步骤 411 中用于计算对称密钥摘要的同一散列算法运行加密的对称密钥。

414 接收人把计算出的对称密钥摘要与从 SC 中收到的摘要相比较。如果相同，接收人则知道加密的对称密钥从未被更改。接收人继续其解密过程。如果不同，接收人丢弃此 SC 并通知发送人。

415 接收人通过步骤 411 中用于计算内容摘要的同一散列算法运行加密的内容。

416 接收人把计算出的内容摘要与从 SC 中收到的摘要相比较。如果相同，接收人则知道加密的内容从未被更改。接收人继续其解密过程。如果不同，接收人丢弃 SC 并通知发送人。

417 接收人使用接收人的私人密钥对加密的对称密钥解密。此步重现对称密钥。PV RECPNT 指接收人的私人密钥。

418 接收人使用对称密钥对加密的内容解密。此步重现内容。

III. 安全数字内容电子销售系统流程

安全数字内容电子销售系统 100 包含几个被系统的不同参与者使用的部件。这些参与者包括内容提供人 101、电子数字内容商店 103、通过最终用户设备 109 的最终用户以及票据交易所 105。一高级别系统流程被用以综述安全数字内容电子销售系统 100。下面所示的流程可在内容流经系统 100 时，对其追踪。此外，它简述了参与者用来进

行购买交易、打开、和使用内容 103 所用的步骤。系统流程中所作的一些假设包括:

● 这是一个用于数字内容服务（点对点界面到 PC）的系统流程。

● 内容提供人 101 以 PCM 未经压缩形式提交音频数字内容(作为一音乐音频的例子)。

● 内容提供人 101 在 ODBC 兼容数据库内具有元数据，或内容提供人 101 将把数据直接加到内容信息处理子系统中，或将以指定的 ASCII 文件格式提供数据。

● 财务结算由电子数字内容商店完成。

● 内容 113 由一个单一内容托管站 111 托管。

那些对此行业熟悉的人应当明白，这些假设可以被更改以迎合数字内容的确切本性，如音乐、录像和程序以及电子销售系统广播。

下面的过程流程如图 1 所示。

步骤过程

121 一个未经压缩的 PCM 音频文件被内容提供者 101 作为内容 113 而提供。其文件名以及内容 113 的内容提供者 101 的独特标识符一同被输入到工作流程管理工具 154。

122 使用内容 113 的内容提供者 101 的独特标识符和由数据库映射模板，元数据被内容信息处理子系统从内容提供者的数据库 160 获取。

123 工作流程管理工具 154 被用于引导内容在内容提供者 101 处流经获取和准备过程。它还可被用于在任何时候对任意一个内容的状态进行追踪。

124 内容 113 的使用条件被加入内容信息处理子系统。这可以通过人工或自动进行。此数据包括拷贝限制规则和任何被认为是需要的其它商业规则。所有的元数据输入可以与数据的音乐处理平行进行。

125 水印工具被用来在内容 113 中隐藏内容提供者 101 认

为是鉴别内容所需的数据。这包括它是被何时获得的、它来自何方（此内容提供者 101）、或其它任何由内容提供者 101 指定的信息。

- 内容处理工具 125 根据所支持的不同压缩级别的需要对内容 113 进行均衡、动态调节和再取样。

- 内容 113 被使用内容处理工具 125 压缩至理想的压缩级别。内容 113 即可被再播放以确认压缩产生了所需的内容 113 质量级别。如果需要，均衡、动态调节、压缩和再播放质量检测可根据需要进行任意多次。

- 内容 113 和其元数据的一个子集被 SC 打包器以一对称密钥加密。此工具然后使用交换所 105 的公共密钥对密钥加密，以产生加密的对称密钥。此密钥可以在任何地方被传送而不会危及内容 113 的安全，因为唯一可对其解密的实体是交换所 105。

126 加密的对称密钥、元数据和其它与内容 113 相关的信息被 SC 打包器工具 152 打包到一个元数据 SC 内。

127 经加密的内容 113 和元数据被打包到一个内容 SC 内。此时，对内容 113 和元数据的处理全部完成。

128 然后元数据 SC 使用内容支付工具（未显示）被发送到内容促销 Web 站点 156。

129 内容支付工具将内容 SC 送至内容托管网点 111。内容托管网点 111 可以驻留于内容提供者 101、交换所 105 或由内容托管所指定的一特殊地点。此网点的 URL 是被加到元数据 SC 中的元数据的一部分。

130 内容促销 Web 网点 156 通知电子数字内容商店 103，新内容 113 被加到系统 100 中。

131 通过使用内容获取工具，电子数字内容商店 103 将与他们想出售的内容 113 相对应的元数据 SC 下载。

132 电子数字内容商店将使用内容获取工具从元数据 SC

中把他们希望用来在其网点促销内容 113 的任何数据提出。如果需要，可对存取此元数据的部分进行保安和收费。

133 对此电子数字内容商店 103 特定的内容 113 的使用条件通过使用内容获取工具而被输入。此使用条件包括对内容 113 的不同压缩级别的零售价和拷贝/播放限制。

134 电子数字内容商店 103 的特定使用条件和最初的元数据 SC 被 SC 打包工具打包到一个报价 SC 内。

135 在电子数字内容商店 103 的网点被更新后，内容 113 即可供上网的最终用户浏览。

136 当一个最终用户发现他/她想要购买的内容 113 后，他/她点击一个内容图标，如一音乐图标，此物品即被放入由电子数字内容商店 103 所维护的他/她的购物车中。当最终用户完成购物时，他们向电子数字内容商店 103 提交一个购买要求以供处理。

137 电子数字内容商店 103 然后与信用卡结算机构联系，以和其当今商业活动的同样方式对资金进行暂时掌管（PLACE A HOLD）。

138 一旦电子数字内容商店 103 收到从信用卡结算机构返回的信用卡授权号，它便将此号存入数据库并调用一 SC 打包工具以建立一个交易 SC。此交易 SC 包括最终用户所购买的内容 113 的所有报价 SC，一个可以追踪回电子数字内容商店 103 的交易 ID，以及可用于鉴别最终用户、压缩级别、使用条件和所购买歌曲的价格清单的信息。

139 交易 SC 然后被传送到最终用户设备 109。

140 当此交易 SC 到达最终用户设备 109 时，它断升最终用户播放器应用程序 195，最终用户播放器应用程序 195 则打开交易 SC 并确认最终用户的购买。最终用户播放器应用程序 195 然后打开每一个报价 SC，并且在另一可选实施例中，可以通知用户估算的下载时间。之后，它要求用户指出用户想在何

时下载内容 113。

141 根据最终用户所要求的下载时间，最终用户播放器应用程序 195 通过建立一订单 SC 被唤醒并启动下载过程，订单 SC 包括内容 113 的加密对称密钥、交易 ID、和最终用户信息以及其它之中。

142 此订单 SC 被发送到交换所 105 以便处理。

143 交换所 105 接收订单 SC，将其打开，并核实所有数据均未经篡改。交换所 105 验证最终用户所购买的使用条件。这些使用条件必须与那些由内容提供者 101 所指定的相吻合。此信息被记载（LOG）入数据库。

144 一旦所有的核对都已结束，被加密的对称密钥即通过使用交换所 105 的私人密钥而被解密。对称密钥然后使用最终用户的公共密钥被加密。这个新被加密的对称密钥然后被 SC 打包器打包到一个许可证 SC 内。

145 许可证 SC 然后被传送到最终用户。

146 许可证 SC 在被最终用户设备 109 收到后被存储于存储器中，直到内容 SC 被下载。

147 最终用户设备 109 要求从内容托管设施 111 发送所购内容 113 的相应执照 SC。

148 内容 113 被送到最终用户设备 109。在接收后，内容 113 被最终用户设备 109 通过使用对称密钥解密。

IV. 版权管理结构模型

A. 结构层次功能

图 5 是一安全数字内容电子销售系统 100 的版权管理结构方块图。从结构上来说，代表安全数字内容电子销售系统 100 的四个层次是：许可证控制层 501、内容标识层 503、内容使用控制层 505 和内容格式化层 507。每一层的总体功能目的和每一层的单个主要功能将在此节中描述。每一层中的功能都完全独立于其它层中的功能。在较宽的限制范围中，一层中的功能可以由类似功能替换而不会影响到其

它层的功能性。显然，一个层的输出必须满足相邻层所能接受的格式和语义。

许可证控制层 501 确保:

- 在销售中数字内容被保护，以防非法拦截和篡改;
- 内容 113 来自一正当的内容所有人，且是由一个经许可的销售商销售的，如电子数字内容商店 103;
- 数字内容的购买者拥有者具有真正的许可应用;
- 在内容 113 的拷贝为购买者或最终用户可用之前，购买者已向销售者付款；以及
- 一交易记录被保留以便出报告。

内容标识层 503 使之能够核实版权和鉴别内容的购买者。内容的版权信息和内容购买者的身份使之能够追踪任何经或未经授权的内容 113 的拷贝的来源。因此，内容标识层 503 提供了一种抗击盗版的方法。

内容使用控制层 505 保证内容 113 的拷贝在购买者的设备上被按照商店使用条件 519 使用。商店使用条件 519 可以指定允许的内容 113 的播放次数和本地拷贝数，及内容 113 是否可被录到外部可携带设备上。内容使用控制层 505 中的功能，记录内容的拷贝/播放使用，并更新拷贝/播放状态。

内容格式化层 507 使之能够将内容 113 从在内容所有人的设备上的初始表现形式格式，转换成与安全数字内容电子销售系统 100 的服务特色和销售方法相容的一种形式。此转换过程可能包括压缩编码和与其相关的预处理，如频率均衡和幅度动态调整。当内容 113 是音频时，在购买者一方，所接收到的内容 113 还需经处理，以得到适合再播放或传送到一可携带设备的适当格式。

B. 功能划分和流程

图 5 中显示的版权管理结构模型，说明了组成安全数字内容电子销售系统 100 和每一层中的密钥功能。

1. 内容格式化层 507

与内容格式化层 507 相关联的一般功能是内容提供者 101 处的内容预处理 502 和压缩 511，以及最终用户设备 109 处的内容解扰频 513 和解压缩 515。上面叙述了进行预处理的要求和具体功能的示例。内容压缩 511 用于压缩内容 113 文件的大小和传送时间。任何适合于内容 113 的类型和传送介质的压缩算法都能用在安全数字内容电子销售系统 100 中。对于音乐 MPEG1/2/4，DolbyAC-2 和 AC-3，索尼适配传输编码（ATRAC），以及低位率的算法都是这种压缩算法的一些典型代表。内容 113 以压缩的格式存储于最终用户设备 109 中，以便减少所必需的存储容量。在使用回放的过程中又将其解压缩。回放时也进行解扰频。扰频的目的和类型将在以后的内容使用控制层 505 的讨论中进行描述。

2. 内容使用控制层 505

内容使用控制层 505 允许规范和执行加在内容 113 使用的用于最终用户设备 109 的条件或限制。无论内容 113 是否被允许第二次拷贝，及第二次拷贝的数量多少，或内容 113 是否可复制到一个外部的便携式的设备上，这些条件能够指定内容 113 所允许的播放的数量。内容提供者 101 设置允许的使用条件 517，并将其传送到 SC 中的电子数字内容商店 103（参照许可证控制层 501 部分）。只要电子数字内容商店 103 不使内容提供者 101 制定的原始条件无效，它就能够增加或缩小使用条件 517。然后，电子数字内容商店 103 将所有的存储使用条件 519（在 SC 中）传送至最终用户设备 109 和交换所 105。交换所 105 在授权该内容 113 发行给最终用户设备 109 之前，要执行使用条件验证 521。

内容使用条件 517 的执行是在最终用户设备 109 中的内容使用控制层 505 完成的。首先，在接收来自最终用户设备 109 的内容标识层 503 的内容 113 的拷贝时，将使内容 113 带有一个拷贝/播放码 523，代表最初的拷贝/播放许可。第二，播放器应用程序 195 在将内容 113 存储在最终用户设备 109 之前将其加密扰频。播放器应用程序 195 为每个内容项生成一个扰频密钥，这个扰频密钥被加密并隐藏于最终用

户设备 109 中。然后，每当最终用户设备 109 读取内容 113 进行拷贝或播放时，最终用户设备 109 在其允许内容 113 解扰频和执行播放和拷贝之前，要对拷贝/播放码进行校验。最终用户设备 109 在原始的内容 113 的付本和任何一个新的第二次拷贝上，还适当地更新拷贝/播放码。这个拷贝/播放编码是在已压缩的内容 113 上使用的。也就是说，在嵌入拷贝/播放码之前，不需将内容 113 解压缩。

最终用户设备 109 使用了一个许可证水印 527，在内容 113 中嵌入拷贝/播放码。只有具有嵌入算法和相关的扰频密钥能力的最终用户播放器应用程序 195 能够读取或修改这些嵌入的数据。对人来说，这些数据是看不见和听不见的，也就是说，这些数据对内容 113 不带来可知觉的退化。由于水印要经历若干步的内容处理、数据压缩、D/A 转换和 A/D 转换、以及由正常的内容处理而带来的信号衰减，水印以任何的表示方式与内容 113 同时存在，包括模拟的表示。在另外一实施例中，最终用户播放器应用程序 195 使用被安全存储的使用条件 519，而不是用许可证水印 527 在内容 113 里嵌入拷贝/播放码。

3. 内容识别层 503

作为内容识别层 503 部分，内容提供者 101 也使用一个许可证水印，在内容 113 中嵌入数据，如内容标识符、内容拥有者和其他信息如发表日期及地理分布区域。该水印在此指版权水印 529。在接收时，最终用户设备 109 用内容购买者名和交易 ID 535（参照下面的许可证控制层 501 部分），及用其他信息如许可证日期和使用条件 517 为内容 113 的拷贝加水印。这水印在此指许可证水印。任何以授权方式或非授权方式获得，和经历了保持内容质量的声音处理的内容 113 的拷贝，都带有版权和许可证水印。内容识别层 503 防止侵犯版权。

4. 许可证控制层 501

许可证控制层 501 保护内容 113 免受非授权中止，并确保内容仅根据具有合适的许可的最终用户设备 109 的一个最终用户单独发行，并用授权的电子数字内容商店 103 成功地完成一个许可购买交易。许可证控制层 501 通过双层加密 531 保护内容 113。使用由内容提供者

101 产生的加密的对称密钥对内容 113 加密。使用交换所的公共密钥加密对称密钥。只有交换所 105 能最初地重新获得这个对称密钥。

用交换所 105 设计的许可证控制为“可信任方”。在对许可证请求 537 发行许可以前（即，对于内容 113 的对称密钥 623 送到最终用户设备 109 之前），交换所 105 验证交易 541 和许可证授权 543 是否完整和真实，及验证电子数字内容商店 103 是否从安全数字内容电子销售系统 100 得到电子内容 113 的销售授权，并使最终用户有一个适当的有许可权的应用程序。审核/报告 545 允许在安全电子数字内容销售系统 100 中产生报告和与其他授权方共享许可交易信息。

许可证控制是通过 SC 处理 533 来实现的。SC 用于在系统操作部件（下面章节有关于 SC 的详细结构）之间销售加密的内容 113 和信息。一个 SC 是用密码写的信息载体，这些信息使用加密的密码，数字签名和数字证认来提供保护，避免电子信息或内容 113 的非授权的中途侦听和修改。SC 也考虑了电子数据的可靠性核对。

对许可证的控制要求内容提供者 101、电子数字内容商店 103 和交换所 105 拥有从可信赖的用于授权那些部件的许可证授权部门得来的正规加密数字认证。最终用户设备 109 不需要有数字认证。

C. 内容销售和许可控制

图 6 以方块图的形式描述了用于图 5 中的许可证控制层的内容销售和许可控制的概况，。图中描述了电子数字内容商店 103，最终用户设备 109 和交换所 105 通过 Internet 内部互连，并且在那些部件之间使用了点到点的传送。内容提供者 101 和电子数字内容商店 103 之间的通信也能够通过 Internet 或其他网络进行。假定最终用户设备 109 和电子数字内容商店 103 之间的内容-购买商务交易是基于标准的 Internet Web 协议。作为基于交互式 Web 的一部分，终端用户用内容 113 的选定范围来购买，提供个人和金融信息，并对购买的条件表示同意。电子数字内容商店 103 能够用协议如 SET 从一获取机构中得到支付授权。

图 6 中也假定电子数字内容商店 103 基于标准的网络协议已经把

最终用户播放器应用程序 195 下载到一个的最终用户设备 109。这种结构要求电子数字内容商店 103 给下载的播放器应用程序 195 指定一个唯一的应用 ID，并且最终用户设备 109 存储它，以便以后应用许可验证（参照以下内容）。

所有的许可流程都开始于内容提供者 101。内容提供者 101 用一个本地产生的加密的对称密钥对内容 113 进行加密，并用交换所 105 的公共密钥 621 对对称密钥 623 进行加密。在另一实施例中,对称密钥不是本地产生的，而是从交换所 105 传送到内容提供者 101。内容提供者 101 以加密的内容 113 为基础生成一个内容 SC 630，并且以加密的对称密钥 623，存储使用条件 519 和其他的内容 113 相关信息为基础生成一个元数据 SC 620。每个内容 113 目标都有一个元数据 SC 620 和一个内容 SC 630。这个内容 113 的目标可以是同一首歌的一个压缩层，或者内容 113 对象可以是唱片集中的每一首歌，或者内容 113 是整个唱片集。每个内容 113 目标,元数据 SC 620 也载有与内容使用控制层 505 有关的使用条件 519。

内容提供者 101 将元数据 SC 620 分配到一个或多个电子数字内容商店 103（601 步），将内容 SC 630 分配到一个或多个内容托管站点（602 步）。每个电子数字内容商店 103，依次产生一个报价 SC 641。报价 SC 641 典型地携有大量同元数据 SC 620 相同信息，包括内容提供者 101 的数字签名 624 以及认证（内容提供者 101 中未显示）101。正如上面所提到的，电子数字内容商店 103 能够增加或减少存储使用条件 519（由内容使用控制层进行处理），这些使用条件 519 最初是由内容提供者 101 定义的。内容 SC 630 和/或元数据 SC 620 能够任意地用内容提供者 101 的一个数字签名 624 来作标记。

在最终用户设备 109 和电子数字内容商店 103（603 步）之间的内容-购买交易完成以后，电子数字内容商店 103 产生并传送给最终用户设备 109 一个交易 SC 640（604 步）。交易 SC 640 包括一个唯一的交易 ID 535，买方姓名（也就是最终用户）（未显示），最终用户设备 109 的公共密钥 661，以及与购买内容 113 有关的报价 SC（s） 641。

图 6 中的交易数据 642 既代表了交易 ID 535，也代表了最终用户的姓名（未显示）。交易数据 642 用交换所 105 的公共密钥 621 进行加密。交易 SC（s）可以任意地由电子数字内容商店 103 的一个数字签名 643 来作为标记。

根据接收交易 SC 640（其中包括报价 SC 641），运行在最终用户设备 109 上的最终用户播放器应用程序 195 依靠一个订单 SC 650（605 步）从交换所 105 请求许可证授权。订单 SC 650 包括加密的对称密钥 623，来自报价 SC 641 的存储使用条件 519，以及交易 SC (s)640 中的加密的交易数据 642，还有最终用户设备 109 中加密的应用 ID 551。在其它的实施例中，订单 SC 650 用最终用户设备 109 中的一个数字签名 652 作标记。

根据最终用户设备 109 上接收订单 SC 650，交换所 105 核实：

1. 电子数字内容商店 103 从安全数字内容电子销售系统 100（存在于交换所 105 的数据库 160 中）处获得授权；

2. 订单 SC 650 没有被改变；

3. 交易数据 642 和对称密钥 623 是完整的和真实的；

4. 最终用户设备 109 购买的电子存储使用条件 519 与由内容提供者 101 设置的使用条件 517 相一致；及

5. 应用 ID 551 有一个正确的结构，并且它由一个授权的电子数字内容商店 103 提供。

如果核实成功，交换所 105 就会将对称密钥 623 和交易数据 642 解密，同时建立并把许可证 SC 660 传送到最终用户设备 109（606 步）。许可证 SC 660 携有用最终用户设备 109 的公共密钥 661 进行加密的对称密钥 623 和交易数据 642。如果任何一个核实不成功，那么交换所 105 就否认对最终用户设备 109 的许可，并通知最终用户设备 109。交换所 105 也立即通知电子数字内容商店 103 校验失败。在另一的实施例中，交换所 105 用它的数字签名 663 对许可证 SC 进行标记。

最终用户设备 109 接收了许可 SC 660 以后，将以前由交换所 105

得到的对称密钥 623 和交易数据 642 解密，并请求内容托管站点 111 的内容 SC 630（607 步）。根据到达内容 SC 630（608 步），最终用户设备 109 用对称密钥 623 将内容 113 进行解密，并如前面图 5 中描述的，将内容 113 和交易数据 642 传递到其它层作为许可证水印，拷贝/播放编码，抗频，和进一步的处理内容 113。

最后，交换所 105 周期性地传送总的交易报告给内容提供者 101 和电子数字内容商店 103 以达到审核和跟踪的目的。

V.安全容器结构

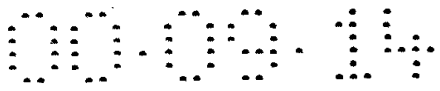
A. 一般结构

安全容器(SC)是一个由若干部分组成的结构，这些组成部分一起定义了内容 113 的一个单元或部分交易，它们也定义了相关信息如使用条件，元数据和加密方法。SC 是以这样的一种方式定义的，即能够校验信息的完整性、完全性和可靠性。SC 中的一些信息可以被加密，因此只有在得到合适的授权后才能读取这些信息。

SC 至少包括一个物资帐单（ROM）部分，这个部分有 SC 和 SC 中每部分相关信息的记录。对每一部分和包含于每部分中的 BOM 记录，用 HASH 算法如 MD—5 计算消息摘要。这些部分的摘要级联起来，而其它摘要从其中计算然后用创建 SC 的实体的私钥进行加密，来生成数字签名。接收 SC 方能够用这个数字签名来校验所有的摘要，由此来验证 SC 和它的所有部分的完整性和完全性。

下面的信息作为记录连同每一部分的记录可被包括在 BOM 中。SC 的类型决定了哪个记录必须包括:

- SC 版本
- SC ID
- SC 的类型（例如，报价，订单,交易，内容，元数据或促销和许可证。）
- SC 的出版者
- SC 的创建日期
- SC 的截止日期



- 交换所的 URL
- 用于所包括的部分（默认为 MD-5）的摘要算法的描述
- 用于数字信号加密（默认为 RSA）的算法的描述
- 数字签名（包括所有级联摘要的加密摘要部分）

SC 可以包含有不止一个 BOM。例如，一个报价 SC641 由最初的元数据 SC 620 部分组成，包括它的 BOM，也包括由电子数字内容商店 103 增加的附加信息和一个新的 BOM。用于元数据 SC 620 BOM 的记录包含于报价 SC 641 BOM 中。这个记录包括有一个用于元数据 SC 620 BOM 的摘要，这个元数据 SC 620 BOM 能够用于验证其完整性，因此，从元数据 SC 620 中包括的完整性部分也能够用存储在元数据 SC 620 BOM 中的部分摘要值来验证。从元数据 SC 620 中没有一部分在新的 BOM 中有记录，而这个新的 BOM 是为报价 SC 641 已生成。只有被电子数字内容商店 103 和元数据 SC 620 BOM 增加的部分在新的 BOM 中才有记录。

SC 还可以包括一个密钥描述部分。密钥描述部分包含有下列的 SC 中的加密部分信息的记录:

- 加密部分的名称。
- 被加密时，这部分使用的名称。
- 用来加密部分的加密算法。
- 或者是一个指示用于对部分进行加密的公共加密密钥的密钥标识符，或是当解密时，用于将加密部分解密的加密了的一个对称密钥。
- 加密算法用于将对称密钥加密。当密钥描述部分中的记录包含有一个对加密的部分进行加密的加密了的对称密钥后，这个字段才能存在。
- 公共加密密钥的密钥标识符，用于将对称密钥加密。只有当密钥描述部分中的记录包含有一个加密的对称密钥和对加密部分进行加密的对称密钥加密算法的标识符后，这个字段才能存在。

如果 SC 不包括任何加密的部分，那么就没有密钥描述部分。

B. 版权管理语言的语法和语义

版权管理语言由许多参数组成，这些参数可以在内容 113 购买后，由最终用户使用内容 113 时的定义限制条件分配数值。使用内容 113 上的限制是使用条件 517。每个内容提供者 101 为它的每个内容 113 项指定了使用条件 517。电子数字内容商店 103 在元数据 SC 中解释使用条件 517，并且用这些信息来提供选择项，希望提供给他们的顾客及为内容 113 增加零售购买信息。当最终用户选择了购买的内容 113 项后，最终用户设备 109 就会根据存储使用条件 519 为内容 113 提出授权请求。在交换所 105 向最终用户发送许可 SC 660 之前，交换所 105 核实被提出请求的存储使用条件 519 是否和所允许的使用条件 517 相一致，使用条件 517 是由元数据 SC 620 中的内容提供者 101 指定的。

当最终用户设备 109 接收被购买的内容 113 时，商店使用条件 519 用水印工具编码成内容 113，或以安全存储使用条件 519 被编码。运行于最终用户设备 109 上的最终用户播放器应用程序 195 可以保证被编码成内容 113 的商店使用条件 519 被执行。

下面是对内容 113 是音乐的实施例中商店使用条件 519 的一个例子:

- 歌曲是可记录的。
- 歌曲可以播放 n 次。

C. 安全容器流程和处理的概述

元数据 SC 620 由内容提供者 101 建立，并用于定义内容 113 项，如歌曲。内容 113 本身不包括在这些 SC 中，因为对于电子数字内容商店 103 和最终用户，为达到读取描述性的元数据的目的进行有效地下载容器，内容 113 的容量明显太大。相反,SC 包括一个指向内容 113 的外部 URL（统一资源定位器）。SC 还包括提供关于内容 113 和任何其它的相关数据的描述性信息的元数据，如用于音乐，CD 封面艺术和/或在音乐内容 113 情况下的数字声音片段。

电子数字内容商店 103 下载经过授权的元数据 SC 620，并建立报价 SC 641。简而言之，报价 SC 641 由某些部分和来自元数据 SC 620

的 BOM，随同电子数字内容商店 103 的附加信息组成。当报价 SC641 建立时，报价 SC 的一个新的 BOM 也建立了。电子数字内容商店 103 通过从元数据 SC 620 中提取元数据信息来使用元数据 SC 620，在它们的 WEB 站点上建立 HTML 网页，这些站点给最终用户显示内容 113 的说明，通常电子内容商店 103 能够购买内容 113。

由电子数字内容商店 103 加到报价 SC 641 中的信息，典型地用于缩减在元数据 SC 620 中指定的使用条件 517 的选定范围，并增加如商店标志的一个图形图象文件和一个 URL 到商店 WEB 站点。元数据 SC 620 中的报价 SC 641 的模板指示那些信息能够被报价 SC 641 中的电子数字内容商店 103 覆盖，并且指出，即便要，什么附加信息是电子数字内容商店 103 所需要的，及在嵌入的元数据 SC 620 中什么部分被保留。

当最终用户决定从电子数字内容商店 103 购买内容 113 时，报价 SC 641 就包含在交易 SC 640 中。电子数字内容商店 103 为每个已购买的内容 113 项建立一个交易 SC 640，包括报价 SC 641，并将其传送到最终用户设备 109 处。最终用户设备 109 接收交易 SC 640，并验证交易 SC 640 和包括于其中的报价 SC 641 的完整性。

订单 SC 650 由最终用户设备 109 为每个购买的内容 113 项建立。信息被包含在报价 SC 641，交易 SC 640 和最终用户设备 109 的结构文件中。订单 SC 650 一次一个被传送到交换所 105。交换所 105 URL 处的订单 SC 650 作为一个记录被包括在元数据 SC 620 的 BOM 中，并又被包括在报价 641 中。

交换所 105 验证并处理订单 SC 650，以把许可证水印 527 所请求的所有事提供给最终用户设备 109，并读取购买的内容 113。交换所 105 的一个功能就是将对称密钥 623 解密，这个对称密钥 623 是将报价 SC 641 中的水印指令和内容 SC 630 中的内容 113 进行解密所必需的。加密的对称密钥 623 记录，事实上不仅仅包含实际的加密的对称密钥 623。在进行加密之前，内容提供者 101 可以任意地将其姓名加入实际的对称密钥 623。具有了和对称密钥 623 一起加密的内容提供者 101

姓名，就可以提供安全性，预防侵犯从合法的 SC 中建立其自己的元数据 SC 620 和内容 SC 630 的内容提供者 101。交换所 105 核实与对称密钥 623 一起加密的内容提供者 101 的姓名，并在 SC 许可证中与内容提供者 101 的姓名相匹配。

如果交换所 105 对水印指令有任何请求的变化，那么交换所 105 就将对称密钥 623 解密，然后修改水印指令，并用一个新的对称密钥 623 将其再次加密。然后，用最终用户设备 109 的公共密钥 661 对对称密钥 623 再次加密。交换所 105 也将 SC 中的其它对称密钥 623 解密，并用最终用户设备 109 的公共密钥 661 将这些对称密钥 623 再次加密。交换所建立一个许可 SC 660，它包括新加密的对称密钥 623 和更新了的水印指令，并将这个许可证 SC 660 传送到与订单 SC 650 相适应的最终用户设备 109。如果订单 SC 650 的处理过程没有完全完成，那么交换所 105 就会返回给最终用户设备 109 一个 HTML 网页或类似的形式来报告授权过程的失败。

许可证 SC 660 把读取内容 113 项所必需的所有东西提供给最终用户设备 109。最终用户设备 109 向内容托管站点 111 请求适当的内容 SC 630。内容 SC 630 有内容提供者 101 建立，并包括加密的内容 113 和元数据部分。最终用户播放器应用程序 195 用来自许可证 SC 660 的对称密钥 623 来将内容 113、元数据和水印指令解密。然后水印指令将附加到内容 113 上，并且内容 113 被扰频和被保存在最终用户设备 109 上。

D. 元数据安全容器 620 的格式

下面的表显示了包括在元数据 SC 620 中的部分。部分列中的每个方框都是一个彼此分离目标，包含于 SC 中并带有 BOM（除了被[]符号包围的部分的名称）。BOM 包括包含在 SC 中每一部分的一个记录。部分存在（Part Exists）列表明这一部分本身是否实际存在于 SC 中，而摘要列表明此列的消息摘要是否已进行计算。尽管全部的原始 BOM 被传送，当一个 SC 包含于另一个 SC（由相关模板决定）中时，某些部分可以不被传送。这是因为所有的 BOM 是由交换所 105 提出

请求来核实原始 SC 中的数字签名。

下面的表格的密钥描述部分各列定义了包括于 SC 密钥描述部分内的记录。密钥描述部分中的记录定义了关于用于对在 SC 部分中加密密钥和或另外 SC 中部分加密的算法信息。每个记录包括了加密部分的名称，如果必要，还包括一个指向其它包含有加密部分的 SC 的 URL。结果名称列定义名称，该名称解密以后被赋给这部分。Encrypt Alg 列定义了用于对这部分进行加密的加密算法。key Id/Enc key 列既定义了一个对该部分进行加密的加密密钥的标识，也定义了一个对该部分进行加密的加密了的对称密钥 623 位串的基 64 编码。Sym Key Alg 列是一个任选的参数，当前面的列是一个加密的对称密钥 623 时，这个参数就可以定义用于对对称密钥进行加密的加密算法。Sym Key ID 列是加密的密钥的一个标识符，当 Key Id/Enc Key 列是一个加密的对称密钥 623 时，这个加密的密钥将用于对对称密钥 623 进行加密。

部分	BOM		密钥说明部分				
	部分存在	摘要	结果名	加密 Alg	Key Id/Enc Key	Sym Key Alg	Sym Key ID
[内容 URL]			输出部分	RC4	Enc Sym Key	RSA	CH Pub Key
[元数据 URL]			输出部分	RC4	ENc Sym Key	RSA	CH Pub Key
	SC 版本						
	SC ID						
	SC 类型						
	SC 出版者						
	日期						
	期满日期						
	交换所 URL						
	摘要算法 ID						
	数字签名 Alg ID						
内容 ID	Yes	Yes					
元数据	Yes	Yes					
使用条件	Yes	Yes					
SC 模板	Yes	Yes					
水印指令	Yes	Yes	输出部分	RC4	Enc Sym Key	RSA	CH Pub Key
密钥说明部分	Yes	Yes					
交换所认证	Yes	No					
认证	Yes	No					
	数字签名						

以下是对上面元数据表中的使用的术语进行描述:

◆ [内容 URL]---密钥描述部分的记录中的一个参数。这是一个 URL，指向与这个元数据 SC 620 关联的内容 SC 630 中加密的内容 113。元数据 SC 620 本身不包含加密的内容 113。

◆ [元数据 URL]--- 密钥描述部分的记录中的一个参数。这是一个 URL，指向与这个元数据 SC 620 关联的内容 SC 630 中加密的元数据。元数据 SC 620 本身不包含加密的元数据。

◆ 内容 ID --- 定义一个唯一的 ID 指定给内容 113 项的部分。如果元数据 SC 620 引用不止一个内容 113 项，那么在这个部分中，就存在不止一个内容 ID

◆ 元数据 --- 含有与内容 113 项有关的信息，如在一首歌曲的情况下，艺术家的名字和 CD 封面艺术等信息的部分。可以有多个元数据部分，其中的有些可被加密。元数据部分的内部结构取决于其包含元数据的类型。

◆ 使用条件 —- 含有各种信息的部分，这些信息包括描述使用选择，规则和加在最终用户上以使用内容 113 的限制等信息

◆ SC 模板 --- 定义用于建立报价，订单，和许可证 SC(s)660 而描述请求和选择信息的模板的部分。

◆ 水印指令 --- 包含有加密指令和用于实现内容 113 中水印的参数的部分。水印指令可以由交换所 105 更改，并在许可证 SC 660 中返回到最终用户设备 109。在密钥描述部分中有一个记录，定义了用于将水印指令加密的加密算法，定义了当这些水印指令解密时使用的输出部分的名称，还定义了用于将水印指令加密的加密了的对称密钥 623 位串的基 64 编码，同时定义了用于将对称密钥 623 加密的加密算法和将对称密钥 623 解密所要求的公共密钥的标识符。

◆ 交换所许可证 --- 从许可证授权或从交换所 105 得到许可证，交换所 105 包含带有标记的交换所 105 的公共密钥 621。

可以存在不止一个许可证，在这种情况下，使用分层结构，用包含有公共密钥的最高层许可证来打开下一层许可证，最低层许可证含有交换所 105 的公共密钥 621。

◆ 许可证 --- 从许可证授权或交换所 105 得到许可证，交换所 105 包含有带有标记的创建 SC 的实体的公共密钥 621。可以存在有不止一个许可证，在这种情况下，使用分层结构，用包含有公共密钥的最高层许可证来打开下一层许可证等等，直到到达含有 SC 创建者的公共密钥的最低层许可证。

◆ SC 版本 --- 由 SC 打包工具指定给 SC 的一个版本号。

◆ SC ID --- 由已创建的 SC 实体指定给 SC 的一个唯一的 ID。

◆ SC 类型 --- 表明了 SC 的类型（如元数据、报价、订单等等）。

◆ SC 出版者 --- 描述了已创建的 SC 实体

◆ 创建日期 ---创建 SC 的日期

◆ 期满日期 --- SC 期满并不再有效的日期

◆ 交换所 URL --- 交换所 105 的地址，在这里最终用户播放器应用程序 195 能与得到能读取内容 113 的适当的授权相配合。

◆ 摘要算法 ID --- 用于计算部分摘要的算法的一个标识符

◆ 数字签名算法 ID --- 用于加密级联部分摘要的摘要的算法标识符，这个加密的值是数字签名。

◆ 数字签名 --- 用创建 SC 实体的公共密钥，对级联部分的摘要进行加密的一个摘要。

◆ 输出部分 --- 当一个加密部分被解密时，赋给输出部分的名称

◆ RSA 和 RC4 --- 用于给对称密钥 623 和数据部分进行加密的默认加密算法

◆ Enc Sym Key --- 当解密时，用在解密一个 SC 部分的加

密密钥位串的基 64 编码。

◆ CH Pub Key --- 表示用于将数据进行加密的交换所公共密钥的一个标识

E. 报价安全容器 641 格式

下面的表显示了包含在报价 SC 641 中的部分。除了一些元数据部分，表中这些部分和元数据 SC 620 中的 BOM 也包含在报价 SC 641 中。

部分	BOM		密钥说明部分				
	部分存在	摘要	结果名	加密 Alg	Key Id/Enc Key	Sym Key Alg	Sym Key ID
[内容 URL]			输出部分	RC4	Enc Sym Key	RSA	CH Pub Key
[元数据 URL]			输出部分	RC4	ENc Sym Key	RSA	CH Pub Key
	SC 版本						
	SC ID						
	SC 类型						
	SC 出版者						
	日期						
	期满日期						
	交换所 URL						
	摘要算法 ID						
	数字签名 Alg ID						
内容 ID	Yes	Yes					
元数据	Yes	Yes					
使用条件	Yes	Yes					
SC 模板	Yes	Yes					
水印指令	Yes	Yes	输出部分	RC4	Enc Sym Key	RSA	CH Pub Key
密钥说明部分	Yes	Yes					
交换所认证	Yes	No					
认证	Yes	No					
	数字签名						

————————————报价 SC Parts————————————

	SC 版本	
	SC ID	
	SC 类型	
	SC 出版者	
	日期	
	期满日期	
	摘要算法 ID	
	数字签名 Alg ID	
元数据 SC BOM	Yes	Yes
附加覆盖字段	Yes	Yes
电子数字内容商店认证	Yes	No
认证	Yes	No
	数字签名	

下面描述了上面的报价 SC 中的使用的，在前面其它的 SC 中没有描述过的术语:

◆ 元数据 SC(s) BOM --- 来自于原始元数据 SC 620 的 BOM。在提供 SC（s） 641 BOM 中的记录包括元数据 SC(s)620 BOM 的摘要。

◆ 附加和覆盖字段 --- 被电子数字内容商店 103 撤销的使用条件信息。这个信息被交换所 105，利用接收到的 SC(s)模板进行验证，以确保被电子数字内容商店 103 撤销的任何东西都在它的授权范围之内。

◆ 电子数字内容商店许可证 --- 一个由交换所 105 提供给

电子数字内容商店 103，并由交换所 105 利用它的私钥标志的许可证。这个许可证由最终用户播放器应用程序 195 用于核实电子数字内容商店是内容 113 的合法销售者。最终用户播放器应用程序 195 和交换所 105 通过用交换所 105 的公共密钥 621 对许可证签名进行解密，能够核实电子数字内容商店是一个授权的销售者。最终用户播放器应用程序 195 保留了交换所 105 的共密钥 621 的一本地拷贝，在安装的过程中，最终用户播放器应用程序 195 接收此拷贝作为其初始化的一部分。

F. 交易安全容器 640 格式

下面的表显示了包含在交易 SC 640 和它的 BOM 的部分和密钥描述部分。

00-09-14

部分	BOM				密钥说明部分		
	部分存在	摘要	结果名	加密 Alg	Key Id/Enc Key	Sym Key Alg	Sym Key ID
	SC 版本						
	SC ID						
	SC 类型						
	SC 出版者						
	日期						
	期满日期						
	摘要算法 ID						
	数字签名 Alg ID						
交易 ID	Yes	Yes	输出部分	RSA	CH Pub Key		
最终用户 ID	Yes	Yes					
最终用户的公共密钥	Yes	Yes					
报价 SC	Yes	Yes					
内容使用选择	Yes	Yes					
HTML 显示	Yes	Yes					
密钥描述部分	Yes	Yes					
电子数字内容商店认证	Yes	No					
	数字签名						

下面描述在前面没有为其他SC描述过的，用于上面的交易SC 640中的一些术语:

◆ 交易 ID 535 --- 由电子数字内容商店 103 指定的唯一标识交易的 ID。

◆ 最终用户 ID --- 在最终用户做购买选择和提供信用卡信息时，由电子数字内容商店 103 得到的最终用户的标识符。

◆ 最终用户的公共密钥 --- 最终用户的公共密钥是交换所用于将对称密钥 623 再次加密。最终用户的公共密在购买交易期间，被传送到电子数字内容商店 103。

◆ 报价 SC --- 所购买的内容 113 项目的报价 SC 640。

◆ 内容使用的选择 ---被最终用户购买的每个内容 113 项的使用条件的一个阵列。每个报价 SC 都有一个入口。

◆ HTML 显示--- 一个或多个 HTML 网页，这些 HTML 网页是由交易 SC 640 接收或最终用户设备 109 和交换所 105 交互期间，最终用户播放器应用程序 195 在 INTERNET 浏览窗口中显示的 HTML 网页。

当最终用户设备 109 接收到交易 SC 640，就会执行以下步骤，以核实 SC 的完整性和可靠性:

1. 用交换所 105 的公共密钥 621 来核实电子数字内容商店 103 许可证的完整性。交换所 105 的公共密钥 621 在安装过程期间，被接收作为最终用户播放器引用 195 初始化的一部分，然后就保存在最终用户设备 109 中。

2. 用电子数字内容商店 103 许可证的公共密钥来核实 SC 的数字签名 643。

3. 核实 SC 部分的 HASH。

4. 核实包含于交易 SC 640 中的每个报价 SC 641 的完整性和真实性。

G. 订单安全容器 650 格式

下表中显示了包含在订单 SC 650 以及它的 BOM 部分和密钥描述部分。这些部分或者为交换所 105 提供用于解密和核实的信息，或者由交换所 105 验证。来自报价 SC 641 的这些部分和 BOM 也包括在订单 SC 650 中。元数据 SC BOM 的 Part Exists 列中的一些字符串表示那些部分中的一部分不包括在订单 SC 650 中。来自元数据 SC 620 的 BOM 还包括无任何变化，因此交换所 105 能够验证元数据 SC 620 和它的部分的完整性。

部分	BOM			密钥说明部分			
	部分存在	摘要	结果名	加密 Alg	Key Id/Enc Key	Sym Key Alg	Sym Key ID
——————————元数据 SC 部分——————————							
[内容 URL]			输出部分	RC4	Enc Sym Key	RSA	CH Pub Key
[元数据 URL]			输出部分	RC4	ENc Sym Key	RSA	CH Pub Key
	SC 版本						
	SC ID						
	SC 类型						
	SC 出版者						
	日期						
	期满日期						
	交换所 URL						
	摘要算法 ID						
	数字签名 Alg ID						
内容 ID	Yes	Yes					
元数据	Some	Yes					
使用条件	Yes	Yes					
SC 模板	Yes	Yes					
水印指令	Yes	Yes	输出部分	RC4	Enc Sym Key	RSA	CH Pub Key
密钥说明部分	Yes	Yes					
交换所认证	Yes	No					
认证	Yes	No					
	数字签名						

——————————报价 SC(s)部分——————————

	SC 版本	
	SC ID	
	SC 类型	
	SC 出版者	
	日期	
	期满日期	
	摘要算法 ID	
	数字签名 Alg ID	
元数据 SC BOM	Yes	Yes
附加覆盖字段	Yes	Yes
电子数字内容商店认证	Yes	No
认证	Yes	No
	数字签名	

00.09.14

---------交易 SC(s)部分---------

	SC 版本				
	SC ID				
	SC 类型				
	SC 出版者				
	日期				
	期满日期				
	摘要算法 ID				
	数字签名 Alg ID				
交易 ID	Yes	Yes	输出部分	RSA	CH Pub Key
最终用户 ID	Yes	Yes	输出部分	RSA	CH Pub Key
最终用户的公共密钥	Yes	Yes			
报价 SC(s)	One Offer Sc(s)	Yes			
内容使用的选择	Yes	Yes			
在浏览器窗口中显示的 HTML	Yes	Yes			
密钥描述部分	Yes	Yes			
电子数字内容商店认证	Yes	No			
	数字签名				

————————————订单 SC 部分————————————

	SC 版本				
	SC ID				
	SC 类型				
	SC 出版者				
	日期				
	期满日期				
	摘要算法 ID				
	数字签名 Alg ID				
报价 SC BOM	Yes	Yes			
交易 SC BOM	Yes	Yes			
加密的信用卡信息	Yes	Yes	输出部分	RSA	CH Pub Key
密钥描述部分	Yes	Yes			
	数字签名				

下面描述在前面其它的 SC 中没有描述过的，上面的订单 SC 650 中使用的术语:

◆ 交易 SC BOM --- 原始交易 SC 640 中的 BOM。订单 SC 650 中的记录包括了交易 SC 640 BOM 的摘要。

◆ 加密的信用卡信息 --- 从最终用户来的任选的加密信息，用信用卡或借卡支付购买物。当创建报价 SC 641 的电子数字内容商店 103 没有处理顾客订单时，就会请求信息，在这种情况下，交换所 105 就可以处理订单。

H. 许可安全容器 660 格式

下面的图表显示了包含在许可证 SC 660 和它的 BOM 中的部分。

正如在密钥描述部分所显示的，对称密钥 623 被请求用于将水印指令、内容 113 解密，并且内容 113 元数据被交换所 105 用最终用户的公共密钥 661 重新加密。当最终用户设备 109 接收许可 SC 660 时，它就将对称密钥 623 解密，并将解密的对称密钥 623 用于读取来自许可证 SC 660 和内容 SC 630 的加密的部分。

部分	BOM		密钥说明部分				
	部分存在	摘要	结果名	加密 Alg	Key Id/Enc Key	Sym Key Alg	Sym Key ID
[内容 URL]			输出部分	RC4	Enc Sym Key	RSA	CH Pub Key
[图元数据 URL]			输出部分	RC4	ENc Sym Key	RSA	CH Pub Key
	SC 版本						
	SC ID						
	SC 类型						
	SC 出版者						
	日期						
	期满日期						
	摘要算法 ID						
	数字签名 Alg ID						
内容 ID	Yes	Yes					
使用条件	Yes	Yes					
交易数据	Yes	Yes					
水印指令	Yes	Yes	输出部分	RC4	Enc Sym Key	RSA	CH Pub Key
密钥描述部分	Yes	Yes					
认证	Yes	No					
	数字签名						

下面描述了在前面其它的 SC 中没有描述过的，上面的许可 SC 650 中的使用到的术语:

- **EU Pub Key** --- 表示用来加密数据的最终用户公共密钥标的

标识符。

◆ 订单 SC 650 ID --- 从订单 SC 650 的 BOM 中取得的 SC ID。

◆ 认证撤回表 --- 认证 ID 的一个任选表，它在前面由交换所 105 发行及加上标记，但不再认为是有效的。由包含在撤回表中的认证来核实的都具有一个签名的任何 SC 是无效的 SC。最终用户播放器应用程序 195 在最终用户设备 109 上存储了一个交换所许可证撤回表的副本。无论撤回表何时被接收，如果新的副本是最合适的的，最终用户播放器应用程序 195 就会替换它的本地副本。撤回表包含有版本号或一个时间标标记（或两者皆有）用以判断哪张表是最新的。

I. 内容安全容器格式

部分	BOM	
	部分存在	摘要
	SC 版本	
	SC ID	
	SC 类型	
	SC 出版者	
	日期	
	期满日期	
	交换所 105 URL	
	摘要算法 ID	
	数字签名算法 ID	
内容 ID	Yes	Yes
加密的内容	Yes	Yes
加密的元数据	Yes	Yes
元数据	Yes	Yes
认证	Yes	No
	数字签名	

下面的表显示了包含于内容 SC 630 以及 BOM 中的部分:

◆ 加密内容 --- 被内容提供者 101 用一个对称密钥 623 加密了的内容 113。

◆ 加密元数据 --- 和内容 113 相关的元数据，它被内容提供者 101 用对称密钥 623 进行了加密。

在内容 SC 630 中不包含有密钥描述部分，因为将加密部分解密所要求的密钥是存在于在交换所 105 处建立的许可证 SC 660 中。

VI.安全容器打包和解包

A. 概述

SC 打包器是一个带有一个 API（应用程序设计接口）的 32 位的 Windows 程序，能调入一个多步或单步过程来创建具有所有指定部分的一个 SC。在内容提供者 101、交换所 105、电子数字内容商店 103 和其它要求 SC 打包的站点上，SC 打包器 151，152，153 的多种硬件平台都支持 Windows 程序。如果必要的话，可以在 SC 中创建并包含有 BOM 和密钥描述部分。一组打包器 API 提供调用程序指定在 BOM 和密钥描述部分产生记录以及在 SC 中包含的部分所必需的信息。部分和对称密钥 623 的加密以及摘要和数字签名的计算也可以由打包器来执行。打包器所支持的加密和摘要算法都包括在打包器代码中，或它们可以通过一个外部接口来调用。

用于创建SC的打包器的接口是由一个接收下列参数的API 来实现的:

◆ 一个级联结构的缓冲器的指针。在缓冲器中的每个结构都是打包器及其执行命令所需信息的命令。打包器命令包括给相关的 BOM 记录的 SC 增加一个部分，给 BOM 增加一个记录，以及给密钥描述部分增加的记录。

◆ 一个描述上面描述的缓冲器中包含的级联结构的数量值。

◆ BOM 部分的名称和位置。

◆为将来使用一个定义的标志或一个保留的标志的每位的值。下列标志是当前定义的:

- 指示在缓冲器中所有的结构被处理了之后，关于 SC 的所有部分是否被捆成为一个单一文件的标志。将所有部分捆成为一个单一的目标是建立 SC 步骤的最后一步。

- 指示关于数字签名是否从 BOM 部分中省略的标志。如果没有设置这个标志，那么就会在捆扎 SC 成为一个单一的目标之前计算数字签名。

在另一实施例中，用于创建 SC 的打包器的接口是由一个接收下列参数的 API 来实现的:

• 首先，通过将指针传递到一个由用来初试化 SC 设置的信息组成的结构来调用 API，以创建一个物资帐单（BOM）部分，这些 SC 设置被表示为 SC BOM 部分中的 IP 记录，为 BOM 部分而使用的名称，用于寻找将要被加入的部分的默认位置，以及一标志值。此 API 返回一个用在随后的打包器 API 的 SC 句柄。

• 打包器有一个每当 SC 增加一个部分时即被使用的 API。这个 API 接收一个已经由前面的打包器 API 返回的 SC 句柄处理、一个由关于增加部分的信息所组成的的结构的指针、以及一标志值。关于增加部分的信息包括有此部分的名称和位置、此部分在 BOM 中使用的名称、增加部分的类型、此部分的散列值、以及标志等等。

• 在所有部分都被加入到 SC 以后，就调用一打包器 API，将包括 BOM 部分的所有部分打包成通常是一个文件的一单独的 SC 体。这个 API 接收一个已经由前面的打包器 API 返回的 SC 句柄处理、为已被打包好的 SC 使用的名称、含有用于给 SC 签名的信息的结构的指针、以及一标志值。

打包器或调用打包器的实体使用一个 SC 模板来建立一 SC。SC 模板含有用于定义正在被建立的 SC 所需的部分和记录的信息。模

板还可以定义加密方法以及用于为对称密钥 623 和被加密部分加密的有关密钥。

打包器有一个用于为 SC 解包的 API。为 SC 解包是一个将 SC 分解为其独立部分的过程。打包器然后可被调用，以将从 SC 中解包而来的任何加密部分进行解密。

B. 物资帐单(BOM)部分

BOM 部分是在建立 SC 时由打包器建立的。BOM 是一个文本文件，它包含对 SC 和 SC 中所含各部分的信息的记录。BOM 中的每个记录都在同一行上，而每一新行指示一个新记录的开始。BOM 通常包括每部分的摘要和一用于验证 SC 的真实性和完整性的数字签名。

BOM 中的记录类型如下所示:

IP

一条 IP 记录包括一组关于 SC 的 Name=Value 对。下述名称被用于专指 SC 的特定性质:

V major.minor.fix

V 属性指定了 SC 的版本。这是用于在其下建立 SC 的 SC 规格的版本号。随后的字符串应当是以主要.次要.定位的形式，其中主要、次要和定位分别是主要版本号、次要版本号和定位层。

ID 值

ID 属性是一个由正在建立这个 SC 的实体为这个特定 SC 指定的一个独特值。这个值的格式在此文件的稍后版本中有所定义。

T 值

T 属性指定了 SC 的类型，可以是以下几种之一:

ORD - 一订单 SC 650。

OFF – 一报价 SC 641。

LIC – 一许可证 SC。

TRA – 一交易 SC 640。

MET – 一元数据 SC 620。

CON – 一内容 SC 630。

A 值

A 属性识别了 SC 的作者或出版者身份。作者/出版者的身份应是无可争议的的，并且/或者在交换所 105 注册过的。

D 值

D 属性指定 SC 建立的日期以及，可根据需要而选用的时间。这个值应当以 yyyy/mm/dd[@hh:mm[ss:[.fsec]][（TZ）]]的形式，代表年/月/日@小时：分钟：秒.秒的小数（时区）。这些值的可选部分被括于[]之中。

E 值

E 属性识别 SC 失效的日期以及可根据需要而选用的时间。这个值应当与前面定义了的 D 属性中使用的值具有同一形式。终止日期/时间应当在任何可能时与交换所 105 的日期/时间相比较。

CCURL 值

CCURL 属性识别交换所 105 的 URL。这个值应当是一个合法的外部 URL 的形式。

H 值

H 属性识别用于为包括在 SC 中的部分计算消息摘要的算法。摘要算法的一个例子是 MD5。

D

一条 D 记录是一个数据或部分加入记录，它包括用于识别部分的类型、部分的名称、部分的（可供选择的）摘要、和一个（可供选择的）指示部分不包括在 SC 中的信息。类型标识符后紧接的 A-记号用于指示此部分不包括在 SC 中。下面是备用的数据或部分记录的类型：

K part_name [摘要]

指定密钥描述部分。

W part_name [摘要]

指定水印指令部分

C part_name [摘要]

指定用于验证数字签名的证书。

T part_name [摘要]

指定使用条件部分。

YF part_name [摘要]

指定报价 SC 641 的模板部分。

YO part_name [摘要]

指定订单 SC 650 的模板部分。

YL part_name [摘要]

指定许可证 SC 660 的模板部分。

ID part_name [摘要]

指定被引用的内容 113 的选项的内容 113 的 ID。

CH part_name [摘要]

指定交换所 105 的认证部分。

SP part_name [摘要]

指定电子数字内容商店 103 的认证部分。

B part_name [摘要]

指定了其部分或其部分的子集包含在这个 SC 中的另一个 SC 的 BOM 部分。

BP part_name sc_ part_name [摘要]

指定了作为一个单独部分包含在这个 SC 中的另一个 SC 的 BOM 部分。sc_part_name 参数是包含在该 SC 中并且由此 BOM 部分定义的 SC 部分的名称。与此相同的一个 BOM 也包括在由 sc_part_name 参数定义的 SC 中。

D part_name [摘要]

指定了数据（或元数据）部分。

S

一条 S 记录是一个用于定义 SC 的数字签名的签名记录。数字签名是如下进行指定的:

S key_identifier signature_string signature_algorithm

S 记录包含用于指示签名的加密密钥的 key_identifier、signature_string，是数字签名位串的基 64 编码的签名串、以及被用于对摘要进行加密以产生数字签名的签名算法。

C. 密钥描述部分

密钥描述部分是由打包器产生的，以提供对 SC 加密部分进行解密所必需的加密密钥的信息。加密部分可以被包括在正被产生的 SC 中或由正被产生的 SC 所引用的其他 SC 中。密钥描述部分是一个文本文件，包含关于加密密钥和对其使用了加密密钥的部分的信息的记录。密钥描述部分中的每个记录都在同一行上，而每一新行指示一个新记录的开始。

下面是在密钥描述部分中使用的记录类型，定义如下：

K encrypted_ part_name ; result_ part_name ; part_ encryption_ algorithm_ identifier;

public_key_ identifier

key_ encryption_ algorithm 和 encrypted_symmetric_key。

K 记录指定了一加密部分，它可以包括在此 SC 中或包括在由此记录引用的其他 SC 中。encrypted_ part_name 或者是此 SC 中一个部分的名称，或者是指向另一个 SC 中的加密部分的名称的 URL。result_ part_name 是给与已解密部分的名称。part_ encryption_ algorithm_ identifier 显示了用于对部分进行加密的加密算法。public_key_ identifier 是一个用于为对称密钥 623 加密的密钥的标识符。

key_ encrypted_ algorithm_ identifier 显示了用于为对称密钥 623 加密的加密算法。被加密的对称密钥是一个用于对部分加密的对称密钥 623 位串的一个基 64 编码。

VII. 交换所 105

A. 概述

交换所 105 负责安全数字内容电子销售系统 100 的版权管理功

能。交换所 105 的功能包括实现电子数字内容商店 103、对内容 113 验证版权、验证购买交易和相关信息的完整性和真实性、将内容加密密钥或对称密钥 623 分发到最终用户设备 109、追踪这些密钥的发送、以及向电子数字内容商店 103 和内容提供者 101 报告交易总结。最终用户设备 109 使用内容加密密钥将其已获授权的内容 113 解锁，而它们对内容 113 所获得的授权通常是通过与已经授权的电子数字内容商店 103 进行的购买交易。在内容加密密钥被送到最终用户设备 109 之前，交换所 105 进行一个验证过程，以对正出售内容 113 的实体的以及最终用户设备 109 对内容 113 的授权的真实性进行验证。这被称为 SC 分析工具 185。在一些配置中，交换所 105 还可通过联合定位的一个位于交换所 105 的系统来处理购买内容 113 的财政结算，此系统执行电子数字内容商店 103 的信用卡授权和开帐单功能。交换所 105 使用例如 IC Verify 和 Taxware 的 OEM 包来处理信用卡处理和当地购物税。

电子数字内容商店实施例

希望以内容 113 的销售商的身份加入安全数字内容电子销售系统 100 的电子数字内容商店 103 向一个或多个为安全数字内容电子销售系统 100 提供内容 113 的数字内容提供者 101 发出请求。只要双方可达成协议，此类请求的发出并没有明确的的过程。当例如音乐商标中的索尼、Time-Warner 等等的数字内容标签决定允许电子数字内容商店 103 出售其内容 113，交换所 105 通常通过 E-mail 被联系以请求将电子数字内容商店 103 加到安全数字内容电子销售系统 100 上。数字内容标签提供电子数字内容商店 103 的名称和其它任何信息，这些信息对交换所 105 为电子数字内容商店 103 创建数字认证所可能需要的。数字认证以一种安全的方式被传送至数字内容标签上，然后再由数字内容标签转发给电子数字内容商店 103。交换所 105 为其所指定的数字认证保留一个数据库。每个认证包括一个版本号、一个唯一的系列号、签名算法、发行人的名称（例如交换所 105 的名称）、认证的有效的期限、电子数字内容商店 103 的名称、电子数字内容商店 103

的公共密钥、和用交换所 105 的私钥签名的所有其它信息的散列码。具有交换所 105 的公共密钥 621 的实体能够验证认证，并可确信如果 SC 带有一个被认证的公共密钥验证为合法有效的签名，此 SC 即可被认为是合法的。

当电子数字内容商店 103 接收到它由交换所 105 创建的数字许可证和处理来自数字内容标签的 SC 所必需的工具后，它就可以开始提供可供最终用户购买的内容 113。电子数字内容商店包括它的认证和交易 SC 640，并用它的数字签名 643 对此 SC 签名。最终用户设备 109 验证电子数字内容商店 103 是否是安全数字内容电子销售系统 100 上的一个合法的内容 113 的销售者，这种验证首先检验数字认证的被注销名单，然后用交换所 105 的公共密钥 621 来验证电子数字内容商店 103 的数字认证中的信息。交换所 105 保存有一份数字认证注销名单。注销名单可被作为一个部分而被包含于交换所 105 创建的认证 SC 660 中。最终用户设备 109 在最终用户设备 109 上保存了一份注销名单的拷贝，因此他们可以将其用于对电子数字内容商店 103 数字认证验证的一部分。每当最终用户设备 109 接收到一个许可证 SC 660，它都判断其是否包括一个新的注销名单，如果是，最终用户设备 109 上的本地撤回表就会被更新。

B. 版权管理过程

订单 SC 分析

在最终用户接收到来自电子数字内容商店 103 的、包含有报价 SC 641 的交易 SC 640 之后，交换所 105 就从最终用户接收一订单 SC 650。订单 SC 650 由包含与以下信息相关的部分组成：关于内容 113 及其使用的信息，关于销售内容 113 的电子数字内容商店 103 的信息，和关于购买内容 113 的最终用户的信息。在交换所 105 开始处理订单 SC 650 中的信息之前，它首先要完成一些处理以保证此 SC 是确实合法的，且此 SC 所含的数据从未以任何形式被破坏过。

验证

交换所通过核实数字签名开始对订单 SC 650 进行验证，然后交

换所 105 验证订单 SC 650 各部分的完整性。为了验证数字签名，交换所 105 首先使用包含于订单 SC 650 中的签名实体的公共密钥 661 对签名的内容 631（如果其经过签名）本身解密。（ 签名实体可以是内容提供者 101、电子数字内容商店 103、最终用户设备 109 或它们的任意组合。）然后，交换所 105 计算 SC 的级联部分摘要的摘要，并将它与数字签名的解密了的内容 113 相比较。如果这两个值相符的话，数字签名就是合法的。为了核实每一部分的完整性，交换所 105 计算这些部分的摘要，并将其与 BOM 中的摘要值相比较。交换所以同样的过程为包含在订单 SC 650 中的元数据和报价 SC 641 核实数字签名和部分的完整性。

对交易和报价 SC 641 数字签名的核实过程也间接地核实电子数字内容商店 103 是否经安全数字内容电子销售系统 100 授权。这是建立在交换所是许可证的发行人的事实基础上的。在另一可供选择的情况下，交换所 105 能够成功使用来自电子数字内容商店 103 的公共密钥，对交易 SC 640 和报价 SC 641 的数字签名进行核实，但其前提是给 SC 签名的实体具有相关私钥的所有权。只有电子数字内容商店 103 具有私钥的所有权。请注意，交换所 105 不必拥有电子数字内容商店 103 的本地数据库。因为商店用交换所公共密钥来对交易 SC 640 和报价 SC 641 的公共密钥签名。

然后，最终用户所购买的内容 113 的商店使用条件 519 就由交换所 105 进行验证，以保证其符合元数据 SC 620 所设置的限制范围。请记住，元数据 SC 620 被包含于定单 SC 650 中。

密钥处理

在对订单 SC 650 的真实性和完整性、电子数字内容商店 103 和商店使用条件 519 的验证都顺利完成以后，对加密的对称密钥 623 和加水印指令的处理都由交换所 105 进行。订单 SC 650 的元数据 SC 620 部分通常在其密钥描述部分有几个经交换所 105 的公共密钥 621 加密的对称密钥 623。对称密钥 623 的加密是在元数据 SC 620 被创建时由内容提供者 101 进行的。

一个对称密钥 623 用于将水印指令解密，其它的则为内容 113 以及任何加密的元数据解密。由于内容 113 可以代表一个单独的歌曲或一个 CD 上的全部歌曲集，那么可以对每首歌曲使用不同的对称密钥 623。水印指令包括在订单 SC 650 的元数据 SC 620 部分中。内容 113 和加密的元数据位于内容 SC 630 中的内容托管站点 111。内容 SC 630 中的加密内容 113 和元数据部分的 URL 以及部分名称都包括在订单 SC 650 的元数据 SC 620 部分的密钥描述部分中。交换所用它的私钥将对称密钥 623 解密，然后用最终用户设备 109 的公共密钥 661 将每个对称密钥 623 加密。最终用户设备 109 的公共密钥 661 是从订单 SC 650 中获得的。新的加密了的对称密钥 623 被包括在交换所 105 返回给最终用户设备 109 的许可证 SC 660 的密钥描述部分。

在对称密钥 623 的处理期间，交换所 105 可对水印指令作更改。如果是这种情况，那么在交换所 105 为对称密钥 623 解密以后，水印指令可被更改并重新加密。新的水印指令将作为其一部分被包含于将返回给最终用户设备 109 的许可证 SC 660 中。

如果对订单 SC 650 的所有处理均顺利完成，交换所就会将许可证 SC 660 返回给最终用户设备 109。最终用户设备 109 使用许可证 SC 660 的信息来下载内容 SC 630，并读取加密了的内容 113 和元数据。水印指令也由最终用户设备 109 执行。

如果交换所 105 不能成功处理订单 SC 650，那么一个 HTML 网页就会被返回给最终用户设备 109，并显示在一个互联网的浏览窗口上。HTML 网页指出交换所 105 不能处理此交易的原因。

在一个可供选择的实施例中，如果用户在设定的销售发行日期之前购买了内容 113 的拷贝，那么被返回的许可证 SC 660 就不带有对称密钥 623。在销售发行日当天或之后，许可证 SC 660 被返回到交换所 105 以接收对称密钥 623。举例而言，内容提供者 101 允许用户在某新歌的发行日之前下载此歌，以使顾客能在内容提供者 101 所设日期之前下载此歌并做好播放此歌的准备。这就使得在发行当天能立即打开内容 113，而不须在发行当天满足频带宽度和下载时间。

C. 国家特定参数

可供选择地，交换所 105 使用最终用户设备 109 的域名，且如可能的话，用信用卡发送帐单的地址来决定最终用户的国家所在地。如果最终用户居住的国家对内容 113 的出售有任何限制，那么交换所 105 就会在将许可证 SC 660 传送到最终用户设备 109 之前，保证其正在处理的交易不违反任何此类限制。电子数字内容商店 103 也被期望象交换所 105 一样履行此类校验，以参与将内容 113 销售到多个国家的管理。交换所 105 尽一切可能来执行此类校验，以防电子数字内容商店 103 忽略了由内容提供者 101 制定的国家特定规则。

D. 审核日志和追踪

交换所 105 对内容 113 的购买交易和报告请求交易中进行的每个操作的信息保留一份审核日志 150。这些信息可被用于多种目的，如安全数字内容电子销售系统 100 的审核、报告的产生、和数据挖掘。

交换所 105 还为电子数字内容商店 103 的帐单子系统 182 供给帐目结算。电子数字内容商店 103 的定价结构由数字内容标签提供给交换所 105。这个信息可以是那些需要告知电子数字内容商店 103 的内容，例如当前特价、批发折扣、以及帐目赤字限额等。交换所 105 用定价信息来追踪电子数字内容商店 103 的余额，并保证它们不超出由内容提供者 101 为其制定的赤字限额。

下面是由交换所 105 记录的典型操作:

- 最终用户设备 109 对许可证 SC 660 发出请求
- 当交换所 105 处理帐单时，信用卡的授权号
- 向最终用户设备 109 分发许可证 SC 660
- 对报告发出请求
- 来自最终用户的通知，表示内容 SC 630 和许可证 SC 660 已被收到并经验证。

下面是由交换所 105 为许可证 SC 660 记录的典型信息:

- 请求的日期和时间
- 购买交易的日期和时间

- 被购买的物品的内容 ID
- 内容提供者 101 的身份
- 商店使用条件 519
- 水印指令的更改
- 由电子数字内容商店 103 加入的交易 ID 535
- 电子数字内容商店 103 的身份
- 最终用户设备 109 的身份
- 最终用户的信用卡信息（如果交换所 105 正在处理帐单）

下面是由交换所 105 为验证最终用户的信用卡而记录的典型信息:

- 请求的日期和时间
- 对信用卡的收费金额
- 被购买的物品的内容 ID
- 由电子数字内容商店 103 加入的交易 ID 535
- 电子数字内容商店 103 的身份
- 最终用户的身份
- 最终用户的信用卡信息
- 从信用卡清算处收到的授权号

下面是当许可证 SC 660 被传送到最终用户设备 109 时由交换所 105 记录的典型信息:

- 请求的日期和时间
- 被购买的物品的内容 ID
- 内容提供者 101 的身份
- 使用条件 517
- 由电子数字内容商店 103 加入的交易 ID 535
- 电子数字内容商店 103 的身份
- 最终用户的身份

下面是当一个报告请求被提出时记录的典型信息:

- 请求的日期和时间

- 报告被送出的日期和时间
- 被请求的报告的类型
- 用于产生报告的参数
- 提出报告请求的实体的标识符

E. 结果报告

报告是由交换所 105 使用交换所 105 在最终用户的购买交易中记录的信息产生的。内容提供者 101 和电子数字内容商店 103 能够通过付款核实界面 183 从交换所 105 提出对交易报告的请求，使其能够用交换所 105 记录的信息协调它们自己的交易数据库。交换所 105 还可向内容提供者 101 和电子数字内容商店 103 提供周期性的报告。

交换所 105 定义一个安全电子界面，它允许内容提供者 101 和电子数字内容商店 103 去请求和接收报告。报告请求 SC 包括了一个由交换所 105 分配给提出请求的实体的认证。交换所 105 使用此认证和这个 SC 的数字签名来证实请求是由一已被授权的实体提出的。这个请求还包括了定义报告范围的参数，如持续时间。交换所 105 验证请求参数以确保请求者只能接收到它们被允许拥有的信息。

如果交换所 105 确认报告请求 SC 是真实和合法的，那么交换所 105 就产生一份报告，并将其打包入一个将被送到提出请求的实体的报告 SC 中。某些报告可以按指定间隔被定期自动地产生，并存储在交换所 105，以便这些报告能够在接收一个请求后立即送出。报告中包含的数据格式在本文件的后续版本中有所定义。

F. 帐单和付款验证

内容 113 的帐单可由交换所 105 或电子数字内容商店 103 处理。在由交换所 105 处理电子内容 113 的帐单的情况下，电子数字内容商店 103 就将最终用户订单分为电子商品和，如果适用的话，实际商品。然后电子数字内容商店 103 就将交易通知给交换所 105，包括最终用户的帐单信息以及需授权的总金额。交换所 105 对最终用户的信用卡授权，并返回给电子数字内容商店 103 一个通知。在交换所 105 对最

终用户的信用卡授权的同时，电子数字内容商店 103 可以就最终用户购买的任何实际商品对其信用卡收取费用。在最终用户设备 109 下载了所有电子物品以后，交换所 105 就会得到通知，从而向最终用户的信用卡收费。这发生在最终用户设备 109 的最后一步，是在最终用户设备 109 能够使用内容 113 之前。

在电子数字内容商店 103 处理电子内容 113 的订单的情况下，直到最终用户设备 105 将订单 SC650 传送到交换所 105，交换所 105 才被通知交易信息。在每个电子选项被下载了以后，最终用户设备 109 也通知给交换所 105。当交换所 105 被发给通知时，它就会给电子数字内容商店 103 传送一个通知，因此电子数字内容商店 103 能够从最终用户的信用卡中收取费用。

G. 重新交易

安全数字内容电子销售系统 100 提供使内容 113 重新交易的能力。这典型地由顾客服务界面 184 实现的。电子数字内容商店 103 提供了一个用户界面，最终用户可以通过它开始一个重新交易。最终用户为了请求一个内容 113 的重新交易，转到购买内容 113 的选项的电子数字内容商店 103 站点。

当最终用户请求一个新的前面购买的内容 113 选项的拷贝时，就进行内容 113 的重新交易，因为内容 113 不能下载或下载的内容 113 不能使用。电子数字内容商店 103 判断最终用户是否有权进行内容 113 的重新交易。如果最终用户有权进行重新交易，那么电子数字内容商店 103 就建立了一个交易 SC 640，它包括重新交易的内容 113 的报价 SC 641。交易 SC 640 被送到最终用户设备 109，并且最终用户执行购买交易的同样的步骤。如果最终用户设备 109 在密钥库中有一个扰频密钥，这个扰频密钥是给经历过重新交易的内容 113 选项的，那么交易 SC 640 就包含有指示最终用户设备 109 删除扰频密码的信息。

当在交换所 105 处理内容 113 购买物的财政结算时，电子数字内容商店 103 在交易 SC640 中包含有一个标志，它被直接传送到订单

SC 650 中的交换所 105。交换所 105 解译在订单 SC 650 中的这个标志，并继续交易而不需向最终用户收取内容 113 的购买的费用。

VIII. 内容提供者

综述

安全数字内容电子销售系统 100 中的内容提供者 101 是数字内容标签或拥有对内容 113 版权的实体。内容提供者 101 的作用是为销售准备内容 113，并产生内容 113 能得到的电子数字内容商店 103 或另售商可下载内容 113 的电子版本的信息。为了给内容提供者提供最大限度的安全性和版权控制，在它们上述各点，提供了一系列的工具，使内容提供者 101 能够准备并安全地将它们的内容 113 打包成 SC，因此，当内容 113 留在内容提供者 101 区域，并且从未被未授权方暴露或读取时，内容 113 是安全的。这就允许内容 113 可以遍布不安全的网络如互联网，被自由销售，而不须担心暴露给黑客或未授权用户方。

提供给内容提供者 101 工具的最终目的是准备并将内容 113 如一首歌曲或一组歌曲打包进内容 SC 630 中，并且将一些信息如描述歌曲的信息、歌曲的认证使用（内容使用条件 517）、和歌曲的促销信息打包成一个元数据 SC 620。为达到此目的，必须提供以下工具：

. 工作流程管理器 154 --- 调度处理活动，并管理请求的同步过程。

. 内容处理工具 155 --- 控制内容 113 文件制备的工具集，包括加水印，预处理（对一个声音的例子来说，任何请求的均衡，动态调节，或重新取样），编码和压缩。

. 元数据吸收和输入工具 161 --- 一工具集，用于收集内容 113 描述信息，这些信息来自于内容提供者的数据库 160 和/或第三方的数据库或数据输入文件和/或来自操作者交互作用，还用于提供方法以指定内容使用条件 517。也提供一个界面，以俘获或提取内容如 CDS 或 DDP 文件的数字声音内容。质量控制工具能够预览准备的内容和元数据。任何元数据或为进一步处理的内容的重新提交所需要的纠正能被实施。

. SC 打包工具 152 --- 将所有的内容 113 和信息加密和打包，并调用 SC 打包器打包成 SC。

. 内容分发工具（没有显示）--- 将 SC 分发到所指定的销售中心，如内容托管站点 111 和电子数字内容商店 103。

. 内容促销 WEB 站点 156 ---为下载通过已授权的电子数字内容商店 103，存储元数据 SC 620 和任意附加的促销物资。

B.工作流程管理器 154

工作流程管理器的用途是允许、追踪、和管理内容 113 的处理活动。这个应用程序可以使多个用户存取及允许调度内容 113，和在 INTRANET 或内容提供者 101 的 EXTRANET 中远端检查状态。这个设计也考虑了协作处理，在这种情况下，多个单机能同时在多个内容 113 上工作，不同的单机能被指定具体的职责，并且这些单机可以分布在全世界。

现在回到图 8，它是对应于图 7 的工作流程管理器 154 的主要处理过程的方块图。图 8 的主要过程总结了由本部分中叙述的工具提供的内容 113 的处理功能。工作流程管理器是负责向这些过程供给作业，并将作业引导给在当前过程完成的基础上的下一个被请求的过程。这是通过一系列每个处理工具调用的应用程序接口（APIs）来完成的:

- 检索下一个要处理的作业
- 指示一个成功完成的过程
- 指示一个未完成的过程及失败的原因
- 提供一个过程的中间状态（允许开始处理一个相关过程只是部分完成）
- 对制造产品得到的指定过程加注释

工作流程管理器 154 还有一个用户界面，图 7 中举例说明了工作流程管理器用户界面 700 的一个例子，它提供了如下功能:

- 一配置面板，提供在处理的不同阶段指定和执行的默认值和条件的规格说明
- 工作流程规则和自动化的处理流程的定制

- 作业安排
- 状态查询和报告
- 为一个与一个或多个处理过程相关的作业增加注释或指令
- 作业管理（即挂起，释放，移动，改变优先权（处理的订单））

每个过程有一个与被工作流程管理器 154 管理有关的队列。所有从工作流程管理器 154 请求作业的过程，都导致工作流程管理器 154 或者在当前的其相关队列中没有作业时，挂起这个过程（工具）进入等待状态，或者返有关执行它们各自的过程所必须的有关作业过程的全部信息。如果一个过程被挂起进入等待状态，那么当工作流程管理器 154 将一个作业放在它的队列上时，这个过程就会重新开始处理。

工作流程管理器 154 也根据一组定义规则，管理流程或处理的订单。如果这些规则有特殊的处理要求或配置具体默认规则的话，它能由内容提供者 101 制定。当一个过程报告它的分配的任务完成时，它就会通知该状态的工作流程管理器 154，工作流程管理器 154 根据定义的规则确定该作业下面放到什么队列上。

指示专门的操作指令或通知的注释，也可或经可编程 API，或经手工通过工作流程管理器用户界面 700 或处理器界面，在任何处理步骤被附到产品上。

在工作流程管理器 154 中的过程在优选实施例中，用 JAVA 实现，但也能用其它程序设计语言如 C/C++，汇编语言，及相当的语言实现。应该清楚，下面描述的工作流程管理器 154 过程能在许多硬件和软件平台上运行。工作流程管理器 154 作为一个完整系统或作为任何它构成的过程，可作为应用程序在计算机可读介质中销售，包括但不限于如 WEB 或在软盘、CD ROM 及可活动硬盘上电子销售

现在回到图 8，该方块图表明了对应于图 7 的工作流程管理器 154 的主要过程。以下内容概述了图 8 的各个过程，并且描述了每个过程所必需的信息或动作。

1. 产品等待动作/信息过程 801

一旦可以得到某过程所必需的全部信息，而且该作业已经成功地结束了所有的相关处理，那么作业就会被置于特定的处理队列之中。在工作流程管理 154 中存在着一个专用的队列，它通常接受具有下述特征的作业：由于缺少信息或者产生了错误阻碍进一步处理，作业目前还得不到处理。这些作业都被存放在产品等待动作/信息过程 801 队列里。这个队列中的每个作业都和某个状态相关联，该状态指示它正在等待的动作或者信息，作业处理过的最后一步过程，以及一旦提供了缺少的或另外的信息或者所需的动作成功地完成后，此作业被加到队列中的下一步或几步过程。

任何过程的结束都会导致工作流程管理器 154 去检查这个队列，并且判断这个队列中的任一作业是否等待由该过程提供的处理（动作）或者信息的结束。假如是这样的话，那个作业将会被加入到合适的处理队列之中。

2. 新内容请求过程 802

内容提供者 101 确定那些希望以电子方式销售和交付的产品（譬如，它可以是一首歌或者是歌曲集）。工作流程管理器 154 的初始功能是使操作者标识这些产品，并且将它们存放在新内容请求过程 802 的队列中。通过配置选项，内容提供者 101 可以指定在产品选择界面上提示什么样的信息。输入足够的信息以唯一地标识产品。另外，可以选择包含额外的字段，以要求手工输入与元数据获取并行起动音频处理阶段所需要的信息。如果不提供手工方式，这种信息可选择从默认的配置设置或者从内容提供者的数据库 160 中检索，在元数据处理的第一个阶段获取它，就象在自动元数据获取过程 803 中一样。内容提供者的数据库 160 中内容 113 的结构和能力决定了内容选择过程。

如果指定了为实现对内容提供者 101 的数据库 160 进行查询所需的信息，那么该作业将由自动元获取过程 803 来处理。在音乐实施例中，为合适地调度产品作音频处理，既要指定产品的类型和要求的压缩级别，又要指定 PCM 或 WAV 音频文件名称。这种信息可当作产

品选择过程部分来输入，或者通过一个用户化的查询界面或 Web 浏览器功能来选择。这种信息的详细说明使得产品能够被调度去作内容处理。

产品选择用户界面提供了一个选项，该选项使得操作者能够确定某产品是否被释放以进行处理或者被挂起以等待进一步的信息输入。如果被挂起，作业将加入到新内容请求过程 802 的队列之中，以等待进一步的动作以完成数据输入和/或释放产品以进行处理。一旦产品被释放，工作流程管理器 154 就评价被指定的信息而且决定作业中那些过程要被通过。

如果提供了足够的信息使得能够对内容提供者 101 的数据库 160 作自动查询，那么该作业将加入到自动元数据获取过程 803 的队列之中。如果还没有为自动元数据获取过程 803 建立好数据库映射表，那么该作业将加入到人工元数据输入过程 804 的队列之中（细节可参考自动元数据获取过程 803 中关于数据库映射表的部分）。

如果指定了必需的用于音频处理的普通信息和用于水印的特殊信息，该作业将加入到水印过程 808 的队列之中（内容处理的第一阶段）。如果在作业被释放时还缺少任何必需的信息，那么该作业连同指示缺少的信息的状态一起将加入到产品等待动作/信息过程的队列之中。

如果状态指示的是内容 113 的文件名，例如这里内容 113 是音频，而且其 PCM 或 WAV 文件丢失，那么这可能表明必需获取（或从数字介质上数字抽取）。音频处理功能要求通过一个标准的文件系统界面可以存取歌曲文件。如果歌曲被存放在外部介质或者一个不能直接为音频处理工具访问的文件系统里，那么这些文件将首先被拷贝到一个可被访问的文件系统之中。如果歌曲是数字格式但是在 CD 或数字磁带上，那么它们将会被抽取到一个可被音频处理工具访问的文件系统中。一旦这些文件都可以被访问，工作流程管理用户界面 700 就被使用为作业指定或选择路径和文件名称，使得该作业能被释放到加水印过程里，假定加水印所必需的所有其它信息已经指定了。

3. 自动元数据获取过程 803

自动元数据获取过程 803 对内容提供者 101 的数据库 160 或已输入数据的分级数据库执行一系列的查询，以使得在自动模式下尽可能多地得到产品信息。自动元数据获取过程 803 要求在将可能的选项加入它的队列之前先要求下列信息:

· 带有能对内容提供者 101 的数据库 160 产生查询的足够信息的数据库映射表。

· 执行查询要求的产品信息。

· 能唯一地定义产品的足够的产品信息。

为了获得处理内容 113 所必需的信息，对内容提供者 101 的数据库 160 执行一个自动查询。例如，如果内容 113 是音乐，那么执行这个查询所必需的信息可能是一套唱片的名称，也可能是 UPC 或一特殊唱片集或一类似被内容提供者 101 所定义的选择标志符。在所要获得的信息中，有的在需要时被指定（详细信息参考自动元数据获取过程 803 部分）。如果获得了所有的必需的信息，那么该作业将在下一个加入到使用条件过程 805 的队列之中。如果缺少任何必需的信息，那么该歌曲将加入到手工元数据输入过程 804 的队列之中。如果在产品等待动作/信息过程 801 队列里的任何作业正在等待在这一步骤中获得的任一信息，那么作业状态将更新，以表示该作业不再等待这类信息。如果那个作业已经没有任何突出的要求，那么它将加入到下一个被定义的队列之中。

4. 手工元数据输入过程 804

手工元数据输入过程 804 为操作者提供了一种输入缺少的信息的方法。它没有相关性条件。一旦指定了所有必需的信息，该作业就将加入到使用条件过程 805 队列之中。

5. 使用条件过程 805

使用条件过程 805 允许对产品的使用和限制条件进行详细说明。使用条件过程 805 可能会要求某些元数据。使用条件详细说明一完成，该作业就被认为符合加入到元数据 SC 创建过程 807 队列的条件，除非在受监督发行过程 806 的选项中已被求或者象工作流程管理器 154

规则中的默认值一样地被设定。在这种情况下，作业将加入到受监督发行过程 806 的队列之中。在加入到元数据 SC 创建过程 807 的队列之前，工作流程管理器 154 将首先保证此过程的所有需要都已得到满足（参考以下内容）。如果不这样的话，作业将加入到产品等待动作/信息过程 801 的队列之中。

6. 受监督发行过程 806

受监督发行过程 806 允许进行质量检查和对为数字内容产品指定的信息的合法性进行验证。它没有任何相关性。在处理产品的任何阶段先前附属于该作业的注释可以被监督器或采取的适当的动作再检查。在再检查所有的信息和注释之后，监督器有下列选项:

· 批准发行以及为元数据 SC 创建过程 807 进行产品排队。

· 修改和/或增加信息以及为元数据 SC 创建过程 807 进行产品排队。

· 为作业增加注释以及为人工元数据输入过程 804 进行再排队。

· 增加注释和将作业排队到产品等待动作/信息过程 801 的队列中。

7. 元数据 SC 创建过程 807

元数据 SC 创建过程 807 将上面收集的所有信息和元数据 SC620 所要求的其它信息聚集在一起，并调用 SC 打包过程，以生成元数据 SC620。这种工具要求下列输入:

· 要求的元数据。

· 使用条件。

· 在这种产品全部质量级别的加密阶段中使用的加密密钥。

这里最后的相关性要求就是在元数据 SC620 可被生成之前，相关的音频对象必须完成音频处理阶段。元数据 SC 创建过程 807 一旦完成，该作业就或者加入到最终质量保证过程 813 的队列，或者加入到基于工作流程规则所定义的内容发放过程 814 的队列中。

8. 加水印过程 808

加水印过程 808 添加版权和其它信息到内容 113 中。对于其内容

113 是一首歌的实施例，这种工具要求下列内容作为输入：

· 歌曲文件名称（如果是唱片集则为多个文件名称）。

· 加水印指令。

· 水印参数（要被包括在水印中的信息）。

加水印过程 808 一完成，如果作业要求的输入是可用的，那么该作业将加入到预处理和压缩过程 809 的队列之中，否则的话，将加入到产品等待动作/信息过程 801 的队列之中。

9. 预处理和压缩过程 809

预处理和压缩过程 809 首先执行任一要求的预处理，用指定的压缩级别将内容 113 编码。将一个作业加入到这个队列中实际上产生了多个队列输入。对所要产品的每个压缩级别创建一个作业。编码过程在多个系统上可并行执行。这种工具要求有下列输入：

· 标有水印的内容的文件名（若内容 113 是一歌曲集，则为多个文件名）。

· 产品质量级别（可以被预设定）。

· 压缩算法（可以被预设定）。

· 产品种类（如果预处理器需要的话）。

编码过程一结束，如果已被工作流程规则所设定，作业都将加入到内容质量控制过程 810 的队列之中。如果没有设定，作业则都将加入到加密过程 811 的队列之中。

如果编码工具的第三方提供者不提供方法以显示已经被处理过的内容 113（例如音频）的百分比，或者不提供方法以表明已被编码的内容 113 的总量占选定内容 113 中全部选择的百分比，在图 11 中给出了一张方法流程图 1100，以为图 8 的内容预处理和压缩工具确定数字内容的编码率。方法开始于步骤 1101，选择所期待的算法和位率。接着，在步骤 1102，进行查询以确定这种算法和编码率是否已有一个先前计算出的比率因子。这个比率因子常常用来确定对一个特定的编码算法和一个特定的位率的压缩率。如果没有储存预先计算出的比率因子，那么将为一个预确定的时间总量对内容 113 的一个采样进行编码。

在优先实施例中预确定的时间周期为几秒钟。这种预确定的时间周期的编码率被用于计算出一个新的比率因子 R_{NEW}。已知时间总量和已被编码的内容 113 的总量计算一个新的比率因子的公式为：R_{NEW}=（被编码的数字内容的长度）/（时间总量），步骤 1108。内容 113 被编码而且通过使用先前计算出的比率因子 R_{NEW} 来显示编码状态，步骤 1109。然后储存这个编码率因子 R_{NEW}，步骤 1107，为这种编码算法和编码比特率以备将来使用。如果被选定的算法已有一个先前计算出的比率因子 R_{STORED}，步骤 1103。内容 113 被编码而且通过使用先前计算出的比率因子 R_{STORED} 显示进度,步骤 1104。同时，将为这个被选定的算法和比特率计算出一个当前的比率因子 $R_{CURRENT}$，步骤 1105。这个当前的比率因子 $R_{CURRENT}$ 被用于更新储存的比率因子 R_{NEW}=（R_{STORED}+$R_{CURRENT}$）/2，步骤 1106。比率因子的重复更新使得对于特定的编码算法和比特率，编码率的确定随着后续的每次使用变得越来越精确。接着，新的比率因子 R_{NEW} 被储存起来以备将来使用，步骤 1107。如果当前的比率因子 $R_{CURRENT}$ 超出了先前储存的比率因子 R_{STORED} 一给定的范围或门限，那么 R_{STORED} 可以不作更新。

随后编码状态表示被显示。编码状态包括：作为一个基于内容 113 的编码率和文件总长度的进度条来显示的总的内容 113 的百分比的显示，以及当前的编码率。编码状态也包括编码剩余时间。编码剩余时间通过内容 113 的文件的总长度除以计算出的编码率 $R_{CURRENT}$ 而能计算出。编码状态能被转移到另一个可以要求调用过程的程序里。这将有助于监督程序编码或者交叉相关性程序进行的编码及更有效的批处理编码。在一可供替代的实施例中，可以理解编码包括了加水印步骤。

10. 内容质量控制过程 810

内容质量控制过程 810 在功能上类似于受监督发行过程 806。这是一个可选的步骤，它允许人去验证迄今为止已被执行的内容处理的质量。除了结束水印过程 808 和预处理和压缩过程 809 的编码部分外，这里没有其它相关性。内容质量控制过程 810 一结束，下列选项成为可用：

·作业能被释放以及被加入到加密过程 811 的队列之中。

·注解能被附上而且一个或多个作业能再入预处理和压缩过程 809 队列之中。

最后的选项要求歌曲文件的带有水印标志的未编码的版本保持可用状态直到内容质量控制过程 810 之后。

11. 加密过程 811

加密过程 811 调用适当的安全数字内容电子销售版权管理功能，以加密每个带有被加水印标志/被编码的歌曲文件。这过程除了完成所有其它的音频处理外没有其它相关性。加密过程 811 一结束，作业就将加入到内容 SC 创建过程 812 的队列之中。

12. 内容 SC 创建过程 812

内容 SC 创建过程 812 可能会要求在内容 SC630 中包括一些元数据文件。如果需要除了内容 113 以外的其它文件，那么将收集文件而且调用 SC 打包过程，以为内容 113（例如一首歌）的每一个压缩级别生成一个内容 SC630。内容 SC 创建过程 812 一结束，根据规定的工作流程规则该歌曲就将被加入到最终质量保证过程 813 的队列，或者被加入到内容发放过程 814 的队列之中。

13. 最终质量保证过程 813

最终质量保证过程 813 是一个可选步骤，它允许在相关联的元数据和内容 SC630 之间进行交叉访问检查，以核实它们能够正确匹配以及所有的包含于其中的信息和内容 113 是正确的。最终质量保证过程 813 一结束，作业将加入到内容发放过程 814 的队列之中。如果发现了问题，那么在大多数情况下作业将不得不重新加入到故障阶段的队列之中。这个阶段重复工作的代价是非常高的，因为除了再处理以改正问题外，产品不得不重新加密和重新打包。强烈推荐采用前面的保证阶段，以确保内容 113 的质量以及信息的精确性和完整性。

14. 内容发放过程 814

内容发放过程 814 的功能是将 SC 发放到合适的托管站点。在 SC 成功传送之后，作业的结束状态被记录，而且作业从队列中删除。如

果在传送 SC 时有问题发生，在重试规定次数之后，作业被标记并与遇到的错误一起，在工作流程管理器工具 154 中作出错处理。

15. 工作流程规则

图 8 的工作流程规则在如下的三个主要系统中起作用：

A. 工作流程管理器工具 154

1. 新内容请求过程 802

2. 产品等待动作/信息过程 801

3. 最终质量保证过程 813

4. 内容发放（和通知）过程 814

B. 元数据吸收和输入工具 161

1. 自动元数据获取过程 803

2. 手工元数据输入过程 804

3. 受监督发行过程 806

4. 元数据 SC 创建过程 807

C. 内容处理工具 155

1. 加水印过程 808（要求版权数据）

2. 预处理和压缩过程 809

3. 内容质量控制过程 810

4. 加密过程 811

5. 内容 SC 创建过程 812

工作流程

内容 113 的选择操作者输入一个新的产品，它将开始出队列到 A1（新内容请求过程 802）。

A1: 当内容 113 的选择的操作者释放它到工作流程管理器工具 154 中时，它将入队列到 B1 之中（自动元数据获取过程 803）。

A2: 来自步骤 B1（自动元数据获取过程 803），

或步骤 B2（手工元数据输入过程 804），

或步骤 B3（受监督发行过程 806），

转向步骤 Before（元数据 SC 创建过程 807），

[需要加密密钥]。

来自步骤 Before（元数据 SC 创建过程 807）

转向步骤 A3（最终质量保证过程 813）或步骤 A4（内容发放过程 814）

[需要内容 SC630]。

来自步骤 C1（加水印过程 808）

转向步骤 C2（预处理和压缩过程 809）

[需要预处理和压缩过程的元数据]

来自步骤 C4（加密过程 811）

转向步骤 C5（内容 SC 创建过程 812）

[需要内容 SC630 打包的元数据]

来自步骤 C5（内容 SC 创建过程 812）

转向步骤 A3（最终质量保证过程 813）或步骤 A4（内容发放过程 814）

[需要元数据 SC620]

A3: 在步骤 A3（最终质量保证过程 813）之后，

入队列 B2（手工元数据输入过程 804），

或者入队列 B3（受监督发行过程 806），

或者加入到质量保证操作者所必需的队列之中。

A4: 在步骤 A4（内容发放过程 814）之后，

为该产品工作流程管理器工具 154 已完成。

B1: 在步骤 B1（自动元数据获取过程 803）之后，

if 步骤 C1（水印过程 808）所必需的元数据存在，then 将一个表示该产品的输入加入到队列 C1。

（也作如下逻辑）

if 不是 1 丢失了任何必需的元数据，就是 2 存在注释直接指向手工元数据提供者，then 也将该产品加入到队列 B2（手工元数据输入过程 804），

else if 该产品要求受监督发行 then 将该产品加入到队列

B3（监督发行过程 806），

else if 产品已有了来自于内容处理工具 155 的所有请求的质量级别的全部信息 then 将该产品加入到队列 Before（元数据 SC 创建过程 807）

else 根据需要加密的密钥标志该产品，及将它加入到队列 A2（产生等待动作/信息过程 801）。

B2: 在步骤 B2（手工元数据输入过程 804）中，

if 步骤 C1（水印过程 808）还未完成 and 步骤 C1 所需要的元数据被显示，then 将一个表示该产品的输入表示加入到队列 C1。

（也作如下逻辑）

if 正好提供了步骤 C2（预处理和压缩过程 809）所需要的元数据， then

（也作如下逻辑）

if 所有的元数据显示能被元数据吸收和输入工具 161 收集，

then

if 该产品监督发行被请求

then 将该产品加入到队列 B3（监督发行过程 806）

else

if 所有来自内容处理工具 155 的步 C4 的信息被显示（加密过程 811），then 将该产品加入到队列 before（元数据创建过程 807）

else 标志按需要加密的密钥标志产品，且将该产品加入到队列 A2（产生等待动作/信息过程 801）之中。

else

if 元数据提供者要求强制性的监督发行 then 将该产品加入到队列 B3（监督发行过程 806）

else 空操作（将产品保持在队列 B2（手工元数据输入过程

804））。

B3: 在 B3（受监督发行过程 806）时，

if 这个操作者正在发送产品，返回步骤 B2（手工元数据输入过程 804），then 将该产品加入到队列 B2 之中。

else if 这个操作者已发行该产品，then

if 所有来自内容处理工具 155 的步 C4 的信息被显示（加密过程 811），then 将该产品加入到队列 before（元数据 SC 创建过程 807）

else 标志按需要加密的密钥产品，且将该产品加入到队列 A2（产生等待动作/信息过程 801）之中。

else 产品仍留在队列 B3（监督发行过程 806）之中。

Before: 在步骤 Before （元数据 SC 创建过程 807）之后，标志产品元数据已被打包。

if 所有的（产品/质量级别）元组都已打包，then

if 内容提供者 101 的配置指定的质量保证 SC，

then 将该产品加入到队列 A3（最终质量保证过程 813）

else 将该产品加入到队列 A4（内容发放过程 814）。

else 标志按需要的内容 113SC 的产品，且该产品加入到队列

A2（产生等待动作/信息过程 801）。

C1: 在步骤 C1 之后（水印过程 808），

if 步骤 C2（预处理和压缩过程 809）所需要的元数据存在 then 为每一个（产品/质量级别）元组创建一个输入，然后将它们加入到队列 C2，

else 标志按需要进行预处理/压缩的元数据产品，且将该产品加入到队列 A2（产生等待动作/信息过程 801）。

C2: 在步骤 C2（预处理和压缩过程 809）之后，

if 内容提供者 101 的配置指定了内容质量控制过程 810，then 将该（产品/质量级别）元组加入到队列 C3（内容质量控制过程 810），

else 将该（产品/质量级别）元组加入到队列 C4（加密过程 811）

之中。

C3: 在步骤 C3（内容质量控制过程 810）之后，将该（产品/质量级别）元组加入到队列 C4（加密过程 811）之中。

C4: 在步骤 C4（加密过程 811）之后，将所需的信息（即：由过程产生且常用于将内容 113 译码的对称密钥）提供给元数据吸收和输入工具 161。

if 已有了内容 SC630 所必需的元数据 then 将这个（产品/质量级别）元组加入到队列 C5（内容 SC 创建过程 812）中，

else 标志为内容 SC630 进行打包需要的元数据产品，

将这个（产品/质量级别）元组加入到队列 A2（产生等待动作/信息过程 801）中。

C5: 在步骤 C5（内容 SC 创建过程 812）之后，标志质量级别而在该质量级别中内容 113 已被打包。

if 所有的（产品/质量级别）元组都已经被打包， then

if 产品被标志的元数据已被打包 then

if 内容提供者 101 的配置指定了质量保证 SC，then 将这个产品加入到队列 A3（最终质量保证过程 813）之中

else 将这个产品加入到队列 A4（内容发放过程 814）之中

else 标志需要的元数据 SC620 产品，且将这个产品加入到队列 A2（产生等待动作/信息过程 801）之中。

else （所有的（产品/质量级别）元组都未被打包）空操作

（另一个（产品/质量级别）元组触发一个动作）。

C. 元数据吸收和输入工具

元数据是由描述内容 113 的数据构成的，例如音乐，唱片标题、艺术家、作词家/作曲家、生产商和唱片的长度。下列描述默认内容 113 是有关音乐的，但是熟悉本领域技术的人能够将它理解为其它的内容类型（例如：视频、节目、多媒体、电影等等）都在本发明实际范围和意思之内。

这个子系统将某些数据聚集在一起，这些数据包括内容提供者 101 提供给电子数字内容商店 103 以帮助产品销售的数据（例如：对音乐而言，其产品包括该艺术家的样例片段、该艺术家的历史、唱片出现在唱片集上的表、和该艺术家以及/或者产品相关的流派），也包括内容提供者 101 提供给购买产品（例如：艺术家、生产商、图集封面、磁道长度）的最终用户的数据，以及内容提供者 101 欲提供给最终用户的不同的购买选项（使用条件 517）。数据打包到元数据 SC620 中，而且对电子数字内容商店 103 而言应是可用的。

为了实现上述目的，提供了下面的工具：

. 自动元数据获取工具

. 手工元数据输入工具

. 使用条件工具

· 受监督的发行工具

这些工具使得内容提供者 101 能够实现上面关于工作流程管理器 154 中所描述的过程。这里说的工具是优先实施例中基于 Java 的一个工具箱，但是也可以使用其它的编程语言，例如 C/C++、汇编语言等等。

1. 自动元数据获取工具

自动元数据获取工具给用户提供了实现上述自动元数据获取过程 803 的功能。自动元数据获取工具常常用来访问内容提供者 101 的数据库 160 以及在没有操作者支持时尽可能多的检索数据。配置方法对于使该过程自动化来说是可用的。内容提供者 101 能够制作默认的数据模板，用该数据模板来标识内容提供者 101 欲提供给最终用户（例如：作曲家、生产商、伴奏者、音轨长度）的数据类型，也用来标识内容提供者 101 提供给电子数字内容商店 103（例如：对音乐而言，包括该艺术家的样例片段、该艺术家的历史、这张唱片出现过的歌曲集的列表、和该艺术家相关的流派）的促销数据类型。默认的数据模板包括：最终用户设备 109 所必需的数据字段，能选择性提供给最终用户设备 109 的数据字段以及一套为电子数字内容商店 103 所用的用

以促销艺术家、歌曲集、和/或者单个歌曲的数据字段样例集。

为了从内容提供者 101 的数据库 160 中提取模板数据字段，自动元数据获取工具使用了一张表，该表映射数据类型（例如：作曲家、生产商、艺术家传记）到数据库中数据能被找到的位置。每个内容提供者 101 都帮助指定适合其环境的映射表。

自动元数据获取工具使用内容提供者 101 的元数据模板和映射表，以从内容提供者 101 的数据库 160 中获取任何可利用的数据。每个产品的状态随着自动元数据获取过程 803 的结果而更新。还缺少任何必需数据的产品被加入到手工元数据输入过程 804 的队列之中，否则，可用于打包到元数据 SC620 中。

2. 手工元数据输入工具

手工元数据输入工具给用户提供了实现上述手工元数据输入过程 804 的功能。手工元数据输入工具允许任何被合适授权的操作者提供缺少的数据。如果该操作者确定缺少的数据难以获得，那么他可以给产品附加说明，而且请求监督发行。因为质量保证的原因，内容提供者 101 可以要求产品进行监督发行。一旦有了所有必需的数据，而且如果不再要求监督发行，那么产品打包到元数据 SC620 是可行的。

3. 使用条件工具

使用条件工具给用户提供了实现上述使用条件过程 805 的能力。通过使用电子交付为内容 113 的销售和租赁（受限制的使用）报价的过程 113 包括到一系列的商业决定。内容提供者 101 可决定哪一个压缩级别内容 113 变为可用。而后对内容 113 的每一个经过压缩且已被编码的版本都指定了一个或多个使用条件。每个使用条件定义了关于使用内容 113 的最终用户的权限以及所有对最终用户的限制条件。

使用条件定义：

1. 这个使用条件所适用的内容 113 的压缩编码的版本。

2. 这个使用条件所包括的用户类型（例如：商业、个人消费者）。

3. 这个使用条件是否允许对内容 113 的购买或者租赁。

对于租赁交易:

· 通常用于限制租赁条款的度量单位。(例如: 天数, 播放次数)。

· 多少天, 播放多少次之后内容 113 将不再演播。

对于购买交易:

· 允许最终用户制作的可播放的拷贝的数量。

· 他/她使用哪些类型的介质制作那些拷贝(例如: 可刻光盘 CD-R, MiniDisk, 个人计算机)。

4. 允许购买/租赁交易发生的时间期间(即: 仅仅只有在有效开始日期之后和在最后有效日期之前, 最终用户才可能进行购买和租赁)。

5. 最终用户能够从其进行这桩购买(租赁)交易的国家。

6. 在这种使用条件下的购买/租赁交易的价格。

7. 水印参数。

8. 需要通知交换所 105 的事件类型。

设置使用条件的一个例子

内容提供者 101 可以决定测试北美市场在 1997 年第四季度期间对少年流行歌手的少年歌曲的再版的接受能力。测试将以两种不同的压缩编码版本得到该歌曲: 384Kbps 和 56Kbps。384Kbps 版本可以购买(并且一个拷贝制作在 MiniDisk 上)或租赁(两个星期), 而 56Kbps 版本仅仅只能购买(而且不制作拷贝)。水印指令对于任何购买/租赁来说是一样的, 内容提供者 101 让交换所 105 去计算每次制作的拷贝。这将产生以下的使用条件:

	使用条件 1	使用条件 2	使用条件 3
压缩编码版本	384Kbps	384Kbs	56Kbps
用户类型	个有消费者	个人消费者	个人消费者
交易类型	购买	租赁	购买
上市日期	1997 年 10 月 1 日至 1997 年 12 月 31 日	1997 年 10 月 1 日至 1997 年 12 月 31 日	1997 年 10 月 1 日至 1997 年 12 月 31 日
国家	美国和加拿大	美国和加拿大	美国和加拿大
水印	标准	标准	标准
通知事件	复制行为	无	无
复制次	1	0	0
至什么媒体	MiniDisc	不适用	不适用
租赁期限	不适用	14 天	不适用
价格	价格 1	价格 2	价格 3

4．元数据 SC620 部分

以下是元数据吸收和输入工具 161 收集的某些种类的数据，这些数据将包含在元数据 SC620 之中。尝试着将这些数据按功能和目的地编组到 SC 的各部分。

产品 ID [src:内容提供商;]

[dest:每个人;]

许可方标签公司 [dest:EMS;最终用户;]

被许可方标签公司 [dest:EMS;最终用户;]

该对象的源（出版商） (分被许可方标签公司) [dest:每个人;]

对象类型 (即,单个对象或一组对象)

对象 ID [dest:每个人;]

国际标准记录码 (ISRC)

国际标准音乐号 (ISMN)

使用条件(src:内容提供商;dest:EMS,最终用户,交换中心 105)
购买的使用条件 (src:EMS;dest:最终用户,交换中心 105)
使用条件集(消费者限制和权利), 对于使用对象
(声音记录)
使用条件组中的单个入口
该使用条件适用的内容 113 的压缩编码版本
该使用条件是否允许购买或租赁内容 113
对于租赁交易:
用于限定租赁期限的测量单位 (如, 日,播放).
在其后不再播放内容 113 的上述单位的数量.
对于购买交易:
允许最终用户制作的可播放拷贝的数量.
可以在什么媒体上制作拷贝 (如, 可录式 CD (CD-R),
MiniDisc, 个人计算机).
允许进行购买/租赁交易的时间段
(即, 最终用户在开始上市日期之后和在上市最后日期之间可以购买/租赁)
指向最终用户可以进行购买或租赁的国家的指针
在这种使用条件下的购买/租赁交易价格
指向加密水印指令和参数的指针
指向需要通知交换中心 105 的事件类型的指针

购买数据 (加密的; 可选信息; src:EMS;dest:最终用户, 交换中心 105)
购买日期
购买价格
帐单发往姓名和地址
消费者姓名和地址
消费者国家(最佳猜测)

无数据 1 (src: 内容提供商; dest: EMS, 最终用户)

一组 {

版权信息

对于作者

对于录音

歌曲名称

主要演员

}

可选信息:

一组附加信息 {

作曲

出版商

制片

乐队

录音日期

发行日期

歌词

轨道名 (解密)/轨道长度

有该记录的唱片集清单

类别

}

无数据 2 (src: 内容提供商; dest: EMS)

一组结构, 每个结构代表不同质量级的相同声音

记录{

声音记录;

声音记录级;

（有可能压缩的）声音记录的尺寸（以字节为单位）；

}

元数据 3 (src: 内容提供商; dest: EMS, 最终用户)

可选信息;

促销材料:

指向演员促销材料的指针{

至演员 WEB 站点的 URL;

演员的背景说明;

与演员有关的访谈(带访谈格式 (如, 文本, 音频, 视频));

访谈(带访谈格式 (如, 文本, 音频, 视频));

最近和将来的音乐会/露面/活动-日期和地点;

}

指向唱片集促销材料的指针{

样品片段(及其格式和压缩级);

制片商的背景说明,和/或作曲, 和/或电影/戏剧/广播,

和/或唱片集的制作, 等.;

与非演员有关的访谈(带访谈格式 (如, 文本, 音频, 视频));

访谈(带访谈格式 (如, 文本, 音频, 视频));

类别;

}

单个促销:

样品片段(及其格式和压缩级);

制片商的背景说明,和/或作曲, 和/或电影/戏剧/广播,

和/或该单个促销的制作, 等.;

样品片段(及其格式和压缩级);

访谈(带访谈格式 (如, 文本, 音频, 视频));

5． 监督发行工具

监督发行工具给用户提供了实现上述监督发行过程 806 的能力。由内容提供者 101 个别指定拥有监督发行权限者，它可以调用一个正在等待受监督发行的产品（即：监督发行过程 806 的队列中的一个产品），检查它的内容 113 及其相关内容，要么

批准它的内容 113 而且发放该产品以打包到元数据 SC620 之中

或者

进行必要的改正而且发放该产品以打包到元数据 SC620 之中

或者

添加注解指出采取的改正动作并再提交该产品加入到手工元数据输入过程 704 之中。

在另一个实施例中，在生成 SC 之后，存在着另一个可选的质量保证步骤，在该步骤中可以打开 SC 的内容 113 和检查它的完整性和精确性，同时，为产品的发行以进入到零售通道而进行最后的批准或否定。

D. 内容处理工具

内容处理工具 115 实际上是一个软件工具的集合，这些软件用于处理数字内容文件，以产生内容的加水印，编码和加密的拷贝。这些工具利用了工业标准数字内容处理工具，以便随其发展用加水印，编码和加密技术，进行插入式的更换。如果选择的工业工具可通过命令行系统调用界面被加载并且传递参数或提供一个工具包，其中的函数可通过 DLL 接口调用，那么内容的处理就能自动化到一定程度。每一工具的前端应用软件为下一可用到的作业查询内容处理工具 115 中的合适队列，检索需要的文件和参数，然后装载工业标准内容处理工具以实现所需要的功能。一旦任务完成，如工具不报告终止状态则可能要求手工更新队列。

虽然仅描述了内容处理工具 115 的通用版本，但用户化还是可能的。内容处理工具 115 可用 JAVA，C/C++或其它类似的软件编写。内容处理工具 115 可用任何微机可读装置包括软磁盘、CD 或通过 Web 站点进行传递。

1. 加水印工具

加水印工具给用户提供了实现上述加水印过程 808 的能力。这个工具利用音频水印技术把内容 113 所有者的版权信息加到歌曲文件中。实际写出来的信息取决于内容提供者 101 和选定的具体加水印技术。该信息对前端加水印工具可用的，以便它可合适地把该信息传给加水印操作。这迫使对元数据吸收和输入工具 161 的同步请求，以确保它已经优先获得了该信息，比如说，允许歌曲的音频文件被处理。只有得到了水印信息歌曲才可以进行音频处理。

在音频处理中水印作为第一步被加上，这是因为对于所有创建的歌曲的编码来说它是公共的。只要经编码后水印继续存在，那么对每首歌曲来说加水印过程仅需出现一次。

已知各种各样的加水印技术并且都可以通过商业途径得到。然而前端加水印工具能够支持各种工业水印工具。

2. 预处理和压缩工具

预处理和压缩工具给用户提供了实现上述预处理和压缩工具过程 809 的能力。音频编码涉及到两个过程。对于一个音乐内容的例子，相对于 PCM 音频流，其编码基本上是一个有损耗压缩算法的应用。编码器通常根据要求的音频质量级别能被调整产生各种各样的重放位流率。较高的质量会导致文件较大，而因为对于高质量的内容 113 文件尺寸能变得相当大，所以高质量内容 113 的下载时间会变长而且在标准 28800bps 的调制解调器上它有时是会被禁止的。

因此，内容提供者 101 可以有选择地提供各种数字内容质量供下载，以便既满足没有耐心而带宽又窄的用户，他不想为下载而长时间地等待，又满足唱片爱好者或高带宽用户，他们或者只购买高质量内容 113 或者拥有高速接入。

压缩算法随技术上不同产生内容 113 的较低位率的复制品。技术的不同源于算法（即：MPEG，AC3，ATRAC）和压缩级别两者。为了得到较高的压缩级别，在被传送到压缩算法之前，通常对数据以较低的采样率进行再次采样。为了使得较少损失保真度或者为了防止某

些频率范围剧烈地跌落并更有效地压缩，数字内容有时也要求进行调整以均衡某些频率的级别或者对录音的力度进行调整。内容预处理要求直接和压缩算法和压缩级别相关。在某些情况下，因为相同流派的歌曲具有类似的力度，内容 113 的风格（例如：音乐流派）常常被成功地用作确定预处理要求的基础。对于某些压缩工具，这些预处理功能是编码过程的一部分。对于其它的，要进行的预处理比压缩优先执行。

除了为销售可下载的音频文件外，每首歌都有一个低位率（LBR）编码片段以允许通过 LBR 流协议对该歌曲进行试样。这个 LBR 的编码也由内容处理工具 155 负责。该片段或者作为一个独立的 PCM 文件或者作为位移和长度的参数由内容提供者 101 提供。

至于加水印，通常希望通过一个 DLL 或命令行系统调用接口能装载编码工具，而且传递预处理和压缩所要求的全部参数。前端编码工具和图元数据吸收和输入工具 161 可能有同步要求，比如说，如果内容是有关音乐的，而且如果确切知道该歌曲的类型是在执行任何音频预处理之前获取于内容提供者的数据库 160。这依赖于所选择的编码工具以及该歌曲的类型是怎么不确定的。如果内容提供者 101 对每一首歌曲改变其编码质量级别的选择，那么也应该在编码步骤之前提供这种信息，而且和由元数据吸收和输入工具 161 生成的元数据保持一致。

现在已经知道各种各样的高质量编码算法和工具。然而前端编码工具能够支持各种工业编码工具。

现在转向图 12，图 12 显示了对应本发明的图 8 中的自动元数据采集工具的一个实施例的流程图。该过程开始于从内容提供者 101 正在检查的介质上读取一个标识符。内容的一个实施例是一个音频 CD 实施例。在音频 CD 实施例中，可得到下列代码：通用价格代码(UPC)，国际标准记录码(ISRC)，国际标准音乐号(ISMN)。这个标志符由适当的内容播放器读出，例如用于音频 CD 的音频 CD 播放器、用于 DVD 电影的 DVD 播放器、用于 DAT 录音的 DAT 录音机等等，见步骤 1201。

接着，这个标志符被用于为内容提供者 101 对数据库 160 进行索引，见步骤 1202。正图 8 中描述的工作流程管理过程所必需的部分或全部信息在数据库 160 和任何其它相关的资源中被检索，见步骤 1203。这种信息可以包括内容 113 和与之相关的元数据。在步骤 1204 中，被检索到的附加信息被用于启始工作流程管理器 154 以创建电子内容 113。应当理解的是，对于介质的几种选择，例如几种音频 CDS，能排成队列以便使得自动元数据获取工具能够为电子销售而创建一系列的内容 113。例如，所有的内容 113 的创建可以源于由内容提供者 101 所检查的一系列 CD 或者甚至是一张或多张 CD 上所选磁道。

在一个可供选择的实施例中，预处理参数可从内容提供者的数据库 160 中被自动地检索到。现在所见到的图 13 是一张自动设置对应本发明的图 8 中预处理和压缩工具的预处理和压缩参数的一种方法的流程图。在该实施例中，内容 113 是音乐。在步骤 1301，音乐（内容 113）被选择以在内容处理工具 155 内进行编码。步骤 1302 所选定的音乐的类型被确定。这能够被手工输入或者使用其它可得到的元数据，例如从图 12 中描述的过程中检索到的附加数据。然后，被选定的音频压缩级别和音频压缩算法被检查，见步骤 1303。接着，通过类型、压缩设置以及在预处理和压缩过程 809 中应当使用的压缩参数的压缩算法来进行查找。

3. 内容质量控制工具

内容质量控制工具向用户提供了实现上述内容质量控制过程 810 的功能。这是一个可选的内容处理工具，它给质量控制技术人员提供了再审查已被编码并加了水印的内容文件的机会，并且依据对内容文件质量的判断将其批准或者丢弃。技术人员能通过进行人工的预处理调整来对内容重新编码直到质量令人满意，或者对歌曲加入标志以重新处理并加入一个描述问题的注解。

这个处理步骤可以被内容提供者 101 配置作为内容处理工作流程的一个可选的或必需的步骤。一个附加的可选最终质量保证过程 813 步骤可在内容的所有 SC 都被打包（即对 CD 上每只歌的 SC）后提供，

在此时对内容编码的质量进行测试，但是在加密和打包之前尽早发现问题可以提供更有效的内容处理。所以，特别要求在这一步保证内容的质量，而不是等待到所有的处理都最终结束后。

4. 加密工具

加密工具向用户提供了实现上述加密过程 811 的功能。内容加密是内容处理工具 155 的最后一步。由编码工具生成的内容的每一个版本现在都被加密。加密工具是 SC 打包器的一项功能。SC 打包器被调用以对歌曲加密，而且返回被使用的产生的加密密钥。该密钥随后被传递到 SC 打包器中以被用于生成元数据 SC 620。

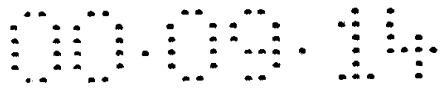
E. 内容 SC 创建工具

一旦聚集了所有的元数据，内容 SC 创建工具就将元数据根据其预期用途来分组归类。这些元数据组被写进文件，以被作为元数据 SC 620 的元数据部分被传递到 SC 打包工具中。每个部分（文件）都有独特的处理要求。一旦相关的歌曲已被处理和加密，并且目标站（内容托管站点 111 的 URL）已被决定，内容 113 的内容 SC 630 就做好了被创建的准备。已经完成处理并满足上述所有要求的内容 113 就被排队在工作流程管理器 154 的打包队列中。

现在内容 SC 创建工具检索所有的由前面步骤中的元数据吸收和输入工具 161 创建所需文件，并且调用 SC 打包机功能以创建元数据 SC 620 和内容 SC 630。这个过程为每首歌创建一个元数据 SC 620 和多个内容 SC 630。举例而言，如果内容是音乐，那么为整首歌的不同质量级别所进行的音频处理过程中创建的每一个音频文件就被打包成分离的内容 SC 630。为样品片段创建的音频文件被作为一个元数据文件而传递，并被包括到元数据 SC 620 中。

F. 最终质量保证工具

最终质量保证工具向用户提供实现上述的最终质量保证过程 813 的能力。一旦一个内容文件的所有 SC 都已被创建，这个内容就可进行最终质量保证检验。质量保证可以在内容 113 准备过程中的不同阶段执行。内容提供者 101 可以选择在每一主要步骤结束时执行质量保



证以避免后来做过份的重复工作，也可等到所有音频准备过程都结束后对所有内容一次性进行质量保证。如果选择了后者，那么就在 SC 的创建结束那一刻进行质量保证。此工具使得歌曲的每一个 SC 都被打开、检验和播放声音。

由于 SC 的内部安全特性，所发现的任何问题，即使是微小的文本改变也要求重新建立 SC。为了避免不必要的重新处理时间，高度建议采取中间阶段的质量保证步骤来确保元数据的精确度，并且将此具体质量保证步骤用于在与这首歌曲相关的 SC 之间检验合适的交叉引用。如果发现问题，检验者可以加入一个附在歌曲上的问题描述，并且将其重新排到适当的处理队列以便进行重新处理。工作流程管理器 154 中的状态被适当地更新以指示歌曲所有相关组件的状态。如果没有发现问题，内容 113 就被加上准备发行的标志或标记。

G. 内容分发工具

内容分发工具向用户提供一个实现上述内容分发处理 814 的能力。一旦内容 113 被批准发行，内容 113 的 SC 就被放置在内容分发处理的队列中。内容分散工具对队列进行监视，并根据内容提供者 101 提供的结构设置立即执行 SC 文件的传送或对一组 SC 文件的成批传送。内容提供者 101 还能选择配置内容分发工具，以便自动地保留队列中的所有 SC，直到它们被人工标志以发行。这就允许内容提供者 101 在他们预定的发行日期之前提前将内容准备好，并且将内容保留直至他们想要发行它们，如一个新的歌曲、电影或游戏。SC 还能够依据设定的发行日期对内容 113 的读取进行控制，因此内容提供者 101 不需对内容 SC 的传送进行实际阻拦，但是此人工发行选项仍可被用于此目的或用于管理传送这些大型文件所需要的网络带宽。

当内容 113 的内容 SC 630 被标志为可以发行时，它就经 FTP 被传送到指定的内容托管站点 111。元数据 SC 620 经过 FTP 被传送到内容促销网站 156。这里，SC 被按级分离一个新内容 113 目录，直到他们能被处理并被结合到内容促销网站 156 中。

图 17 是一个按本发明用图 8 中的自动元数据采集工具自动地检

索附加信息的可选实施例的流程图。这个过程类似于上面图 8 中描述的过程。然而，监督发行 806 和内容质量控制 809 的质量检验被组合成一个质量检验，称为质量控制 1704，在元数据 SC 创建 807 和内容 SC 创建 812 之前执行质量检验。在 SC 创建以前执行质量检验删去了将内容 113 和相关的元数据 SC 620 解包的步骤。另外，在这个实施例中，产品等待动作/信息 801 的队列已被删除了。作业依据所请求的操作而被放入具体处理队列中。例如，如果作业要求人工元数据，即附加元数据需被输入，这个作业就被放在人工元数据输入队列中。自动元数据采集 803 同新内容请求已被并在一起，以在元数据吸收和输入工具 161 和内容处理工具 155 之前预先出现。最后，需要重要指出的是使用条件 804 在自动元数据采集 803 处和人工元数据输入 803 期间都被输入。因此，许多使用条件在自动元数据采集 803 步骤期间能被自动地填充。

H. 内容促销 Web 站

为了更有效地分发关于内容提供者 101 提供的可通过电子下载出售的信息，并且为了给电子数字内容商店 103 得到所需文件，以使此内容 113 能够被下载到其用户，每个内容提供者 101 应有一个安全的 Web 站以居留这些信息。这与一些内容提供者 101 现今使用的让需要此信息的其零售商和其他人获得促销内容的方法类似。在此类服务已经存在的情况下，一个附加的部分可被加入到 Web 站，在此 Web 站，电子数字内容商店 103 能够去看可通过下载而出售的内容表单。

内容提供者 101 完全控制此 Web 站的设计和布局，或者可以选择使用承包的 Web 服务器方案作为安全数字内容电子销售系统 100 所提供的部分工具箱。为实现他们自己对服务的设计，内容提供者 101 只需对访问他们站点的电子数字内容商店 103 提供到元数据 SC 620 的链接。这样是通过使用安全数字内容电子销售系统 100 的工具箱而完成的。选择过程以及什么信息被显示由内容提供者 101 自行判断。

通过 FTP 被接收入一个新内容目录的来自内容分散工具的元数据 SC 620 被内容促销网站 156 进行处理。这些容器可被 SC 预览工具打

开，以显示或提取来源于容器的信息。然后这些信息能够被用于更新HTML 网页并且/或者向此服务维护的可搜索数据库加入信息。SC 预览工具实际上是电子数字内容商店 103 用于打开并处理元数据 SC 620 的内容采集工具的一个子集。详细信息请参照内容采集工具部分。然后元数据 SC 620 文件应被移至一个由内容促销 Web 站 156 维护的永久目录。

一旦元数据 SC 620 已被组合到内容促销网站 156，它的可获得性就被公布。内容提供者 101 可以每当一个新的元数据 SC 620 被加到网站时，内容提供者 101 向所有预订电子数字内容商店 103 发送一个通知，或者可以每天（或以预定的周期）就当天（或那个周期）被加入网站的所有元数据 SC 620 发出一个通知。这类通知是经由与电子数字内容商店 103 的 Web 服务器的标准 HTTP 交换，通过发送一包含有涉及被加入的元数据 SC 620 的参数所定义的 CGI 串被实现的。此消息由后面所描述的电子数字内容商店 103 的通知接口模块进行处理。

I. 内容托管

娱乐业每年生产数以千计的内容标题，比如 CD，电影和游戏，并将其加入当前可以获得的数以万计的内容标题。安全数字内容电子销售系统 100 的设计可以支持现今商店中所有能够得到的所有内容标题。

安全数字内容电子销售系统 100 每天下载至客户的内容标题的数量可以是成千上万的。对于大量的标题，就需要大数量的带宽。对计算机磁盘空间和带宽的需要用多个内容托管站点 111 分散的，可变大小地实现。此系统也支持世界各地的用户。这就要求有海外站点以向全球用户加速传递。

安全数字内容电子销售系统 100 上的内容托管的设计允许内容提供者 101 托管它们自己的内容 113 或共享一个或一套公共设备。

安全数字内容电子销售系统 100 上的内容托管由包含所有安全数字内容电子销售系统 100 所提供的内容 113 的多个内容托管站点 111

以及含有内容提供者提供的当前热门产品的几个二级内容网站（未显示）组成。内容托管站点 111 的数量随着使用此系统的最终用户的数量而改变。二级内容站点托管有限数量的歌曲，但它们将代表这个系统中使用的带宽的大部分。二级内容站点在主要站点上的容量增至其最大容量时被引入网络。二级内容站点可以位于网络读取点（NAP）的附近，以协助加快下载时间。它们也可位于全球不同的地理区域以加快下载时间。

如果内容提供 101 选择在其自己的系统中托管其所有的内容 113，它们就可作为一个单一的内容托管站点 111，用或不用附加的二级内容站点均可。这就使他们能够建造自己的可升级的分布式系统。在另一实施例中，电子数字内容商店 103 也能为某些内容 113 充当内容托管站点 111。这个实施例要求在电子数字内容商店 103 和内容提供者 101 之间存在一特殊的财政协议。

1. 内容托管站点

内容 113 由本说明的内容提供者部分中描述的内容支付工具，经 FTP 或 HTTP 被加入内容托管站点 111，或通过以例如磁带、CD ROM、闪烁存储器或其它计算机可读媒介内容发送的脱机方法被加入到内容托管站点 111 中。由内容提供者 101 创建的元数据 SC 620 中包含有一个指示内容 113 的内容 SC 630 的 URL 所在处的字段。这个 URL 对应一个内容托管站点 111。如果报价 SC 641 中的内容提供者 101 允许，电子数字内容商店 103 能够覆盖这个 URL。当最终用户设备 109 想要下载内容 SC 630 时，最终用户设备 109 与内容托管站点 111 通信。

最终用户设备 109 通过向内容托管站点 111 传送许可证 SC 660 来提出对内容 SC 630 的请求。这与交换所 105 返回的许可证 SC 660 是同一个。许可证 SC 660 的数字签名可被校验以决定它是否是一个合法的许可证 SC 660。如果是一个合法的许可证 SC 660，下载就可以开始，或者将下载请求转到另一个内容托管站点 111。

2. 由安全数字内容电子销售系统 100 提供的内容托管站点 111

对于安全数字内容电子销售系统 100 来说，哪个站点被用于下载内容 113 的决定是由最初接收到对内容 SC 630 的请求的起初内容站点作出的。这个站点使用以下信息来作出此决定:

- 存在托管请求内容 113 的二级内容站点吗？（多数由安全数字内容电子销售系统 100 提供的内容 113 只位于一级站点上）;
- 最终用户设备 109 的地理位置在哪里？（此信息能在最终用户设备 109 提出请求时从最终用户设备 109 中得到，并在订单 SC 650 中被传递到交换所 105）;
- 适当的二级站点是否已被建立并在运行中？（有时二级站点可以是脱机的）;
- 二级站点的负载有多大？（在一些情况下，当一个二级站点被活动堵塞时，另一个不很繁忙的站点可能被选择）。

在把内容 SC 630 发送到最终用户设备 109 之前，对最终用户的请求要进行分析和验证。存在一个数据库以保存所有曾被用于下载内容 113 的许可证 SC 的 ID。这个数据库将被检查以确保最终用户设备 109 对每份被购买的内容 113 只能发出一次请求。这将防止恶意用户重复访问内容托管站点 111 以期望降低内容托管站点 111 的速度，还防止了对内容 SC 630 的非法下载。

根据对每一件内容 113 的顾客需求，内容 113 可以被定期地升级和降级到二级内容站点。

内容托管路由器

内容托管路由器（未显示）位于内容托管站点 111 上，它接收所有来自想要下载内容 113 的最终用户的请求。它执行对最终用户请求的合法性检验，以确保他们确实购买了内容 113。一个关于二级内容站点的状态的数据库被维护着，它包括二级内容站点具有什么样的内容 113 以及它们当前的状态如何。此当前状态包括在站点上的活动数量及站点是否在关闭维修。

到达内容托管路由器的唯一接口是当内容 113 被要求下载时由

最终用户设备 109 发送的许可证 SC 660。这个许可证 SC 660 包括了显示用户被允许下载内容 113 的信息。

二级内容站点

二级内容站点（未显示）托管着安全数字内容销售系统 100 的最受欢迎的内容 113。这些站点在地理上遍布全球，并靠近网络读取点（NAP）以加速下载时间。当一级的内容托管站点 111 接近饱和容量时，这些站点就被加入到系统中。

IX. 电子数字内容商店

A. 综述 – 对多个电子数字内容商店 103 的支持

电子数字内容商店 103 实质上是零售商。它们是为将出售给顾客的内容 113 进行促销的实体。对于内容 113 的销售，它包括数字内容零售网络站点、数字内容零售商店、或任何愿意参与向顾客进行内容 113 促销的商业机构。这些商业机构可以只对电子内容 113 的销售进行促销,也可以选择将电子产品的销售加到它们当前所提供出售的其它产品中。将可下载的电子产品引入电子数字内容商店 103 的服务业务是通过为电子数字内容商店 103 开发的、作为安全数字内容销售系统 100 的一部分的一组工具而实现的。

这些工具被电子数字内容商店 103 用于:

. 获得由内容提供者 101 打包的元数据 SC 620

. 从这些 SC 中提取内容 113 用于创建它们的服务业务的输入

. 创建报价 SC 641，以描述它们提供出售的可下载的内容 113

. 通过创建交易 SC 640 并将其发送给最终用户设备 109 来处理对销售的确认和开始下载

. 管理一个关于可下载的内容 113 的出售和每个下载的状况的交易日志

. 处理对状况的通知以及对交易授权的请求

. 执行帐户调解

这些工具被设计成使得电子数字内容商店 103 在选择如何将可下载的电子内容 113 的销售组合到其服务中时具有灵活性。这些工具可被如此使用，以要求交换所 105 处理关于被购买的可下载内容的一切财政结算，尽管这并不是必须的。这些工具还可被使用，使电子数字内容商店 103 能够为其顾客提供全部服务并自己处理财政交易，包括提供促销和特价。这些工具使得电子数字内容商店 103 能够迅速地将可下载内容 113 的销售组合到其现有服务中。另外，电子数字内容商店 103 不必托管可下载的内容 113，也不必管理它的发布。这些功能由内容提供者 101 选择的内容托管站点 111 来执行。

在首选的实施例中，电子数字内容商店 103 的工具是用 Java 实现的，但是也可使用其他的编程语言如 C/C++，汇编语言和类似语言。应当说明，下面描述的电子数字内容商店 103 的工具可以在各种硬件和软件平台上运行。电子数字内容商店 103 可以以一个整体或作为其任一组成组件，而被作为一个应用程序在计算机可读介质中被销售，计算机可读介质包括但不限制于例如网络的电子销售或者软盘，CD ROMS 和可移动的硬盘驱动器。

在另一个实施例中，电子数字内容商店 103 的组件是程序员的软件工具包的一部分。这个工具包可使预先定义的接口成为下述通用电子数字内容商店 103 的组件和工具的一个部分。这些预先确定的接口采用 APIs 或应用程序接口的形式。使用这些 API 的开发者能从一个高层应用程序中实现组件的任一功能。通过给这些组件提供 API，程序员能够迅速地开发一个用户化的电子数字内容商店 103 而不须重新创建任一组件的功能和资源。

电子数字内容商店 103 不局限于基于网络的服务报价。所提供的工具可被所有愿意销售下载的电子内容 113 的电子数字内容商店 103 使用，无论其使用何种发送基础设施或发送方式将内容 113 发送给最终用户。通过卫星和电缆基础设施提供的广播服务也使用这些同样的工具来获得、打包和追踪电子内容 113 的销售。供销售的电子产品的显示和将这些电子产品发送给最终用户的方法是以广播为基础的服务

业务与点到点的交互式 Web 服务类型的业务的主要不同。

B.点到点的电子数字内容销售服务

点到点主要表示在电子数字内容商店 103 和最终用户设备 109 之间的一种一对一的交互服务。这通常代表通过电话或电缆调制解调器连接而提供的基于互联网的服务。除互联网以外的网络也可由这种模式支持，只要它们符合 Web 服务器/客户浏览器模式。图 9 的方块图描述了电子数字内容商店 103 的主要工具、组件和过程。

1. 集成要求

安全数字内容电子销售系统 100 不仅创建了新的在线企业，还为已经存在的企业提供了一种将可下载的电子内容 113 结合到它们当前的产品目录中的方法。提供给电子数字内容商店 103 的工具组简化了这种结合所需的努力。内容获得工具 171 和 SC 打包工具 153 为电子数字内容商店 103 提供了一种方法，以从参与的内容提供者 101 处获得关于它们有何物品可供出售的信息，并创建将这些可下载的物品索引成为其产品目录中一个选项所必须的文件。这个过程是分批驱动的，能在很大程度上自动化，并且只在将新的内容 113 结合入站点时被执行。

安全数字内容电子销售所用工具的设计使得电子可下载内容 113 的销售能被结合到典型的基于网络的电子数字内容商店 103（即 Columbia House online, Music Boulevard, @Tower）或类似体，只需对它们当前内容 113 的零售式样做极小变动。存在几种可能的结合方法，在首选的实施例中，电子数字内容商店 103 为所有的产品查询、预览、选择（购物车）和购买提供支持。每个电子数字内容商店 103 与其顾客建立顾客忠诚度，并不断提供消费刺激并促销其产品，就象它们目前所做的那样。在安全数字内容电子销售系统 100 中，电子数字内容商店 103 只需指出其产品目录中哪个产品可供电子下载，并允许顾客在进行购买选择时能够选择电子下载选项。在另一实施例中，顾客的购物车能够包含电子（内容 113）和实物选择的混合。在顾客已经结帐且电子数字内容商店 103 已经完成了财政结算并加以记录或

已经通知其邮寄和处理功能来处理所购买的实物产品后，电子数字内容商店 103 的商业处理功能就调用交易处理器模块 175 来处理所有的电子下载。它仅仅传递所需的信息，而从那一点起的所有过程均由安全数字内容电子销售系统 100 的工具组处理。在另一实施例中，如果电子数字内容商店 103 只想销售可下载的产品或想将实际产品与可下载产品的财政结算分离开来，使用安全数字内容电子销售系统 100 的工具来处理财政结算使得用其它方法进行交易处理也是可能的。

为了处理产品的下载，电子数字内容商店 103 对每个从内容提供者 101 的内容促销网站 156 得到的可下载的产品都被给予一个产品 ID（未显示）。这个产品 ID 与顾客对可下载产品的购买选项有关。这个产品 ID 就是电子数字内容商店 103 传给交易处理器模块 175 的，用于鉴别用户所购买的产品。被创建用于描述产品的 SC（报价 SC）被与电子数字内容商店 103 隔离，并被保存于报价数据库 181 中以简化对这些物品的管理，并使它们的存在对于电子数字内容商店 103 相对透明。

交易处理器模块 175 和其它附加功能被作为 WEB 服务器端可执行程序(即 CGI 和 NSAPI,ISAPI 可调用功能)或仅 API 提供一个 DLL 或 C 目标库。这些功能对与交换所 105 之间的最终用户交互和可选择接触的运行时间进行处理。这些功能与 Web 服务器的商业服务交互，以便为最终用户设备 109 创建并下载启动内容 113 的下载过程所必需的文件。它们还处理可选择的交互，以提供授权，并接收动作完成的通知。

一个帐户调解工具 179 也被提供，以协助电子数字内容商店 103 与交换所 105 联系，以便依据其自己和交换所 105 的交易记录对帐户进行调解。

2. 内容获取工具 171

内容获取工具 171 负责与内容促销 Web 站点 156 的连接，以便预览并下载元数据 SC 620。由于内容促销站点是一个标准的 Web 站点，所以电子数字内容商店 103 就能用 Web 浏览器来浏览该个站点。这

个浏览特征是随内容提供者 101 的站点设计变化。一些站点可以用许多促销信息的窗口来提供广大的查询能力。另外一些站点可以有一个简单的与标题表从中选择的执行者或新的发行。所有的站点包括选择包含对一首歌曲或歌曲集的促销和描述信息的元数据 SC 620。

另一方面，电子商店 103 可以通过 FTP 预订内容更新，和自动地接收更新。

查看元数据

内容获取工具 171 是一个网络浏览器帮助应用程序，当在内容促销网络站点 156 选择了一个元数据 SC 620 链时，就运行内容获取工具 171。SC 的选择导致它能够被下载到电子数字内容商店 103，并运行帮助应用程序。内容获取工具 171 打开元数据 SC 620，并把其中未加密的信息显示出来。显示的信息包括抽取元数据 173，就一个音乐例子来说，与歌曲相关的图形、图象和描述这首歌曲的信息，如果片段包含在元数据 SC 620 中，那么还可以听到这首歌曲的预览片段。在一个内容 113 是音乐的例子中，如果内容提供者 101 提供歌曲或歌曲集的促销信息，歌曲集的标题以及艺术家也显示出来。这个信息做为一系列相链的 HTML 网页在浏览器窗口中显示。可购买的内容 113 如歌曲和歌词和任何其它的内容提供者 101 想要保护的元数据，对零售内容网络站点 180 都不能读取。

在另外一个实施例中，内容提供者 101 为酬金提供了可选的促销内容。在本实施例中，这种促销内容在元数据 SC 620 中被加密。打开这个数据的财政结算能被处理通过交换所 105，用电子数字内容商店 103 支付所指酬金。

抽取元数据

除了预览的性能以外，这个工具还提供了两个附加的特性：元数据的抽取和报价 SC 641 的准备。元数据抽取选择项的选择促使电子内容商店 103 输入到存储元数据的路径和文件名。二进制的元数据如

图形和声音预览片段作为独立的文件被保存。文本元数据存储在用ASCII 定义的文本文件中，零售内容网络站点 180 能够将这个文本文件输入到它的数据库中。描述 ASCII 定义的文本文件的格式的表也是在一个独立的 TOC 文件中创建的。附加选项可用来允许提取成其它NLS（国家语言支持）支持的格式。

提取数据中提供的一种重要的信息内容是产品 ID。产品 ID 是电子数字内容商店 103 的商业处理功能所需的，用于识别交易处理模块 175（更多信息参看交易处理部分）和用户已经购买的内容 113。交易处理模块 175 用该产品 ID 来合适地从报价数据库 181 中检索合适的报价 SC 641，随后下载到最终用户设备 109。电子数字内容商店 103 对于在它的站点上如何显示可下载内容 113 的报价有完全的控制能力。只需要为安全数字内容电子销售系统 100 配合合适的工具保留一个提供给该产品 ID 的交叉引用。这里提供的这些信息，就可以允许电子数字内容商店 103 将这个产品或内容 113 集合到它的产品目录中，并同时用报价 SC 641 创建过程来销售页面（数据库），因为两个过程都用同一个产品 ID 来访问产品。这在后面作进一步描述。

报价 SC 创建打包器 153

电子数字内容商店 103 需要创建一个报价 SC 641 来描述用于销售的可下载内容 113。加入到报价 SC 641 中的许多信息是来自元数据 SC 620。内容获取工具 171 通过以下步骤创建报价 SC 641:

· 根据元数据 SC 620 中报价 SC 模板定义，从元数据 SC 620 中删除不要求包括在报价 SC 641 的部分

· 根据该工具中为电子数字内容商店 103 配置的选项所指定的默认值的定义，增加需要的附加部分

· 根据元数据 SC 620 中报价 SC 模板定义，增加需要的输入和选择

· 调用 SC 打包器来将信息打包成 SC 格式

由播放器应用程序 195（在以后作进一步描述）在最终用户设备

109 显示的元数据被保存在元数据 SC 620 中。其他的只被电子数字内容商店 103 用做输入 WEB 服务器数据库的促销元数据从元数据 SC 620 中删除。由内容提供者 101 提供的版权管理信息，如水印指令、加密的对称密钥 623 和定义允许使用的目标的使用条件 517 也被保留。

这个拆开的元数据 SC 620 包含在报价 SC 641 中。电子数字内容商店 103 还将它自己的调用存储使用条件 519 或购买选择项的使用条件加到报价 SC 641 上。这可以通过一组默认值交互地或自动来实现。如果电子数字内容商店 103 设定为交互式处理，那么电子数字内容商店 103 就可以用内容提供者 101 的定义，用许可目标使用条件 517 的设置现场支付。然后，他可以选择他想要报价给他的顾客的选项。现在这就变成了新的使用条件或存储使用条件 519。为了自动处理过程，电子数字内容商店 103 设定了一组为所有内容 113 报价的默认购买选项。这些默认值可以自动地被检查，而不必具有内容提供者 101 定义的使用条件 517 的许可，并且如果不矛盾的话，这些默认值就设置在报价 SC 641 中。

一旦创建了报价 SC 641，它就被存储在报价数据库 181 中，并且用元数据 SC 620 中预先指定的商品 ID 来检索。当为打包而连接报价数据库 181 去检索时，商品 ID 通过电子数字内容商店 103 识别由用户购买的可下载的内容 113 和传输到最终用户。详见交易处理模块 175 部分。

在另外一个实施例中，电子数字内容商店 103 在它的站点上托管内容 SC 641。这个实施例要求对报价 SC 641 做些改变，如用电子数字内容商店 103 的 URL 代替内容托管站点 111 的 URL。

3. 交易处理模块 175

电子数字内容商店 103 控制到交换所 105 的订单。另一方面，电子数字内容商店 103 可以直接从交换所 105 中请求财政票据交换。最终用户请求可下载的内容 113 的处理有两个基本的方式。如果电子

数字内容商店 103 不想处理购买的财政结算，并且没有专门的促销或刺激调节商品的销售，并且不用购物车来比喻成批购买请求，就可选择将它的内容 113 下载页面直接连到报价 SC 641 文件上。这些报价 SC 641 必须已用包含在元数据中的零售定价信息来建立。在报价 SC 641 中还包括一个特殊的 HTML 报价页面，它显示了带有条款和销售条件的购买选项。当报价 SC 641 被建立，该页面由创建的模板建立。当最终用户点击指向链到报价 SC 641 上时，报价 SC 641 就被下载到浏览器最终用户设备 109，运行一个打开的容器，并显示包含在报价 SC 641 中的报价页面的帮助器应用程序。这个页面包括了一个表单，用于收集顾客信息包括信用卡信息和购买选项的选择。然后，这个表单为财政结算和处理直接被提交给交换所 105。可选择地，这个表单可以包含使用最终用户的信用卡信息或工业标准的本地交易处理器的字段。

现在描述一个电子数字内容商店 103 处理订单的实施例。更为典型的处理购买请求的方式是允许电子数字内容商店 103 处理财政结算，然后给最终用户提交载授权。这个方式允许电子数字内容商店 103 将可下载的内容 113 和其他报价出售的商品在它的站点上集成起来，提供购买请求的成批处理，并且对用户来说只有一个合并计算收费（比喻通过购物车）而不是对每个下载请求单独收取费用，并且允许电子数字内容商店 103 直接追踪他的顾客的购买模式和提供专门的促销和联合购买权。在这种环境下，可下载的内容 113 的报价就包含在它的购物页面内，当该页面被最终用户选中，就加到购物车上及给予处理，并作为在电子数字内容商店 103 的当前购物方式进行财政结算。一旦财政结算完成，电子数字内容商店 100 的商业处理过程就调用交易处理模块 175 以完成交易。

交易处理模块 175

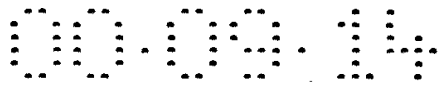
交易处理模块 175 的作用是用最终用户设备 109 把所必须的信息汇总起来，以起动和处理购买的内容 113 的下载。这个信息打包成一

个交易 SC 640，它将被 WEB 服务器送回到最终用户设备 109 作为购买提交的响应。交易处理模块 175 需要从电子数字内容商店 103 的商业处理过程中的三种信息：购买的内容 113 的产品 ID，交易数据 642 和确认购买结算的一个 HTML 页面或 CGI URL。

商品 ID 是一个提供给电子数字内容商店 103 的，与正售出的内容 113 相关的在元数据 SC 620 中的值。这个商品 ID 用于从报价数据库 181 中检索相关的报价 SC 641。

交易数据 642 是一个由电子数字内容商店 103 的交易处理过程提供的信息结构，电子数字内容商店 103 随后将用于使交换所 105 处理与由电子数字内容商店 103 执行的财政结算交易，并用于提供用户身份信息，将其包括在下载给最终用户设备 109 的内容 113 的水印中。当交换所 105 接收到一个有效合法的订单 SC 650 时，它就记录了一个指示出售的内容 113 的交易，电子数字内容商店 103 销售它和相关的包含有最终用户名称和交易 ID 535 的交易数据 642。交易数据 535 提供一涉及财政结算的交易。这个信息随后被交换所 105 返回到电子数字内容商店 105，用于核对它的帐户和从内容提供者 101（或它的代理）接收到的帐单声明。交换所交易记录 178 能被内容提供者 101 用于确定它的哪个内容 113 已售出，并且为了它拥有版权，使它能够给每个电子数字内容商店 103 建立一个订单。除了帐单以外的其他的电子方法能在内容提供者 101 和电子数字内容商店 103 之间选择一个用来结帐。

交易 SC 640 中提供的信息和交易 SC 640 的安全性和完整性为交换所 105 提供了充分的可靠性，即购买交易是合法的，因而在交换所 105 记录此销售之前不需进一步的验证。然而，电子数字内容商店 103 在其帐户被收取费用之前，可以选择请求证实（对内容提供者 101 来说，被记录于交换所 105 中的交易表示电子数字内容商店 103 已为此内容 113 的销售接收了钱款）。这个证实/通知的请求由交易数据 SC 642 中的一个标志来表示。在这种情况下，交换所 105 与电子数字内容商店 103 联系，并在对其帐户收取费用之前，从电子数字内容商店 103



中接收授权并给出加密密钥 623。交易 ID 535 被作为证实请求的一部分从交换所 105 中传送到电子数字内容商店 103，使电子数字内容商店 103 能够将此请求与一个与最终用户执行的先前交易联系起来。此交易 ID 535 可以是电子数字内容商店 103 想要使用的任一唯一的值，并且只被用于此目的。

交易数据 642 还包括顾客的名称。这个名称可以来自用户进行购买时填写的购买表格中的用户名一栏，也可来自从前在用户向电子数字内容商店 103 注册过程中记录的信息，或是从与此交易中所使的信用卡相关的信用卡信息中获得的正式名。这个名后来被包含在许可证水印 527 中。

交易数据 642 还包含被最终用户购买的商店使用条件 519。这个信息被包含在许可证水印 527 中，并被最终用户设备 109 用于拷贝和播放控制。

交易处理器模块 175 所要求的最后一个参数是通知购买结算的 HTML 页面或 CGI URL。这个参数的目的是使电子数字内容商店 103 将一个财政结算的通知和任何其它想要包含于其中的信息通知给最终用户。HTML 页面或 CGI URL 被包含在交易 SC 640 中，并且在交易 SC 640 被接收和处理时被显示在最终用户设备 109 的浏览器窗口中。

交易 SC 640 是在处理了购买提交后，从电子数字内容商店 103 用 HTTP 回复给最终用户。将 SC 作为直接 HTTP 回复而发送迫使 SC 处理器帮助应用程序被自动加载在最终用户设备 109 上，因此使得交易自动完成而不必进一步依靠由最终用户启动动作。此过程在后面的最终用户设备 109 和播放器应用程序 195 章节中有更详细描述。

当交易处理器模块 175 用所需参数被调用时，它建立一个包含有交易数据 642、交易通知 HTML 网页、或其它含有 SC 所需的安全特性的 URL 引用的交易 SC 640，并且检索和嵌入与购买相关的报价 SC 641。它还记录关于这个交易的信息，以便将来由通知接口模块 176 和帐户调解工具 179 使用。

4. 通知接口模块 176

通知接口模块 176 是一个 WEB 服务器端的可执行例程（CGI 或可被 NSAPI, ISAPI 或类似物调用的功能）。它处理来自于交换所 105、最终用户设备 109、内容托管站点 111 和内容提供者 101 的可选择的请求和通知。电子数字内容商店 103 可以选择请求通知的事件是:

- 来自交换所 105 的通知，说明最终用户设备 109 请求了一个加密密钥 623 且交换所正发出指定的内容 113 的加密密钥 623。这个通知能够任意地被配置，使得在加密密钥 623 被送至最终用户设备 109 之前向电子数字内容商店 103 请求核实。
- 来自内容托管站点 111 的通知，说明内容 SC 630 已经被发送到最终用户设备 109。
- 来自于最终用户设备 109 的通知，说明内容 SC 630 和许可证 SC 660 已经被收到，并且被成功用于处理内容 113 或发现已被破坏。
- 来自于内容提供者 101 的通知，说明新的内容 113 已经被放入内容促销网站。

这些通知都不是安全数字内容电子销售系统流程 100 中所必须的步骤，但是它们都被作为可选项来提供，以使电子数字内容商店 103 有机会在销售的满意完成时结束其记录。通过告知电子数字内容商店 103 在交易的财政结算之后发生了什么操作或是在试图完成销售当中出现了什么错误，它还提供了在处理顾客服务请求时有可能需要的信息。在另一种可供选择的情况下，许多这些状态可以通过客户服务接口 184 从交换所 105 中根据需要获得。

对于可在内容促销 Web 站 156 得到的新的内容 113 的通知的频率由内容提供者 101 决定。通知可以在每个新的元数据 SC 620 被加入时发出，也可每天将所有的当日加入的新的元数据 SC 620 一起发出。

所有的这些通知都成为交易记录 178 中的登录。如果电子数字内容商店 103 想要对这些通知自行处理，它可以拦截 CGI 的调用，执行其唯一功能，然后可选择地将请求传递给通知接口模块 176。

5. 帐户调解工具 179

帐户调解工具 179 与交换所 105 联系以将交易记录 178 与交换所 105 的记录相比较。这是一个可选择使用的过程，它能帮助电子数字内容商店 103 对于安全数字内容电子销售系统 100 的帐目更加放心。

在另外一个实施例中，此工具能被更新来为对内容提供者 101 和交换所 105 的自动周期付款提供电子资金转帐。它还能被设计用于当从交换所 105 收到电子帐单时，在将帐单与交易记录 178 调解后自动地处理付款。

C. 广播电子数字内容销售服务

广播主要指的是一对多的传输方法，在最终用户设备 109 和电子数字内容商店 103 之间没有用于对收视和收听的要求进行用户化的个人联系。这通常是通过一个数字卫星或电缆基础设施提供的，在其上的内容 113 被预先安排，因此所有的最终用户设备 109 都接收到同一个信息流。

还可以定义一个混合的模型，令电子数字内容商店 103 可以提供了一个以这样的方式组织的电子内容服务，使得它既能经 INTERNET 连接提供一个 Web 销售接口，也可通过广播服务提供一个更高频带宽度的卫星或有线销售接口，而在站点设计上有很多的共同之处。如果 IRD 后通道串行接口与网络相连，且 IRD 支持 Web 浏览，那么最终用户就能通过后部通道串行接口以通常的方式浏览数字内容服务，预览和选择以供购买的内容 113。用户能够通过 INTERNET 连接选择高质量的可下载内容 113、购买这些选择、并接收所需的许可证 SC 660，然后请求将内容 113（内容 SC 630）通过更高频带广播接口发送。Web 服务能够根据广播时间表指示哪个内容 113 能以此种方式下载，或完全基于购买的内容 113 建立广播信息流。这个方法使得基于网络的数字内容服务能与一广播设备签订合同以将高质量的内容 113 发送给配备有适当的设备的用户，使得有限数量的特定内容 113（如歌曲或 CD）每天都能以这种方式被获得，而其整个目录可以通过网络接口被略低质量地下载。

其他的广播模型能设计成不具有到最终用户设备 109 的网络接口。在这种模型中，促销内容被打包入专门格式化的数字流以便广播传递给最终用户设备 109（即 IRD），在这里经特殊处理来将数字流解码，并向最终用户展示可以从其中进行购买选择的促销内容。

实际购买选择的开始仍应通过从最终用户设备 109 到交换所 105 的后部通道通信，并利用 SC 来执行所有的数据交换。提供给电子数字内容商店 103 的工具组已经以这样的一种方式来建造和开发，使得大部分工具既可应用于点到点的互联网服务业务，也可应用于广播卫星或电缆业务。被电子内容 Web 站电子数字内容商店 103 用于获得并管理内容 113 以及制备 SC 的工具，也可被基于卫星的电子数字内容商店 103 用于管理和制备内容 113，以便于在广播基础设施上销售。通过 Web 服务销售的 SC 与通过广播服务销售的是相同的。

X. 最终用户设备 109

在最终用户设备 109 上用于安全数字内容电子销售系统 100 的应用程序实现两个主要功能：第一，SC 处理和拷贝控制；第二，重放加密的内容 113。无论最终用户设备 109 是一台个人电脑还是一个专用电子用户设备，它必须能够实现这些基础功能。最终用户设备 109 还提供了多种附加特性和功能，例如创建播放表、管理数字内容库、在播放内容时展示信息和图像、以及向外部介质设备记录。这些功能根据这些应用程序所支持的服务和设计应用所面对的设备类型而改变。

A. 综述

现在参照图 10，图中显示的是主要组件和处理过程以及最终用户设备 109 的操作流程。为支持基于 PC 机的 Web 接口内容 113 服务而设计的应用由两个可执行的软件应用程序组成：SC 处理器 192 和播放应用程序 195。SC 处理器 192 是一个可执行的应用程序，它被作为一个帮助器应用而被配置于最终用户 Web 浏览器 191，以处理 SC 文件/MIME 类型。每当从电子数字内容商店 103、交换所 105 和内容托管站点 111 接收到 SC 时，浏览器就会执行这个应用。它负责执行 SC

的所有所需处理，并最终将内容 113 加到最终用户的数字内容库 196 中。

播放器应用程序 195 是一独立的可执行的应用程序，最终用户装入它以在其数字内容库 196 中执行内容 113、管理其数字内容库 196、并在允许时创建内容 113 的拷贝。播放器应用程序 195 和 SC 处理器 192 应用都能用 Java、C/C++、或任何等效的软件编写。在优选实施例中，这些应用能够从计算机可读取的形式如网站被下载。然而，其它的传递机制也是可能的，如被传送到软盘或 CD 等计算机可读的介质上。

对内容 113 信息的查询和浏览、预览例如歌曲片段等、选择要购买的歌曲都是经由最终用户 Web 浏览器 191 来处理的。电子数字内容商店 103 与当今许多内容 113 的零售 Web 站以同样方法来提供购物体验。对于最终用户来说，与当今基于 Web 的内容 113 的购买所不同之处是他们现在可以选择可下载的内容 113 目标，以将其添加到他们的购物车上。如果电子数字内容商店 103 除了可下载的目标以外还有其它可供出售的商品，最终用户的购物车中就有可能具有一个实际商品和电子可下载的商品的组合。直到最终用户结束选购并向电子数字内容商店 103 提交其最终购买授权后，才涉及到安全数字内容电子销售最终用户设备 109。在此之前，所有的联系都是在电子数字内容商店 103 的 Web 服务器和最终用户设备 109 上的浏览器 191 之间进行的。这包括样品数字内容片段的预览。数字内容片段不被打包到 SC 中，而是作为可下载文件被结合到电子数字内容商店 103 的 Web 服务中，或者是从一个流服务器提供。内容 113 的片段的格式不由系统结构来决定。在另外一个实施例中，播放器应用程序 195 能直接与电子数字内容商店 103 或交换所 105 联系，或脱机使用一个促销 CD。

B. 应用程序安装

播放器应用程序 195 和帮助器应用程序 1981 都打包成一个可以自动安装的可执行程序，此程序在许多 Web 站上可供下载。交换所 105 担当一个在公共 Web 站上托管下载主页的核心位置。它包含了许多地

址的链接，从这些地址可以下载安装程序包。安装程序包可以在所有的内容托管站点 111 获得，来为下载请求提供地理上的分散。每个参加的电子数字内容商店 103 可以在其站点提供可供下载的程序包，或仅提供到达交换所 105 的公共 Web 站上的下载 Web 页的链接。

任何想要购买可下载的内容 113 的最终用户都下载并安装这个程序包。其安装已被包含于这个可下载的程序包中。它将帮助器应用程序 198 和播放器应用程序 195 解包并安装，而且将帮助器应用程序 198 配置到已安装的 Web 浏览器中。

作为安装的一部分，一个公共/私有密钥 661 对为最终用户设备 109 而被创建，以用于处理订单和许可证 SC 660。一个随机对称密钥（安全用户密钥）也被产生，以用于保护许可证数据库 197 中的歌曲加密密钥。安全用户密钥（未显示）的保护是通过将这个密钥分为多个部分并将密钥的部分存储在最终用户的计算机的多个地方来实现的。这个区域的代码由反篡改软件技术来保护，以便不泄露这个密钥是被如何分开的以及它被存储在哪里。防止甚至包括最终用户在内的对这个密钥的读取有助于防止盗版或与其他计算机共享内容 113。参看 SC 处理器 192 部分以获得如何使用这些密钥的详细信息。

反篡改软件技术是一种防止黑客非法进入一个计算机软件应用的方法。通常，黑客需要了解和/或更改软件来消除使用上的限制。现实中，没有任何现存的计算机程序不能被黑客攻击的；这是反篡改软件不能称为“抗篡改”的原因。但是黑客攻击一个反篡改保护应用程序所需的努力通常阻止了大多数黑客，因为付出的努力不值得可能的收益。此处，这种努力可能获得的是读取内容 113 的一部分的密钥，也许是 CD 上的单个歌曲。

反篡改软件技术的一种类型来自于 IBM。引用这种代码的一种产品是 IBM ThinkPad 770 便携式电脑。这里，反篡改软件被用于保护计算机中的 DVD 电影播放器。关注着数字电影的到来和制作完美拷贝的容易程度的数字内容提供者，如好莱坞工作室，坚持要求 DVD 盘上的电影具有拷贝保护机制。IBM 的反篡改软件使战胜这些拷贝保

护机制变得困难。这是反篡改软件的一个非常典型的应用；这个软件被用于强迫规则在某些受保护类型上内容 113 的使用。

IBM 的反篡改软件为攻击者设置了几种类型的障碍。第一，它包含了能战胜黑客使用的标准软件工具或至少减少该标准软件工具的有效性的技术：调试程序和反汇编程序。第二，它包含自我完整性检测，因此任一更改甚至是很小一点更改都将被发觉，并引起错误操作。最后，它包含了困惑机制，对黑客的正确操作进行误导。后一技术主要是 ad hoc，但是前两个的建立是依据了密码术中有名的工具：加密和数字签名。

C. 安全容器处理器 192

当最终用户就其已收集在购物车里的商品向电子数字内容商店 103 提交最终购买授权时，他的 Web 浏览器保持活动以等待来自 Web 服务器的反应。电子数字内容商店 103 上的 Web 服务器处理购买并且实现财政结算，然后向最终用户设备 109 返回一个交易 SC 640。SC 处理器 192（帮助器应用程序 198）由 Web 浏览器启动以处理与交易 SC 640 相关的 SC mime 类型。图 14 是按照本发明的图 10 中所描述的一个播放器应用程序 195 的用户界面屏幕的例子，此播放器应用程序 195 正在将内容下载给本地库。

SC 处理器 192 打开交易 SC 640 并提取其中包含的响应 HTML 页面和报价 SC 641。响应 HTML 网页被展示在浏览器窗口，确承最终用户的购买。报价 SC 641 被随后打开并且从中提取出内容 113（例如歌曲或曲集）的名称和计划的下载时间，1401 步。然后一个带有此信息的新窗口被显示，并且给予最终用户选择以安排对内容 113（例如，音乐、歌曲或整个曲集）的下载，1402 步。最终用户可以选择立即下载或将下载安排在未来某个时间。如果选择了未来的时间，下载安排信息就被保存在一个记录中，并且如果最终用户设备 109 在那个安排的时间到来时提供了电力，那么下载就在这个时间开始。如果在安排的下载时间时计算机不是激活的或通信连接没有激活，那么计算机在下一次被加电时，最终用户就被提示以重新安排下载时间。

当安排的下载时间到来时或如果请求即时下载，SC 处理器 192 就利用从交易 SC 640、报价 SC 641、和在安装时产生的最终用户的公共密钥 661 中的信息创建订单 SC 650。此订单 SC 650 经由 HTTP 请求被传送给交换所 105。当交换所返回许可证 SC 660 时，帮助器应用程序 198 被重新调用以处理许可证 SC 660。然后许可证 SC 660 被打开，且内容托管站点 111 的 URL 就从被引用的订单 SC 650 中提取。许可证 SC 660 然后通过浏览器经 http 请求被送到指定的内容托管站点 111，请求内容 SC 630 的下载。当内容 SC 630 返回到浏览器时，帮助器应用程序 198 就被再次重新调用。SC 处理器 192 显示正被下载的内容 113 的名称以及一个下载进度指示器和估计的所需完成时间。

当内容 113 被 SC 处理器 192 接收时，它就将内容 113 的数据加载到存储缓冲器中进行解密。缓冲器的容量大小根据加密算法和加水印技术 193 的需要而定，是尽可能小的容量，以减少暴露给黑客代码的未加密的内容 113 的数量。当缓冲器被充满时，它被用从许可证 SC 660 中提取的最终用户的密钥 623（对应于公共密钥 661）解密，而密钥 623 本身首先要用私钥进行解密。解密了的缓冲器然后被传送给加水印函数。

加水印 193 从许可证 SC 660 中提取加水印指令并将这个指令用最终用户的私钥解密。水印数据然后被从许可证 SC 660 中提取，它包括了交易信息，如购买者在向其购买了此内容 113 的电子数字内容商店 103 注册时所用的姓名，或从信用卡注册信息中得来的购买者姓名，如果电子数字内容商店 103 不提供注册功能。水印中还包括购买的日期和由电子数字内容商店 103 分配的交易 ID 535，以参照为这个交易登记的具体记录。商店使用条件 519 也被包括于其中，以便由播放器应用程序 195 的拷贝控制使用。

加水印 193 被以反篡改代码技术保护以便不泄露水印指令，从而防止黑客发现水印的位置和水印技术。这防止黑客对水印进行删除或更改。

在将任何所需水印记入到此内容缓冲器后，缓冲器被传递给重新加密 194 的抗频功能 194。一个例如 IBM 的 SEAL 加密技术的处理器有效安全加密算法被用来使用一个随机对称密钥将内容 113 重新加密。一旦下载、解密和重新加密 194 过程完成，被内容提供者 101 用于最初加密内容 113 的加密密钥 623 即被销毁，而新的 SEAL 密钥是使用在安装时创建和隐藏的保密用户密钥被自身加密了的。此时这个新被加密 Seal 密钥被存储在许可证数据库 107 中。

在内容提供者 101 处执行的不同来源以及在最终用户设备 109 处执行的用户水印可能需要成为工业标准而生效。这些标准仍然在演化。允许将控制信息嵌入音乐中并对其多次更新的技术已经存在。在拷贝控制标准变得更加稳定之前，可供选择的拷贝控制方法被提供给安全数字内容电子销售系统 100，使其不须依靠拷贝控制水印而在顾客设备中提供版权管理。存储和播放/录音使用条件安全是利用加密了的 DC 库集合 196 实现的，DC 库集合 196 是依赖最终用户设备 109 并通过反篡改环境被保护的。当标准被采用时，软件挂钩在适当的位置以支持拷贝控制水印。对水印 AAC 和其它在不同压缩级别被编码的声音流的支持当前是存在的，但是若要被作为唯一的拷贝控制来使用，这个技术当前仍然有些不成熟。

解密和重加密 194 过程是由反篡改代码技术所保护的代码的另一个领域，以使之不会泄露原先的内容 113 加密密钥、新 SEAL 密钥、安全用户密钥、以及安全用户密钥的各部分被藏在哪里和密钥是如何被分割的。

解密和重加密 194 的过程有两个目的。存储被如 SEAL 那样的算法加密的内容 113 能快于实时地解密，并且在执行解密时比象 DES 那样更加工业标准类型的算法要求少得多的处理器应用。这使得播放器应用程序 195 能够实现实时同步的内容 113 的解密—解码—回放，而不需在解码和回放之前将内容 113 的整个文件解密。SEAL 算法的有效性和一个高效解码算法不但允许同时操作(从加密文件的流回放)，还允许此过程在一个较低能的系统处理器上被执行。因此该应用程序

能够在低至 60MHZ 的奔腾系统甚至可能更低的最终用户设备 109 上被支持。将内容 113 被最终存储于其中的加密格式与最初的加密格式分离使得在选择最初的内容加密算法时有更大的灵活性。因此，被广泛接纳了的和证实了的工业标准算法可以被使用，从而进一步增强了数字内容工业标准对于安全数字内容电子销售系统 100 的接受程度。

解密和重加密 194 过程的第二个目的是删除内容提供者 101 使用加密此内容 113 的最初主加密密钥 623 必须被存在已获此内容 113 许可证的每一个最终用户设备 109 上的要求。作为许可证 SC 660 的一部分，这个加密的主密钥 623 仅在最终用户设备 109 的硬盘上被储藏了很短的时间，并且只在内存里有一段很短的无阻碍时间。在这个运行阶段，密钥 623 通过反篡改码技术被保护。一旦这个解密和重加密的阶段完成，就不再需要以任何形式在最终用户设备 109 上保留这个密钥 623，这样就大大减少了黑客盗版的可能性。

一旦歌曲被重加密，它就被存储在数字内容库 196 中。播放器应用程序 195 要求使用的所有元数据都是从相关的报价 SC 641 中提取的，并也被存储在数字内容库 196 中，1403 步。这个元数据中的任一被加密部分，例如歌曲的歌词，都以与上面为其它内容所描述的同样方式被解密和重加密。用于加密内容 113 的同一 SEAL 密钥被用于任何需要被加密的相关元数据。

D.播放器应用程序 195

1. 综述

安全数字内容电子销售播放器应用程序 195（这里所指的就是播放器应用程序 195）既类似于 CD,DVD 或其他数字内容播放器，也类似于 CD,DVD 或其他的数字内容存储管理系统。最简单地，它运行内容 113，如播放歌曲或影视。在另一层次上，它提供给最终用户一个管理他/她的数字内容库 196 的工具。并且重要的是，它还提供内容集合的编辑和播放，如许多歌曲（这里指的是播放表）。

播放器应用程序 195 是根据收集的组件装配起来的，这些组件可以个别地进行选择和按内容提供者 101 和电子数字内容商店 103 的要

求定制。播放器的普通型式被描述，但是定制（用户化）也是可能的。

现在参照图 15，显示了一个运行在图 10 中的最终用户设备 109 上的播放器应用程序 195 的主要组件和处理过程的方块图。

有若干个组件集合，它们组成了播放器目标管理器 1501 的子系统:

1.最终用户接口组件 1509

2.拷贝/播放管理组件 1504

3.解密 1505，解压缩 1506，回放组件 1507 并可能包含录制。

4.数据管理 1502 和库访问组件 1503

5.应用程序间通信组件 1508

6.其他组件（安装等等）

可以从各个这种集合中在下列要求的基础上挑选组件:

- 平台（Windows,Unix 或等效系统）
- 通信协议（网络，电缆等等）
- 内容提供者 101 或电子数字内容商店 103
- 硬件（CD,DVD,等等）
- 交换所 105 技术以及其它。

下面的章节详细地描述了各种组件集合。最后一章详细描述了这些组件是如何装配在普通播放器中，以及讨论组件如何被用户化。

在另外一个实施例中，播放器应用程序 195 和 SC 处理器 192 的组件都可以作为程序员的软件工具包的一部分而得到。这个工具包能够使预先定义的接口与上面列出的普通播放器应用程序的组件连接起来。这些预先定义了的接口具有 API 即应用程序接口的形式。使用这些 API 的开发者能够实现来自高层应用程序的组件的任何功能特性。通过提供这些组件的 API，程序员能够迅速地开发一个定制的播放器应用程序 195，而不须重新创建任何组件的函数和资源。

2. 最终用户接口组件 1509

这个集合中的组件联合起来提供了播放器应用程序 195 的在屏幕

上的显示。注意，这个设计没有建立这些组件的确定的安排。一种这样的安排被提供在普通的播放器中。根据内容提供者 101 和/或电子数字内容商店的要求和其它的要求，替代的安排是可以存在的。

这个集合被组合成子群，首先这些组件用于展示最终用户显示 1510 和处理称为最终用户控制 1511 的控制，用于如声音的回放和元数据的表示这类低层的功能。接着，最终用户显示组件 1510 按特定功能组（播放表，数字内容库）进一步划分，然后，目标-容器组件用于这些低层的组件的分组和安放。

在下面的组件列表中，任何涉及创建 CD 或拷贝内容 113 到一个 CD 或其他的可记录的介质，仅仅应用于播放器应用程序 195 具有允许这样的功能的情况。还要注意的是，术语 CD 在此上下文中是一通用词汇，它还可以代表各种其他的外部记录设备，如 MiniDisk 或 DVD。

图 16 是图 15 中按照本发明的播放器应用程序 195 的用户接口屏幕的一个例子。最终用户控制 1511 的功能包括（1601-1605 显示了最终用户接口的对应屏幕）：

运行内容 113 的控制：

- 播放/停止按钮
- 播放按钮
- 停止按钮
- 暂停按钮
- 向前跳过按钮
- 向后跳过按钮
- 音量控制
- 音轨位置控制/显示
- 音频通道音量级别显示及其它。

显示与内容 113 相关的元数据的控制：

- 封面图按钮
- 封面图目标

- 艺术家图片按钮
- 艺术家图片目标
- 音轨表按钮
- 音轨表信息目标
- 音轨表选择目标（点击以播放）
- 音轨名称目标
- 音轨信息目标
- 音轨歌词按钮
- 音轨歌词目标
- 音轨艺术家名称目标
- 音轨注解（Credits）按钮
- 音轨注解目标
- CD 名称目标
- CD 注解按钮
- CD 注解目标
- 普通（可配置的）元数据按钮
- 普通元数据目标以及其它。

最终用户显示 1510 的功能包括（最终用户接口的对应屏幕被显示于 1601-1605）：

显示容器的播放表

- 播放表管理按钮
- 播放表管理窗口
- 数字内容搜索按钮
- 数字内容搜索定义目标
- 数字内容搜索提交按钮
- 数字内容搜索结果目标
- 拷贝选择的搜索结果项到播放表按钮
- 播放表目标（可编辑的）
- 播放表保存按钮

- 播放表播放按钮
- 播放表暂停按钮
- 播放表重启动按钮
- 根据播放表创建 CD 的按钮以及其它。

数字内容库 196 的显示

- 数字内容库按钮
- 数字内容库窗口
- 数字内容分类按钮
- 数字内容分类目标
- by-artist 按钮
- by-genre 按钮
- by-label 按钮
- by-category 按钮
- 删除按钮
- 加入到播放表按钮
- 拷贝到 CD 的按钮
- 歌曲表目标
- 歌曲表显示容器和其它

容器和其它:

- 播放器窗口容器
- 音频控制容器
- 元数据控制容器
- 元数据显示容器
- 工具栏容器目标
- 样品按钮
- 下载按钮
- 购买按钮
- 录制按钮
- 播放器名称目标

- 标签/提供者/商店广告目标
- 标签/提供者/商店 URL 按钮
- 艺术家 URL 按钮以及其它

3. 拷贝/播放管理组件 1504

这些组件处理设置加密密钥、水印处理、拷贝管理以及其它。接口也存在用于和交换所 105 进行通信，传送购买请求，和其它，用于特定的服务如按次付款或每次对内容 113 的访问被记帐的情况。目前，到交换所 105 的通信功能是由 SC 过程 192 来处理的。

由最终用户设备 109 上的播放器应用程序 195 对内容 113 的使用被记录到一个例如许可证数据库 197 的数据库中。播放器应用程序 195 对内容 113 的每次使用的跟踪能够被传送到一个或多个记录站点如交换所 105 或内容提供者 101 或是电子数字内容商店 103，或是设计并连接到传送基础设施 107 的任何站点。这个传送能在预定的时期被调度以上载使用信息到一个记录站点上。当传送基础设施 107 不因网络交通而拥挤时，一个预定的时间期望在清晨。播放器应用程序 195 使用熟知的技术，在一个排定的时间唤醒，并且传送来自本地记录数据库的信息到记录站点。通过检查这个记录站点信息，内容提供者 101 能够测定他们的内容 113 的受欢迎性。

在另外一个实施例中，不是记录内容 113 的使用以便以后上载到一个记录站点上，而是在每次使用内容 113 的期间，内容 113 的使用都会上载到记录站点。例如，当复制或拷贝存储在最终用户设备 109 上的内容 113 到一个外部设备如 DVD 盘，数字磁带，闪存，miniDisk 或等效的可读/写可移动的介质上时，这个使用就会更新到记录站点上。这可能是当内容 113 购买时所传送的使用条件 206 中对于拷贝内容 113 的一个前提。这就确保了在内容 113 的播放复制或其它作用时，内容提供者 101 能够精确地跟踪他们的内容 113 的使用。

另外，其他关于内容 113 的信息也能被上载到记录站点。例如，如果内容 113 已经被复制或拷贝到一个授权了的外部设备如 DVD 盘，数字磁带或 miniDisk 上，内容 113 被执行的最后时间（例如小时

或日）；内容 113 被执行了多少次等信息也能被上载到记录站点。在最终用户设备 109 上的一个单一的播放器应用程序 195 有多个不同的用户的情况下，如一个家庭中的不同成员，内容 113 的使用者的标识符和使用信息被一起传送到记录站点上。通过检验上载到记录站点的使用信息，内容提供者 101 能根据实际使用，使用者的标识符和内容 113 已被执行的次数测定内容 113 的受欢迎性。实际使用的测量使这个系统比使用采样方法如电视的 Nielsen 评级方案或电话测量的系统更加符合实际，在使用采样方法的系统中，只有有限数量的用户在任何一个时间被抽样并推断出结果。在当前的实施例中，用户的实际的使用能被测量，记录返回到一个指定的 Web 站点如电子数字内容商店 103 或内容提供者 101。

4. 解密 1501，解压缩 1506 和回放组件 1506

这些组件使用由拷贝/播放管理组件得到的密钥，以便解锁从数据管理和库访问组件中获得的音频数据，应用适当的解压缩来准备其回放，并使用系统音频服务程序来播放它。在一个供替代的实施例中，从数据管理和库访问组件得到的音频数据能被拷贝到可移动的介质如 CD，软磁盘，磁带或 miniDisk 上。

5. 数据管理 1502 和库访问组件 1503

这些组件用于存储和检索最终用户系统的各种存储设备上的歌曲数据，还处理有关存储的歌曲的信息的请求。

6. 应用程序间通信组件 1508

这些组件用于安全数字内容电子销售播放器和其他的可以调用播放器应用程序 195 或播放器应用程序 195 程序在实现其功能时需要使用的应用（例如浏览器，帮助器-app 和/或插件程序等等）之间的配合。例如，当激活一个 URL 控制时，它就调用适当的浏览器并指示它加载适当的页面。

7. 其他杂项组件

各个没有归于上面类别的组件（例如安装）被组合在这里。

8. 通用播放器

在这部分中讨论的是将上面的组件组合成播放器应用程序 195 的一个版本。由于该播放器应用程序 195 根据软件目标，进行过用户化设计，因此仅仅是多个可能的不同例子中的一个。

播放器目标管理器 1501 是一个将所有的其他组件结合起来的软件结构。正如上面部分所讨论的，在此图中播放器目标管理器 1501 下面的块是任何播放器所必需的，但是可以用特别指明的版本替换，这取决于例如使用的加密或扰频的格式，音频压缩的类型，访问内容 113 的库的方法和其它这类事情。

在播放器目标管理器 1501 上面的是可变目标 1512，它主要得自于和正在被播放或搜索的内容 113 相关的元数据。借助最终用户显示 1510 和从最终用户控制 1511 接收到的输入，使得这些可变目标为最终用户设备 109 可利用。所有的目标都是可配置的，并且所有容器的布局都是用户化的。这些目标可以用 C/C++，Java 或任何等效编程语言实现。

使用播放器应用程序 195

下面的实施例是用于一个例子其中运行在最终用户设备 109 上的播放器应用程序 195 是一个音频播放器，这里的内容 113 是音乐。熟悉本领域的人可以理解，播放器应用程序 195 也能支持其他类型的内容 113。通常音乐迷有一保存歌曲的 CD 库。所有这些都可以在安全数字内容电子销售系统 100 中得到。已经从电子数字内容商店 103 中购买的一组歌曲被存储于他或她的系统上的数字内容库 196。类似于实际 CD 的歌曲组被存储作为播放表。在某些情况下，播放表完全仿效 CD（例如，可商业购得的 CD 的所有音轨都已从一个电子数字内容商店 103 购买当作这个 CD 的在线版本,并且被一个等同于 CD 播放表的播放表定义）。但是大多数播放表是由最终用户装配成整体来组合他们已经存储在他们系统上的数字内容库中的歌曲。然而，为了下面的讨论，当提及术语播放表时，我们使用了一个用户制作的音乐 CD 的例子。

当最终用户明确地起动播放器应用程序 195，而不是通过从 SC

处理器 192 应用程序调用来启动它时，它就对被访问过的最后的播放表进行预先装载。如果在数字内容库 196 中没有播放表存在，那么播放表编辑器就会自动启动（除非用户已经经由一个优选设置关闭了这个特性）。参看下面的播放表，有更多详细信息。

播放器应用程序 195 也可根据参数，被一特定歌曲调用，在这种情况下，它马上进入歌曲播放状态。在另一可选情况下，歌曲可被准备好以便播放，但是要等待最终用户的行动而进行。请参见下面的歌曲播放获得关于此种情况的更多信息。

播放表（对应于最终用户接口 1603 的屏幕）：

当最终用户调用播放表功能后，可得到的功能如下：

- 打开播放表
- 调用数字内容库来显示一个存储的播放表名单以供选择。也请参照下面的数字内容库以得到更多信息。
- 编辑播放表
- 调用播放表编辑器（参照下面），如果已经加载了一个播放表，这个播放表编辑器就已准备好当前的播放表。否则，编辑器创建一个空的播放表来开始。
- 运行播放表
- 歌曲从所选的那一首开始被逐一播放的（或者是从播放表的最前面开始，如果没有选择任何歌曲时）。播放表编辑器中的选择设置影响回放的顺序。然而有一些可使用的控制以优先于播放表的那些播放选项。
- 播放歌曲
- 只播放从播放表中选择的歌曲。参照下面的歌曲播放以获得更多信息。
- 播放表信息
- 显示与播放表有关的信息

- 歌曲信息
- 显示与播放表中被选择的歌曲有关的信息
- 访问 Web 站
- 将与此播放表有关的 Web 站加载到浏览器中
- 库管理程序
- 打开数字内容库管理窗口。同样参看下面的数字内容库管理以获得更多信息。

播放表编辑器（对应于最终用户接口 1603 的屏幕）:

当调用播放表编辑器时，最终用户的可选项如下:

- 查看/加载/删除播放表。
- 数字内容库管理程序被调用来显示一系列存储的播放表供选择一个进行加载或删除。参看下面数字内容库管理程序的更多信息
- 保存播放表
  - 播放表的当前版本保存在数字内容库 196 中。
  - 删除歌曲
  - 将当前选择的歌曲从播放表中删除
  - 添加歌曲
  - 以歌曲搜索的方式来调用数字内容库，选择歌曲加入到播放表中。参看下面数字内容库管理程序的更多信息
  - 设置歌曲信息
  - 显示并允许改变播放表中的被选的歌曲的有关信息。

这个信息存储在播放表中，并且不会改变数字内容库 196 中存储的歌曲的有关信息。以下事物能够被改变:

- 显示的歌曲标题
- 最终用户关于歌曲的注释
- 播放歌曲而引起的延迟
- 播放歌曲后继续的延迟
- 当播放歌曲时歌曲中的开始点

- 当播放歌曲时歌曲中的终止点
- 随机方式的权重
- 歌曲的音量调整及其它。

设置播放表的属性：显示并允许改变此播放表的属性。设置如下属性：

- 播放表标题
- 播放表方式（随机、顺序的等等）
- 重复的方式（播放一次、结束时重新开始等等）
- 最终用户关于此播放表的注释

库管理程序（对应于最终用户接口 1601 的屏幕）：

- 打开数字内容库管理程序窗口。参看下面的数字内容库管理程序的更多信息

歌曲播放

当准备好播放一首歌曲时，或者用这首歌曲作为一个参数调用播放器应用程序 195，或者通过从播放表或数字内容库管理程序中选择一首歌曲播放，有以下最终用户的选择：（对应于最终用户接口 1601 的屏幕）

- 播放
- 暂停
- 停止
- 后跳
- 前跳
- 调整音量
- 调整音轨位置
- 观看歌词
- 观看注解
- 观看 CD 封面
- 观看艺术家图

- 观看音轨信息
- 观看其他元数据
- 访问 Web 站点
- 播放表
- 库管理程序以及其它。

数字内容库管理程序

当选择歌曲或播放表（参照上面）时，就隐含地调用数字内容库管理程序，或可以在它自己的窗口中被打开以管理最终用户系统上的歌曲库。在那种情况下，最终用户的选择项有:

对于歌曲:

根据艺术家，类别，标签，其它将所有歌曲排序
根据艺术家，类别，标签，其它选择歌曲
将选择的歌曲添加到当前播放表中
将歌曲拷贝到 CD 中（如果被允许）
删除歌曲
将歌曲添加到类别中以及其它
对于播放表:
根据名称排序
根据类别排序
根据关键字搜索
根据包含的歌曲标题搜索
加载所选的播放表
重命名播放表
删除播放表
根据所选的播放表创建 CD（如果被允许）以及其它。

现在转向图 18，它是按照本发明运行在最终用户设备 109 上用以

一个一个单独地追踪内容的过程的流程图。内容 ID 1802 是在内容准备期间由内容提供者 101 提供的。在一个实施例中，内容 ID 1802 在用安全容器打包工具进行内容创建的过程中是内容 SC 630 的一部分。在另外一个实施例中，内容 ID 1802 是元数据 SC 620（包含有促销数据）的一部分。内容 ID 1802 是一个标识符，它对于正在被处理的内容来说是唯一的。

正如前面早先讨论的，在由交易处理器模块 175 建立的交易 SC 640 中，交易 ID 535 连同内容 ID 1802 是交易数据 642 的一部分。交易 ID 535 对于所有来自于最终用户设备 109 的购买交易的每一个购买交易都是一个唯一的标识符。另外，项目号 1806 是一个由电子数字内容商店 103 产生的，对于每一个，对于每一块，每一成分或标题这些形成交易的部分都是唯一的标识符。规定的项目号 1806 追踪交易 ID 535 下的每个购买的项目。

现在将注意力集中到最终用户设备 109 上的由其接收的操作。另外，带有内容 ID 1802 的也包含在交易 ID 535 中的报价 SC 被接收。购买 ID 1802 是在最终用户设备 109 上创建的。在一个实施例中，购买 ID 是一个三个号码连接的操作 1810，逐一地是内容 ID 1802 和交易 ID 535 和项目号 1806。可以理解，除了连接操作 1810，其他类型的连接能用于产生购买 ID 1812 例如将三个号或其他导致一个唯一购买 ID 1812 的数学组合杂列在一起。将三个号组合的处理能使用前面讨论的在播放器应用程序中的反篡改代码技术来完成，以保护对购买 ID 计算的非授权访问。

一旦一个唯一的购买 ID 1812 被创建并且与内容 113 的每个部分建立关联，在最终用户设备 109 上的播放器应用程序 195 能够为内容 113 的每个部分追踪存储使用条件 519，即使有不止一个相同内容 113 的拷贝，如存储在最终用户设备 109 上的一首歌曲。

尽管已经公开了本发明的一个具体的实施例，熟悉本领域中技能的人能够理解，不脱离本发明的精神和范围可以对这个具体的实施例

做某些改变。因此，对于这个具体的实施例来说，这个发明的范围不受限制的，并且它意味着所附的权力要求书覆盖任何和全部的这样的应用程序，修改和本发明范畴的这些实施例。

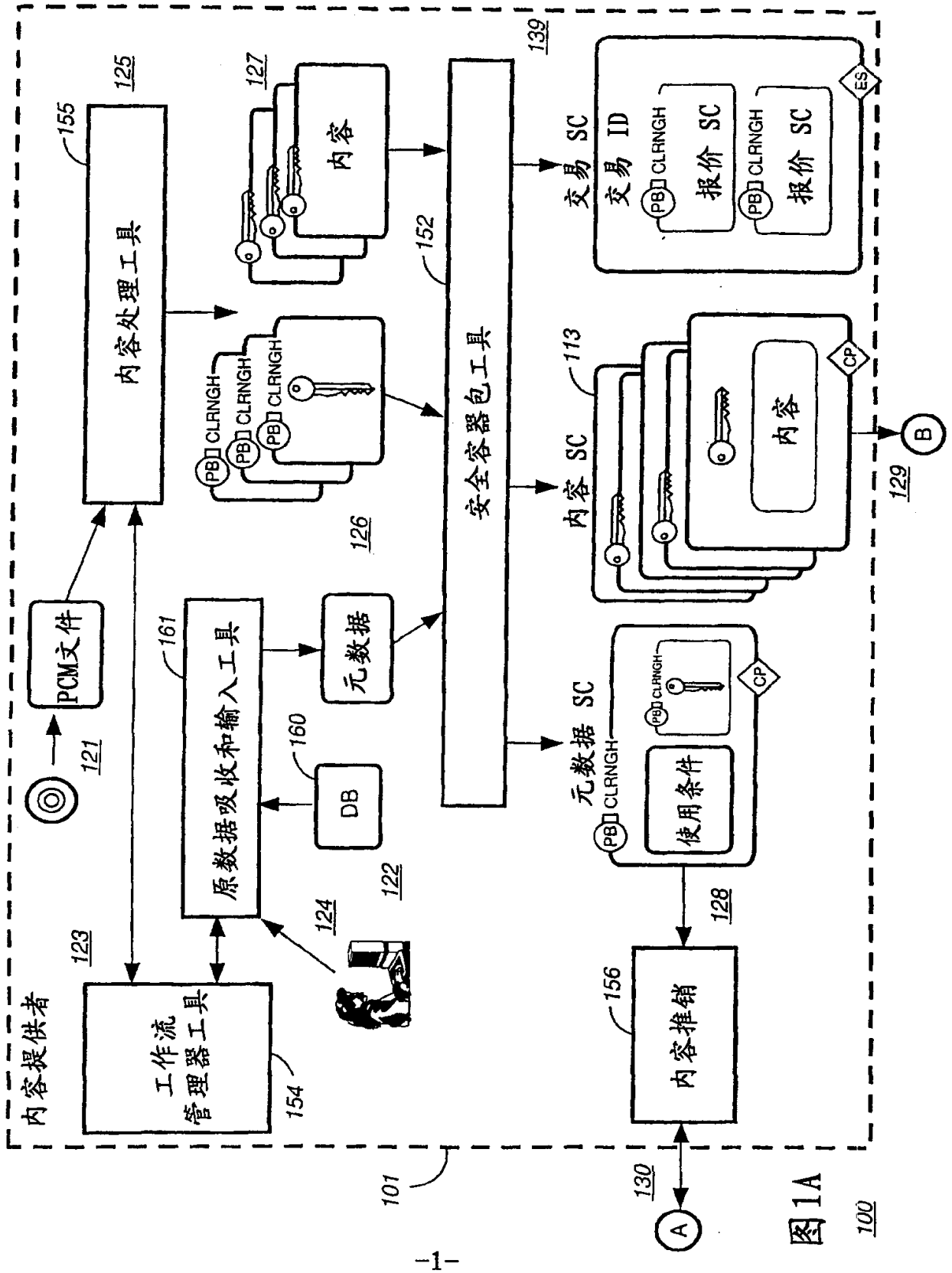

内容提供者
101
PCM文件
121
内容处理工具
125
155
原数据吸收和输入工具
161
160
DB
122
元数据
126
123
工作流管理器工具
154
124
内容
127
PB CLRNGH
PB CLRNGH
PB CLRNGH
安全容器包工具
152
139
交易 SC
交易 ID
PB CLRNGH
报价 SC
PB CLRNGH
报价 SC
ES
内容 SC
113
内容
CP
129
B
元数据 SC
PB CLRNGH
使用条件
PB CLRNGH
CP
128
内容推销
156
130
A
100

图1A

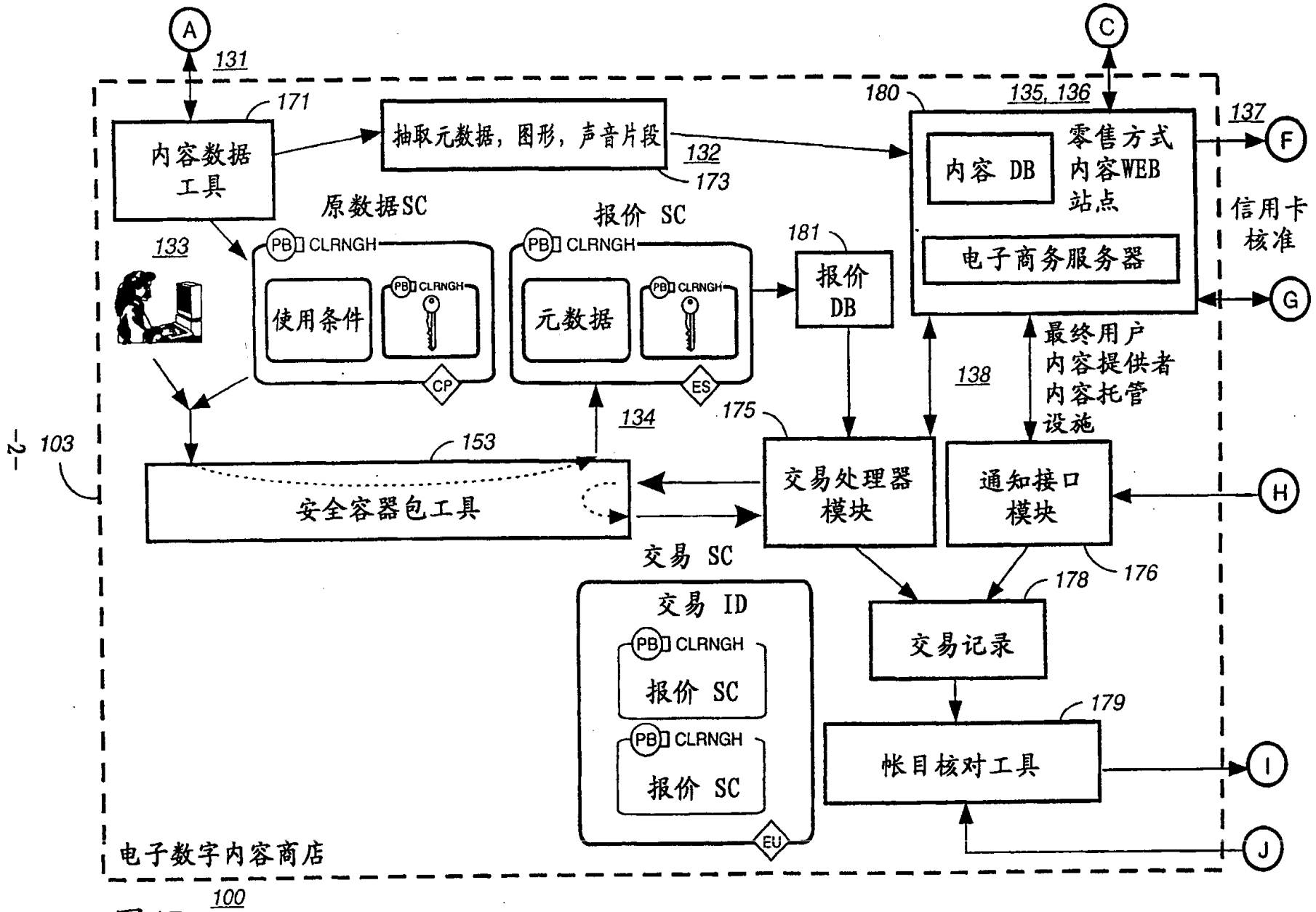

A
131
171
内容数据工具
抽取元数据，图形，声音片段
132
173
C
180
135, 136
137
F
内容 DB
零售方式内容WEB站点
信用卡核准
电子商务服务器
G
原数据SC
报价 SC
133
PB CLRNGH
使用条件
元数据
CP
ES
181
报价DB
138
最终用户内容提供者内容托管设施
134
175
153
103
安全容器包工具
交易处理器模块
通知接口模块
H
交易 SC
交易 ID
178
176
交易记录
179
帐目核对工具
I
J
电子数字内容商店
100

图1B

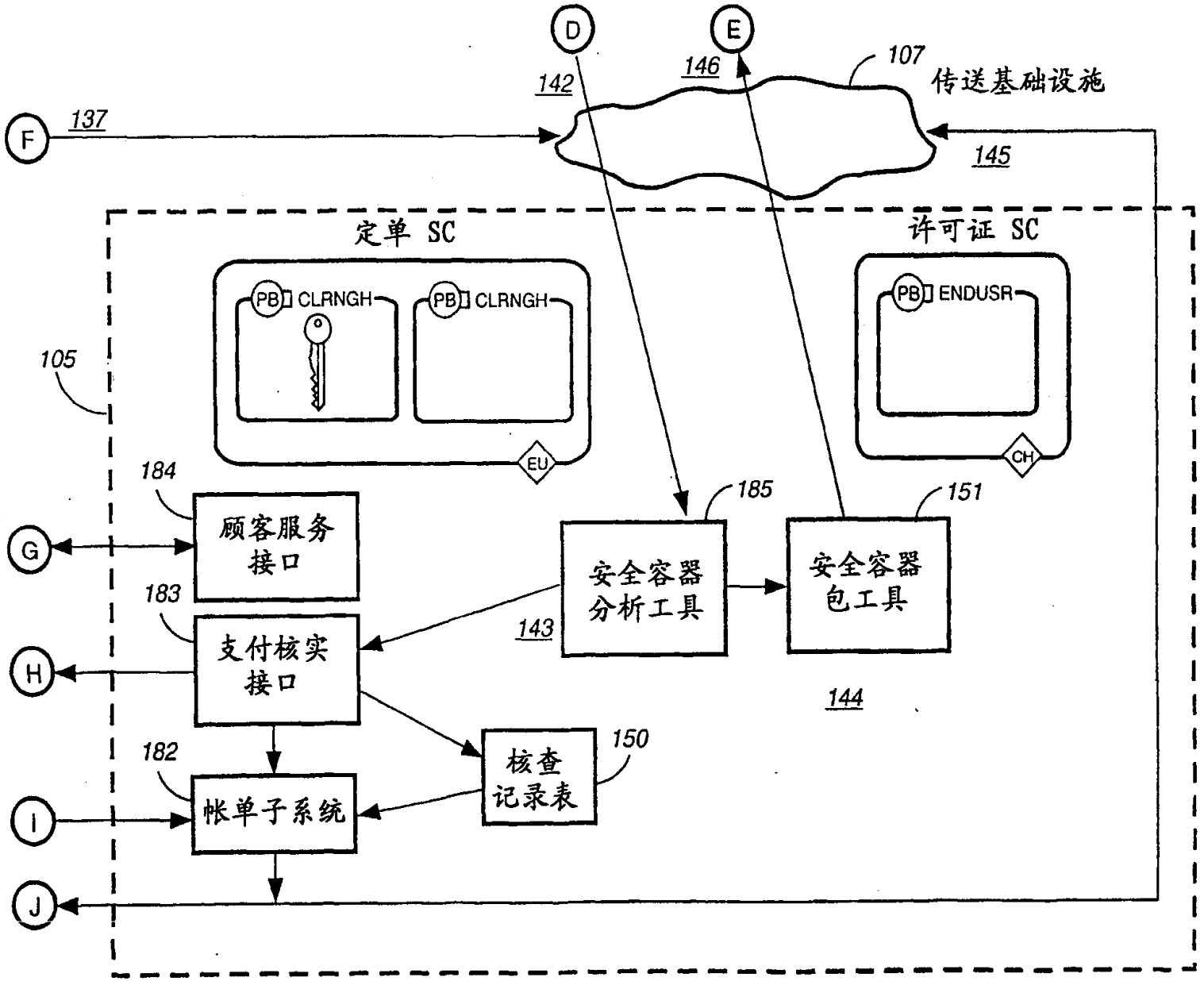
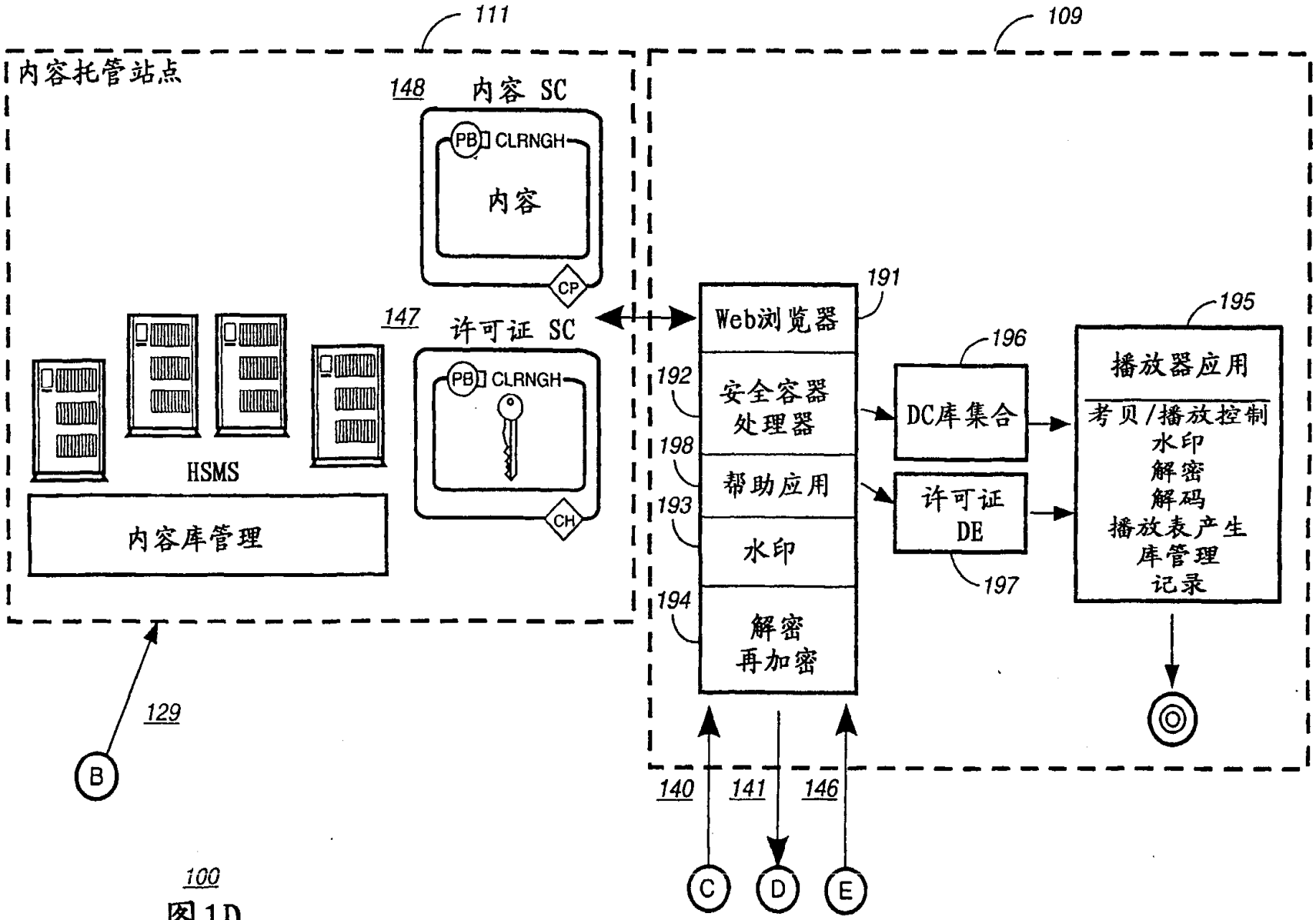

D
E
142
146
107
传送基础设施
F
137
145
定单 SC
许可证 SC
PB CLRNGH
PB CLRNGH
PB ENDUSR
105
EU
CH
184
185
151
顾客服务接口
安全容器分析工具
安全容器包工具
G
183
143
支付核实接口
H
144
150
182
核查记录表
帐单子系统
I
J
100

图1C


111
109
内容托管站点
148
内容 SC
PB
CLRNGH
内容
CP
147
许可证 SC
PB
CLRNGH
CH
HSMS
内容库管理
129
B
191
Web浏览器
192
安全容器
处理器
198
帮助应用
193
水印
194
解密
再加密
196
DC库集合
许可证
DE
197
195
播放器应用
考贝/播放控制
水印
解密
解码
播放表产生
库管理
记录
140
141
146
C
D
E

100

图1D

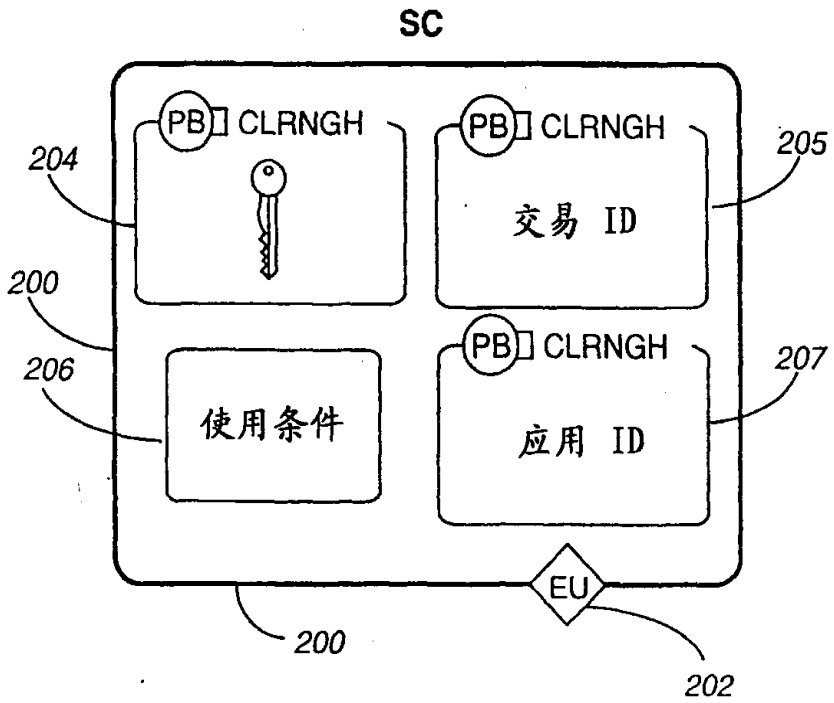
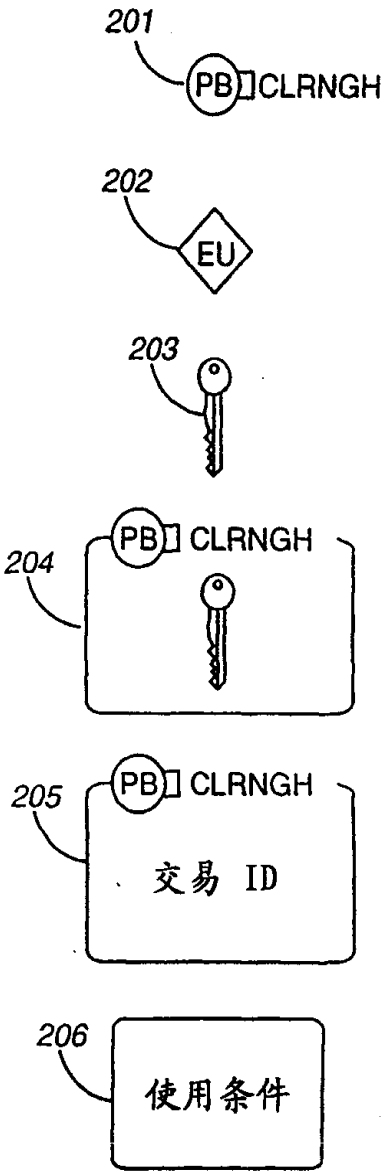

SC
PB CLRNGH
204
PB CLRNGH
交易 ID
205
200
206
使用条件
PB CLRNGH
应用 ID
207
EU
200
202

图 2


201
PB CLRNGH
202
EU
203
204
PB CLRNGH
205
PB CLRNGH
交易 ID
206
使用条件

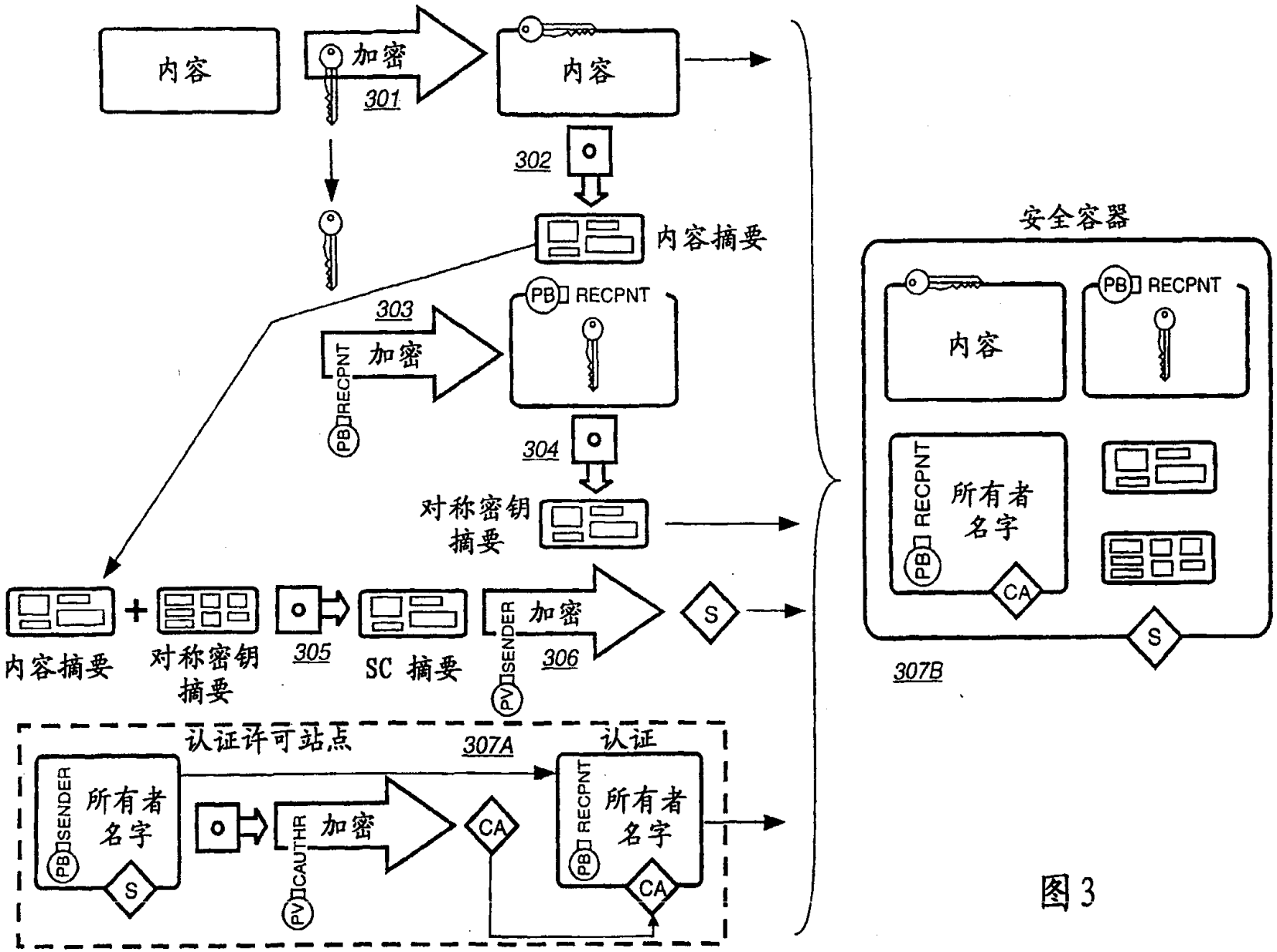

内容
加密
301
内容
302
内容摘要
PB RECPNT
303
加密
PB RECPNT
304
对称密钥
摘要
内容摘要
对称密钥
摘要
305
SC 摘要
PV SENDER
加密
306
S
认证许可站点
307A
认证
PB SENDER
所有者
名字
S
PV CAUTHR
加密
CA
PB RECPNT
所有者
名字
CA
安全容器
内容
PB RECPNT
PB RECPNT
所有者
名字
CA
S
307B

图 3

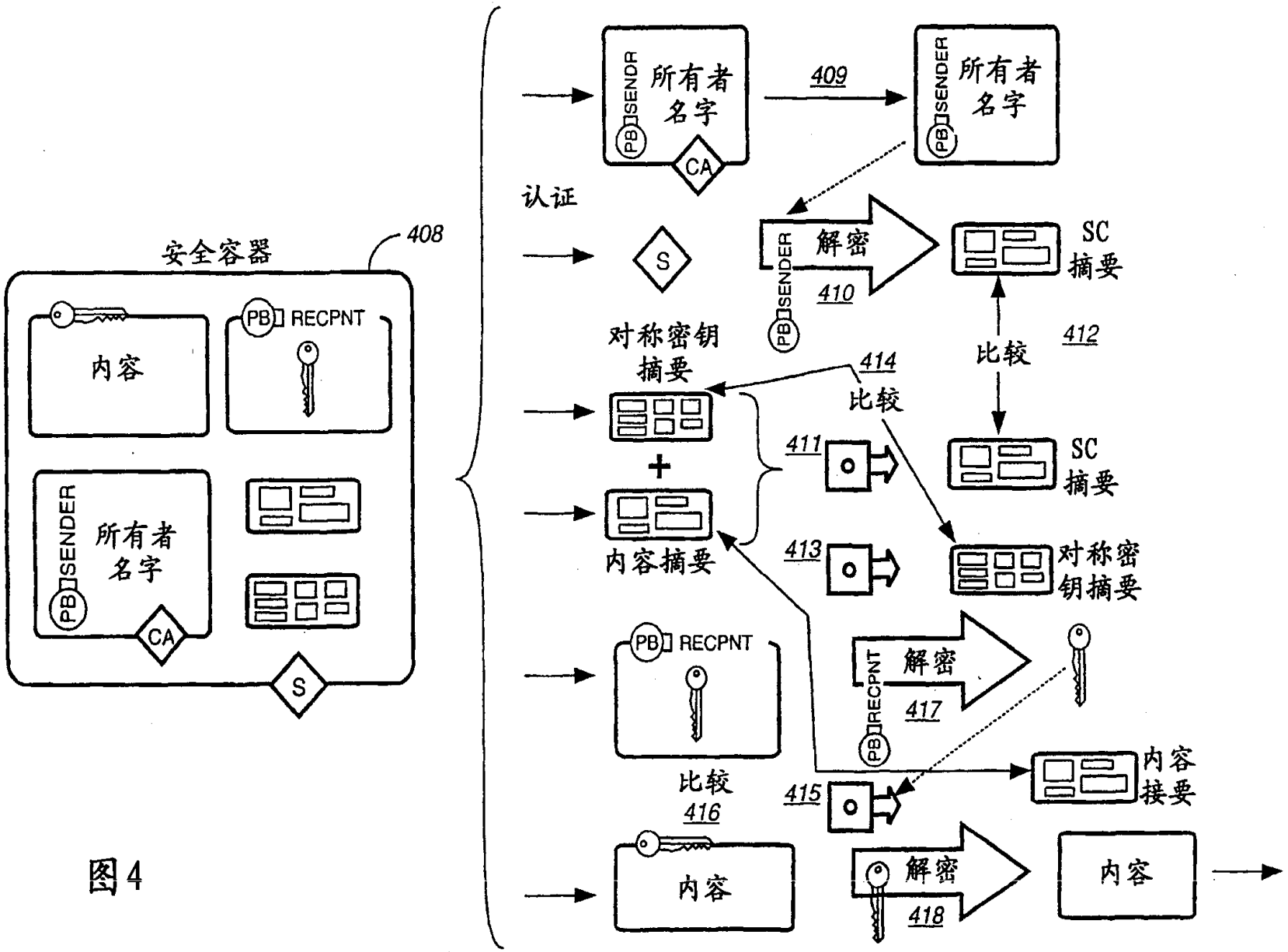

安全容器
408
内容
PB RECPNT
PB SENDER
所有者名字
CA
S
所有者名字
409
认证
解密
410
SC摘要
比较
412
对称密钥摘要
414
比较
411
SC摘要
内容摘要
413
对称密钥摘要
PB RECPNT
解密
417
内容接要
比较
416
415
内容
解密
418
内容

图4

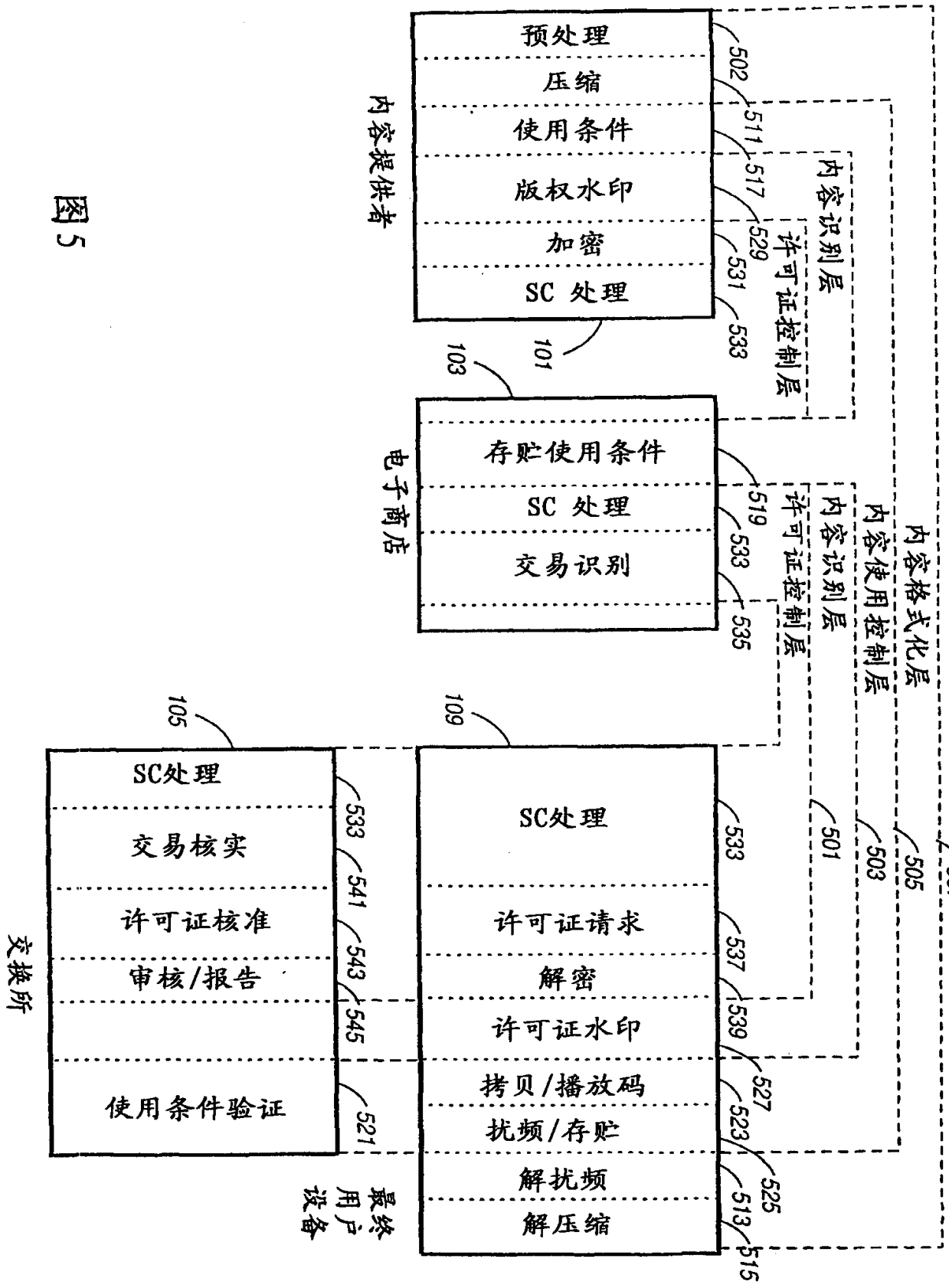

内容格式化层
内容使用控制层
内容识别层
许可证控制层
内容提供者
预处理
压缩
使用条件
版权水印
加密
SC 处理
502
511
517
529
531
533
101
103
电子商店
存贮使用条件
SC 处理
交易识别
519
533
535
105
109
交换所
SC处理
交易核实
许可证核准
审核/报告
使用条件验证
533
541
543
545
521
最终用户设备
SC处理
许可证请求
解密
许可证水印
拷贝/播放码
扰频/存贮
解扰频
解压缩
533
537
539
527
523
525
513
515
501
503
505
507

图 5

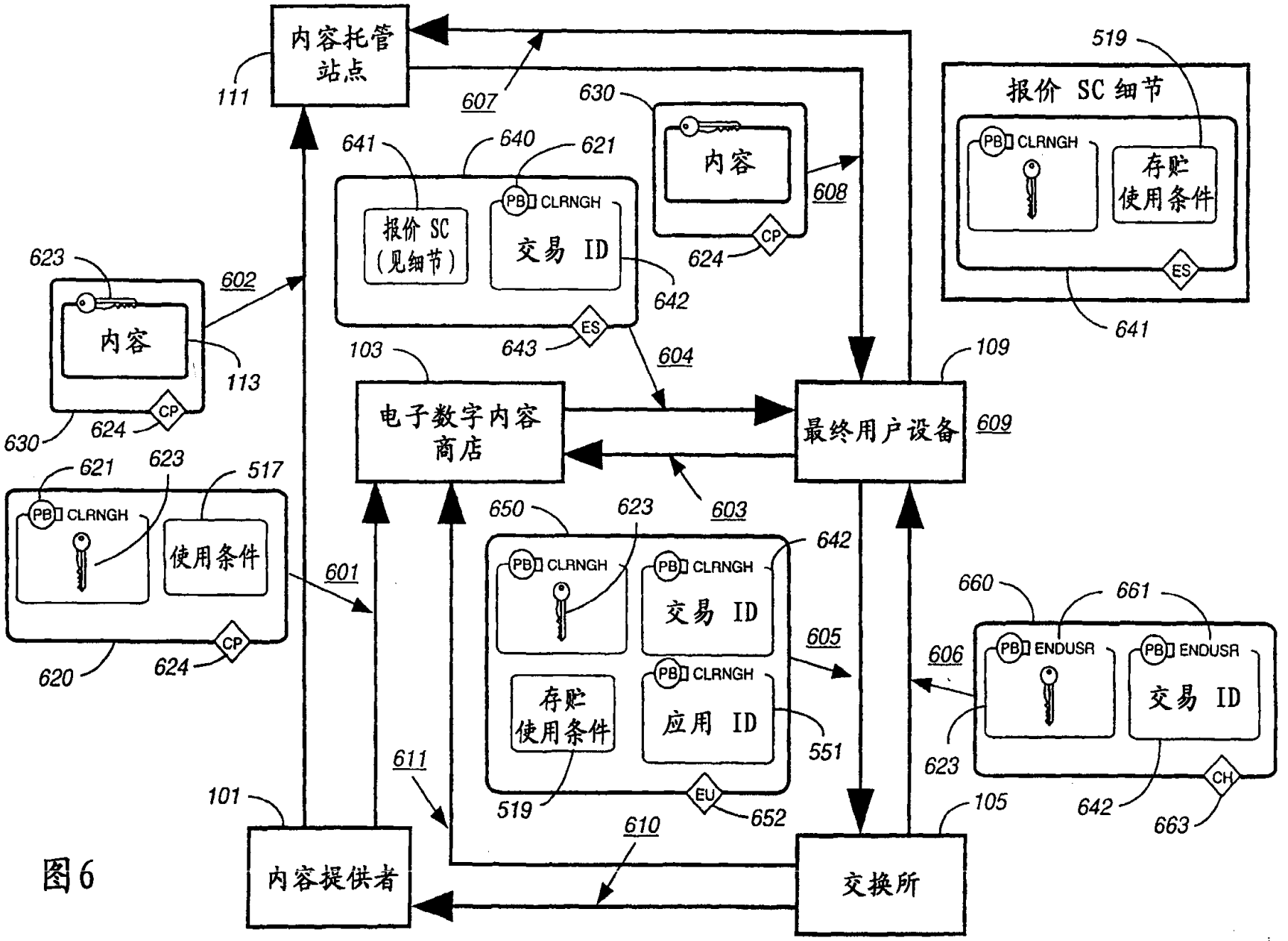

内容托管站点
111
607
519
报价 SC 细节
PB CLRNGH
存贮使用条件
ES
641
630
内容
608
CP
624
641
640
621
报价 SC（见细节）
PB CLRNGH
交易 ID
642
ES
643
604
623
602
内容
113
CP
630
624
103
电子数字内容商店
109
最终用户设备
609
603
621
623
517
PB CLRNGH
使用条件
CP
620
624
601
650
623
642
PB CLRNGH
PB CLRNGH
交易 ID
605
存贮使用条件
PB CLRNGH
应用 ID
551
519
EU
652
660
661
606
PB ENDUSR
PB ENDUSR
交易 ID
623
642
CH
663
611
101
610
105
内容提供者
交换所

图6

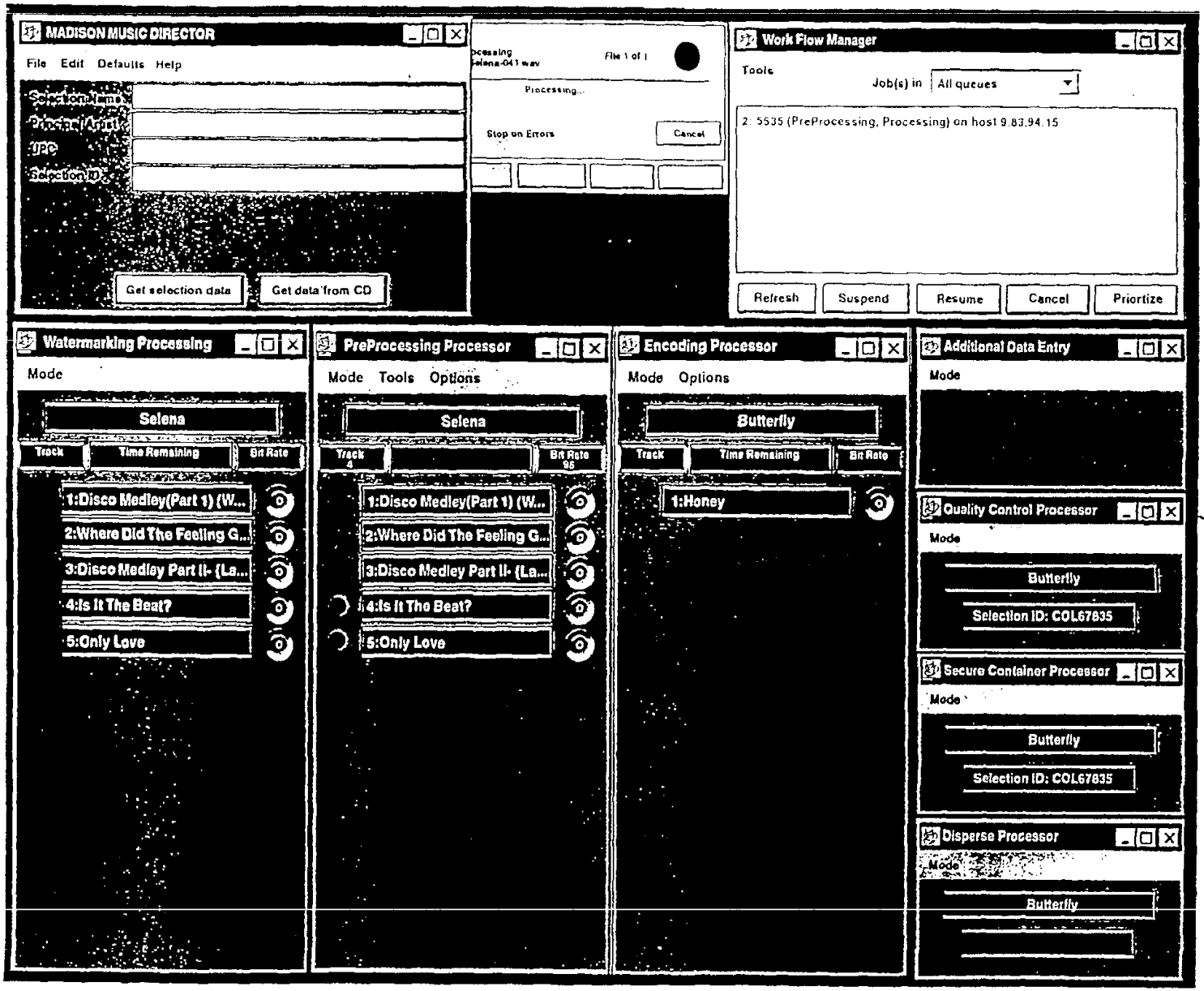

MADISON MUSIC DIRECTOR
File Edit Defaults Help
Get selection data
Get data from CD
Stop on Errors
Cancel
Work Flow Manager
Tools
Job(s) in All queues
2: 5535 (PreProcessing, Processing) on host 9.83.94.15
Refresh
Suspend
Resume
Cancel
Priortize
Watermarking Processing
Mode
Selena
Track
Time Remaining
Bit Rate
1:Disco Medley(Part 1) (W...
2:Where Did The Feeling G...
3:Disco Medley Part II- (La...
4:Is It The Beat?
5:Only Love
PreProcessing Processor
Mode Tools Options
Selena
Track
Bit Rate
1:Disco Medley(Part 1) (W...
2:Where Did The Feeling G...
3:Disco Medley Part II- (La...
4:Is It The Beat?
5:Only Love
Encoding Processor
Mode Options
Butterfly
Track
Time Remaining
Bit Rate
1:Honey
Additional Data Entry
Mode
Quality Control Processor
Mode
Butterfly
Selection ID: COL67835
Secure Container Processor
Mode
Butterfly
Selection ID: COL67835
Disperse Processor
Mode
Butterfly
700

图 7

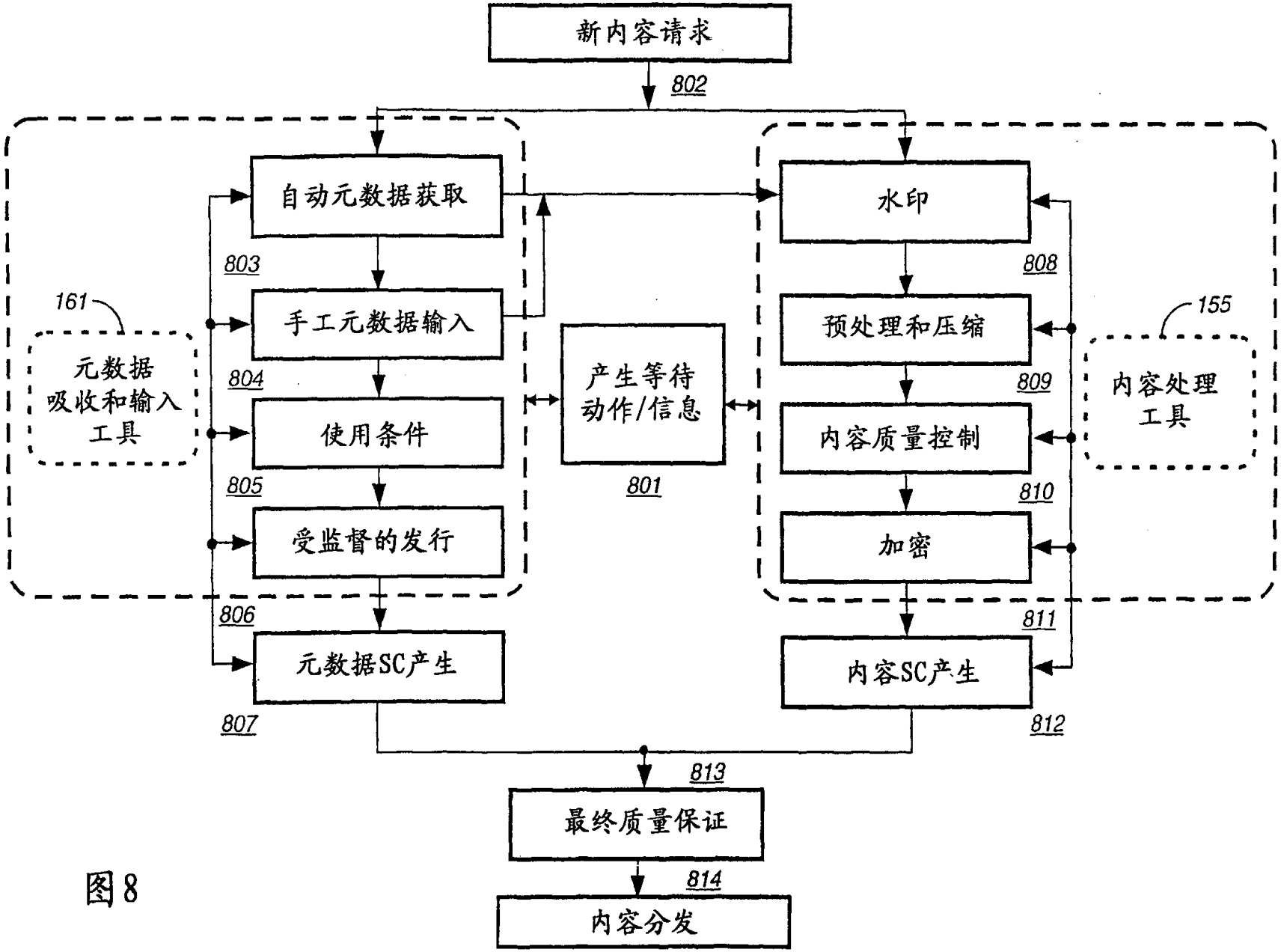

新内容请求
802
自动元数据获取
803
161
手工元数据输入
804
元数据
吸收和输入
工具
使用条件
805
受监督的发行
806
元数据SC产生
807
产生等待
动作/信息
801
水印
808
预处理和压缩
809
内容质量控制
810
加密
811
内容SC产生
812
155
内容处理
工具
813
最终质量保证
814
内容分发

图8

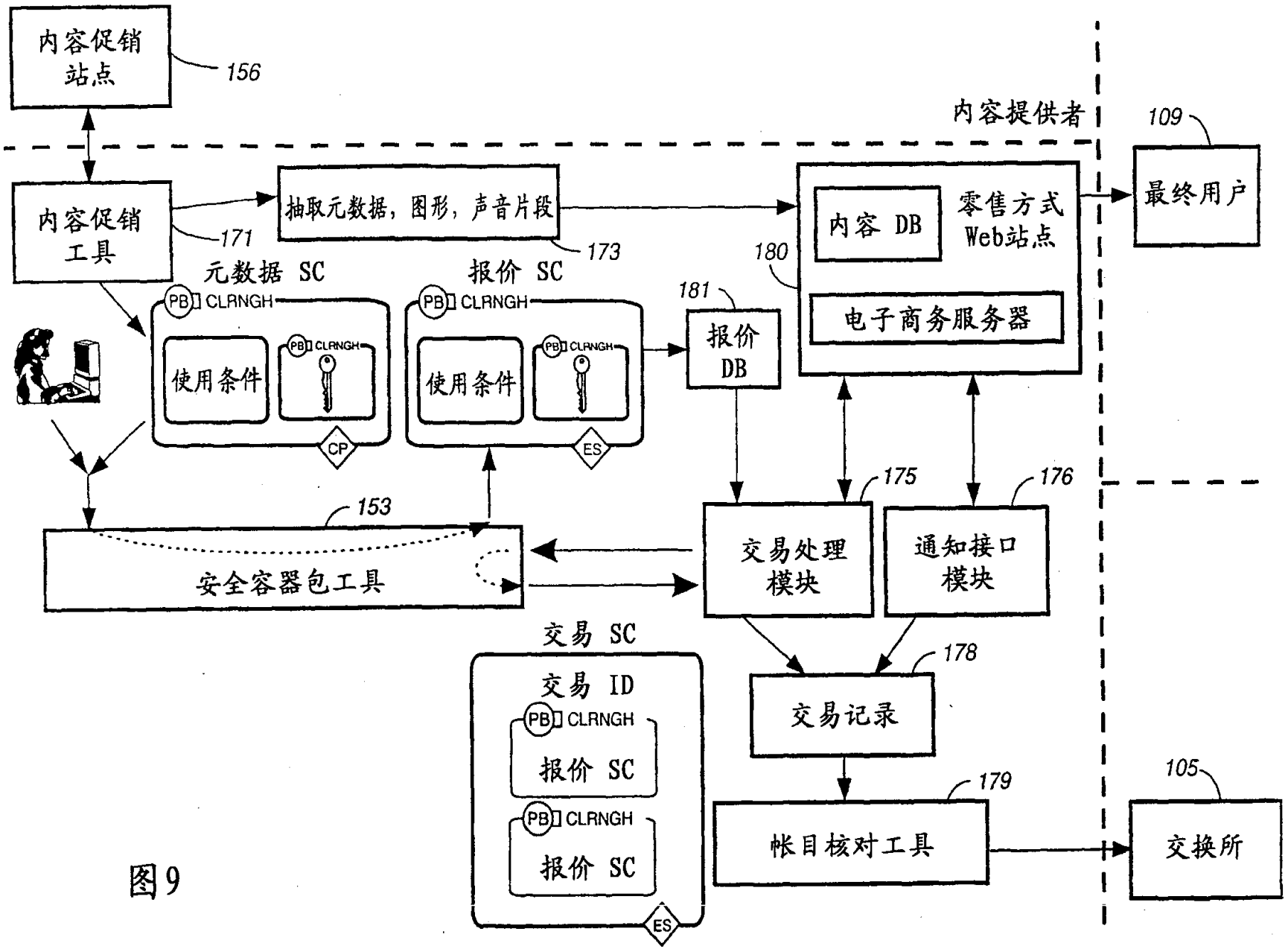

内容促销站点
156
内容提供者
109
最终用户
内容促销工具
171
抽取元数据，图形，声音片段
173
内容 DB
零售方式Web站点
180
电子商务服务器
元数据 SC
报价 SC
PB CLRNGH
使用条件
CP
ES
181
报价DB
153
安全容器包工具
交易处理模块
175
通知接口模块
176
交易 SC
交易 ID
178
交易记录
179
帐目核对工具
105
交换所

图9

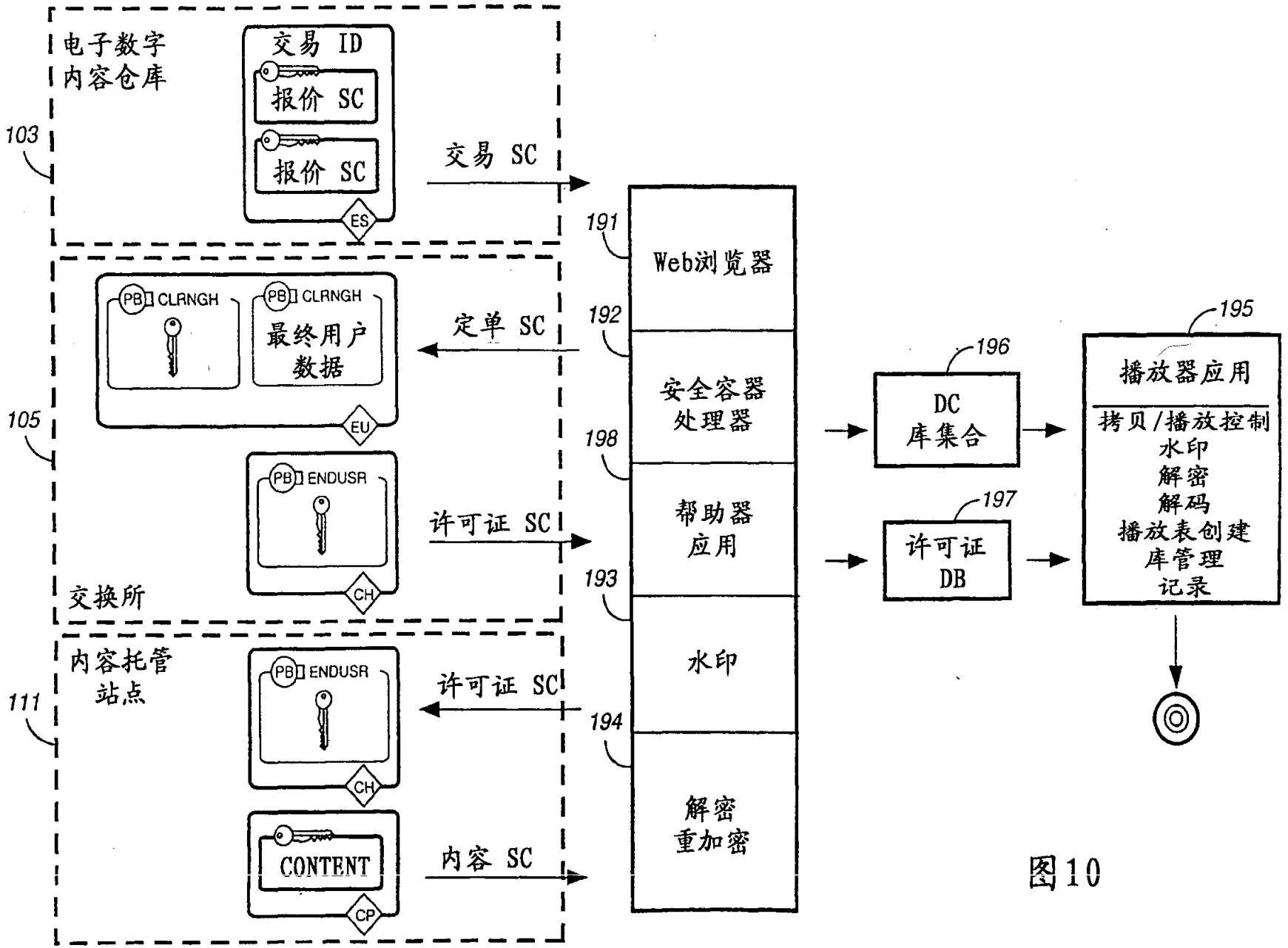

电子数字
内容仓库
103
交易 ID
报价 SC
报价 SC
ES
交易 SC
105
PB CLRNGH
PB CLRNGH
最终用户
数据
EU
定单 SC
PB ENDUSR
CH
许可证 SC
交换所
内容托管
站点
111
PB ENDUSR
CH
许可证 SC
CONTENT
CP
内容 SC
191
Web浏览器
192
安全容器
处理器
198
帮助器
应用
193
水印
194
解密
重加密
196
DC
库集合
197
许可证
DB
195
播放器应用
拷贝/播放控制
水印
解密
解码
播放表创建
库管理
记录

图10

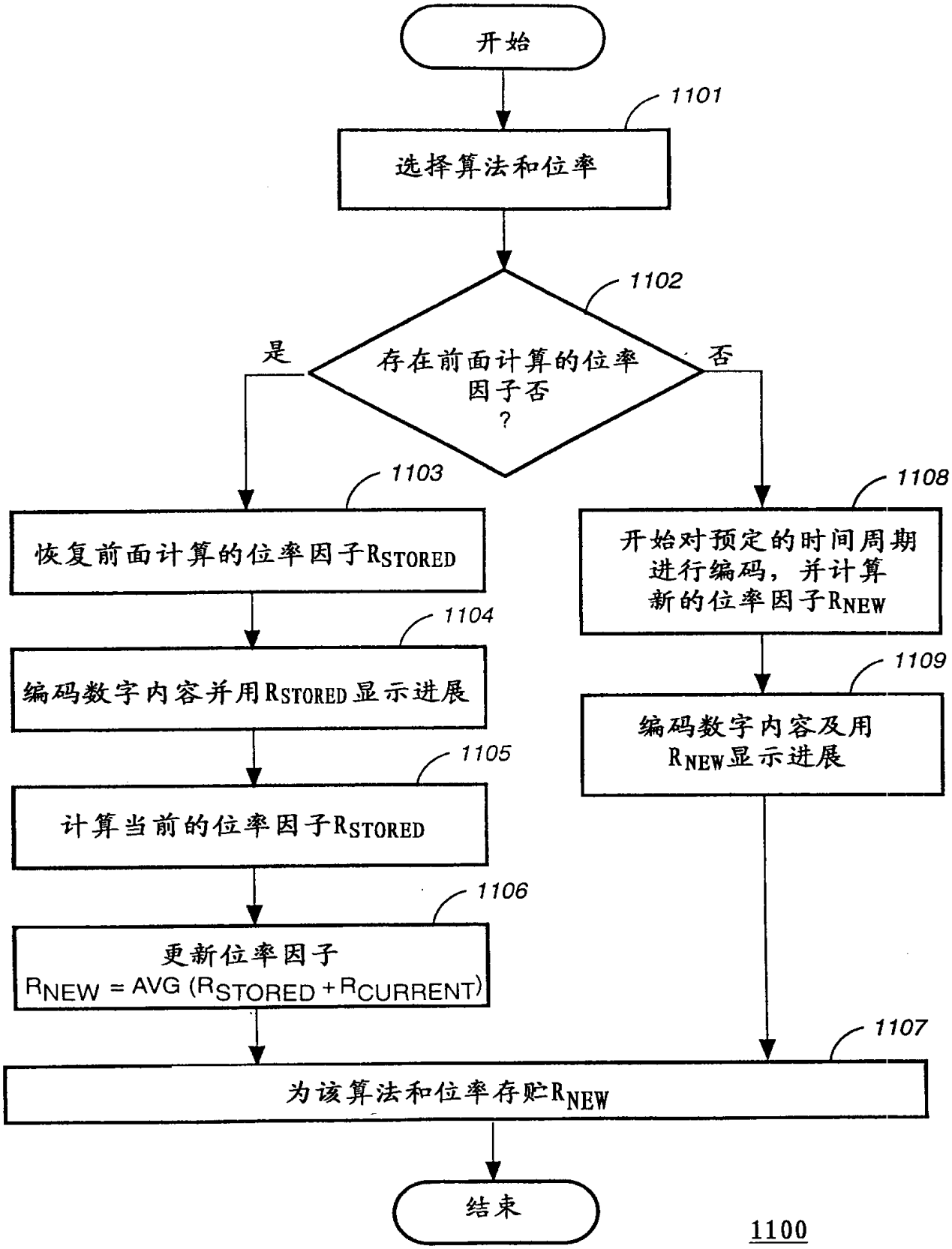

开始
1101
选择算法和位率
1102
存在前面计算的位率因子否?
是
否
1103
恢复前面计算的位率因子RSTORED
1104
编码数字内容并用RSTORED显示进展
1105
计算当前的位率因子RSTORED
1106
更新位率因子
RNEW = AVG (RSTORED + RCURRENT)
1108
开始对预定的时间周期进行编码，并计算新的位率因子RNEW
1109
编码数字内容及用RNEW显示进展
1107
为该算法和位率存贮RNEW
结束
1100

图11

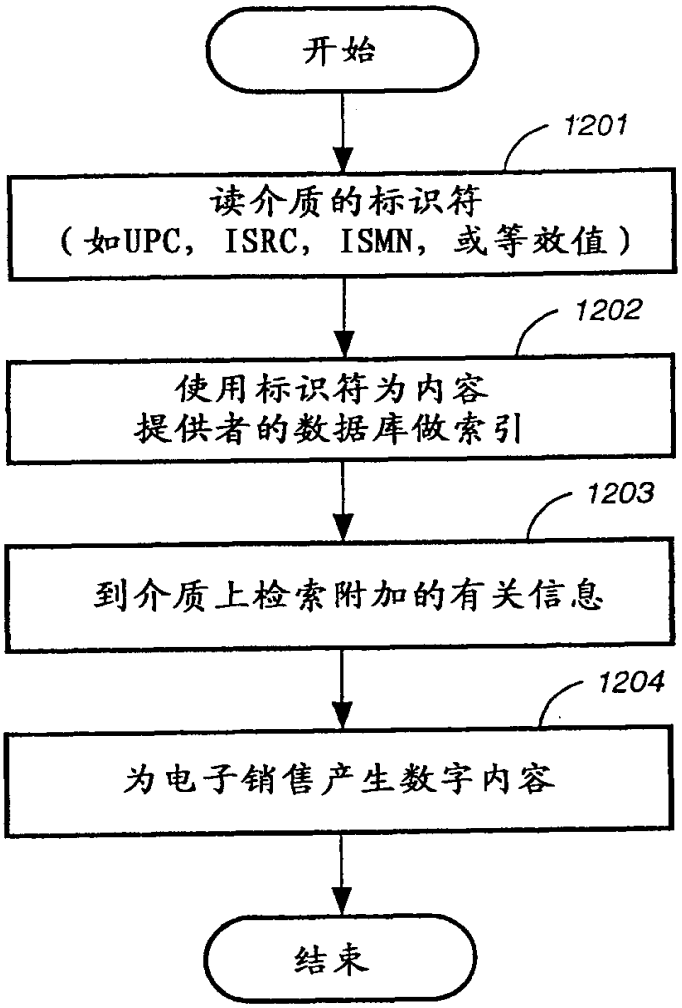

开始
1201
读介质的标识符
（如UPC，ISRC，ISMN，或等效值）
1202
使用标识符为内容
提供者的数据库做索引
1203
到介质上检索附加的有关信息
1204
为电子销售产生数字内容
结束

图12

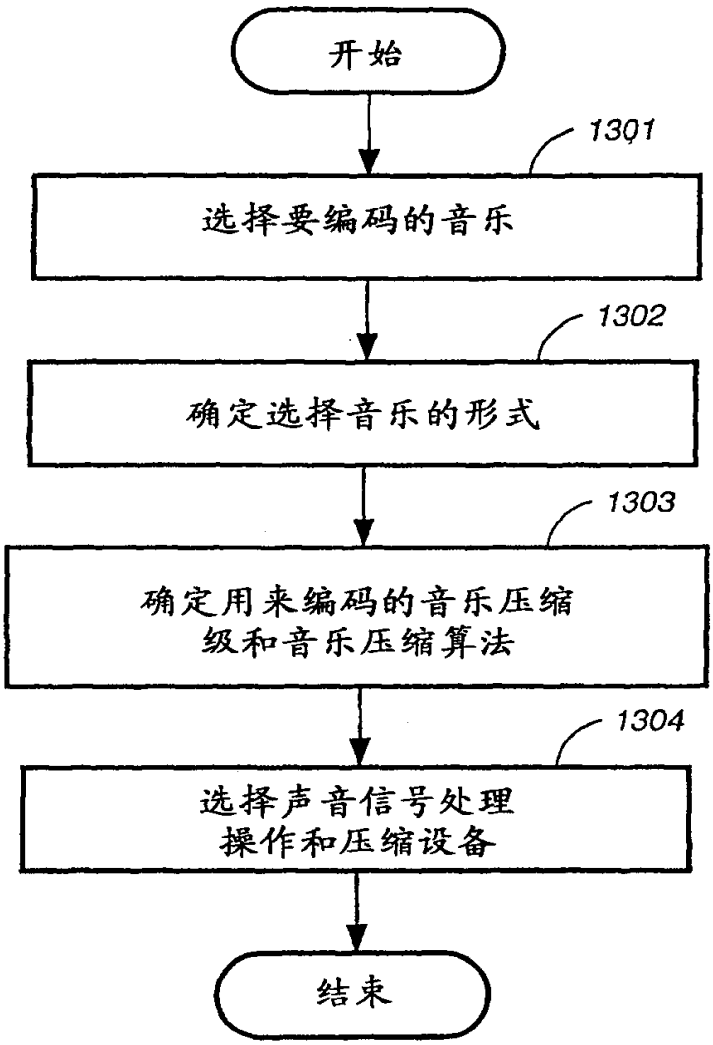

开始
1301
选择要编码的音乐
1302
确定选择音乐的形式
1303
确定用来编码的音乐压缩
级和音乐压缩算法
1304
选择声音信号处理
操作和压缩设备
结束

图13

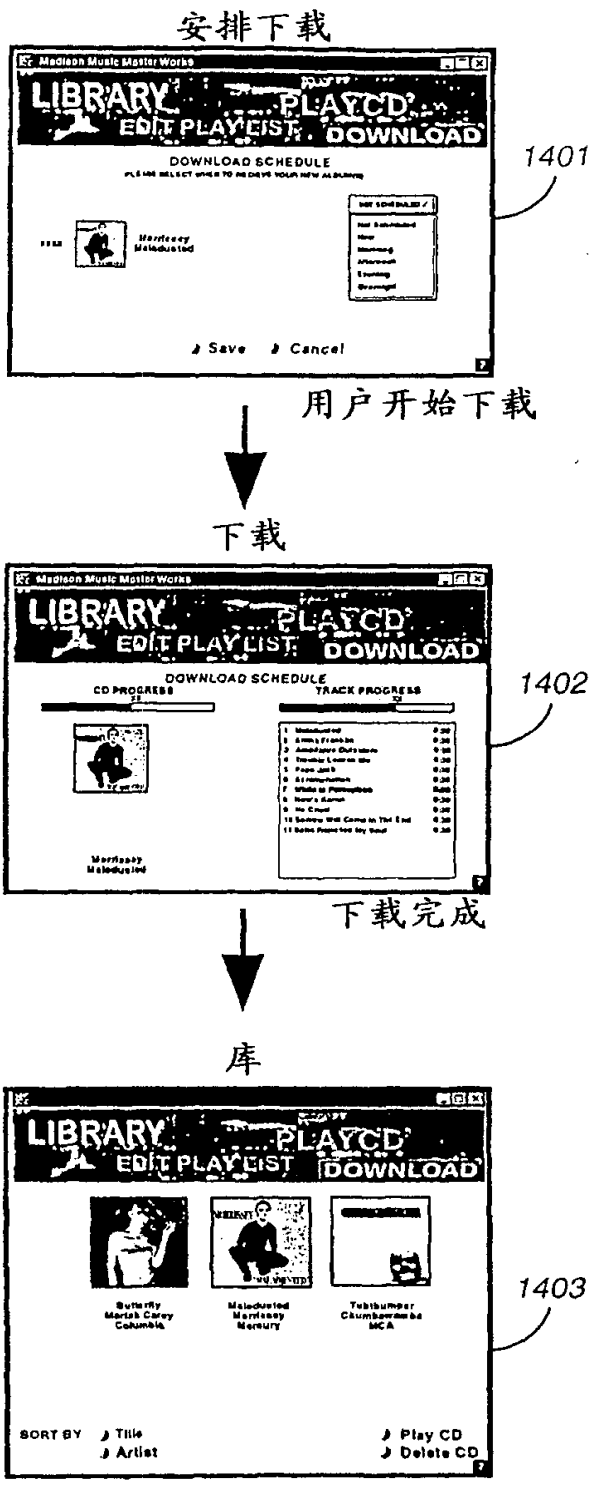

安排下载
LIBRARY
PLAYCD
EDIT PLAYLIST
DOWNLOAD
DOWNLOAD SCHEDULE
Save
Cancel
1401
用户开始下载
下载
LIBRARY
PLAYCD
EDIT PLAYLIST
DOWNLOAD
DOWNLOAD SCHEDULE
CD PROGRESS
TRACK PROGRESS
1402
下载完成
库
LIBRARY
PLAYCD
EDIT PLAYLIST
DOWNLOAD
1403
SORT BY
Title
Artist
Play CD
Delete CD

图 14

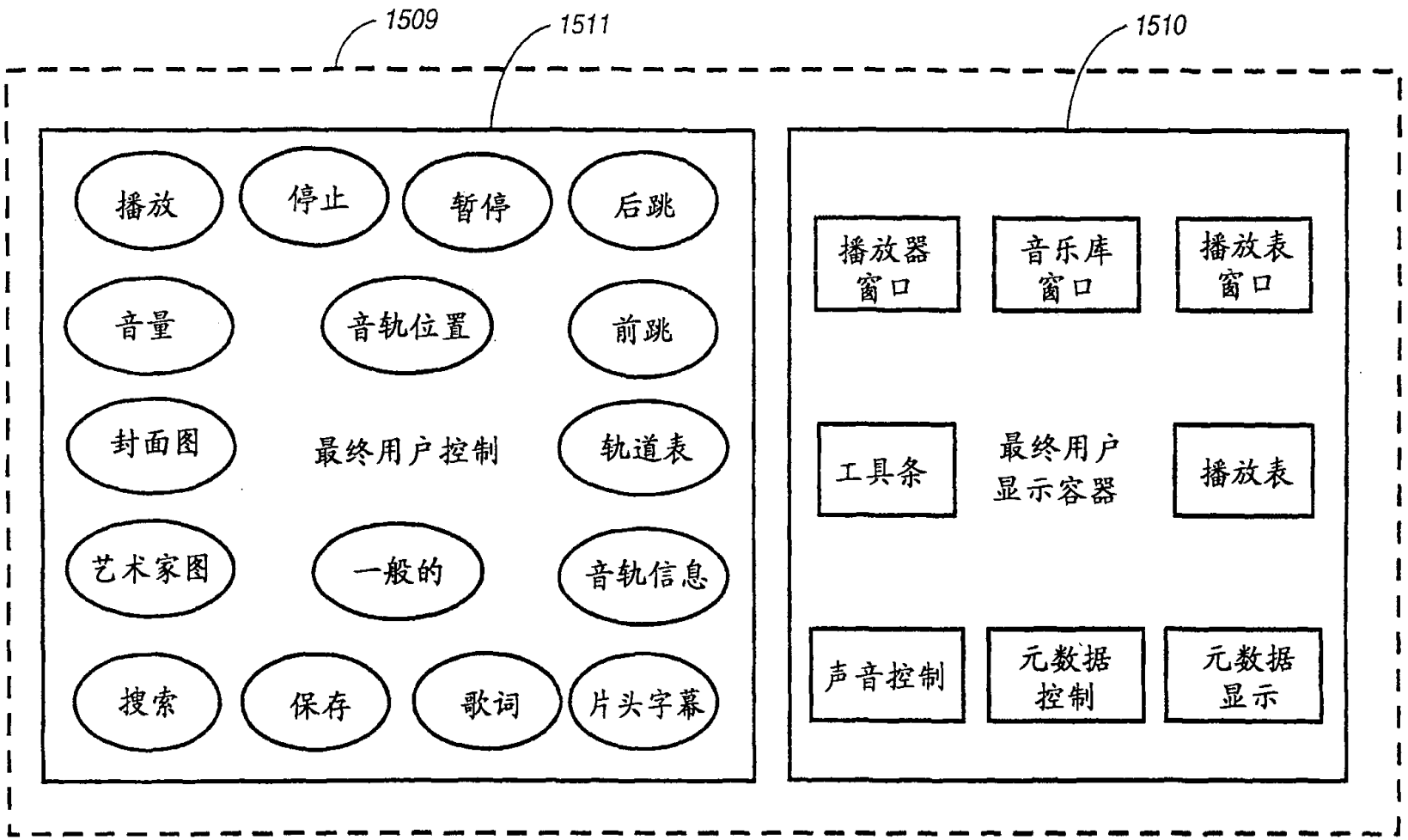

1509
1511
1510
播放
停止
暂停
后跳
音量
音轨位置
前跳
封面图
最终用户控制
轨道表
艺术家图
一般的
音轨信息
搜索
保存
歌词
片头字幕
播放器窗口
音乐库窗口
播放表窗口
工具条
最终用户显示容器
播放表
声音控制
元数据控制
元数据显示

图15A

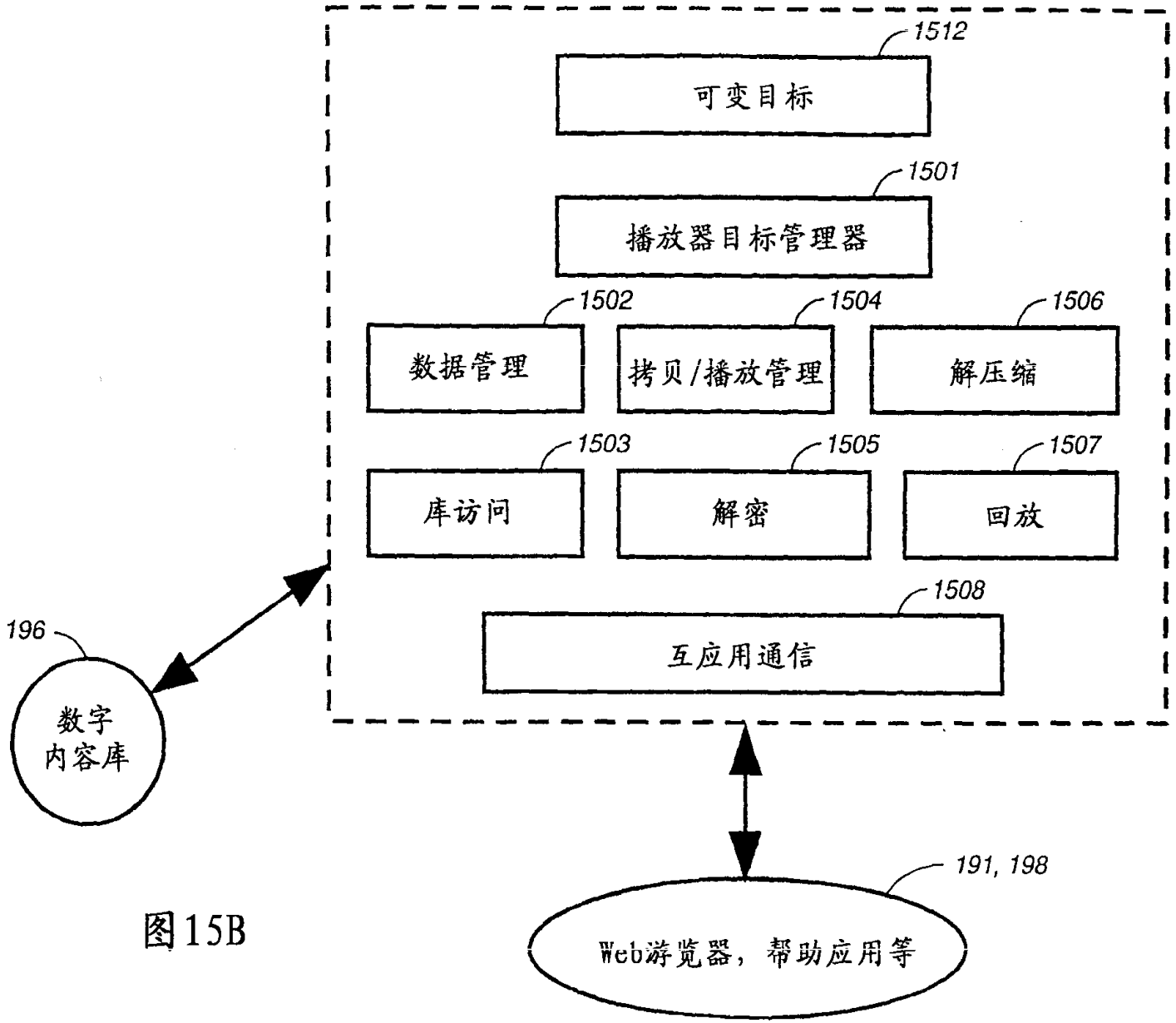

1512
可变目标
1501
播放器目标管理器
1502
数据管理
1504
拷贝/播放管理
1506
解压缩
1503
库访问
1505
解密
1507
回放
1508
互应用通信
196
数字
内容库
191, 198
Web游览器，帮助应用等

图15B

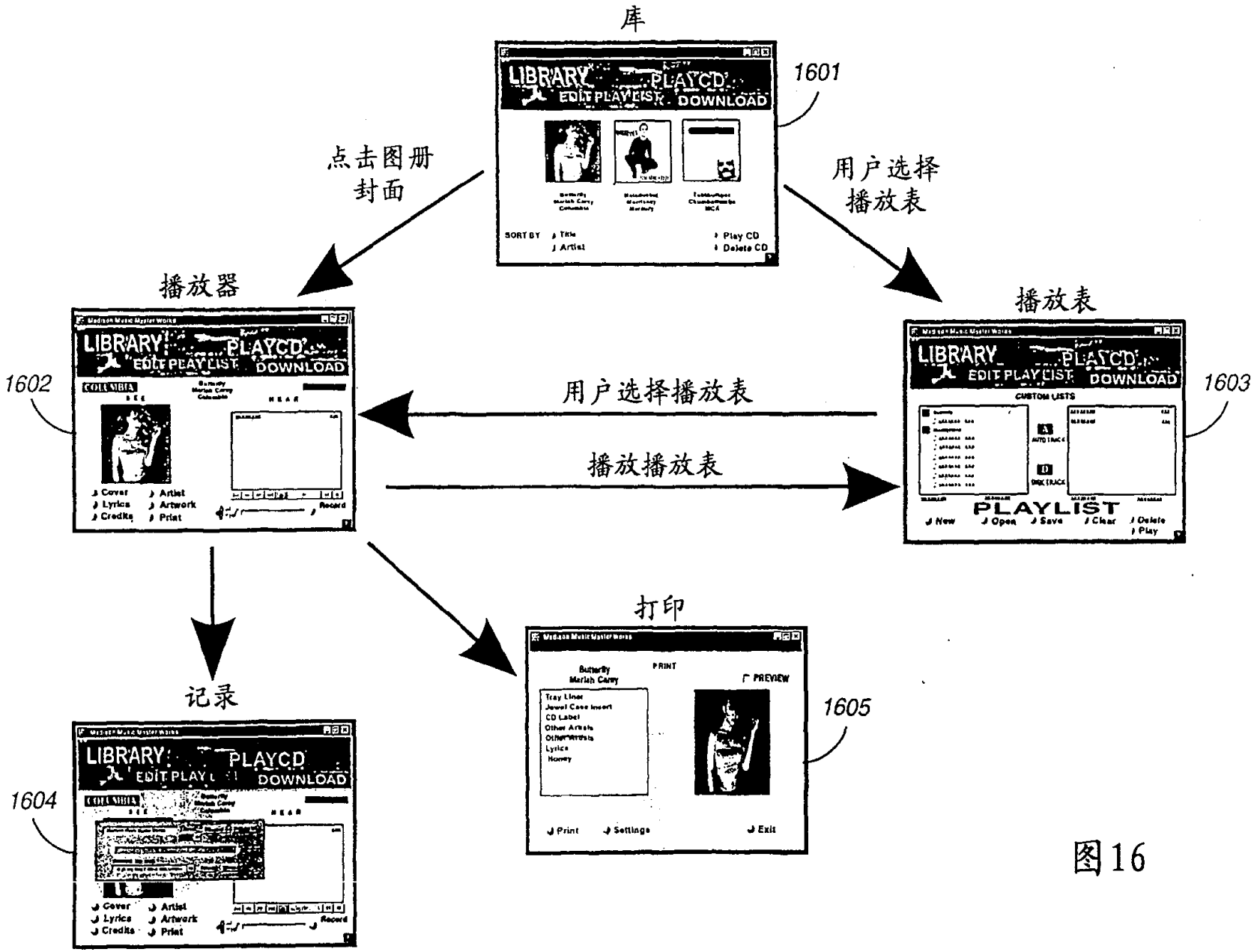

库
1601
LIBRARY
PLAYCD
EDIT PLAYLIST
DOWNLOAD
SORT BY
Title
Artist
Play CD
Delete CD
点击图册
封面
用户选择
播放表
播放器
播放表
1602
1603
用户选择播放表
播放播放表
Cover
Artist
Lyrics
Artwork
Credits
Print
Record
CUSTOM LISTS
PLAYLIST
New
Open
Save
Clear
Delete
Play
记录
打印
1604
1605
PRINT
PREVIEW
Butterfly
Mariah Carey
Tray Liner
Jewel Case Insert
CD Label
Other Artists
Lyrics
Honey
Print
Settings
Exit

图16

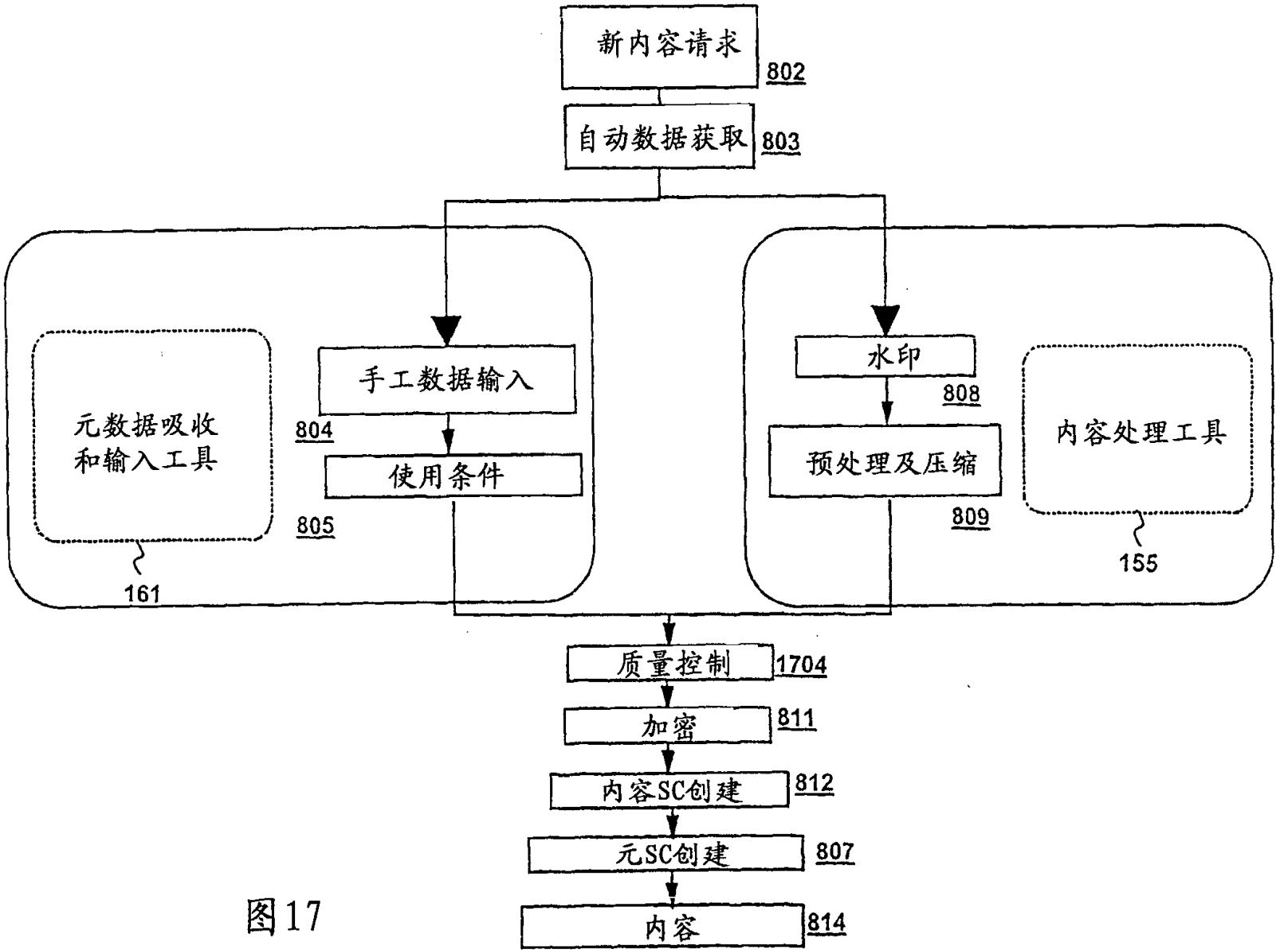

新内容请求
802
自动数据获取
803
元数据吸收
和输入工具
161
手工数据输入
804
使用条件
805
水印
808
预处理及压缩
809
内容处理工具
155
质量控制
1704
加密
811
内容SC创建
812
元SC创建
807
内容
814

图17

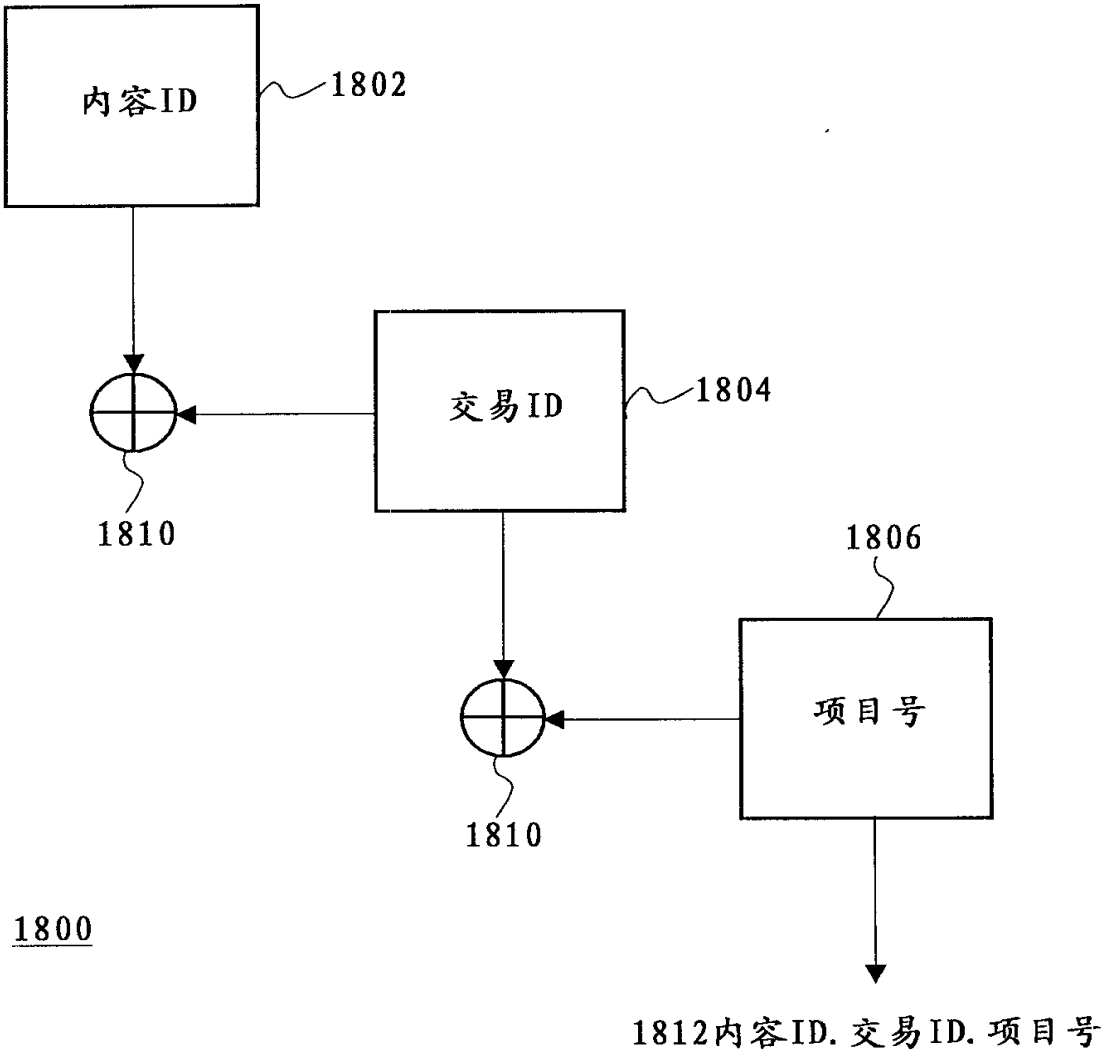

内容ID
1802
交易ID
1804
1810
1806
项目号
1810
1800
1812内容ID. 交易ID. 项目号

图18