[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 9/14
H04L 12/16

[12]发明专利申请公开说明书

[21]申请号 01111470.3

[43]公开日 2001年9月19日

[11]公开号 CN 1313688A

[22]申请日 2001.3.14 [21]申请号 01111470.3

[30]优先权

[32]2000.3.14 [33]JP [31]069697/2000

[71]申请人 索尼公司

地址 日本东京都

[72]发明人 鄉直美 栗原章

[74]专利代理机构 柳沈知识产权律师事务所

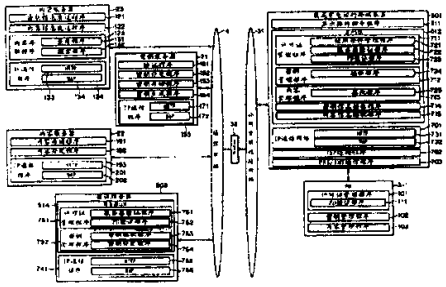
代理人 马 莹

权利要求书4页 说明书20页 附图页数10页

[54]发明名称 信息提供、信息处理的设备和方法以及程序存储介质

[57]摘要

本发明致力于在防止非授权的内容使用的同时，快速下载内容。PD验证 程序验证集成有电话的终端装置。服务器验证程序验证密钥服务器。服务器LCM控制从集成有电话的终端装置接收关于用于识别密钥服务器的数据的请 求和一密钥。服务器LCM以用于识别密钥服务器的数据为基础，发送关于该 密钥的请求给密钥服务器，并从密钥服务器接收所请求的密钥。密钥分发程 序发送该密钥给集成有电话的终端装置。



ISSN1008-4274

权 利 要 求 书

1. 一种信息提供设备，它包括:

第一验证部件，用来验证第一信息处理单元;

第二验证部件，用来验证第二信息处理单元;

接收控制部件，用来控制从所述第一信息处理单元接收关于用于识别所述第二信息处理单元的数据的传输请求和一密钥;

通信控制部件，用来控制通信，以使得将关于以用于识别所述第二信息处理单元的所述数据为基础的所述密钥的传输请求，发送给所述第二信息处理单元，并使得所述密钥从所述第二信息处理单元接收到；以及

传输控制单元，用于控制将所述密钥向所述第一信息处理单元的传输。

2. 根据权利要求 1 的信息提供设备，其中所述第一信息处理单元为便携装置，而所述第二信息处理单元为密钥服务器。

3. 根据权利要求 1 的信息提供设备，其中所述数据和所述密钥适用于构造可用的内容数据。

4. 根据权利要求 1 的信息提供设备，其中所述信息提供设备用作具有密钥管理程序和许可证管理程序的验证服务器。

5. 根据权利要求 4 的信息提供设备，其中所述密钥管理程序和所述许可证管理程序包括在服务器中许可服从模块。

6. 根据权利要求 4 的信息提供设备，其中所述第一信息处理单元为个人计算机，并且如果所述验证服务器不可用，还具有一般来说执行与普通许可服从模块同样的处理的许可服从模块。

7. 根据权利要求 4 的信息提供设备，其中所述许可证管理程序具有一服务器验证程序和一便携装置验证程序。

8. 一种信息提供方法，包括步骤:

验证第一信息处理单元;

验证第二信息处理单元;

控制从所述第一信息处理单元接收关于用于识别所述第二信息处理单元的数据的传输请求和一密钥;

控制通信，以使得将关于以用于识别所述第二信息处理单元的所述数据为基础的所述密钥的传输请求，发送给所述第二信息处理单元，并使得所述

密钥从所述第二信息处理单元接收到；以及

控制将所述密钥向所述第一信息处理单元的传输。

9. 根据权利要求 8 的信息提供方法，其中所述第一信息处理单元为便携装置，而所述第二信息处理单元为密钥服务器。

10. 根据权利要求 8 的信息提供方法，其中所述数据和所述密钥适用于构造可用的内容数据。

11. 根据权利要求 8 的信息提供方法，其中所述信息提供方法有密钥管理程序和许可证管理程序的验证服务器。

12. 根据权利要求 11 的信息提供方法，其中所述密钥管理程序和所述许可证管理程序包括在服务器中许可服从模块。

13. 根据权利要求 11 的信息提供方法，其中所述第一信息处理单元为个人计算机，并且如果所述验证服务器不可用，还具有一般来说执行与普通许可服从模块同样的处理的许可服从模块。

14. 根据权利要求 11 的信息提供方法，其中所述许可证管理程序具有一服务器验证程序和一便携装置验证程序。

15. 一种存储计算机可读程序的程序存储介质，其中的程序包括步骤：

验证第一信息处理单元；

验证第二信息处理单元；

控制从所述第一信息处理单元接收关于用于识别所述第二信息处理单元的数据的传输请求和一密钥；

控制通信，以使得将关于以用于识别所述第二信息处理单元的所述数据为基础的所述密钥的传输请求，发送给所述第二信息处理单元，并使得所述密钥从所述第二信息处理单元接收到；以及

控制将所述密钥向所述第一信息处理单元的传输。

16. 一种信息处理设备，包括：

验证部件，用来验证第一信息提供单元；

传输控制部件，用来控制将关于用于识别提供密钥的第二信息处理单元的数据的传输请求发送到所述第一信息提供单元的传输，以及所述密钥的传输；以及

接收控制部件，用来控制从所述第二信息提供单元提供和发送到所述第一信息提供单元的所述密钥的接收。

17. 根据权利要求 16 的信息处理设备，其中所述第一信息提供单元为验证服务器，而所述第二信息提供单元为密钥服务器。

18. 根据权利要求 16 的信息处理设备，其中所述数据和所述密钥适用于构造可用的内容数据。

19. 根据权利要求 16 的信息处理设备，其中所述第一信息提供单元用作具有密钥管理程序和许可证管理程序的验证服务器。

20. 根据权利要求 19 的信息处理设备，其中所述密钥管理程序和所述许可证管理程序包括在服务器中许可服从模块。

21. 根据权利要求 20 的信息处理设备，其中所述信息处理设备为个人计算机，并且如果所述验证服务器不可用，还具有一般来说执行与普通许可服从模块同样处理的同样的许可服从模块。

22. 根据权利要求 20 的信息处理设备，其中所述信息处理设备构造成一便携装置，并且具有与所述验证服务器的所述服务器许可服从模块协同执行交叉验证的客户许可服从模块。

23. 一种信息处理方法，包括步骤:

验证第一信息提供单元;

控制将关于用于识别提供密钥的第二信息处理单元的数据的传输请求发送到所述第一信息提供单元的传输，以及所述密钥的传输;

控制从所述第二信息提供单元提供和发送到所述第一信息提供单元的所述密钥的接收。

24. 根据权利要求 23 的信息处理方法，其中所述第一信息提供单元为验证服务器，而所述第二信息提供单元为密钥服务器。

25. 根据权利要求 23 的信息处理方法，其中所述数据和所述密钥适用于构造可用的内容数据。

26. 根据权利要求 23 的信息处理方法，其中所述第一信息提供单元用作具有密钥管理程序和许可证管理程序的验证服务器。

27. 根据权利要求 26 的信息处理方法，其中所述密钥管理程序和所述许可证管理程序包括在服务器中许可服从模块。

28. 根据权利要求 27 的信息处理方法，其中所述信息处理设备为个人计算机，并且如果所述验证服务器不可用，还具有一般来说执行与普通许可服从模块同样处理的同样的许可服从模块。

29. 根据权利要求 27 的信息处理方法，其中所述信息处理设备构造成一便携装置，并且具有与所述验证服务器的所述服务器许可服从模块协同执行交叉验证的客户许可服从模块。

30. 一种存储计算机可读程序的程序存储介质，其中的程序包括步骤：

验证第一信息提供单元；

控制将关于用于识别提供密钥的第二信息处理单元的数据的传输请求发送到所述第一信息提供单元的传输，以及所述密钥的传输；

控制从所述第二信息提供单元提供和发送到所述第一信息提供单元的所述密钥的接收。

说　明　书

信息提供、信息处理的设备和方法以及程序存储介质

总的来说，本发明涉及信息提供设备和方法、信息处理设备和方法以及程序存储介质。更具体地说，本发明涉及提供用来解密内容的密钥或使用被加密的内容的信息提供设备和方法、信息处理设备和方法以及程序存储介质。

参考图 1，这里展示了一说明现有技术的数字数据传输系统的一种配置的示意图。个人计算机 1 连接到例如由一局域网或因特网构成的通信网络 4。个人计算机 1 从内容服务器 22 接收或者从一 CD（光盘）读取音乐数据（以后称为内容）、按预定压缩模式（例如 ATRAC3（商标））压缩接收到的数据、按诸如 DES（数据加密标准）这样的预定加密算法将它们加密以及记录作为结果生成的内容。

个人计算机 1 也记录指示被记录的加密的内容的使用条件的使用条件数据。

例如，该使用条件数据指示能够同时使用满足该使用条件的内容的便携装置（也称为 PD）的数量（即能够检出内容的 PD 个数，这将在随后描述）。当一段内容按由该使用条件指定的次数检出时，个人计算机 1 再现这一内容。

个人计算机 1 的显示操作指令程序 11 显示与记录在个人计算机 1 中的内容有关的数据（例如音乐标题或使用条件），并且例如输入一检出指令用以使服从 SDMI（保密数字音乐班权）标准的软件模块 LCM （许可服从模块）12，执行例如相应于该指令的检出操作。

个人计算机 1 的 LCM 12 由一组仅当满足由各个内容的版权持有人指定的使用条件时才控制使用内容的模块构建，从而防止基于未允许第二次使用内容的版权侵犯。该使用条件包括该内容的再现条件、拷贝条件、移动条件以及积聚条件。

LCM 12 验证连接到个人计算机 1 的装置是否是应允的一个，并且执行诸如通过安全的方法移动内容这样的处理。LCM 与该处理一起生成必要的密钥，管理所生成的密钥，并且用该密钥加密该内容，或者控制与所连接的装置的通信。

LCM 12 也检查所装载的便携介质 3 的有效性、添加由服务器 5 指定的使

用条件到内容（加密的）、并将该内容存储在便携介质 3 中。

个人计算机 1 的 LCM 12 将被存储的加密内容和与该内容有关数据（例如音乐标题或使用条件）供给所连接的便携装置 2，从而更新该使用条件（这种更新在以后称为检出（checkout））。更具体地说，当进行检出时，按 1 递减允许的、关于该内容的使用条件的检出次数，该允许的检出次数存储在个人计算机 1 中。当该允许的检出次数为 0 时，不能够检出相关的内容。

便携装置 2 在装入的便携介质 3 中存储从个人计算机 1 供给的内容（即检出的内容）以及与那一内容有关的数据（例如音乐标题或使用条件）。

集成了诸如快闪存储器的存储介质的便携介质 3 构造成可以拆卸地安装在便携装置 2 上。

便携装置 2 以使用条件为基础再现存储在便携介质 3 中的内容，并将被再现的内容输出给例如耳机（未显示）。

例如，如果用户企图在超过作为再现限制而设置的再现次数的前提下，再现存储在便携装置 2 中的某段内容，则便携装置 2 阻止该企图。

用户可以从个人计算机 1 中移出存储内容的便携装置 2 以便带走，并再现存储在便携介质 3 中的内容以便例如通过例如耳机装置聆听所再现的音乐。

当便携装置 2 经由例如 USB 电缆连接到个人计算机 1 时，便携装置 2 和个人计算机 1 相互交叉验证。这种交叉验证是基于询问-应答（challenge-response）模式的。在该询问-应答模式中，对于由个人计算机 1 生成的某一值（或询问），便携装置 2 用利用由个人计算机 1 共享的秘密密钥生成的值（或应答）进行应答。

服务器 5 积聚按预定算法压缩和加密的内容并依据个人计算机 1 的要求分发所积聚的内容。服务器 5 容纳有密钥服务器 21、内容服务器 22 和购货服务器 23。

密钥服务器 21 积聚内容密钥，用来解密从内容服务器 22 供给个人计算机 1 的内容，并且响应个人计算机 1 的请求供给相关的内容密钥给个人计算机 1。在开始内容密钥供给操作之前，密钥服务器 21 和个人计算机 1 相互交叉验证。密钥服务器 21 用由该交叉验证生成的临时密钥加密内容密钥，并发送加密的内容密钥给个人计算机 1。个人计算机 1 用共享的临时密钥解密所收到的内容。

内容服务器 22 按照个人计算机 1 的请求，经由通信网络 4 将所请求的内容（加密的）和其使用条件供给个人计算机 1。

购货服务器 23 提供与将由内容服务器 22 提供的内容有关的数字数据（例如包括有音乐标题和价格组成的内容清单）给个人计算机 1，并且响应来自个人计算机 1 的内容购买请求，给个人计算机 1 供给内容服务器 22 的 URL（同一资源定位符），其中内容服务器 22 供给所请求的内容和密钥服务器 21 的 URL，而密钥服务器 21 供给内容密钥，用来解密所供给的内容。

以下参考图 2 描述现有技术的数字传输系统的性能的结构。除显示操作指令程序 11 和 LCM 12 的之外，个人计算机 1 还执行 IP（因特网协议）通信程序 13、ISP（因特网服务提供商）连接程序 14 和 PHS（个人方便电话系统）/IMT（国际移动无线通信系统）通信程序 15。

PHS/IMT 通信程序 15 适合于将要经由公用交换线路网络 31 执行的通信。ISP 连接程序 14 适合于连接 ISP 32。IP 通信程序 13 包括诸如 HTTP（超文本传输协议）71 和 WAP（无线接入协议）72 这样的协议，并且进行经由通信网络 4 与密钥服务器 21、内容服务器 22 或购货服务器 23 通信。

LCM 12 由许可证管理程序 51、密钥管理程序 52、内容管理程序 53、密钥信息接收程序 54 和内容信息接收程序 55 组成。

许可证管理程序 51 用来依据内容的使用条件管理该内容的使用，它由使用条件管理程序 61、CD 剥离程序（ripping program）62、转换器程序 63 和 PD 验证程序 64 组成。

使用条件管理程序 61 以内容的使用条件为基础控制许可或禁止检出存储在个人计算机 1 中的内容，并且在检出该内容时更新使用条件数据。CD 剥离程序 62 从装入个人计算机 1 中的 CD 读取内容，并且生成相关于所读取的内容的使用条件。

转换器程序 63 转换内容的加密模式或编码模式。PD 验证程序 64 验证装入个人计算机 1 中的便携装置 2。

密钥管理程序 52 验证密钥服务器 21 并从密钥服务器 21 接收内容密钥来管理所收到的、与该内容有关的内容密钥。密钥管理程序 52 由服务器验证程序 65 和接收程序 66 组成。

服务器验证程序 65 按将要描述的方式验证密钥服务器 21。接收程序 66 经由通信网络 4 从密钥服务器 21 接收内容密钥。

内容管理程序 53 经由通信网络 4 从内容服务器 22 接收内容及其使用条件数据，并且记录所收到的内容及其使用条件数据。内容管理程序 53 的接收程序 67 从内容服务器 22 接收该内容及其使用条件数据。

密钥信息接收程序 54 接收密钥服务器 21 的 URL，而密钥服务器 21 从购货服务器 23 供给相关于所要的内容段的内容密钥。内容信息接收程序 55 从购货服务器 23 接收关于用户所请求的内容的内容 ID 以及用来识别供给所请求的内容的内容服务器 22 的 URL。

便携装置 2 执行许可证管理程序 81、密钥管理程序 82 和内容管理程序 83。

许可证管理程序 81 由使用条件管理程序 91、PC 验证程序 92 和 PM 验证程序 93 组成。使用条件管理程序 91 用来以内容的使用条件为基础管理该内容的再现次数。PC 验证程序 92 用来验证个人计算机 1。PM 验证程序 93 用来验证便携介质 3。

密钥管理程序 82 用预先存储在便携介质 3 中的存储密钥加密从个人计算机 1 供给的内容密钥，并且当所加密的内容密钥存储在便携介质 3 时，管理该加密的内容密钥。

当从个人计算机 1 发送来的内容存储在便携介质 3 时，内容密钥管理程序 83 管理该从个人计算机 1 发送来的内容。

便携介质 3 执行许可证管理程序 101、密钥管理程序 102 和内容管理程序 103。

许可证管理程序 101 具有用来验证便携装置 2 的 PD 验证程序 111，并存储该内容的使用条件数据，以控制例如以该使用条件数据为基础的内容的读取。密钥管理程序 102 用预先存储的存储密钥加密从便携装置 2 供给的内容密钥，以管理该加密的内容密钥。内容管理程序 103 存储从便携装置 2 供给的内容以管理所供给的内容。

购货服务器 23 执行密钥信息发送程序 121、内容信息发送程序 122、内容存取程序 123 和 IP 通信程序 124。

密钥信息发送程序 121 经由通信网络 4 给个人计算机 1 发送密钥服务器 21 的 URL，其中密钥服务器 21 供给相关于由个人计算机 1 的用户请求的内容密钥。

内容信息发送程序 122 经由通信网络 4 给个人计算机 1 发送内容服务器

22 的 URL，其中内容服务器 22 供给由个人计算机 1 的用户请求的内容。

浏览器程序 123 由查看程序 131 和搜索程序 132 组成，个人计算机 1 的用户通过查看程序 131 查看和聆听该内容，而通过搜索程序 132 搜索所要的内容段。

IP 通信程序 124 例如包括诸如 HTTP 133 和 WAP 134 这样的协议，经由通信网络 4 与个人计算机 1 通信。

密钥服务器 21 执行验证程序 151、密钥分发程序 152、密钥存储程序 153、密钥生成程序 154 和 IP 通信程序 155。

验证程序 151 例如验证个人计算机 1。密钥分发程序 152 分发存储在密钥存储程序 153 中的内容密钥给所验证的个人计算机 1。密钥存储程序 153 存储由密钥生成程序 154 生成的内容密钥。密钥生成程序 154 生成与特定的内容段相关的内容密钥。

IP 通信程序 155 包括诸如 HTTP 171 和 WAP 172 这样的协议，例如用以经由通信网络 4 与个人计算机 1 通信。

内容服务器 22 执行内容存储程序 191、内容分发程序 192 和 IP 通信程序 193。

内容存储程序 191 存储由与内容 ID 相关的内容密钥加密的内容。内容存储程序 191 按照来自个人计算机 1 的请求给个人计算机 1 分发相应于存储在内容存储程序 191 中的内容 ID 的内容。

IP 通信程序 193 包括诸如 HTTP 201 和 WAP 202 这样的协议，用以经由通信网络 4 与个人计算机 1 通信。

下面参考图 3 和 4 所示的流程图，描述个人计算机 1 下载内容和检出所下载的内容给便携装置 2 的处理。在 S101 步中，个人计算机 1 的 PHS/IMT 通信程序 15 建立与公用交换线路网络 31 的连接。在 S201 步中，例如公用交换线路网络 31 中的地面站（未显示）建立与个人计算机 1 的连接。

在 S102 步中，个人计算机 1 的 ISP 连接程序 14 建立与 ISP 32 的连接。在 S301 步中，ISP 32 建立与个人计算机 1 的连接。

在 S103 步中，个人计算机 1 的 IP 通信程序 13 建立与购货服务器 23 的 IP 通信。在 S401 步中，购货服务器 23 的 IP 通信程序 124 建立与个人计算机 1 的 IP 通信。

在 S402 步中，购货服务器 23 的内容存取程序 123 经由通信网络 4 给个

人计算机 1 发送用来浏览的数字数据（关于选择的内容）。在 S104 步中，个人计算机 1 的浏览器程序（未显示）显示相应于收到的、用来供用户浏览的数字数据的图像或文本。个人计算机 1 的浏览器程序也有能力使得用户能够按数据流再现方式试看下载的内容，并使得购货服务器 23 的内容存取程序 123 能够按关键词搜索特定的内容段，以显示该搜索结果。根据个人计算机 1 的用户请求重复 S402 和 S104 的处理。

在 S105 步中，个人计算机 1 的浏览器程序发送购买请求给购货服务器 23。在 S403 步中，购货服务器 23 的内容存取程序 123 从个人计算机 1 接收该购买请求。

在 S404 步中，购货服务器 23 的内容信息发送程序 122 经由通信网络 4 给个人计算机 1 发送包括内容服务器 22 的 URL 的内容信息，而其中的内容服务器 22 分发在 S403 步中收到的购买请求中指定的内容。在 S106 步中，个人计算机 1 的内容信息接收程序 55 从购货服务器 23 接收内容信息。

在 S405 步中，购货服务器 23 的密钥信息发送程序 121 经由通信网络 4 给个人计算机 1 发送诸如密钥服务器 21 的 URL 这样的密钥信息，而其中的密钥服务器 21 分发在 S403 步中收到的购买请求中指定的内容的内容密钥。在 S107 步中，个人计算机 1 的密钥信息接收程序 54 从购货服务器 23 接收密钥信息。

在 S108 步中，个人计算机 1 的 IP 通信程序 13 利用包括在 S106 步获得的内容信息中的、内容服务器 22 的 URL，建立与内容服务器 22 的 IP 通信。在 S501 步中，内容服务器 22 的 IP 通信程序 193 建立与个人计算机 1 的 IP 连接。

在 S109 步中，个人计算机 1 的内容管理程序 53 经由通信网络 4 发送在 S106 步获得的内容 ID 给内容服务器 22。在 S502 步中，内容服务器 22 从个人计算机 1 接收该内容 ID。在 S503 步中，内容服务器 22 的内容分发程序 192 从内容存储程序 191 中读取相应于在 S502 步收到的内容 ID 的内容（加密的），并经由通信网络 4 将该内容分发给个人计算机 1。在 S110 步中，个人计算机 1 的内容管理程序 53 的接收程序 67 从内容服务器 22 接收该内容。

在 S111 步中，个人计算机 1 的 IP 通信程序 13 以包含在 S107 步中获得的密钥信息中的密钥服务器 21 的 URL 为基础，建立与密钥服务器 21 的 IP 通信。在 S601 步中，密钥服务器 21 的 IP 通信程序 155 建立与个人计算机 1 的

IP 通信。

在 S112 步中，个人计算机 1 的密钥管理程序 52 的服务器验证程序 65 验证密钥服务器 21。在 S602 步中，密钥服务器 21 的验证程序 151 验证个人计算机 1。

密钥服务器 21 预先存储主密钥 KMS，个人计算机 1 预先存储专用密钥 KPP 和个人计算机 1 的 ID。个人计算机也预先存储主密钥 KMP，而且密钥服务器 21 也预先存储其 ID 和专用密钥 KPS。

密钥服务器 21 从个人计算机 1 接收该个人计算机 1 的 ID 并将散列函数用于收到的 ID 和该密钥服务器 21 的主密钥 KMS，以生成与个人计算机 1 的专用密钥 KPP 同样的密钥。

个人计算机 1 从密钥服务器 21 接收密钥服务器 21 的 ID，并将散列函数应用于所接收的 ID 和个人计算机 1 的主密钥 KMP，以生成与密钥服务器 21 的专用密钥 KPS 同样的密钥。因此，该共同专用密钥由个人计算机 1 和密钥服务器 21 共享。利用这些专用密钥生成临时密钥。

在 S113 步中，个人计算机 1 的密钥管理程序 52 发送一内容 ID 给密钥服务器 21。在 S603 步中密钥服务器 21 从个人计算机 1 接收该内容 ID。在 S604 步中，密钥服务器 21 的密钥分发程序 152 读取存储在密钥存储程序 153 中、与该内容 ID 相关的内容密钥，并将该内容密钥（由临时密钥加密过的）发送给个人计算机 1。在 S114 步中，个人计算机 1 的密钥管理程序 52 的接收程序 66 从密钥服务器 21 接收该内容密钥。密钥管理程序 52 用临时密钥解密收到的内容密钥。

当个人计算机 1 的用户指令显示操作指令程序 11 检出收到的内容时，执行 S115 步的处理和其后续处理。

在 S115 步中，个人计算机 1 的许可证管理程序 51 的 PD 验证程序 64 验证便携装置 2。在 S701 步中，便携装置 2 的许可证管理程序 81 的 PC 验证程序 92 验证个人计算机 1。

在 S115 和 S701 步中的个人计算机 1 和便携装置 2 之间的交叉验证处理是基于询问-应答模式的。与 S112 和 S602 步中的密钥服务器 21 和个人计算机 1 之间的交叉验证相比，询问-应答模式要求更少的计算负担。个人计算机 1 和便携装置 2 都以同样的计算操作从应答中生成一临时密钥，并共享所生成的临时密钥。

在 S116 步中，个人计算机 1 的内容管理程序 53 分发加密的内容给便携装置 2。在 S702 步中，便携装置 2 的内容管理程序 83 从个人计算机 1 接收该内容，并将所收到的内容提供给便携介质 3 的内容管理程序 103。便携介质 3 的内容管理程序 103 存储所收到的内容。

应该注意到，当便携介质 3 装载在便携装置 2 时，便携装置 2 和便携介质 3 相互交叉验证。

在 S117 步中，个人计算机 1 的密钥管理程序 52 分发相应于在 S166 步分发的内容的内容密钥（用在便携装置 2 和便携介质 3 之间共享的临时密钥加密过的）给便携装置 2。在 S703 步中，便携装置 2 的密钥管理程序 82 从个人计算机 1 中接收该内容密钥，并将所收到的内容密钥提供给便携介质 3 的密钥管理程序 102。便携介质 3 的密钥管理程序 102 解密所接收的内容密钥并存储被解密的内容密钥。

如上所述，现有技术在计算能力和存储容量方面比个人计算机 1 小。例如，如果便携终端装置试图从内容服务器 22 下载内容，以及从密钥服务器 21 中下载相应的内容密钥，则大量的验证负担降低了处理速度，以至于不足以在实际应用中实现。

因此本发明的目的是提供在防止任何非授权的内容使用的同时，即使以受限制的处理能力，也适合于实际应用的快速内容下载能力。

在实施本发明中以及根据其一方面，提供一种信息提供设备，它包括：第一验证部件，用来验证第一信息处理单元；第二验证部件，用来验证第二信息处理单元；接收控制部件，用来控制从第一信息处理单元接收关于用于识别该第二信息处理单元的数据的传输请求和一密钥；通信控制部件，用来控制该通信，以使得将关于以用于识别该第二信息处理单元的数据为基础的密钥的传输请求，发送给该第二信息处理单元，并使得该密钥从该第二信息处理单元接收到；以及传输控制部件，用于控制将该密钥向第一信息处理单元的传输。

在实施本发明中以及根据其另一方面，提供一种信息提供方法，它包括步骤：验证第一信息处理单元；验证第二信息处理单元；控制从第一信息处理单元接收关于用于识别该第二信息处理单元的数据的传输请求和一密钥；控制该通信，以使得将关于以用于识别该第二信息处理单元的数据为基础的密钥的传输请求，发送给该第二信息处理单元，并使得该密钥从该第二信息

处理单元接收到；控制将该密钥向第一信息处理单元的传输。

在实施本发明中以及根据其另一方面，提供一种存储计算机可读程序的程序存储介质，其中的程序包括步骤：验证第一信息处理单元；验证第二信息处理单元；控制从第一信息处理单元接收关于用于识别该第二信息处理单元的数据的传输请求和一密钥；控制该通信，以使得将关于以用于识别该第二信息处理单元的数据为基础的密钥的传输请求，发送给该第二信息处理单元，并使得该密钥从该第二信息处理单元接收到；控制将该密钥向第一信息处理单元的传输。

在实施本发明中以及根据其另一方面，提供一种信息处理设备，它包括：验证部件，用来验证第一信息提供单元；传输控制部件，用来控制将关于用于识别提供密钥的第二信息处理单元的数据的传输请求发送到第一信息提供单元的传输，以及该密钥的传输；以及接收控制部件，用来控制从第二信息提供单元提供和发送到第一信息提供单元的密钥的接收。

在实施本发明中以及根据其不同方面，提供一种信息处理方法，它包括步骤：验证第一信息提供单元；控制将关于用于识别提供密钥的第二信息处理单元的数据的传输请求发送到第一信息提供单元的传输，以及该密钥的传输；控制从第二信息提供单元提供和发送到第一信息提供单元的密钥的接收。

在实施本发明中以及根据其不同方面，提供一种存储计算机可读程序的程序存储介质，其中的程序包括步骤：验证第一信息提供单元；控制将关于用于识别提供密钥的第二信息处理单元的数据的传输请求发送到第一信息提供单元的传输，以及该密钥的传输；控制从第二信息提供单元提供和发送到第一信息提供单元的密钥的接收。

在叙述于权利要求 1 的信息提供设备、叙述在权利要求 8 中的信息提供方法以及叙述在权利要求 15 中的程序存储介质中，验证第一信息处理单元；验证第二信息处理单元；控制从第一信息处理单元接收关于用于识别该第二信息处理单元的数据的传输请求和密钥；以用于识别该第二信息处理单元的数据为基础，发送关于密钥的传输请求给该第二信息处理单元；控制从该第二信息处理单元接收密钥；以及控制向第一信息处理单元发送该密钥。

在叙述于权利要求 16 的信息处理设备、叙述在权利要求 23 的信息处理方法以及叙述在权利要求 30 的程序存储介质中，验证第一信息提供单元；控制将关于用于识别提供密钥的第二信息处理单元的数据的传输请求发送到第

一信息提供单元的传输，以及该密钥的传输；从第二信息提供单元向第一信息提供单元提供密钥；以及控制所提供的密钥的接收。

通过参考展示本发明的优选实施例的附图，以及对下列描述和附录的权利要求研究，本发明的上述和其它目的、特征和优点以及实现它们的方式会更加明显，本发明本身也会得到最好的理解。

参照结合附图的描述，可以看出本发明的这些和其它目的，其中：

图 1 为说明常规的数字数据传输系统的结构示意图；

图 2 为说明常规的数字数据传输系统的功能结构示意图；

图 3 为描述个人计算机从服务器下载内容并将下载的内容检出到便携装置的处理流程图；

图 4 为描述个人计算机从服务器下载内容并将下载的内容检出到便携装置的处理流程图；

图 5 为说明结合本发明的数字数据传输系统一个实施例的结构示意图；

图 6 为说明集成有电话的终端装置的结构方框图；

图 7 为说明验证服务器的结构方框图；

图 8 为说明结合本发明的数字数据传输系统的功能结构示意图；

图 9 为描述集成有电话的终端装置下载内容的处理流程图；和

图 10 为描述集成有电话的终端装置下载内容的处理流程图。

结合附图，通过示例的方法将进一步详细描述本发明。

参照图 5，示出结合本发明的数字数据传输系统的一个实施例。在参照图 5 时，那些与前面在图 1 中描述的组件相同的组件采用相同的标号，并略去对它们的描述。

集成有电话的终端装置 501 以适应与便携介质 3-1 可分离的方式构建，并以无线方式与通信网络 4 相连接。集成有电话的终端装置 501 通过通信网络 4 下载从内容服务器 22 接收的内容（以预定模式压缩并加密），并将下载的内容与诸如该内容的使用条件之类的数据一起存储到装入的便携介质 3-1。

基于与内容相关的使用条件，集成有电话的终端装置 501 再现存储在便携介质 3-1 中的内容并将再现内容输出到未示出的耳机或扬声器。携带集成有电话的终端装置 501，其用户就可以在任何期望的地方下载任何期望的内容，以将下载的内容存储到便携介质 3-1。用户使集成有电话的终端装置 501 再现存储在便携介质 3-1 中的内容，以通过例如耳机的装置来欣赏例如与内

容相关的音乐。

集成有电话的终端装置 501 的显示操作指令程序 511 显示与数据相关的内容（比如，音乐标题或使用条件），并且当用户输入下载指令时，使客户 LCM 512 执行相应的处理。集成有电话的终端装置 501 的客户 LCM 512 与验证服务器 503 的服务器 LCM 514 合作，执行下载例如内容及其使用条件的处理序列。

为了防止由于未允许第二次使用内容引起的版权侵犯，集成有电话的终端装置 501 的客户 LCM 512 由一组仅当满足由各个内容的版权持有人指定的使用条件时才控制使用内容的模块构建，从而防止基于未允许第二次使用内容的版权侵犯。该使用条件包括该内容的再现条件、拷贝条件、移动条件以及积聚条件。

客户 LCM 512 验证装入到集成有电话的终端装置 501 的便携介质 3-1 是否是允许的一个，并将服务器 5 规定的使用条件数据以安全的方式添加到内容上（加密），以及将该内容存储到便携介质 3-1。与内容移动一起，客户 LCM 512 生成所需的密钥、管理该密钥并控制与连接的便携介质 3-1 的通信。

个人计算机 502 连接到通信网络 4。个人计算机 502 将从内容服务器 22 接收或者从一 CD 读取的内容的压缩模式和加密模式转换为诸如 DES 之类的预定的压缩模式和预定的加密模式，存储所生成的内容。个人计算机 502 记录所记录的加密内容的使用条件的数据。

个人计算机 502 的显示操作指令程序 11 显示与内容有关的数据（例如音乐标题或使用条件），并且当用户输入下载指令或检出指令时，使个人计算机 502 的 LCM 513 执行相应的下载操作或检出操作。

个人计算机 502 的 LCM 513 由一组仅当满足由各个内容的版权持有人指定的使用条件时才控制使用内容的模块构建，从而防止基于未应允的第二次使用该内容的版权侵害。该使用条件包括该内容的再现条件、拷贝条件、移动条件以及积聚条件。

LCM 513 验证连接到个人计算机 502 的便携装置 2 是否是允许的一个，并且以安全的方法执行比如内容移动处理。与内容移动一起，LCM 513 生成所需的密钥、管理该密钥并加密内容或控制与连接的装置通信。

LCM 513 还检验便携装置 2 的合法性。当装入便携介质 3-2 时，便携装置 2 检验便携介质 3-2 的合法性。如果发现便携装置 2 和便携介质 3-2 合法，

则 LCM 513 将服务器 5 规定的使用条件添加到内容上（加密），并将作为结果的内容检出到便携介质 3-2。便携装置 2 将从个人计算机 502 检出的内容与和内容有关的数据一起存储到装入的便携介质 3-2。

如果验证服务器 503 可用，则个人计算机 502 的 PC LCM 521（按照 LCM 513 的部分或全部功能构建）与验证服务器 503 的服务器 LCM 514 合作，执行下载内容及其使用条件的顺序处理。

如果验证服务器 503 不可用，则个人计算机 502 的 LCM 513 象 LCM 12 那样验证密钥服务器 21，以下载内容及其使用条件。

验证服务器 503 经由执行服务器 LCM 514 验证密钥服务器 21，响应交叉验证的集成有电话的终端装置 501 或交叉验证的个人计算机 502 的请求。在交叉验证密钥服务器 21 之后，验证服务器 503 从密钥服务器 21 接收内容密钥，并将接收到的内容密钥提供给集成有电话的终端装置 501 或个人计算机 502。

集成有电话的终端装置 501 或个人计算机 502 不需要密钥服务器 21 验证，并且可以只经由用验证服务器 503 执行验证来获得相应的内容密钥，而用验证服务器 503 的验证的处理负担低于以密钥服务器 21 的验证。

图 6 示出集成有电话的终端装置 501 的结构。CPU（中央处理单元）601 执行存储在 ROM（只读存储器）602 或 RAM（随机存取存储器）603 中的程序。由 EEPROM（电可擦除只读程序存储器）或快闪存储器构成的 ROM 602 通常存储由 CPU 601 使用的程序和计算参数的主要固定值。比如由 SRAM（静态随机存取存储器）构成的 RAM 603 存储由 CPU 601 在执行中将要使用的程序和在执行中时时改变的参数。

由输入键或麦克风构成的输入块 605 由用户操作，向 CPU 601 输入命令或输入话音。由液晶显示器件构成的显示块 606 以文字或图像的形式显示各种信息。

音频再现块 607 再现通信块 608 提供的另一方的话音数据或经由接口 609 从便携介质 3-1 提供的内容，并发出再现话音信号的声音。

通信块 608 连接到公用交换线路网络 31，并将 CPU 601 提供的数据（比如，内容传输请求）或从输入块 605 提供的用户话音数据存储在预定信息包中，以及将该信息包经由公用交换线路网络 31 发送。同时，通信块 608 将存储在收到的信息包中的数据（比如内容）或经由公用交换线路网络 31 收到的

另一方的话音数据输出给 CPU 601、RAM 603、音频再现块 607 或接口 609。

接口 609 将 CPU 601、RAM 603 或通信块 608 提供的数据存储到便携介质 3-1，以及从装入的便携介质 3-1 中读出诸如内容之类的数据，并将该数据提供给 CPU 601、RAM 603 或音频再现块 607。

接口 610 连接到外部附加的驱动器 631。驱动器 631 从装入到驱动器 631 中的磁盘 641、光盘（包括 CD-ROM）642、磁光盘 643 或半导体存储器 644 读取数据或程序，并将这些数据或程序经由接口 610 和总线 604 提供给 ROM 602 或 RAM 603。

从 CPU 601 到接口 610 的所有组件经由总线 604 相互连接。

图 7 示出验证服务器 503 的内部结构。CPU 651 运行各种应用程序（随后将详细描述）和 OS（操作系统）。ROM 652 通常存储由 CPU 651 使用的程序和计算参数的主要固定值。RAM 653 存储由 CPU 651 在执行中将要使用的程序和在执行中时时改变的参数。这些经由比如由 CPU 总线构成的主总线 654 相互连接。

主总线 654 经由桥接器 655 连接到诸如 PCI（周边元件互连/接口）总线之类的外部总线 656 上。

当向 CPU 651 输入命令时，由用户经由键盘 658 操作。当在显示监视器 660 上指示一点或选择项目时，由用户经由点击装置 659 操作。由液晶显示器件或 CRT（阴极射线管）构成的显示监视器 660 以文字或图像形式显示各种信息。HDD（硬盘驱动器）661 驱动硬盘，将由 CPU 651 要使用的程序或信息记录到硬盘或从硬盘读出。

驱动器 662 从装入到驱动器 662 中的磁盘 681、光盘 682、磁光盘 683 或半导体存储器 684 读取存储的数据或程序，并将这些数据或程序经由接口 657、外部总线 656、桥接器 655 和主总线 654 提供给 RAM 653。

从键盘 658 到驱动器 662 的这些组件连接到接口 657，接口 657 经由外部总线 656、桥接器 655 和主总线 654 连接到 CPU 651。

连接到通信网络 4 的通信块 663 将 CPU 651 或 HDD 661 提供的数据（比如，内容密钥）存储到预定信息包中，并将它们在通信网络 4 上发送。同时，通信块 663 将存储在收到的信息包中的数据（比如，内容 ID）在通信网络 4 上输出给 CPU 651、RAM 653 或 HDD 661。

通信块 663 经由外部总线 656、桥接器 655 和主总线 654 连接到 CPU 651。

下面参照图 8 描述结合本发明的数字数据传输系统的功能结构。在参照图 8 时，那些与前面在图 2 中描述的组件相同的组件采用相同的标号，并略去对它们的描述。

集成有电话的终端装置 501 运行显示操作指令程序 511、客户 LCM 512、IP 通信程序 701、ISP 连接程序 702 和 PHS/IMT 通信程序 703。

PHS/IMT 通信程序 703 经由公共交换线路网络 31 进行通信。ISP 连接程序与 ISP 32 进行连接。IP 通信程序 701 包括诸如 HTTP 731 和 WAP 732 的协议，并经由通信网络 4 与密钥服务器 21、内容服务器 22、购货服务器 23、或验证服务器 503 进行通信。

客户 LCM 512 由许可证管理程序 711、密钥管理程序 712、内容管理程序 713、密钥信息接收程序 714 和内容信息接收程序 715 组成。

许可证管理程序 711 基于内容使用条件管理内容的使用，并且由使用条件管理程序 721、服务器验证程序 722 和 PM 验证程序 723 组成。

使用条件管理程序 721 控制存储在便携介质 3-1 上的内容再现的允许或禁止，并且当再现存储在便携介质 3-1 中的内容时，使得便携介质 3-1 更新存储在便携介质 3-1 上的使用条件数据。服务器验证程序 722 经由通信网络 4 验证验证服务器 503。当便携介质 3-1 装入到集成有电话的终端装置 501 时，PM 验证程序 723 验证便携介质 3-1。

密钥管理程序 712 从验证服务器 503 接收内容密钥，并通过将其存储到与相应内容相关的便携介质 3-1 中管理该内容密钥。密钥管理程序 712 包括用于从验证服务器 503 接收内容密钥的接收程序 724。

内容管理程序 713 从内容服务器 22 接收内容（加密的）及其使用条件，并将接收到的内容及其使用条件存储到便携介质 3-1。内容管理程序 713 的接收程序 725 从内容服务器 22 接收内容及其使用条件。

密钥信息接收程序 714 从购货服务器 23 接收识别用于提供相应内容的内容密钥的密钥服务器 21 的 URL。内容信息接收程序 715 从购货服务器 23 接收识别用于提供期望内容的内容服务器 22 的 URL 以及用于识别内容的内容 ID。

验证服务器 503 运行服务器 LCM 514 和 IP 通信程序 741。

服务器 LCM 514 包括许可证管理程序 751 和密钥管理程序 752。

许可证管理程序 751 包括用于验证密钥服务器 21 的服务器验证程序 761

和用于验证集成有电话的终端装置 501 的 PD 验证程序 762。

密钥管理程序 752 包括密钥接收程序 763，用于经由通信网络 4 从密钥服务器 21 接收内容密钥；和密钥分发程序 764，用于经由通信网络 4 将接收到的内容密钥分发给集成有电话的终端装置 501。

IP 通信程序 741 包括 HTTP 765 和 WAP 766 的协议，并经由通信网络 4 与密钥服务器 21 或集成有电话的终端装置 501 通信。

下面参照图 9 和 10 所示的流程描述集成有电话的终端装置 501 下载内容的处理过程。在步骤 S1001，集成有电话的终端装置 501 的 PHS/IMT 通信程序 703 建立与公共交换线路网络 31 的通信。在步骤 S1101，比如未示出的公共交换线路网络 31 的地面站与集成有电话的终端装置 501 建立连接。

在步骤 S1002，经由集成有电话的终端装置 501 和公共交换线路网络 31 之间的连接，集成有电话的终端装置 501 的 ISP 连接程序 702 建立与 ISP 32 的连接。在步骤 S1201，经由集成有电话的终端装置 501 和公共交换线路网络 31 之间的连接，ISP 32 建立与集成有电话的终端装置 501 的连接。

经由集成有电话的终端装置 501 和 ISP 32 之间的连接，运行集成有电话的终端装置 501 与密钥服务器 21、内容服务器 22、购货服务器 23 或验证服务器 503 之间的顺序处理过程。

在步骤 S1003，集成有电话的终端装置 501 的 IP 通信程序 701 建立与购货服务器 23 的 IP 通信。在步骤 S1301，购货服务器 23 的 IP 通信程序 124 建立与购货服务器 23 的 IP 通信。

在步骤 S1302，购货服务器 23 的内容存取程序 123 经由通信网络 4 向集成有电话的终端装置 501 发送用于查看（或用于内容选择）的数字数据。在步骤 S1004，未示出的集成有电话的终端装置 501 的浏览器程序在用于用户查看的显示块 606 上显示相应于收到的数字数据的文字或图像。集成有电话的终端装置 501 的浏览器程序同时还使得音频再现块 607 以数据流再现的方式再现由用户试听的内容，或使得购货服务器 23 的内容存取程序 123 基于用户输入的关键字搜索期望的内容，并在显示块 606 上显示结果。

重复步骤 S1302 和 S1004 用于集成有电话的终端装置 501 的用户请求的处理过程，一直到比如用户决定购买内容为止。

在步骤 S1005，集成有电话的终端装置 501 的浏览器程序经由通信网络 4 向购货服务器 23 发送购买请求。在步骤 S1303，购货服务器 23 的内容存取

程序 123 接收从集成有电话的终端装置 501 发送的购买请求。

在步骤 S1304，响应在步骤 S1303 中收到的购买定单，购货服务器 23 的内容信息发送程序 122 经由通信网络 4 给集成有电话的终端装置 501 发送内容信息，这些内容信息包括用于分发内容的内容服务器 22 的 URL 和用于识别内容的内容 ID。在步骤 S1006，集成有电话的终端装置 501 的内容信息接收程序 715 接收来自购货服务器 23 的内容信息。

在步骤 S1305，购货服务器 23 的密钥信息发送程序经由通信网络 4 给集成有电话的终端装置 501 发送密钥信息，比如分发在步骤 S1303 中收到的购买请求中规定内容的内容密钥的密钥服务器 21 的 URL。在步骤 S1007 中，集成有电话的终端装置 501 的密钥信息接收程序 714 接收购货服务器 23 发送的密钥信息。

在步骤 S1008，集成有电话的终端装置 501 的 IP 通信程序 701 基于包含在 S1006 步中获得的内容信息中的内容服务器 22 的 URL 建立与内容服务器 22 的 IP 通信。在步骤 S1401，内容服务器 22 的 IP 通信程序 193 建立与集成有电话的终端装置 501 的 IP 通信。

在步骤 S1009，集成有电话的终端装置 501 的内容管理程序 713 经由通信网络 4 将 S1006 步获得的内容 ID 发送到内容服务器 22。在步骤 S1402，内容服务器 22 接收从集成有电话的终端装置 501 发送的内容 ID。在 S1403 步中，内容服务器 22 的内容分发程序 192 从内容存储程序 191 读取相应于 S1402 步中收到的内容 ID 的内容（加密的），并经由通信网络 4 分发给集成有电话的终端装置 501。

在步骤 S1010，集成有电话的终端装置 501 的内容管理程序 713 的接收程序 725 接收从内容服务器 22 发送来的内容。内容管理程序 713 通过接口 609 将所收到的内容供给便携介质 3-1，并使内容管理程序 103 存储该内容。

在步骤 S1011，集成有电话的终端装置 501 的 IP 通信程序 701 基于 S1007 步中获得的、密钥服务器 21 的 URL，建立与验证服务器 503 的 IP 通信。在 S1501 步中，验证服务器 503 的 IP 通信程序 741 建立与集成有电话的终端装置 501 的 IP 通信。

在步骤 S1012，集成有电话的终端装置 501 的许可证管理程序 711 的服务器验证程序 722 验证验证服务器 503。在步骤 S1502，验证服务器 503 的许可证管理程序 751 的 PD 验证程序 762 验证集成有电话的终端装置 501。

在步骤 S1012 和步骤 S1502，按询问-应答模式执行集成有电话的终端装置 501 和验证服务器 503 之间的交叉验证处理。与在步骤 S112 和 S602 中密钥服务器 21 和个人计算机 1 之间的交叉验证处理相比，该询问-应答模式需要更少的计算负担，因此在较少的计算能力和存储容量下提供快速执行。集成有电话的终端装置 501 和验证服务器 503 都从该应答用同一计算操作生成一临时密钥，并共享所生成的临时密钥。

如果在步骤 S1012 和步骤 S1502 中的交叉验证失败（即发现该交叉验证的对方不合法），则终止用集成有电话的终端装置 501 下载内容的处理，而不下载内容。

在步骤 S1013，集成有电话的终端装置 501 的密钥管理程序 712 发送该内容 ID 给验证服务器 503。在步骤 S1503 中， 验证服务器 503 接收从集成有电话的终端装置 501 供给的内容 ID。在步骤 S1014，集成有电话的终端装置 501 的密钥管理程序 712 发送在步骤 S1007 中收到的密钥信息给验证服务器 503。在步骤 S1504 中，验证服务器 503 接收从集成有电话的终端装置 501 供给的密钥信息。

在步骤 S1505，验证服务器 503 的 IP 通信程序 741 建立与密钥服务器 21 的 IP 通信。在步骤 S1601，密钥服务器 21 的 IP 通信程序 155 建立与验证服务器 503 的 IP 通信。

在步骤 S1016，验证服务器 503 的许可证管理程序 751 的服务器验证程序 761 验证密钥服务器 21。在步骤 S1602，密钥服务器 21 的验证程序 151 验证验证服务器 503。

例如，密钥服务器 21 预先存储主密钥 KMSS，而验证服务器 503 事先存储专用密钥 KPCC 和验证服务器 503 的 ID。此外，验证服务器 503 预先存储主密钥 KMCC，而密钥服务器 21 存储密钥服务器 21 的 ID 和专用密钥 KPSS。

密钥服务器 21 接收验证服务器 503 的 ID，并将散列函数应用于收到的 ID 和密钥服务器 21 的主密钥 KMSS，以生成与验证服务器 503 的专用密钥 KPCC 一样的密钥。

验证服务器 503 接收密钥服务器 21 的 ID，并将散列函数应用于收到的 ID 和验证服务器 503 的主密钥 KMCC，以生成与密钥服务器 21 的专用密钥 KPSS 一样的密钥。因此，该共同的密钥在验证服务器 503 和密钥服务器 21 之间共享。利用这些专用密钥生成一临时密钥。

如果在步骤 S1506 和步骤 S1602 中的验证失败（即如果发现该验证的对方不合法），则终止用集成有电话的终端装置 501 进行的内容下载处理，而不下载指定的内容，使得集成有电话的终端装置 501 不能使用该内容。

在步骤 S1507，验证服务器 503 的密钥管理程序 752 将在步骤 S1503 中获得的内容 ID 发送给密钥服务器 21。在步骤 S1603，密钥服务器 21 接收验证服务器 503 提供的内容 ID。在步骤 S1604，密钥服务器 21 的密钥分发程序 152 读取存储在密钥存储程序 153 中、与内容 ID 相关的内容密钥，并将该内容密钥（由在密钥服务器 21 和验证服务器 503 之间共享的临时密钥加密）发送给验证服务器 503。在步骤 S1508，验证服务器 503 的密钥管理程序 752 的密钥接收程序 763 接收密钥服务器 21 发送的内容密钥。

在步骤 S1509，验证服务器 503 的密钥管理程序 752 的密钥分发程序 764 通过在密钥服务器 21 和验证服务器 503 之间共享的临时密钥解密在步骤 S1508 中收到的内容密钥，然后通过在集成有电话的终端装置 501 和验证服务器 503 之间共享的临时密钥加密内容密钥，将作为结果的内容密钥在通信网络 4 上发送给集成有电话的终端装置 501。在步骤 S1015，集成有电话的终端装置 501 的密钥管理程序 712 的接收程序 724 接收验证服务器 503 发送的内容密钥。密钥管理程序 712 通过在集成有电话的终端装置 501 和验证服务器 503 之间共享的临时密钥解密收到的内容密钥，并将解密的内容密钥提供给便携介质 3 的密钥管理程序 102，在密钥管理程序 102 中存储内容密钥。

在步骤 S1012 和 S1502 进行的、在集成有电话的终端装置 501 和验证服务器 503 之间的交叉验证需要比在集成有电话的终端装置 501 和密钥服务器 21 之间的交叉验证更少的计算量，而不要求高计算性能和大存储量。因此，即使以受到限制的处理能力，集成有电话的终端装置 501 也可以通过该交叉验证，在防止任何非授权内容的使用的同时，快速地下载使用的内容。

此外，集成有电话的终端装置 501 可以在内容下载后马上将其存储到便携介质 3。因此，用户不需命令集成有电话的终端装置 501 做象内容检出这样的操作，从而能够毫不费时和费力就能使用该内容。

此外，服务器 LCM 514 可以由验证服务器 503 的管理员集中而迅速地更新（例如版本更新）。而且客户 LCM 512 比现有技术的 LCM 12（例如服务器验证程序 722 的规模可以做得比现有技术的服务器验证程序 65 小）容量要小。因此，集成有电话的终端装置 501 可以明显快速地更新客户 LCM 512。

应该指出的是，当验证服务器503可用时，个人计算机502的PC LCM 521可以执行与集成有电话的终端装置501的客户LCM 512相同的处理。如果验证服务器503不可用，则个人计算机502的LCM 513可以执行与现有技术的LCM 12相同的处理。

在上面的描述中，将内容描述为音乐数据。但是本领域的技术人员非常清楚，内容也可以为静止图像数据、活动图像数据、文本数据或程序。

在上面的描述中，集成有电话的终端装置501或个人计算机502下载内容。但是本领域的技术人员非常清楚，除了集成有电话的终端装置501和个人计算机502之外，移动电话、PDA（个人数字助理）、具有通信和图像处理能力的数字盒式录像机、具有通信能力的电子记事本或便携个人计算机也可以下载内容。

在上面的描述中，集成有电话的终端装置501借助PHS或IMT进行必需的通信。但是本领域的技术人员非常清楚，作为选择，集成有电话的终端装置501也可以借助W-CDMA（码分多址）、卫星通信、卫星广播、PSTN（公共交换电话网）、xDSL（x数字用户线路）、ISDN（集成服务数字网络）或专用网络等进行通信。

上述的处理过程序列可以经由硬件或软件执行。经由软件执行由事先在专用硬盘设备中安装了构成该软件的程序的计算机或从程序存储介质中安装了这些程序的能够执行各种任务的通用个人计算机支持。

用于存储计算机可读和可执行程序的程序存储介质可以是由如图8或图9所示的磁盘641或681（包括软盘）、光盘642或682（包括CD-ROM（只读光盘）和DVD（数字通用盘））、磁光盘643或683（包括MD（小型盘））、半导体存储器RAM 644或684或ROM 602或652、或HDD661构成的在其上临时或永久存储程序的信息包介质。程序从诸如局域网、因特网及数字卫星广播之类的有线或无线通信媒体经由所必需的通信块608或663存储在程序存储介质中。

应该指出的是，描述存储在程序存储介质中的程序的步骤不仅可以按所述顺序的时间先后的方式执行，而且可以以并行或不连续的方式执行。

还应该指出的是，这里所使用的系统表示整个由多个组件单元构成的设备。

在叙述于权利要求1的信息提供设备、叙述在权利要求8中的信息提供

方法以及叙述在权利要求 15 中的程序存储介质中，验证第一信息处理单元；验证第二信息处理单元；控制从第一信息处理单元接收关于用于识别该第二信息处理单元的数据的传输请求和密钥；以用于识别该第二信息处理单元的数据为基础，发送关于密钥的传输请求给该第二信息处理单元；控制从该第二信息处理单元接收密钥；以及控制向第一信息处理单元发送该密钥。因此，即使处理能力受到限制，第一信息处理单元也可以在防止任何非授权内容使用的同时，快速下载使用的内容。

在叙述于权利要求 16 的信息处理设备、叙述在权利要求 23 的信息处理方法以及叙述在权利要求 30 的程序存储介质中，验证第一信息提供单元；控制将关于用于识别提供密钥的第二信息处理单元的数据的传输请求发送到第一信息提供单元的传输，以及该密钥的传输；从第二信息提供单元向第一信息提供单元提供密钥；以及控制所提供的密钥的接收。因此，即使处理能力受到限制，系统也可以在防止非授权使用的同时，快速下载内容。

尽管使用特定条件描述了本发明的优选实施例，但是此描述仅用于说明的目的，并且应该理解在不脱离所附权利要求的构思和范围的情况下，可以对其进行各种修改和变化。

说　明　书　附　图

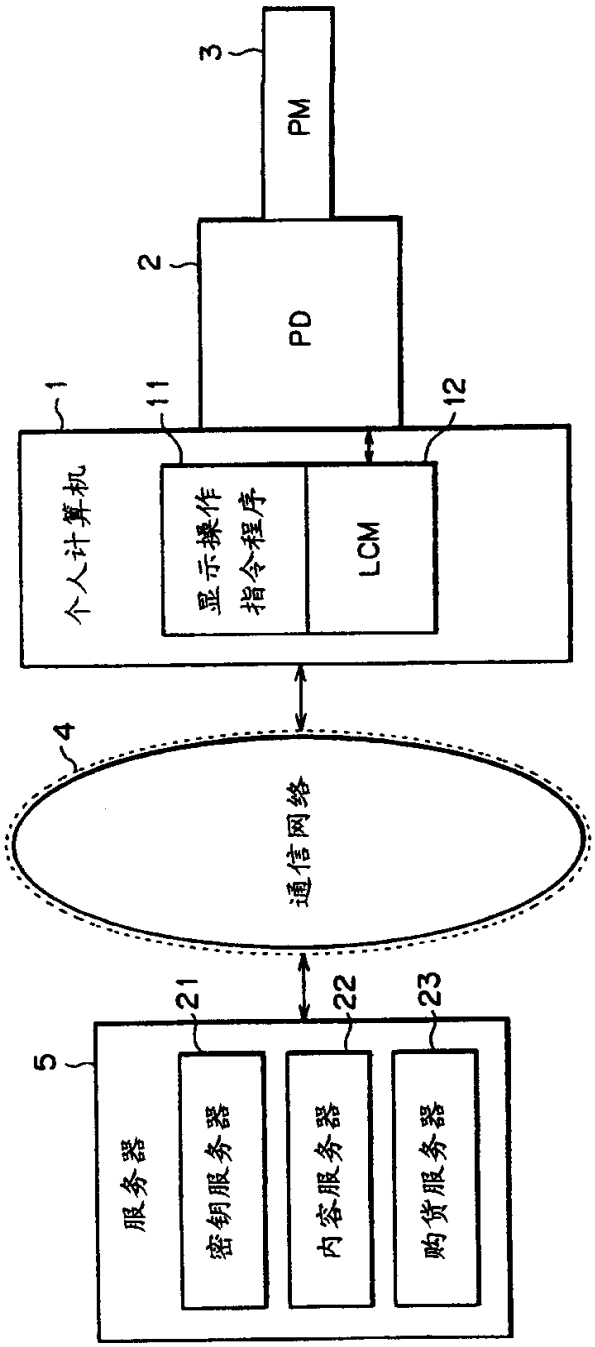

3
PM
2
PD
1
11
12
个人计算机
显示操作指令程序
LCM
4
通信网络
5
21
22
23
服务器
密钥服务器
内容服务器
购货服务器

图 1

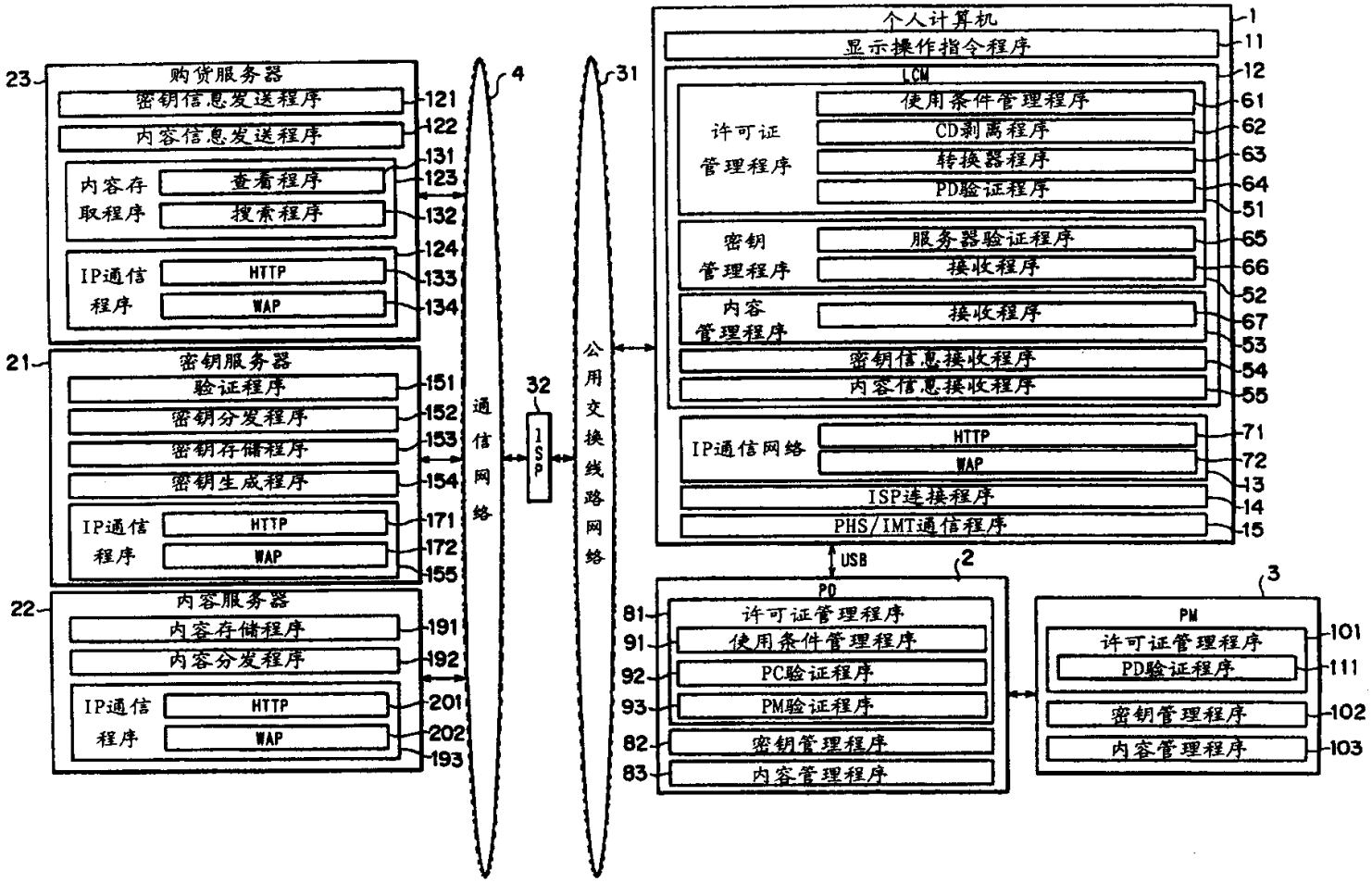

个人计算机
1
显示操作指令程序
11
LCM
12
许可证管理程序
使用条件管理程序
61
CD剥离程序
62
转换器程序
63
PD验证程序
64
51
密钥管理程序
服务器验证程序
65
接收程序
66
52
内容管理程序
接收程序
67
53
密钥信息接收程序
54
内容信息接收程序
55
IP通信网络
HTTP
71
WAP
72
73
ISP连接程序
74
PHS/IMT通信程序
75
USB
2
PD
许可证管理程序
81
使用条件管理程序
91
PC验证程序
92
PM验证程序
93
密钥管理程序
82
内容管理程序
83
3
PM
许可证管理程序
101
PD验证程序
111
密钥管理程序
102
内容管理程序
103
公用交换线路网络
31
通信网络
4
32
ISP
购货服务器
23
密钥信息发送程序
121
内容信息发送程序
122
内容存取程序
查看程序
131
搜索程序
123
132
IP通信程序
HTTP
124
WAP
133
134
密钥服务器
21
验证程序
151
密钥分发程序
152
密钥存储程序
153
密钥生成程序
154
IP通信程序
HTTP
171
WAP
172
155
内容服务器
22
内容存储程序
191
内容分发程序
192
IP通信程序
HTTP
201
WAP
202
193

图 2

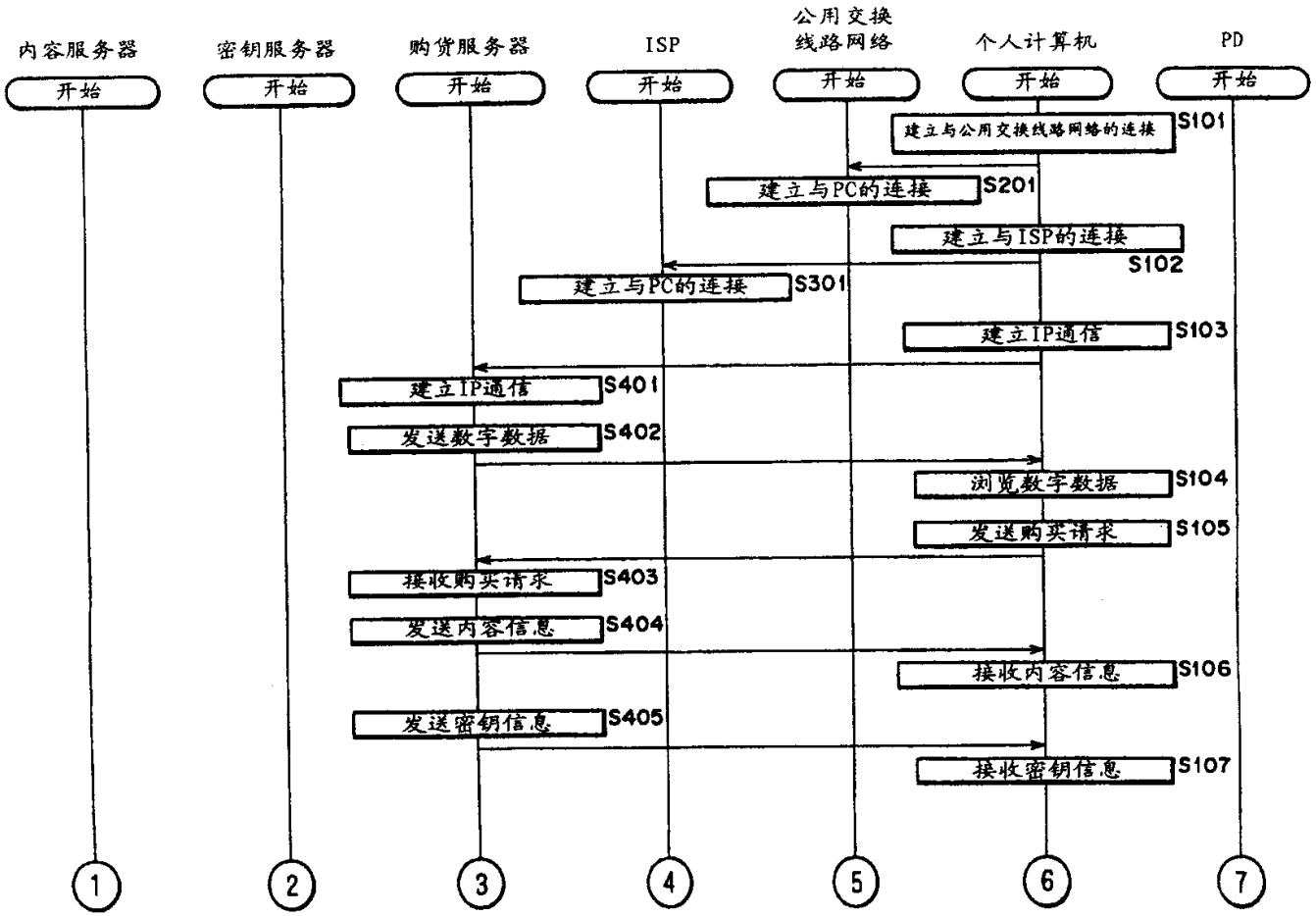

内容服务器
密钥服务器
购货服务器
ISP
公用交换线路网络
个人计算机
PD
开始
建立与公用交换线路网络的连接
S101
建立与PC的连接
S201
建立与ISP的连接
S102
建立与PC的连接
S301
建立IP通信
S103
建立IP通信
S401
发送数字数据
S402
浏览数字数据
S104
发送购买请求
S105
接收购买请求
S403
发送内容信息
S404
接收内容信息
S106
发送密钥信息
S405
接收密钥信息
S107
1
2
3
4
5
6
7

图 3

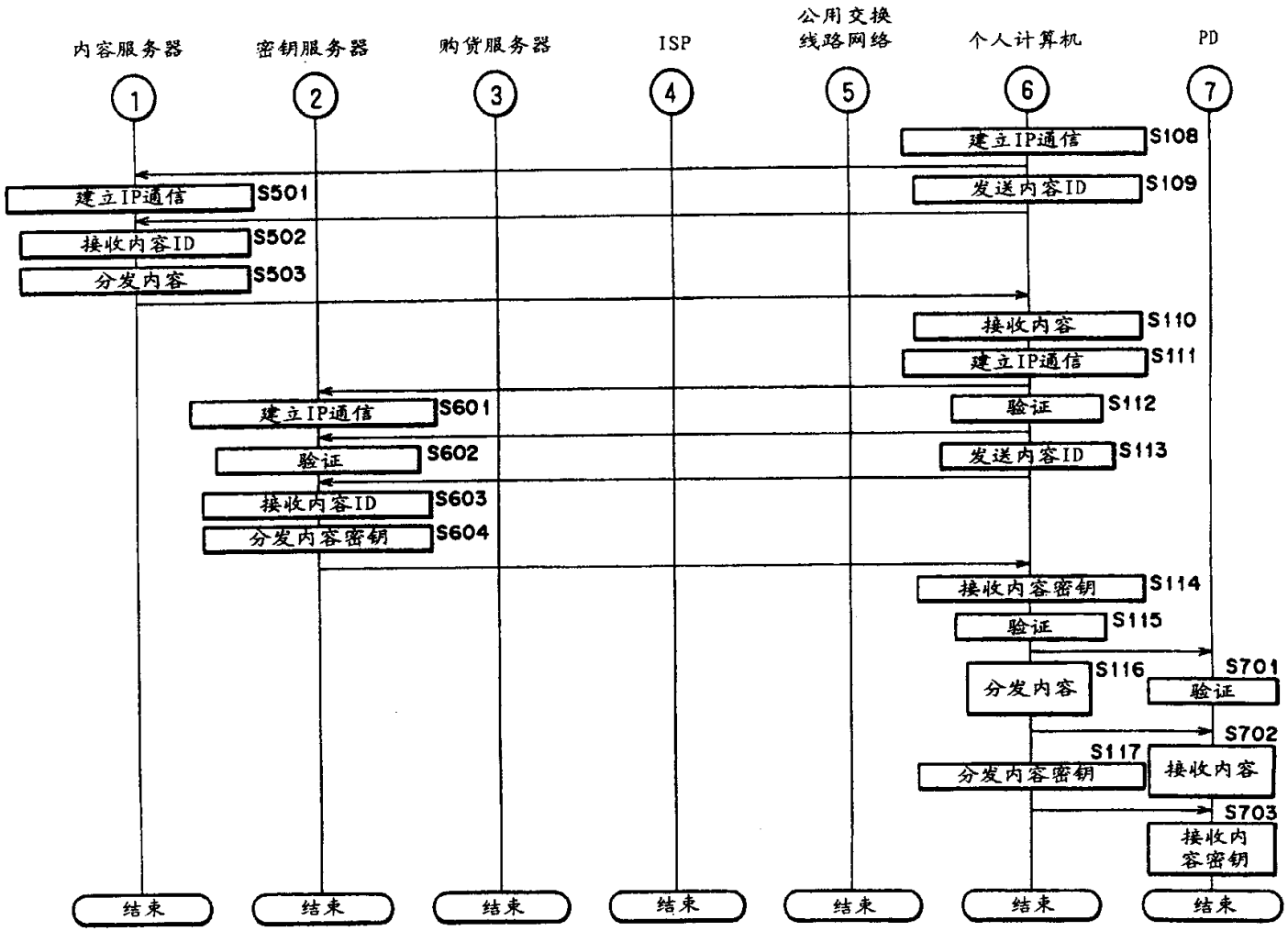

内容服务器
密钥服务器
购货服务器
ISP
公用交换线路网络
个人计算机
PD
1
2
3
4
5
6
7
建立IP通信 S108
发送内容ID S109
建立IP通信 S501
接收内容ID S502
分发内容 S503
接收内容 S110
建立IP通信 S111
建立IP通信 S601
验证 S112
验证 S602
发送内容ID S113
接收内容ID S603
分发内容密钥 S604
接收内容密钥 S114
验证 S115
分发内容 S116
验证 S701
分发内容密钥 S117
接收内容 S702
接收内容密钥 S703
结束
结束
结束
结束
结束
结束
结束

图 4

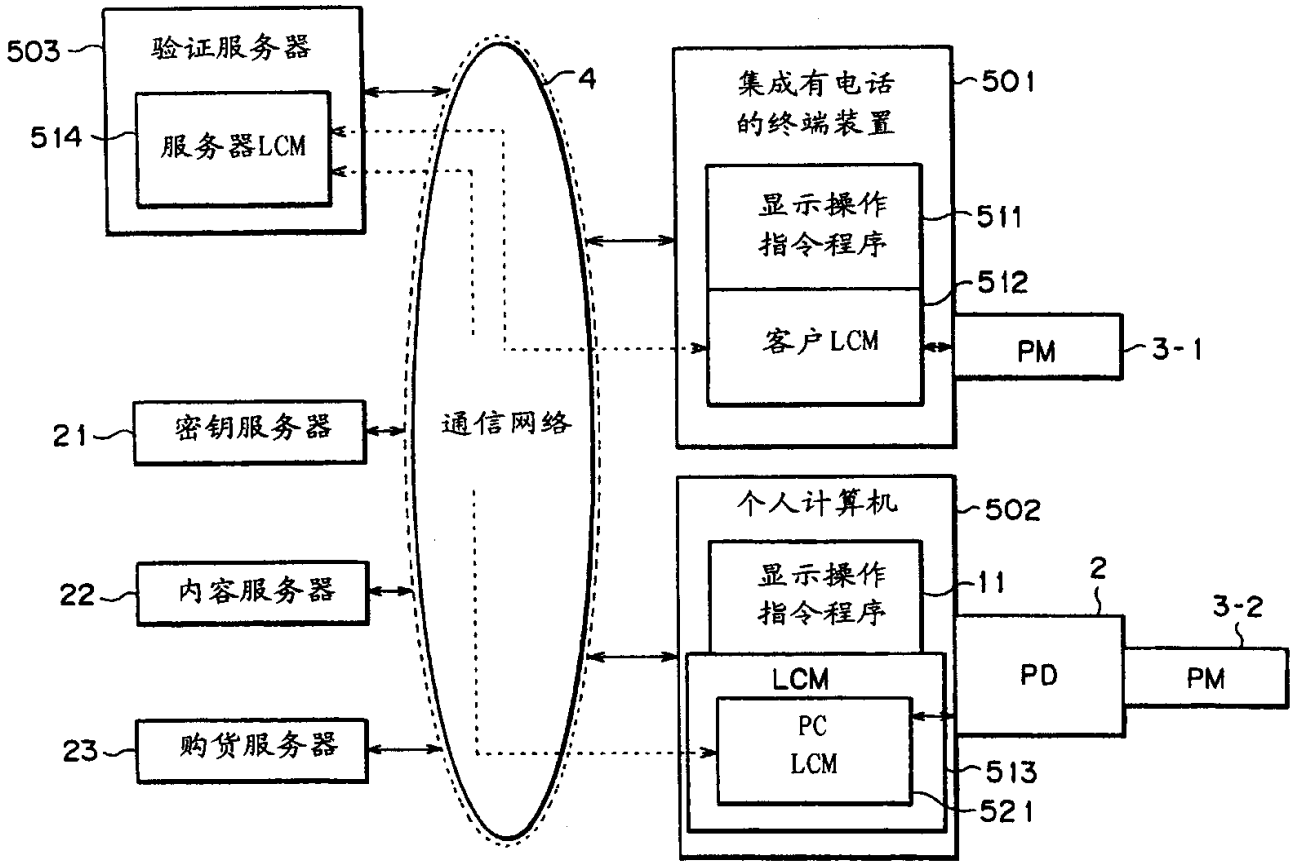

503
验证服务器
514
服务器LCM
4
通信网络
集成有电话
的终端装置
501
显示操作
指令程序
511
512
客户LCM
PM
3-1
21
密钥服务器
22
内容服务器
23
购货服务器
个人计算机
502
显示操作
指令程序
11
2
3-2
LCM
PC
LCM
PD
PM
513
521

图 5

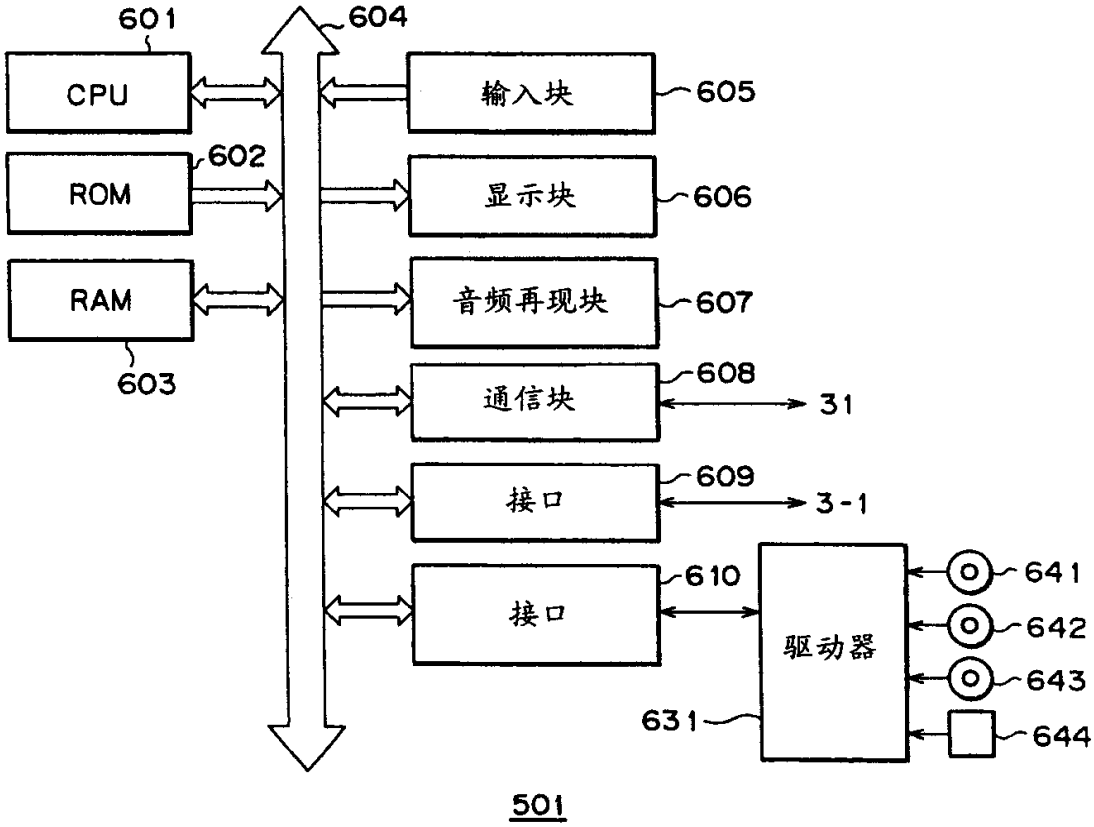

601
604
CPU
输入块
605
602
ROM
显示块
606
RAM
音频再现块
607
603
608
通信块
31
609
接口
3-1
610
接口
驱动器
641
642
643
631
644
501

图 6

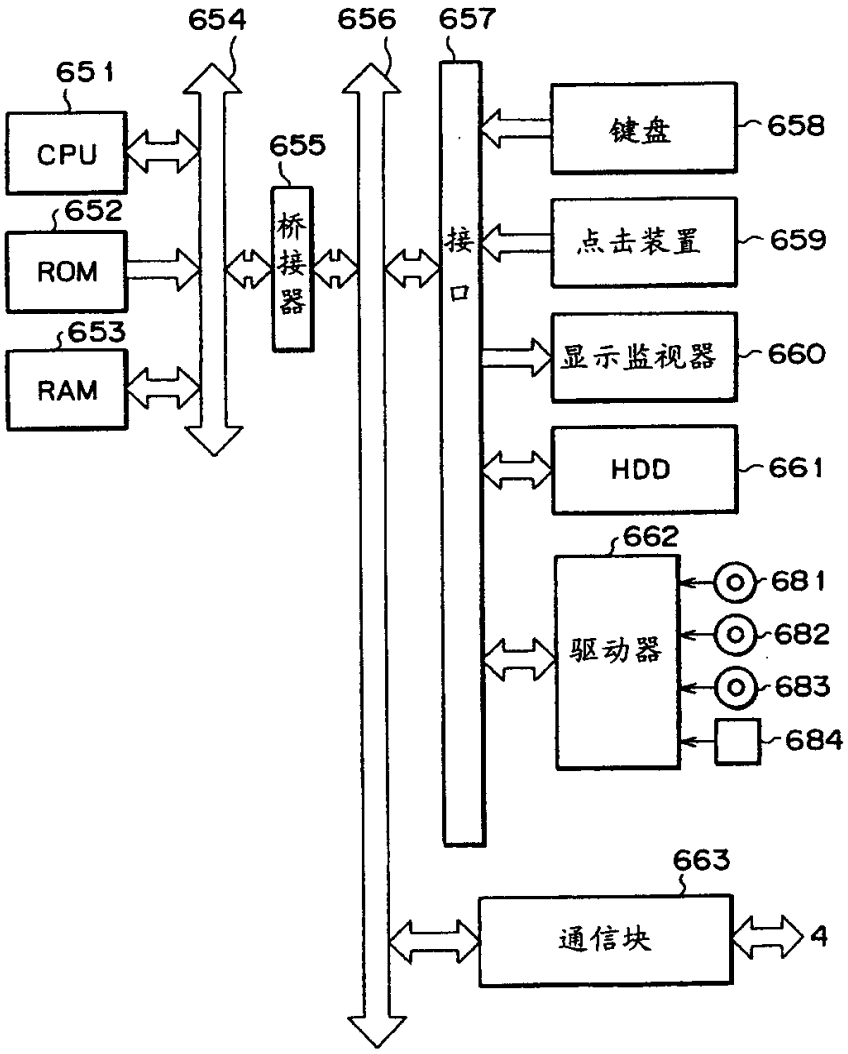

654
656
657
651
CPU
655
652
ROM
桥接器
653
RAM
接口
键盘
658
点击装置
659
显示监视器
660
HDD
661
662
681
驱动器
682
683
684
663
通信块
4
503

图 7

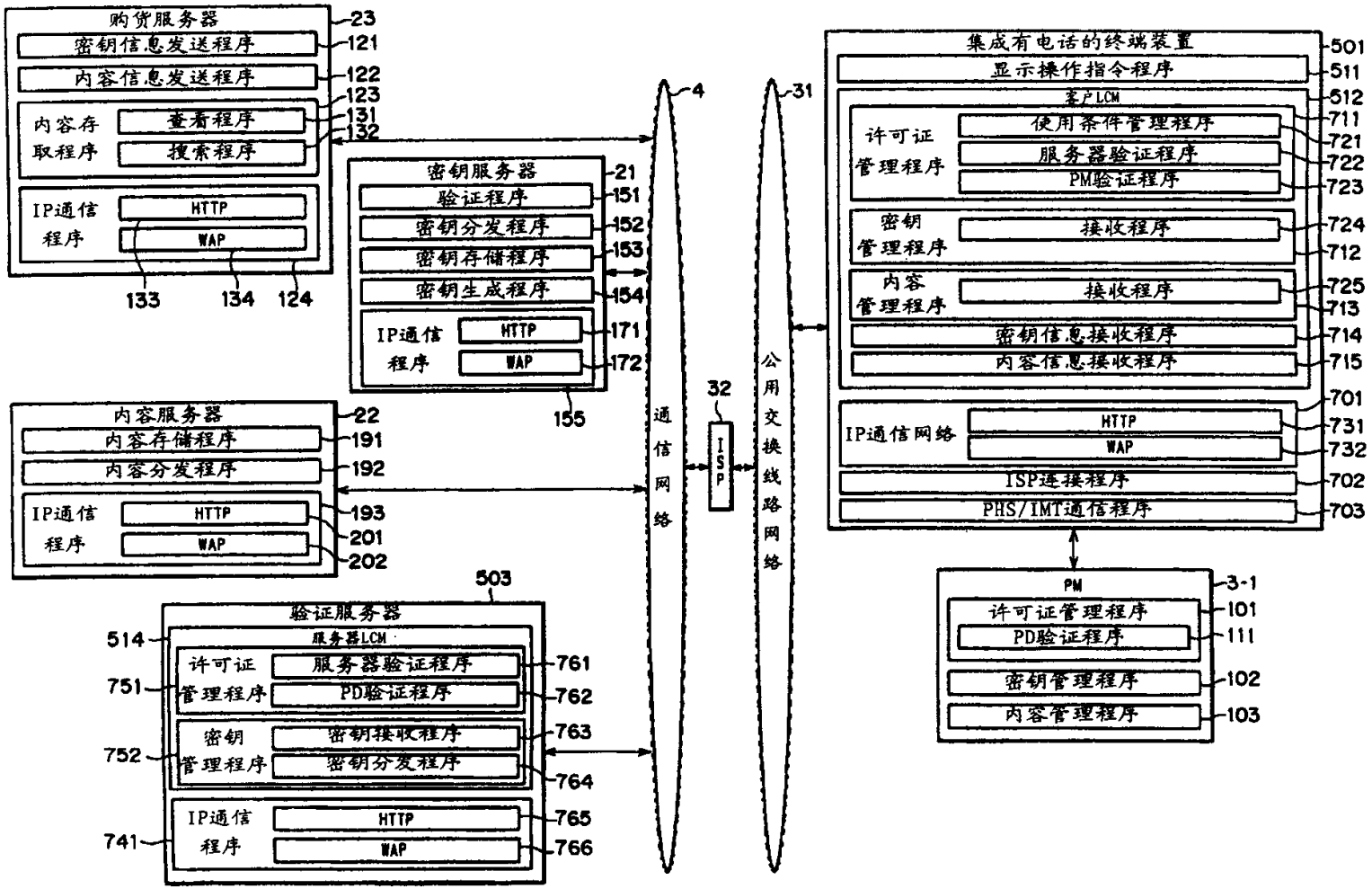

购货服务器
23
密钥信息发送程序
121
内容信息发送程序
122
内容存取程序
查看程序
123
131
搜索程序
132
IP通信程序
HTTP
WAP
133
134
124
密钥服务器
21
验证程序
151
密钥分发程序
152
密钥存储程序
153
密钥生成程序
154
IP通信程序
HTTP
WAP
171
172
155
内容服务器
22
内容存储程序
191
内容分发程序
192
IP通信程序
HTTP
WAP
193
201
202
503
验证服务器
514
服务器LCM
许可证管理程序
服务器验证程序
751
761
PD验证程序
762
密钥管理程序
密钥接收程序
752
763
密钥分发程序
764
IP通信程序
HTTP
765
741
WAP
766
4
通信网络
32
ISP
31
公用交换线路网络
集成有电话的终端装置
501
显示操作指令程序
511
客户LCM
512
许可证管理程序
使用条件管理程序
711
721
服务器验证程序
722
PM验证程序
723
密钥管理程序
接收程序
724
712
内容管理程序
接收程序
725
713
密钥信息接收程序
714
内容信息接收程序
715
IP通信网络
HTTP
701
731
WAP
732
ISP连接程序
702
PHS/IMT通信程序
703
PM
3-1
许可证管理程序
101
PD验证程序
111
密钥管理程序
102
内容管理程序
103

图 8

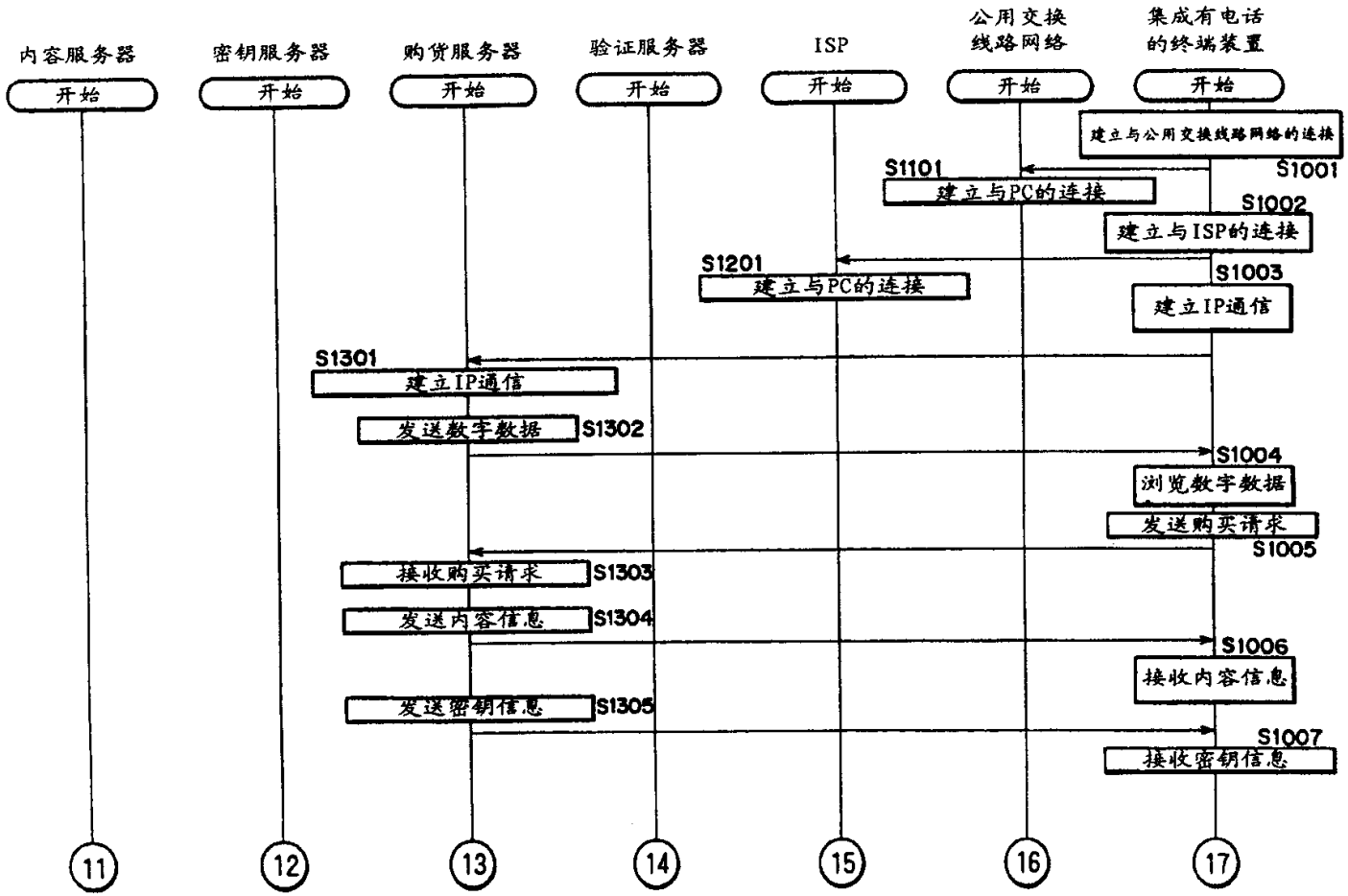

内容服务器
密钥服务器
购货服务器
验证服务器
ISP
公用交换线路网络
集成有电话的终端装置
开始
建立与公用交换线路网络的连接
S1001
S1101
建立与PC的连接
S1002
建立与ISP的连接
S1201
建立与PC的连接
S1003
建立IP通信
S1301
建立IP通信
发送数字数据
S1302
S1004
浏览数字数据
发送购买请求
S1005
接收购买请求
S1303
发送内容信息
S1304
S1006
接收内容信息
发送密钥信息
S1305
S1007
接收密钥信息
11
12
13
14
15
16
17

图 9

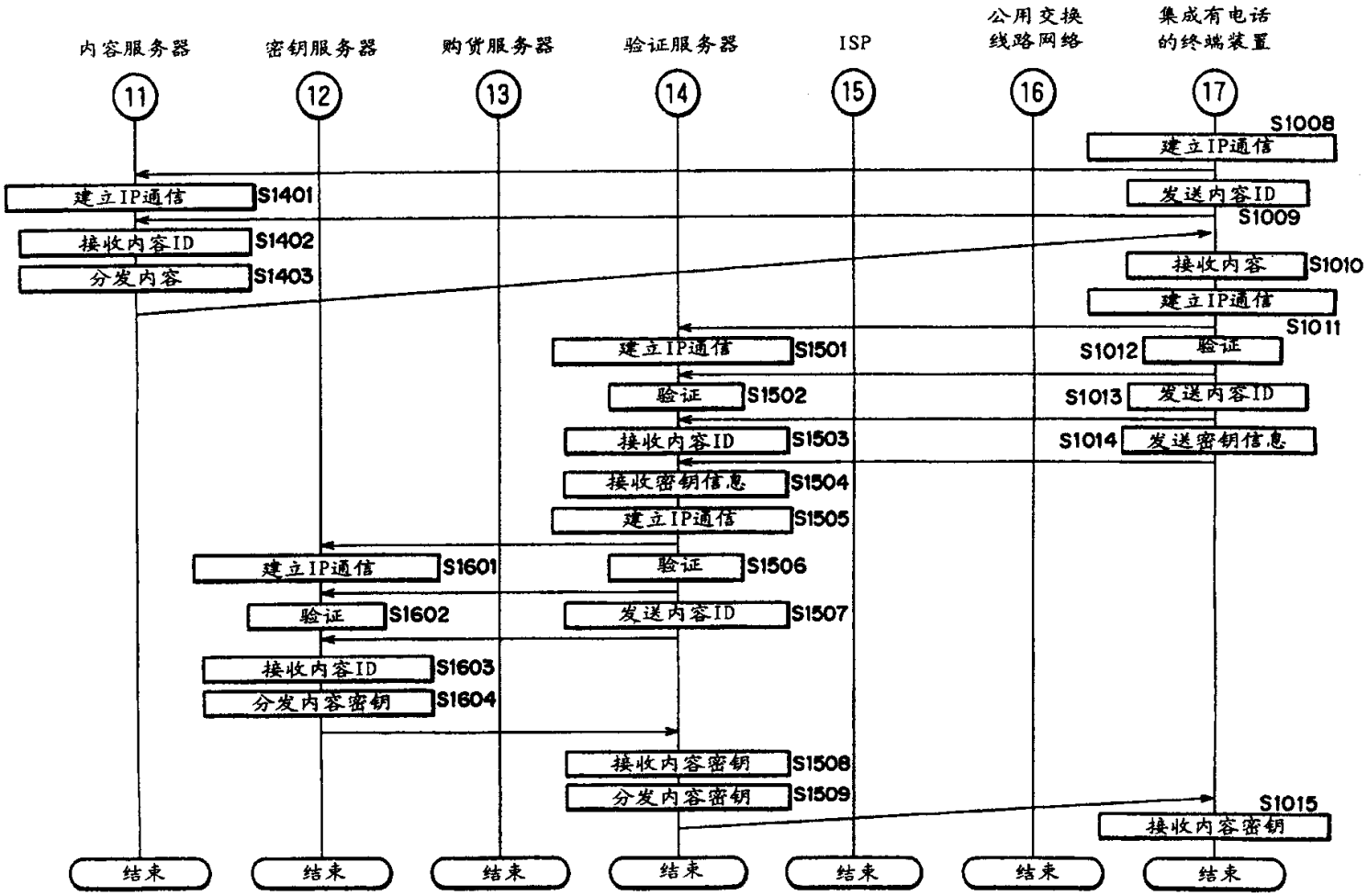

内容服务器
密钥服务器
购货服务器
验证服务器
ISP
公用交换线路网络
集成有电话的终端装置
11
12
13
14
15
16
17
S1008
建立IP通信
建立IP通信 S1401
发送内容ID
S1009
接收内容ID S1402
分发内容 S1403
接收内容 S1010
建立IP通信
S1011
建立IP通信 S1501
S1012 验证
验证 S1502
S1013 发送内容ID
接收内容ID S1503
S1014 发送密钥信息
接收密钥信息 S1504
建立IP通信 S1505
建立IP通信 S1601
验证 S1506
验证 S1602
发送内容ID S1507
接收内容ID S1603
分发内容密钥 S1604
接收内容密钥 S1508
分发内容密钥 S1509
S1015
接收内容密钥
结束
结束
结束
结束
结束
结束
结束

图 10