



[12] 发明专利说明书

专利号 ZL 01803390.3

[45] 授权公告日 2009 年 7 月 8 日

[11] 授权公告号 CN 100512095C

[22] 申请日 2001.11.1 [21] 申请号 01803390.3

[30] 优先权

[32] 2000.11.1 [33] JP [31] 334183/00

[86] 国际申请 PCT/JP2001/009607 2001.11.1

[87] 国际公布 WO2002/037746 日 2002.5.10

[85] 进入国家阶段日期 2002.7.1

[73] 专利权人 索尼株式会社

地址 日本东京

共同专利权人 索尼计算机娱乐公司

[72] 发明人 吉野贤治 石桥义人 秋下彻

白井太三 冈 诚 吉森正治

[56] 参考文献

US5673316A 1997.9.30

审查员 于洪蕊

[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 王以平

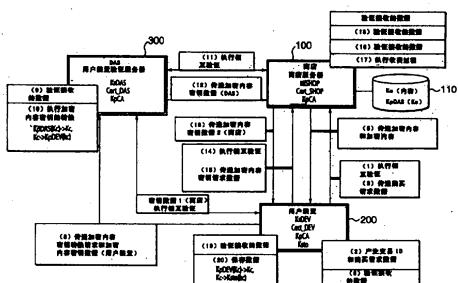
权利要求书 4 页 说明书 109 页 附图 76 页

[54] 发明名称

内容传送系统和内容传送方法

[57] 摘要

本发明涉及内容传送系统和内容传送方法，当用户装置(DEV)向商店服务器发送内容购买请求时，商店服务器把由用户装置验证服务器(DAS)的公共密钥加密的内容密钥KpDAS(Kc)发送给用户装置。当用户装置把加密内容密钥发送给用户装置验证服务器时，用户装置验证服务器对内容密钥(Kc)解密，并且对其进行重新加密，以便把该密钥改变成用用户装置的内容密钥(Kc)加密的内容密钥KpDEV(Kc)。用户装置验证服务器把改变后的内容密钥发送给商店服务器，并且根据收费已完成的条件，商店服务器把改变后的内容密钥发送给用户装置。



1、一种内容传送系统，包括：

向商店服务器传送内容购买请求的用户装置；

从用户装置接收内容购买请求，管理利用内容密钥 K_c 加密的加密内容，并且还管理不能用保存在用户装置中的密钥解密的加密内容密钥的商店服务器；和

执行密钥转换过程，使得把加密内容密钥转换成可利用保存在用户装置中的密钥解密的形式的用户装置验证服务器，所述用户设备验证服务器包括许可证管理数据库；

其中如果完成了收取用户装置所购买内容的费用的过程，则商店服务器把由用户装置验证服务器转换成可由保存在用户装置中的密钥解密的形式的加密内容密钥提供给用户装置，

其中，所述许可证管理数据库记录其中由所述用户装置验证服务器执行密钥转换过程的内容交易的历史，以便监控和管理需要用于收取用户装置所购买内容的费用的过程的内容交易，和

其中用户装置验证服务器执行密钥转换过程，以致利用用户装置验证服务器的保密密钥 K_{sDAS} 对加密内容密钥 K_{pDAS} (K_c) 解密，从而获得内容密钥 K_c ，随后用用户装置的公共密钥 K_{pDEV} 重新对内容密钥 K_c 加密，从而产生加密内容密钥 K_{pDEV} (K_c)；以及将所得到的加密内容密钥保存到用户装置的存储装置中。

2、按照权利要求 1 所述的内容传送系统，

其中不能用保存在用户装置中的密钥解密的加密内容密钥是利用用户装置验证服务器的公共密钥 K_{pDAS} 加密的加密内容密钥 K_{pDAS} (K_c)。

3、按照权利要求 1 所述的内容传送系统，

其中用户装置验证服务器从用户装置接收不能用保存在用户装置中的密钥解密的加密内容密钥，用户装置验证服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给商店服务

器，并且

如果已完成收费过程，则商店服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给用户装置。

4、按照权利要求 1 所述的内容传送系统，

其中用户装置验证服务器从商店服务器接收不能用保存在用户装置中的密钥解密的加密内容密钥，用户装置验证服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给商店服务器，并且

如果完成了收费过程，则商店服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给用户装置。

5、按照权利要求 1 所述的内容传送系统，还包括：

把加密内容传送给用户装置的内容传送服务器，其中响应从用户装置接收内容购买请求，商店服务器把内容传送请求发送给内容传送服务器，并且

其中响应从商店服务器收到内容传送请求，内容传送服务器把加密内容传送给用户装置。

6、按照权利要求 1 所述的内容传送系统，

其中由用户装置产生并且被传送给商店服务器的内容购买请求数据包括识别请求数据发往商店的商店 ID；识别内容交易的交易 ID；识别购买请求内容的内容 ID；和用户装置的数字签名；并且

其中商店服务器通过验证写入内容购买请求数据中的数字签名，检查数据的完整性是否被保持；根据内容购买请求数据把新的条目添加到商店管理数据库中；设置指出与添加的条目相关的过程状态的状态信息；并且根据状态信息，管理与商店相关的程序列的转变。

7、按照权利要求 1 所述的内容传送系统，其中当用户装置验证服务器从用户装置或者商店服务器收到密钥转换请求时，用户装置验证服务器把新的条目添加到由用户装置验证服务器管理的数据库中，设置指出与添加条目相关的过程状态的状态信息，并且根据状态信息，管理与用户装置验证服务器相关的程序列的转变。

8、一种内容传送方法，包括下述步骤：

把内容购买请求从用户装置传送给商店服务器；

在商店服务器接收来自用户装置的内容购买请求；

在用户装置验证服务器中，把不能用保存在用户装置中的密钥解密的形式的加密内容密钥转换成可用保存在用户装置中的密钥加密的形式的加密内容密钥；

如果用户装置完成了与内容购买相关的收费过程，从商店服务器把由用户装置验证服务器转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥提供给用户装置；

将其中由所述用户装置验证服务器执行密钥转换过程的内容交易的历史记录在用户设备验证服务器的许可证管理数据库中，以便监控和管理需要用于收取用户装置所购买内容的费用的过程的内容交易；

其中用户装置验证服务器执行密钥转换，以致利用用户装置验证服务器的保密密钥 KsDAS 对加密内容密钥 KpDAS (Kc) 解密，随后用用户装置的公共密钥 KpDEV 重新加密，从而产生加密内容密钥 KpDEV (Kc)；以及将所得到的加密内容密钥保存到用户装置的存储装置中。

9、按照权利要求 8 所述的内容传送方法，

其中不能用保存在用户装置中的密钥解密的形式的加密内容密钥是利用用户装置验证服务器的公共密钥 KpDAS 加密的加密内容密钥 KpDAS (Kc)。

10、按照权利要求 8 的述的内容传送方法，

其中用户装置验证服务器从用户装置接收不能用保存在用户装置中的密钥解密的加密内容密钥，用户装置验证服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给商店服务器，并且

如果已完成收费过程，则商店服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给用户装置。

11、按照权利要求 8 所述的内容传送方法，

其中用户装置验证服务器从商店服务器接收不能用保存在用户装置中的密钥解密的加密内容密钥，用户装置验证服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给商店服务器，并且

如果完成了收费过程，则商店服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给用户装置。

12、按照权利要求 8 所述的内容传送方法，

其中由用户装置产生并且被传送给商店服务器的内容购买请求数据包括识别请求数据发往商店的商店 ID；识别内容交易的交易 ID；识别购买请求内容的内容 ID；和用户装置的数字签名；和

其中商店服务器通过验证写入内容购买请求数据中的数字签名检查数据的完整性是否被保持；根据内容购买请求数据把新的条目添加到商店管理数据库中；设置指出与添加的条目相关的过程状态的状态信息；并且根据状态信息管理与商店相关的过程序列的转变。

13、按照权利要求 8 所述的内容传送方法，其中当用户装置验证服务器从用户装置或者商店服务器收到密钥转换请求时，用户装置验证服务器把新的条目添加到由用户装置验证服务器管理的数据库中，设置指出与添加条目相关的过程状态的状态信息，并且根据状态信息，管理与用户装置验证服务器相关的过程序列的转变。

内容传送系统和内容传送方法

技术领域

本发明涉及一种内容传送系统和一种内容传送方法。更具体地说，本发明涉及一种内容传送系统和一种内容传送方法，其中以改进的方式执行提供内容的实体和接收内容的实体之间的内容交易，从而获得高的安全性。这里，术语“系统”用于描述若干装置的逻辑集合，并且不必要求所述若干装置被布置在单一机箱中。

背景技术

现在通过诸如因特网之类网络散布各种软件数据，例如游戏程序、音频数据、图像数据和文件生成程序（下面把这样的数据称为内容）是非常常见的。通过网络进行商业交易和结算，例如在线购物、银行账户结算或者售票也是常见的。

就用于这类目的的网络数据通信来说，一般在确认数据发送者和数据接收者是经过授权的发送者和接收者之后才传送数据，以确保安全。确保数据传输安全的一种已知技术是在对数据加密之后传送数据。另一种技术是在数据上写入数字签名。

通过对加密数据进行预定的解密处理，可把加密数据转换成其初始形式（纯文本）。在本领域中，使用加密密钥对信息加密和使用解密密钥对信息解密的数据加密和解密技术为人们所熟知。

使用加密密钥和解密密钥的各种数据加密和解密技术在本领域中为人们熟知。一种这样的技术是公共钥加密法。在公共钥加密法中，发送者和接收者使用不同的密钥，其中一个密钥是允许非特定用户使用的公共密钥，另一密钥是保密的保密密钥。例如，公共密钥被用作数据加密密钥，保密密钥被用作解密密钥。另一例子是保密密钥被用作鉴别码生成密钥，公共密钥被用作鉴别码验证密钥。

在公钥加密法中，与共用密钥既用于加密又用于解密的共用密钥加密法不同，应保密的保密密钥由特定的个人持有。从而，公钥加密法的优点在于密钥易于管理。但是，和共用密钥加密法相比，在公钥加密法中数据处理速度低。由于数据处理速度低，主要在诸如数字签名或者需要较小数据大小的保密密钥的传输之类应用中采用公钥加密法。公钥加密法的典型例子是 RSA (Rivest-Shamir-Adelman) 加密系统。在该技术中，使用两个非常大的素数（例如 150 位的素数）的乘积，因为难以把两个非常大的素数（例如 150 位的素数）的乘积因数分解为多个素数。

在公钥加密法中，允许大量的非特定用户使用相同的公共密钥，并且通常由称为公共密钥证书的证书来认证散布的公共密钥的正确性。例如，用户 A 产生一对公共密钥和保密密钥，并且把产生的公共密钥发送给认证机构，从认证机构获得公共密钥证书。用户 A 向公众公布公共密钥证书。非特定用户通过预定的程序从公共密钥证书获得公共密钥，并且在利用公共密钥对文件等加密之后把所述文件等传送给用户 A。当收到该文件时，用户 A 利用保密密钥对接收的文件解密。用户 A 还可把他/她的利用保密密钥加密的签名附到文件或类似物中，非特定用户可通过预定的程序利用公共密钥证书抽取的公共密钥来验证该签名。

在公钥加密法中，公共密钥证书由认证机构 (CA) 或者发布机构 (IA) 发布，其中响应从用户接收 ID 和公共密钥，认证机构在添加诸如认证机构的 ID 和有效期以及在添加认证机构的签名之后发布证书。

公共密钥证书具有关于证书的版本号、发布机构向证书的用户分配的证书的序列号、数字签名中使用的算法和参数、认证机构的名称、证书的有效期、证书的用户的名称（用户 ID）、证书的用户的公共密钥和数字签名的信息。

数字签名是通过对除数字签名之外的所有上述数据，即证书的版本号、发布机构向证书的用户分配的证书的序列号、数字签名中使用

的算法和参数、认证机构的名称、证书的有效期、证书的用户的名称、证书的用户的公共密钥应用散列函数产生散列值，随后利用认证机构的保密密钥对所得到的散列值加密而产生的数据。

当用户使用公共密钥证书时，用户利用用户所具有的认证机构的公共密钥验证公共密钥证书的数字签名，并且用户从公共密钥证书抽取公共密钥。于是，希望使用公共密钥证书的所有用户需要具有认证机构的共用公共密钥。

例如，在基于使用由认证机构发布的公共密钥证书的公钥加密法的数据传输系统中，提供内容的商店在利用用户装置的公共密钥对内容加密之后向用户传送该内容。当用户装置从提供内容的商店收到加密数据时，用户装置利用对应于用户装置的公共密钥的保密密钥对加密内容解密。

但是，在许多实际的内容交易中，内容由既不是内容许可证持有人又不是具有内容版权的内容制作者的内容提供商提供给用户。大部分的这种情况中，内容提供商在不确认用户是授权用户的情况下向该用户提供内容。即，在某些情况下，内容被提供或者销售给未经授权的用户。

在上述内容交换系统中，虽然从购买内容的用户向销售内容的内容提供商支付内容的费用，但是不能确保许可费是支付给内容的许可证持有者或者具有内容版权的内容制作者。在目前的许多系统中，内容提供商评估销售量并对外公布，根据内容提供商公布的销售量从内容提供商向许可者持有者或者具有内容版权的内容制作者支付许可费。

即，在常规的内容提供系统中，许可证持有者或者具有内容版权的内容制作者无法知道实际的销售量，无法了解内容是否以适当的方式被散布。

鉴于常规内容提供系统中的问题，本发明的目的是提供一种内容传送系统和内容传送方法，所述内容传送系统和内容传送方法允许许可者持有者或者具有内容版权的内容制作者获得有关在内容提供商

和用户之间进行的实际内容交换的准确信息，并且允许在充分保护内容的版权的同时散布内容。

发明内容

根据本发明的第一方面，提供一种内容传送系统，它包括向商店服务器传送内容购买请求的用户装置（DEV）；从用户装置接收内容购买请求，管理利用加密密钥 K_c 加密的加密内容并且还管理不能用保存在用户装置中的密钥解密的加密内容密钥的商店服务器（SHOP）；和执行密钥转换过程，从而把加密内容密钥转换成可利用保存在用户装置中的密钥解密的形式的用户装置验证服务器（DAS）；其中如果完成了收取用户装置购买内容的费用的过程，则商店服务器把由用户装置验证服务器转换成可由保存在用户装置中的密钥解密的形式的加密内容密钥提供给用户装置。

在根据本发明的内容传送系统中，不能用保存在用户装置中的密钥解密的加密内容密钥最好是利用用户装置验证服务器（DAS）的公共密钥 K_{pDAS} 加密的加密内容密钥 $K_{pDAS}(K_c)$ ，用户装置验证服务器（DAS）执行密钥转换过程，以致利用用户装置验证服务器（DAS）的保密密钥 K_{sDAS} 对加密内容密钥 $K_{pDAS}(K_c)$ 解密，并且随后用用户装置（DEV）的公共密钥 K_{pDEV} 重新加密，从而产生加密内容密钥 $K_{pDEV}(K_c)$ 。

在根据本发明的内容传送系统中，用户装置验证服务器最好从用户装置接收不能用保存在用户装置中的密钥解密的加密内容密钥，用户装置验证服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给商店服务器，并且如果已完成收费过程，则商店服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给用户装置。

在根据本发明的内容传送系统中，用户装置验证服务器最好从商店服务器接收不能用保存在用户装置中的密钥解密的加密内容密钥，用户装置验证服务器把转换成可用保存在用户装置中的密钥解密的形

式的加密内容密钥传送给商店服务器，并且如果完成了收费过程，则商店服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给用户装置。

内容传送系统最好还包括把加密内容传送给用户装置的内容传送服务器，其中响应从用户装置收到内容购买请求，商店服务器把内容传送请求发送给内容传送服务器，其中响应从商店服务器收到内容传送请求，内容传送系统把加密内容传送给用户装置。

在根据本发明的内容传送系统中，由用户装置产生并且被传送给商店服务器的内容购买请求数据最好包括识别请求数据发往的商店的商店 ID；识别内容交易的交易 ID；识别购买请求内容的内容 ID；和用户装置的数字签名，其中商店服务器通过验证写入内容购买请求数据中的数字签名，检查数据的完整性是否被保持；根据内容购买请求数据把新的条目添加到商店管理数据库中；设置指出与添加的条目相关的过程状态的状态信息；并且根据状态信息，管理与商店相关的过程序列的转变。

最好，在根据本发明的内容传送系统中，当用户装置验证服务器从用户装置或者商店服务器收到密钥转换请求时，用户装置验证服务器把新的条目添加到由用户装置验证服务器管理的数据库中，设置指出与添加条目相关的过程状态的状态信息，并且根据状态信息，管理与用户装置验证服务器相关的过程序列的转变。

根据本发明的第二方面，提供一种管理在商店服务器和用户装置之间销售的内容的传递的用户装置验证服务器，其中响应从商店服务器或者用户装置收到密钥转换请求，用户装置验证服务器把与在商店服务器和用户装置之间销售的内容相关的密钥，从不能用保存在用户装置中的密钥解密的加密形式转换成可用保存在用户装置中的密钥解密的加密形式，其中用户装置验证服务器验证写入密钥转换请求中的商店服务器的数字签名或者用户装置的数字签名，并且如果验证表明密钥转换请求有效，则用户装置验证服务器进行密钥转换。

根据本发明的第三方面，提供一种把用于对加密内容解密的内容

密钥提供给用户装置的商店服务器，其中商店服务器以这样的方式保存用于对内容加密的内容密钥，使得用于对内容加密的内容密钥被加密成不能用保存在用户装置中的密钥解密的形式，其中如果已成功完成响应用户装置发出的内容购买请求的收费过程，则商店服务器把通过管理内容传送的用户装置验证服务器（DAS）执行的密钥转换过程产生的加密内容密钥传送给用户装置，从而呈不能用保存在用户装置中的密钥解密的加密内容密钥被转换成可用保存在用户装置中的密钥解密的形式。

在根据本发明的商店服务器中，商店服务器最好包括用于传送加密内容的内容传送服务器。

根据本发明的第四方面，提供一种产生内容购买请求、把内容购买请求传送给商店服务器并且再现内容的内容再现装置，其中内容再现装置通过执行包括下述步骤的过程获得内容密钥：通过商店服务器接收加密内容密钥，所述加密内容密钥通过由管理内容传送的用户装置验证服务器（DAS）执行的密钥转换过程产生，从而不能用保存在内容再现装置中的密钥解密的加密内容密钥被转换成可用保存在内容再现装置中的密钥解密的形式；验证包含在收到的加密内容密钥数据中的商店服务器和用户装置验证服务器（DAS）的签名；并且如果验证指出数据未被篡改，则从接收的加密内容密钥数据中抽取加密内容密钥，从而获得内容密钥。

根据本发明的第五方面，提供一种内容传送方法，包括下述步骤：把内容购买请求从用户装置（DEV）传送给商店服务器（SHOP）；在商店服务器（SHOP）接收来自用户装置的内容购买请求；在用户装置验证服务器（DAS）中，把不能用保存在用户装置中的密钥解密的形式的加密内容密钥转换成可用保存在用户装置中的密钥加密的加密内容密钥；并且如果用户装置完成了与内容购买相关的收费过程，从商店服务器把由用户装置验证服务器转换成可用保存在用户装置中的密钥解密的加密内容密钥提供给用户装置。

在根据本发明的内容传送方法中，不能用保存在用户装置中的密

钥解密的加密内容密钥最好是利用用户装置验证服务器（DAS）的公共密钥 KpDAS 加密的加密内容密钥 KpDAS（Kc），用户装置验证服务器（DAS）执行密钥转换过程，以致利用用户装置验证服务器（DAS）的保密密钥 KsDAS 对加密内容密钥 KpDAS（Kc）解密，并且随后用用户装置（DEV）的公共密钥 KpDEV 重新加密，从而产生加密内容密钥 KpDEV（Kc）。

在根据本发明的内容传送方法中，用户装置验证服务器最好从用户装置接收不能用保存在用户装置中的密钥解密的加密内容密钥，用户装置验证服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给商店服务器，并且如果已完成收费过程，则商店服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给用户装置。

在根据本发明的内容传送方法中，用户装置验证服务器最好从商店服务器接收不能用保存在用户装置中的密钥解密的加密内容密钥，用户装置验证服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给商店服务器，并且如果完成了收费过程，则商店服务器把转换成可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给用户装置。

在根据本发明的内容传送方法中，由用户装置产生并且被传送给商店服务器的内容购买请求数据最好包括识别请求数据发往的商店的商店 ID；识别内容交易的交易 ID；识别购买请求内容的内容 ID；和用户装置的数字签名；其中商店服务器通过验证写入内容购买请求数据中的数字签名检查数据的完整性是否被保持；根据内容购买请求数据把新的条目添加到商店管理数据库中；设置指出与添加的条目相关的过程状态的状态信息；并且根据状态信息管理与商店相关的过程序列的转变。

在根据本发明的内容传送方法中，最好当用户装置验证服务器从用户装置或者商店服务器收到密钥转换请求时，用户装置验证服务器把新的条目添加到由用户装置验证服务器管理的数据库中，设置指出

与添加条目相关的过程状态的状态信息，并且根据状态信息，管理与用户装置验证服务器相关的程序序列的转变。

根据本发明的第六方面，提供一种程序提供介质，用于提供可在计算机系统中运行，从而执行内容密钥传送过程的计算机程序，所述计算机程序包括下述步骤：接收由管理内容传送的用户装置验证服务器（DAS）产生的，可用保存在用户装置中的密钥解密的加密内容密钥；根据用户装置发出的内容购买请求执行收费过程；并且如果成功完成收费过程，则把可用保存在用户装置中的密钥解密的形式的加密内容密钥传送给用户装置。

根据本发明第六方面的程序提供介质是向能够执行各种程序代码的通用计算机系统提供呈计算机可读形式的计算机程序的介质。该介质不局限于特定的类型，相反可以是各种介质，例如可采用诸如 CD、FD 或 MD 之类的存储介质或者诸如网络之类的传输介质。

程序提供介质限定计算机程序和存储介质之间结构或功能方面的合作关系，用于在计算机系统上实现特定计算机程序的功能。即，通过借助程序提供介质把特定的计算机程序安装到计算机系统上，能够在计算机系统上实现协同操作，从而实现和本发明其它方面实现的功能相类似的功能。

参考附图，根据下述实施例的具体说明，本发明的这些及其它目的和特征将更加明显。

附图说明

图 1 图解说明根据本发明的内容传送系统和内容传送过程；

图 2 图解说明根据本发明的内容传送系统中商店服务器的结构；

图 3 图解说明根据本发明的内容传送系统中商店服务器的购买管理数据库的数据结构；

图 4 图解说明根据本发明的内容传送系统中商店服务器的控制装置的结构；

图 5 图解说明根据本发明的内容传送系统中用户装置验证服务器

的结构；

图 6 图解说明根据本发明的内容传送系统中用户装置验证服务器的许可证管理数据库的结构；

图 7 图解说明根据本发明的内容传送系统中用户装置的结构；

图 8 图解说明根据本发明的内容传送系统中用户装置的购买管理数据库的结构；

图 9 图解说明根据本发明的内容传送系统中传送公共密钥证书的方式；

图 10 图解说明根据本发明的内容传送系统中可采用的签名生成过程；

图 11 图解说明根据本发明的内容传送系统中可采用的签名验证过程；

图 12 图解说明根据本发明的内容传送系统中可采用的相互验证过程（使用对称密钥）；

图 13 图解说明根据本发明的内容传送系统中可采用的相互验证过程（使用不对称密钥）；

图 14 图解说明根据本发明的内容传送系统中在实体之间传送的数据的数据结构；

图 15 图解说明根据本发明的内容传送系统中可采用的签名验证过程；

图 16 图解说明根据本发明的内容传送系统中执行的密钥转换过程；

图 17 图解说明根据本发明的内容传送系统中在实体之间传送的数据的数据结构；

图 18 图解说明根据本发明的内容传送系统中在实体之间传送的数据的数据结构；

图 19 图解说明根据本发明的内容传送系统中执行的内容密钥存储过程；

图 20 图解说明根据本发明的内容传送系统中商店服务器的状态

转变；

图 21 图解说明根据本发明的内容传送系统中用户装置的状态转变；

图 22 图解说明根据本发明的内容传送系统中用户装置验证服务器的状态转变；

图 23 图解说明根据本发明的内容传送系统中商店服务器和用户装置之间的过程流程（部分 1）；

图 24 图解说明根据本发明的内容传送系统中商店服务器和用户装置之间的过程流程（部分 2）；

图 25 图解说明根据本发明的内容传送系统中用户装置验证服务器和用户装置之间的过程流程；

图 26 图解说明根据本发明的内容传送系统中用户装置验证服务器和商店服务器之间的过程流程；

图 27 图解说明根据本发明的内容传送系统中商店服务器和用户装置之间的过程流程（部分 1）；

图 28 图解说明根据本发明的内容传送系统中商店服务器和用户装置之间的过程流程（部分 2）；

图 29 图解说明在根据本发明的采用内容传送服务器的变型内容传送系统中执行的内容传送过程；

图 30 图解说明在根据本发明的采用内容传送服务器的变型内容传送系统中执行的内容传送过程；

图 31 图解说明根据本发明的变型内容传送系统中执行的内容传送过程；

图 32 图解说明根据本发明的内容传送系统中在实体之间传送的数据的数据结构；

图 33 图解说明根据本发明的内容传送系统中在实体之间传送的数据的数据结构；

图 34 图解说明根据本发明的内容传送系统中在实体之间传送的数据的数据结构；

图 35 图解说明根据本发明其中不执行相互验证的内容传送过程；

图 36 图解说明根据本发明其中不执行相互验证的内容传送过程的变型；

图 37 图解说明根据本发明其中使用电子票券的内容传送过程；

图 38 图解说明根据本发明的内容传送系统中票券发行服务器的结构；

图 39 图解说明根据本发明的内容传送系统中票券发行服务器的票券发行管理数据库；

图 40 图解说明根据本发明的内容传送系统中用户装置的购买管理数据库；

图 41 图解说明根据本发明的内容传送系统中用户装置验证服务器的许可证管理数据库；

图 42 图解说明根据本发明的内容传送系统中内容传送服务器的结构；

图 43 图解说明根据本发明的内容传送系统中内容传送服务器的传送管理数据库；

图 44 图解说明根据本发明的内容传送系统中票券交换服务器的结构；

图 45 图解说明根据本发明的内容传送系统中票券发行服务器的票券交换管理数据库；

图 46 图解说明根据本发明的内容传送系统中在实体之间传送的数据的数据结构；

图 47 图解说明根据本发明的内容传送系统中在实体之间传送的数据的数据结构；

图 48 图解说明根据本发明的内容传送系统中票券发行服务器的状态转变；

图 49 图解说明根据本发明的内容传送系统中用户装置验证服务器的状态转变；

图 50 图解说明根据本发明的内容传送系统中内容传送服务器的

状态转变；

图 51 图解说明根据本发明的内容传送系统中用户装置的状态转变；

图 52 图解说明根据本发明的内容传送系统中票券交换服务器的状态转变；

图 53 图解说明根据本发明其中使用电子票券的内容传送过程的具体例子；

图 54 图解说明根据本发明其中使用日志记录服务器的内容传送过程；

图 55 图解说明根据本发明的内容传送系统中购买日志的数据结构的例子；

图 56 图解说明根据本发明的内容传送系统中日志记录服务器的结构；

图 57 图解说明根据本发明的内容传送系统中用户装置和商店服务器之间的过程流程（部分 1）；

图 58 图解说明根据本发明的内容传送系统中用户装置和商店服务器之间的过程流程（部分 2）；

图 59 图解说明根据本发明的内容传送系统中购买请求数据的格式的例子和销售数据的格式的例子；

图 60 图解说明根据本发明的内容传送系统中可采用的用于产生完整性检查值（ICV）的过程；

图 61 图解说明根据本发明的内容传送系统中用户装置和日志记录服务器之间的过程流程（部分 1）；

图 62 图解说明根据本发明的内容传送系统中用户装置和日志记录服务器之间的过程流程（部分 2）；

图 63 图解说明根据本发明的内容传送系统中内容提供者和日志记录服务器之间的过程流程；

图 64 图解说明根据本发明的内容传送系统中商店服务器和日志记录服务器之间的过程流程；

图 65 图解说明根据本发明的内容传送系统中商店服务器和日志记录服务器之间的过程流程；

图 66 图解说明根据本发明的内容传送系统中采用的属性信息；

图 67 图解说明根据本发明的内容传送系统中可采用的包括属性信息的公共密钥证书；

图 68 图解说明根据本发明的内容传送系统中可采用的公共密钥证书和属性证书；

图 69 图解说明在根据本发明的内容传送系统中执行的新发出公共密钥证书的过程；

图 70 图解说明在根据本发明的内容传送系统中执行的更新公共密钥证书的过程；

图 71 图解说明在根据本发明的内容传送系统中执行的新发出属性证书的过程；

图 72 图解说明在根据本发明的内容传送系统中执行的包括属性检查步骤的内容传送过程；

图 73 图解说明在根据本发明的内容传送系统中执行的包括属性检查步骤的相互验证过程；

图 74 图解说明在根据本发明的内容传送系统中执行的包括属性检查步骤的内容传送过程；

图 75 图解说明在根据本发明的内容传送系统中执行的包括属性检查步骤的数据验证过程；

图 76 图解说明在根据本发明的内容传送系统中执行的包括属性检查步骤的数据验证过程。

具体实施方式

下面结合附图，参考优选实施例更详细地说明本发明。

关于下述项目进行说明：

1. 借助加密内容密钥转换管理内容的传送

1. 1 系统结构：基本内容传送模型 1

1. 2 基本内容传送模型 1 的变型
1. 3 基本内容传送模型 2
2. 利用电子票券管理内容的传送
3. 使用日志记录服务器管理内容的传送
4. 属性证书或者包括属性数据的公共密钥证书的使用
1. 借助加密内容密钥转换管理内容的传送
1. 1 系统结构：基本内容传送模型 1

图 1 图解说明根据本发明一个实施例的内容传送系统和内容传送方法。这里术语“系统”用于描述若干装置的逻辑集合，不必要求所述若干装置被布置在单一机箱中。

在图 1 所示的内容传送系统中，主要部分是向用户装置提供内容的商店服务器（SHOP）100，从商店服务器 100 接收内容的用户装置 200 和用作适当管理内容交换的管理服务器的用户装置验证服务器（DAS）300。注意图 1 中虽然只表示了一个商店服务器 100、一个用户装置 200 和一个用户装置验证服务器，实际的系统可包括若干这样的装置。在这种实际系统中，根据具体的内容交换沿着各种路径传送信息。即，图 1 图解说明内容交换中数据流动的一个例子。

商店服务器

图 2 图解说明图 1 中所示的内容传送系统中的商店服务器 100 的结构。商店服务器 100 具有内容数据库 110，其中保存通过利用内容密钥对要销售的内容加密获得的加密内容数据 K_c （内容）和通过利用用户装置验证服务器（DAS）的公共密钥 K_{pDAS} 对内容密钥 K_c 加密获得的加密内容密钥 $K_{pDAS}(K_c)$ 。如图 2 中所示，每个加密内容数据 K_c （内容）被分配一个内容标识符（ID），从而可利用分配的内容 ID 识别各个加密内容数据 K_c （内容）。

商店服务器 100 还包括用于保存内容销售管理数据的销售管理数据库 120，内容销售管理数据包括内容 ID 和内容 ID 指示的内容出售给的用户装置的标识符。商店服务器 100 还包括从内容数据库 110 抽取将提供给用户装置的内容，响应内容的销售产生将被保存到销售管

理数据库 120 中的销售数据，与用户 200 和用户装置验证服务器 300 通信，并且在通信过程中对数据加密/解密的控制装置 130。

图 3 图解说明销售管理数据库 120 的数据结构。销售管理数据库 120 包括商店处理号，它是由商店服务器产生的用于识别商店服务器进行的内容交换的编号；用于识别已发出内容购买请求的用户装置的装置 ID；当在用户装置和商店之间进行内容交换时由用户装置产生的作为内容交换的标识符的交换 ID；识别交换内容的内容 ID；以及指示和内容交换有关的商店服务器状态的状态信息。如同后面所述，状态将随着内容交易的进行而更新。

控制装置 130 由计算机构成，其中存储加密程序和通信程序，如图 2 中所示，从而控制装置 130 也用作加密装置和通信装置。以安全的方式把控制装置 130 的加密装置在加密过程中使用的密钥数据等保存到控制装置的存储装置中。保存在商店服务器 100 中，供加密过程使用的诸如加密密钥之类的数据包括商店服务器的保密密钥 KsSHOP，商店服务器的公共密钥证书 Cert_SHOP，和发布公共密钥证书的认证机构（CA）的公共密钥 KpCA。

图 4 图解说明控制装置 130 的结构的一个例子。参见图 4，下面说明控制装置 130 的结构。控制单元 131 包括用于执行各种处理程序，从而控制由图 4 中所示的控制装置 130 的各个部分执行的控制过程的中央处理器（CPU）。ROM（只读存储器）132 保存诸如 IPL（初始程序载入器）之类的程序；RAM（随机存取存储器）133 包括用于保存由控制单元 131 执行的程序，例如数据库管理程序、加密程序和通信程序的存储区。RAM 还包括当执行程序时用作工作区的存储区。

显示单元 134 包括诸如液晶显示器或 CRT 之类的显示装置，并在控制单元 131 的控制下在程序的执行过程中显示各种数据，例如将向其传送内容的用户数据。输入单元 135 包括键盘和诸如鼠标之类的指示器。各种命令和数据从这些输入装置被输入输入单元 135 中，输入单元 135 再把命令和数据传送给控制单元 131。HDD（硬盘驱动器）136 保存各种程序，例如数据库管理程序、加密程序和通信程序，另

外还保存各种数据。

驱动器 137 控制对各种存储介质，例如诸如 HD(硬盘)或 FD(软盘)之类磁盘、诸如 CD-ROM(紧致光盘 ROM)之类的光盘、诸如小磁盘之类的磁光盘、或者诸如 ROM 或快速存储器之类的半导体存储器的存取。诸如磁盘之类的各种存储介质被用于存储程序或数据。网络接口 138 用作通过无线网络或有线网络，例如因特网或诸如电话线之类通信线路的通信的通信接口。

使用按照上述方式构成的控制装置 130，商店服务器 100 执行各种过程，例如商店服务器 100 和用户装置 200 之间内容交易中的加密过程或者商店服务器 100 和用户装置验证服务器 300 之间的验证过程。

用户装置验证服务器

图 5 图解说明用户装置验证服务器 (DAS) 300 的结构。用户装置验证服务器 300 具有许可证管理数据库 320。图 6 图解说明许可证管理数据库 320 的结构。许可证管理数据库 320 具有关于内部产生的用于识别内容交换中由用户装置验证服务器 (DAS) 执行的过程的 DAS 过程编号，识别发出内容购买请求的用户装置的装置 ID，当进行内容交换时由用户装置产生的作为内容交换的标识符的交易 ID，识别交易内容的内容 ID、识别执行内容交易的商店服务器的商店 ID，由商店发出的用于识别商店执行的过程的商店过程编号的信息，以及指示和内容交换有关的用户装置验证服务器 (DAS) 的状态信息。如同后面所述，状态随着内容交换的进行而更新。

用户装置验证服务器 (DAS) 300 包括和用户装置 200 或者商店服务器 100 通信并且对通信中的数据加密/解密的控制装置 330。正如商店服务器的控制装置的情况一样，控制装置 330 也用作加密装置和通信装置。按照前面参考图 4 说明的相似方式构成用户装置验证服务器 (DAS) 300。以安全的方式把控制装置 330 的加密装置在加密过程中使用的密钥数据等保存到控制装置的存储装置中。保存在用户装置验证服务器 (DAS) 300 中供加密过程使用的诸如加密密钥之类的的数据包括用户装置验证服务器 (DAS) 300 的保密密钥 KsDAS，用户装

置验证服务器 (DAS) 300 的公共密钥证书 Cert_DAS 和发出公共密钥证书的认证机构 (CA) 的公共密钥 KpCA。

用户装置

图 7 图解说明用户装置 200 的结构。用户装置 200 购买内容并使用购买的内容。用户装置的一个具体例子是再现所购买内容的内容再现装置。用户装置包括购买管理数据库 220。图 8 图解说明购买管理数据库 220 的数据结构。购买管理数据库包括当执行内容交换时由用户装置产生的作为内容交换的标识符的交换 ID，识别交易内容的内容 ID，识别执行内容交易的商店服务器的商店 ID，指示和内容交易相关的用户装置的状态的状态信息，以及识别用户装置的装置 ID。如同后面所述，状态信息随着内容交易的进行而更新。

用户装置 200 包括用于和商店服务器 100 或者用户装置验证服务器 300 通信，并且对通信中的数据加密/解密的控制装置 230。正如商店服务器的情况一样，控制装置 230 也用作加密装置和通信装置。按照类似于前面参考图 4 说明的方式构造用户装置 200。以安全的方式把控制装置 230 的加密装置在加密过程中使用的密钥数据等保存到控制装置的存储装置中。保存在用户装置 200 中供加密过程使用的诸如加密密钥之类的数据包括用户装置的保密密钥 KsDEV，用户装置的公共密钥证书 Cert_DEV，发出公共密钥证书的认证机构 (CA) 的公共密钥 KpCA，以及用作当内容被保存到诸如用户装置的硬盘之类存储装置中时，对内容加密的加密密钥的存储密钥 Ksto。

公共密钥证书

下面参考图 9 说明分别被商店服务器 (SHOP) 100、用户装置 (DEVICE) 200 和用户装置验证服务器 (DAS) 300 持有的公共密钥证书。

公共密钥证书指的是由称为认证机构 (CA) 的第三方发出的证书，以表明公共密钥是被授权用户持有的有效密钥，从而确保可以安全的方式传送利用公共密钥加密的数据，并且可利用该公共密钥充分进行发送方和接收方之间的相互验证。图 9A 表示了公共密钥证书的一种

格式。

在图 9A 中，版本号表明证书格式的版本。

由公共密钥发布机构（CA）向公共密钥证书分配一个序列号。

在字段“签名算法和算法参数”中，说明用于把数字算法写入公共密钥证书中的签名算法和参数。椭圆曲线加密法或 RSA 都可用作签名算法，其中在采用椭圆曲线加密法的情况下，说明参数和密钥长度，而在采用 RSA 的情况下说明密钥长度。

在“发布者”字段中，以知名名称的形式描述公共密钥证书的发布者，即公共密钥认证机构（CA）的名称。

在“证书的有效期”字段中，描述证书的有效期。更具体地说，在该字段中描述起始日期和到期日。

在“公共密钥证书的用户的名称（ID）”字段中，描述向其颁发证书的用户的名称。更具体地说，例如描述用户装置的 ID 或者服务提供者的 ID。

在“用户的公共密钥”字段中，描述和密钥算法或者密钥信息自身的信息。

公共密钥证书还包括认证机构的签名。更具体地说，利用公共密钥认证机构（CA）产生数字签名，并被写入公共密钥证书的数据中。公共密钥证书的用户可利用公共密钥认证机构（CA）的公共密钥验证签名，检查公共密钥证书是否有效，未被篡改。

下面参考图 10 说明基于公共密钥加密法产生数字签名的方法。在图 10 所示的例子中，根据标准 EC-DSA(椭圆曲线数字签名算法)IEEE P1363/D3 产生数字签名。这里举例来说采用椭圆曲线加密法（ECC）对公共密钥加密。注意在本发明中，加密法并不局限于椭圆曲线加密法（ECC），也可采用另一加密法，例如 RSA(Rivest-Shamir-Adleman) 加密法（ANSI X9.31）对公共密钥加密。

如下所述借助图 10 中所示的处理步骤产生数字信号。在步骤 S1 中，设置下述参数：首数 p；椭圆曲线的系数 a 和 b（其中椭圆曲线由 $4a^3+27b^2 \neq 0 \pmod{p}$ 给出）；椭圆曲线的基点 G；G 的阶数 r 和保

密密钥 K_s ($0 < K_s < r$)。在步骤 S2 中，计算消息 M 的散列值，例如 $f = \text{Hash}(M)$ 。

如下所述利用散列函数计算散列值。当把消息输入散列函数时，散列函数把指定消息转换成具有由预定数目的二进制位组成的数据长度的压缩形式，并且输出该结果。散列函数的特征在于难以根据散列值(输出)猜测初始消息(输入)。如果输入散列函数的数据的一个二进制位发生变化，结果是散列值的许多二进制位发生变化。另外难以根据具有相同散列值的大量候选数值中识别出正确的输入数据。散列函数的具体例子包括 MD4、MD5、SHA-1 和 DES-CBC。当采用 DES-CBC 时，最终输出值 MAC (检查值 ICV) 被用作散列值。

在下一步骤 S3 中，产生随机数 u ($0 < u < r$)。在步骤 S4 中，通过将基点 G 乘以 u 确定坐标 $V(X_v, Y_v)$ 。如下定义与椭圆曲线的加法和加倍相关的算术运算。

当 $P = (X_a, Y_a)$, $Q = (X_b, Y_b)$, $R = (X_c, Y_c) = P+Q$ 时，如果 $P \neq Q$ ，则如下进行加法：

$$X_c = \lambda^2 - X_a - X_b$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (Y_b - Y_a) / (X_b - X_a)$$

另一方面，如果 $P = Q$ ，则如下进行加倍：

$$X_c = \lambda^2 - 2X_a$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (3(X_a)^2 + a) / (2Y_a)$$

通过使用上述等式，将点 G 乘以 u (这可如下完成)。首先计算 G 、 $2 \times G$ 、 $4 \times G$ 等等。随后加入对应于通过展开 u 获得的二进制数的为“1”的位的 $2^i \times G$ (这里通过把 G 加倍 i 次得到 $2^i \times G$ ，其中 i 表示从 u 的 LSB 计数的二进制位的位置)。这是易于理解的计算方法，不过该计算需要较长的时间)。

在步骤 S5，计算 $c = X_v \bmod r$ 。在步骤 S6，确定 c 是否等于 0。如果 $c \neq 0$ ，则过程进行到步骤 S7，计算 $d = [(f + cK_s) / u] \bmod r$ 。在步

步骤 S8，确定 d 是否等于 0。如果 $d \neq 0$ ，则过程进行到步骤 S9，其中 c 和 d 被输出为数字信号数据。例如，如果 r 的长度为 160 位，则最后得到的数字信号数据的长度为 320 位。

在步骤 S6 确定 $c=0$ 的情况下，过程返回步骤 S3 产生新的随机数。类似地，如果在步骤 S8 确定 $d=0$ ，则过程返回步骤 S3 产生新的随机数。

下面参考图 11 说明根据公共密钥加密法验证数字签名的方法。在步骤 S11，给出下述参数：消息 M ；首数 p ；椭圆曲线的系数 a 和 b （其中椭圆曲线由 $y^2=x^3+ax+b$ 给出）；椭圆曲线的基点 G ； G 的阶数和公共密钥 G 及 $K_s \times G$ ($0 < K_s < r$)。在步骤 S12 中，确定数字签名数据 c 和 d 是否满足条件： $0 < r$ 和 $0 < d < r$ 。如果该条件被满足，则过程前进到步骤 S13，计算消息 M 的散列值，例如 $f=Hash(M)$ 。之后在步骤 S14 中，计算 $h=1/d \bmod r$ ，并且在步骤 S15 中计算 $h_1=fh \bmod r$ 和 $h_2=ch \bmod r$ 。

在步骤 S16 中，利用在前一步骤中计算的 h_1 和 h_2 计算点 $P=(X_p, Y_p) = h_1 \times G + h_2 \cdot K_s \times G$ 。由于验证数字签名的一方知道公共密钥 G 和 $K_s \times G$ ，因此能够按照和图 10 中步骤 S4 中所示相似的方式使椭圆曲线上的一点乘以标量值。在步骤 S17 中，点 P 为极大点。如果点 P 不是极大点，则过程前进到步骤 S18。（实际上，在步骤 S16 中确定点 P 是否是极大点，因为如果点 P 是极大点，则当计算 $P=(X, Y)$ 和 $Q=(X, -Y)$ 之和时，不能计算 λ ，从而证明 $P+Q$ 是极大点）。在步骤 S18，计算 $X_p \bmod r$ ，并把结果与数字信号数据 c 进行比较。如果结果是等于 c ，则过程进行到步骤 S19，其中确定该数字信号有效。

在确定数字签名有效的情况下，可推断数据未被篡改，从而可推断数字签名是由具有对应于公共密钥的保密密钥的一方产生的。

如果在步骤 S12 中确定数字信号数据 c 或者 d 不满足 $0 < c < r$ 或者 $0 < d < r$ ，则过程跳转到步骤 S20。同样在步骤 S17 中确定点 P 是极大点的情况下，过程跳转到步骤 S20。当在步骤 S18 中确定 $X_p \bmod r$ 不等于数字信号数据 c 时，过程也跳转到步骤 S20。

在步骤 S20 中，确定数字签名无效。这种情况下，推断数据已被篡改或者数据签名由不具有对应于公共密钥的保密密钥的一方产生。

从而，如果公共密钥证书包括由认证机构按照上述方式写入的数字签名，则公共密钥证书的用户可验证数字信号，以检查该证书是否有效，未被篡改。再次参见图 9，用户装置的公共密钥证书 Cert_DEV 被保存到用户装置中，其中如图 9B 中所示，公共密钥证书 Cert_DEV 包括用户装置 ID 和用户装置的公共密钥 KpDEV。图 9C 表示保存在商店服务器中的商店服务器的公共密钥证书 Cert_SHOP，其中公共密钥证书 Cert_SHOP 包括商店 ID 和商店服务器的公共密钥 KcSHOP。图 9D 表示保存在用户装置验证服务器中的用户装置验证服务器的公共密钥证书 Cert_DAS，其中公共密钥证书 Cert_DAS 包括用户装置验证服务器 ID 和用户装置验证服务器的公共密钥 KpDAS。如上所述，用户装置、商店服务器和用户装置验证服务器都具有它们自己的公共密钥证书。

内容购买过程

再次参见图 1，下面说明用户装置从商店服务器购买内容并使用所购买内容的过程。如下所述，在图 1 中该过程按照从 (1) - (20) 的步骤进行。虽然在本实施例中执行实体之间的相互验证（步骤 (1)、(7) 和 (11)），不过根据情况也可省略相互验证。

(1) 相互验证

当用户装置 200 希望从商店服务器 100 购买内容时，首先在用户装置 200 和商店服务器 100 之间进行相互验证。在相互验证中，确定将在其间传送数据的两个装置是否是正确的装置。如果成功通过相互验证，则开始数据传输。最好在相互验证中产生话路密钥，并且在后续的数据传输过程中，通过把话路密钥用作共用密钥对数据加密。

下面参考图 12 说明基于对称密钥加密法的相互验证的过程。在图 12 中所示的过程中，DES 被用作对称密钥加密法，也可采用另一类似的对称密钥加密方案。

首先，装置 B 产生一个 64 位的随机数 Rb，并且把 Rb 和装置 B

的标识符 ID (b) 一起传送给装置 A。响应接收到 Rb 和 ID (b)，装置 A 产生一个 64 位的随机数 Ra，并且按照 Ra、Rb 和 ID (b) 的顺序，用 DES 的 CBC 模式对 Ra、Rb 和 ID (b) 加密。所得到的加密数据被返回给装置 B。

响应接收到加密数据，装置 B 利用密钥 Kab 对接收的数据解密。更具体地说，如下进行接收数据的解密。首先，利用密钥 Kab 对加密数据 E1 解密，获得随机数 Ra。之后，利用密钥 Kab 对加密数据 E2 解密。通过执行所得到的解密数据和 E1 之间异或操作获得 Rb。最后，利用密钥 Kab 对加密数据 E3 解密，并且进行所得到的解密数据和 E2 之间的异或操作获得 ID (b)。在借助上述过程获得的 Ra、Rb 和 ID (b) 中，把 Rb 和 ID (b) 与从装置 B 传来的 Rb 及 ID (b) 进行比较。如果它们等于从装置 B 传来的初始数据，则装置 B 确定装置 A 是授权装置。

之后，装置 B 产生将在验证后使用的话路密钥 Kses（利用随机数产生该话路密钥 Kses）。按照 DES 的 CBC 模式，利用密钥 Kab 以 Rb、Ra 和 Kses 的顺序对 Rb、Ra 和 Kses 加密并将其传送给装置 A。

当收到数据时，装置 A 利用密钥 Kab 对收到的数据解密。可按照与装置 B 执行的解密类似的方式对接收的数据解密，从而这里不对其作进一步的说明。这样获得 Rb、Ra 和 Kses，并把 Rb 和 Ra 与从装置 A 传来的初始数据进行比较。如果成功通过验证，则装置 A 确定装置 B 是授权装置。在成功通过相互验证后执行的通信中，话路密钥 Kses 被用于保证数据保密。

在上述验证中，接收的数据被确定为无效的情况下，相互验证失败并且终止该过程。

现在参考图 13 说明一种使用 160 位椭圆曲线加密法的相互验证方法，所述 160 位椭圆曲线加密法是公共密钥加密方案之一。虽然在图 13 中所示的过程中 ECC 被用作公共密钥加密方案，但是也可采用另一种公共密钥加密方案。此外，密钥大小并不局限于 160 位。在图 13 中，首先装置 B 产生 64 位随机数 Rb，并将其传送给装置 A。当收到

Rb 时，装置 A 产生 64 位随机数 Ra 和小于首数 p 的随机数 Ak。通过把基点 G 乘以 Ak 计算点 Av=Ak × G。随后产生 Ra、Rb 和 Av（X 和 Y 坐标）的数字签名 A.Sig，并且将其和装置 A 的公共密钥证书一起传送给装置 B。这里，Ra 和 Rb 的长度为 64 位，Av 的 X 和 Y 坐标的长度为 160 位，从而产生总长度为 448 位的数字签名。

当使用公共密钥证书时，用户利用用户持有的公共密钥认证机构（CA）410 的公共密钥，验证公共密钥证书的数字签名。如果成功通过数字签名的验证，则从公共密钥证书抽取公共密钥并使用该公共密钥。于是要求公共密钥证书的任意用户具有公共密钥认证机构（CA）的共用公共密钥。可按照和上面参考图 11 说明的相似方式验证数字签名。

当收到装置 A 的公共密钥证书、Ra、Rb、Av 和数字签名 A.Sig 时，数字装置 B 验证从装置 A 接收的 Rb 是否等于装置 B 产生的初始值。如果验证表明 Rb 等于初始值，则随后利用认证机构的公共密钥验证写入装置 A 的公共密钥证书中的数字签名，并且抽取装置 A 的公共密钥。之后，利用抽取的装置 A 的公共密钥验证数字签名 A.Sig。如果成功通过数字签名的验证，则装置 B 把装置 A 看作为授权装置。

之后，装置 B 产生小于首数 p 的随机数 Bk。之后，通过把基点 G 乘以 Bk 计算点 Bv=Bk × G。随后产生 Rb、Ra、Bv（X 和 Y 坐标）的数字签名 B.Sig，并将其和装置 B 的公共密钥证书一起传送给装置 A。

当收到装置 B 的公共密钥证书、Rb、Ra、Bv 和数字签名 B.Sig 时，数字装置 A 验证从装置 B 接收的 Ra 是否等于装置 A 产生的初始值。如果验证表明 Ra 等于初始值，则随后利用认证机构的公共密钥验证写入装置 B 的公共密钥证书中的数字签名，并且抽取装置 B 的公共密钥。之后，利用抽取的装置 B 的公共密钥验证数字签名 B.Sig。如果成功通过数字签名的验证，则装置 A 把装置 B 看作为授权装置。

如果成功通过相互验证，则装置 B 计算 Bk × Av（通过把椭圆曲线上的点 Av 乘以随机数 Bk），并且装置 A 计算 Ak × Bv。在之后进行的通信中，所得到的点的 X 坐标的低位 64 位被用作话路密钥（在

根据对称密钥加密法 64 位密钥被用作对称密钥的情况下)。可根据 Y 坐标产生话路密钥。如果不采用低位 64 位，则也可采用另一组二进制位。在相互验证之后执行的保密通信中，除了数据的加密之外，数字签名也被添加到数据中。

在上述验证中数字签名或者接收的数据被确定为无效的情况下，相互验证失败，过程被终止。

在成功通过相互验证之后进行的通信中，在相互验证过程中产生的话路密钥被用于对数据解密。

(2) 交易 ID 和购买请求数据的产生，及

(3) 购买请求数据的传输

如果成功通过商店服务器 100 和用户装置 200 之间的相互验证，则用户装置 200 产生内容购买请求数据。图 14A 图解说明购买请求数据的数据结构。购买请求数据包括识别内容购买请求发往的商店服务器 100 的商店 ID，根据随机数由用户装置 200 的加密装置产生的作为内容交易的标识符的交易 ID，和指示用户装置所希望购买内容的内容 ID。此外，关于上述数据的用户装置的数字签名被添加到购买请求数据中。购买请求数据和用户装置的公共密钥证书一起被传送给商店服务器 100。注意，如果在相互验证过程中或者在相互验证过程之前，公共密钥证书已被传送给商店，则不需要重新传送公共密钥证书。

(4) 接收数据的验证

当商店服务器 100 从用户装置 200 收到诸如图 14A 中所示的购买请求，则商店服务器 100 验证接收的数据。参考图 15 详细说明该验证过程。首先，商店服务器 100 验证包含在接收数据中的用户装置的公共密钥证书 Cert_DEV (S51)。如前所述通过利用认证机构的公共密钥 KpCA，验证写入公共密钥证书中的认证机构的签名（图 11），完成该验证。

如果成功通过验证，即如果确定公共密钥证书未被篡改（如果步骤 S52 中的答案为是），则过程进行到步骤 S53。但是，如果未通过验证（如果步骤 S52 中的答案为否），则在步骤 S57 中确定公共密钥

证书已被篡改，并且终止使用公共密钥证书的过程。在步骤 S53，从公共密钥证书抽取用户装置的公共密钥 KpDEV。在步骤 S54，根据 KpDEV 验证写入购买请求数据中的用户装置的签名（图 11）。如果成功通过该验证，即如果确定购买请求数据未被篡改（如果步骤 S55 中的答案为是），则在步骤 S56 确定接收的数据是有效的内容购买请求数据。但是，如果没有通过验证（如果步骤 S55 中的答案为否），则在步骤 S57 确定购买请求数据已被篡改，并且终止与购买请求数据相关的过程。

（5）加密内容和加密内容密钥数据 1（商店）的传输

如果商店服务器 100 执行的验证指出购买请求数据有效，未被篡改，则商店服务器 100 把保存在内容数据库 110 中的加密内容和加密内容密钥数据 1（商店）传送给用户装置。即，传送通过利用内容密钥对内容加密得到的加密内容 Kc（内容）和通过利用用户装置验证服务器（DAS）300 的公共密钥对内容密钥 Kc 加密得到的加密内容密钥数据 KpDAS（Kc）。

图 14B 图解说明加密内容密钥数据 1（商店）的数据结构。加密内容密钥数据 1（商店）包括识别已发出内容购买请求的用户装置的用户装置 ID，购买请求数据（除用户装置的公共密钥证书之外图 14A 中所示的数据），响应内容交易的起动由商店服务器 100 产生的商店过程编号和加密内容密钥数据 KpDAS（Kc）。此外，关于上述数据的商店服务器 100 的数字签名被添加到加密内容密钥数据 1（商店）中。加密内容密钥数据 1（商店）和商店服务器 100 的公共密钥证书一起被传送给用户装置 200。注意，如果在相互验证过程中或者相互验证过程之前，公共密钥证书已被传送给用户装置，则不需要重新传送公共密钥证书。

（6）接收数据的验证

当用户装置 200 从商店服务器 100 收到图 14B 中所示的加密内容 Kc（内容）和加密内容密钥数据 1（商店），则用户装置 200 验证加密内容密钥数据 1（商店）。按照上面参考图 15 中所示的处理流程说

明的相似方式进行验证。即，用户装置 200 首先利用认证机构（CA）的公共密钥 KpCA，验证从商店服务器 100 接收的商店服务器的公共密钥证书。之后，用户装置 200 利用从公共密钥证书中抽取的商店服务器的公共密钥 KpSHOP，验证写入图 14B 中所示的加密内容密钥数据 1（商店）中的商店签名。

（7）相互验证

如果在从商店服务器 100 接收加密内容 Kc（内容）和加密内容密钥数据 1（商店）之后，用户装置 200 完成了加密内容密钥数据 1（商店）的验证，则用户装置 200 随后访问用户装置验证服务器 300。当访问用户装置验证服务器 300 时，在用户装置和用户装置验证服务器 300 之间进行相互验证。以和商店服务器 100 和用户装置 200 之间的前述相互验证相似的方式执行这种相互验证。

（8）加密密钥数据（用户装置）和加密内容密钥转换请求的传输

如果成功通过用户装置 200 和用户装置验证服务器 300 之间的相互验证，则用户装置 200 把包括从商店服务器 100 接收的加密内容密钥 KpDAS（Kc）的加密密钥数据（用户装置）传送给用户装置验证服务器 300，用户装置 200 请求用户装置验证服务器 300 执行加密内容密钥的转换。

图 14C 图解说明加密内容密钥数据（用户装置）的数据结构。加密内容密钥数据（用户装置）包括识别加密内容密钥的转换请求发往的用户装置验证服务器 300 的用户装置验证服务器 ID 和从商店服务器 100 接收的加密内容密钥数据（除商店公共密钥证书外图 14B 中所示的数据）。此外，关于上述数据的用户装置 200 的数字签名被添加到加密内容密钥数据（用户装置）中。加密内容密钥数据（用户装置）和商店服务器 100 的公共密钥证书以及用户装置 200 的公共密钥证书一起被传送给用户装置验证服务器 300。在用户装置验证服务器 300 已具有用户装置的公共密钥证书和商店服务器的公共密钥证书的情况下，不需要重新传送这些证书。

（9）当用户装置验证服务器 300 从用户装置 200 收到加密内容密

钥数据（用户装置）和加密内容密钥转换请求（图 14C）时，用户装置验证服务器 300 验证加密内容密钥转换请求。按照上面参考图 15 中所示的处理流程说明的相似方式进行验证。即，用户装置 300 首先利用认证机构（CA）的公共密钥 KpCA 验证从用户装置 200 接收的用户装置的公共密钥证书。之后，用户装置 300 利用从公共密钥证书抽取的用户装置的公共密钥 KpDEV 验证写入图 14A 中所示的购买请求数据中的数字签名和写入图 14C 中所示的加密内容密钥数据（用户装置）中的数字签名。此外，用户装置 300 利用认证机构（CA）的公共密钥 KpCA 验证商店服务器的公共密钥证书。之后，用户装置 300 利用从公共密钥证书抽取的商店服务器的公共密钥 KpSHOP，验证写入加密内容密钥数据 1（用户装置）中的商店签名（图 14C 中由（5）表示）。

（10）加密内容密钥的转换

在由用户装置验证服务器 300 执行的关于加密内容密钥数据（用户装置）和从用户装置 200 接收的加密内容密钥转换请求的验证中，如果确定密钥转换请求有效，则用户装置验证服务器（DAS）300 利用用户装置验证服务器 300 的保密密钥 KsDAS 对包含在加密内容密钥数据（用户装置）中的加密内容密钥，即通过利用用户装置验证服务器（DAS）300 的公共密钥 KpDAS 对内容密钥 Kc 加密获得的加密数据 KpDAS（Kc）解密，从而获得内容密钥 Kc。此外，用户装置验证服务器 300 利用用户装置的公共密钥 KpDEV 对获得的内容密钥 Kc 加密，从而产生加密的内容密钥 KpDEV（Kc）。即，密钥被转换，使得 KpDAS（Kc）→ Kc → KpDEV（Kc）。

图 16 图解说明由用户装置验证服务器 300 执行的加密内容密钥转换过程。首先，用户装置验证服务器（DAS）300 从接收自用户装置 200 的加密内容密钥数据（用户装置）中抽取利用用户装置验证服务器（DAS）300 的公共密钥 KpDAS 加密的内容密钥数据 KpDAS（Kc）（步骤 S61）。之后，用户装置验证服务器 300 利用用户装置验证服务器 300 的保密密钥 KsDAS 对加密内容密钥数据解密，从而获得内容

密钥 Kc（步骤 S62）。此外，用户装置验证服务器 300 利用用户装置的公共密钥 KpDEV 重新对获得的内容密钥 Kc 加密，从而产生加密内容密钥 KpDEV（Kc）（步骤 S63）。在完成上述过程之后，在许可证管理数据库（图 6）中描述的状态被设置为“密钥转换完成”。

（11）相互验证

如果用户装置验证服务器 300 完成了加密内容密钥的密钥转换，则用户装置验证服务器 300 随后访问商店服务器。当访问商店服务器 100 时，在用户装置验证服务器 300 和商店服务器 100 之间进行相互验证。按照和商店服务器 100 和用户装置 200 之间的上述相互验证相似的方式进行这种相互验证。

（12）加密内容数据的传输

如果成功通过用户装置验证服务器 300 和商店服务器 100 之间的相互验证，则用户装置验证服务器 300 把加密内容密钥数据（DAS）传送给商店服务器 100。

图 17D 图解说明加密内容密钥数据（DAS）的数据结构。加密内容密钥数据（DAS）包括识别内容购买请求发往的商店服务器 100 的商店 ID，加密内容密钥数据（用户装置）（除商店的公共密钥证书和用户装置的公共密钥证书外图 14C 中所示的数据），和借助上述密钥转换过程由用户装置验证服务器 300 产生的加密内容密钥数据 KpDEV（Kc）。此外，关于上述数据的用户装置 300 的数字签名被添加到加密内容密钥数据（DAS）中。加密内容密钥数据（DAS）和用户装置验证服务器 300 的公共密钥证书以及用户装置 200 的公共密钥证书一起被传送给商店服务器。在商店服务器已具有这些证书的情况下，不需要重新传送这些证书。

在可认为用户装置验证服务器 300 高度可靠的情况下，可不以图 17D 中所示的形式构成加密内容密钥数据（DAS），在图 17D 中所示的形式中，以其初始形式包括由用户装置产生的加密内容密钥数据（用户装置）（由（8）表示），相反可以这样构成加密内容密钥数据（DAS），如图 18D' 中所示，用户装置 ID、交易 ID、内容 ID、商店过程编号和

利用用户装置的公共密钥加密的内容密钥 KpDEV (Kc) 被用户装置验证服务器 300 抽取，并且加密内容密钥数据 (DAS) 由抽取的这些数据加上用户装置验证服务器 300 的数字签名构成。这种情况下，不必验证加密内容密钥数据 (用户装置) (图 17D 中由 (8) 表示)，从而只须把用户装置验证服务器 300 的公共密钥证书附到加密内容密钥数据 (DAS) 上即可。

(13) 接收数据的验证

当商店服务器 100 从用户装置验证服务器 300 接收加密内容密钥数据 (DAS) (图 17D) 时，商店服务器 100 验证加密内容密钥数据 (DAS)。按照上面参考图 15 中所示的处理流程说明的相似方式执行该验证。即，商店服务器 100 首先利用认证机构 (CA) 的公共密钥 KpCA 验证从用户装置验证服务器 300 接收的用户装置验证服务器的公共密钥证书。之后，商店服务器 100 利用用户装置验证服务器 300 的公共密钥 KpDAS 验证写入图 17D 所示的加密内容密钥数据 (DAS) 中的数字签名。此外，商店服务器 100 利用认证机构 (CA) 的公共密钥 KpCA 验证用户装置的公共密钥证书。之后，商店服务器 100 利用从公共密钥证书抽取的用户装置的公共密钥 KpDEV，验证由用户装置写入包含在图 17D 中所示的加密内容密钥数据 (DAS) 中的 (8) 加密内容密钥数据 (用户装置) 中的数字签名。另一方面，可利用商店服务器 100 的公共密钥 KpSHOP 执行加密内容密钥数据 (用户装置) 的验证。

在商店服务器 100 接收呈上面参考图 18D' 说明的简化形式的加密内容密钥数据 (DAS) 的情况下，商店服务器 100 利用认证机构 (CA) 的公共密钥 KpCA 验证用户装置验证服务器的公共密钥证书，随后商店服务器 100 利用用户装置验证服务器 300 的公共密钥 KpDAS，验证图 18D' 中所示的加密内容密钥数据 (DAS) 的数字签名。

(14) 相互验证，和

(15) 加密内容密钥请求的传输

之后，用户装置 200 把加密内容密钥请求数据传送给商店服务器

100. 在和传送前一请求的话路不同的话路中传送加密内容密钥请求数据的情况下，再次执行相互验证，并且只有当成功通过相互验证时才把加密内容密钥请求数据从用户装置 200 传送给商店服务器 100。

图 17E 图解说明加密内容密钥请求数据的数据结构。加密内容密钥请求数据包括识别内容购买请求发往的商店服务器 100 的商店 ID，由用户装置 200 产生的用于识别内容交易的交易 ID，指出用户装置所希望购买内容的内容 ID，和包含在由商店产生并且作为内容密钥数据 1（商店）传送给用户装置 200 的数据（图 14B）中的商店过程编号。此外，关于上述数据的用户装置的数字签名被添加到加密内容密钥请求数据中。加密内容密钥请求数据和用户装置的公共密钥证书一起被传送给商店服务器 100。在商店服务器已具有该证书的情况下，不需要重新传送该证书。

（16）验证，和

（17）收费过程

当商店服务器 100 从用户装置收到加密内容密钥请求数据时，商店服务器 100 验证加密内容密钥请求数据。按照上面参考图 15 说明的相似方式执行该验证过程。在完成数据验证之后，商店服务器 100 执行与内容交易相关的收费过程。执行该收费以便从用户的账户收取内容的费用。在内容的版权持有者、商店和用户装置验证服务器等等之间分配关于内容收取的费用。

注意在收费过程之前，要求用户装置验证服务器 300 执行加密内容密钥转换，从而不能只通过商店服务器 100 和用户装置之间的过程就执行收费过程。除非已进行了密钥转换，否则用户装置 200 不能对加密内容密钥解码，从而用户装置 200 不能使用内容。其中用户装置验证服务器执行转换的所有内容交易的历史被记录到前面参考图 6 说明的许可证管理数据库中，从而可监控和管理需要收费过程的任意内容交易。这可防止任意商店独自进行内容销售交易，从而防止未经授权销售内容。

（18）加密内容密钥数据 2（商店）的传输

在完成收费过程之后，商店服务器 100 把加密内容密钥数据 2(商店)传送给用户装置 200。

图 17F 图解说明加密内容密钥数据 2(商店)的数据结构。加密内容密钥数据 2(商店)包括识别发出加密内容密钥请求的用户装置 200 的用户装置 ID，和从用户装置验证服务器 300 接收的加密内容密钥数据 (DAS) (除用户装置的公共密钥证书和用户装置验证服务器的公共密钥证书外图 17D 中所示的数据)。此外，关上上述数据的商店服务器 100 的数字签名被添加到加密内容密钥数据 2(商店)中。加密内容密钥数据 2(商店)和商店服务器 100 的公共密钥证书以及用户装置验证服务器 300 的公共密钥证书一起被传送给用户装置 200。在用户装置 200 已具有用户装置验证服务器的公共密钥证书和商店服务器的公共密钥证书的情况下，不需要重新传送这些证书。

在用户装置验证服务器 300 由高度可靠的第三方管理，并且商店服务器 100 从用户装置验证服务器 300 接收呈上面参考图 18D'说明的简化形式的加密内容密钥数据 (DAS) 的情况下，商店服务器 100 把呈图 18F'中所示形式的加密内容密钥数据 2(商店)传送给用户装置。即，呈图 18D'中所示简化形式的包括商店服务器签名的加密内容密钥数据 (DAS) 和商店服务器 100 的公共密钥证书以及用户装置验证服务器 300 的公共密钥证书一起被传送给用户装置 200。

(19) 接收数据的验证

当用户装置 200 从商店服务器 100 收到加密内容密钥数据 2(商店)时，用户装置 200 验证加密内容密钥数据 2(商店)。按照和上面参考图 15 中所示的流程说明的相似方式进行验证。即，用户装置 200 首先利用认证机构 (CA) 的公共密钥 KpCA 验证从商店服务器 100 接收的商店服务器的公共密钥证书。之后，用户装置 200 利用从公共密钥证书抽取的商店服务器 100 的公共密钥 KpSHOP 验证写入图 17F 中所示的加密内容密钥数据 2(商店)中的数字签名。此外，用户装置 200 利用认证机构 (CA) 的公共密钥 KpCA 验证用户装置验证服务器 300 的公共密钥证书。之后，用户装置 200 利用从公共密钥证

书抽取的用户装置验证服务器 300 的公共密钥 KpDAS, 验证写入包含在图 17F 中所示的加密内容密钥数据 2(商店)中的(12)加密内容密钥数据(DAS)中的数字签名。另一方面, 可利用用户装置 200 的公共密钥 KpDEV 执行加密内容密钥数据(用户装置)的验证。

(20) 数据的存储

在用户装置 200 验证了从商店服务器 100 接收的加密内容密钥数据 2(商店)之后, 用户装置 200 利用用户装置 200 的保密密钥 KsDEV 对已利用用户装置 200 的公共密钥 KpDEV 加密并且包含在加密内容密钥数据 2(商店)中的加密内容密钥 KpDEV(Kc)解密, 随后用户装置 200 利用用户装置的存储密钥 Ksto 对内容密钥加密, 从而产生加密内容密钥 Ksto(Kc)。所得到的加密内容密钥 Ksto(Kc)被保存到用户装置 200 的存储装置中。当使用内容时, 利用存储密钥 Ksto 对加密内容密钥 Ksto(Kc)解密, 从而获得内容密钥 Kc, 并且利用获得的内容密钥 Kc 对加密内容 Kc(内容)解密, 从而再现内容。

图 19 图解说明用户装置 200 执行的获得并保存内容密钥 Kc 的过程的流程。首先, 用户装置 200 从接收自商店服务器 100 的加密内容密钥数据 2(商店)中抽取利用用户装置 200 的公共密钥 KpDEV 加密的加密内容密钥 KpDEV(Kc)(步骤 S71), 用户装置 200 利用用户装置 200 的保密密钥 KsDEV 对加密内容密钥 KpDEV(Kc)解密, 从而抽取内容密钥 Kc(步骤 S72)。

此外, 利用用户装置的存储密钥对内容密钥 Kc 加密, 从而产生加密内容密钥 Ksto(Kc), 并且把所得到的加密内容密钥 Ksto(Kc)保存到用户装置 200 的存储装置(内部存储器)中(步骤 S73)。

当完成上述过程时, 用户装置能够获得加密内容 Kc(内容)以及和加密内容相关的内容密钥 Kc, 从而用户装置能够使用所述内容。注意如上所述, 只有当用户装置验证服务器 300 已完成加密内容密钥转换时, 用户装置 200 才能使用内容。这意味着在不向用户装置验证服务器 300 通知销售交易, 商店服务器 100 就不能向用户装置 200 销售内容, 从而用户装置 200 不能使用内容, 除非把销售交易告知用户装

置验证服务器 300。用户装置验证服务器执行密钥转换的所有内容交易的历史被保存到前面参考图 6 说明的许可证管理数据库中，从而可监控和管理需要收费过程的任意内容交易。因此能够在内容的版权持有者、商店、用户装置验证服务的所有者等等之间恰当地分配通过收费过程收取的内容费用。

装置状态的转变

图 1 中所示的商店服务器 100、用户装置 200 和用户装置验证服务器 (DAS) 300 根据指示过程状态的状态信息，确定与内容交易相关的一系列过程内的下一过程。为图 3 中所示的商店服务器的销售管理数据库、图 6 中所示的用户装置验证服务器的许可证管理数据库和图 8 中所示的用户装置的购买管理数据库中的各个内容交易保存并管理状态信息。

下面参考图 20 说明商店服务器 100 的状态转变。当商店服务器从用户装置 200 收到内容购买请求数据时，商店服务器起动一个过程(图 1 中所示的过程 (3))。当收到来自于用户装置 200 的数据时，商店服务器 100 验证接收的数据。如果成功通过验证，则状态被设置成“购买请求被接受”状态。但是，如果数据验证指示购买请求无效，则立即或者在重复该过程预定次数之后终止该过程（在本具体例子中为购买请求接受过程），并且把状态设置成“购买请求被拒绝”状态。只有当状态处于“购买请求被接受”状态时过程才进行到下一步骤。

如果状态被改变成“购买请求被接受”状态，则商店服务器 100 把加密内容密钥数据 1 (商店) 传送给用户装置 200 (图 1 中的过程步骤 (5))。如果商店服务器 100 收到来自于 YR 的确认响应时，状态被改变成“密钥 1 被传送”状态。但是，如果密钥数据 1 的传送已失败，则立即或者在重复该过程预定次数之后终止该过程（在本具体情况下为密钥数据 1 的传送），并且把状态设置成“密钥 1 的传送失败”状态。只有当状态处于“密钥 1 的输送失败”状态时该过程才进行到下一步骤。

如果状态被改变成“密钥 1 被传送”状态，则商店服务器 100 接收来自于用户装置验证服务器的加密内容密钥数据（DAS）（图 1 中的过程过程（12））并验证接收的数据。如果成功通过验证，则状态被设置成“完成密钥的接收”状态。但是，如果数据验证指出接收的数据不是有效的加密内容密钥数据（DAS），则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为密钥的接收），并且把状态设置成“密钥的接收失败”状态。只有当状态处于“完成密钥的接收”状态时过程才进行到下一步骤。

如果状态被改变成“完成密钥的接收”状态时，商店服务器 100 从用户装置 200 接收加密内容密钥传输请求数据（图 1 中的过程步骤（15）），并验证接收的数据。如果成功通过验证，则状态被改变成“完成加密内容密钥传输请求的接收”状态。但是如果数据验证指出加密内容密钥传输请求数据无效，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为加密内容密钥传输请求数据的接收），并且随后把状态设置成“加密内容密钥请求接收失败”状态。只有当状态处于“完成加密内容密钥传输请求的接收”状态时过程才进行到下一步骤。

如果状态被改变成“完成加密内容密钥传输请求的接收”状态，则商店服务器 100 执行收费过程（图 1 中的过程步骤（17））。在完成收费过程之后，状态被改变成“收费结束”状态。但是，如果由于从用户装置的特定账户接收费用的故障的缘故，没有成功完成收费过程，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为收费过程），并且把状态设置成“收费失败”状态。只有当状态处于“收费完成”状态时过程才进行到下一步骤。

如果状态被改变成“收费完成”状态，则商店服务器 100 把加密内容密钥数据 2（商店）传送给用户装置（图 1 中的过程步骤（18））。在完成加密内容密钥数据 2（商店）的传送之后，如果商店服务器 100 接收来自用户装置的确认响应时，商店服务器 100 把状态设置成“密钥 2 传送状态”。但是，如果密钥数据 2（商店）的传送失败，则状

态被改变成“密钥 2 传送失败”状态。只有当状态处于“密钥 2 传送”状态时，过程才进行到下一步骤，在本具体情况下，所述下一步骤是结束步骤。如果状态处于“密钥 2 传送失败”状态，则不执行后续步骤，而是立即或者在重复该过程预定次数之后终止该过程（本具体情况下为密钥数据 2（商店）的传送）。在商店服务器 100 中，对于各个内容交易按照上述方式改变状态。

下面参考图 21 说明用户装置 200 的状态转变。用户装置 200 通过向商店服务器 100 传送内容购买请求数据（图 1 中所示的过程（3））启动一个过程。如果用户装置 200 从商店服务器 100 接收指出内容购买请求数据已被商店服务器 100 成功接收的响应，则状态被设置成“购买请求传送完成”状态。但是，如果没有从商店服务器 100 接收指出商店服务器 100 已成功接收内容购买请求数据的响应，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为购买请求的传输），并且把状态设置成“购买请求传输失败”状态。只有当状态处于“购买请求传送完成”状态时过程才进行到下一步骤。

如果状态被改变成“购买请求传送完成”状态，则用户装置 200 接收来自于商店服务器 100 的加密内容密钥数据 1（商店）（图 1 中的过程步骤（5）），并且验证接收的数据。如果从商店服务器 100 成功接收加密内容密钥数据，则状态被设置成“完成密钥 1 的传送”状态。但是，如果数据验证指出接收的数据不是有效的加密内容密钥数据，则立即或者在重复预定次数之后终止该过程（本具体情况下为密钥 1 的接收），并且状态被设置成“密钥 1 的接收失败”状态。只有当状态处于“密钥 1 的接收完成”状态时过程才进行到下一步骤。

如果状态被改变成“完成密钥 1 的传送”状态，则用户装置 200 把加密内容密钥数据（用户装置）传送给用户装置验证服务器 300（图 1 中的处理步骤（8））并且等待来自用户装置验证服务器 300 的响应。如果从用户装置验证服务器 300 收到确认响应，则状态被改变成“完成密钥的传送”状态。但是，如果没有收到确认响应，则立即或者在

重复预定次数之后终止该过程（本具体情况下为密钥的传送），并且把状态设置成“密钥的传送失败”状态。只有当状态处于“完成密钥的传送”状态时过程才进行到下一步骤。

如果状态被改变成“完成密钥的传送”状态，则用户装置200把加密内容密钥传送请求数据传送给商店服务器300（图1中的过程步骤（15）），并等待来自商店服务器100的响应。如果从商店服务器100收到确认响应，则状态被改变成“完成加密内容密钥传送请求的传送”状态。但是，如果没有收到确认响应，则立即或者在重复预定次数之后终止该过程（本具体情况下为加密内容密钥传送请求的传送），并且把状态设置成“加密内容密钥传送请求的传送失败”状态。只有当状态处于“完成加密内容密钥传送请求的传送”状态时该过程才进行到下一步骤。

如果状态被改变成“完成加密内容密钥传送请求的传送”状态，则用户装置200从商店服务器100接收加密内容密钥数据2（商店）（图1中的过程步骤（18））并验证接收的数据。如果成功通过数据验证，则状态被设置成“完成密钥2的接收”状态。立即或者在重复该过程预定次数之后终止该过程（本具体情况下为加密内容密钥数据2（商店）的接收），并且状态被设置成“密钥2的接收失败”状态。如果状态处于“完成密钥2的接收”状态，则过程结束。在装置200中，对于各个内容交易按照上述方式改变状态。

下面参考图22说明用户装置验证服务器300的状态转变。当用户装置验证服务器300从用户装置200接收加密内容密钥数据（用户装置）（图1中的过程（8））时，用户装置验证服务器300起动一个过程。当从用户装置200接收数据时，用户装置验证服务器300验证接收的数据。如果成功通过验证，则状态被设置成“完成密钥的接收”状态。但是，如果数据验证指出接收的数据无效，则立即或者在重复预定次数之后终止该过程（本具体情况下为加密内容密钥数据（用户装置）的接收），并且把状态设置成“密钥接收失败”状态。只有当状态处于“完成密钥接收”状态时过程才进行到下一步骤。

如果状态被改变成“完成密钥接收”状态，则用户装置验证服务器 300 执行内容密钥转换过程（图 1 中的过程步骤（10）。如果成功完成内容密钥转换，则状态被设置成“完成密钥转换”状态。这里，假定总是成功完成密钥转换，因此状态总是被设置成“完成密钥转换”状态。

如果状态被改变成“完成密钥转换”状态，则用户装置验证服务器 300 把加密内容密钥数据（DAS）传送给商店服务器 100（图 1 中的过程步骤（12））并等待来自商店服务器 100 的响应。如果从商店服务器 100 收到确认响应，则状态被改变成“完成密钥传送”状态。但是，如果没有收到确认响应，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为加密内容密钥数据（DAS）的传送），并且把状态设置成“密钥传送失败”状态。如果状态处于“完成密钥传送”状态，则过程结束。在用户装置验证服务器 300 中，对于各个内容交易按照上述方式改变状态。

内容购买过程

响应从用户装置 200 向商店服务器 100 发出内容购买请求，如下所述在商店服务器 100、用户装置 200 和用户装置验证服务器 300 之间执行数据传送/接收。该过程包括下述 A、B、C 和 D 四个部分。

A. 商店服务器和用户装置之间的过程（图 1 中的过程步骤（1）-（6））

该过程的部分 A 包括用户装置 200 和商店服务器 100 之间的相互验证步骤，用户装置 200 向商店服务器 100 传送内容购买请求的步骤和商店服务器 100 向用户装置 200 传送密钥 1（商店）的步骤。

B. 用户装置验证服务器和用户装置之间的过程（图 1 中的过程步骤（7）-（9））

该过程的部分 B 包括进行用户装置 200 和用户装置验证服务器 300 之间的相互验证的步骤，传送加密内容密钥数据的步骤，用户装置验证服务器 300 验证接收的数据的步骤。

C. 用户装置验证服务器和商店服务器之间的过程（图 1 中的过

程步骤 (11) - (13))

该过程的部分 C 包括进行用户装置验证服务器 300 和商店服务器 100 之间的相互验证的步骤，传送加密内容密钥数据 (DAS) 的步骤和商店服务器 100 验证接收数据的步骤。

D. 商店服务器和用户装置之间的过程 (图 1 中的过程步骤 (14) - (19))

该过程的部分 D 包括进行用户装置 200 和商店服务器 100 之间的相互验证的步骤，用户装置 200 把加密内容密钥请求数据传送给商店服务器 100 的步骤，商店服务器 100 把密钥 2 (商店) 传送给用户装置 200 的步骤和用户装置 200 验证接收数据的步骤。

首先参考图 23 和 24 说明在商店服务器和用户装置之间执行的该过程的部分 A (图 1 中的步骤 (1) - (6))。

在图 23 和 24 中，商店服务器执行的过程表示在左侧，用户装置执行的过程表示在右侧。在该流程图中，商店服务器执行的步骤由 S10xx 表示，用户装置执行的步骤由 S20xx 表示，用户装置验证服务器执行的步骤由 S30xx 表示。

在该过程的开始，如图 23 中所示，在商店服务器和用户装置之间进行相互验证 (步骤 S1001 和 S2001)。按照上面参考图 12 和 13 说明的相似方式进行相互验证。在后续数据传输中，在根据需要利用在相验证过程中产生的话路密钥进行加密之后传送数据。如果成功通过相互验证，则商店服务器把新的商店过程编号作为新的过程条目添加到销售管理数据库 (图 3) 中 (步骤 S1003)。

另一方面，如果成功通过相互验证，则用户装置根据例如随机数产生应用于当前内容交易的交易 ID，并且用户装置把交易 ID 作为新的条目添加到购买数据库 (图 8) 中 (步骤 S2003)。之后，用户装置把内容购买请求数据传送给商店服务器 (步骤 S2004)。即，传送图 14A 中所示的 (3) 购买请求数据。

如果商店服务器从用户装置接收内容购买请求数据 (步骤 S1004)，则商店服务器验证接收的数据 (步骤 S1005)。根据上面参

考图 11 说明的流程进行数据验证。如果接收数据的验证结果指出数据未被篡改并且该数据有效，则商店服务器向用户装置传送指示已成功接收内容购买请求数据的消息（步骤 S1008），并且商店服务器把在销售管理数据库中描述的状态设置成“完成购买请求的接收”状态（步骤 S1010）。如果接收数据的验证结果指出数据已被篡改，并且该数据无效，商店服务器向用户装置传送指示接收数据无效的消息（步骤 S1007），并且商店服务器设置在销售管理数据库中描述的状态，以便指出购买请求已被拒绝（步骤 S1009）。

当收到数据已被商店服务器成功接收的消息时（步骤 S2005 和 S2006），用户装置设置在购买管理数据库中描述的状态，以便指出购买请求已被成功传送。但是，在用户装置从商店服务器收到指出购买请求已被拒绝的消息时（步骤 S2005 和 S2006），用户装置设置在购买管理数据库中描述的状态，以便指出购买请求已被拒绝。

在商店服务器已把在销售管理数据库中描述的状态设置成指出购买请求已被接受（步骤 S1010）之后，商店服务器产生加密内容密钥数据 1（商店）（图 14B）（步骤 S1011），并且把利用内容密钥 Kc 加密的加密内容 Kc（内容）传送给用户装置（步骤 S1012）。此外，商店服务器把图 14B 中所示的加密内容密钥数据 1（商店）传送给用户装置（步骤 S1013）。

在把在购买管理数据库中描述的状态设置成指出购买请求已被成功传送（步骤 S2007）之后，用户装置从商店服务器接收利用内容密钥 Kc 加密的加密内容 Kc（内容）（步骤 S2009），此外还接收加密内容密钥数据 1（商店）（图 14B）（步骤 S2010）。

在步骤 S2021 中，用户装置进行在步骤 S2009 和 S2010 中接收的数据的验证（图 11）。如果接收数据的验证结果指出数据未被篡改，并且数据有效，则用户装置向商店服务器传送指出数据已被成功接收的消息（步骤 S2023），并且用户装置把在购买管理数据库中描述的状态设置成指出密钥 1 已被成功接收（步骤 S2025）。如果接收数据的验证结果指出数据已被篡改，并且数据无效，则用户装置向商店服

务器传送指出接收数据无效的消息（步骤 S2024），并且用户装置把在购买管理数据库中描述的状态设置成指出密钥 1 的接收已失败（步骤 S2026）。之后，用户装置断开与商店服务器的连接（步骤 S2027）。

如果商店服务器从用户装置收到表示数据已被用户装置成功接收的消息（步骤 S1021），则商店服务器把在销售管理数据库中描述的状态设置成指出密钥 1 已被成功传送（步骤 S1024）。但是，如果来自用户装置的消息表示数据无效，则商店服务器把在销售管理数据库中描述的状态设置成指出密钥 1 的传送已失败（步骤 S1023）。之后，商店服务器断开与用户装置的连接（步骤 S1025）。

在步骤 S1002 和 S2002 中的相互验证失败的情况下，或者在步骤 S1009 中状态被设置成“购买请求接收失败”状态的情况下，或者在步骤 S2008 中状态被设置成“购买请求传送失败”的情况下，终止该过程并关闭通信连接。

现在参考图 25 中所示的流程图说明在用户装置验证服务器和用户装置之间执行的该过程的部分 B（图 1 中的步骤（7）-（9））。

首先进行用户装置验证服务器和用户装置之间的相互验证（步骤 S3001 和 S2031）。按照上面参考图 12 和 13 说明的相似方式执行相互验证。在后续数据传输中，在根据需要利用在相互验证过程中产生的话路密钥加密之后传送数据。如果成功通过相互验证，则用户装置验证服务器把新的 DAS 过程编号作为新的过程条目添加到许可证管理数据库（图 6）中（步骤 S3003）。

另一方面，如果成功通过相互验证，则用户装置产生加密内容密钥数据（用户装置）（图 14C）（步骤 S2033），并将其传送给用户装置验证服务器（步骤 S2034）。

如果用户装置验证服务器从用户装置收到加密内容密钥数据（用户装置）（步骤 S3004），则用户装置验证服务器验证接收的数据（步骤 S3005）。根据上面参考图 11 说明处理流程进行数据验证。如果接收数据的验证结果指出数据未被篡改，并且数据有效，则用户装置验证服务器向用户装置传送指出加密内容密钥数据（用户装置）已被成

功接收的消息（步骤 S3008），并且用户装置验证服务器把在许可证管理数据库中描述的状态设置成指出密钥已被成功接收（步骤 S3010）。如果接收数据的验证结果指出数据已被篡改并且数据无效，则用户装置验证服务器向用户装置传送指出接收的数据无效的消息（步骤 S3007），并且用户装置验证服务器把在许可证管理数据库中描述的状态设置成指出密钥的接收已失败（步骤 S3009）。之后，用户装置验证服务器关闭与用户装置的连接（步骤 S3011）。

如果用户装置从用户装置验证服务器收到确认响应（步骤 S2035 和 S2036），则用户装置把在销售管理数据库中描述的状态设置成“完成密钥传送”状态（步骤 S2037）。但是在用户装置从用户装置验证服务器收到否定确认响应（步骤 S2035 和 S2036）的情况下，用户装置把在销售管理数据库中描述的状态设置成“密钥传送失败”状态（步骤 S2038）。之后，断开与用户装置验证服务器的连接（步骤 S2039）。

在步骤 S3002 和 S2032 中的相互验证已失败的情况下，终止该过程并且断开连接。

下面参考图 26 中所示的流程图说明在用户装置验证服务器和商店服务器之间进行的该过程的部分 C（图 1 中的步骤（11）-（13））。

首先进行用户装置验证服务器和商店服务器之间的相互验证（步骤 S3021 和 S1031）。按照上面参考图 12 和 13 说明的相似方式进行该相互验证。在后续数据传送中，在根据需要利用在相互验证过程中产生的话路密钥加密之后传送数据。如果成功通过相互验证，则用户装置验证服务器产生加密内容密钥数据(DAS)（图 17D）（步骤 S3023），并将其传送给商店服务器（步骤 S3024）。

另一方面，如果成功通过相互验证，则商店服务器从用户装置验证服务器接收加密内容密钥数据(DAS)（图 17D）（步骤 S1033），并且验证接收的数据（步骤 S1034）。根据上面参考图 11 说明的处理流程执行数据验证。如果接收数据的验证结果指出数据未被篡改并且数据有效，则商店服务器向用户装置验证服务器传送确认响应（步骤

S1036），并把在销售管理数据库中描述的状态设置成“完成密钥的接收”状态（步骤 S1038）。如果接收数据的验证结果指出数据已被篡改并且数据无效，则商店服务器向用户装置验证服务器传送否定确认响应（步骤 S1037），并把在销售管理数据库中描述的状态设置成“密钥接收失败”状态（步骤 S1039）。之后，断开与用户装置验证服务器的连接（步骤 S1040）。

如果用户装置验证服务器从商店服务器收到确认响应（步骤 S3025 和 S3026），则用户装置验证服务器把在许可证管理数据库中描述的状态设置成“完成密钥传送”状态（步骤 S3028）。但是，在用户装置验证服务器从商店服务器收到否定确认响应（步骤 S3025 和 S3026）的情况下，在许可证管理数据库中描述的状态被设置成“密钥传送失败”状态（步骤 S3027），并且断开与商店服务器的连接（步骤 S3029）。

在步骤 S3022 和 S1032 中的相互验证失败的情况下，过程被终止，并且关闭通信连接。

下面参考图 27 和 28 说明在商店服务器和用户装置之间进行的部分 D 过程（图 1 中的步骤（14）-（19））。

过程一开始，在商店服务器和用户装置之间进行相互验证（步骤 S1051 和 S2051）。按照上面参考图 12 和 13 说明的相似方式进行相互验证。在后续数据传输中，在根据需要利用在相互验证过程中产生的对话密钥加密之后传送数据。如果成功通过相互验证，则用户装置产生加密内容密钥传送请求数据（图 17E）（步骤 S2053）并将其传送给商店服务器（步骤 S2054）。

如果商店服务器从用户装置收到加密内容密钥传送请求（步骤 S1054），则商店服务器验证接收的数据（步骤 S1055）。根据上面参考图 11 说明的处理流程进行数据验证。如果接收数据的验证结果指出数据未被篡改并且数据有效，则商店服务器向用户装置传送指出已成功接收加密内容密钥请求数据的消息（步骤 S1058），并且商店服务器把在销售管理数据库中描述的状态设置成“完成加密内容密钥传

送请求的接收”状态（步骤 S1060）。如果接收数据的验证结果指出数据已被篡改并且数据无效，则商店服务器向用户装置传送指出接收数据无效的消息（步骤 S1057），并把在销售管理数据库中描述的状态设置成“加密内容密钥传送请求接收失败”状态（步骤 S1059）。

如果用户装置从商店服务器收到确认响应（步骤 S2055 和 S2056），则用户装置把在购买管理数据库中描述的状态设置成“完成加密内容密钥传送请求的传送”状态（步骤 S2057）。但是，在用户装置从商店服务器收到否定确认响应（步骤 S2055 和 S2056）的情况下，用户装置把在购买管理数据库中描述的状态设置成“加密内容密钥传送请求传送失败”状态（步骤 S2058）。

在商店服务器中，在把在购买管理数据库中描述的状态设置成“完成加密内容密钥传送请求的接收”状态（步骤 S1060）之后，商店服务器产生加密内容密钥数据 2（商店）（图 17F）（步骤 S1061），并将其传送给用户装置（步骤 S1062）。

另一方面，在用户装置中，在把在购买管理数据库中描述的状态设置成“完成加密内容密钥传送请求的传送”状态（步骤 S2057）之后，用户装置从商店服务器接收加密内容密钥数据 2（商店）（图 17F）（步骤 S2059）。

在步骤 S2071 中，用户装置执行在步骤 S2059 中接收的数据的验证（图 11）。如果接收数据的验证结果表明数据未被篡改并且数据有效，则用户装置向商店服务器传送表明数据已被成功接收的消息（步骤 S2073），并且用户装置把在购买管理数据库中描述的状态设置成指出密钥 2 已被成功接收（步骤 S2075）。如果接收数据的验证结果指出数据已被篡改并且数据无效，则用户装置向商店服务器传送表明接收数据无效的消息（步骤 S2074），并且用户装置把在购买管理数据库中描述的状态设置成指出密钥 2 的接收已失败（步骤 S2076）。之后，用户装置关闭与商店服务器的连接（步骤 S2077）。

如果商店服务器从用户装置收到指出数据已被用户装置成功接收的消息（步骤 S1071），则商店服务器把在销售管理数据库中描述的

状态设置成指出密钥 2 已被成功传送（步骤 S1074）。但是，如果来自用户装置的消息指出数据无效，则商店服务器把在销售管理数据库中描述的状态设置成指出密钥 2 的传送已失败（步骤 S1073）。之后，商店服务器关闭与用户装置的连接（步骤 S1075）。

在步骤 S1052 和 S2052 中的相互验证已失败的情况下，终止该过程并且关闭连接。

基本内容传送模型 1 的变型

上面已说明了基于图 1 中所示的基本内容传送模型 1 的内容购买/传送过程。但是，系统结构并不局限于图 1 中所示的系统结构，相反如下所述只要由用户装置验证服务器执行内容密钥转换，就可以不同方式构成就该系统。

在图 29 中所示的例子中，商店服务器的功能由一个商店服务器和一个内容传送服务器分别执行，商店服务器 100 从用户装置 200 接收内容购买请求，内容传送服务器 400 把内容传送给用户装置 200。虽然不进行实体之间的相互验证，但是可按照上面参考基本内容分配模型 1 说明的相似方式执行相互验证。

如果商店服务器 100 从用户装置 200 收到购买请求数据，则商店服务器 100 验证接收的数据（图 29 中的过程步骤（3））。如果接收数据被确定为有效，则商店服务器 100 向内容传送服务器 400 发送内容传送请求（图 29 中的过程步骤（4））。内容传送服务器 400 验证从商店服务器 100 接收的内容传送请求数据。如果接收的数据有效，则内容传送服务器 400 从内容数据库 410 取回加密内容和加密内容密钥数据（内容传送服务器），并传送接收的数据（图 29 中的过程步骤（6））。这里，加密内容密钥数据（内容传送服务器）对于上述实施例中的加密内容密钥数据 1（商店），加密内容密钥数据（内容传送服务器）包括利用用户装置验证服务器的公共密钥 KpDAS 加密的内容密钥 Kc KpDAS（Kc）。

在用户装置 200 从内容传送服务器 400 收到加密内容和加密内容密钥数据（内容传送服务器）之后，按照和图 1 中所示的系统执行的

过程相似的方式执行其后的过程。

在本变型系统中，商店服务器 100 的主要功能是从用户装置接收内容请求数据，验证接收的请求数据，从用户装置验证服务器接收密钥转换后的加密内容密钥，并将其传送给用户装置。但是，内容的管理和传送不由商店服务器 100 执行。相反，当商店服务器从用户装置收到内容请求时，商店服务器根据请求的内容从若干内容传送服务器中选择某一内容传送服务器，例如音乐内容传送服务器或者游戏内容传送服务器，并且商店服务器把内容请求传送给选择的内容传送服务器。本系统中，虽然利用因特网双向进行用户装置和服务器之间的通信，但是也可从内容传送服务器和用户装置单方向进行内容传送服务器和用户装置之间的通信，从而可使用卫星通信线路来获得高的传输速度。

图 30 图解说明一种系统结构，其中和图 29 中所示的系统一样，商店服务器的功能由一个商店服务器和一个内容传送服务器以独立的方式实现，以致商店服务器 100 从用户装置 200 接收内容购买请求，但是内容从内容传送服务器 400 被发送给用户装置 200。与图 29 中所示系统的差别在于商店服务器 100 不向内容传送服务器 400 传送内容传送请求，但是用户装置验证服务器 300 向内容传送服务器 400 传送内容传送请求。

当商店服务器 100 从用户装置 200 收到购买请求数据时，商店服务器 100 验证接收的请求数据（图 30 中的步骤（3））。在购买请求数据的验证之后，商店服务器 100 向用户装置验证服务器 300 传送内容传送请求（图 30 中的步骤（4））。当收到内容传送请求时，用户装置验证服务器 300 验证接收的内容传送请求（图 30 中的步骤（5））。验证之后，用户装置验证服务器 300 向内容传送服务器 400 发送内容传送请求（图 30 中的步骤（6））。内容传送服务器 400 验证从用户装置验证服务器 300 接收的内容传送请求数据。如果成功通过验证，则内容传送服务器 400 从内容数据库 410 取回加密内容和加密内容密钥数据（内容传送服务器），并将其传送给用户装置 200（图 30 中的

步骤(8)。这里，加密内容数据(内容传送服务器)对应于上述实施例中的加密内容密钥数据1(商店)，并且包括利用用户装置验证的公共密钥KpDAS加密的内容密钥Kc，即包括KpDAS(Kc)。

在用户装置200从内容传送服务器400接收加密内容和加密内容密钥数据(内容传送服务器)之后执行的过程类似于上述图1中所示系统中执行的过程。

在本变型系统中，当向商店服务器100发出内容购买请求时，用户装置验证服务器300可获得关于用户装置200的信息。即，用户装置验证服务器300可在从用户装置200接收密钥转换请求之前，获得关于用户装置200的信息。这使用户装置验证服务器300能够在从用户装置200接收密钥转换请求的时刻，检查密钥转换请求是否由已注册为内容购买请求装置的相同装置所发出。

1. 3 基本内容传送模型 2

参见图31，下面说明和基本内容传送模型1略有不同的基本内容传送模型2。在该基本内容传送模型2中，不进行用户装置200和用户装置验证服务器300之间的数据传输。下面主要说明图31中所示的处理步骤(1)-(19)中与基本内容传送模型1不同的步骤。虽然在本实施例中，进行实体之间的相互验证(步骤(1)、(7)和(13))，不过根据情况也可省略相互验证。

(1) 相互验证

当用户装置200希望从商店服务器100购买内容时，首先在用户装置200和商店服务器100之间进行相互验证。按照上面参考图12和13说明的相似方式进行相互验证。在后续数据传输中，在根据需要利用在相互验证过程中产生的话路密钥加密之后传送数据。

(2) 交易ID和购买请求数据的产生，及

(3) 购买请求数据的传输

如果成功通过商店服务器100和用户装置200之间的相互验证，则用户装置200产生内容购买请求数据。图32G图解说明购买请求数据的数据结构。购买请求数据包括识别内容购买请求发往的商店服务

器 100 的商店 ID, 根据随机数由用户装置 200 的加密装置以内容交易的标识符的形式产生的交易 ID, 和指示用户装置所希望购买内容的内容 ID。此外, 关于上述数据的用户装置的数字签名被添加到购买请求数据中。购买请求数据和用户装置的公共密钥证书一起被传送给商店服务器 100。注意如果在相互验证过程中或者在相互验证之前, 公共密钥证书已被传送给商店服务器, 则不需要重新传送公共密钥证书。

(4) 接收数据的验证

当商店服务器 100 从用户装置 200 收到如图 32G 中所示的购买请求时, 商店服务器 100 验证接收的数据。按照上面参考图 11 说明的相似方式进行验证。

(5) 加密内容和购买接受数据的传输

如果商店服务器 100 进行的验证指出购买请求数据有效, 未被篡改, 则商店服务器 100 向用户装置传送加密内容和购买接受数据。这里, 传输给用户装置的数据只包括通过利用内容密钥对内容加密获得的加密内容数据 K_c (内容), 以及指出购买请求已被接受的购买接受数据, 但是该数据不包括通过利用用户装置验证服务器 (DAS) 300 的公共密钥对内容密钥 K_c 加密获得的加密内容密钥数据 K_{pDAS} (K_c)。

图 32H 图解说明购买请求接受数据的数据结构。购买接受数据包括识别已发出内容购买请求的用户装置 200 的用户装置 ID, 购买请求数据 (除用户装置的公共密钥证书之外图 32G 中所示的数据), 响应内容交易的起动由商店服务器 100 产生的商店过程编号。此外, 关于上述数据的商店服务器 100 的数字签名被添加到购买请求接受数据中。购买请求接受数据和商店服务器 100 的公共密钥证书一起被传送给用户装置 200。注意如果在相互验证过程中或者在相互验证之前, 公共密钥证书已被传送给用户装置, 则不需要重新传送该公共密钥证书。

(6) 接收数据的验证

当用户装置 200 从商店服务器 100 接收加密内容 K_c (内容) 和图

32H 1(商店)中所示的购买请求接受数据时，用户装置 200 验证购买请求接受数据。按照上面参考图 15 中所示的处理流程说明的相似方式进行验证。即，用户装置 200 首先利用认证机构 (CA) 的公共密钥 KpCA 验证从商店服务器 100 接收的商店服务器的公共密钥证书。之后，用户装置 200 利用从公共密钥证书中抽取的商店服务器的公共密钥 KpSHOP，验证写入图 32H 中所示的购买请求接受数据中的商店签名。

(7) 相互验证，和

(8) 加密内容密钥数据 1(商店)的传输

之后，商店服务器 100 访问用户装置验证服务器 300。当访问用户装置验证服务器 300 时，在商店服务器 100 和用户装置验证服务器 300 之间进行相互验证。如果成功通过相互验证，则商店服务器 100 把加密内容密钥数据 1(商店)传送给用户装置验证服务器 300。

图 32I 图解说明加密内容密钥数据 1(商店)的数据结构。加密内容密钥数据 1(商店)包括识别加密内容密钥的转换请求发往的用户装置验证服务器 300 的用户装置验证服务器 ID，从用户装置 200 接收的购买请求数据(除用户装置的公共密钥证书外图 32G 中所示的数据)和商店过程编号。此外，关于上述数据的商店服务 100 的数字签名被添加到加密内容密钥数据 1(商店)中。加密内容密钥数据 1(商店)和商店服务器 100 的公共密钥证书以及用户装置 200 的公共密钥证书一起被传送给用户装置验证服务器 300。在用户装置验证服务器 300 已具有用户装置的公共密钥证书和商店服务器的公共密钥证书的情况下，不需要重新传送这些证书。

(9) 接收数据的验证

当用户装置 300 从商店服务器 100 收到加密内容密钥数据 1(商店) (图 32I) 时，用户装置 300 验证加密内容密钥数据 1(商店)。按照上面参考图 15 中所示的处理流程说明的相似方式进行验证。即，用户装置验证服务器 300 首先利用认证机构 (CA) 的公共密钥 KpCA 验证从商店服务器 100 接收的公共密钥证书。之后，用户装置验证服

务器 300 利用从公共密钥证书中抽取的商店服务器的公共密钥 KpSHOP，验证写入图 32I 中所示的加密内容密钥数据 1（商店）中的数字签名。此外，用户装置验证服务器 300 利用认证机械（CA）的公共密钥 KpCA 验证用户装置的公共密钥证书。之后，用户装置验证服务器 300 利用从公共密钥证书中抽取的用户装置的公共密钥 KpDEV，验证由用户装置写入包含在图 32I 中所示加密内容密钥数据 1（商店）中的购买请求数据中的数字签名。

（10）加密内容密钥的转换

在由用户装置验证服务器 300 执行的关于从商店服务器 100 接收的加密内容密钥数据 1（商店）的验证中，如果确定接收的数据被确定为有效，则用户装置验证服务器（DAS）300 利用用户装置验证服务器（DAS）300 的保密密钥 KsDAS 对包含在加密内容密钥数据 1（商店）中的加密内容密钥，即通过利用用户装置验证服务器（DAS）300 的公共密钥 KpDAS 对内容密钥 Kc 加密获得的加密数据 KpDAS（Kc）解密，从而获得内容密钥 Kc。此外，用户装置验证服务器 300 利用用户装置的公共密钥 KpDEV 对获得的内容密钥 Kc 加密，从而产生加密内容密钥 KpDEV（Kc）。即，密钥被转换，以致 KpDAS（Kc）→ Kc → KpDEV（Kc）。根据上面参考图 16 说明的处理流程执行该密钥转换过程。

（11）加密内容数据的传输

之后，用户装置验证服务器 300 把加密内容密钥数据（DAS）传送给商店服务器 100。

图 33J 图解说明加密内容密钥数据（DAS）的数据结构。加密内容密钥数据（DAS）包括识别内容购买请求发往的商店服务器 100 的商店 ID，加密内容密钥数据 1（商店）（除商店的公共密钥证书和用户装置的公共密钥证书之外图 32I 中所示的数据），和通过上述密钥转换过程由用户装置验证服务器 300 产生的加密内容密钥数据 KpDEV（Kc）。此外，关于上述数据的用户装置 300 的数字签名被添加到加密内容密钥数据（DAS）中。加密内容密钥数据（DAS）和用

户装置验证服务器 300 的公共密钥证书及用户装置 200 的公共密钥证书一起被传送给商店服务器 100。在商店服务器已具有这些证书的情况下，不需要重新传送这些证书。

在用户装置验证服务器 300 由高度可靠第三方管理的情况下，可不按照图 33J 中所示的形式构成加密内容密钥数据（DAS），在图 33J 中加密内容密钥数据 1（商店）（图 33J 中由（8）表示）以其初始形式包含于其中，而是可这样构成，如图 33J' 中所示，商店 ID、用户装置 ID、交易 ID、内容 ID、商店过程编号和利用用户装置的公共密钥加密的内容密钥 KpDEV（Kc）由用户装置验证服务器 300 抽取，并且加密内容密钥数据（DAS）由抽取的这些数据加上用户装置验证服务器 300 的数字签名构成。这咱情况下，只把用户装置验证服务器 300 的公共密钥证书附加到加密内容密钥数据（DAS）上。

（12）接收数据的验证

当商店服务器 100 从用户装置验证服务器 300 收到加密内容密钥数据（DAS）（图 33J）时，商店服务器 100 验证加密内容密钥数据（DAS）。按照上面参考图 15 中所示的处理流程说明的相似方式进行验证。即，商店服务器 100 首先利用认证机构（CA）的公共密钥 KpCA，验证从用户装置验证服务器 300 接收的用户装置验证服务器的公共密钥证书。之后，商店服务器 100 利用用户装置验证服务器 300 的公共密钥 KpDAS 验证写入图 33J 中所示的加密内容密钥数据（DAS）中的数字签名。在商店服务器 100 接收上面参考图 33J' 描述的简化形式的加密内容密钥数据（DAS）的情况下，按照相似的方式进行验证。此外，根据需要可验证包含在图 33J 中所示的加密内容数据（DAS）中的加密内容密钥 1（商店）。

（13）相互验证，和（14）加密内容密钥请求的传输

之后，用户装置 200 把加密内容密钥请求数据传送给商店服务器。在和传送前一请求的话路不同的话路中传送加密内容密钥请求数据的情况下，再次进行相互验证，并且只有当成功通过相互验证时才从用户装置 200 把加密内容密钥请求数据传送给商店服务器 100。

(15) 验证，和

(16) 收费过程

当商店服务器 100 从用户装置收到加密内容密钥请求数据时，商店服务器 100 验证加密内容密钥请求数据。按照上面参考图 15 说明的相似方式进行验证过程。在完成数据验证之后，商店服务器 100 执行与内容交易相关的收费过程。执行该收费过程以便从用户账户收取该内容的费用。在内容的版权持有者、商店和用户装置验证服务器的所有者等等之间分配收取的内容费用。

和上述基本模型 1 中一样，为了执行收费过程，要求用户装置验证服务器 300 已完成加密内容密钥转换，从而不能仅仅通过商店服务器 100 和用户装置之间的过程就执行收费过程。除非已完成密钥转换，否则用户装置 200 不能对加密内容密钥解密，从而用户装置 200 不能使用该内容。其中用户装置验证服务器执行密钥转换的所有内容交易的历史被记录到前面参考图 6 说明的许可证管理数据库中，从而可监控和管理需要收费过程的任意内容交易。这可防止任何商店单独进行内容销售交易，从而防止未经授权销售内容。

(17) 加密内容密钥数据 2(商店)的传输

在完成收费过程之后，商店服务器 100 把加密内容密钥数据 2(商店)传送给用户装置 200。

图 33K 图解说明加密内容密钥数据 2(商店)的数据结构。加密内容密钥数据 2(商店)包括识别已发出加密内容密钥请求的用户装置 200 的用户装置 ID，以及从用户装置验证服务器 300 接收的加密内容密钥数据(DAS)(除用户装置验证服务器的公共密钥证书之外图 33J 中所示的数据)。此外，关于上述数据的商店服务器 100 的数字签名被添加到加密内容密钥数据 2(商店)中。加密内容密钥数据 2(商店)和商店服务器 100 的公共密钥证书及用户装置验证服务器 300 的公共密钥证书一起被传送给用户装置 200。在用户装置 200 已具有用户装置验证服务器的公共密钥证书以及商店服务器的公共密钥证书的情况下，不需要重新传输这些证书。

在用户装置验证服务器 300 由高度可靠的第三方管理，并且商店服务器 100 从用户装置验证服务器 300 接收呈上面参考图 33J'说明的简化形式的加密内容密钥数据（DAS）的情况下，商店服务器 100 把呈图 34K'中所示形式的加密内容密钥数据 2（商店）传送给用户装置。即，包括商店服务器的签名的呈图 33J'中所示简化形式的加密内容密钥数据（DAS）和商店服务器 100 的公共密钥证书以及用户装置验证服务器 300 的公共密钥证书一起被传送给用户装置 200。

(18) 接收数据的验证

当用户装置 200 从商店服务器 100 接收加密内容密钥数据 2（商店）时，用户装置 200 验证加密内容密钥数据 2（商店）。按照上面参考图 15 中所示的处理流程说明的相似方式进行验证。即，用户装置 200 首先利用认证机构（CA）的公共密钥 KpCA 验证从商店服务器 100 接收的商店服务器的公共密钥证书。之后，用户装置 200 利用从公共密钥证书中抽取的商店服务器 100 的公共密钥 KpSHOP，验证写入图 33K 中所示加密内容密钥数据 2（商店）中的数字签名。此外，用户装置 200 利用认证机构（CA）的公共密钥 KpCA 验证用户装置验证服务器 300 的公共密钥证书。之后，用户装置 200 利用从公共密钥证书抽取的用户装置验证服务器 300 的公共密钥 KpDAS，验证写入包含在图 33J 中所示加密内容密钥数据 2（商店）中的（11）加密内容密钥数据（DAS）中的数字签名。此外，根据需要可验证包含在图 33J 中所示加密内容密钥数据（DAS）中的加密内容密钥 1（商店）。

(19) 数据的存储

在用户装置 200 验证了从商店服务器 100 接收的加密内容密钥数据 2(商店)之后，用户装置 200 利用用户装置 200 的保密密钥 KsDEV 对利用用户装置 200 的公共密钥 KpDEV 加密的，并且包含在加密内容密钥数据 2(商店)中的加密内容密钥 KpDEV(Kc)解密，随后用户装置 200 利用用户装置的存储密钥 Ksto 对该内容密钥加密，从而产生加密内容密钥 Ksto(Kc)。所得到的加密内容密钥 Ksto(Kc)被保存在用户装置 200 的存储装置中。当使用该内容时，利用存储密钥

Ksto 对加密内容密钥 Ksto (Kc) 解密，从而获得内容密钥 Kc，并且利用获得的内容密钥 Kc 对加密内容 Kc (内容) 解密，从而再现内容。

在基本分配模型 2 中，如上所述，在用户装置 200 和用户装置验证服务器 300 之间不进行数据传输，用户装置 200 只和商店服务器 100 进行数据传输。这可减少施加在用户装置上的处理负荷。

1. 2 基本内容传送模型 2 的变型

下面说明图 31 中所示基本内容传送模型 2 的变型的例子。在图 35 中所示的例子中，商店服务器的功能由一个商店服务器和一个内容传送服务器分别实现，以致商店服务器 100 从用户装置 200 接收内容购买请求，并且内容传送服务器 400 把内容传送给用户装置 200。在该变型模型中，不进行传送数据的实体之间的相互验证，但是每个实体验证写入所接收数据中的数字签名。但是，可按照和基本内容分配模型 2 相似的方式进行相互验证。

如果商店服务器 100 从用户装置 200 收到购买请求数据，则商店服务器 100 验证接收的数据（图 35 中的过程步骤（3））。如果确定接收的数据有效，则商店服务器 100 向内容传送服务器 400 发送内容传送请求（图 35 中的过程步骤（4））。内容传送服务器 400 验证从商店服务器 100 接收的内容传送请求数据。内容传送服务器 400 从内容数据库 410 取回加密内容，并传送取回的数据（图 35 中的过程步骤（6））。

如果用户装置 200 从内容传送服务器 400 收到加密内容，则用户装置 200 验证接收的数据。如果接收的数据有效，则用户装置 200 向内容传送服务器 400 发送指出加密内容已被成功接收的消息。内容传送服务器 400 验证接收的数据。如果接收的数据有效，则内容传送服务器 400 向用户装置验证服务器 300 传送加密内容密钥数据（内容传送服务器），并且请求用户装置验证服务器 300 执行加密内容密钥转换过程（图 35 中的过程步骤（10））。

在用户装置验证服务器 300 从内容传送服务器 400 收到加密内容密钥数据（内容传送服务器）和加密内容密钥转换请求时，除了不进

行相互验证之外，按照上面参考图 31 说明的实施例相似的方式进行其后的过程。

在本变型内容分配模型中，在不进行相互验证的情况下，用户装置向商店服务器传送内容购买请求，并且接收加密内容。如果商店服务器 100 从用户装置接收内容购买请求，则商店服务器仅仅通过验证写入其中的数字签名来验证接收的内容购买请求数据。此外，如果商店服务器 100 从用户装置验证服务器收到已经过密钥转换过程的加密内容密钥，则商店服务器 100 通过验证写入其中的数字签名来验证该加密内容密钥。类似地，当内容传送服务器 400 从商店服务器收到数据时，内容传送服务器 400 通过验证写入其中的数字签名来验证接收的数据，并且如果成功通过验证则传输内容。

商店服务器 100 不管理或传输内容。而是当商店服务器从用户装置收到内容请求时，商店服务器根据所请求的内容从若干内容传送服务器中选择某一个内容传送服务器，例如音乐内容传送服务器或者游戏内容传送服务器，并且商店服务器向选择的内容传送服务器发送内容传送请求。在该系统中，虽然通过利用因特网双向进行用户装置和商店服务器之间的通信，不过也可只从内容传送服务器和用户装置单向进行内容传送服务器和用户装置之间的通信，从而可使用卫星通信线路为获得高的传输速度。

本实施例中，在不进行相互验证的情况下仅仅通过检查数字签名来验证数据，从而提高了处理效率。

图 6 图解说明了一种系统结构，和图 35 中所示的系统一样，商店服务器的功能由一个商店服务器和一个内容传送服务器分别实现，以致商店服务器 100 从用户装置 200 接收内容购买请求，并且在不进行相互验证的情况下验证写入其中的签名，从内容传送服务器 400 把内容传送给用户装置 200。和图 35 中所示系统的差别在于商店服务器 100 不向内容传送服务器 400 传输内容传送请求，而是用户装置验证服务器 300 向内容传送服务器 400 传输内容传送请求。

当商店服务器 100 从用户装置 200 收到购买请求数据时，商店服

务器 100 验证接收的请求数据（图 36 中的步骤（3））。验证购买请求数据之后，商店服务器 100 向用户装置验证服务器 300 传送加密内容密钥数据 1（商店）（图 36 中的步骤（4））。当收到内容传送请求时，用户装置验证服务器 300 验证接收的内容传送请求（图 36 中的步骤（5））。验证之后，用户装置验证服务器 300 向内容传送服务器 400 传输内容传送请求（图 36 中的步骤（6））。内容传送服务器 400 验证从用户装置验证服务器 300 接收的内容传送请求数据。如果成功通过验证，则内容传送服务器 400 从内容数据库 410 取回加密内容，并将其传送给用户装置 200（图 36 中的步骤（8））。其后执行的过程和上述图 35 中所示系统中执行的过程相似。

在该变型系统中，当向商店服务器 100 发出内容购买请求时，用户装置验证服务器 300 可获得关于用户装置的信息。即，用户装置验证服务器 300 可在从内容传送服务器 400 接收密钥转换请求之前获得关于用户装置的信息。这使用户装置验证服务器 300 能够在从内容传送服务器 400 接收密钥转换请求的时候，检查密钥转换请求是否由和已注册为内容购买请求装置相同的装置发出。在认为 DAS 高度可靠的情况下，不必要求内容传送服务器验证从商店服务器接收的数据，从而可提高处理效率。

在根据本发明的内容传送系统中，如上所述，除非用户装置验证服务器已完成加密内容密钥转换，否则即使用户装置已获得加密内容 K_c （内容），用户装置也不能使用该内容。这意味着在不向用户装置验证服务器通知销售交易的情况下，商店服务器不能向用户装置销售内容，从而除非把销售交易通知用户装置验证服务器，否则用户装置不能使用内容。其中由用户装置验证服务器进行密钥转换的所有内容交易的历史被记录到由用户装置验证服务器管理的许可证管理数据库（图 6）中，以致监控和管理所有商店执行的所有内容销售交易。从而能够在内容的版权持有者、商店和用户装置验证服务器的所有者等等之间正确分配通过商店执行的收费过程获得的金额。这可防止欺诈使用所述内容。

2. 使用电子票券的内容传送模型

如下所述，可发出包括获利共享信息的电子票券，所述获利共享信息指出应在内容的版权持有者、制作者、许可证持有者、商店等等之间分配的通过销售（提供）内容获得的金额，并且可根据在电子票券中描述的获利共享信息支付金额。

图 37 图解说明其中根据在电子票券中描述的获利共享信息支付金钱的系统。如图 37 中所示，该内容传送系统包括从用户装置接收内容购买请求，并且发行其中描述关于内容费用的分配比例的信息的电子票券的票券发行服务器 610，发出内容购买请求的用户装置（DEV）620，执行密钥转换从而正确进行内容交易的用户装置验证服务器（DAS）630，诸如提供内容的内容提供者（CP）之类的内容传送服务器 640，和根据电子票券中描述的信息执行诸如费用转账之类交换过程的票券交换服务器 650.

票券发行服务器

图 38 图解说明图 37 中所示的内容传送系统中的票券发行服务器（TIS）610 的结构。如果票券发行服务器 610 从用户装置 620 收到购买请求，则票券发行服务器 610 发出电子票券，其中描述指出如何共享被请求内容的收益的信息。

票券发行服务器（TIS）610 具有票券管理数据库 612，其中描述响应内容交易发出票券的历史。更具体地说，当发出票券时，内容售给的用户装置的标识符、内容标识符以及内容价格被记录在票券管理数据库 612 中，以致这些数据彼此相关。票券发行服务器 610 还包括用于验证从用户装置 620 接收的内容购买请求，控制票券管理数据库，根据票券中描述的信息向用户装置收费，与用户装置通信，以及在通信中对数据加密/解密的控制装置 613。

图 39 图解说明票券管理数据库 612 的数据结构。票券管理数据库 612 描述和当票券发行服务器响应内容交易发出票券时，以票券标识符的形式内部产生的票券编号，识别发出内容购买请求的用户装置的装置 ID，当在用户装置和票券发行服务器之间进行内容交易时由用户

装置产生的作为内容交易的标识符的交易 ID，识别进行交易的内容的内容 ID，识别根据在由票券发行服务器 610 发出的电子票券中描述的信息接受费用的实体，诸如版权持有者、许可证持有者、管理者和内容销售者的票券用户 ID，支付给由票券用户 ID 指示的相应实体的金额，应执行使用票券的交换的有效期有关的信息，以及指出和票券发行服务器 610 进行的发行和管理票券相关状态的状态信息。如同后面所述，该状态随着内容交易的进行而更新。

如图 38 中所示，票券发行服务器 610 的控制装置 613 由其中存储加密程序和通信程序的计算机构成，从而控制装置 613 也可用作加密装置和通信装置。以安全的方式把控制装置 613 的加密装置在加密过程中使用的密钥数据等保存到控制装置中的存储装置中。保存在票券发行服务器 610 中供加密过程使用的诸如加密密钥之类的数据包括票券发行服务器 610 的保密密钥 KsTIS，票券发行服务器 610 的公共密钥证书 Cert_TIS，发出公共密钥证书的认证机构（CA）的公共密钥 KpCA。

按照前面参考图 4 说明的控制装置相似的方式构成控制装置 613。即，控制装置 613 包括 CPU（中央处理器）、ROM（只读存储器）、RAM（随机存取存储器）、显示器、输入装置、存储装置和通信接口。

用户装置

按照和图 1 中所示系统中采用的用户装置相似的方式构成用户装置（DEV）620。即，按照上面参考图 7 说明的相似方式构成用户装置 620。保存在用户装置 620 中供加密过程使用的诸如加密密钥之类的数据包括用户装置的保密密钥 KsDEV，用户装置的公共密钥证书 Cert_DEV，发出公共密钥证书的认证机构（CA）的公共密钥 KpCA，和当把内容保存到诸如用户装置的硬盘之类的存储装置中时，用作对内容加密的加密密钥的存储密钥 Ksto。

在图 37 中所示的票券管理系统中使用的用户装置 620 的购买管理数据库具有管理票券的能力。图 40 图解说明购买管理数据库的数据结构。购买管理数据库具有和当进行内容交易时由用户装置产生的交易

ID, 识别进行交易的内容的内容 ID, 识别响应内容交易而发出票券的票券发行者的票券发行者 ID, 由票券发行服务器 610 分配的票券编号, 识别票券发往的实体的票券接收者 ID 有关的信息, 以及指出涉及内容交易的用户装置的状态的状态信息。如后所述, 该状态随着内容交易的进行而更新。

用户装置验证服务器

按照和图 1 中所示的系统中采用的用户装置验证服务器相似的方式构成用户装置验证服务器 (DAS) 630。即, 按照参考图 5 说明的相似方式构成用户装置验证服务器 630。保存在用户装置验证服务器 630 中供加密过程使用的诸如加密密钥之类的数据包括用户装置验证服务器 (DAS) 300 的保密密钥 KsDAS, 用户装置验证服务器 (DAS) 300 的公共密钥证书 Cert_DAS, 和发出公共密钥证书的认证机构 (CA) 的公共密钥 KpCA。

在图 37 中所示的票券管理系统中使用的用户装置验证服务器 630 的许可证管理数据库具有管理票券的能力。图 41 图解说明许可证管理数据库的数据结构。许可证管理数据库描述和内部产生的用于识别在内容交易中由用户装置验证服务器 (DAS) 630 执行的过程的 DAS 过程编号、识别发出内容购买请求的用户装置的装置 ID、当进行内容交易时由用户装置产生的交易 ID、识别进行交易的内容的内容 ID、识别响应内容交易发出票券的票券发行者的票券发行者 ID, 由票券发行服务器 610 分配的票券编号有关的信息, 以及指出涉及内容交易的用户装置验证服务器 (DAS) 的状态的状态信息。如后所述, 该状态随着内容交易的进行而更新。

内容传送服务器

图 42 图解说明图 37 中所示内容传送系统中的内容传送服务器 640 的结构。内容传送服务器 640 的一个例子是具有内容数据库 644 的内容提供者 (CP), 所述内容数据库 644 包括通过利用内容密钥对要销售的内容加密产生的加密内容数据 Kc (内容), 和通过利用用户装置验证服务器 (DAS) 的公共密钥 KpDAS 对内容密钥 Kc 加密获得的加

密内容密钥 KpDAS (Kc)。如图 42 中所示，内容 ID 被分配给各个加密内容数据 Kc (内容)，从而可利用内容 ID 识别各个加密内容。

内容传送服务器 640 还包括用于存储并管理内容传送数据的内容传送数据库 642。内容传送管理数据库 642 具有管理票券的能力。图 43 图解说明内容传送管理数据库的数据结构。内容传送管理数据库 642 描述和当传送内容时由内容传送服务器 640 产生的传送过程编号，识别进行交易的内容的内容 ID，识别内容发往的用户装置的用户装置 ID，识别响应内容交易发出票券的票券发行者的票券发行者 ID，票券发行者分配的票券编号有关的信息，以及指出内容交易过程中内容传送服务器的状态的状态信息。如后所述，该状态随着内容交易的进行而更新。

内容传送服务器 640 包括从内容数据库 644 取回要传送的内容，响应交易产生在内容传送管理数据库 642 中描述的交易数据，与用户装置 620 等通信，以及在通信过程中对数据加密/解密的控制装置 643。如图 42 中所示，控制装置 643 由其中保存加密程序和通信程序的计算机构成，从而控制装置 643 也可用作加密装置和通信装置。由控制装置 643 的加密装置在加密过程中使用的密钥数据等以安全的方式保存在控制装置中的存储装置中。保存在内容传送服务器 640 中供加密过程使用的诸如加密密钥之类数据包括内容传送服务器 640 的保密密钥 KsCP，内容传送服务器 640 的公共密钥证书 Cert_CP，和发出公共密钥证书的认证机构 (CA) 的公共密钥 KpCA。

按照和前面参考图 4 说明的控制装置相似的方式构造控制装置 643。即，控制装置 643 包括 CPU (中央处理器)、ROM (只读存储器)、RAM (随机存取存储器)、显示器、输入装置、存储装置和通信接口。

票券交换服务器

图 44 图解说明图 37 中所示的内容传送系统中的票券交换服务器 (TES) 650 的结构。票券交换服务器 650 从不同的实体接收电子票券，并且在验证接收的数据之后，通过在账户之间转账或者改变电子货币

的余额，根据票券中描述的信息执行交换过程。更具体地说，票券交换服务器 650 可以是安装在银行中的管理相应实体的银行账户的服务器。

票券交换服务器 650 具有根据响应内容交易发出的票券，管理与交换过程相关的数据的票券交换管理数据库 652。票券交换服务器 650 还包括用于验证从实体接收的票券，控制票券交换管理数据库，与实体通信以及在通信过程中对数据加密/解密的控制装置 653。

图 45 图解说明票券交换管理数据库 652 的数据结构。票券交换管理数据库 652 具有响应接收的票券，由票券交换服务器内部产生的用于识别票券交换过程的 TES 过程编号，识别根据票券请求交换的实体的交换请求者 ID，识别响应内容交易发出票券的票券发行者的标志着发行者 ID，由票券发行服务器 610 分配的票券编号，根据票券交换的金额，识别购买内容的用户装置的用户装置 ID，当执行内容交易时由用户装置产生的交易 ID，以及指出由票券交换服务器执行的交换过程的状态的状态信息。如后所述，该状态随着内容交易的进行而更新。

票券交换服务器 650 包括产生并更新在票券交换管理数据库 652 中描述的数据，验证接收的票券，与实体通信，并且在通信过程中对数据加密/解密的控制装置 653。如图 44 中所示，控制装置 653 由其中保存加密程序和通信程序的计算机构成，从而控制装置 653 还可用作加密装置和通信装置。由控制装置 653 的加密装置在加密过程中使用的密钥数据等保存在控制装置中的存储装置中。保存在票券交换服务器中借助加密过程使用的诸如加密密钥之类数据包括票券交换服务器 650 的保密密钥 KsTES，票券交换服务器 650 的公共密钥证书 Cert_TES，和发出公共密钥证书的认证机构(CA)的公共密钥 KpCA。

按照和前面参考图 4 说明的控制装置相似的方式构成控制装置 653。即，控制装置 653 包括 CPU(中央处理器)、ROM(只读存储器)、RAM(随机存取存储器)、显示器、输入装置、存储装置和通信接口。

内容购买过程

再次参见图 37，说明一个过程，其中用户装置向票券发行服务器发出内容购买请求，用户装置获得内容，用户装置把获得的内容保存在用户装置中，从而可使用该内容，并且根据在票券中描述的获利共享信息支付（交换）通过销售内容获得的金钱。在图 37 中，该过程如下所述按照从（1）-（32）的步骤顺序进行。

（1）相互验证

当用户装置 620 希望购买内容时，首先在用户装置 620 和票券发行服务器 610 之间进行相互验证。按照上面参考图 12 和 13 说明的相似方式进行相互验证。在后续的数据传输中，在根据需要利用在相互验证过程中产生的话路密钥加密之后传送数据。

（2）交易 ID 和购买请求数据的产生，及

（3）购买请求数据的传输

如果成功通过票券发行服务器 610 和用户装置 620 之间的相互验证，则用户装置 620 产生内容购买请求数据。图 46M 图解说明了购买请求数据的数据结构。购买请求数据包括识别发出内容购买请求的用户装置 620 的用户装置 ID，根据随机数由用户装置 620 的加密装置产生的作为内容交易的标识符的交易 ID，和指出用户装置所希望购买内容的内容 ID。此外，关于上述数据的用户装置的数字签名被添加到购买请求数据中。根据需要，把供验证签名之用的用户装置的公共密钥证书附加到购买请求数据上。

（4）接收数据的验证

当票券发行服务器 610 从用户装置 620 收到如图 46M 中所示的购买请求时，票券发行服务器 610 验证接收的数据。按照前面参考图 15 说明的相似方式进行验证。

（5）收费过程，

（6）电子票券的发行，和

（7）电子票券的传输

之后，票券发行服务器 610 执行与内容交易相关的收费过程，并且发出电子票券。这里，发出低于根据银行账户的余额或者用户的电

于货币金额规定的交易上限的电子票券。发出的电子票券被传送给用户装置 620。

图 47A 和 47B 图解说明电子票券的数据结构的例子。在图 47A 中所示的例子中，在电子票券中描述的获利共享信息只包括将向其支付金钱的一个接收实体。如图 47A 中所示，电子票券包括票券发行者 ID，票券发行过程编号，指示根据在票券中描述的信息被给付费用的实体的票券用户 ID，根据票券要支付的金额，其间接收实体可根据电子票券进行收款过程（结算）的电子票券的有效期，以及从用户装置传送给票券发行服务器的购买请求数据（图 46M）。电子票券还包括指出票券发行日期的数据。此外，票券发行服务器的数字签名被添加到该数据中。另外，如果需要，把票券发行服务器的公共密钥证书附加到电子票券上供验证签名之用。

图 47B 表示包括获利共享信息的电子票券的数据格式，所述获利共享信息指出应支付给若干接收实体的金额。如图 47B 中所示，电子票券包括若干票券发行者 ID（票券用户 1-票券用户 n 的 ID），电子票券中说明了要支付给由票券用户 ID 识别的相应票券用户的金额。即，各个接收实体可收到对应于该实体 ID 的金额。

在图 37 中所示的过程的例子中，票券发行服务器 610 发出供操作内容传送服务器的内容提供者（CP）使用的电子票券，另外还发出供用户装置验证服务器（DAS）使用的电子票券。根据销售的内容确定向哪些实体发出票券。在某些情况下，电子票券被发给内容的作者等等。票券发行服务器具有一个表格，其中针对各个内容 ID，说明票券应发给哪些实体，以及应向相应的实体支付的金额。当票券发行服务器从用户装置收到内容购买请求时，票券发行服务器检测在内容购买请求中描述的内容 ID，并且根据该表格确定应发给票券的实体以及要向实体支付的金额。之后，票券发行服务器根据确定结果发出票券。

（8）接收数据的验证

当用户装置 620 从票券发行服务器 610 收到票券时，用户装置 620 验证接收的票券。按照上面参考图 15 中所示的处理流程说明的相似方

式进行验证。即，用户装置 620 首先利用认证机构（CA）的公共密钥 KpCA 验证票券发行服务器的公共密钥证书。随后用户装置 620 从公共密钥证书抽取票券发行服务器的公共密钥 KpTIS，并且利用抽取的公共密钥 KpTIS 验证该票券的签名。

（9）相互验证，和

（10）（供 CP 使用）电子票券的传输

之后，用户装置 620 访问内容传送服务器 640，并且在它们之间进行相互验证。如果成功通过相互验证，则用户装置 620 向内容传送服务器 640 传送电子票券（供 CP 使用）。

（11）接收数据的验证，和

（12）加密内容和加密内容密钥的传输

在由内容传送服务器 640 执行的关于电子票券（供 CP 使用）的验证中，如果确定电子票券未被篡改，从而电子票券有效，则内容传送服务器 640 向用户装置传送加密内容和加密内容密钥。即，传送通过利用内容密钥对内容加密获得的加密内容 Kc（内容）和通过利用用户装置验证服务器（DAS）630 的公共密钥对内容密钥 Kc 加密获得的加密内容密钥数据 KpDAS（Kc）。

（13）接收数据的验证，

（14）相互验证，和

（15）电子票券（供 DAS 使用）及密钥转换请求的传输

当用户装置 620 从内容传送服务器 640 收到加密内容和加密内容密钥时，用户装置 620 验证接收的数据。验证之后，用户装置 620 访问用户装置验证服务器 630 并且执行与用户装置验证服务器 630 的相互验证。如果成功通过相互验证，则用户装置 620 向用户装置验证服务器 630 传送电子票券（DAS）和密钥转换请求。这里，密钥转换请求用于由用户装置验证服务器的公共密钥加密的加密内容密钥 Kc 的转换，其中加密内容密钥 Kc 从内容传送服务器 640 接收。即，响应密钥转换请求，用户装置验证服务器 630 按照和前面参考图 1 说明的密钥转换过程相似的方式，把加密内容密钥 KpDAS（Kc）转换成利

用用户装置的公共密钥 KpDEV 加密的加密内容密钥 KpDEV (Kc)。

(16) 接收数据的验证, 和

(17) 加密内容密钥的转换

如果用户装置验证服务器 630 从用户装置 620 收到电子票券（供 DAS 使用）和关于加密内容密钥 KpDAS (Kc) 的转换请求，则用户装置验证服务器 630 验证该电子票券（供 DAS 使用）和关于加密内容密钥的转换请求。如果验证结果表明电子票券有效，未被篡改，并且密钥转换请求有效，则用户装置验证服务器 630 利用用户装置验证服务器 630 的保密密钥 KsDAS 对通过利用用户装置验证服务器 (DAS) 630 的公共密钥 KpDAS 对内容密钥 Kc 加密获得的加密数据 KpDAS (Kc) 解密，从而获得内容密钥 Kc。此外，用户装置验证服务器 630 利用用户装置的公共密钥 KpDEV 对获得的内容密钥 Kc 加密，从而产生加密内容密钥 KpDEV (Kc)。即，密钥被转换，以致 KpDAS (Kc) → Kc → KpDEV (Kc)。按照前面参考图 16 说明的相似方式进行该转换过程。

(18) 加密内容密钥的传输

(19) 接收数据的验证, 和

(20) 数据的存储

用户装置验证服务器 630 把通过密钥转换产生的加密内容密钥 KpDEV (Kc) 传送给用户装置 620。如果用户装置 620 从用户装置验证服务器 630 收到加密内容密钥 KpDEV (Kc)，则用户装置 620 验证接收的数据。验证之后，用户装置 620 利用用户装置 620 的保密密钥 KsDEV 对加密内容密钥 KpDEV (Kc) 解密，随后用户装置 620 利用用户装置 620 的存储密钥 Ksto 对内容密钥加密，从而产生加密内容密钥 Ksto (Kc)。所得到的加密内容密钥 Ksto (Kc) 保存在用户装置 620 的存储装置中。当使用内容时，利用存储密钥 Ksto 对加密内容密钥 Ksto (Kc) 解密，从而获得内容密钥 Kc，并且利用得到的内容密钥 Kc 对加密内容 Kc (内容) 解密，从而再现内容。

(21) 相互验证, 和

(22) 电子票券(供 CP 使用)的传输

在把加密内容传送给用户装置 620 之后，内容传送服务器 640 访问票券交换服务器 650 并且执行与票券交换服务器 650 的相互验证。如果成功通过相互验证，则内容传送服务器 640 向票券交换服务器 650 传送供内容传送服务器 650 使用的电子票券(供 CP 使用)。

(23) 接收数据的验证和交换过程

如果票券交换服务器 650 进行的验证指出电子票券(供 CP 使用)是未被篡改的有效票券，则票券交换服务器 650 根据在接收的电子票券(供 CP 使用)中描述的信息进行交换过程。通过把电子票券(供 CP 使用)中规定的金额从用户装置的账户转移到管理内容传送服务器的内容提供者(CP)事先登记的银行账户或者电子货币账户中来完成交换过程。另一方面，可通过把在电子票券中规定的金额从票券发行服务器从用户预收的作为保证金的金额中转移到内容提供者(CP)的账户中来完成交换过程。只有当由票券交换服务器 650 执行的在票券中描述的有效期的验证指出有效期还没有期满时才进行上述交换过程或者结算过程。

(24) 交换过程报告的传输

在完成基于电子票券(供 CP 使用)的交换过程之后，票券交换服务器 650 向内容传送服务器 640 传送指出交换过程的结果的报告。

图 46N 图解说明交换过程报告的数据结构的一个例子。交换过程报告包括识别票券交换过程的票券交换过程 ID，识别请求基于票券的交换的实体的交换请求者 ID，以票券为基础的交换的金额，识别响应内容交易发出票券的票券发行者的票券发行者 ID，由票券发行服务器 610 分配的票券编号，以及票券交换服务器 650 进行票券交换过程的票券交换过程日期。票券交换服务器 650 的电子签名被添加到交换过程报告中。此外，如果需要，票券交换服务器的公共密钥证书被附加到交换过程报告上用于验证签名。

(25) 接收数据的验证

当内容传送服务器 640 从票券交换服务器 650 收到交换过程报告

时，内容传送服务器 640 验证接收的交换过程报告。如果数据验证指出报告有效，则可推断已正确地把分配给管理内容传送服务器的内容提供者的特定金额传送给内容提供者。

- (26) 相互验证，
- (27) 电子票券的传输（供 DAS 使用），
- (28) 接收数据的验证和交换过程，
- (29) 交换过程报告的传输，和
- (30) 接收数据的验证

类似于在内容传送服务器 640 和票券交换服务器 650 之间进行的上述过程 ((21) - (25))，在用户装置验证服务器 630 和票券交换服务器 650 之间同样以电子票券（供 DAS 使用）为基础进行同样的过程。

- (31) 相互验证，
- (32) 交换过程报告的传输，和
- (33) 接收数据的验证

在票券交换服务器 650 完成基于从相应实体接收的电子票券的交换过程之后，进行票券交换服务器 650 和票券发行服务器 610 之间的相互验证，并且从票券交换服务器 650 向票券发行服务器 610 传送类似于传送给相应实体的交换报告（图 46N）。票券发行服务器 610 检查从票券交换服务器 650 接收的交换报告，确认与发出的票券相关的交换过程已完成。

装置状态的转变

图 37 中所示的实体，例如票券发行服务器 610，根据表示内容交易的步骤序列中的过程状态的状态信息，确定下一步要进行的过程。利用图 39 中所示的票券发行管理数据库和图 40 中所示的用户装置的购买管理数据库，管理每个内容交易的状态信息。

下面参考图 48 说明票券发行服务器 610 的状态转变。当票券发行服务器 610 从用户装置 620 收到内容购买请求数据（图 37 中的过程 (3)）时，票券发行服务器 610 起动一个过程。当从用户装置 620 收

到数据时，票券发行服务器 610 验证接收的数据。如果成功通过验证，则状态被设置成“购买请求被接受”状态。但是，如果数据验证指出购买请求无效，则立即或者在重复预定次数之后终止该过程（本例中为购买请求接收过程），并且把状态设置成“购买请求被拒绝”状态。只有当状态为“购买请求被接受”状态时，该过程才进行到下一步。

如果状态被改变成“购买请求被接受”状态，则票券发行服务器 610 向用户装置 620 传送电子票券（图 37 中的步骤（7））。如果票券发行服务器 610 从用户装置收到确认响应，则状态被设置成“票券传送完成”状态。但是，如果没有收到确认响应，则立即或者在重复预定次数之后终止该过程（本例中为电子票券的传输），并且把状态设置成“票券传送失败”状态。只有当状态为“票券传送完成”状态时，该过程才进行到下一步骤。

如果状态被改变成“票券传送完成”状态，则票券发行服务器 610 从票券交换服务器收到交换报告，并且验证接收的报告（图 37 中的步骤（32）和（33））。如果成功通过验证，则状态被改变成“完成交换报告的接收”状态。但是，如果验证指出接收的报告无效，则立即或者在重复预定次数之后终止该过程（本例中为报告的接收和验证），并且把状态设置成“交换报告接收失败”状态。在票券发行服务器 610 中，对于各个内容交易按照相似的方式改变状态。

下面参考图 49 说明用户装置验证服务器 630 的状态转变。当用户装置验证服务器 630 从用户装置 620 收到加密内容密钥 KpDAS (Kc)（图 37 中的过程（15））时，用户装置验证服务器 630 起动一个过程。当从用户装置 620 收到包括电子票券 (DAS) 的数据时，用户装置验证服务器 630 验证接收的数据。如果成功通过验证，则状态被设置成“完成密钥的接收”状态。但是，如果状态验证指出接收的数据无效，则立即或者在重复预定次数之后终止该过程（本具体情况下为加密内容密钥数据（用户装置）的接收），并且把状态设置成“密钥接收失败”状态。只有当状态为“完成密钥接收”状态时过程才进行到

下一步骤。

如果状态被改变成“完成密钥接收”状态，则用户装置验证服务器630执行内容密钥转换过程（图37中的步骤（17））。如果成功完成内容密钥转换，则状态被设置成“完成密钥转换”状态。这里，假定总是成功完成密钥转换，因此状态总是被设置成“完成密钥转换”状态。

如果状态被改变成“完成密钥转换”，则用户装置验证服务器630把加密内容密钥数据（DAS）传送给用户装置620（图37中的步骤（18）），并且等待用户装置620的响应。如果从用户装置620收到确认响应，则状态被改变成“完成密钥传输”状态。但是，如果没有收到确认响应，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为加密内容密钥数据（DAS）的传输），并且状态被设置成“密钥传输失败”状态。

如果状态被改变成“密钥传输完成”状态，则用户装置验证服务器630向票券交换服务器650传送电子票券（供DAS使用）（图37中的步骤（27）），并且等待票券交换服务器650的响应。如果从票券交换服务器650收到确认响应，则状态被设置成“完成票券交换请求的传输”状态。但是，如果没有收到确认响应，则立即或者在重复预定次数之后终止该过程（本具体情况下为票券交换请求的传输），并且把状态设置成“票券交换请求传输失败”状态。

如果状态被改变成“完成票券交换请求的传输”状态，则用户装置验证服务器630从票券交换服务器650接收交换过程报告，并且验证接收的报告（图37中的步骤（29）和（30））。如果成功通过验证，则状态被设置成“完成交换过程报告的接收”状态，并且终止该过程。但是，如果数据验证指出接收的报告无效，则立即或者在重复预定次数之后终止该过程（本具体情况下为报告的接收和验证），并且把状态设置成“交换报告接收失败”状态。在用户装置验证服务器630中，对于各个内容交易按照上述方式改变状态。

下面参考图50说明内容传送服务器640的状态转变。当内容传送

服务器从用户装置 620 收到电子票券（供 CP 使用）（图 37 中的步骤（10））时，内容传送服务器 640 起动一个过程。当从用户装置 620 收到数据时，内容传送服务器 640 验证接收的数据。如果成功通过验证，则状态被设置成“完成电子票券的接收”状态。但是，如果数据验证指出接收的数据无效，则立即或者在重复预定次数之后终止该过程（本具体情况下为票券的接收），并且状态被设置成“电子票券接收失败”状态。只有当状态为“完成电子票券的接收”状态时过程才进行到下一步骤。

如果状态被改变成“完成电子票券的接收”状态，则内容传送服务器 640 把加密内容和加密内容密钥数据 KpDAS (Kc) 传送给用户装置 620（图 37 中的步骤（12）），并且等待用户装置 620 的响应。如果从用户装置 620 收到确认响应，则状态被设置成“传送完成”状态。但是，如果没有收到确认响应，则立即或者在重复预定次数之后终止该过程（本具体情况下为加密内容和加密内容密钥数据 KpDAS (Kc) 的传输），并且状态被设置成“传送失败”状态。

如果状态被改变成“传送完成”状态，则内容传送服务器 640 向票券交换服务器 650 传送电子票券（供 CP 使用）（图 37 中的步骤（22）），并等待票券交换服务器 650 的响应。如果从票券交换服务器 650 收到确认响应，则状态被设置成“完成票券交换请求的传输”状态。但是，如果没有收到确认响应，则立即或者在重复预定次数之后终止该过程（本具体情况下为票券交换请求的传输），并且把状态设置成“票券交换请求传输失败”状态。

如果状态被改变成“完成票券交换请求的传输”状态，则内容传送服务器 640 从票券交换服务器 650 接收交换过程报告，并验证接收的报告（图 37 中的步骤（24）和（25））。如果成功通过验证，则状态被设置成“完成交换过程报告的接收”状态，并且终止该过程。但是如果数据验证指出接收的报告无效，则立即或者在重复预定次数之后终止该过程（本具体情况下为报告的接收和验证），并且状态被设置成“交换报告接收失败”状态。在内容传送服务器 640 中，对

于各个内容交易按照上述方式改变状态。

下面参考图 51 说明用户装置 620 的状态转变。用户装置 620 通过向票券发行服务器 610 传送购买请求数据（图 37 中的步骤（3））启动一个过程。如果用户装置 620 从票券发行服务器 610 收到指出内容购买请求数据已被票券发行服务器 610 成功接收的响应，则状态被设置成“完成购买请求传输”状态。但是，如果没有收到指出内容购买请求数据已被票券发行服务器 610 成功接收的响应，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为购买请求的传输），并且把状态设置成“购买请求传输失败”状态。只有当状态为“完成购买请求传输”状态时过程才进行到下一步骤。

如果状态被改变成“完成购买请求传输”状态，则用户装置 620 从票券发行服务器 610 接收电子票券（图 37 中的步骤（7）和（8）），并验证接收的数据。如果从票券发行服务器 610 接收的票券被确定为有效，则状态被设置成“完成电子票券的接收”状态。但是，如果数据验证指出接收的票券无效，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为票券的接收），并且状态被设置成“电子票券接收失败”状态。只有当状态为“完成电子票券的接收”状态时过程才进行到下一步骤。

如果状态被改变成“完成电子票券的接收”状态，则用户装置 620 向内容传送服务器 640 传送电子票券（图 37 中的步骤（10）），并且等待内容传送服务器 640 的响应。如果从内容传送服务器 640 收到确认响应，则状态被改变成“完成电子票券的传输”状态。但是如果沒有收到确认响应，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为票券的传输），并且把状态设置成“电子票券传输失败”状态。只有当状态为“完成电子票券的传输”状态时过程才进行到下一步骤。

如果状态被改变成“完成电子票券的传输”状态，则用户装置 620 从内容传送服务器 640 接收加密内容和加密内容密钥 KpDAS (Kc)，并且验证接收的数据（图 37 中的步骤（12）和（13））。

如果成功通过数据验证，则状态被设置成“完成密钥 1 的接收”状态。但是，如果没有通过数据验证，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为密钥数据的接收），并且状态被设置成“密钥 1 传输失败”状态。

如果状态被改变成“完成密钥 1 的传输”状态，则用户装置 620 把电子票券（供 DAS 使用）和加密内容密钥 KpDAS（Kc）传送给用户装置验证服务器 630（图 37 中的步骤（15）），并等待用户装置验证服务器 630 的响应。如果从用户装置验证服务器 630 收到确认响应，则状态被设置成“完成密钥转换请求的传输”状态。但是，如果没有收到确认响应，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为电子票券（供 DAS 使用）和加密内容密钥 KpDAS（Kc）的传输），并且把状态设置成“密钥转换请求传输失败”状态。只有当状态为“完成密钥转换请求的传输”状态时过程才进行到下一步骤。

如果状态被改变成“完成密钥转换请求的传输”状态时，用户装置 620 从用户装置验证服务器 630 接收加密内容密钥 KpDAS（Kc），并验证接收的数据（图 37 中的步骤（18）和（19））。如果成功通过数据验证，则状态被设置成“完成密钥 2 的接收”状态。但是如果通过数据验证，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为密钥数据的接收），并且把状态设置成“密钥 2 接收失败”状态。

下面参考图 52 说明票券交换服务器 650 的状态转变。响应从具有根据电子票券接收一部分销售金额的权利的实体收到电子票券（图 37 中的步骤（22）和（27）），票券交换服务器 650 起动一个过程。票券交换服务器 650 验证接收的票券。如果成功通过验证，则状态被设置成“完成电子票券的接收”状态。但是，如果数据验证指出接收的数据无效，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为票券的接收），并且把状态设置成“电子票券接收失败”状态。只有当状态为“完成电子票券的接收”状态时过程才进

行到下一步骤。

如果状态被改变成“完成电子票券的接收”状态，则票券交换服务器 650 执行基于电子票券的交换过程。通过把电子票券（供 CP 使用）中规定的金额从用户装置的账户转移到管理内容传送服务器的内容提供者（CP）事先登记的银行账户或者电子货币账户中来完成交换过程。另一方面，可通过把在电子票券中规定的金额从票券发行服务器从用户预收的作为保证金的金额中转移到内容提供者（CP）的账户中来完成交换过程。在完成交换过程之后，状态被改变成“完成交换过程”状态。但是如果交换过程失败，则状态被改变成“交换过程失败”状态。

如果状态被改变成“完成交换过程”状态，则票券交换服务器 650 向传送票券的每个实体传送交换报告（图 37 中的步骤（24）和（29）），并且等待相应实体的响应。如果从每个实体收到确认响应，则状态被设置成“完成交换过程报告的传输”状态，并且终止该过程。但是，如果没有收到确认消息，则立即或者在重复该过程预定次数之后终止该过程（本具体情况下为交换过程报告的传输），并且状态被设置成“交换过程报告传输失败”状态。在票券交换服务器 650 中，对于各个内容交易按照上述方式改变状态。

图 53 图解说明其中票券发行者发出票券并且利用票券结清内容费用的系统的具体例子。如果票券发行者 801 从用户装置 802 收到内容购买请求，则票券发行者执行与内容交易相关的收费过程并且发出电子票券。这里，在根据用户的银行账户或者电子货币账户的余额规定的交易上限内发出电子票券。在图 53 中所示的例子中，票券发行者向用户装置发出收取 1000 日元内容费用的电子票券。

在图 53 中所示的例子中，总额 1000 日元被这样分配，以致 300 日元作为销售费用被支付给作为票券发行者的商店，100 日元作为许可费用被支付给操纵内容传送系统的许可证持有者（用户装置验证服务器）803，600 日元作为内容费用被支付给内容制作者（内容传送服务器）。

如果票券发行者 801 从用户装置收到购买请求，则票券发行者根据内容 ID 确定内容费用分配比例，并且向将接收内容费用的分配金额的所有实体发出同样多的电子票券。在图 53 中所示的例子中，票券发行者 801 发出用于向许可证持有者 803 支付 100 日元的许可证费用的电子票券和用于向用户内容制作者支付 600 日元的内容费用的电子票券，并且把这些电子票券传送给用户装置 802。注意传送的每个电子票券包括票券发行者写入的签名。

用户装置 802 分别把电子票券传送给许可证持有者 803 和内容制作者 804。许可证持有者 803 和内容制作者 804 验证接收的电子票券。在确认电子票券有效之后，许可证持有者 803 和内容制作者 804 的票券传送给银行（票券交换服务器）805。票券交换服务器 805 验证数字签名，以确认票券有效。确认之后，票券交换服务器 805 转移规定数量的金额。在上述过程中，银行（票券交换服务器）根据票券发行者写在电子票券上的签名验证票券。还验证票券中的购买请求数据中由用户装置写入的签名。

传送票券的内容制作者和许可证持有者可在包括电子票券的数据上写上他们的签名，银行（票券交换服务器）可验证这些签名。

在图 53 中所示的系统中，票券发行者（商店）801 自己向银行（票券交换服务器）805 传送电子票券，以便接收分配的内容费用金额，即本例中的 300 日元。

使用电子票券的上述交换过程确保分配的内容费用金额被正确地支付给相应的实体。如果内容制作者 804 从用户装置 802 收到电子票券，则内容制作者 804 验证接收的电子票券。验证之后，内容制作者 804 把利用内容密钥 K_c 加密的加密内容和利用许可证持有者（用户装置验证服务器）的公共密钥 K_{pDAS} 加密的加密内容密钥 $K_{pDAS}(K_c)$ 传送给用户装置 802。

用户装置 802 把从内容制作者 804 收到的加密内容密钥 $K_{pDAS}(K_c)$ 和电子票券（DAS）一起传送给许可证持有者 803。许可证持有者验证接收的电子票券。验证之后，许可证持有者对加密内容密钥

KpDAS (Kc) 进行密钥转换过程。即，通过利用用户装置的公共密钥 KpDEV 对内容密钥加密产生加密内容密钥 KpDEV (Kc)。所得到的加密内容密钥 KpDEV 被传送给用户装置 802。用户装置 802 利用用户装置 802 的保密密钥 KsDEV 对加密内容密钥 KpDEV (Kc) 解密，获得内容密钥 Kc。内容密钥 Kc 可保存在用户装置 802 中。这种情况下，在利用用户装置的存储密钥 Ksto 加密之后保存内容密钥 Kc。

本系统中，如上所述，如果内容传送服务器（例如内容提供者）收到票券发行者发出的票券，则内容传送服务器验证接收的票券。如果验证表明接收的票券有效，则内容传送服务器把加密内容和加密内容密钥传送给用户装置。另一方面，如果许可证持有者（用户装置验证服务器）收到电子票券，则许可证持有者验证收到的票券。如果验证表明收到的票券有效，则许可证持有者执行加密密钥转换，并且把所得到的密钥转换后的加密密钥传送给用户装置。从而确保分配的内容费用金额被正确地支付给相应的收款人，并且用户装置能够使用内容。

3. 日志记录服务器内容传送的管理

现在说明一种内容传送系统，其中涉及用户装置产生的购买的历史数据作为日志数据累积在用户装置中，并且由系统管理装置收集所述日志数据，从而使得能够监控内容散布的实际状态。

图 54 图解说明包括日志记录系统的内容传送系统。如图 54 中所示，该内容传送系统主要由向用户装置提供内容的商店服务器 (SHOP) 901、从商店服务器 901 接收内容的用户装置 (DEVICE) 902 和记录与内容交易相关的日志，从而管理内容交易的日志记录服务器 903 组成。内容传送系统还包括提供内容的内容提供者 905，产生各种信息，例如与从内容提供者 905 接收的内容相关的使用限制信息，把产生的信息作为标题添加到内容中，并且向商店服务器 901 提供所得到的数据的编辑服务器 904，和发出实体的公共密钥证书 (Cert_xxx) 的认证机构 (CA)。

在图 54 中所示的系统中，内容提供者 905 和编辑服务器 904 是向

商店服务器提供要散布内容的实体的例子。注意向商店服务器提供内容的方式并不局限于图 54 中所示，而是可以各种方式向商店服务器提供要散布的内容。例如，内容可由内容提供者直接提供给商店服务器。另一方面，内容可由具有该内容版权的作者通过若干服务提供者提供给商店服务器。

在图 54 中所示的系统中，出于简化和易于理解的目的，只采用一个内容提供者 905 作为具有接收一部分内容销售钱款的权利的实体的典型例子。在图 54 中所示的例子中，保证内容提供者 905 可接收按照根据由日志记录服务器 903 记录的日志数据管理的内容销售数据分配给内容提供者 905 的正确金额。在图 54 中所示的系统包括也具有接收一部分内容销售钱款的另一实体的情况下，该实体也可接收根据由日志记录服务器 903 记录的日志数据分配给它的正确金额。

在图 54 中所示的系统中，按照与在图 1 中的所示系统中采用的商店服务器相似方式构成商店服务器 901。即，商店服务器 901 包括能够执行加密/解密过程和通信过程的控制单元，商店服务器 901 藉此执行与不同装置的内容交易序列，并且管理内容交易期间的状态。内容提供者 905 和编辑服务器 904 都包括能够执行加密/解密过程和通信过程的控制单元，从而执行与不同装置的内容交易序列并且管理内容交易期间的状态。

用户装置

用户装置 902 的结构和上面参考图 7 说明的用户装置结构相似，包括能够进行加密/解密过程和通信过程的控制装置 230（图 7）。但是，本实施例的控制装置 230 的不同之处在于每次进行内容购买过程时控制装置 230 产生日志数据，并且把产生的日志数据保存到购买管理数据库 220 中。

图 55（A）和 55（B）图解说明由用户装置 902 产生并且保存于其中的日志数据的数据结构的两个例子。在图 55（A）中所示的例子中，日志数据包括识别用户装置 902 通过内容交易从商店服务器 901 获得的内容的内容 ID，识别用户装置的用户装置 ID（ID_DEV），识

别与之进行内容交易的商店的商店 ID (ID_SHOP)，和指出进行内容交易的日期的日期信息。此外，日志数据包括由用户装置写入的签名 (Sig_Dev)。当日志记录服务器从用户装置收到购买日志时，日志记录服务器验证写入其中的数字签名。在图 55B 中所示的例子中，日志数据包括销售数据，指出收到内容的日期的接收日期数据，和由用户装置写入的签名 (Sig_Dev) 销售数据由商店服务器 901 响应用户装置 902 发出的内容购买请求而产生，以便指出该内容已售出。后面将更详细地说明销售数据。

在内容购买过程中，用户装置 902 产生诸如图 55 中所示的日志数据，并将其保存到用户装置 902 中。日志数据还被传送给日志记录服务器 903。更具体地说，当用户装置更新用户装置的公共密钥证书时，用户装置把截止到该时刻已保存的日志数据传送给日志记录服务器 903。后面将更详细地说明上述过程的顺序。

日志记录服务器

图 56 图解说明日志记录服务器 903 的结构。如图 56 中所示，日志记录服务器 903 包括日志管理数据库 9031。日志管理数据库 9031 保存从不同的用户装置接收的日志数据（图 55）。

日志记录服务器 903 包括与诸如用户装置 902 之类的装置或者与商店服务器 901 通信，并且在通信过程中进行加密/解密的控制装置 9032。和前面说明的商店服务器的控制装置的情况一样，控制装置 9032 也用作加密/解密装置和通信装置。按照和前面参考图 4 说明的相似方式构成控制装置 9032。控制装置 9032 的加密装置在加密过程中使用的密钥数据等以安全的方式保存在控制装置的存储装置中。供加密过程之用，保存在日志记录服务器 903 中的诸如加密密钥之类的数据包括日志记录服务器 903 的保密密钥 KsLOG，日志记录服务器 903 的公共密钥证书 Cert_LOG，和发出公共密钥证书的认证机构 (CA) 的公共密钥 KpCA。

响应从用户装置 902 收到日志数据，日志记录服务器 903 执行公共密钥证书发出过程。更具体地说，当日志记录服务器 903 从用户装

置 902 收到将作为更新公共密钥的公共密钥时，日志记录服务器 903 把收到的公共密钥传送给认证机构 906，并且请求认证机构 906 发出公共密钥证书。如果日志记录服务器 903 收到认证机构 906 发出的公共密钥证书，则日志记录服务器 903 将其传送给用户装置 902。后面将更详细地说明该过程的序列。

A. 内容购买过程

在本实施例中，过程包括如下列举并且同样显示在图 54 上部的四部分。

- A. 内容购买过程
- B. 日志的传输和公共密钥证书的更新
- C. 内容销售的准备
- D. 销售额的检查

下面说明该过程的各个部分。

A. 内容购买过程

如下参考图 57 和 58 中所示的流程图说明的那样进行内容购买过程。在图 57 和 58 中，由用户装置进行的过程表示在左侧，由商店服务器进行的过程表示在右侧。过程一开始，如图 57 中所示，在商店服务器和用户装置之间进行相互验证（步骤 S1501 和 S1601）。

按照上面参考图 13 说明的相似方式利用公共密钥进行相互验证。更具体地说，通过利用由认证机构（CA）906 发出的，并且具有分配给其的有效期的公共密钥证书来进行相互验证。为了通过相互验证，要求用户装置具有其有效期还未期满的公共密钥证书。如后所述，为了更新公共密钥证书，要求向日志记录服务器 903 传送日志。

根据需要使用在相互验证过程中产生的话路密钥 Kses 在相互验证之后进行的通信中对数据加密，或者产生 ICV（完整性检查值）。后面将更详细地说明 ICV 的产生。

如果成功通过相互验证，则用户装置基于随机数产生应用于当前内容交易的交易 ID，并且产生内容购买请求数据（步骤 S1502）。图 59A 图解说明购买请求数据的格式的例子。

购买请求数据包括上面说明的交易 ID (TID_DEV)，识别内容的内容 ID，识别用户装置的用户装置 ID (ID_DEV)，内容价格，发出购买请求的日期/时间，和用户装置的签名 (Sig.Dev)。

此外，用户装置产生购买请求数据的完整性检查值 (ICV)，并将其传送给商店服务器 (步骤 1503)。在上述过程中，通过把散列函数应用于要检查完整性的数据来确定完整性检查值 (ICV)，例如 $ICV = \text{hash} (Kicv, C1, C2 \dots)$ ，其中 $Kicv$ 是 ICV 产生密钥， $C1$ 和 $C2$ 是要检查完整性的数据的信息，并且要检查数据的重要信息的消息验证码 (MAC) 被用作 $C1$ 和 $C2$ 。

图 60 图解说明利用 DES 加密过程产生 MAC 值方法的例子。如图 60 中所示，感兴趣的消息被分成若干部分，每个部分都由 8 个字节组成 (下面消息的分割部分用 $M1, M2, \dots MN$ 表示)。首先，计算初始值 (IV) 和 $M1$ 之间的异或 (其中结果由 $I1$ 表示)。之后，把 $I1$ 应用于 DES 加密单元，利用密钥 ($K1$) 对 $I1$ 加密 (其中加密后的输出用 $E1$ 表示)。计算 $E1$ 和 $M2$ 之间的异或，并且把结果 $I2$ 应用于 DES 加密单元，从而利用密钥 $K1$ 对其加密 (其中所得到的结果表示为 $E2$)。之后，重复上述过程直到该消息的所有部分被加密为止。最终的输出 EN 被用作消息验证码 (MAC)。在上述过程中，要检查的数据的一部分被用作该消息。

数据的完整性检查值 (ICV) 由利用 ICV 产生密钥 $Kicv$ 产生的 MAC 值给出。在接收装置，为收到的数据产生 ICV，并且把该 ICV 与为确保有效的数据，例如由原始数据的传送装置产生的数据产生的 ICV 进行比较。如果比较结果指出 ICV 相等，则确定该数据未被篡改。如果比较结果指出 ICV 不同，则确定数据已被篡改。

这里，在相互验证过程中产生的话路密钥 $Kses$ 被用作 ICV 产生密钥。用户装置通过利用话路密钥 $Kses$ 产生购买请求数据 (图 59A) 的完整性检查值 ($ICV1$)，并且把购买请求数据和 $ICV1$ 一起传送给商店服务器。

商店服务器通过把话路密钥 $Kses$ 应用于接收的数据产生完整性

检查值 $ICV1'$, 并将其和从用户装置接收的 $ICV1$ 进行比较, 以确定 $ICV1$ 是否等于 $ICV1'$ 。如果 $ICV1=ICV1'$, 则确定数据未被篡改。此外, 商店服务器验证写入购买请求数据中的数字签名(步骤 S1603)。通过利用用户装置的公共密钥进行数字签名的验证。从用户装置的公共密钥证书 $Cert_DEV$ 抽取公共密钥。这里, 要求公共密钥证书的有效期还没有到期。如果公共密钥证书的有效期已经期满, 则商店服务器在签名的验证中不使用该公共密钥证书, 并且购买请求被拒绝。如果成功通过 ICV 的检查和签名的验证, 则商店服务器产生销售数据(步骤 S1604)。

销售数据具有图 59B 中所示的数据结构。销售数据包括由商店服务器产生的交易 ID(TID_SHOP), 识别商店的商店 ID(ID_SHOP), 销售日期/时间, 和表示要支付给管理员的售出内容的费用金额的管理费信息。这里, 管理员指的是内容销售系统的管理实体(系统拥有者)。在图 54 中所示的例子中, 管理员是管理日志记录服务器 903 的实体。

销售数据还包括指出要支付给内容提供者的要给予 CP 的金额信息。销售数据还包括购买请求数据(图 59A), 并且商店的签名($Sig.SHOP$)被写入销售数据中。

在图 59B 中所示的销售数据的数据结构中, 在销售数据中描述的获利共享信息只包括指出要支付给两个实体, 即操纵系统的系统持有者(SH)和内容提供者(CP)的金额的信息。但是, 如果还有其它实体接收分配的内容费用金额, 则还要描述要支付给这些实体的金额。

如果在通过 ICV 检查和签名验证之后产生销售数据(步骤 S1604), 则商店服务器产生指出购买请求已被接受的购买请求接受数据, 并且利用话路密钥 $Kses$ 产生购买请求接受数据的完整性检查值($ICV2$)。购买请求接受数据和相关的完整性检查值($ICV2$)被传送给用户装置(步骤 S1605)。在 ICV 检查或者签名验证失败的情况下, 商店服务器产生包括指出购买请求已被拒绝的消息的购买请求拒绝数据, 并且利用话路密钥 $Kses$ 产生购买请求拒绝数据的完整性检查值($ICV2$)。购买请求拒绝数据和完整性检查值($ICV2$)一起被传送给

用户装置（步骤 S1606）。

在商店服务器已把购买请求接受数据传送给用户装置的情况下，商店服务器还把销售数据（图 59B），带有利用话路密钥 Kses 产生的完整性检查值（ICV3）的标题（与内容相关的信息，包括指出使用内容的方式的信息）和内容传送给用户装置（步骤 S1607）。

如果用户装置收到内容、购买请求响应（接受或拒绝）数据和完整性检查值 ICV2（步骤 S1504），则用户装置验证 ICV2 并且检查购买请求响应（步骤 S1505）。如果 ICV2 的检查指出数据未被篡改，并且如果购买请求已被接受，则用户装置接收销售数据（图 59B）和带有完整性检查值（ICV3）的标题（与内容相关的信息，包括指出使用内容的方式的信息）（步骤 S1506）。用户装置检查 ICV3 并且验证写入销售数据中的签名。如果 ICV3 和签名都有效，则用户装置把内容接收确认响应和相关的完整性检查值 ICV4 一起传送给商店服务器。

但是，如果判定步骤 S1507 的答案为否，则过程跳到步骤 S1509，其中用户装置把内容接收失败响应和相关的完整性检查值 ICV4 一起传送给商店服务器。

如果商店服务器收到内容接收响应（确认或者否定确认）和相关的完整性检查值 ICV4（步骤 S1608），则商店服务器检查 ICV4（步骤 S1611）。在来自用户装置的响应指出内容已被用户装置成功接收的情况下，商店服务器针对售出内容向用户装置收费（步骤 S1613）。和前一实施例中一样，通过从用户装置的账户或者信用卡账户接收规定的金额，完成收费过程。在收费过程之后，商店服务器把收费完成消息和相关的完整性检查值 ICV5 传送给用户装置（步骤 S1614）。在步骤 S1611 或者 S1612 的答案为否的情况下，过程跳到步骤 S1615。在步骤 S1615，商店服务器把收费失败消息和相关的完整性检查值 ICV5 一起传送给用户装置。

如果用户装置收到收费完成（或者收费失败）消息和相关的完整性检查值 ICV5，则用户装置检查 ICV5，并且确定收费是否已成功完成。如果确定收费已成功完成，则用户装置产生购买日志（图 55）并

将其保存到用户装置的存储器中。之后，用户装置使用内容。在步骤 S1512 或 S1513 中答案为否的情况下，过程跳到步骤 S1514。在步骤 S1514 中，用户装置删除从商店服务器接收的标题和内容。

参见图 61 和 62，说明在用户装置和日志记录服务器之间进行的密钥更新过程和日志传输过程。在图 61 和 62 中，由用户装置执行的过程表示在左侧，由日志记录服务器执行的过程表示在右侧。当希望从商店服务器购买内容的用户装置更新保存在用户装置中的用户装置的公共密钥证书时执行这些过程。只有在规定的有效期内用户装置的公共密钥证书才是有效的，从而需要每隔一段特定的时间更新公共密钥证书。首先说明图 61 中表示的过程。

首先，在用户装置和日志记录服务器之间进行相互验证（步骤 S1521 和 S1721）并产生话路密钥。如果成功通过相互验证，则用户装置从用户装置的存储器读取购买日志，并且把购买日志和利用话路密钥 Kses 产生的相关完整性检查值（ICV1）一起传送给日志记录服务器（步骤 S1522）。

如果日志记录服务器收到购买日志和相关的完整性检查值 ICV1（步骤 S1722），则日志记录服务器检查 ICV1（步骤 S1723）。如果 ICV1 有效，则日志记录服务器把接收的购买日志保存到数据库中（步骤 S1724）。日志记录服务器还可验证由用户装置写入购买日志中的数字签名，以确认购买数据未被篡改。随后日志记录服务器把日志接收确认数据和利用话路密钥 Kses 产生的相关完整性检查 ICV2 一起传送给用户装置（步骤 S1725）。但是，如果步骤 S1723 中 ICV1 的验证失败，则日志记录服务器把日志接受失败消息和利用话路密钥 Kses 产生的相关完整性检查值 ICV2 一起传送给用户装置（步骤 S1726）。

如果用户装置收到日志接收消息和相关的完整性检查值 ICV2（步骤 S1523），则用户装置验证完整性检查 ICV2。如果 ICV2 有效并且如果日志接收消息指出日志数据已被日志记录服务器成功接收（步骤 S1524），则用户装置产生将被用作更新后的公共密钥的公共密钥（KpDEV）和对应的保密密钥（KsDEV）（步骤 S1525），并把产生

的公共密钥（KpDEV）和相关的完整性检查值（ICV3）一起传送给日志记录服务器（步骤 S1526）。

如果日志记录服务器从用户装置收到公共密钥（KpDEV）和相关的完整性检查值 ICV3，则日志记录服务器验证完整性检查值 ICV3（步骤 1731）。如果成功通过验证，则日志记录服务器把公共密钥接收确认消息和相关的完整性检查值 ICV4 一起传送给用户装置（步骤 S1732）。但是，如果验证指出完整性检查值 ICV3 无效，则日志记录服务器把公共密钥接收失败消息和相关的完整性检查值 ICV4 一起传送给用户装置（步骤 S1733）。

在日志记录服务器把公共密钥接收确认消息和相关的完整性检查值 ICV4 一起传送给用户装置（步骤 S1732）的情况下，日志记录服务器把接收的公共密钥传送给认证机构（CA），并且请求认证机构发出公共密钥证书。如果日志记录服务器收到更新后的用户装置的公共密钥证书（Cert_DEV）（步骤 S1734），则日志记录服务器把更新后的公共密钥证书（Cert_DEV）和相关的完整性检查值 ICV5 一起传送给用户装置（步骤 S1735）。

如果用户装置收到公共密钥接收确认/失败消息和相关的完整性检查值 ICV4，则用户装置验证完整性检查值 ICV4。如果完整性检查值 ICV4 有效，并且如果公共密钥已被日志记录服务器成功接收（步骤 S1532），则用户装置接收更新后的公共密钥证书及相关的完整性检查值 ICV5（步骤 S1533）并验证完整性检查值 ICV5 和收到的公共密钥证书（步骤 S1534）。如果成功通过完整性检查值 ICV5 和公共密钥证书的验证，则用户装置从公共密钥证书抽取公共密钥，并将其和用户装置传送的初始公共密钥进行比较（步骤 S1535）。如果接收的公共密钥和初始的公共密钥相同，则用户装置把对应于更新后的公共密钥的保密密钥和接收的公共密钥证书保存到用户装置的存储器中（步骤 S1536）。随后用户装置删除该日志（该日志已被传送给日志记录服务器）（步骤 S1537）。

在判定步骤 S1532、S1534 和 S1535 之一中答案为否的情况下，不

更新公共密钥证书并且终止该过程。

下面参考图 63 中所示的流程图说明在内容提供者和日志记录服务器之间进行的检查销售额的过程。日志记录服务器保存销售钱款共享信息，所述销售钱款共享信息指出根据从用户装置收到的购买日志把作为内容费用收取的钱款给予一个实体或者在若干实体之间分配的方式。响应收到销售额通知请求，日志记录服务器根据获利共享信息传送响应消息。日志记录服务器可根据在购买日志中描述的内容 ID 以及根据获利共享信息，计算已销售内容的要支付给相应实体的金额。在日志记录服务器收到的日志数据包括图 55B 中所示的销售数据的情况下，日志记录服务器可根据在销售数据中描述的获利共享信息，计算要支付给相应实体的金额。

首先，在内容提供者和日志记录服务器之间进行相互验证（步骤 S1521 和 S1721），产生话路密钥 Kses。如果成功通过相互验证，则日志记录服务器从内容提供者（CP）的公共密钥证书 Cert_CP 抽取内容提供者的标识符 ID_CP（步骤 S1722），并且根据保存在数据库中的日志信息产生指出要支付给由 ID_CP 指示的内容提供者的金额的销售额数据（步骤 S1723）。如上所述，获得的日志数据包括指出要支付给内容提供者的金额的数据，并且据此确定要支付给相应内容提供者的金额。日志记录服务器把销售额数据和相关的完整性检查值 ICV1 一起传送给内容提供者（CP）（步骤 S1724）。

如果内容提供者（CP）从日志记录服务器收到销售额数据和相关的完整性检查值 ICV1（步骤 S1522），则内容提供者（CP）检查完整性检查值 ICV1，确认数据未被篡改（步骤 S1523），并且把销售额数据保存到存储器中（步骤 S1524）。如果完整性检查值 ICV1 的验证指出数据已被篡改，则不把数据保存到存储器中，并且终止处理过程。这种情况下，内容提供者（CP）重新向日志记录服务器发送销售额数据请求。

现在参见图 64 和 65 中所示的流程图，下面说明在商店服务器、日志记录服务器和内容提供者之间进行的销售额报告过程。商店服务

器保存并管理指出内容销售额的数据。商店服务器传送指出特定时期的销售额的所有数据或者传送指出各个实体的销售额的数据。图 64 图解说明其中指出由商店服务器完成的内容销售交易的所有数据被传送给日志记录服务器的过程。图 65 图解说明其中指出由特定内容提供者提供的内容的销售额有选择地被传送给该特定内容提供者的过程。

首先说明图 64 中所示的过程。首先在商店服务器和日志记录服务器之间进行相互验证(步骤 S1631 和 S1731), 并且产生话路密钥 Kses。如果成功通过相互验证, 则商店服务器读取特定时段的所有销售额数据, 并把它们和相关的完整性检查值 ICV1 一起传送给日志记录服务器 (步骤 S1632)。

如果日志记录服务器从商店服务器收到所有销售额数据和相关的完整性检查值 ICV1 (步骤 S1732), 则日志记录服务器验证完整性检查值 ICV1, 以确认该数据未被篡改 (步骤 S1733)。确认之后, 日志记录服务器把所有销售额数据保存到存储器中 (步骤 S1734)。但是, 如果完整性检查值 ICV1 的验证指出该数据无效, 则终止该过程, 而不把该数据保存到存储器中。这种情况下, 日志记录服务器重新请求商店服务器传送销售额数据。

现在参考图 65, 说明特定内容提供者的销售额数据的传输过程。首先, 在商店服务器和内容提供者之间进行相互验证 (步骤 S1641 和 S1741), 并且产生话路密钥 Kses。如果成功通过相互验证, 则商店服务器从内容提供者的通过相互验证过程获得的公共密钥证书 Cert_CP 读取内容提供者的标识符 ID_CP (步骤 S1642)。商店服务器根据抽取的标识符 ID_CP 取回销售额数据, 从而获得由特定内容提供者提供的内容的销售额数据 (步骤 S1643)。随后商店服务器把销售额数据和相关的完整性检查值 ICV1 一起传送给日志记录服务器(步骤 S1644)。

如果日志记录服务器从商店服务器收到销售额数据和相关的完整性检查值 ICV1 (步骤 S1742), 则日志记录服务器验证完整性检查值 ICV1, 以确定该数据未被篡改 (步骤 S1743)。确认之后, 日志记录

服务器把销售额数据保存到存储器中（步骤 S1744）。但是，如果完整性检查值 ICV1 的验证指出数据已被篡改，则终止该过程，不把数据保存到存储器中。这种情况下，日志记录服务器重新请求商店服务器传送销售额数据。

本系统中，能够响应用户装置的公共密钥证书的更新而获得内容购买日志数据，从而确保管理日志记录服务器的系统持有者能够了解关于内容销售的实际状态。在和商店服务器的相互验证中需要用户装置的公共密钥证书，其中为了购买内容，要求公共密钥证书的有效期尚未期满。此外，由于利用从公共密钥证书抽取的公共密钥验证写入由用户装置发出的购买请求数据等中的签名，因此还要求用户装置应具有尚未期满的公共密钥证书。即，为了购买内容，用户装置需要把日志数据传送给日志记录服务器，并且用户装置需要在公共密钥证书的有效期期满之前更新公共密钥证书。公共密钥证书的有效期可被设置成例如一个月或三个月，从而管理日志记录服务器的系统持有者可累积规定的有效期内的日志数据。

从而，确保日志记录服务器的系统持有者能够从用户装置获得日志数据，从而能够监控和管理内容销售的状态。此外，能够根据在日志数据中描述的获利共享信息正确地把分配的金额支付给相应的收款人，例如内容提供者。

此外，在本实施例中，通过把在相互验证中产生的话路密钥 Kses 用作生成密钥，产生用于将在实体之间传送的数据的完整性检查值 (ICV)，并且数据和产生的完整性检查值 (ICV) 一起被传送，从而获得数据传输方面的高安全性。

虽然在上述实施例中，执行了用户装置和商店服务器之间的相互验证，签名的产生和签名的验证，不过也可只执行这些过程之一。例如，可进行相互验证，签名的产生或者签名的验证。这种情况下，当执行这些过程之一时，都需要尚未到期的公共密钥证书。

4. 属性证书和包括属性数据的公共密钥证书的使用

下面说明属性证书或包括属性数据的公共密钥证书的使用方式。

在按照上述方式之一构成的内容传送系统中，商店持有者可能假装表现为用户装置并且进行欺诈的内容交易。还可能在内容提供者和商店之间进行欺诈的内容交易。此外，当用户装置起动与某些服务器的通信，试图进行授权的交易时，如果服务器假装表现为是获得授权的商店服务器，则当用户装置把指示用户装置的信用卡账号的数据传送给欺诈服务器以便购买内容时，该服务器有可能欺诈获得用户装置的信用卡账号。用户装置也有可能假装它是商店，欺诈地把内容销售给另一用户装置。这样的欺诈行为使得系统管理员难以了解内容散布的实际状态。

如下所述，属性证书或包括属性数据的公共密钥证书可用于防止这样的欺诈交易。

属性数据指的是指出实体类型的数据，所述实体是内容传送系统的一个成员，例如用户装置（DEVICE）、商店（SHOP）、内容提供者（CP）、系统持有者（SH）或者发出授权公共密钥证书或者属性证书的认证机构。

图 66 是图解说明在属性数据中描述的数据的一些例子的表格。如图 66 中所示，不同的代码被分配给相应的实体。例如，“0000”被分配给从商店的用户装置接收关于公共密钥证书或者属性证书的发出请求，并且检查该请求的认证机构。“0001”作为属性代码被分配给接收通过内容传送系统散布的内容的许可费用的服务提供者或者系统持有者。在前面说明的例子中，服务提供者是操纵执行密钥转换过程的用户装置验证服务器的实体或者操纵获得并记录日志信息的日志信息记录服务器的实体。

类似地，“0002”被分配给向用户装置销售内容的商店，“0003”被分配给内容提供者，即操纵内容传送服务器响应商店（内容销售者）发出的请求，把内容传送给用户的实体，“0004”被分配给购买并使用内容的用户装置。另外，根据实体的类型，把不同的代码分配给与内容传送相关的其它实体。并不要求只向商店分配一个代码。如果存在角色或功能不同的多个商店，则根据角色或者功能可分配不同的

代码，以便区分这些商店。类似地，根据某些类别可向用户装置分配不同的属性代码。

可在公共密钥证书中说明属性信息。另一方面，可在和公共密钥证书分开发出的属性证书中说明属性信息。图 67 图解说明包括属性信息的公共密钥证书的格式例子。

在图 67 中所示的例子中，公共密钥证书包括证书的版本编号，由公共密钥认证机构（CA）分配给证书的用户的证书序列号，用于写入签名的算法和参数，认证机构的名称，证书的有效期，证书用户的名称（例如用户装置 ID），证书用户的公共密钥，诸如“0000”、“0001”、“…”、“nnnn”之类上述属性信息和数字签名。证书的序列号可由例如总共 16 个字节表示，所述 16 个字节包括分别表示发出证书日期的年、月、日的 4 个、2 个、2 个字节，再加上 8 个字节的序列号。用户名称可以是由认证机构给出的名称，或者可由随机数或者序列号给出。另一方面，用户的名称可由指出类别的高位字节加上指出序列号的低位字节表示。

数字签名是通过把散列函数应用于包括证书的版本编号、由公共密钥认证机构（CA）分配给证书的用户的证书序列号，用于写入签名的算法和参数，认证机构的名称，证书的有效期，证书用户的名称，证书用户的公共密钥以及属性数据的整个数据，并且随后利用认证机构的保密密钥对所得到的散列值加密产生的数据。

公共密钥认证机构（CA）发出如图 67 中所示的公共密钥证书，当公共密钥证书的有效期到期时更新公共密钥证书，并且产生、管理和分发有欺诈行为的用户名单，以便排除这些用户（这个过程被称为撤销）。

当用户使用公共密钥证书时，用户通过利用用户持有的认证机构的公共密钥 K_pCA 验证写入公共密钥证书上的数字信号。如果成功通过验证，则用户从公共密钥证书抽取公共密钥，并且使用抽取的公共密钥。于是，要求希望使用公共密钥证书的任意用户具有公共密钥认证机构的共用公共密钥。

图 68A 图解说明不包括任何属性信息的公共密钥证书的数据格式，图 68B 图解说明属性证书的数据格式。如图 68A 中所示，不具有任何属性信息的公共密钥证书由除属性信息之外包含在图 67 中所示的公共密钥证书中的数据组成。这种公共密钥证书也由公共密钥认证机构发出。另一方面，属性证书由属性认证机构（AA）发出。

图 68B 中所示的属性证书包括证书的版本编号和对应于由属性认证机构（AA）发出的属性证书的公共密钥证书的序列号。所提供的序列号和对应公共密钥证书的序列号相同，以致该序列号用作使两种证书彼此相连的连接数据。当实体希望使用属性证书检查正在与其进行通信的另一实体的属性时，该实体首先通过检查属性证书的序列号和公共密钥证书的序列号相同，来确认属性证书是与公共密钥证书相连的属性证书，随后该实体从属性证书读取属性信息。证书的序列号可由例如总共 16 个字节表示，所述 16 个字节包括分别指示发出证书日期的年、月、日的 4 个、2 个、2 个字节，以及 8 个字节的序列号。属性证书还包括用于写入数字签名的算法和参数，属性认证机构的名称，证书的有效期以及证书用户的名称（例如用户装置 ID）。证书的用户名称和公共密钥证书的用户名称相同，其中由认证机构以可区别的形式确定该名称。证书的用户名称也可由随机数或者序列号给出。另一方面，证书的用户名称可由表示类别的高位字节加上表示序列号的低位字节表示。属性证书还包括诸如“0000”、“0001”…、“nnnn”之类属性信息和属性认证机构（AA）的数字签名。

通过把散列函数应用于包括证书的版本编号，公共密钥证书的序列号，用于写入数字签名的算法和参数，认证机构的名称，证书的有效期，证书的用户名称和属性数据的整体数据从而产生散列值，随后利用属性认证机构的保密密钥对所得到的散列值加密产生数字签名。

属性认证机构（AA）发出如图 68B 中所示的属性证书，当属性证书的有效期到期时更新属性证书，并且产生、管理和分发有欺诈行为的用户名单，以便排除这些用户（该过程被称为撤销）。

图 69 图解说明新发出由参与内容交易的新用户装置和新商店服

务器使用的公共密钥证书的过程。这里，假定商店服务器 1010 和用户装置 1020 的结构和前面参考图 1 说明的结构相似。服务提供者或者系统持有者 (SH) 1030 管理整个内容传送过程。具体地说，服务提供者执行上述内容密钥转换过程，并且获得当用户装置购买内容时由用户装置产生的日志信息，从而监控内容散布的状态。在图 69 中所示的例子中，服务提供者还用作接收并检查来自商店服务器 1010 或用户装置 1020 的公共密钥证书或者属性证书发出请求的注册机构 (RA)。虽然在图 69 中所示的本系统中，服务提供者 1030 作为系统持有者 (SH) 和注册机构 (RA)，但是也可由不同的实体单独实现这些功能。

在图 69 中，与向用户装置 1020 发出新的公共密钥证书相关的程序包括步骤 (A1) - (A8)，与向商店服务器 1010 发出新的公共密钥证书相关的程序包括步骤 (B1) - (B7)。首先说明向用户装置 1020 新发出公共密钥证书的程序。

(A1) 相互验证

首先在用户装置 1020 和服务提供者 1030 之间进行相互验证。但是此时用户装置 1020 还不具有公共密钥证书，从而在相互验证中用户装置 1020 不能使用公共密钥证书。为此，根据前面参考图 12 说明的对称密钥加密法进行相互验证。即，利用共用保密密钥和标识符 (ID) 进行相互验证 (该过程的细节参见图 12)。

(A2) 公共密钥和对应保密密钥的产生

(A3) 请求发出公共密钥证书

(A4) 请求的检查及请求发出公共密钥证书，和

(A5) 请求发放公共密钥证书

相互验证之后，用户装置 1020 利用用户装置 1020 的加密单元产生要注册的公共密钥和对应的保密密钥，并且把证书发出请求和产生的公共密钥一起传送给服务提供者 1030。当收到发放公共密钥证书的请求时，服务提供者 1030 检查该请求。如果确定用户装置 1020 满足希望获得公共密钥证书的实体应满足的条件时，服务提供者 1030 把证书发放请求传送给公共密钥认证机构 (CA) 1040。在上述过程中，如

果要发出的公共密钥证书应包括如图 68A 中所示的属性信息，则服务提供者 1030 根据实体的 ID 确定已发出证书发放请求的实体。

参与内容传送的用户装置具有事先保存的用户装置标识符 (ID) 和保密密钥 (保密信息)，其中用户装置 ID 和保密密钥由服务提供者 1030 管理。服务提供者 1030 根据从用户装置接收的 ID 检查保密信息数据库，以确认用户装置 ID 已注册。确认之后，服务提供者 1030 抽取保密密钥，按照图 12 中所示的方式利用抽取的保密密钥执行与用户装置的相互验证。只有当成功通过相互验证时，服务提供者 1030 才确定用户装置是允许参与内容传送的授权装置。

- (A6) 公共密钥证书的发放
- (A7) 公共密钥证书的传输，和
- (A8) 公共密钥证书的传输

如果公共密钥认证机构 1040 从服务提供者 1030 收到发放公共密钥证书的请求，则公共密钥认证机构 1040 发出包括用户装置的公共密钥和公共密钥认证机构 1040 的数字签名的公共密钥证书（呈图 67 或 68A 中所示的形式）。所得到的公共密钥证书被传送给服务提供者 1030。服务提供者 1030 把从公共密钥认证机构 1040 收到的公共密钥证书传送给用户装置 1020。用户装置 1020 把收到的公共密钥证书和在步骤 (A2) 中产生的保密密钥保存到用户装置 1020 中，从而可在相互验证、数据加密、数据解密等中使用公共密钥证书。

除了商店服务器 1010 必须被服务提供者 1030 授权为内容销售实体之外，执行的向商店服务器 1010 发出公共密钥证书的过程基本上类似于执行的向用户装置发出公共密钥证书的过程。为此，商店服务器 1010 需要把商店服务器 1010 的公共密钥传送给服务提供者 1030，并且请求服务提供者 1030 授予许可证（图 69 中的 B2）。只有当商店服务器 1010 同意遵守由服务提供者 1030 建立的内容销售政策时，才授予许可证。如果服务提供者 1030 确定商店服务器 1010 具有根据服务提供者 1030 建立的政策销售内容的能力，并且如果商店服务器 1010 同意遵守该政策，则服务提供者 1030 执行向商店服务器 1010 发出公

共密钥证书所必需的过程。发出公共密钥证书的后续过程类似于上面说明的向用户装置发出公共密钥证书的过程。

下面参考图 70 说明更新公共密钥证书的过程。如图 67 或 68A 中所示，公共密钥证书只在规定的一段时间内有效。如果公共密钥证书的有效期已期满，则实体不能使用该公共密钥证书。于是，在当前的公共密钥证书到期之前需要进行更新过程，以便获得有效期更新后的公共密钥证书。

在图 70 中，更新用户装置 1020 的公共密钥证书的程序包括步骤 (A1) - (A8)，更新商店服务器 1010 的公共密钥证书的程序包括步骤 (B1) - (B7)。首先说明更新用户装置 1020 的公共密钥证书的程序。

(A1) 相互验证

首先在用户装置 1020 和服务提供者 1030 之间进行相互验证。此时，用户装置 1020 已具有目前有效的公共密钥证书，从而按照前面参考图 13 说明的相似方式利用公共密钥证书进行相互验证。但是，如果用户装置 1020 的公共密钥证书已到期，则可按照和在上面参考图 12 说明的发出新的公共密钥证书的过程中进行的相互验证相似的方式，根据标识符 (ID) 利用共用保密密钥进行相互验证。

(A2) 新的公共密钥和对应保密密钥的产生

(A3) 请求更新公共密钥证书

(A4) 请求的检查和请求更新公共密钥证书

(A5) 请求更新公共密钥证书

在成功通过相互验证之后，用户装置 1020 利用用户装置 1020 的加密单元产生将在更新后的证书中使用的公共密钥以及对应的保密密钥，并且把证书更新请求和产生的公共密钥一起传送给服务提供者 1030。当收到更新公共密钥证书的请求时，服务提供者 1030 检查接收的更新请求。如果必要的条件被满足，则服务提供者 1030 把证书更新请求传送给公共密钥认证机构 (CA) 1040。在上述过程中，如果要发出的公共密钥证书应包括如图 68A 中所示的属性信息，则服务提供者

1030 根据实体的 ID 确定发出证书更新请求的实体。

- (A6) 公共密钥证书的更新
- (A7) 公共密钥证书的传输，和
- (A8) 公共密钥证书的传输

如果公共密钥认证机构 1040 从服务提供者 1030 收到更新公共密钥证书的请求，则公共密钥认证机构 1040 发出包括用户装置的新公共密钥和公共密钥认证机构 1040 的数字签名的公共密钥证书（呈图 67 或图 68A 中所示的形式）。所得到的公共密钥证书被传送给服务提供者 1030。服务提供者 1030 把从公共密钥认证机构 1040 收到的公共密钥证书传送给用户装置 1020。用户装置 1020 把收到的公共密钥证书和在步骤 (A2) 中产生的保密密钥保存到用户装置 1020 中，从而可在相互验证、数据加密、数据解密等中使用公共密钥证书。

除了必须更新许可证（图 70 中的 (B2)）之外，执行的更新商店服务器 1010 的公共密钥证书的过程基本上类似于更新用户装置的公共密钥证书的过程。如果服务提供者 1030 确定将允许更新商店服务器 1010 的许可证，则服务提供者 1030 执行更新商店服务器 1010 的公共密钥证书所必需的后续过程。执行的更新公共密钥证书的后续过程类似于关于用户装置的上述过程。

参见图 71，说明新发出属性证书的过程。这里，假定属性证书具有图 68B 中所示的形式。在发出呈图 68A 中所示形式的公共密钥证书之后发出属性证书。在图 71 中，与向用户装置 1020 发出新的属性证书相关的程序包括步骤 (A1) - (A7)，和向商店服务器 1010 发出新的属性证书相关的程序包括步骤 (B1) - (B7)。首先说明向用户装置 1020 新发出属性证书的程序。

(A1) 相互验证

首先在用户装置 1020 和服务提供者 1030 之间进行相互验证。此时，用户装置 1020 已具有由公共密钥认证机构发出的公共密钥证书，从而利用该公共密钥证书进行相互验证。

(A2) 请求发出属性证书

(A3) 检查请求和请求发出公共密钥证书，和

(A4) 请求发出属性证书

如果成功通过相互验证，则用户装置 1020 把关于发出属性证书的请求传送给服务提供者 1030。响应收到发出属性证书的请求，服务提供者 1030 检查收到的请求。如果确定接收的请求满足该实体应满足的要求，则服务提供者 1030 把证书发出请求传送给属性认证机构 (AA) 1050。在上述检查过程中，服务提供者 1030 根据实体的 ID 检查已传出证书发出请求的实体的属性。如前所述，参与内容传送的任何用户装置都具有事先保存的它们自己的用户装置标识符 (ID)，其中用户装置 ID 由服务提供者 1030 管理。服务提供者 1030 把从用户装置收到的用户装置 ID 和在服务提供者 1030 中登记的用户装置 ID 进行比较，检查该用户装置是否是允许参与内容传送的授权装置。

(A5) 属性证书的发放

(A6) 属性证书的传输，和

(A7) 属性证书的传输

当从服务提供者 1030 收到发出属性证书的请求时，属性认证机构 1050 发出包括用户装置的属性信息和属性认证机构 1050 的数字签名的属性证书（图 68B），并且将其传送给服务提供者 1030。服务提供者 1030 把从属性认证机构 1050 收到的属性证书传送给用户装置 1020。用户装置把收到的属性证书保存到用户装置中，从而可在内容交易中的属性确认过程中使用该属性证书。

执行的向商店服务器 1010 发出属性证书的过程 ((B1) - (B7)) 基本上类似于执行的向用户装置发出公共密钥证书的过程。此外，按照和发出新的属性证书的过程相似的方式更新服务器 1010 的属性证书。

下面说明执行内容交易的过程，包括利用属性证书或者利用包括属性信息的公共密钥证书检查属性。

图 72 图解说明当进行相互验证时执行属性确认的过程。图 72 中所示的系统结构和图 1 中所示的系统结构相似。即，图 72 中所示的系

统包括销售内容的商店服务器 1010，购买内容的用户装置 1020 和在上述服务提供者的控制下工作的用户装置验证服务器 1030。在图 72 中，如下所述按照从（1）-（20）的步骤顺序进行该过程。

（1）相互验证和属性确认

当用户装置 1020 希望从商店服务器 1010 购买内容时，首先在用户装置 1020 和商店服务器 1010 之间进行相互验证。在相互验证中，确定将在其间传送数据的这两个装置是否是正确的装置。如果成功通过相互验证，则开始数据传输。最好，在相互验证过程中产生话路密钥，并且通过在后续数据传输过程中把话路密钥用作共用密钥对数据加密。这样进行基于公共密钥的相互验证，使得首先验证公共密钥证书的认证机构的签名，随后抽取位于另一端的实体的公共密钥，并且如同前面参考图 13 详细说明的那样，利用抽取的公共密钥进行相互验证。

之后，在本实施例中，进行属性确认。在属性数据包含在商店服务器 1010 正与之通信的装置的公共密钥证书中的情况下，商店服务器 1010 确认属性信息指出商店服务器 1010 正在通信的装置是用户装置。在公共密钥证书中不包含任何属性数据的情况下，商店服务器 1010 利用属性证书检查属性。属性证书包括由属性认证机构利用其保密密钥写入的数字签名。商店服务器 1010 利用属性认证机构的公共密钥 KpAA 验证写入属性证书中的数字签名，以确认证书有效。在确认在属性证书中描述的序列号和/或用户 ID 和在公共密钥证书中描述的序列号和/或用户 ID 相同之后，商店服务器 1010 检查在证书中描述的属性信息。

另一方面，在用户装置 1020 中，如果属性数据包含在用户装置 1020 正与之通信的装置的公共密钥证书中，则用户装置 1020 确认属性信息指出用户装置 1020 正在通信的装置是商店服务器。在公共密钥证书中不描述属性数据的情况下，属性证书被用于检查该属性。这种情况下，用户装置 1020 通过利用属性认证机构的公共密钥 KpAA 验证写入属性证书中的数字签名，以确认该证书有效。此外，用户装置

1020 确认在属性证书中描述的序列号和/或用户 ID 和在公共密钥证书中描述的序列号和/或用户 ID 相同。之后，用户装置 1020 检查在证书中描述的属性信息。

如果商店服务器 1010 通过检查在发出内容购买请求的实体的公共密钥证书或者属性证书中描述的属性信息，确认该实体是用户装置，并且如果用户装置 1020 按照上述方式通过检查在内容购买请求发往的实体的公共密钥证书或者属性证书中描述的属性信息，确认该实体是商店时，则过程可进行到下一步骤。

图 73A 和 73B 是图解说明检查属性的过程的流程图，其中图 73A 图解说明利用包括属性数据的公共密钥证书的属性检查过程，图 73B 图解说明利用属性证书的属性检查过程。

首先说明图 73A 中所示的流程。首先在步骤 S2101 中，利用公共密钥证书进行相互验证（图 13）。如果成功通过相互验证（如果步骤 S2101 中的答案为是），则从正与之进行通信的装置的公共密钥证书中抽取属性信息。如果属性信息有效（如果步骤 S2104 的答案为是），则确定已成功通过相互验证和属性确认（步骤 S2105），过程进行到下一步骤。这里，在用户装置访问商店服务器以购买内容的情况下，如果属性为“商店”则认为属性有效，但是如果属性具有不同于“商店”的属性代码，则认为该属性无效。更具体地说，在向商店服务器发出内容购买请求的情况下，比较属性代码的步骤包含在内容购买请求序列（处理程序）中。在属性代码比较步骤中，把分配给“商店”的代码“0002”和在正与之进行通信的实体的公共密钥证书或者属性证书中描述的属性代码进行比较。如果代码相互匹配，则认为该属性有效，如果代码相互不匹配，则认为该属性无效。另一方面，把从正与之进行通信的实体的公共密钥证书或者属性证书中抽取的属性代码显示在显示器上，从而人类用户可确定显示的属性代码是否和该实体应具有的属性代码相同。如果判定步骤 S2102 或者 S2104 的答案为否，则确定相互验证或者属性确认已失败（步骤 S2106），终止该过程。

在关于结合正在与之通信的商店进行处理而执行的处理程序中，检查从正在与之通信的实体的公共密钥证书或者属性证书中抽取的属性代码是否和分配给“商店”的代码“0002”相符。另一方面，密钥转换请求序列（程序）由用户装置和用户装置验证服务器执行，检查从正与之通信的实体的公共密钥证书或者属性证书抽取的属性代码是否和分配给“用户装置验证服务器”的代码“0001”相符。类似地，当在假定为特殊类型的实体之间，例如在商店和用户装置验证服务器之间的通信中，执行过程序列（程序），检查从正与之通信的实体的公共密钥证书或者属性证书抽取的属性代码，以确定其是否和预期的代码相符。

下面参考图 73B 说明利用属性证书的过程。首先在步骤 S2201 中，利用公共密钥证书进行相互验证（图 13）。如果成功通过相互验证（如果步骤 S2202 中的答案为是），则利用属性认证机构的公共密钥验证正与之通信的实体的属性证书（步骤 S2203）。如果成功通过验证，则通过检查属性证书具有和公共密钥证书相同的序列号，进一步确认属性证书和公共密钥证书相连。如果成功完成确认（如果判定步骤 S2204 中的答案为是），则从具有和公共密钥证书相同序列号的属性证书中抽取属性信息（步骤 S2205）。如果属性信息有效（如果判定步骤 S2206 中的答案为是），则确定已成功通过相互验证和属性确认（步骤 S2207），过程进行到下一步骤。如果判定步骤 S2202、S2204 和 S2206 任一的答案为否，则确定相互验证或属性确认已失败（步骤 S2208），并且终止该过程。

（2）交易 ID 和购买请求数据的产生，和

（3）购买请求数据的传输

如果成功通过商店服务器 1010 和用户装置 1020 之间的相互验证和属性确认，则用户装置 1020 产生内容购买请求数据。购买请求数据的数据结构类似于前面说明的图 14A 中所示的数据结构。购买请求数据包括识别内容购买请求发往的商店服务器 1010 的商店 ID，根据随机数由用户装置 1020 的加密装置产生的作为内容交易的标识符的交

易 ID，以指出用户装置所希望购买内容的内容 ID。另外，关于上述数据的用户装置的数字签名被添加到购买请求数据中。

(4) 接收数据的验证

当商店服务器从用户装置 1020 收到如图 14A 中所示的购买请求时，商店服务器验证接收的数据。和前面参考图 15 说明的一样，首先通过验证用户装置的公共密钥证书 Cert_DEV，随后从公共密钥证书抽取用户装置的公共密钥 KpDEV，最后利用用户装置的公共密钥 KpDEV 验证写入购买请求数据中的用户装置的签名，进行验证。

如果成功通过验证，即如果确定购买请求数据未被篡改，则确定接收的数据是有效的内容购买请求数据。但是，如果没有通过验证，则确定购买请求数据已被篡改，终止与购买请求数据相关的过程。

(5) 加密内容和加密内容密钥数据 1(商店) 的传输

如果商店服务器 1010 进行的验证指出购买请求数据是未被篡改的有效数据，则商店服务器 1010 把加密内容和加密内容密钥数据 1(商店) 传送给用户装置。在上述过程中，加密内容和加密内容密钥数据 1(商店) 均从内容数据库获得，其中加密内容是在利用内容密钥对内容加密而产生之后保存在内容数据库中的数据 Kc(内容)，加密内容密钥是在利用用户装置验证服务器(DAS) 1030 的公共密钥对内容密钥 Kc 加密而产生之后保存在内容数据库中的数据 KpDAS(Kc)。

这里，加密内容密钥数据 1(商店) 的数据结构和图 14B 中所示的数据结构相似。即，加密内容密钥数据 1(商店) 包括识别发出内容购买请求的用户装置 1020 的用户装置 ID，购买请求数据(除用户装置的公共密钥证书之外图 14A 中所示的数据)，响应内容交易由商店服务器 1010 产生的商店过程编号，和加密内容密钥数据 KpDAS(Kc)。此外，关于上述数据的商店服务器 1010 的数字签名被附到加密内容密钥数据 1(商店) 上。加密内容密钥数据 1(商店) 和商店服务器 1010 的公共密钥证书一起被传送给用户装置 1020。注意，如果在相互验证之前或者在相互验证过程中，公共密钥证书已被传送给用户装置，则不需重新传送公共密钥证书。

(6) 接收数据的验证

当用户装置 1020 从商店服务器 1010 收到加密内容 K_c (内容) 和图 14B 中所示的加密内容密钥数据 1 (商店) 时, 用户装置 1020 验证加密内容密钥数据 1 (商店)。按照和上面参考图 15 中所示的处理流程相似的方式进行验证。即, 用户装置 1020 首先利用认证机构 (CA) 的公共密钥 K_{pCA} 验证从商店服务器 1010 接收的商店服务器的公共密钥证书。之后, 用户装置 1020 利用从公共密钥证书中抽取的商店服务器的公共密钥 K_{pSHOP} 验证写入图 14B 中所示的加密内容密钥数据 1 中的商店签名。

(7) 相互验证和属性确认

如果用户装置 1020 在从商店服务器 1010 收到加密内容 K_c (内容) 和加密内容密钥数据 1 (商店) 之后完成加密内容密钥数据 1 (商店) 的验证, 则用户装置 1020 访问用户装置验证服务器 1030, 并且在用户装置 1020 和用户装置验证服务器 1030 之间进行相互验证和属性确认。按照和商店服务器 1010 与用户装置 1020 之间的相互验证和属性确认相似的方式进行该过程。

(8) 加密密钥数据 (用户装置) 和加密内容密钥转换请求的传输

如果成功通过用户装置 1020 和用户装置验证服务器 1030 之间的相互验证, 则用户装置 1020 把从商店服务器 1010 收到的加密内容密钥 K_{pDAS} (K_c) 传送给用户装置验证服务器 1030, 并且用户装置 1020 请求用户装置验证服务器 1030 执行加密内容密钥的转换。这里, 加密内容密钥数据 (用户装置) 的数据结构和图 14C 中所示的数据结构相似。包括识别加密内容密钥转换请求发往的用户装置验证服务器 1030 的用户装置验证服务器 ID 和从商店服务器 1010 接收的加密内容密钥数据 (除商店公共密钥证书之外图 14B 中所示的数据)。此外, 关于上述数据的用户装置 1020 的数字签名被添加到加密内容密钥数据 (用户装置) 中。加密内容密钥数据 (用户装置) 和商店服务器 1010 的公共密钥证书及用户装置 1020 的公共密钥证书一起被传送给用户装置验证服务器 1030。在用户装置验证服务器 1030 已具有用户装置的公

共密钥证书和商店服务器的公共密钥证书的情况下，不需要重新传送这些证书。

(9) 接收数据的验证

当用户装置验证服务器 1030 从用户装置 1020 收到加密内容密钥数据（用户装置）和加密内容密钥转换请求（图 14C）时，用户装置验证服务器 1030 验证从用户装置 1020 接收的用户装置的公共密钥证书。按照上面参考图 15 中所示的处理流程相似的方式进行验证。即，用户装置 1020 首先利用认证机构（CA）的公共密钥 KpCA 验证从用户装置 1020 接收的用户装置的公共密钥证书。之后，用户装置 1030 利用用户装置的公共密钥 KpDEV 验证写入图 14C 中所示的加密内容密钥数据（用户装置）中的数字签名。此外，用户装置 1030 利用认证机构（CA）的公共密钥 KpCA 验证商店服务器的公共密钥证书。之后，用户装置 1030 利用从公共密钥证书抽取的商店服务器的公共密钥 KpSHOP，验证写入包含在图 14C 中所示的加密内容密钥数据（用户装置）中的（5）加密内容密钥数据 1 中的商店签名。在以图 14C 中所示的格式包含从用户装置发出的消息的情况下，根据需要验证该消息。

(10) 加密内容密钥的验证

在由用户装置验证服务器 1030 执行的关于从用户装置 1020 收到的加密内容密钥数据（用户装置）和加密内容密钥转换请求的验证中，如果确定密钥转换请求有效，则用户装置验证服务器 1030 利用用户装置验证服务器 1030 的保密密钥 KsDAS，对包含在加密内容密钥数据（用户装置）中的加密内容密钥，即通过利用用户装置验证服务器（DAS）1030 的公共密钥 KpDAS 对内容密钥 Kc 加密得到的加密数据 KpDAS（Kc）解密，从而获得内容密钥 Kc。此外，用户装置验证服务器 1030 利用用户装置的公共密钥 KpDEV 对得到的内容密钥 Kc 加密，从而产生加密内容密钥 KpDEV（Kc）。即，密钥被转换，以致 $KpDAS(Kc) \rightarrow Kc \rightarrow KpDEV(Kc)$ 。

之后，如同前面参考图 16 说明的一样，从加密内容密钥数据（用户装置）抽取利用用户装置验证服务器（DAS）1030 的公共密钥 KpDAS

加密的内容密钥数据 KpDAS (Kc)，并且利用用户装置验证服务器 1030 的保密密钥 KsDAS 对其解密，从而获得内容密钥 Kc。随后利用用户装置的公共密钥 KpDEV 对获得的内容密钥 Kc 重新加密，产生加密内容密钥 KpDEV (Kc)。

(11) 相互验证和属性确认

如果用户装置验证服务器 1030 已完成加密内容密钥转换，则用户装置验证服务器 1030 访问商店服务器 1010，并且在用户装置验证服务器 1030 和商店服务器 1010 之间进行相互验证和属性确认。按照和在商店服务器 1010 和用户装置 1020 之间的相互验证及属性确认相似的方式进行该过程。

(12) 加密内容数据的传输

如果成功通过用户装置验证服务器 1030 和商店服务器 1010 之间的相互验证和属性确认，则用户装置验证服务器 1030 把加密内容密钥数据 (DAS) 传送给商店服务器 1010。这里，加密内容密钥数据 (DAS) 的数据结构和图 17D 中所示的数据结构相似，包括识别内容购买请求发往的商店服务器 1010 的商店 ID，加密内容密钥数据（用户装置）（除商店的公共密钥证书及用户装置的公共密钥证书之外图 14C 中所示的数据），和通过上述密钥转换过程由用户装置验证服务器 1030 产生的加密内容密钥数据 KpDEV (Kc)。此外，关于上述数据的用户装置 1030 的数字签名被添加到加密内容密钥数据 (DAS) 中。加密内容密钥数据 (DAS) 和用户装置验证服务器 1030 的公共密钥证书及用户装置 1020 的公共密钥证书一起被传送给商店服务器 1010。在商店服务器已具有这些证书的情况下，不需要重新传送这些证书。

在用户装置验证服务器 1030 由高度可靠的第三方管理的情况下，可不按照图 17D 中所示的形式构成加密内容密钥数据 (DAS)，在图 17D 中所示的形式中，以其初始形式包含由用户装置产生的加密内容密钥数据（用户装置）（由 (8) 表示），而是这样构成加密内容密钥数据 (DAS)，以致如图 18D' 中所示，用户装置 ID、交易 ID、内容 ID、商店过程编号和利用用户装置的公共密钥加密的内容密钥 KpDEV

(Kc) 被用户装置验证服务器 1030 抽取，并且加密内容密钥数据 (DAS) 由抽取的这些数据加上用户装置验证服务器 1030 的数字签名构成。这种情况下，不必验证加密内容密钥数据 (用户装置) (图 17D 由 (8) 表示)，从而只需把用户装置验证服务器 1030 的公共密钥证书附到加密内容密钥数据 (DAS) 上即可。

(13) 接收数据的验证

当商店服务器 1010 从用户装置验证服务器 1030 收到加密内容密钥数据 (DAS) (图 17D) 时，商店服务器 1010 验证加密内容密钥数据 (DAS)。按照上面参考图 15 中所示的处理流程说明的相似方式进行验证。即，商店服务器 1010 首先利用认证机构 (CA) 的公共密钥 KpCA，验证从用户装置验证服务器 1030 接收的用户装置验证服务器的公共密钥证书。之后，商店服务器 1010 利用用户装置验证服务器 1030 的公共密钥 KpDAS 验证写入图 17D 中所示的加密内容密钥数据 (DAS) 中的数字签名。此外，商店服务器 1010 利用认证机构 (CA) 的公共密钥 KpCA 验证用户装置的公共密钥证书。之后，商店服务器 1010 利用从公共密钥证书抽取的用户装置的公共密钥 KpDEV，验证由用户装置写入包含在图 17D 中所示的加密内容密钥数据 (DAS) 中的 (8) 加密内容密钥数据 (用户装置) 中的数字签名。在以图 14 中所示的格式包含从用户装置发出的消息的情况下，根据需要验证该消息。

在商店服务器 1010 收到呈上面参考图 18D' 说明的简化形式的加密内容密钥数据 (DAS) 的情况下，商店服务器 1010 利用认证机构 (CA) 的公共密钥 KpCA 验证用户装置验证服务器的公共密钥证书，随后商店服务器 1010 利用用户装置验证服务器 1030 的公共密钥 KpDAS 验证图 18D' 中所示的加密内容密钥数据 (DAS) 的数字签名。

(14) 相互验证和属性确认，和

(15) 加密内容密钥请求的传输

之后，用户装置 1020 把加密内容密钥请求数据传送给商店服务器。在和传送前一请求的话路不同的话路中传送加密内容密钥请求数

据的情况下，再次进行相互验证，并且只有当成功通过相互验证时，才从用户装置 1020 把加密内容密钥请求数据传送给商店服务器 1010。在以图 14C 中所示的格式中包含从用户装置发出的消息的情况下，根据需要验证该消息。

图 17E 图解说明加密内容密钥请求数据的数据结构。即，加密内容密钥请求数据包括识别内容购买请求发往的商店服务器 1010 的商店 ID，根据随机数由用户装置 1020 的加密装置产生的作为内容交易的标识符的交易 ID，指出用户装置所希望购买内容的内容 ID，以及包含在由商店产生的，并且作为内容密钥数据 1（商店）传送给用户装置 1020 的数据（图 14B）中的商店过程编号。此外，关于上述数据的用户装置的数字签名被添加到加密内容密钥请求数据中。加密内容密钥请求数据和用户装置的公共密钥证书一起被传送给商店服务器 1010。在商店服务器已具有证书的情况下，不需要重新传送该证书。

（16）验证，和

（17）收费过程

当商店服务器 1010 从用户装置收到加密内容密钥请求数据时，商店服务器 1010 验证加密内容密钥请求数据。按照上面参考图 15 说明的相似方式进行验证过程。在完成数据验证之后，商店服务器 1010 执行和内容交易相关的收费过程。执行收费过程，以便从用户账户收取内容费用。在内容的版权持有者、商店和用户装置验证服务器的所有者等之间分配收取的内容费用。

注意在收费过程之前要求用户装置验证服务器 1030 进行加密内容密钥转换，从而不能只通过商店服务器 1010 和用户装置之间的过程就执行收费过程。用户装置 1020 不能对加密内容密钥解密，从而用户装置 1020 不能使用内容，除非已进行密钥转换。其中用户装置验证服务器执行的密钥转换的所有内容交易的历史记录在前面参考图 6 说明的许可证管理数据库中，从而可监控和管理需要收费过程的任意内容交易。这可防止任意商店单独进行内容销售交易，从而防止未经授权销售内容。

(18) 加密内容密钥数据 2(商店) 的传输

如果商店服务器 1010 完成了收费过程，则商店服务器 1010 把加密内容密钥数据 2(商店) 传送给用户装置 1020。

这里，加密内容密钥数据 2(商店) 的数据结构和图 17F 中所示的相似，包括识别发出加密内容密钥请求的用户装置 1020 的用户装置 ID，从用户装置验证服务器 1030 收到的加密内容密钥数据(DAS)(除用户装置的公共密钥证书和用户装置验证服务器的公共密钥证书之外图 17D 中所示的数据)。此外，关于上述数据的商店服务器 1010 的数字签名被添加到加密内容密钥数据 2(商店) 中。加密内容密钥数据 2(商店) 和商店服务器 1010 的公共密钥证书及用户装置验证服务器 1030 的公共密钥证书一起传送给用户装置 1020。在用户装置 1020 已具有用户装置验证服务器的公共密钥证书和商店服务器的公共密钥证书的情况下，不需要重新传送这些证书。

在用户装置验证服务器 1030 由高度可靠的高度可靠的第三方管理，并且商店服务器 1010 从用户装置验证服务器 1030 接收呈上面参考图 18D'说明的简化形式的加密内容密钥数据(DAS)的情况下，商店服务器 1010 把呈图 18F'中所示形式的加密内容密钥数据 2(商店) 传送给用户装置。即，呈图 18D'中所示简化形式，包括商店服务器的签名的加密内容密钥数据(DAS) 和商店服务器 1010 的公共密钥证书以及用户装置验证服务器 1030 的公共密钥证书一起被传送给用户装置 1020。

(19) 接收数据的验证

当用户装置 1020 从商店服务器 1010 收到加密内容密钥数据 2(商店) 时，用户装置 1020 验证加密内容密钥数据 2(商店)。按照上面参考图 15 中所示的处理流程说明的相似方式进行验证。即，用户装置 1020 首先利用认证机构(CA)的公共密钥 KpCA，验证从商店服务器 1010 接收的商店服务器的公共密钥证书。之后，用户装置 1020 利用从公共密钥证书中抽取的商店服务器 1010 的公共密钥 KpSHOP 验证写入图 17F 中所示的加密内容密钥数据 2(商店) 中的数字签名。此外，用户装置 1020 利用认证机构(CA)的公共密钥 KpCA 验证用

户装置验证服务器 1030 的公共密钥证书。之后，用户装置 1020 利用从公共密钥证书抽取的用户装置验证服务器 1030 的公共密钥 KpDAS，验证写入包含在图 17F 中所示的加密内容密钥数据 2(商店)中的(12)加密内容密钥数据(DAS)中的数字签名。在以图 17F 中所示的格式包含某些消息的情况下，根据需要验证该消息。

(20) 数据的存储

在用户装置 1020 验证了从商店服务器 1010 收到的加密内容密钥数据 2(商店)之后，用户装置 1020 利用用户装置 1020 的保密密钥 KsDEV 对利用用户装置 1020 的公共密钥 KpDEV 加密并且包含在加密内容密钥数据 2(商店)中的加密内容密钥 KpDEV(Kc)解密，并且随后用户装置 1020 利用用户装置的存储密钥 Ksto 对内容密钥加密，从而产生加密内容密钥 Ksto(Kc)。得到的加密内容密钥 Ksto(Kc)被保存到用户装置 1020 的存储装置中。当使用该内容时，利用存储密钥 Ksto 对加密内容密钥 Ksto(Kc)解密，从而获得内容密钥 Kc，并且利用得到的内容密钥 Kc 对加密内容 Kc(内容)解密，从而再现内容。

在本实施例中，如上所述，在起动与通过两个实体之间的通信的内容传送相关的过程之前，检查位于相对通信端的实体的属性，如果位于相对通信端的实体的属性是预期类型装置，例如用户装置的属性，则执行该过程。这可防止欺诈的内容销售交易。例如，能够防止商店假装成是用户装置从而进行欺诈内容交易。还能够防止服务器假装成是授权商店服务，从而欺诈获得用户装置的信用卡账号。

例如，一旦用户装置根据属性检查确定正与之通信的实体是商店，则确保用户装置能够毫无风险地向商店发出内容购买请求。另一方面，如果属性检查指出用户装置正与之通信的实体是用户装置验证服务器，则确保用户装置能够毫无风险地向用户装置验证服务器发出诸如密钥转换请求之类的请求。在根据本实施例的系统中，属性检查使得能够知道位于相对通信端的实体的类型，确保能够根据位于相对通信端的实体的类型恰当地执行过程。此外，能够防止把保密数据传送给

错误的实体，从而能够防止数据泄漏出去。

现在参见图 74，下面说明在验证写入接收数据中的签名以确认数据的完整性得到保持，并且检查属性之后，在不进行相互验证的情况下执行内容交易的过程。

除了不进行相互验证之外，图 74 中所示的过程和图 72 中所示的过程相似。在图 74 中，如下所述，过程按照步骤（1）-（16）的顺序进行。

- (1) 交易 ID 和购买请求数据的产生，和
- (2) 购买请求数据的传输

首先，用户装置 1020 产生内容购买请求数据并将其传送给商店服务器 1010。这里，购买请求数据（用户装置）的数据结构和图 14A 中所示的相似。

(3) 接收数据的验证

当商店服务器从用户装置 1020 收到如图 14A 中所示的购买请求时，商店服务器 1010 验证接收的数据。在本实施例中，除了检查购买请求数据的完整性是否被保持之外，还检查属性信息。

图 75 图解说明对于公共密钥证书包括属性信息的情况确认接收的数据的流程。如果商店服务器 1010 收到消息、签名（购买请求数据）和用户装置的公共密钥证书（步骤 S2301），则商店服务器 1010 利用公共密钥认证机构的公共密钥 KpCA 验证用户装置的公共密钥证书（步骤 S2302）。如果成功通过验证（如果步骤 S2303 中的答案为是），则从公共密钥证书抽取用户装置的公共密钥 KpDEV（步骤 S2304），并且利用用户装置的公共密钥 Kp_DEV 验证写入购买请求中的用户装置的签名（步骤 S2305）。如果成功通过验证（如果步骤 S2306 中的答案为是），则从公共密钥证书抽取属性信息（步骤 S2307），并且确定属性是否有效（本具体情况下，确定属性信息是否表示该装置是用户装置）（步骤 S2308）。如果属性有效，即如果成功通过确认（步骤 S2309），则过程进行到下一步骤。如果判定步骤 S2303、S2306 和 S2308 中任一的答案为否，则确定确认已失败（步骤 S2310），并终止

处理。

现在参见图 76 中所示的流程图，下面说明利用公共密钥证书和属性证书验证接收的数据的过程。首先，商店服务器 1010 接收消息、签名（购买请求数据）和用户装置的公共密钥证书及属性证书（步骤 S2401）。商店服务器 1010 利用公共密钥认证机构的公共密钥 KpCA，验证用户装置的公共密钥证书（步骤 S2402）。如果成功通过验证（如果步骤 S2403 中的答案为是），则从公共密钥证书抽取用户装置的公共密钥 KpDEV（步骤 S2404），并且利用用户装置的公共密钥 KpDEV 验证写入购买请求数据中的用户装置的签名（步骤 S2405）。如果成功通过验证（如果步骤 S2406 中的答案为是），则随后利用属性认证机构的公共密钥 KpAA 验证属性证书（步骤 S2407）。如果成功通过验证（如果步骤 S2408 中的答案为是），则从属性证书抽取属性信息（步骤 S2409），并且确定属性是否有效（本具体情况下，确定属性信息是否指示该装置是用户装置）（步骤 S2410）。如果属性有效，即如果成功通过验证（步骤 S2411），则过程进行到下一步骤。如果判定步骤 S2403、S2406、S2408 和 S2410 中任一的答案为否，则确定验证已失败（步骤 S2412），并且终止处理。

（4）加密内容和加密内容密钥数据 1（商店）的传输

如果商店服务器 1010 进行的验证指出购买请求数据是未被篡改的有效数据，并且如果属性被确认，则商店服务器 1010 把加密内容和加密内容密钥数据 1（商店）（图 14B）传送给用户装置。

（5）接收数据的验证

当用户装置 1020 从商店服务器 1010 收到加密内容 Kc（内容）和图 14B 中所示的加密内容密钥数据 1（商店）时，用户装置 1020 验证加密内容密钥数据 1（商店）并且还确认属性。按照上面参考图 75 或 76 中所示的处理流程说明的相似方式进行验证。如果在公共密钥证书或者在属性证书中描述的属性不是“商店”，则终止处理。

（6）加密密钥数据（用户装置）和加密内容密钥转换请求的传输之后，用户装置 1020 把从商店服务器 1010 收到的加密内容密钥

KpDAS (Kc) 传送给用户装置验证服务器 1030，并且用户装置 1020 请求用户装置验证服务器 1030 执行加密内容密钥（图 14C）的转换。

(7) 接收数据的验证

当用户装置验证服务器 1030 从用户装置 1020 收到加密内容密钥数据（用户装置）和加密内容密钥转换请求（图 14C）时，用户装置验证服务器 1030 验证加密内容密钥转换请求。按照上面参考图 75 或 76 中所示的处理流程说明的相似方式进行验证，其中还进行属性确认。如果在公共密钥证书或者在属性证书中描述的属性不是“用户装置”，则终止处理。

(8) 加密内容密钥的转换

之后，用户装置验证服务器 1030 转换该密钥，以致 KpDAS (Kc) → Kc → KpDEV (Kc)。

(9) 加密内容数据的传输

之后，用户装置验证服务器 1030 把加密内容密钥数据 (DAS) 传送给商店服务器 1010。这里，加密内容密钥数据 (DAS) 的数据结构和图 17D 中所示的相似。

(10) 接收数据的验证

当商店服务器 1010 从用户装置验证服务器 1030 收到加密内容密钥数据 (DAS)（图 17D）时，商店服务器 1010 验证加密内容密钥数据 (DAS)。按照上面参考图 75 或 76 中所示的处理流程说明的相似方式进行验证，其中还进行属性确认。如果在公共密钥证书或者在属性证书中描述的属性不是用户装置验证服务器（服务提供者），则终止处理。

(11) 加密内容密钥请求的传输

之后，用户装置 1020 把加密内容密钥请求数据传送给商店服务器。加密内容密钥请求数据具有如图 17E 中所示的数据结构。

(12) 验证，和

(13) 收费过程

当商店服务器 1010 从用户装置收到加密内容密钥请求数据时，商

店服务器 1010 验证加密内容密钥请求数据。按照上面参考图 75 和 76 中所示的处理流程说明的相似方式进行验证，其中还进行属性确认。如果在公共密钥证书或者在属性证书中描述的属性不是用户装置，则终止处理。在完成数据验证之后，商店服务器 1010 进行与内容交易相关的收费过程。

(14) 加密内容密钥数据 2(商店) 的传输

如果商店服务器 1010 已完成收费过程，则商店服务器 1010 把加密内容密钥数据 2(商店) 传送给用户装置 1020。这里，加密内容密钥数据 2(商店) 的数据结构和图 17F 中所示的相似。

(15) 接收数据的验证，和

(16) 数据的存储

当用户装置 1020 从商店服务器 1010 收到加密内容密钥数据 2(商店) 时，用户装置 1020 验证加密内容密钥数据 2(商店)。按照上面参考图 75 或 76 中所示的处理流程说明的相似方式进行验证，其中还进行属性确认。如果在公共密钥证书或者在属性证书中描述的属性不是“商店”，则终止处理。在验证数据之后，用户装置 1020 执行存储过程。即，用户装置 1020 利用用户装置 1020 的保密密钥 KsDEV，对已利用用户装置 1020 的公共密钥 KpDEV 加密的加密内容密钥 KpDEV(Kc) 解密，随后用户装置 1020 利用用户装置 1020 的存储密钥 Ksto 对内容密钥加密，从而产生加密内容密钥 Ksto(Kc)。得到的加密内容密钥 Ksto(Kc) 被保存到用户装置 1020 的存储装置中。

在图 74 中所示的过程中，如上所述，不是在进行相互验证时而是在验证接收数据的签名时检查属性，从而简化了过程，并且可更高效地进行内容交易。

在利用属性数据检查实体的属性的上述实施例中，由服务提供者进行密钥转换。但是，也可在其中使用日志记录服务器的系统中采用属性检查。此外，在多个实体之间传输数据的通用系统中，可根据实体的具体功能定义相应实体的属性，并且可在公共密钥证书或属性证书中描述定义的各个实体的属性，从而使得任意实体都能知道正在与

之通信的另一实体的属性，从而在数据通信中获得较高的安全性。除了在常规技术中执行的相互验证和/或签名验证之外，还执行属性检查过程。例如，在一般的数据通信中只进行签名验证或者只进行相互验证，只有当必需时才进行属性检查过程。即，根据所需的安全程度，可执行签名验证、相互验证和属性检查之一或者它们的组合。

上面已参考具体实施例详细说明了本发明。对于本领域的技术人员来说，在不脱离本发明的精神和范围的情况下，可对用于举例说明的实施例作出不同的修改和替换。即，上面举例说明了各个实施例，但是本发明并不局限于此。本发明的范围仅由附加的权利要求所限定。

总之，本发明提供一种内容传送系统和内容传送方法，其中当用户装置向商店服务器发出内容购买请求时，如果成功完成与内容购买请求相关的收费过程，则商店服务器以可利用保存在用户装置中的密钥解密的形式把加密内容密钥传送给用户装置，从而保证能够高度可靠地执行收费过程。

本发明还提供一种内容传送系统和内容传送方法，其中响应用户装置发出的内容购买请求，管理内容传送的用户装置验证服务器把利用用户装置验证服务器（DAS）的公共密钥加密的内容密钥 KpDAS (Kc)转换成利用用户装置的公共密钥加密的内容密钥 KpDEV(Kc)，从而确保用户装置验证服务器能够监控商店和用户装置之间的内容销售交易的实际状态。

本发明还提供一种内容传送系统和内容传送方法，其中当在用户装置、商店和用户装置验证服务器之间进行数据通信时，至少执行相互验证和签名产生/验证之一，从而确保高度安全的数据通信并且能够检查数据的完整性是否被保持。

图 1

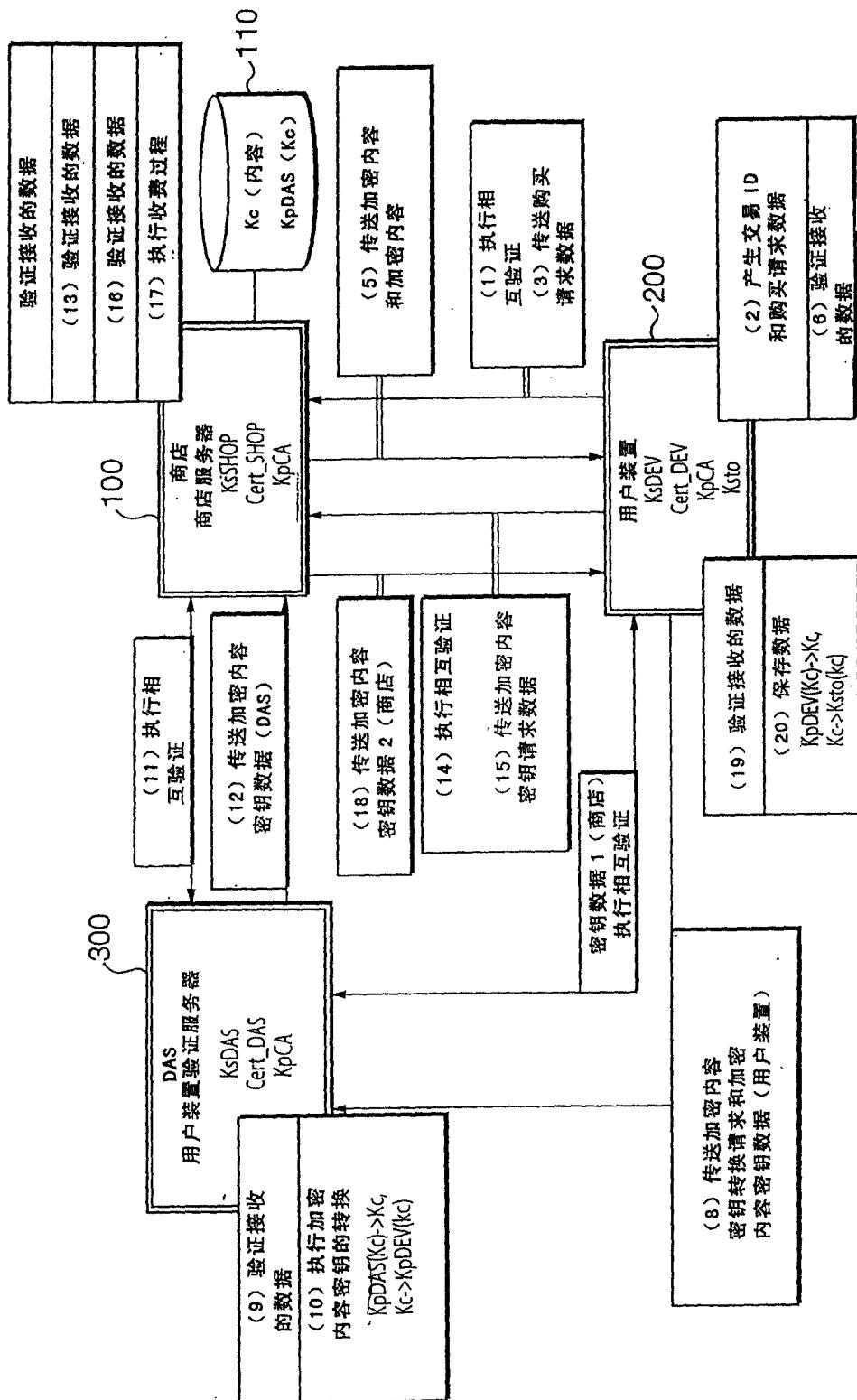


图 2

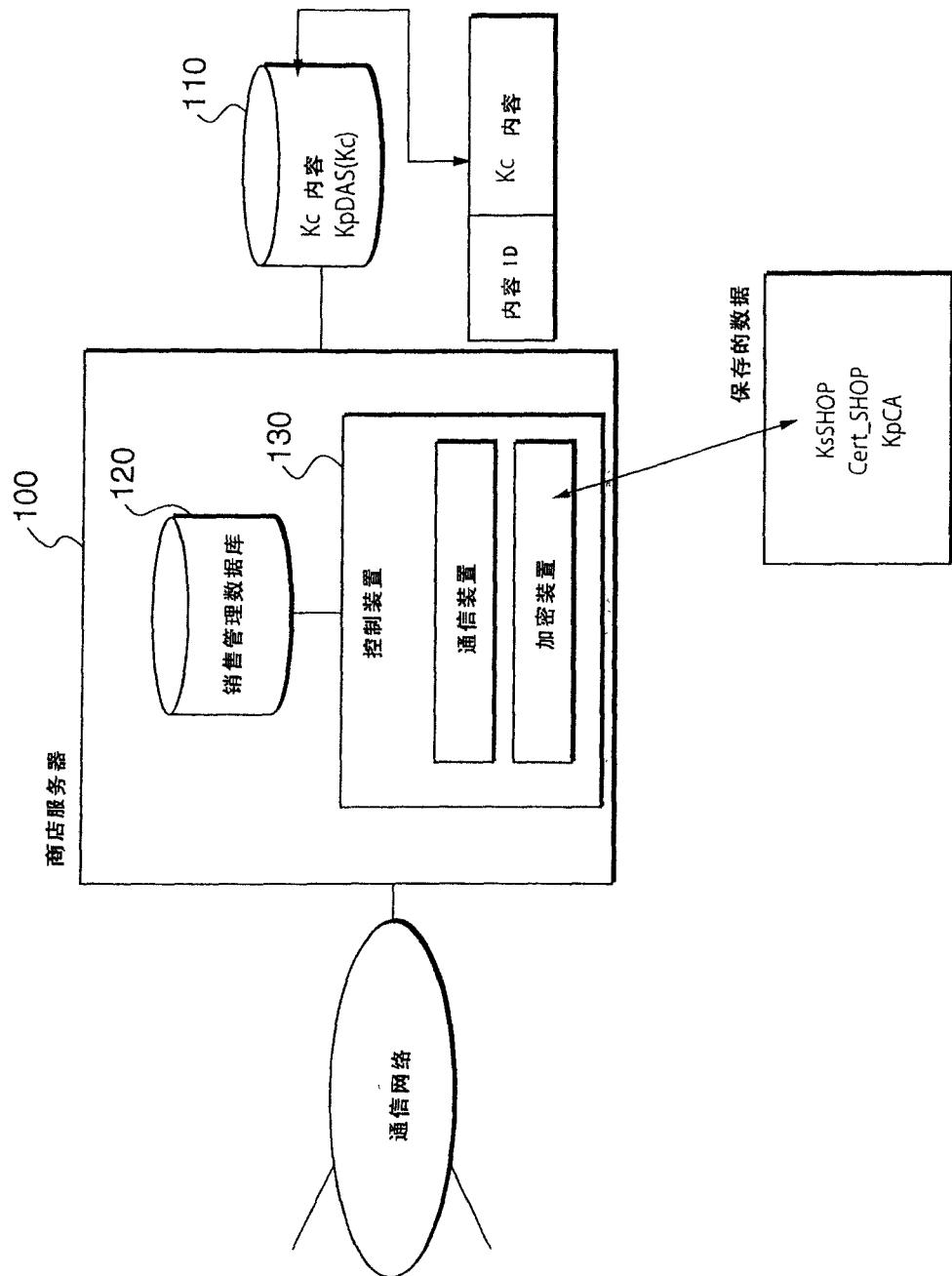


图 3

商店过程编号	装置 ID	交易 ID	内容 ID	状态
10001	1234567890	999888777	5000	成功完成密钥 2 的传送
10002	2345678901	666555444	4050	成功完成收费过程
10003	3456789012	333222111	1000	成功完成加密内容 密钥传输请求的接收
10004	4567890123	0009998888	3000	成功完成密钥的接收
10005	5678901234	7776665555	5050	成功完成密钥 1 的传输
10006	6789012345	4443332222	2050	成功完成购买请求的接收

商店服务器的购买管理数据库

图 4

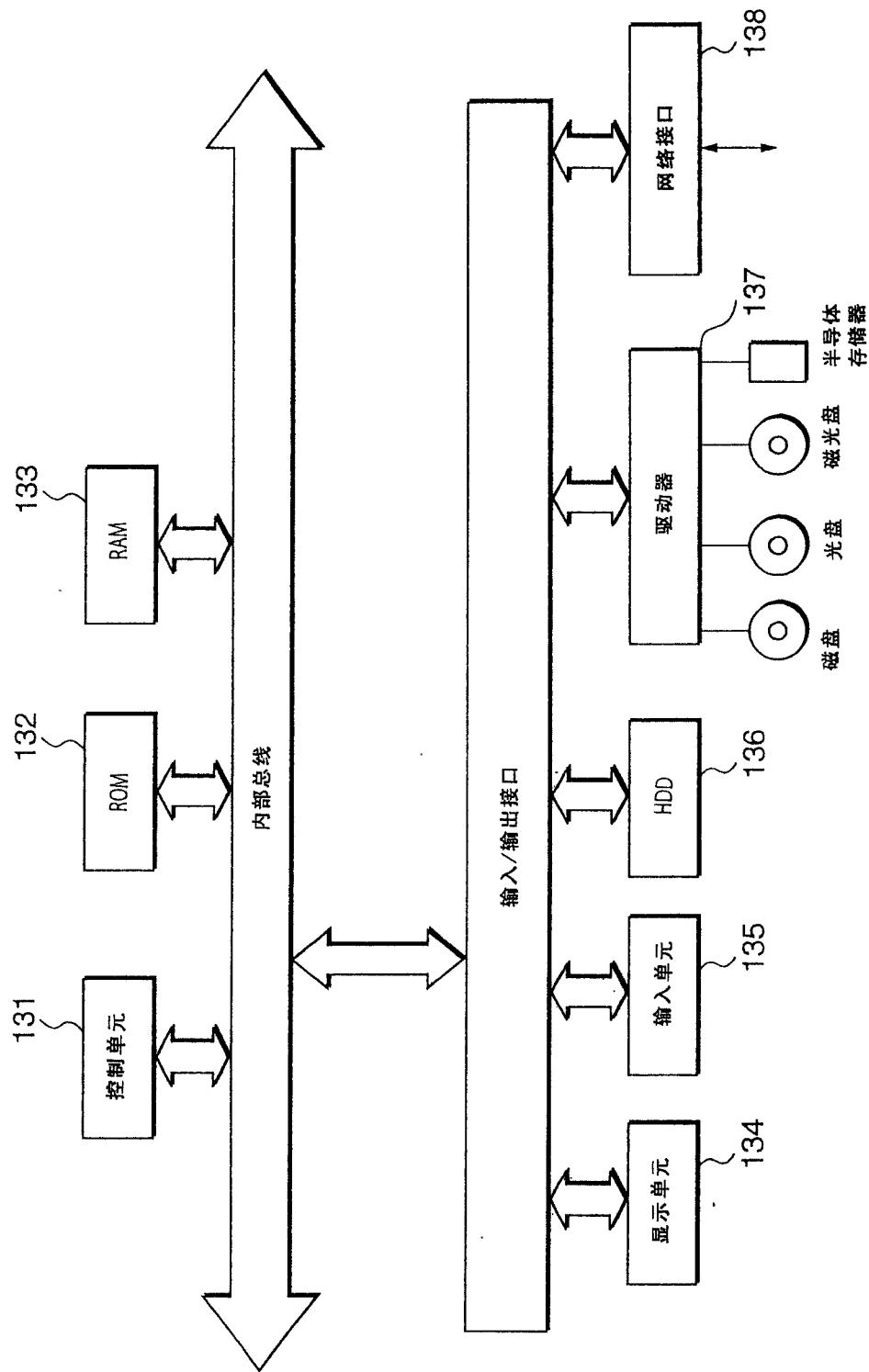


图 5

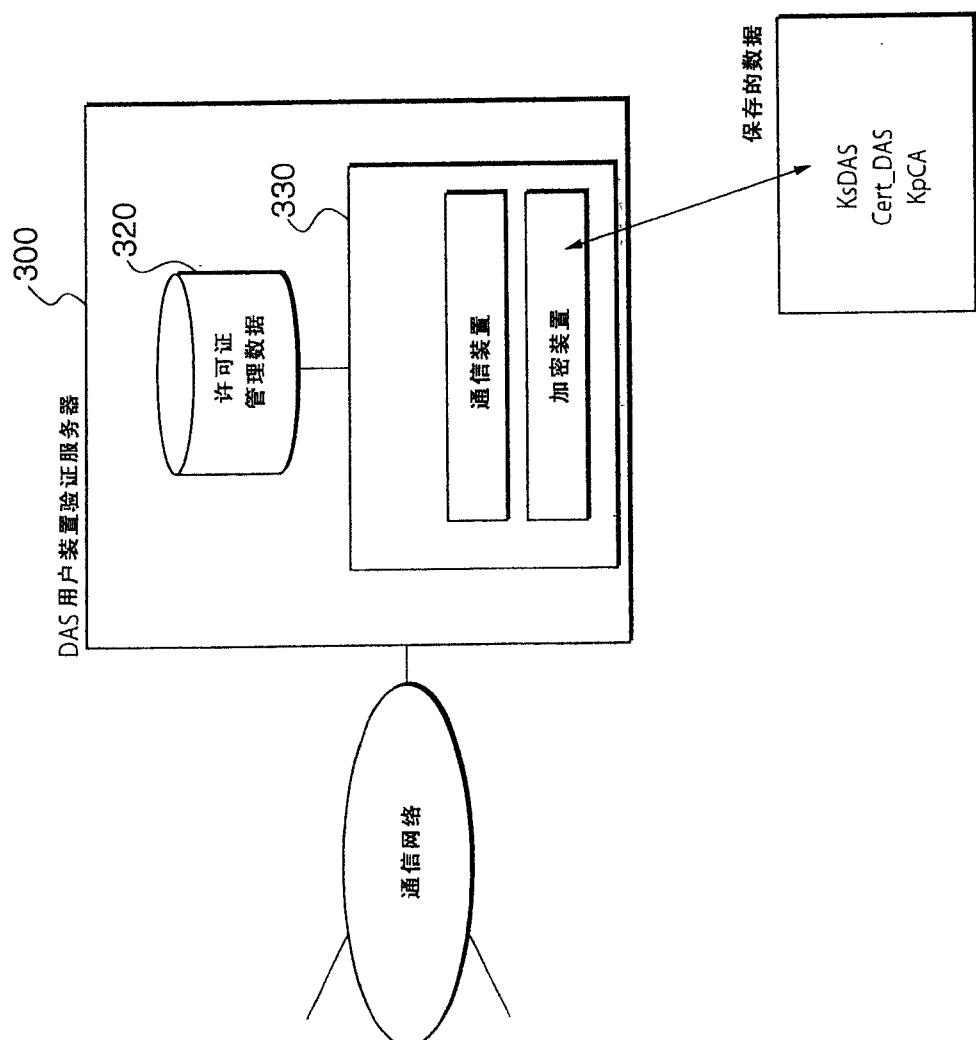


图 6

DAS 过程编号	装置 ID	交易 ID	内容 ID	商店 ID	商店过 程编号	状态
50001	1234567890	99988777	5000	1234	10001	完成密 钥传输
50002	2345678901	66655444	4050	1234	10002	完成密 钥转换

用户装置验证服务器的许可证管理数据库

图 7

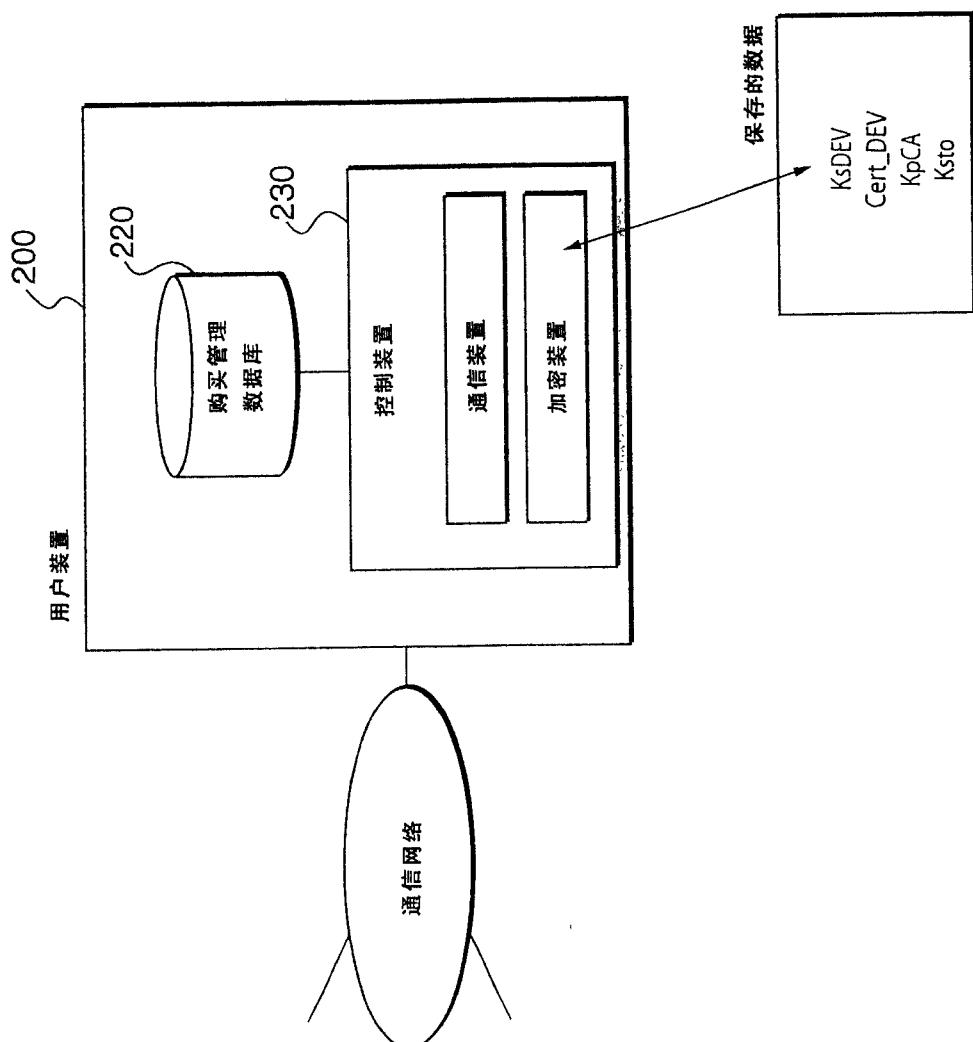


图 8

装置 ID : 1234567890			
交易 ID	内容 ID	商店 ID	状态
9999888777	5000	1234	完成密钥 2 的接收
666555444	4050	9876	完成购买 请求的传输

用户装置的购买管理数据库

图 9

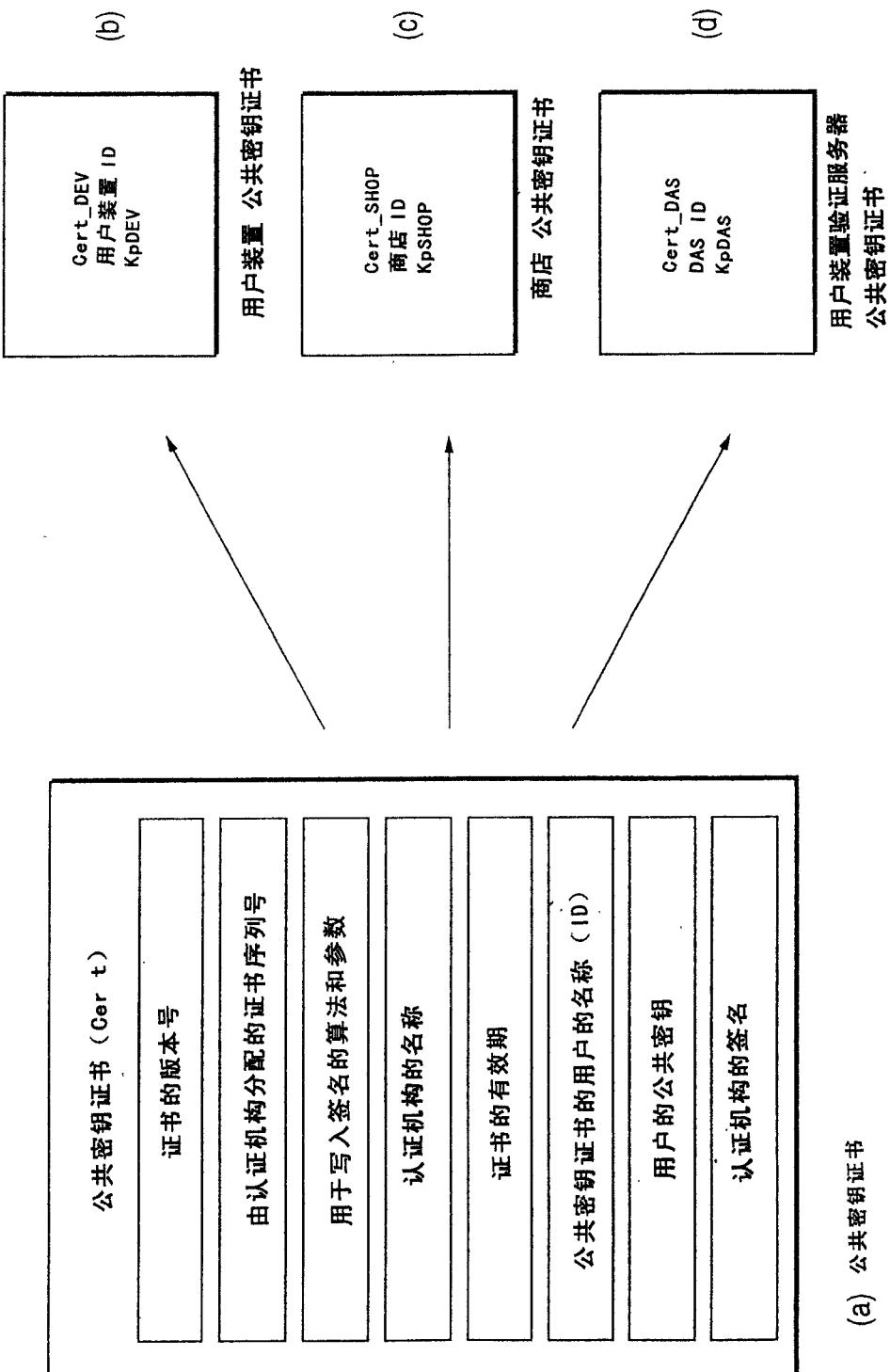


图 10

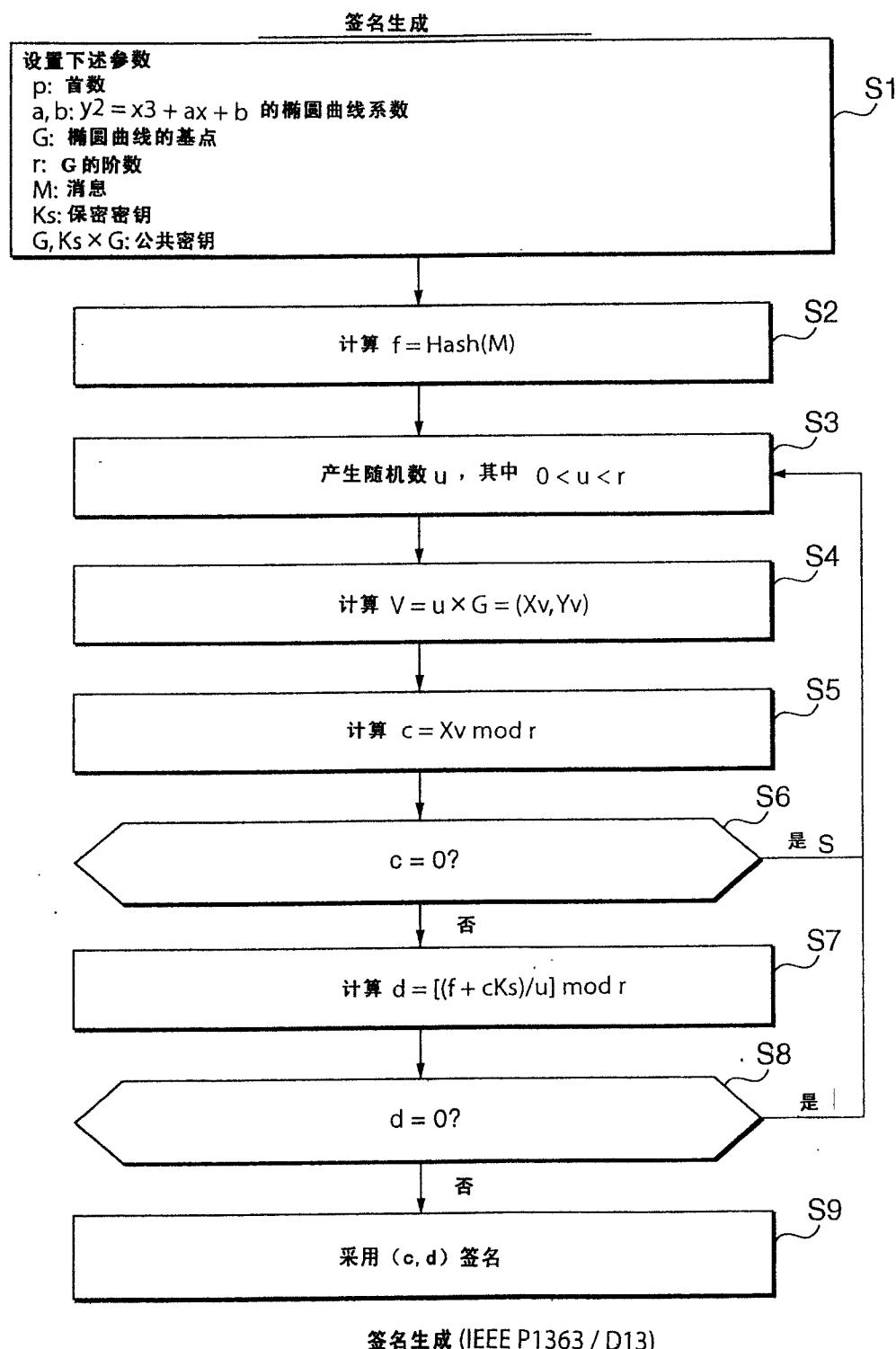


图 11

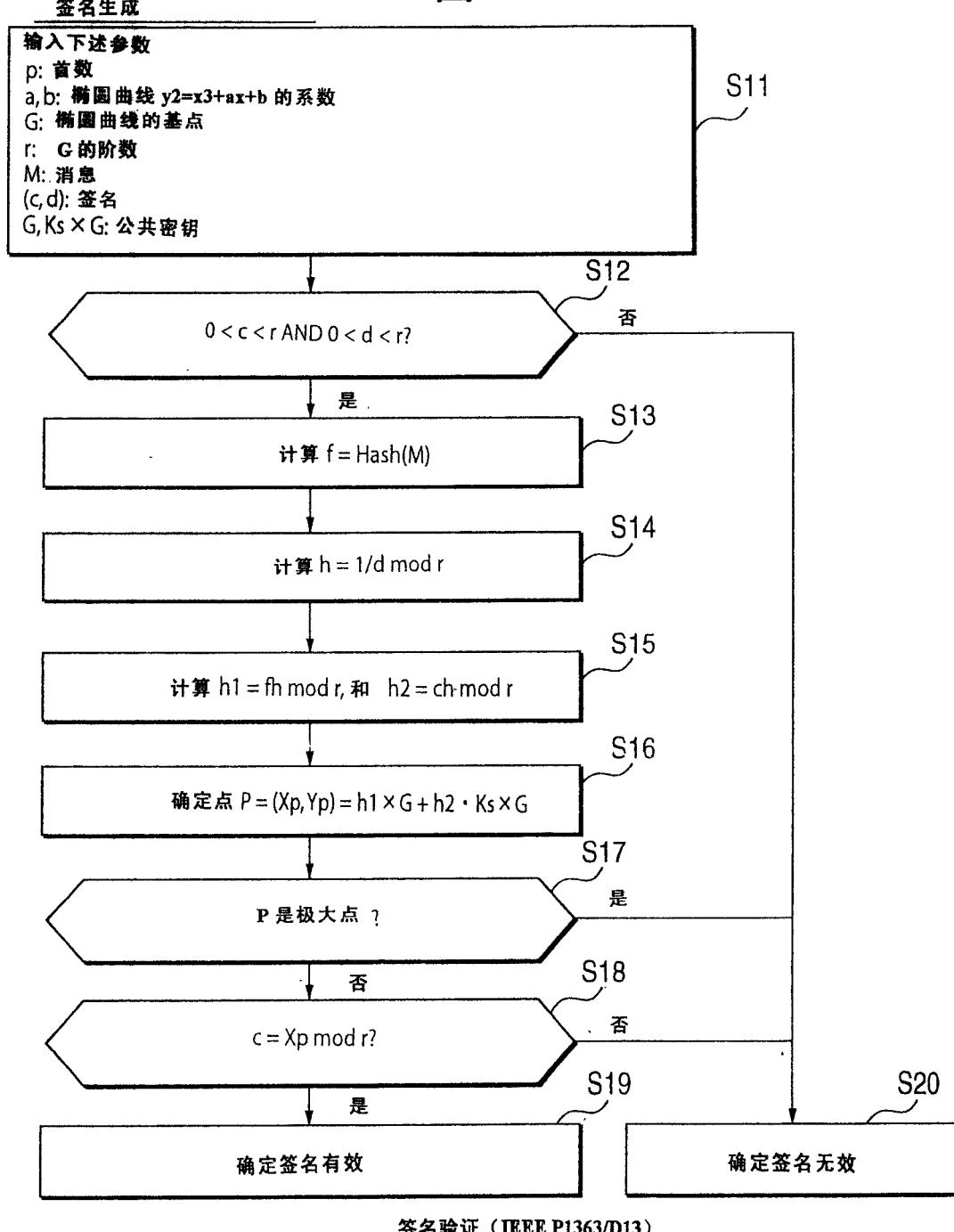


图 12

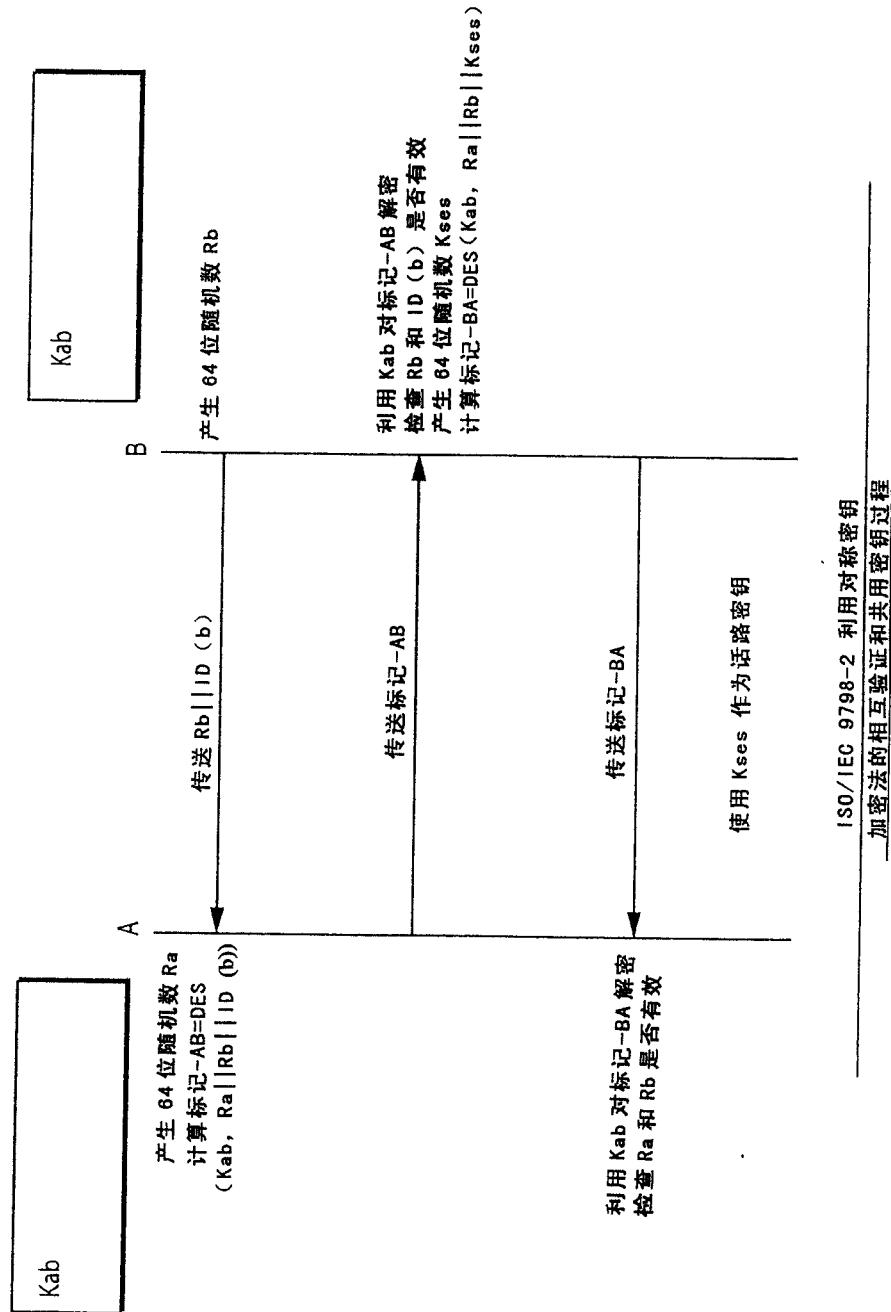


图 13

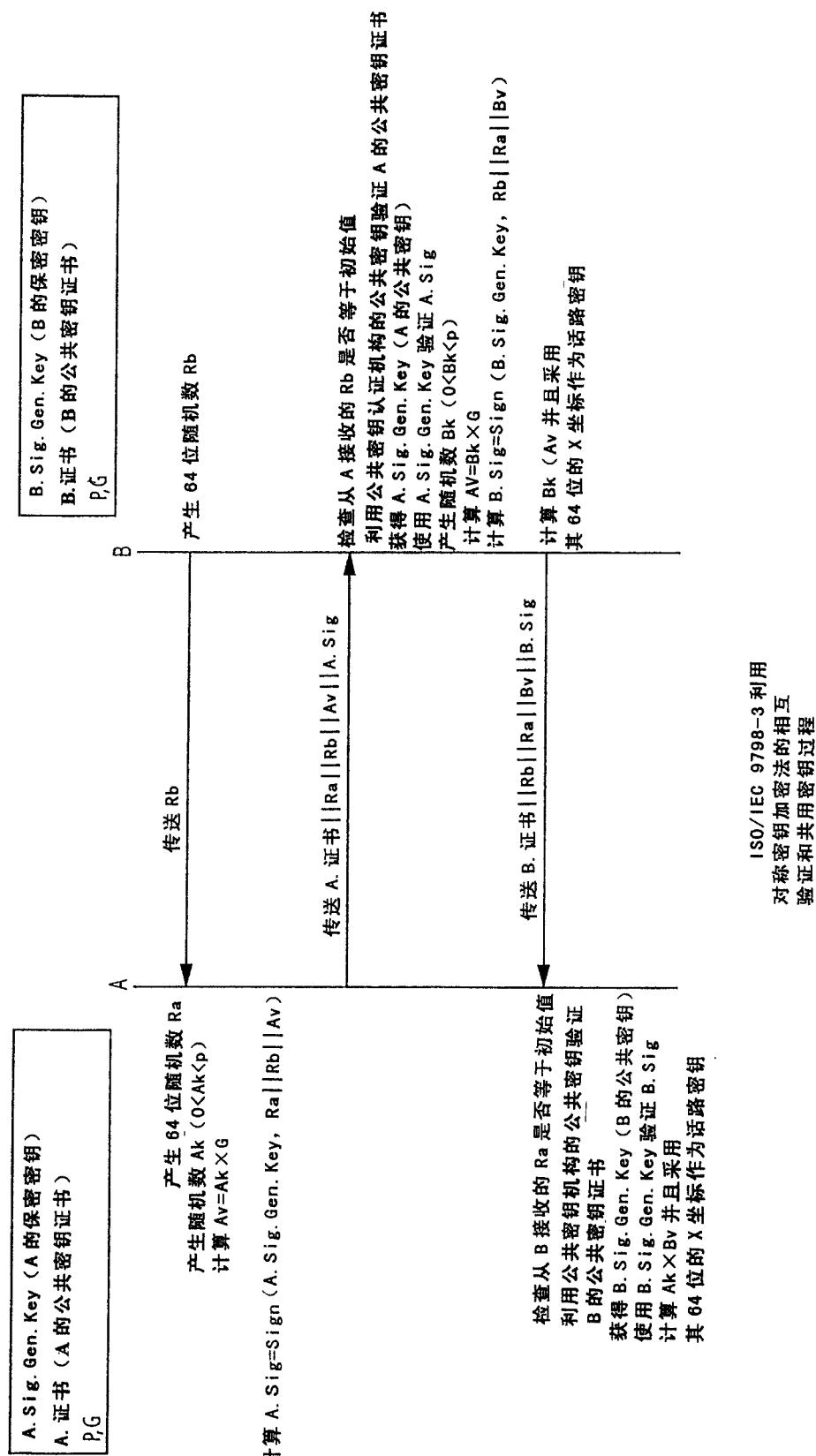


图 14

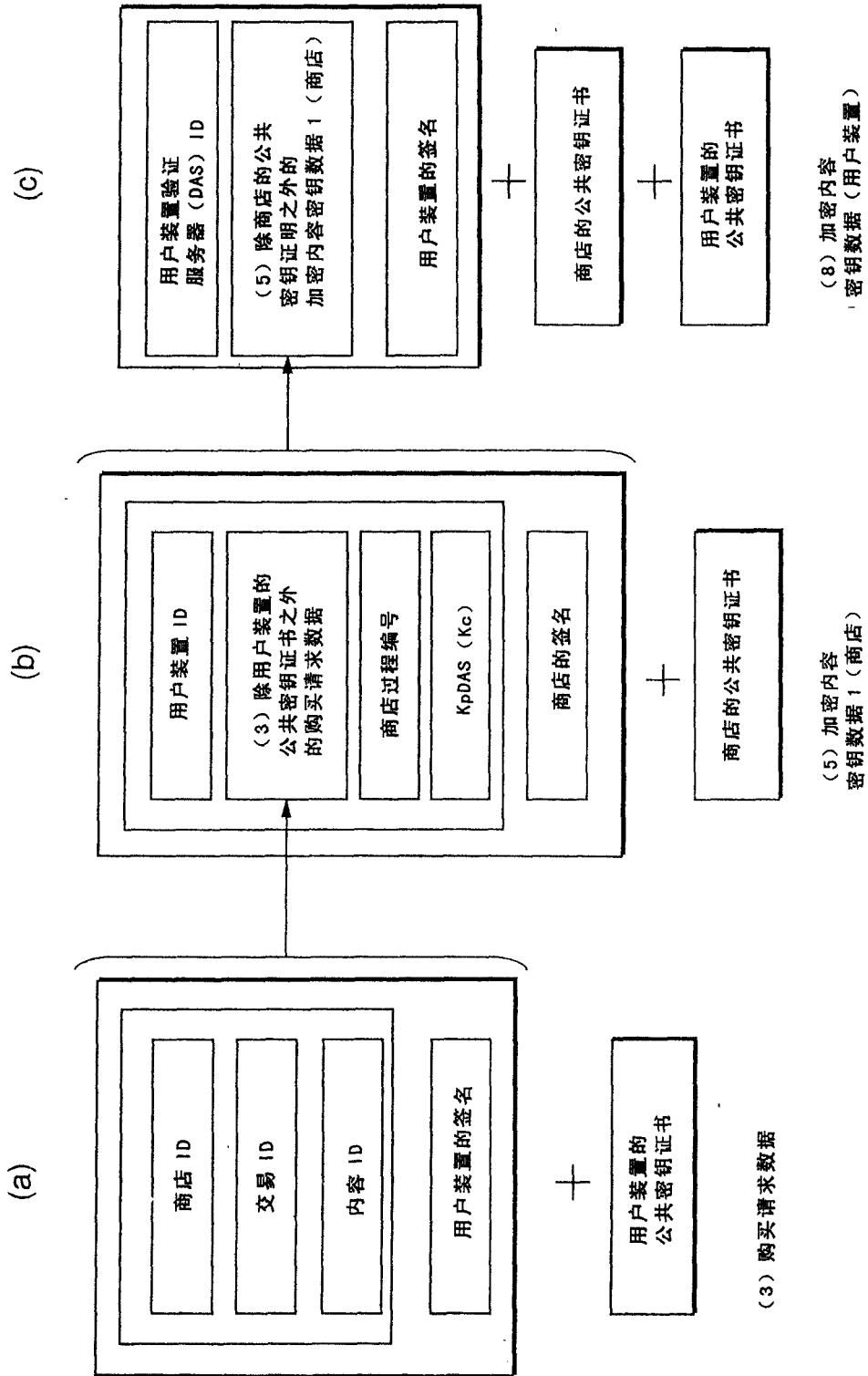


图 15

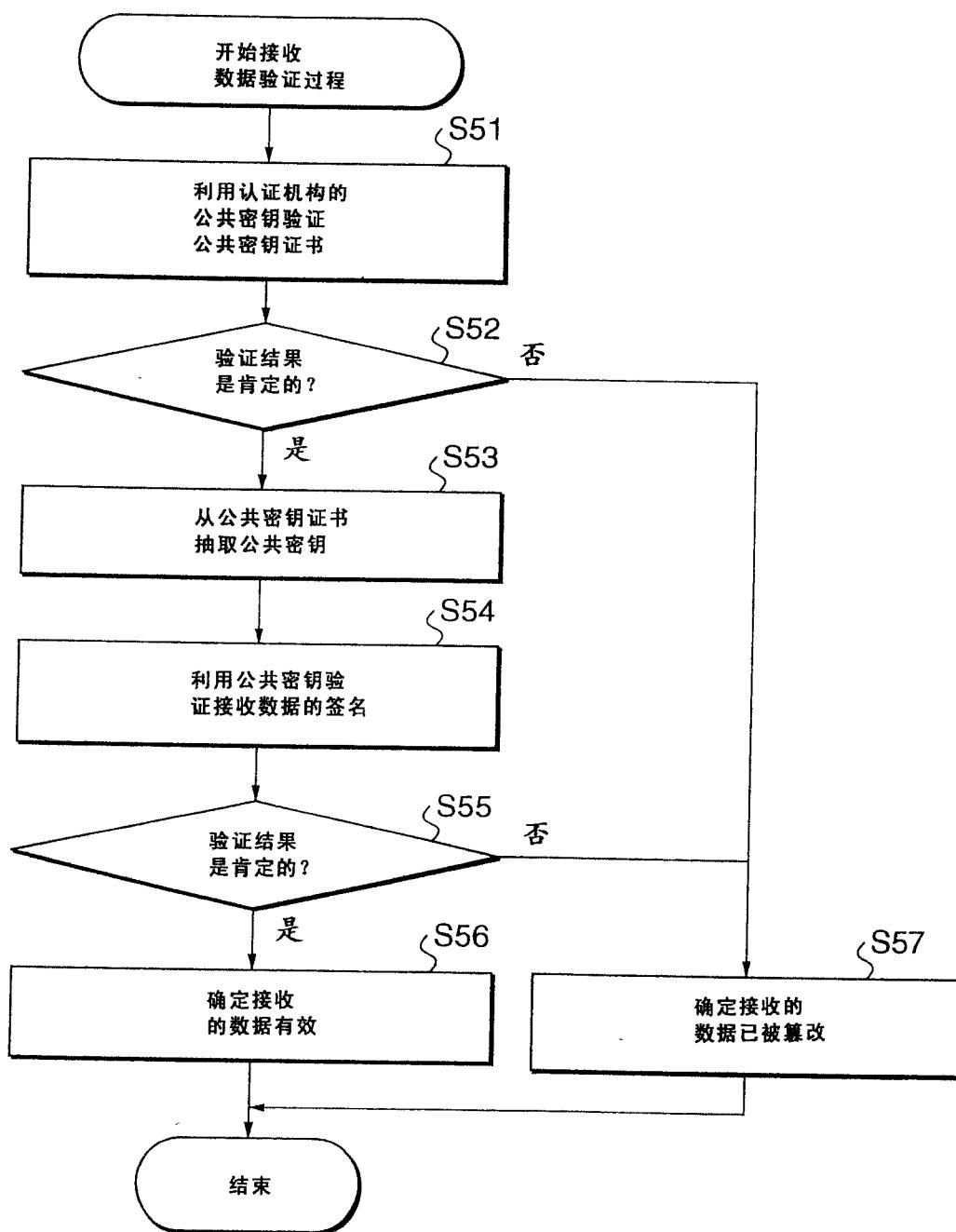


图 16

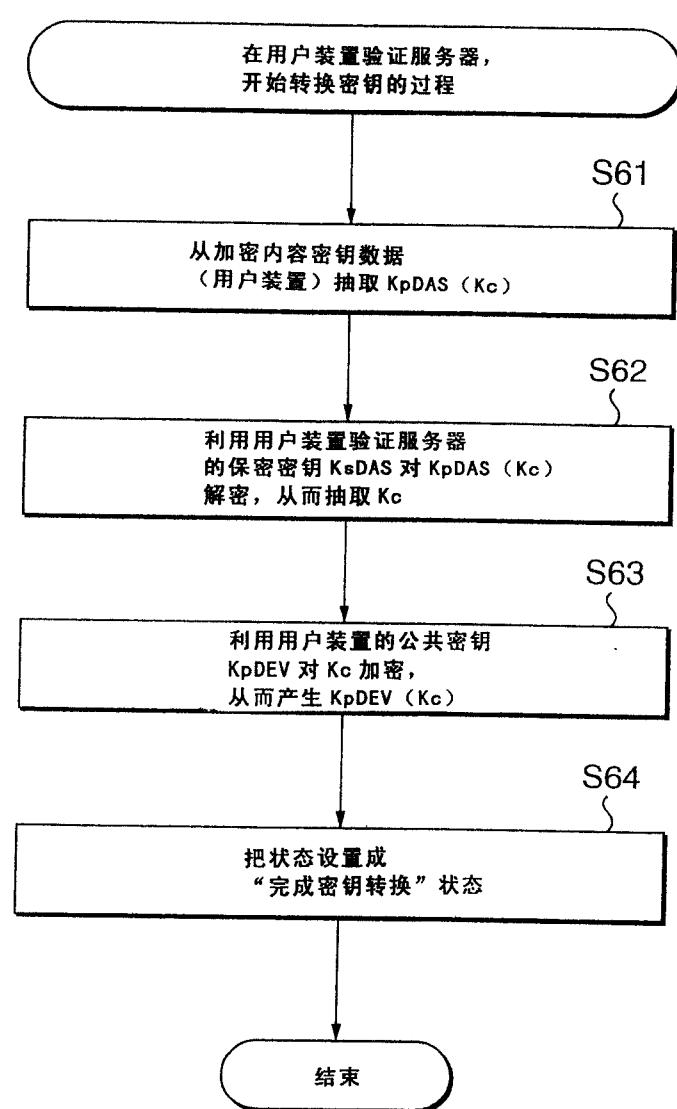


图 17

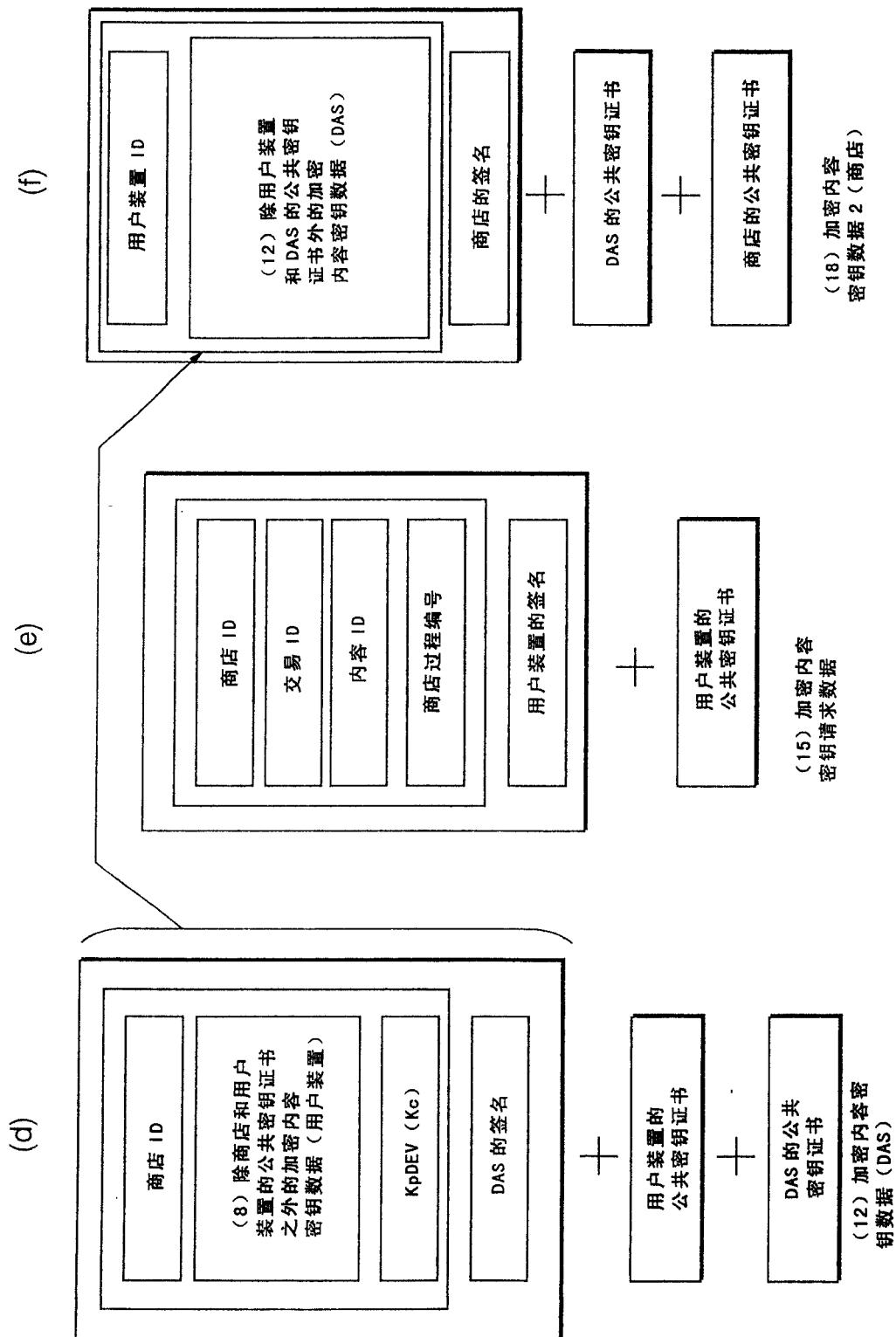


图 18

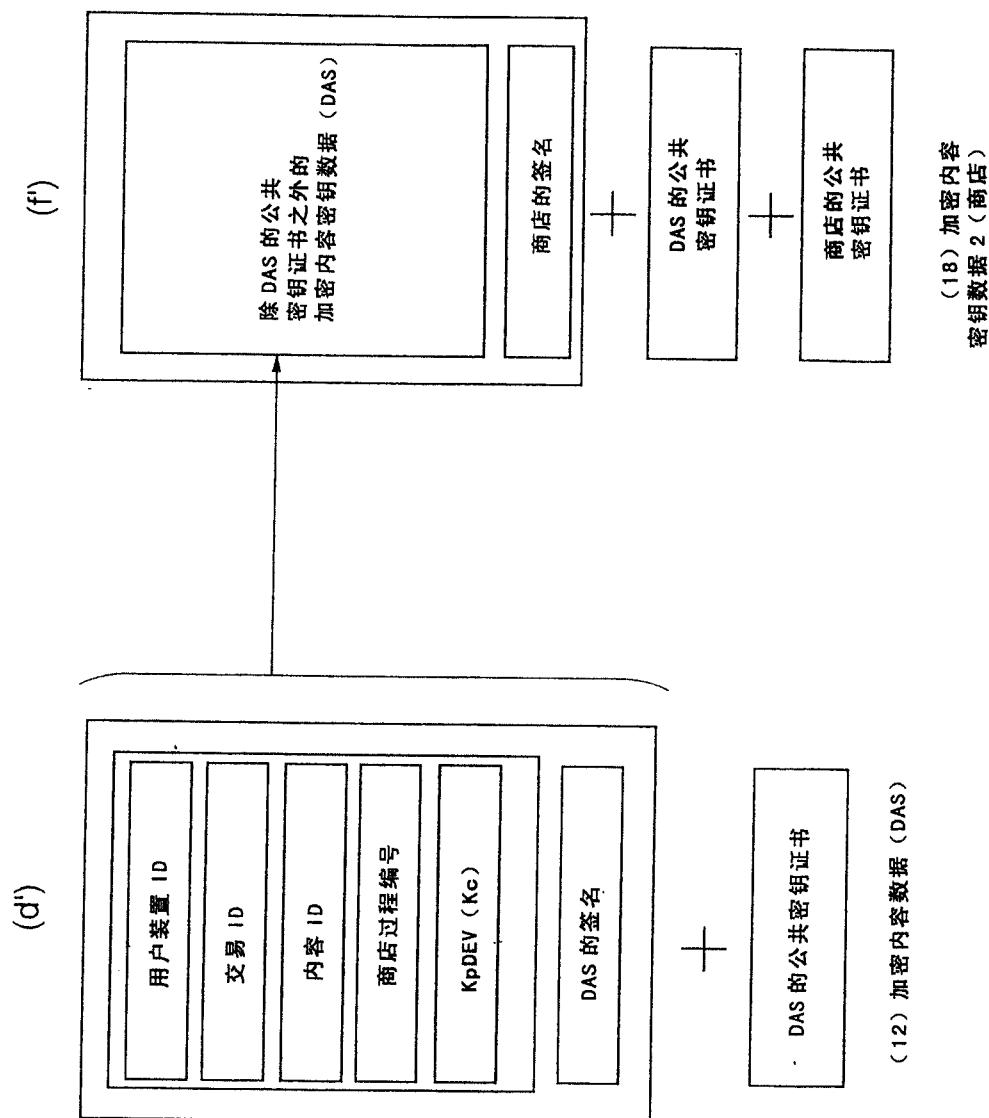


图 19

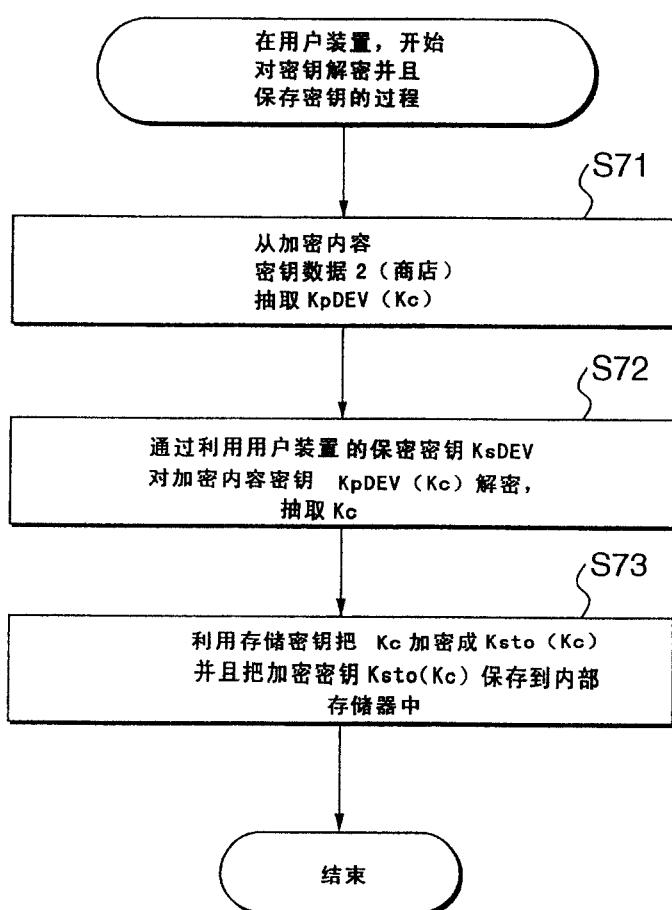


图 20

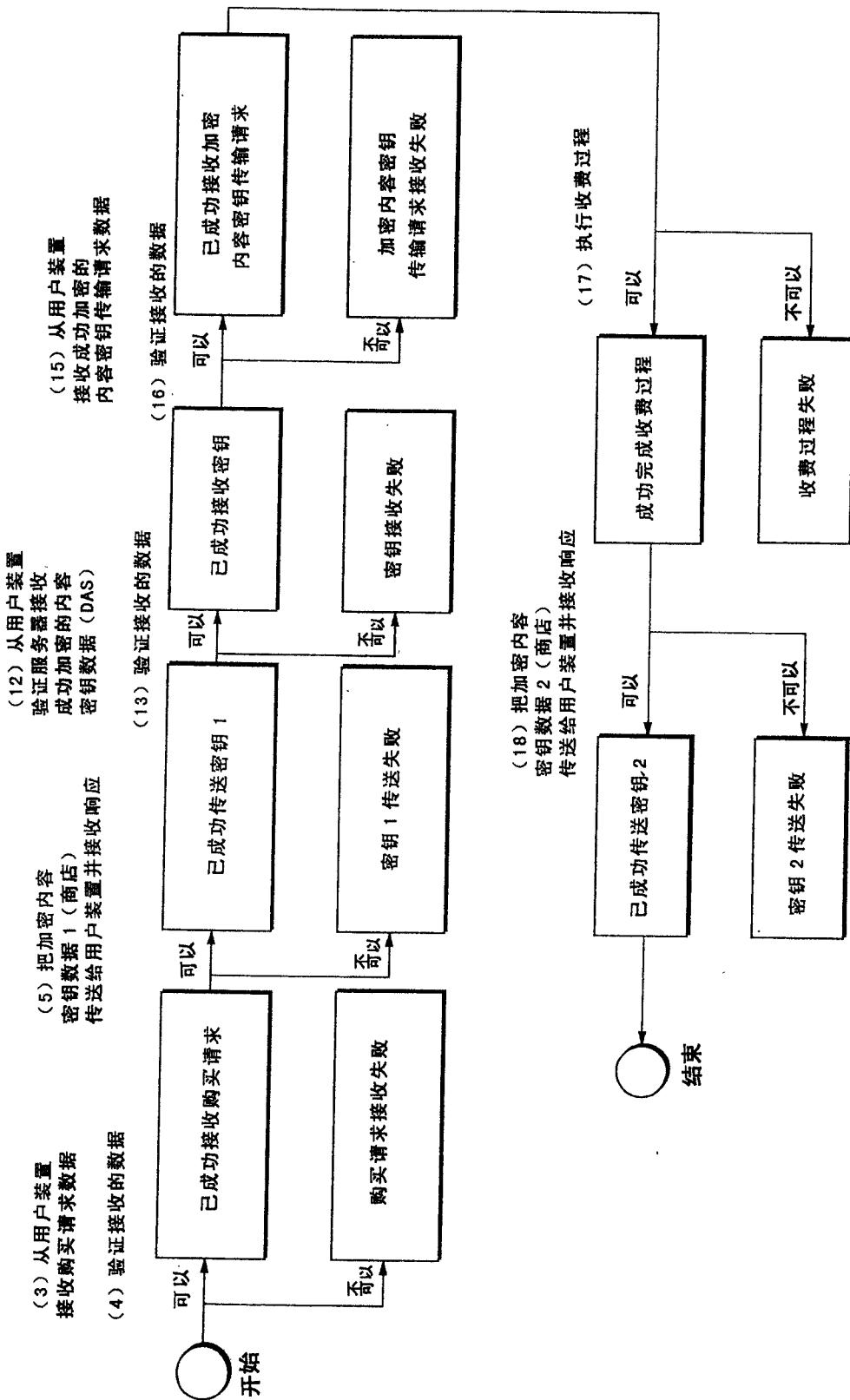


图 21

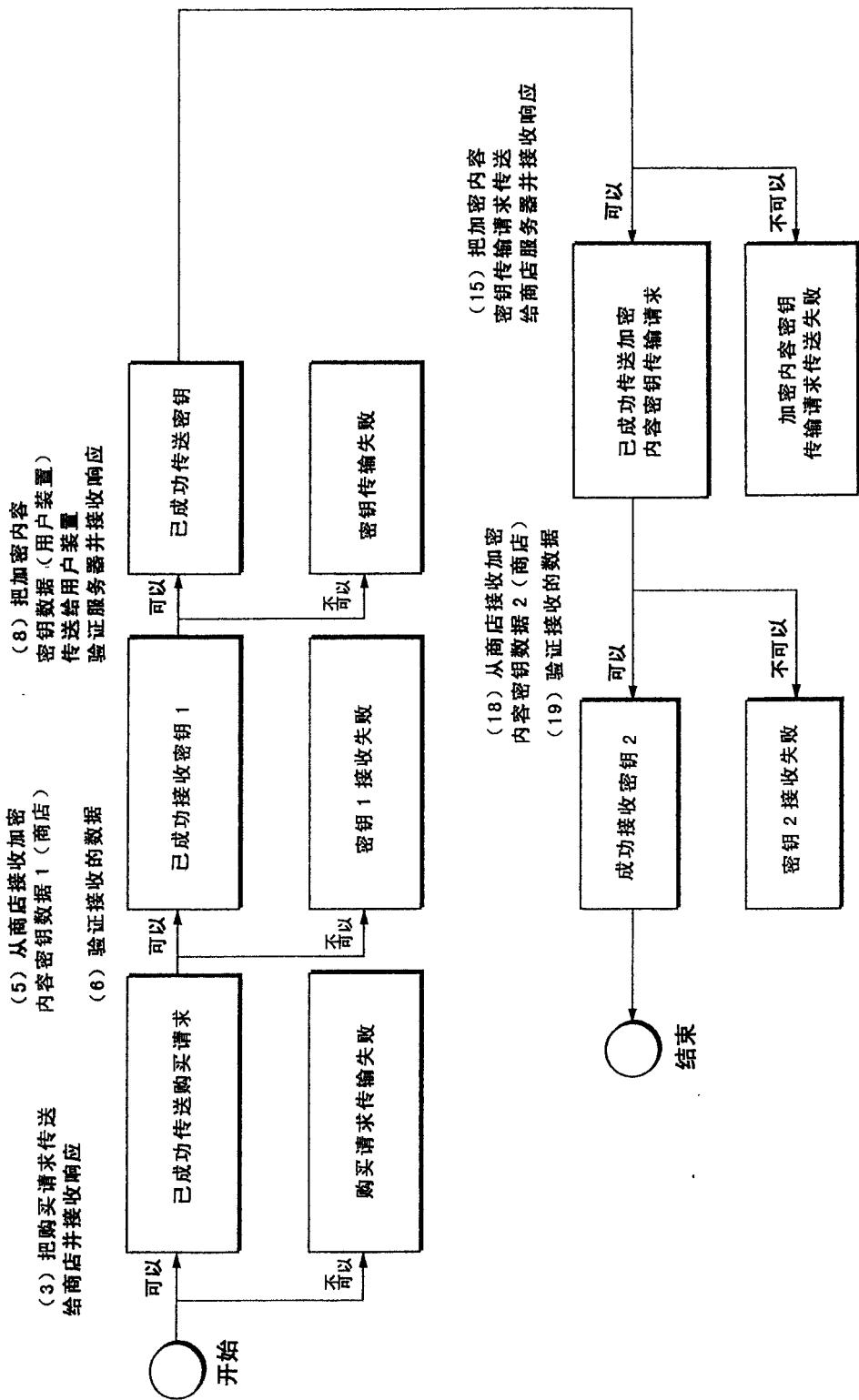


图 22

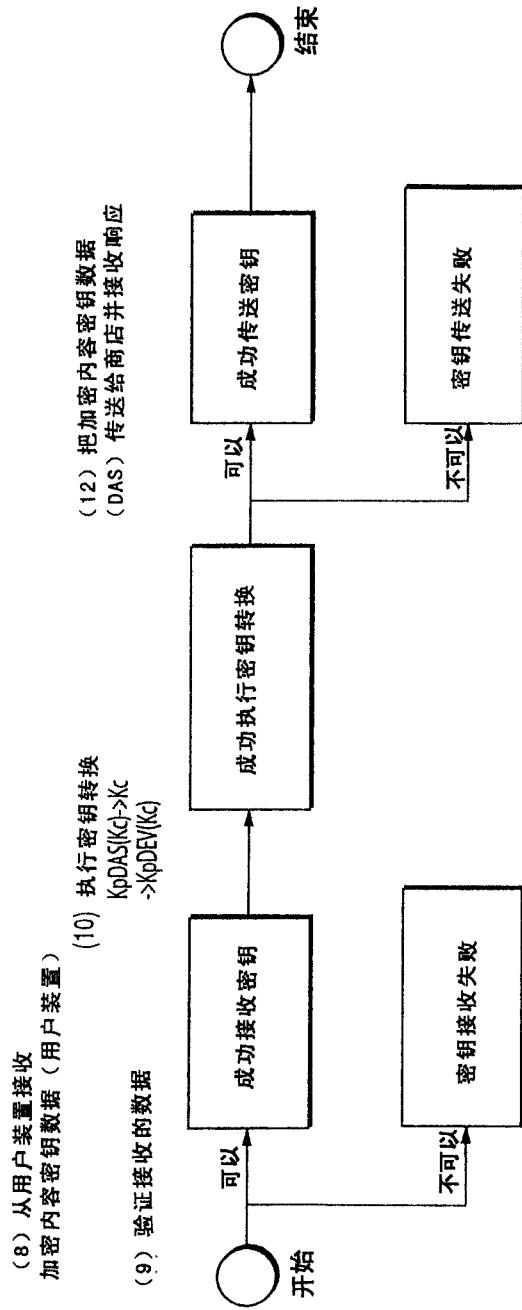


图 23

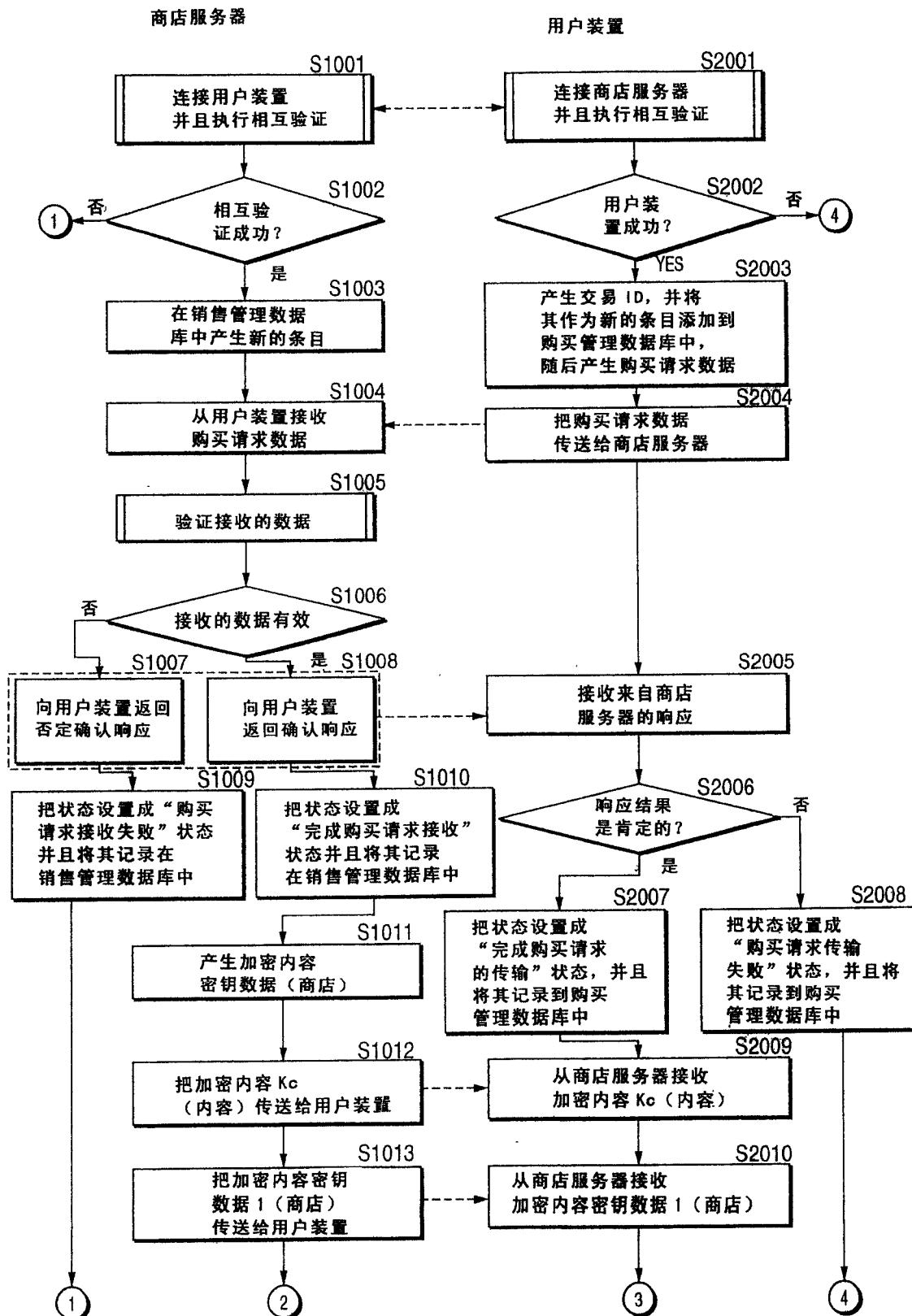


图 24

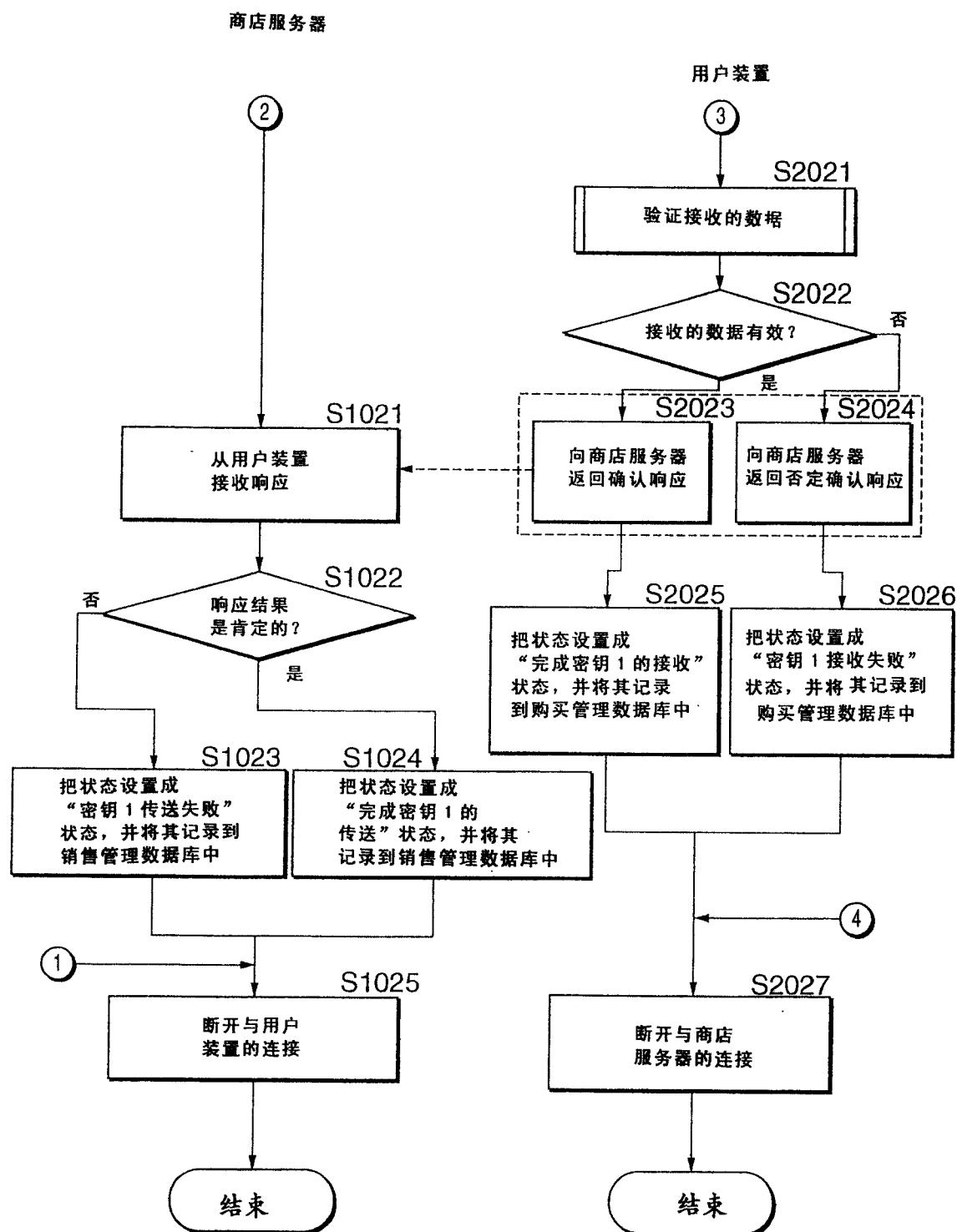


图 25

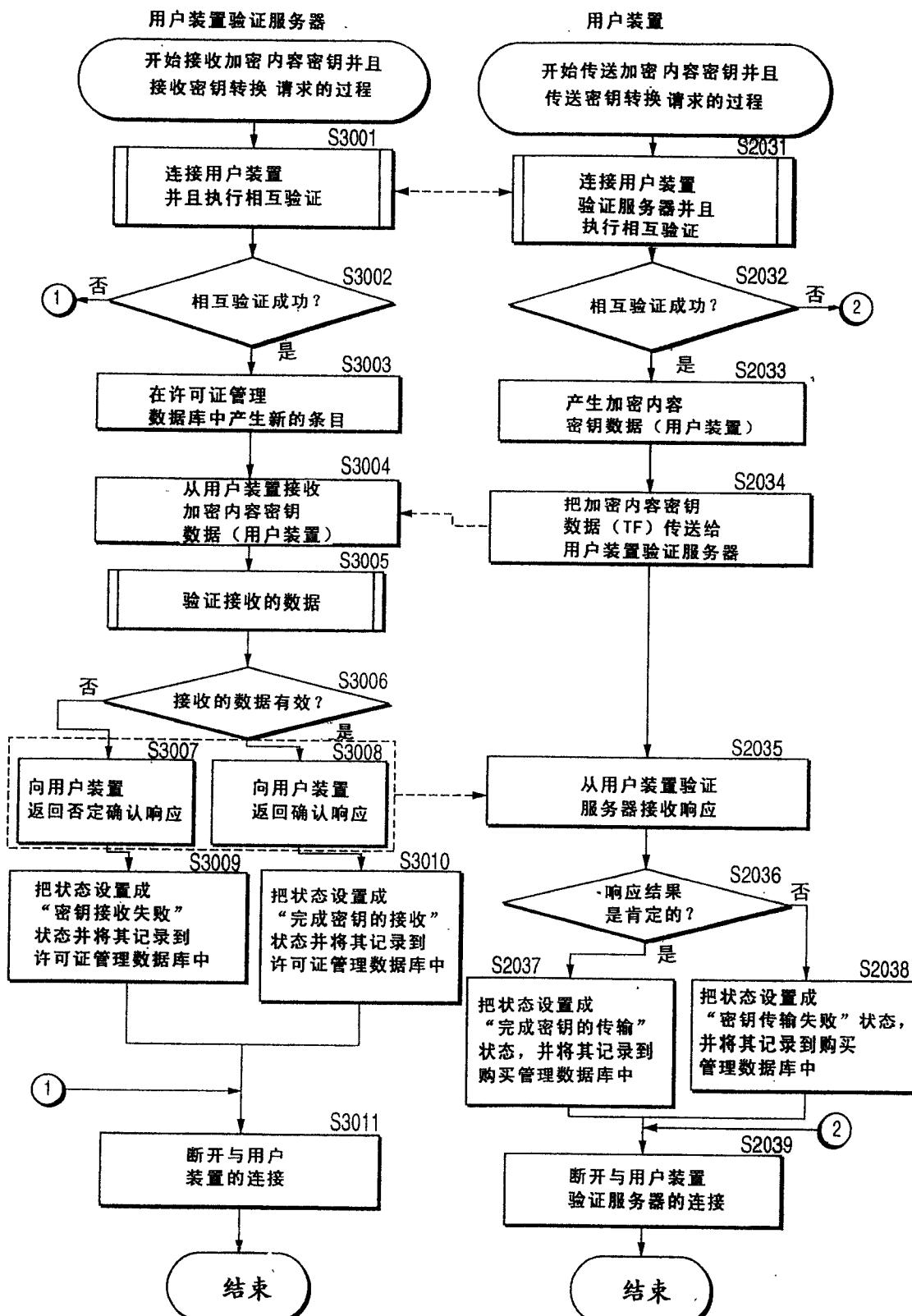
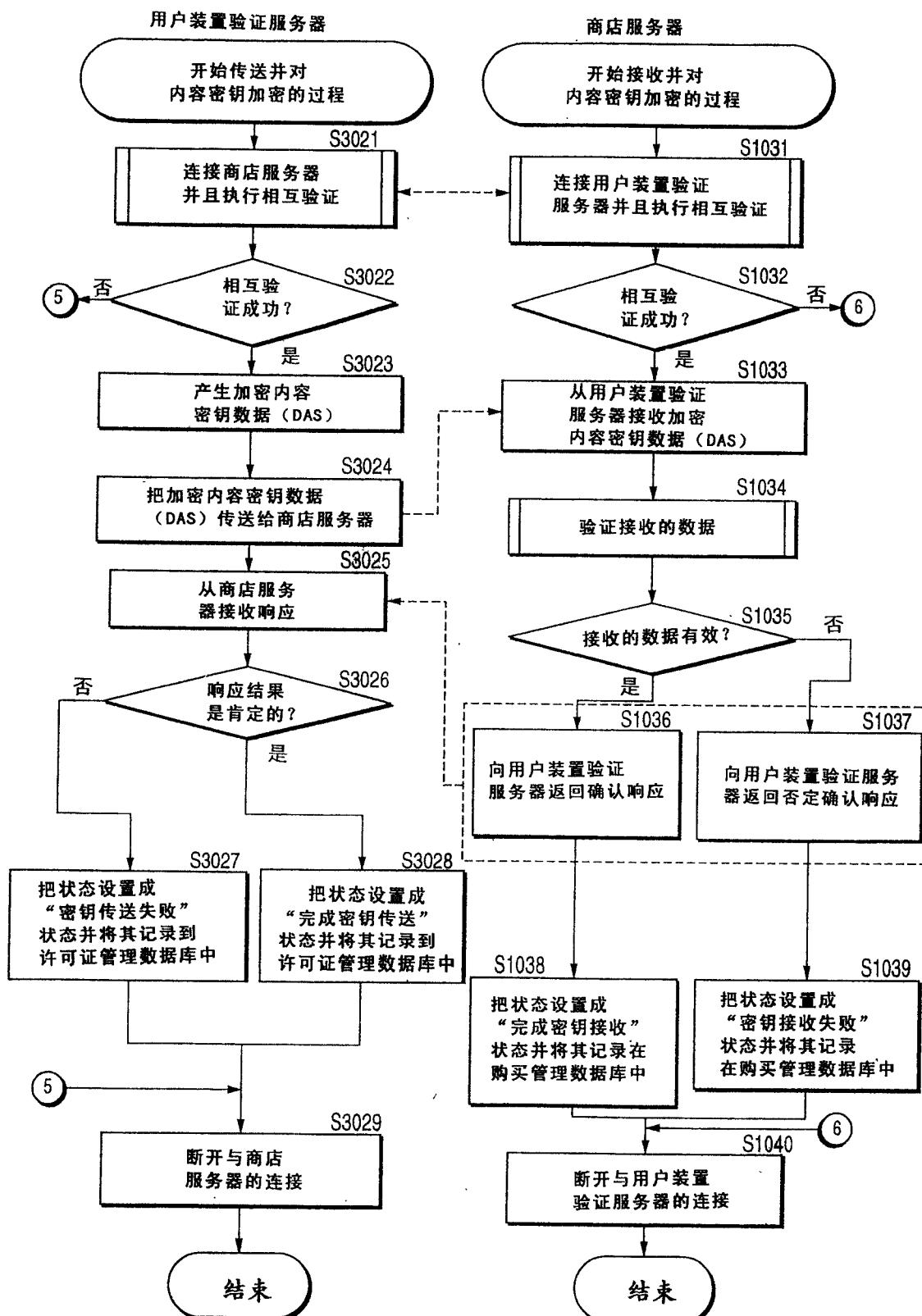


图 26



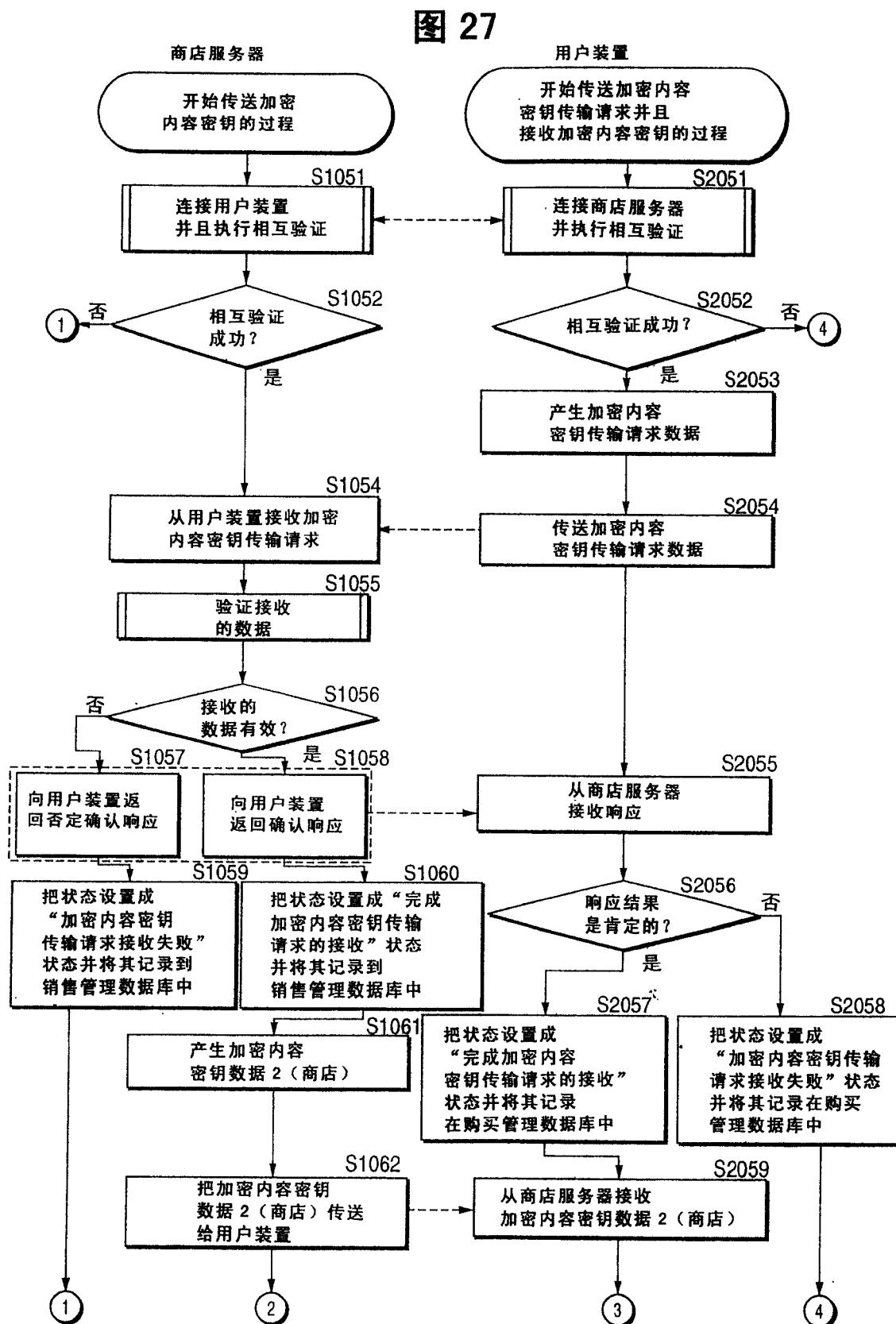


图 28

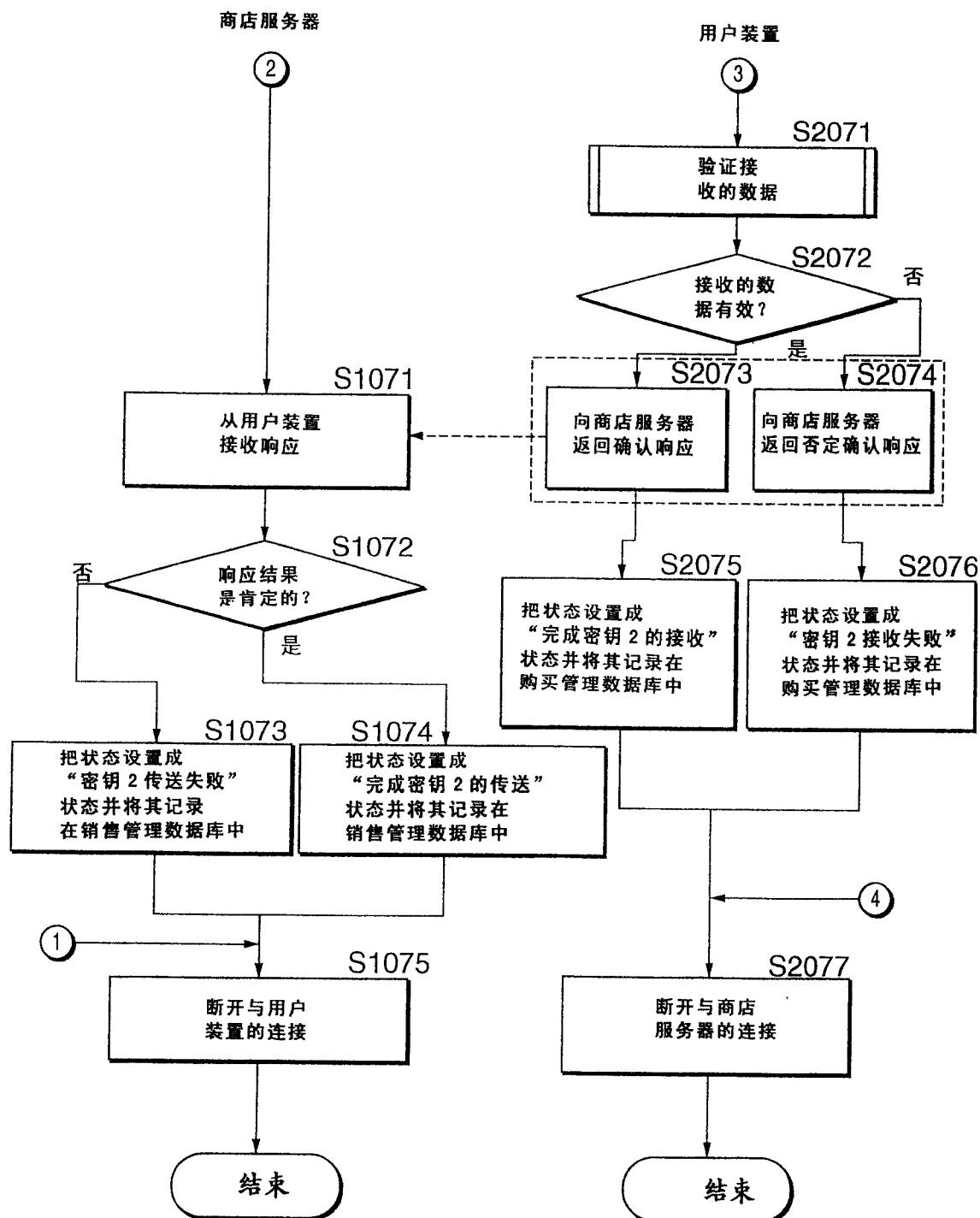


图 29

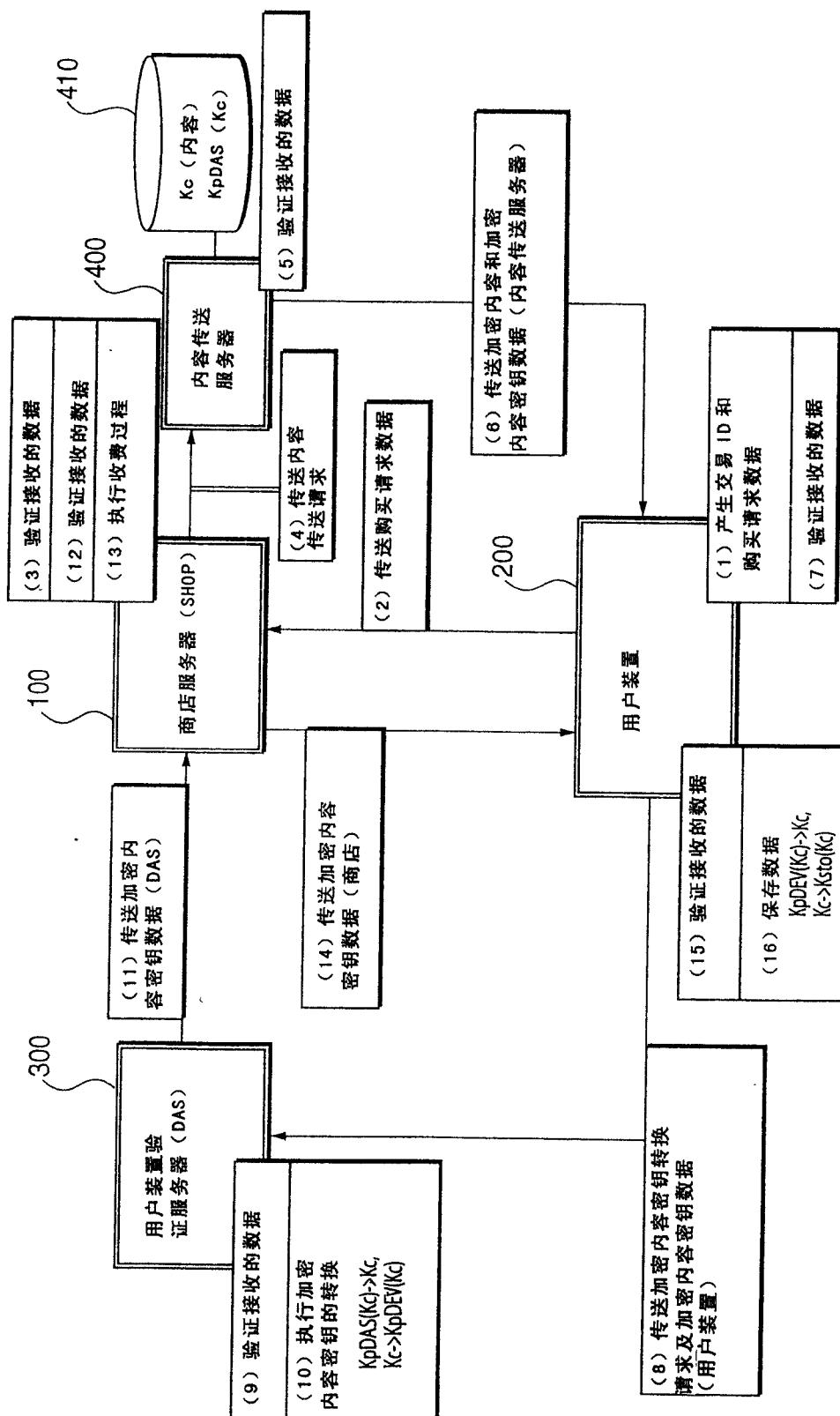


图 30

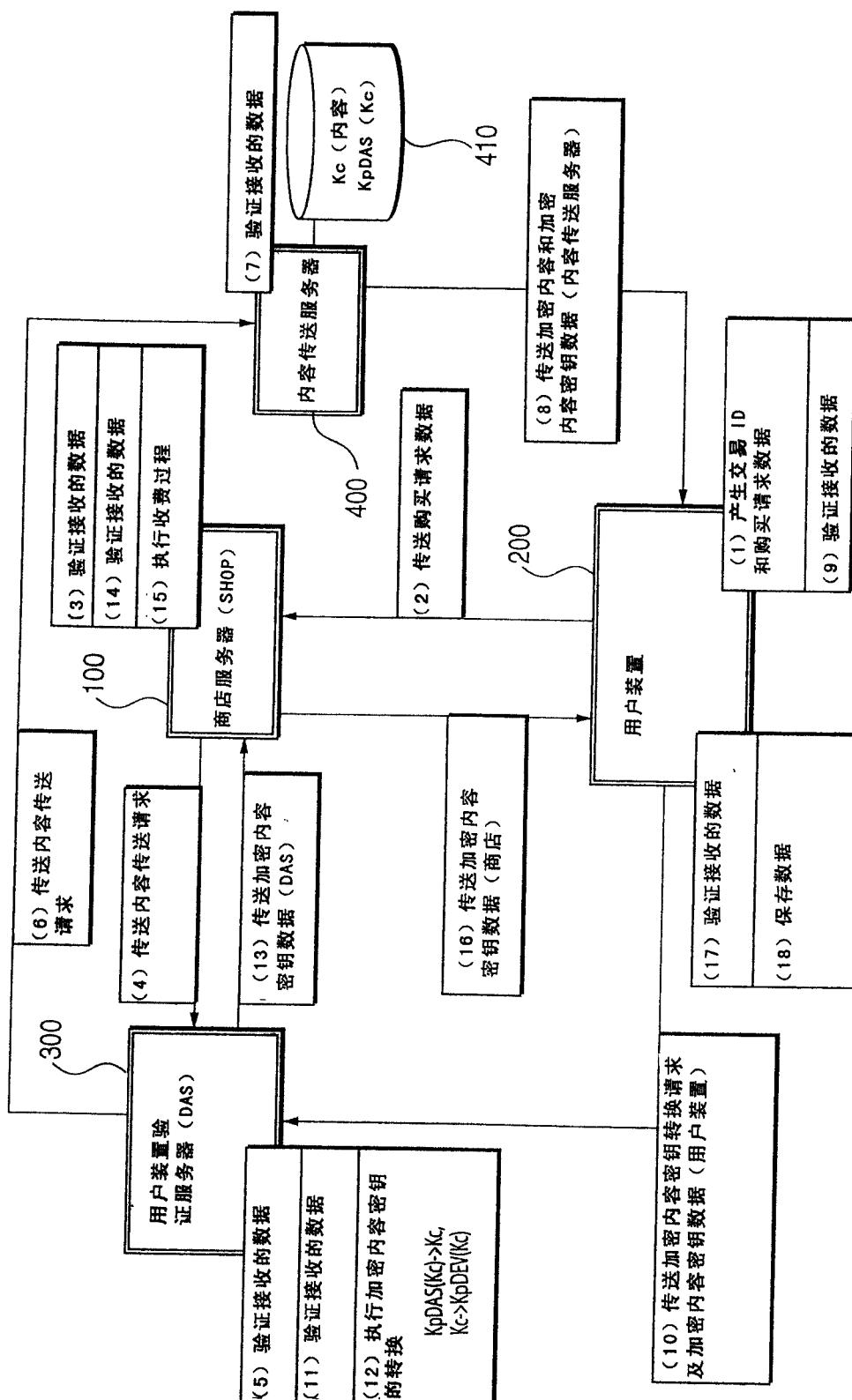


图 31

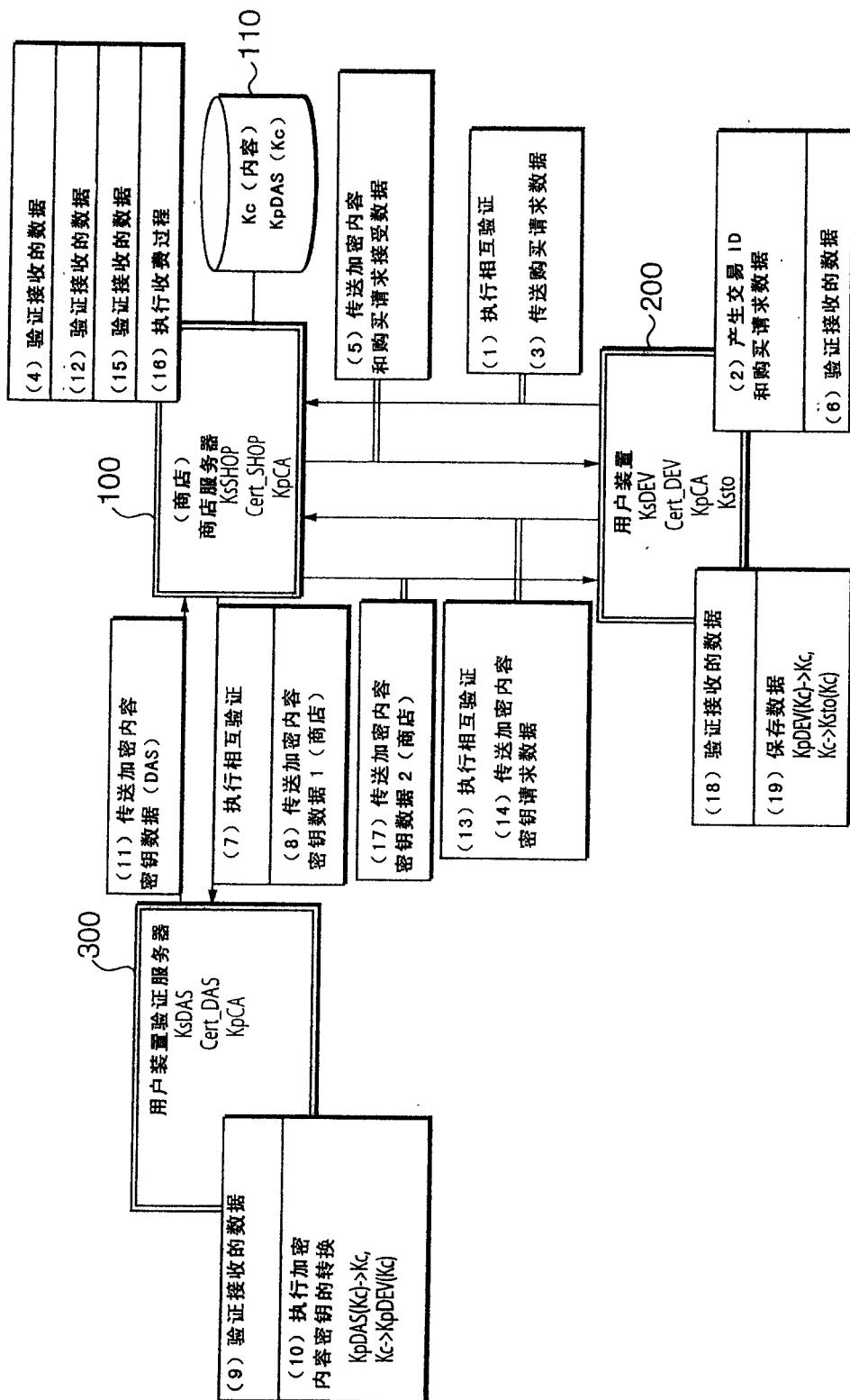


图 32

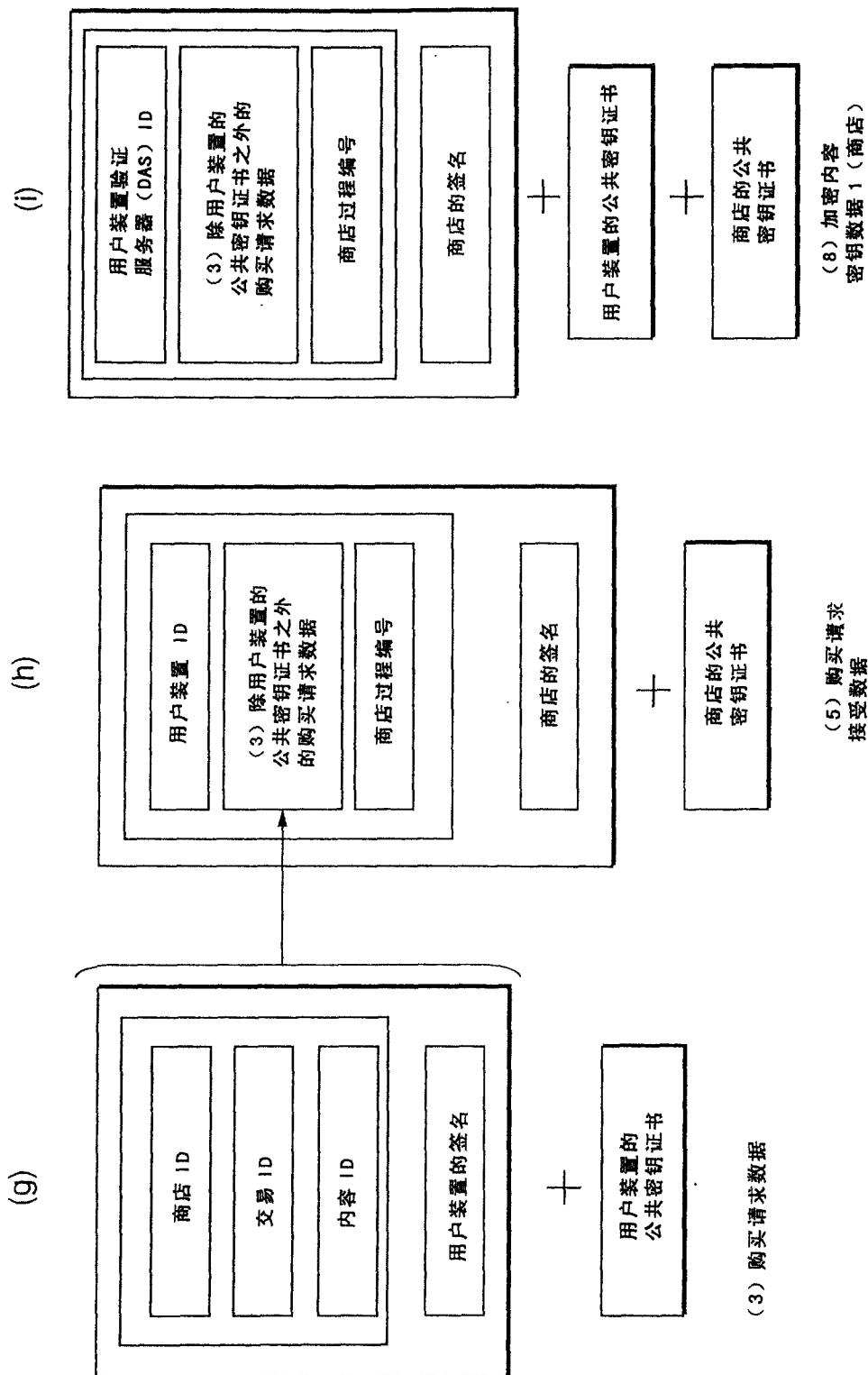
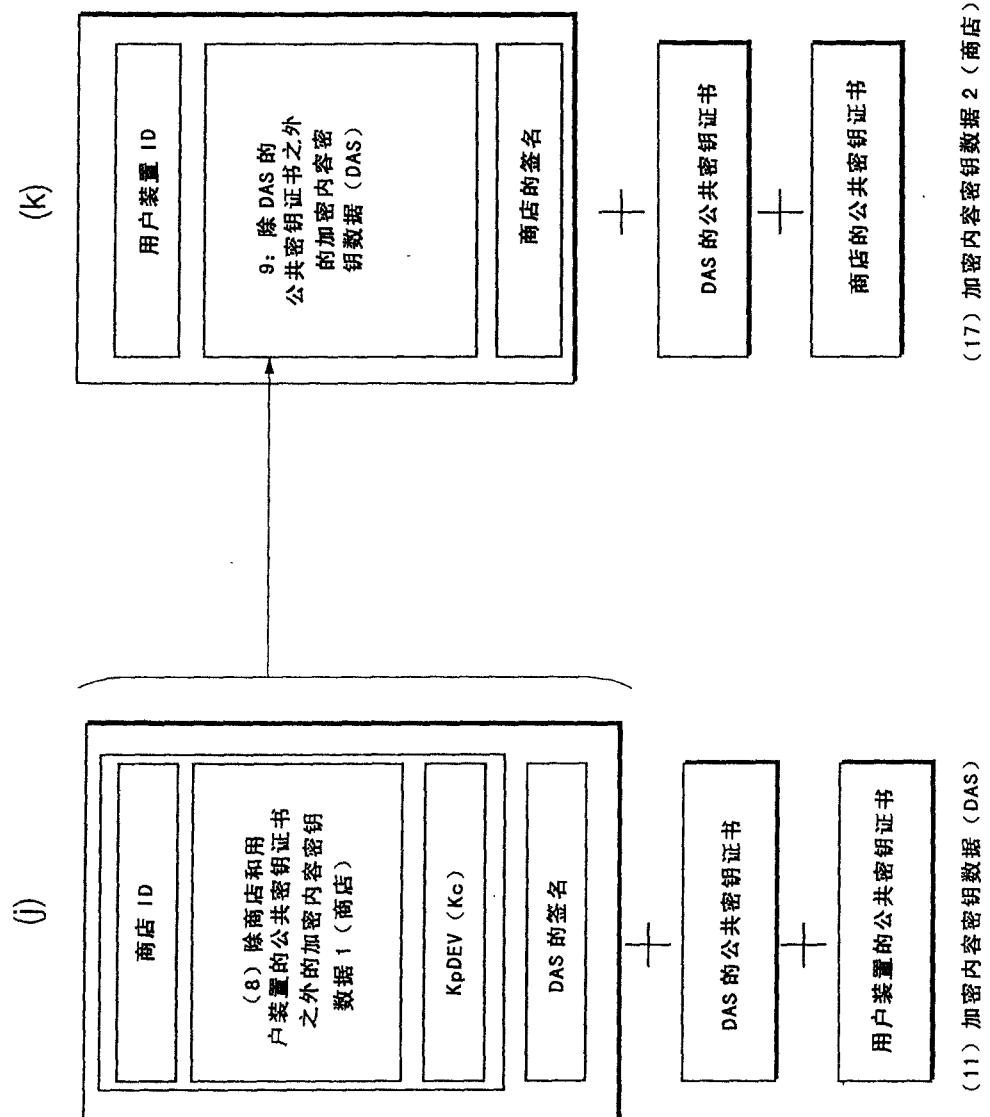


图 33



(17) 加密内容密钥数据 2 (商店)

(11) 加密内容密钥数据 (DAS)

图 34

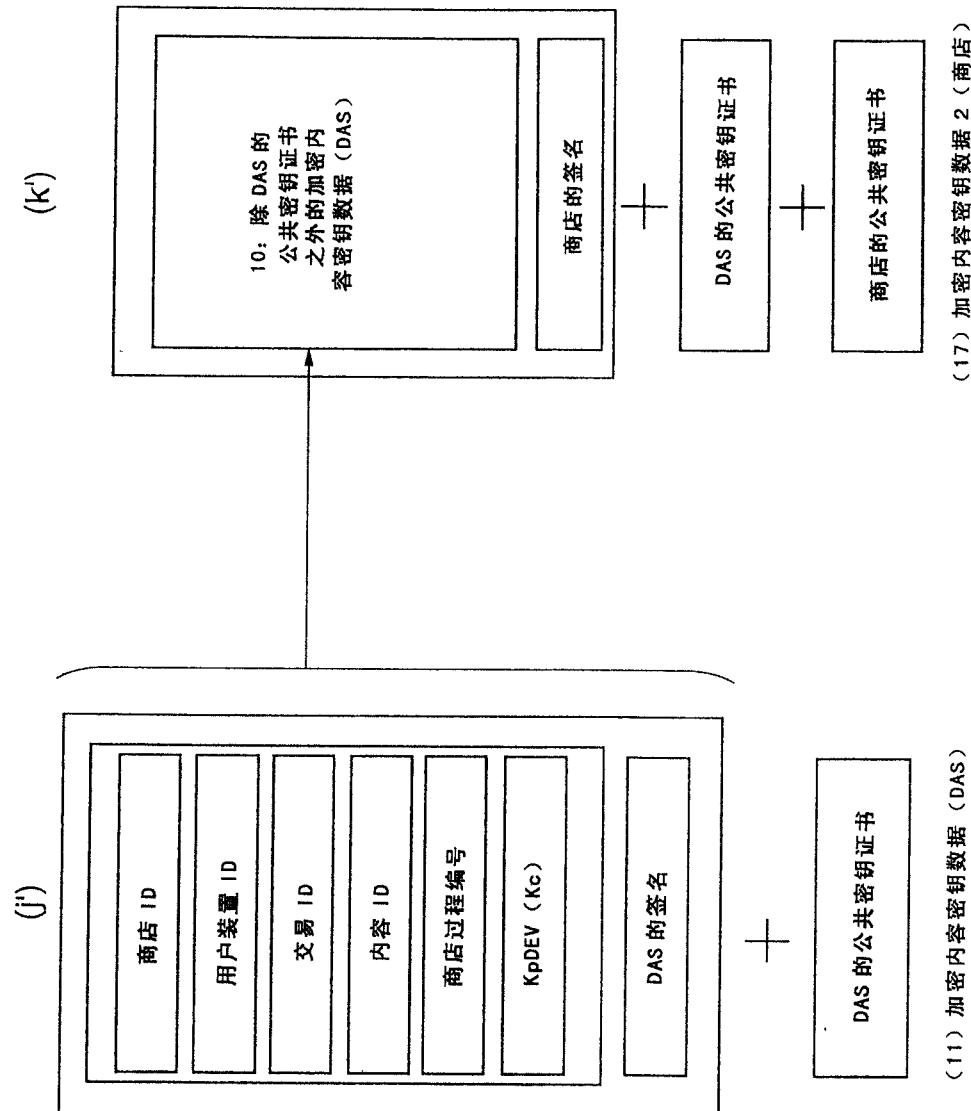


图 35

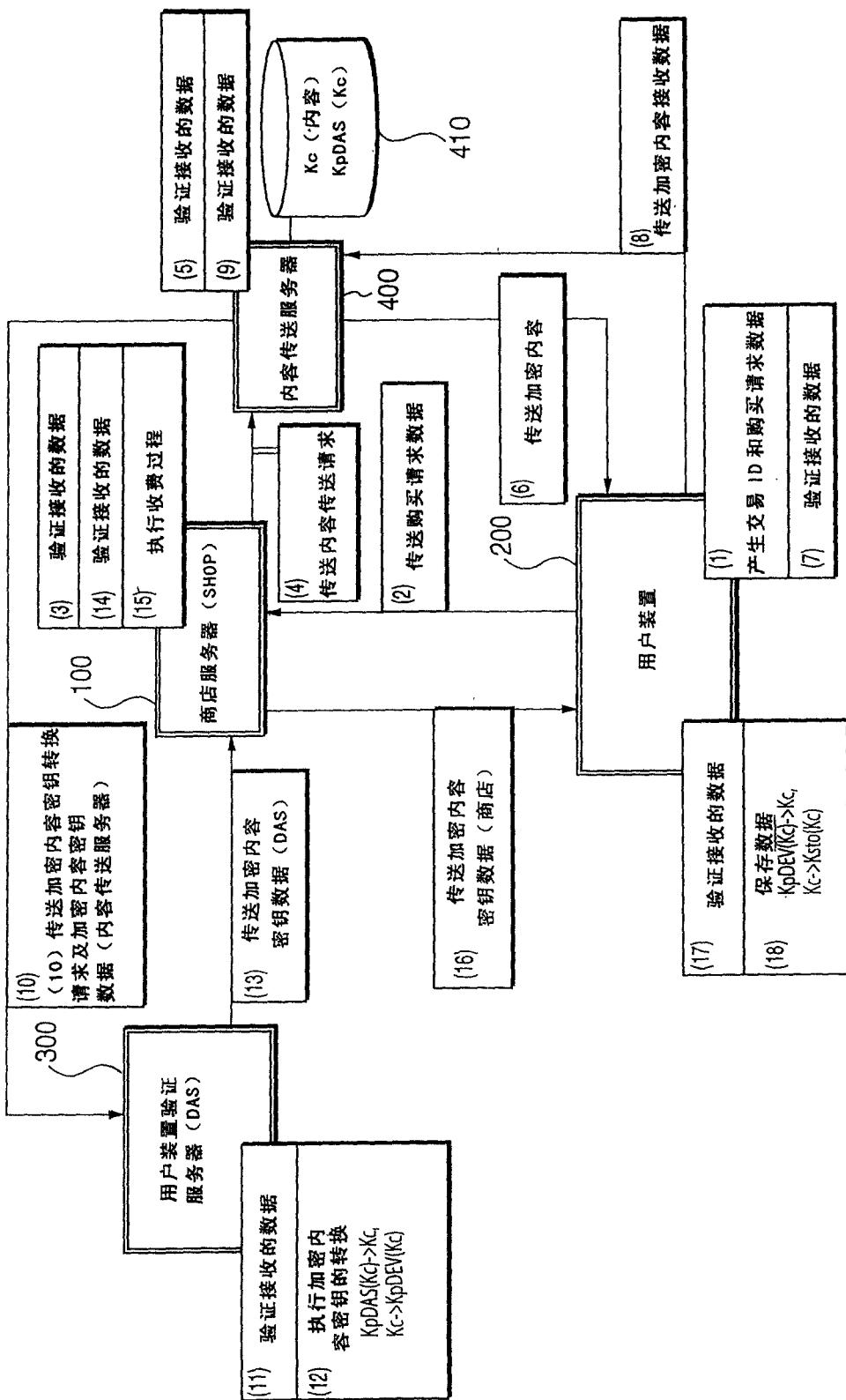


图 36

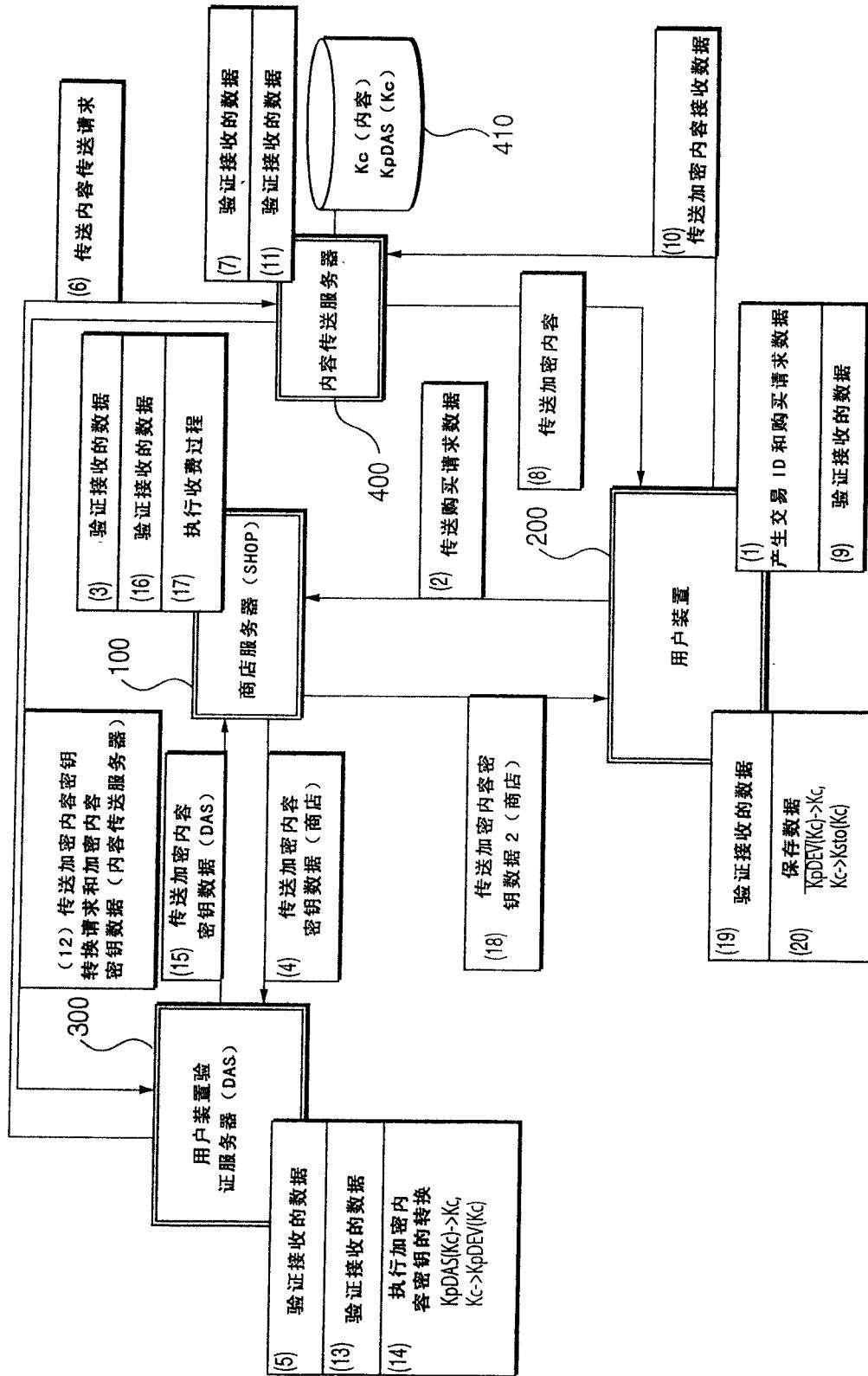


图 37

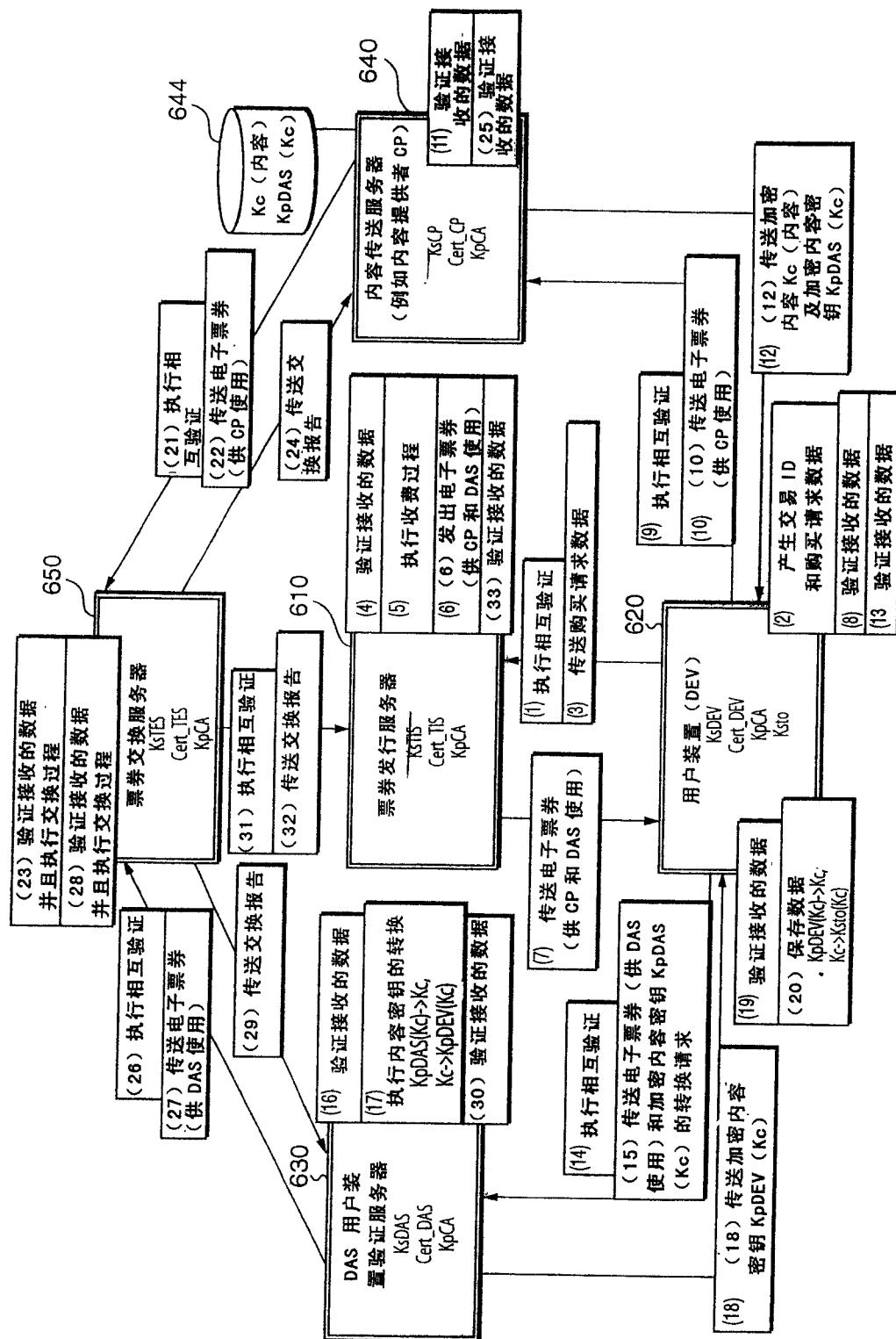


图 38

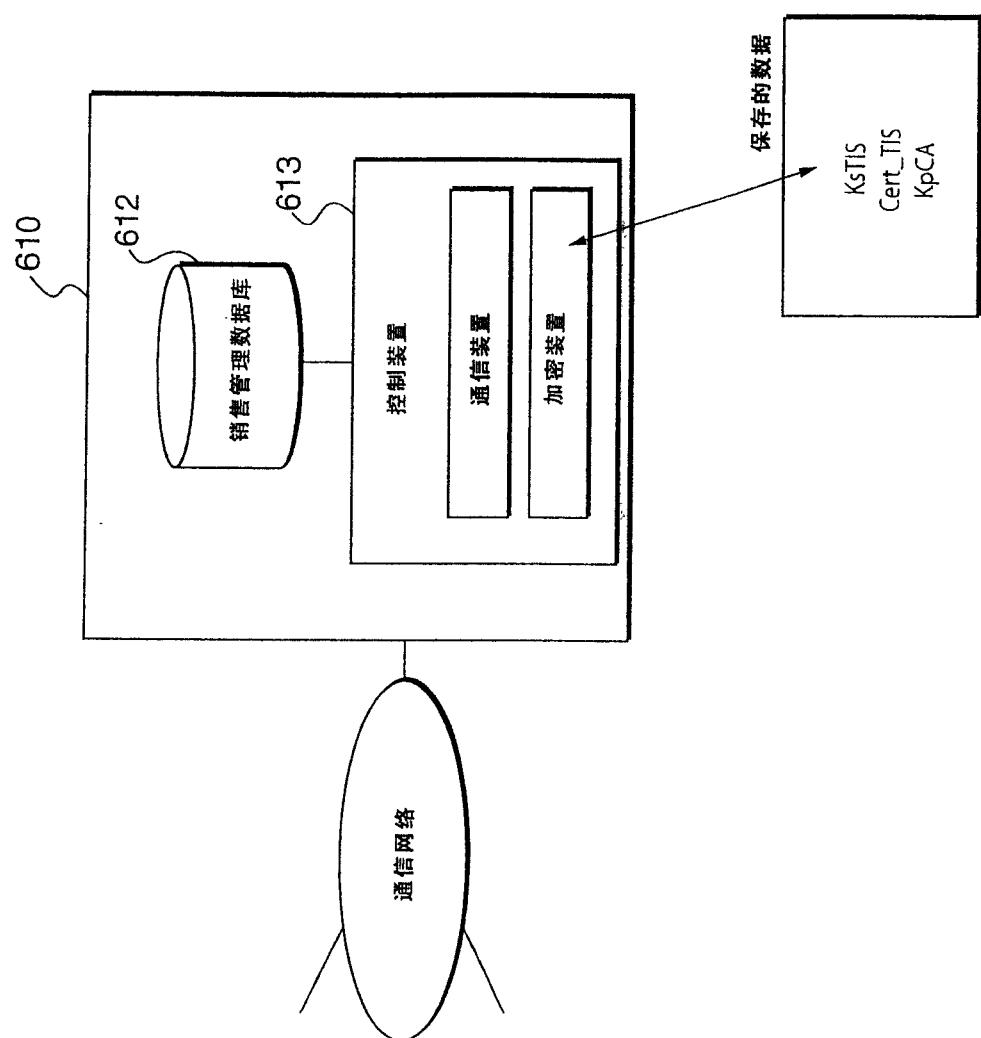


图 39

票券发行过程编号	装置 ID	交易 ID	内容 ID	票券用户 ID	金额	有效期	状态
10001	1234567890	999888777	5000	22231234	¥1000	00/04/01	成功接收交換报告
10002	2345678901	666555444	4050	223345634	¥250	00/07/31	成功传送电子票券
10003	3456788901	321655444	4021	345645234	¥800	00/07/31	成功传送购买请求

票券发行服务器的票券发行管理数据库

图 40

交易 ID	内容 ID	票券发行者 ID	票券发行过程编号	票券地址 ID	状态
999888777	5000	1234	10001	1234567890	成功完成密钥 2 的接收
666555444	4050	1534	12345	2345678901	成功完成密钥 1 的接收
999888779	5010	2351	15435	2233567890	成功完成电子票券的传送
333555444	4320	0989	10302	成功完成电子票券的接收
2133545445	3232	3549	22543	成功完成购买请求的传送

用户装置的购买管理数据库

图 41

DAS 过程编号	装置 ID	交易 ID	内容 ID	票券发行者 ID	票券发行过程编号	状态
50001	1234567890	9999888777	5000	331234	10001	成功完成交换报告的接收
50002	2345678901	6665554444	7050	345634	10025	成功完成票券 交换请求的传送
50003	345688901	321655444	8021	645334	10200	成功完成密钥的传送
50004	5567778902	123555444	3245	321632	10325	成功完成密钥的转换
50005	5435678445	335655321	2651	764545	12300	成功完成密钥的接收

用户装置验证服务器的许可证管理数据库 -

图 42

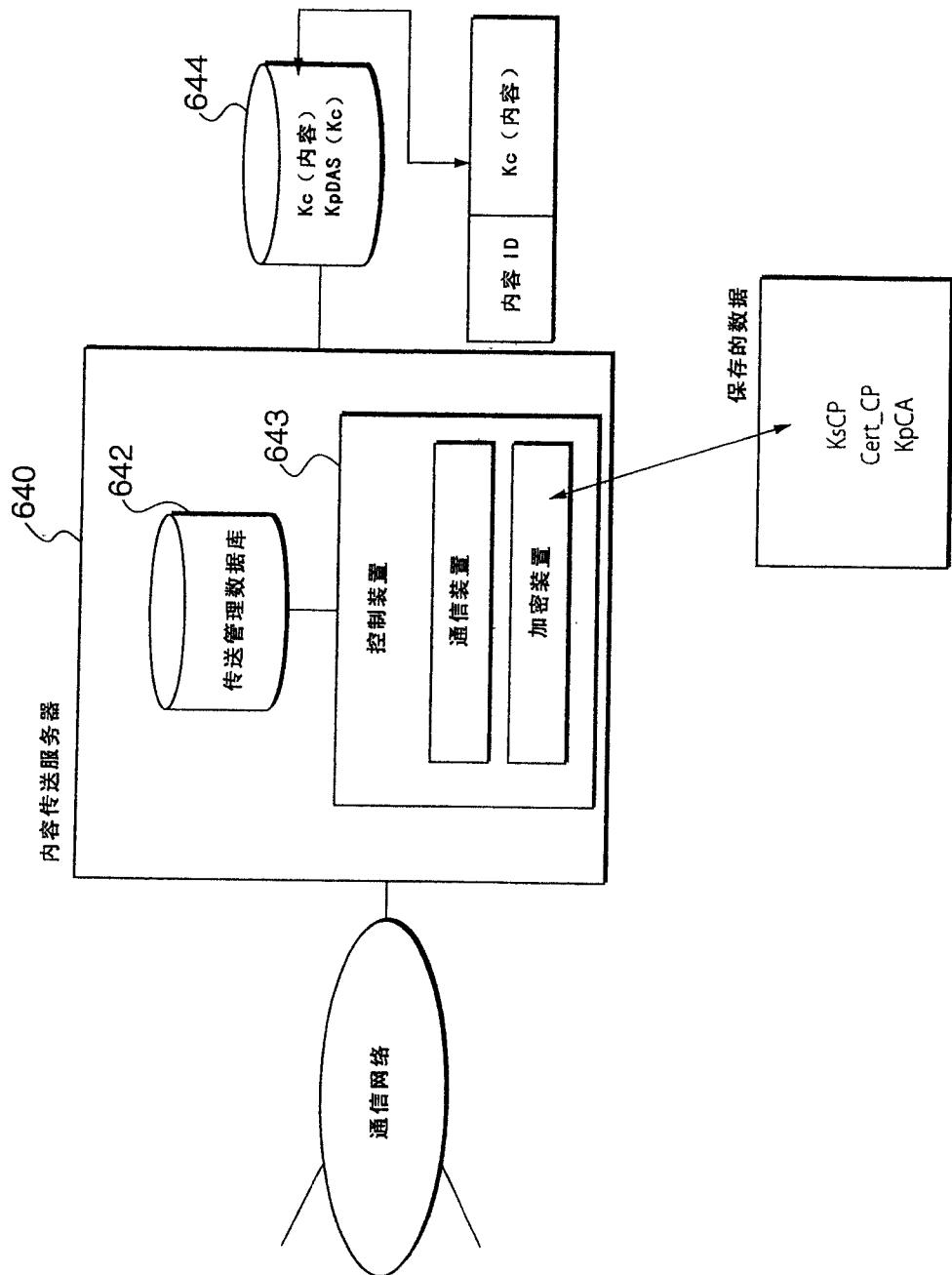


图 43

内容传送服务器过程编号	内容 ID	装置 ID	票券发行者 ID	票券发行过程编号	状态
999888777	5000	1234567890	1234	12345	成功完成交換报告的接收
666555444	4050	3427781534	2345	23456	成功完成票券 交換请求的传输
999888779	5010	2355643551	1545	22335	成功完成传送
333555444	4320	4987390989	1030	32423	成功完成电子票券的接收
213354445	3232	3542416759	2253	44323	成功完成电子票券的接收

内容传送服务器
的传送管理数据库

图 44

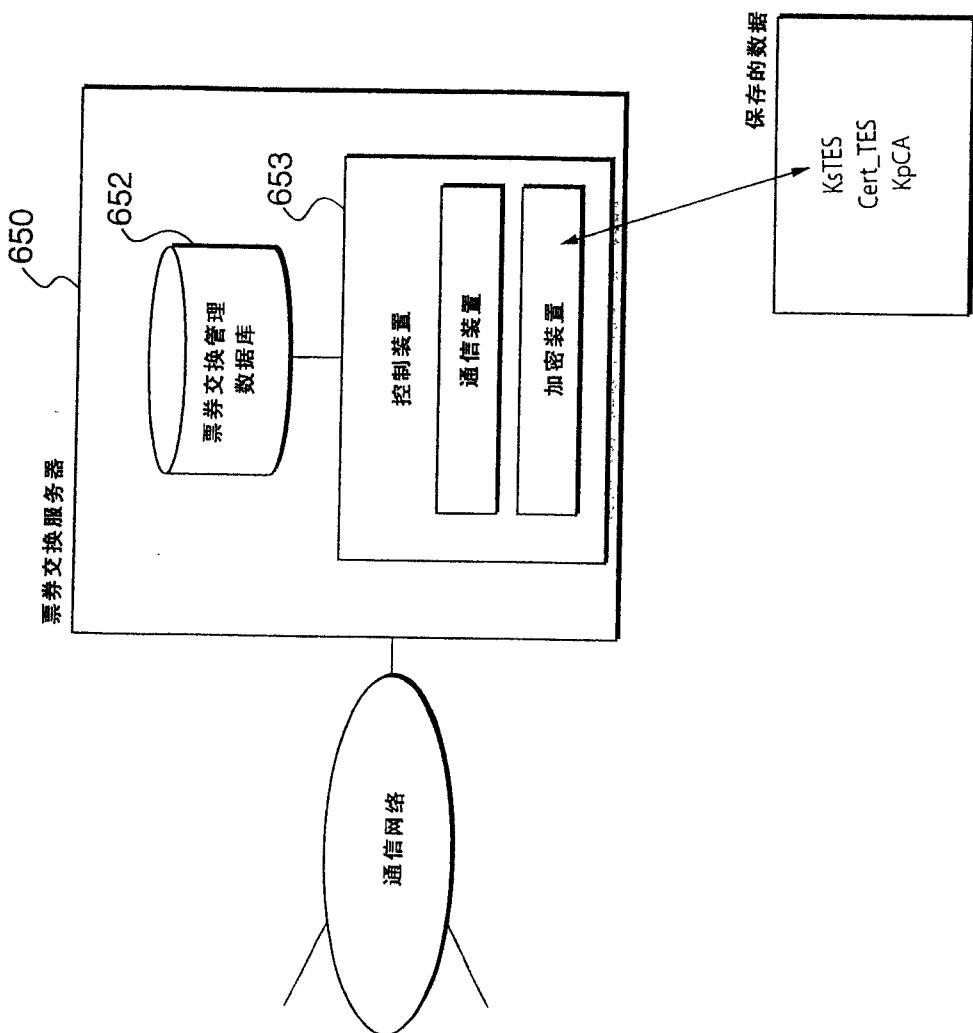
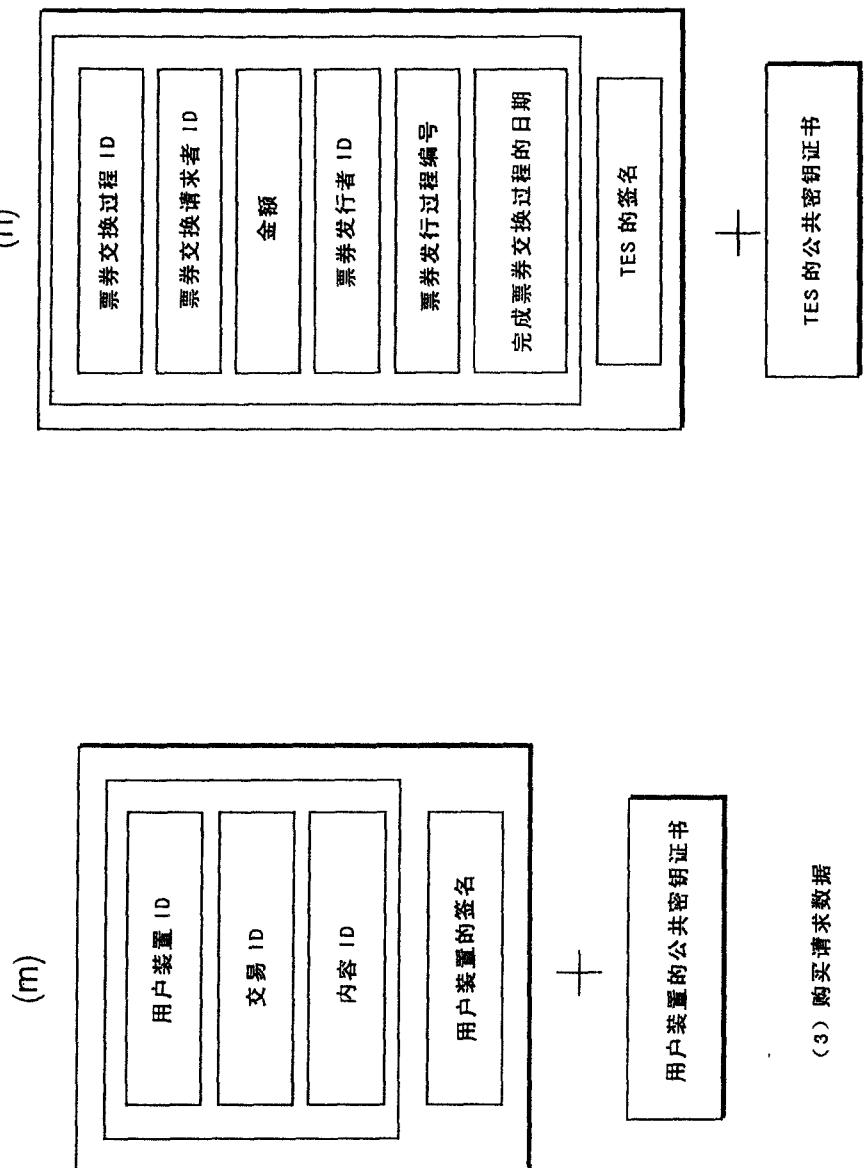


图 45

票券交换服务器 过程编号	交易请求者 ID	票券发行者 ID	票券发行过程编号	金额	装置 ID	交易 ID	状态
50001	12345	1234	10023	¥1000	1234567890	999888777	成功完成交换报告的传送
50002	23450	4455	10455	¥250	2345678901	6665554444	完成交换过程
50003	33201	2354	10254	¥800	3456788901	3216554444	成功完成电子票券的接收

票券发行服务器
的票券交换管理数据库

图 46



(3) 购买请求数据

(24), (29), (32) 交换报告

图 47

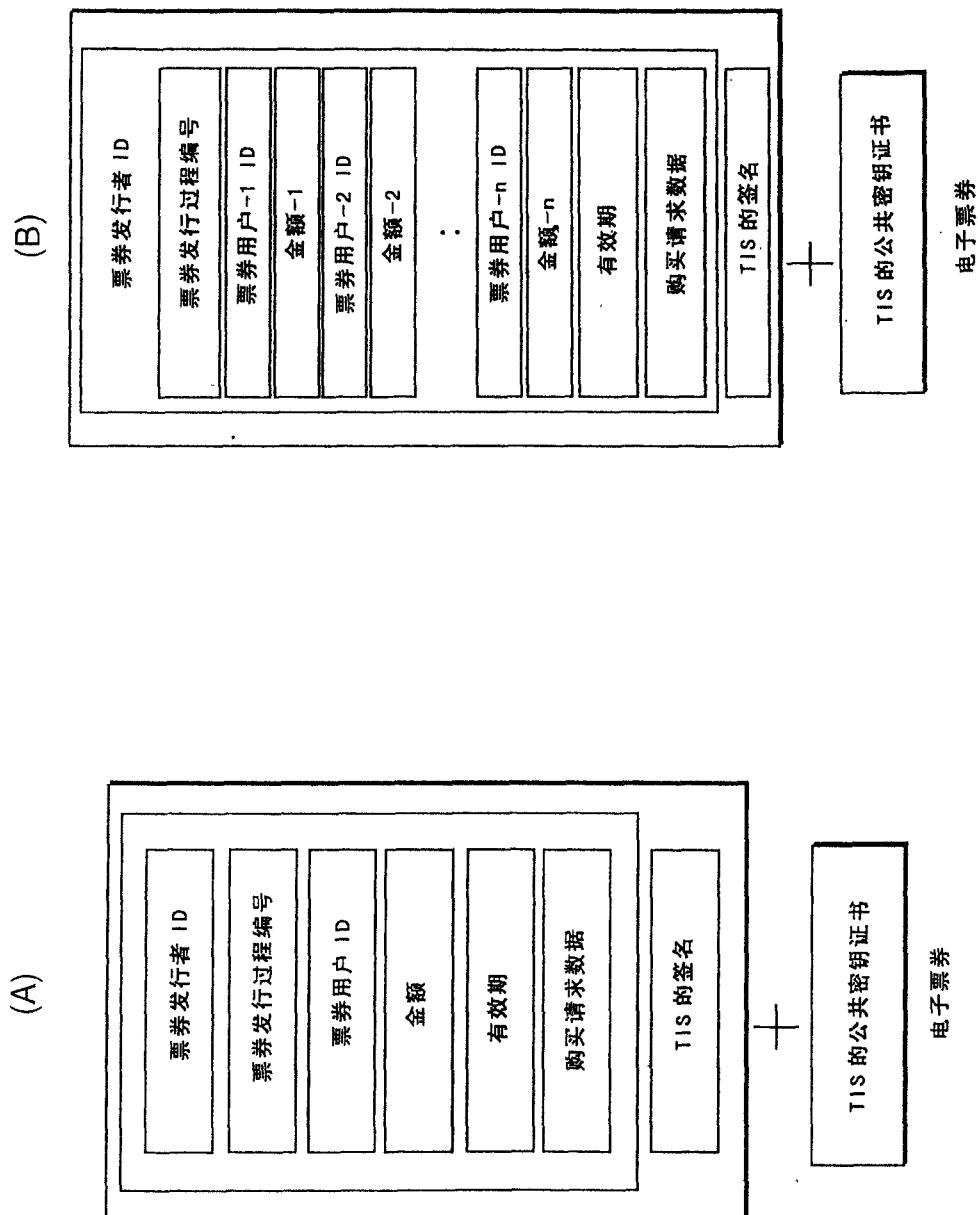


图 48

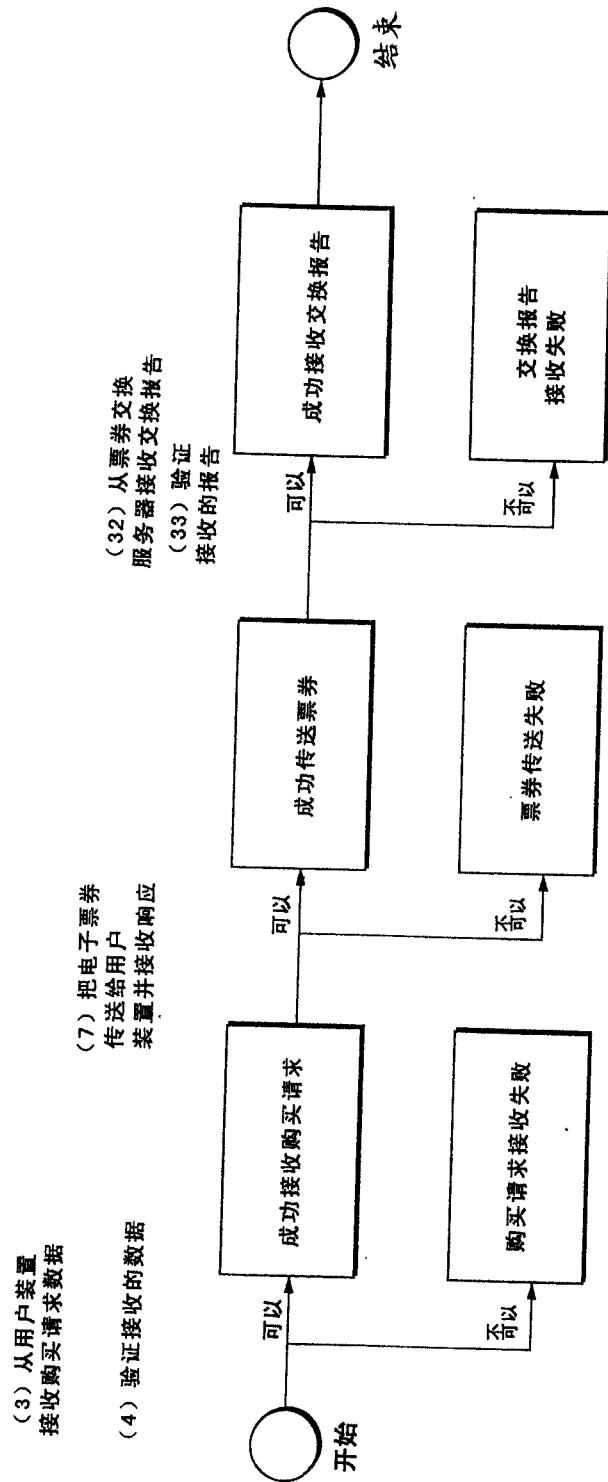


图 49

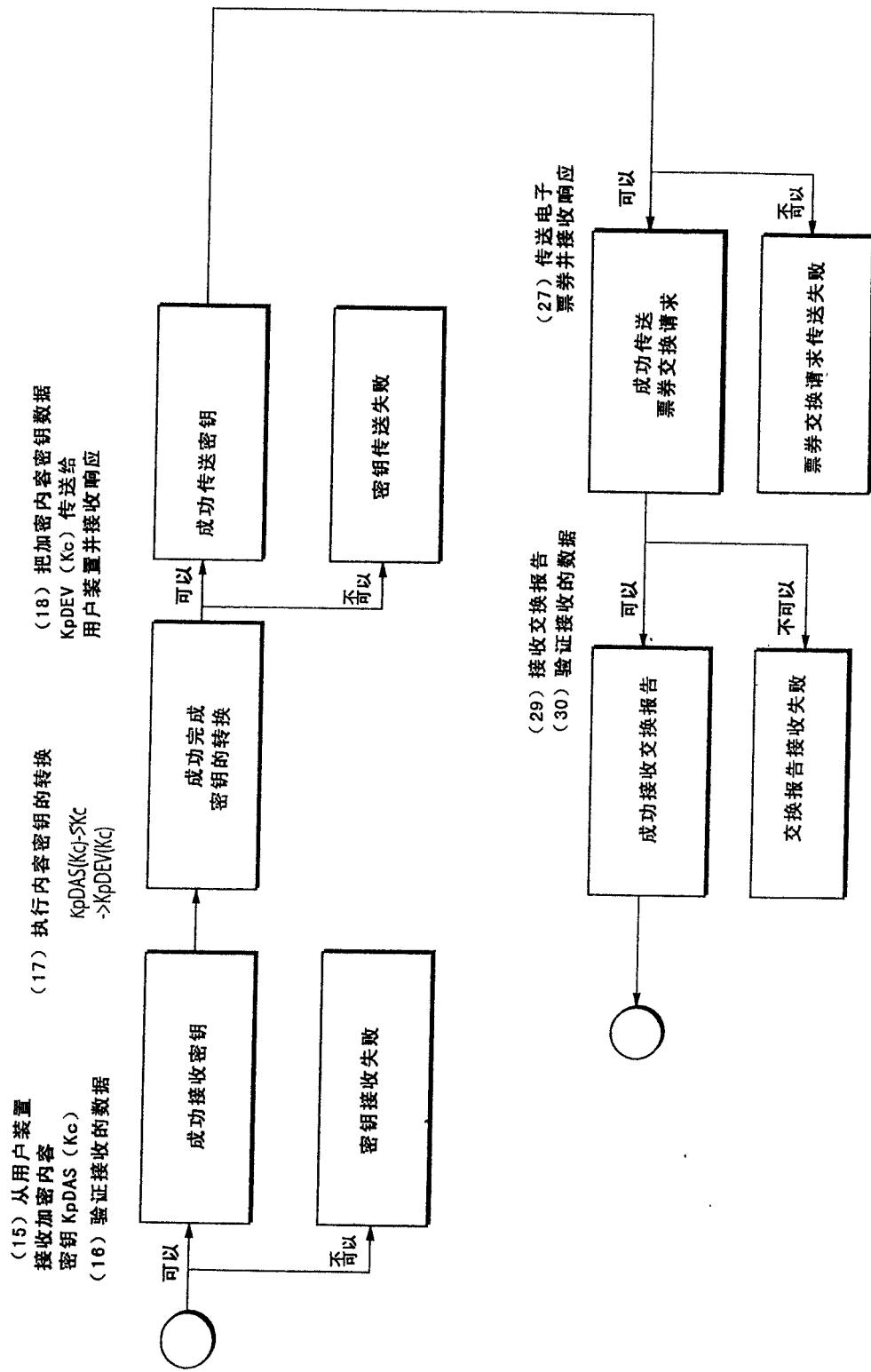


图 50

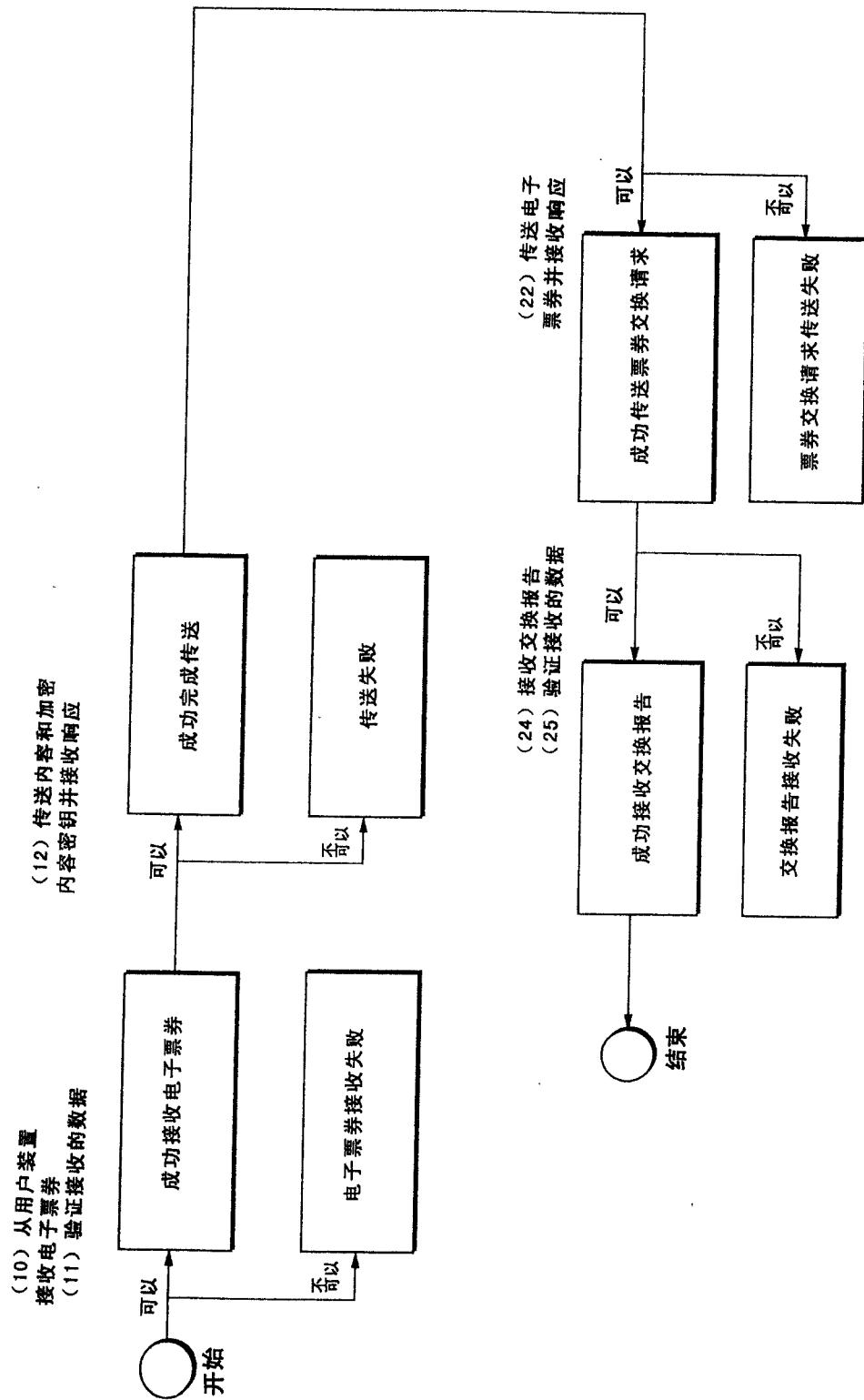


图 51

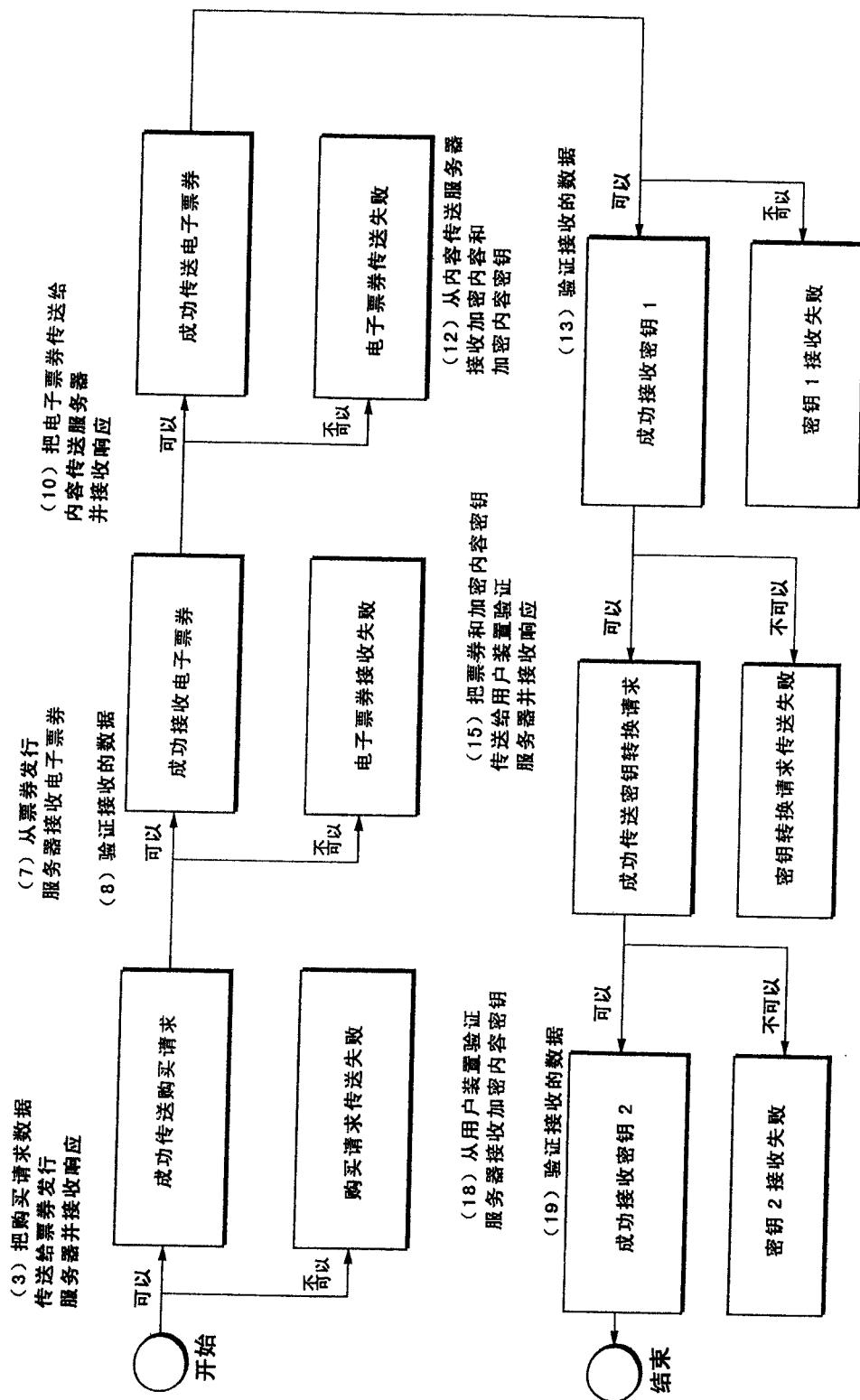


图 52

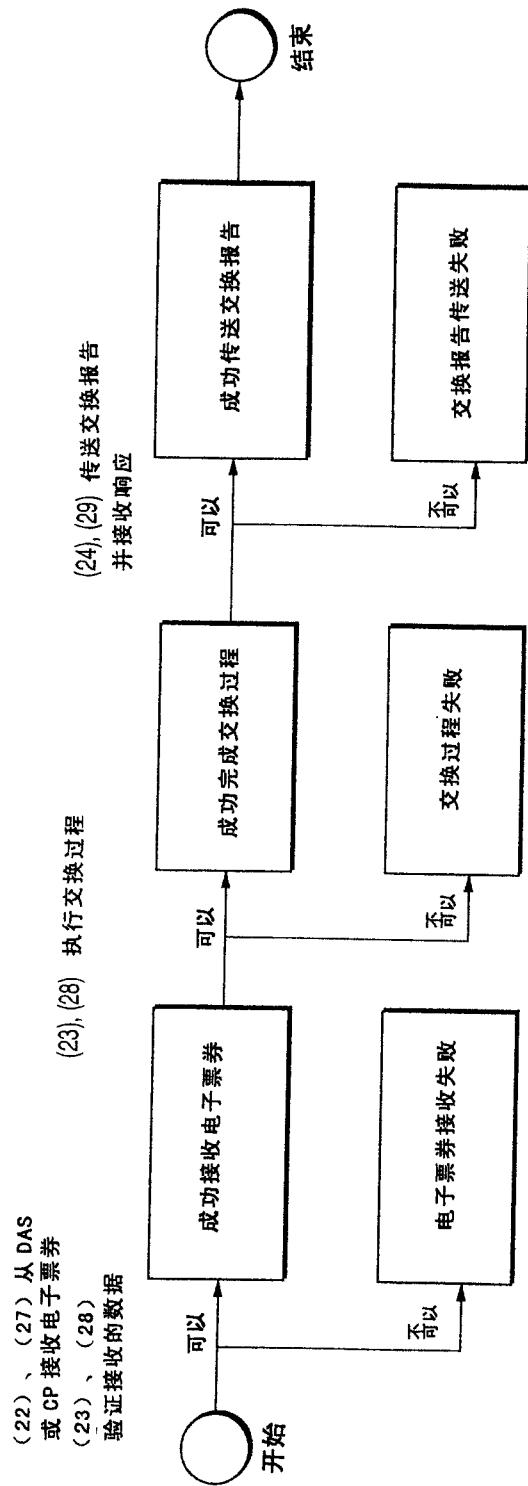


图 53

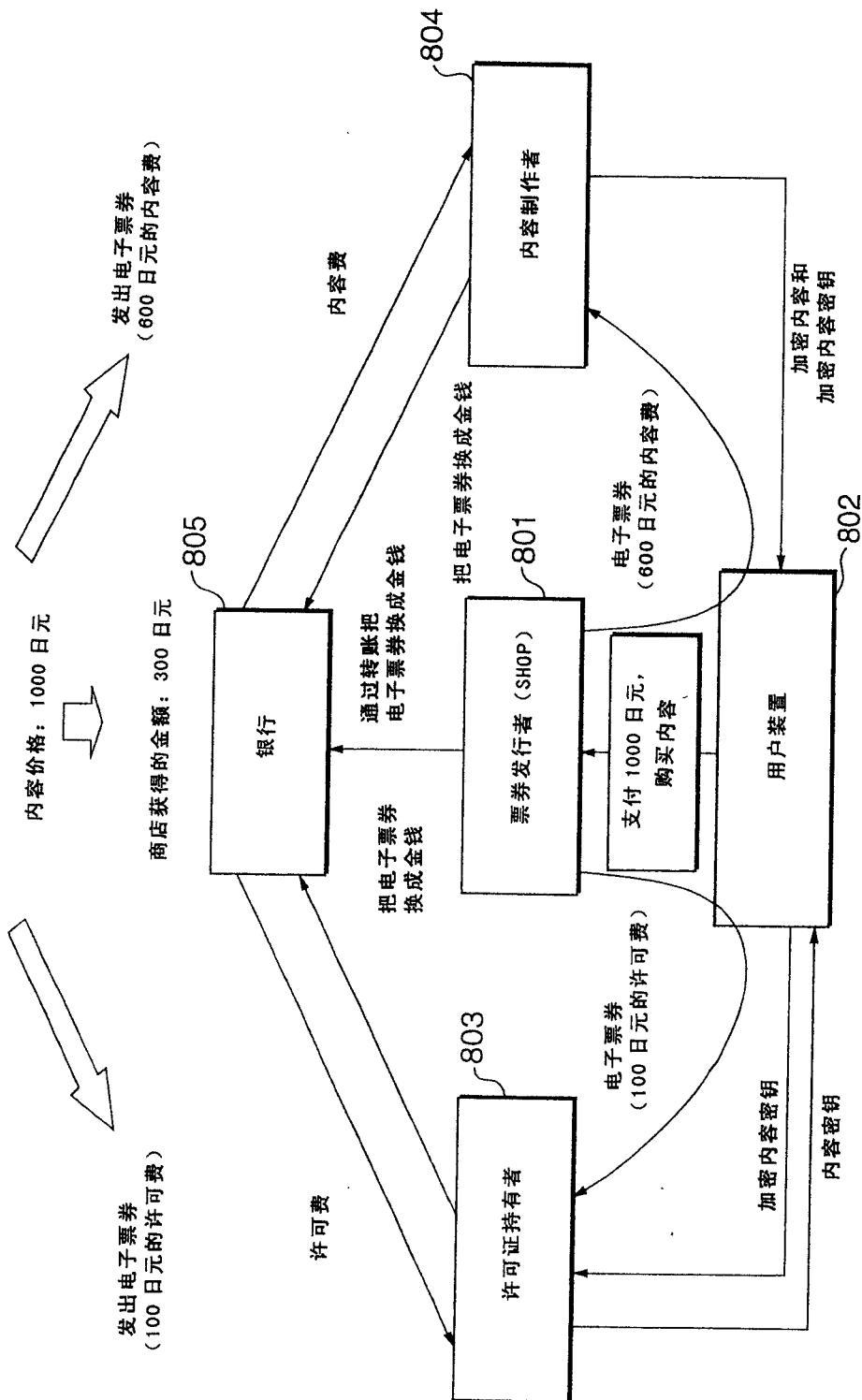


图 54

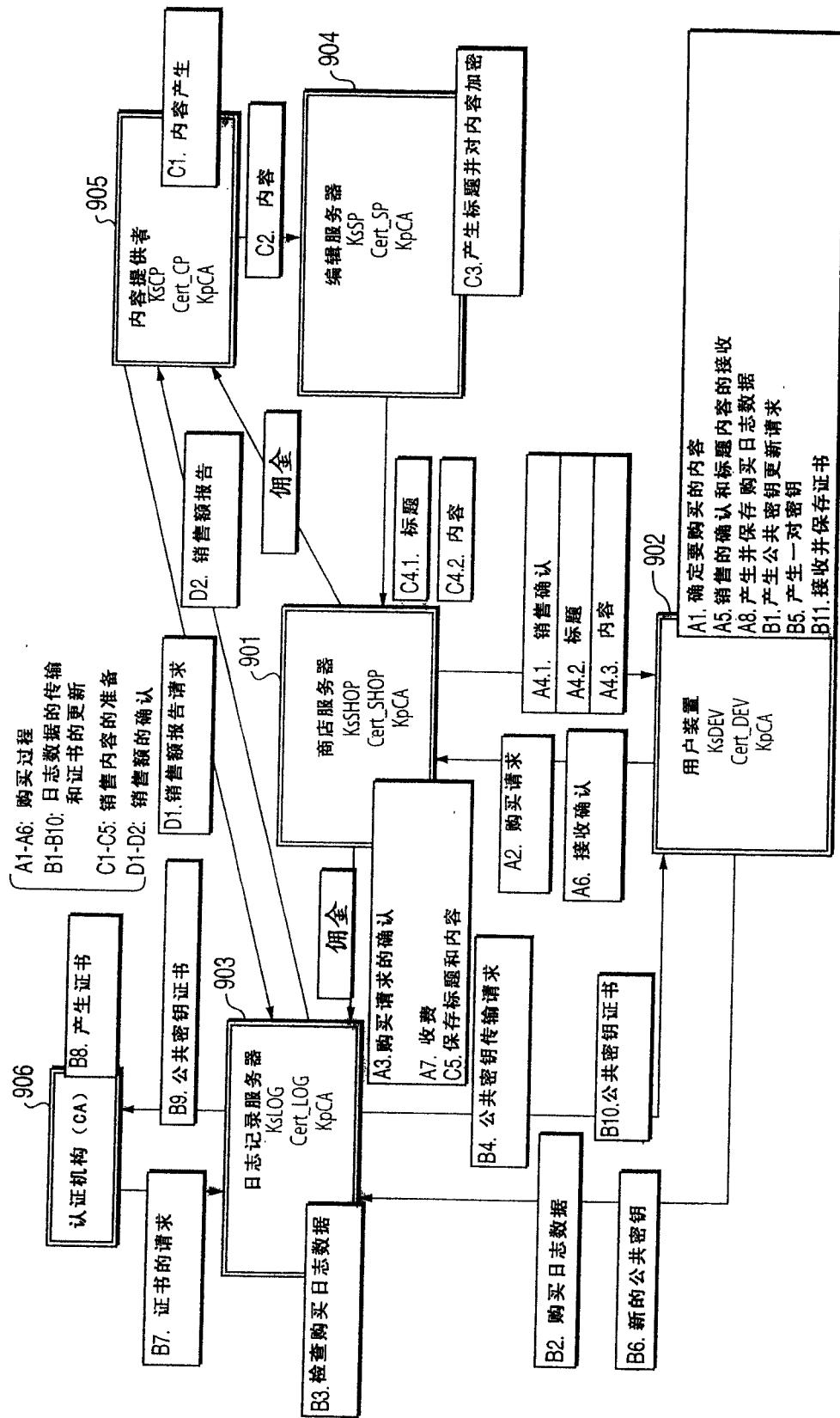


图 55

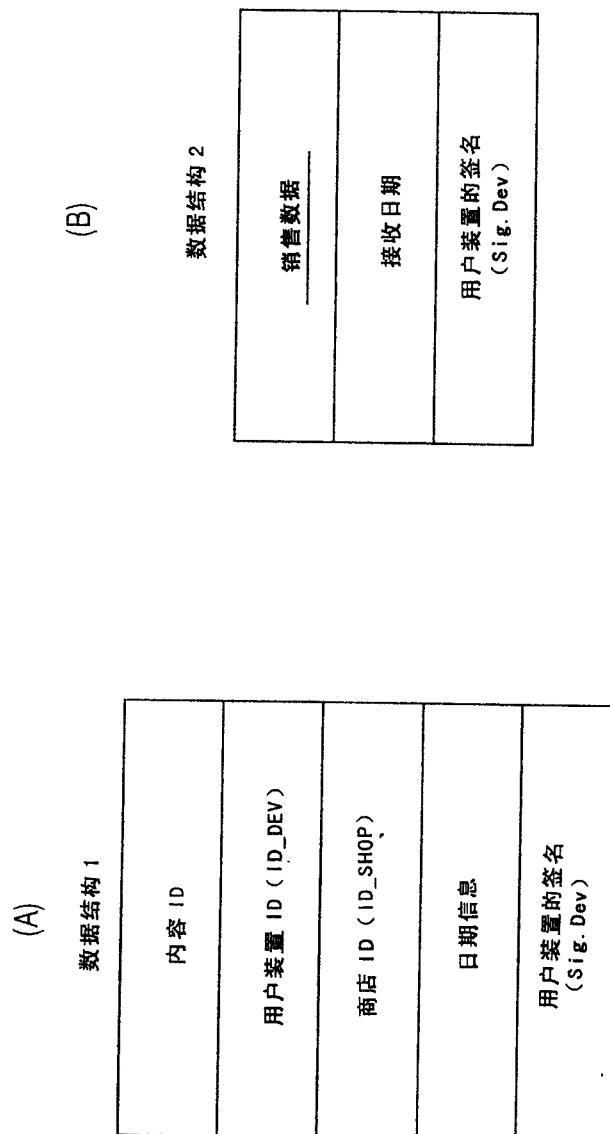


图 56

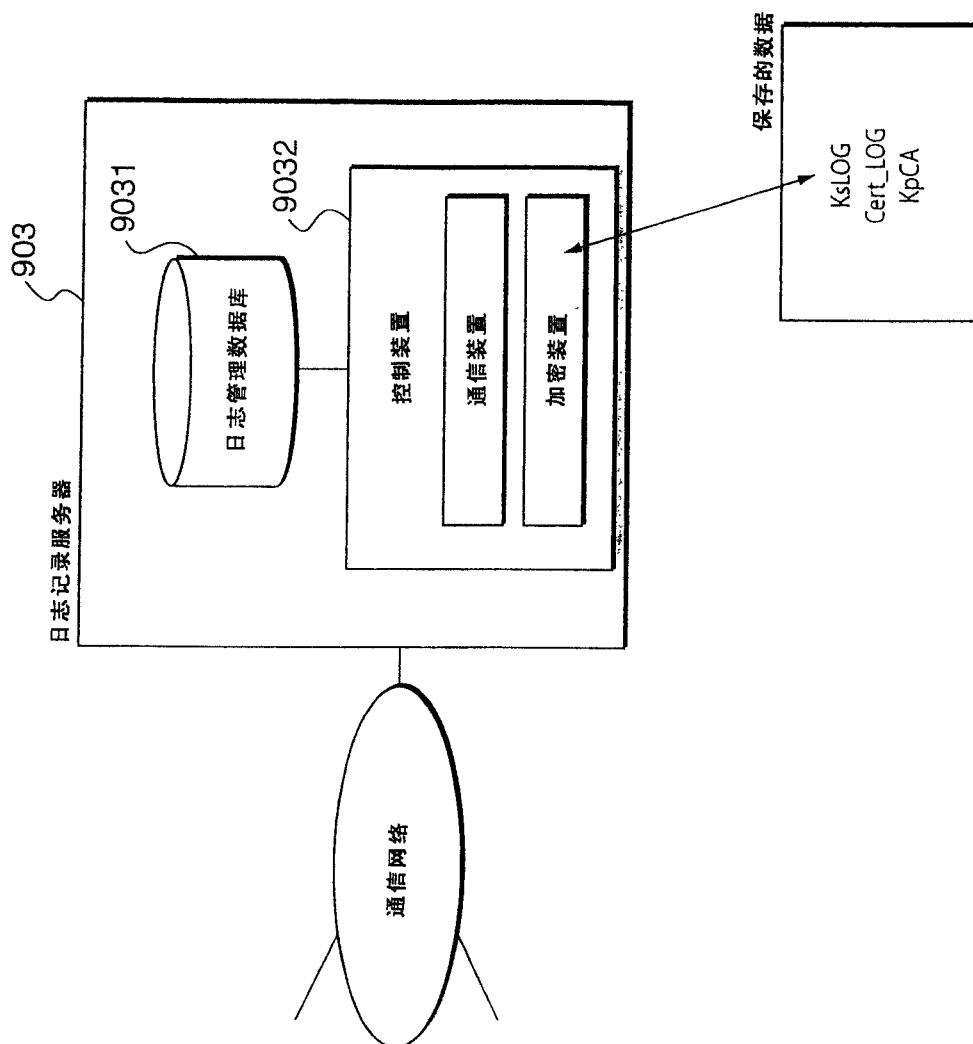


图 57

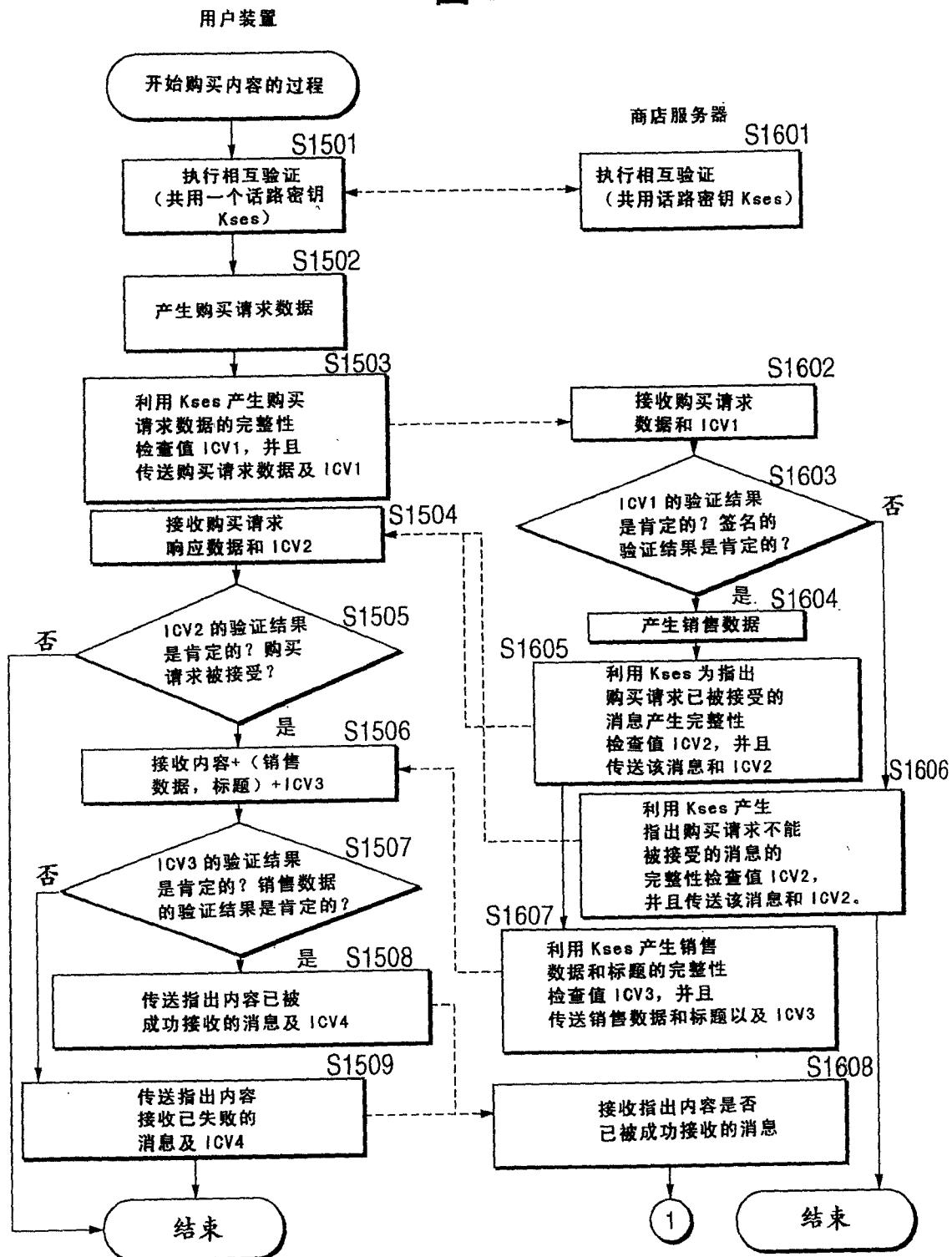


图 58

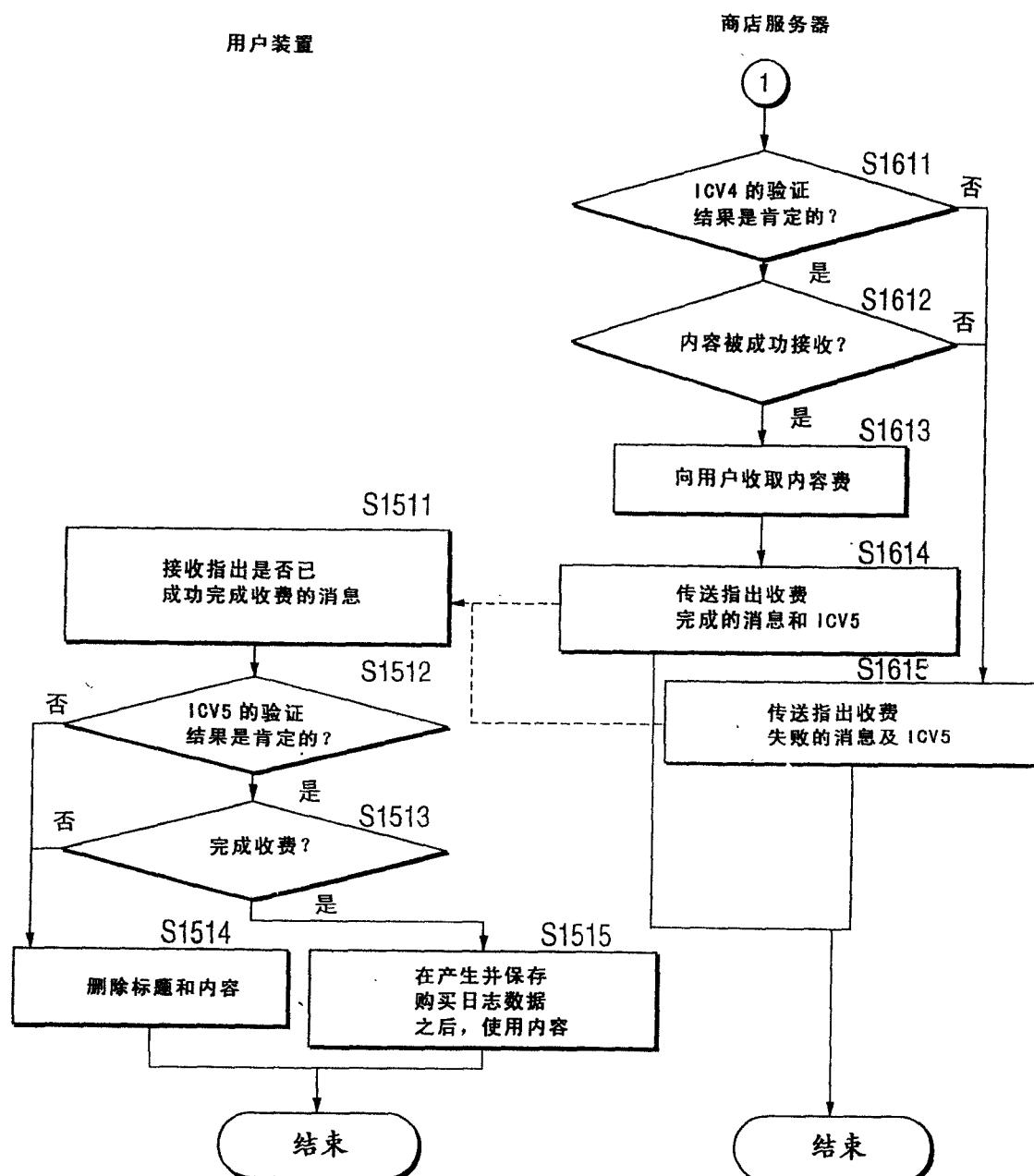


图 59

购买请求数据的格式	
(A)	交易 ID (TID_DEV)
	内容 ID
	用户装置 ID (ID_DEV)
	建议价格
	请求数据
	用户装置的签名 (Sig.Dev)
(B) 销售数据的格式	
	商店 ID (ID_SHOP).1
	销售数据
	要支付给系统持有者的佣金
	要支付给 CP 的金额
	购买请求数据
	商店的签名 (Sig.SHOP)

图 60

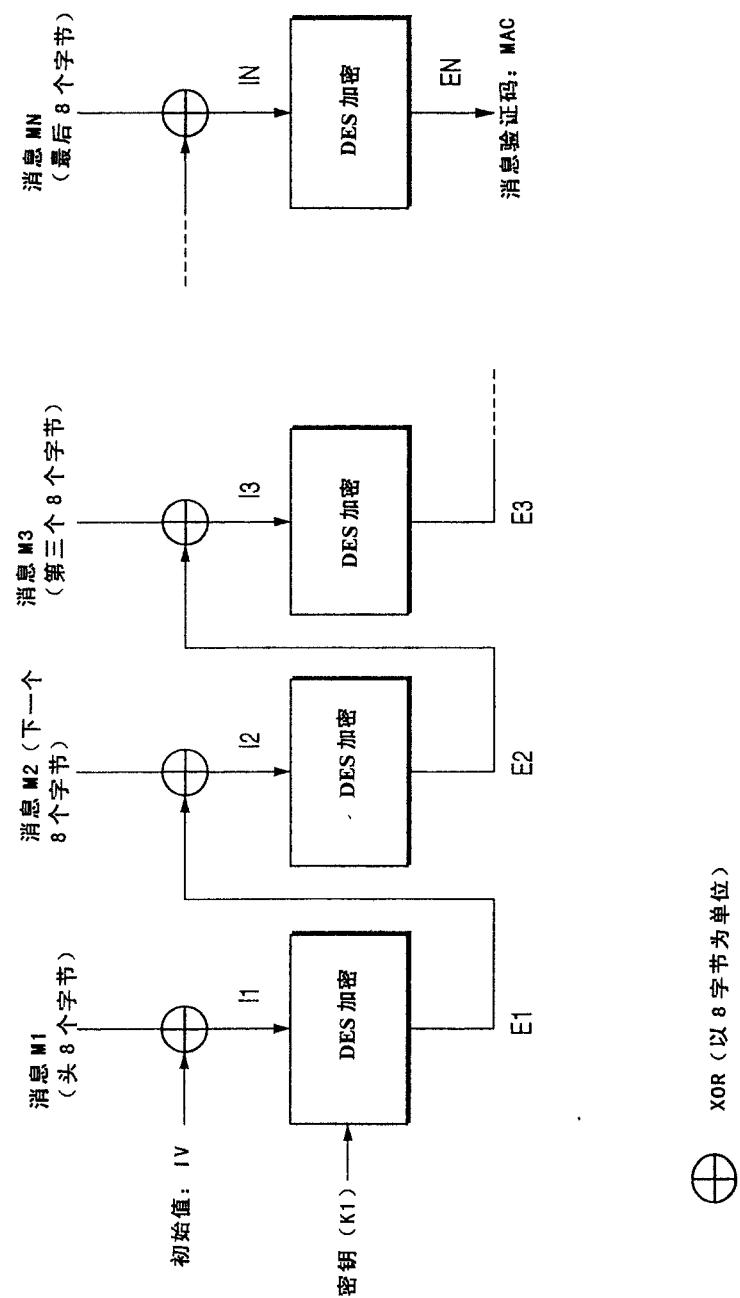


图 61

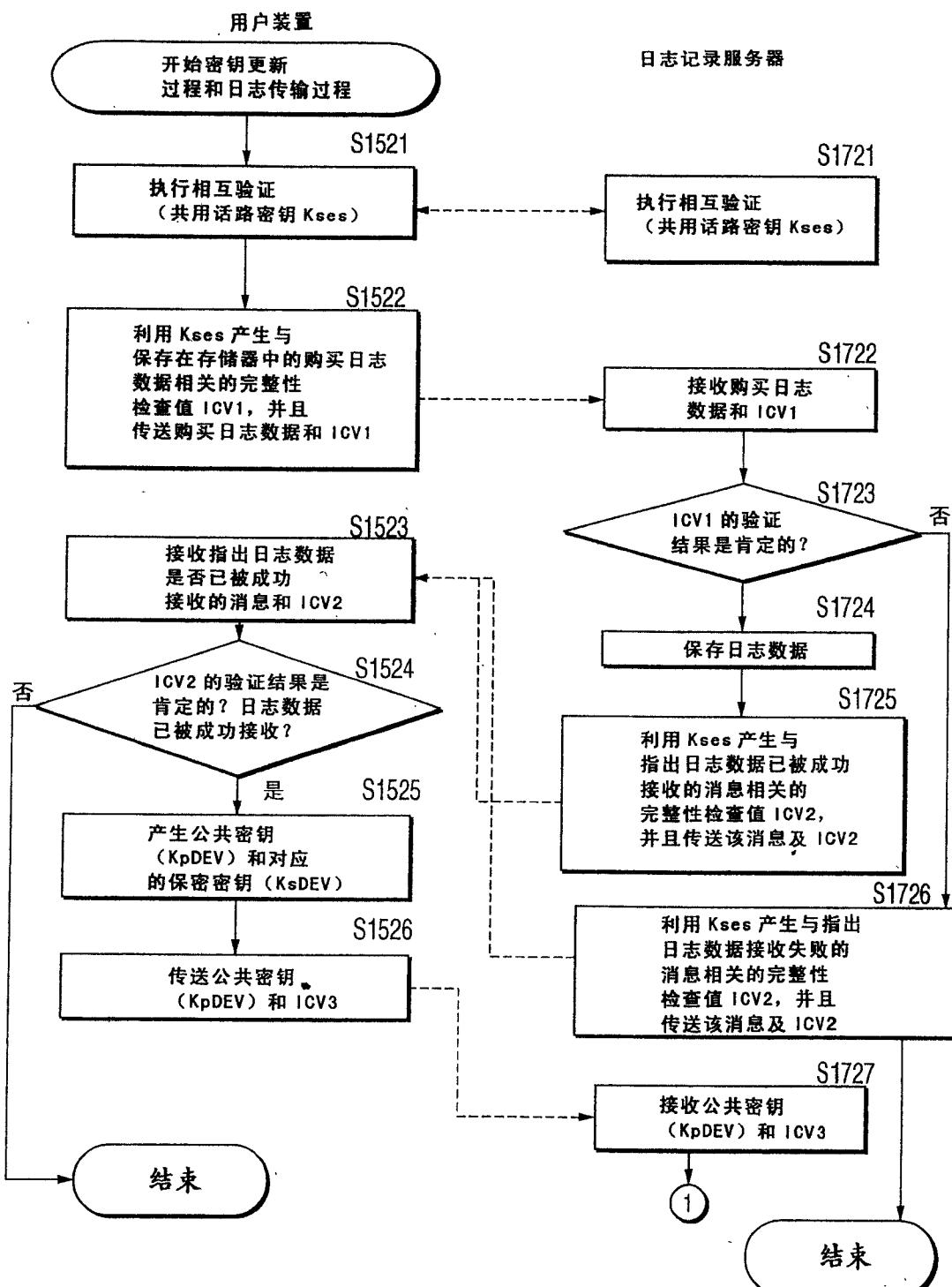


图 62

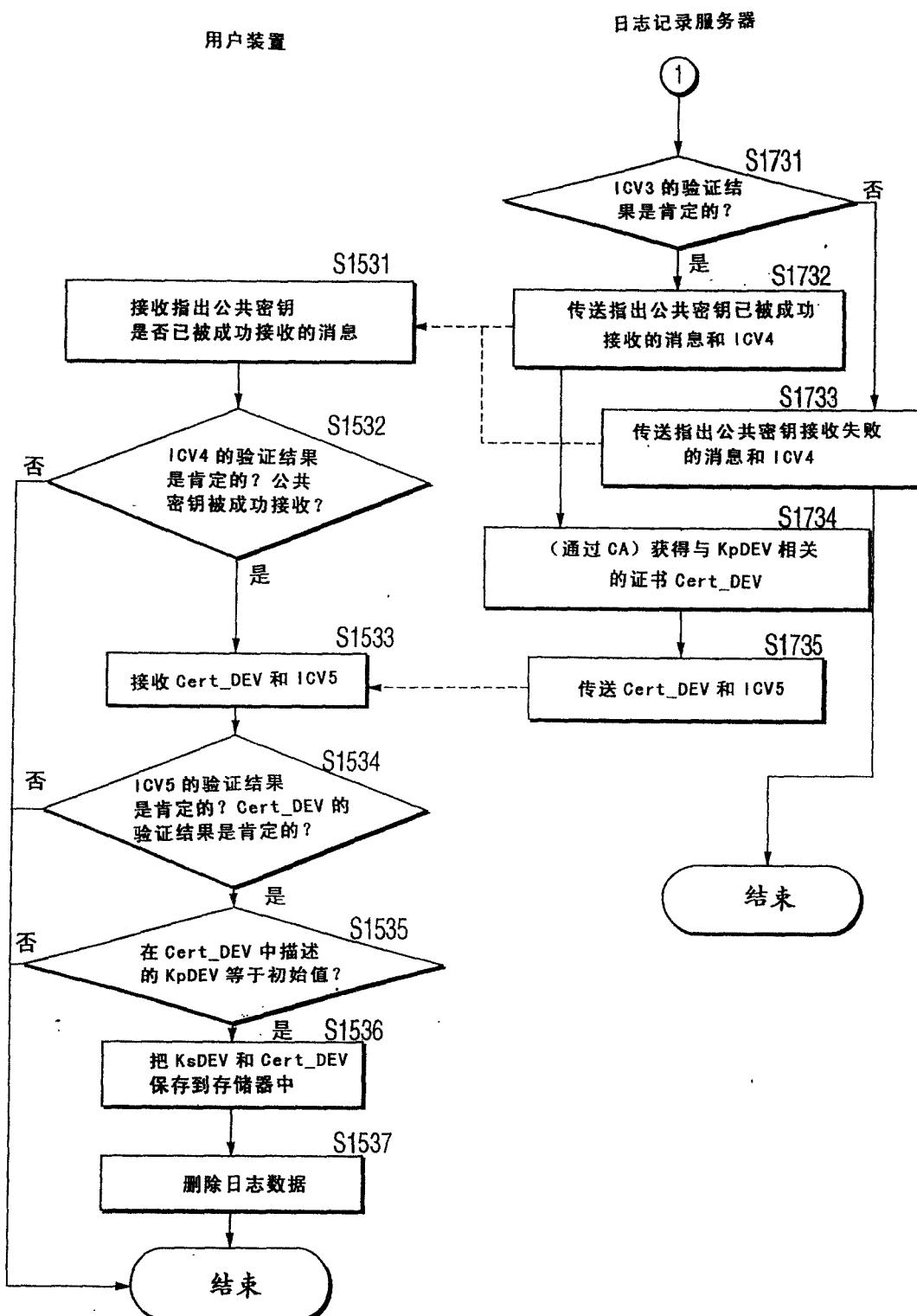


图 63

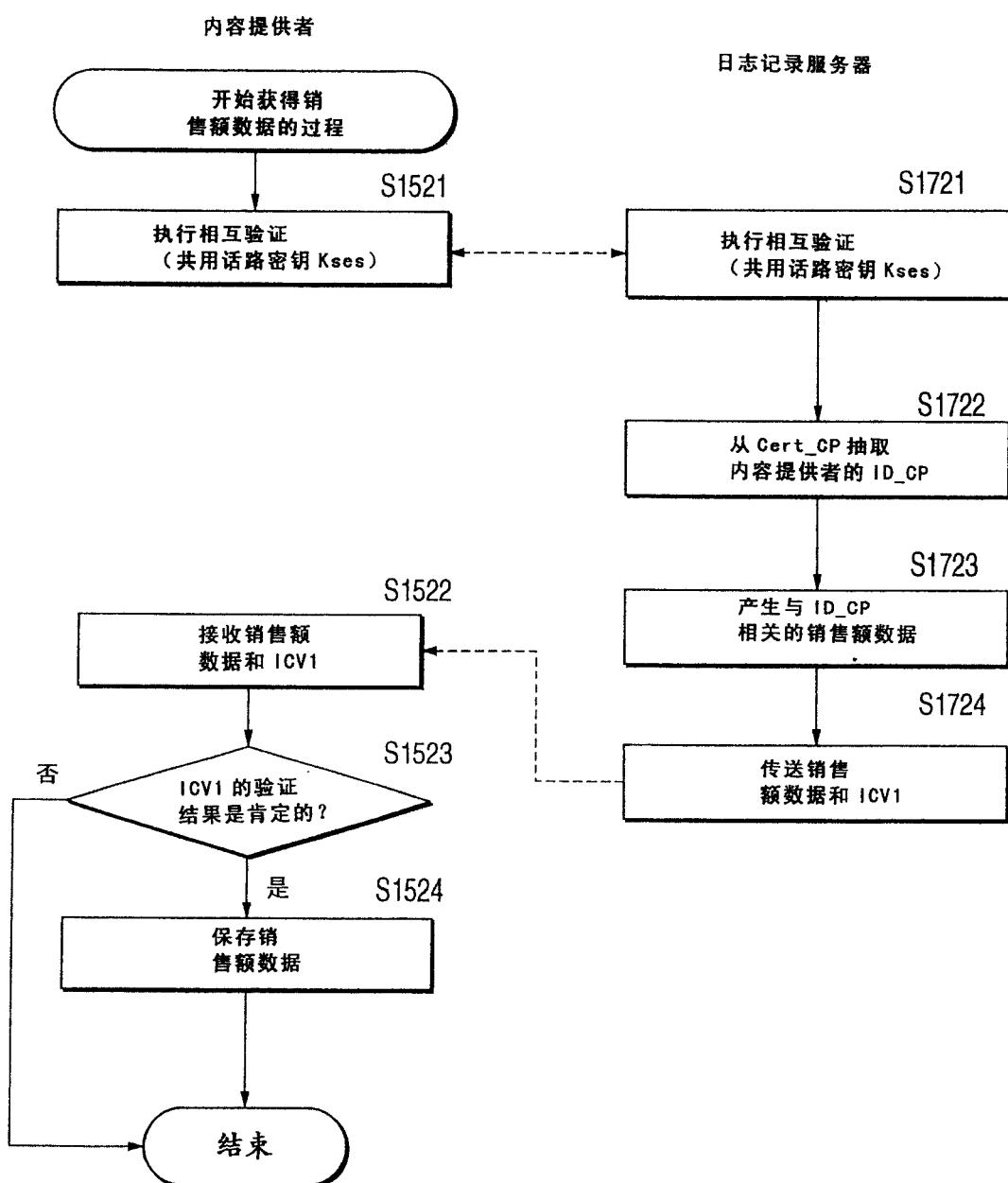


图 64

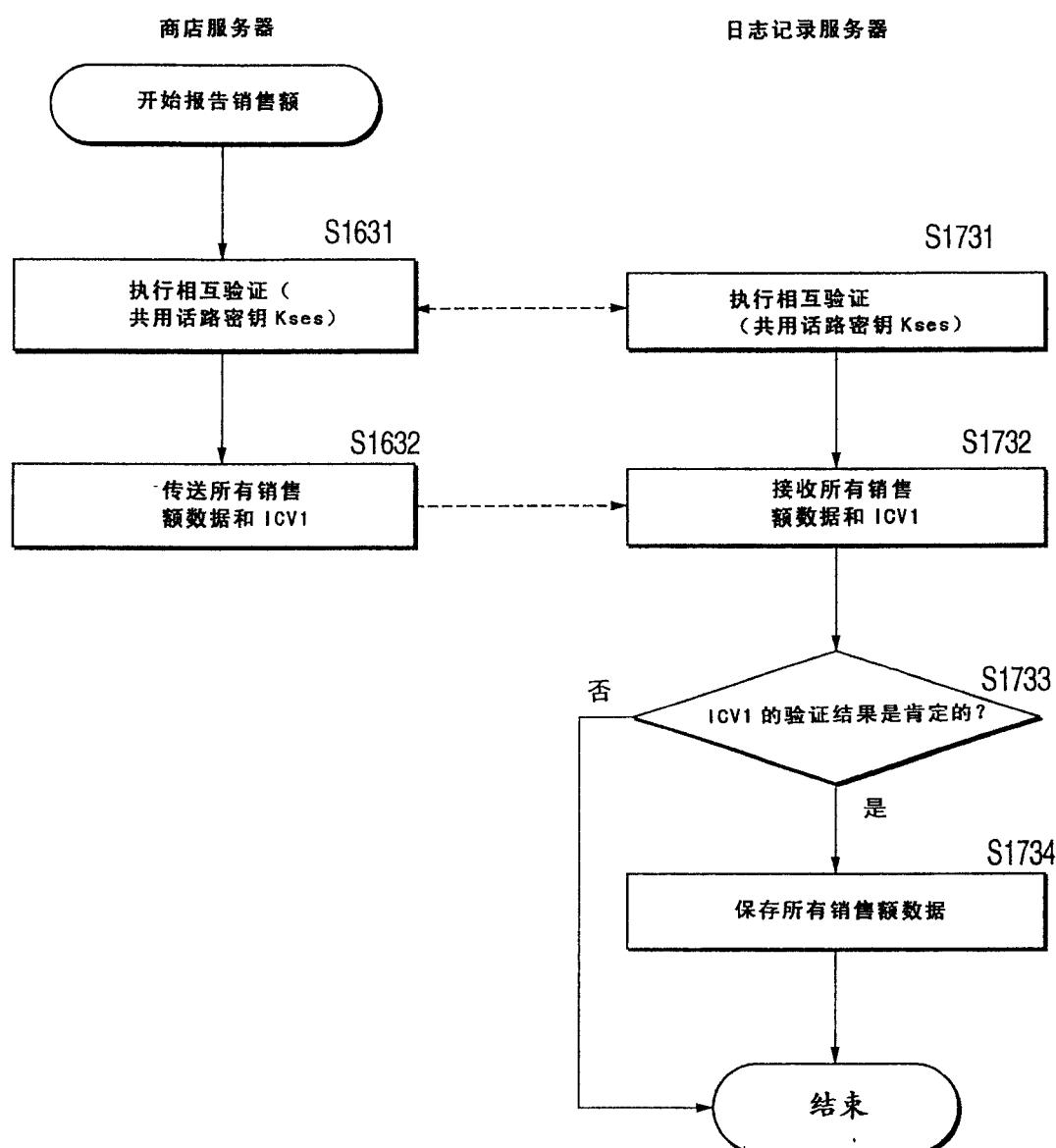


图 65

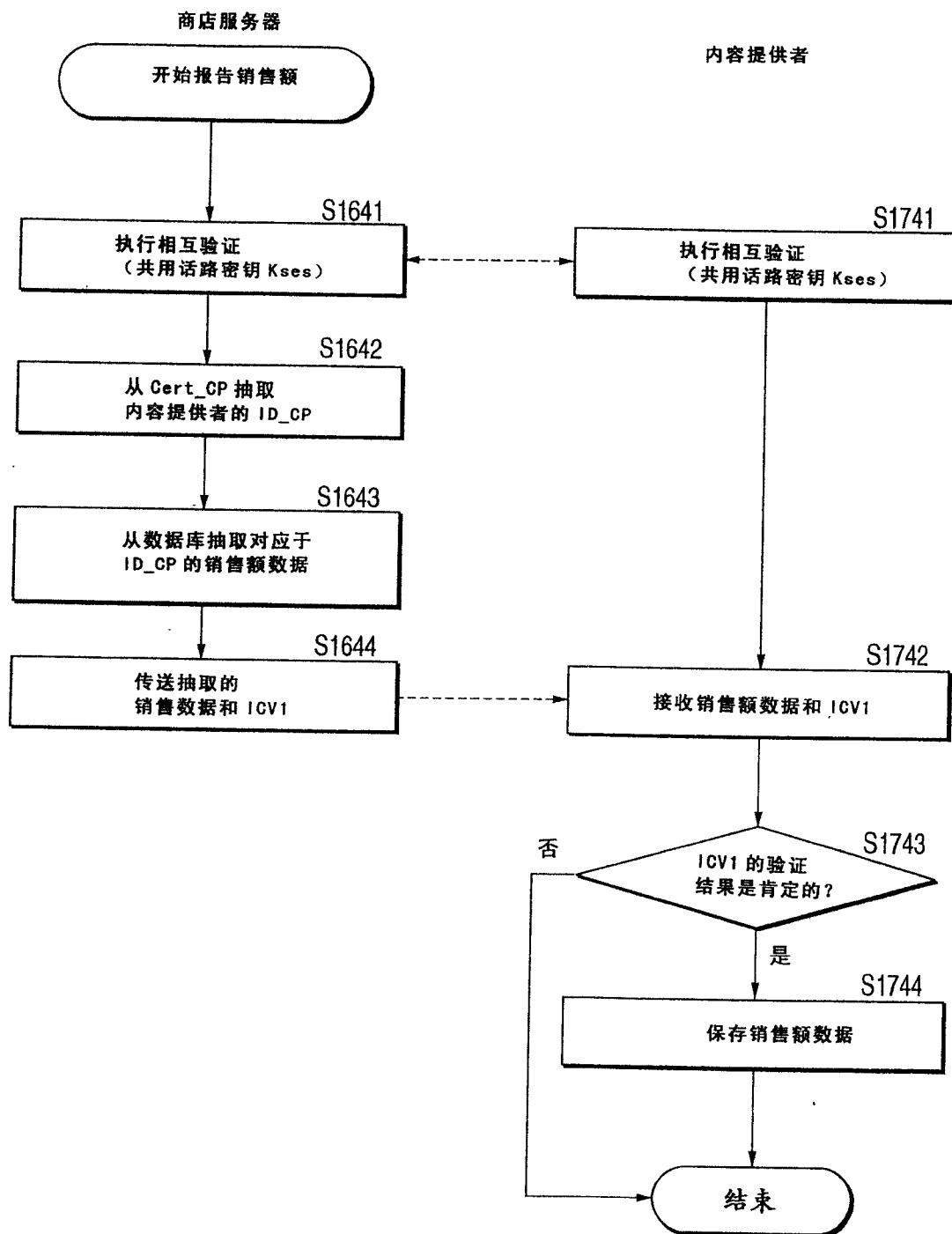


图 66

属性代码 (2字节)	实体	功能
0000	注册机构 (RA)	检查是否应发出公钥证书或者属性证书
0001	系统持有者 (SH)	收取在系统中散布的内容的许可费，更具体地说执行包括用于对内容解密的密钥的转换和日志数据的采集的过程
0002	内容销售者 (SHOP)	向用户提供关于内容的信息并且收取内容费
0003	内容传送服务器	响应来自内容销售者的请求向用户传送内容
0004	用户装置	购买并使用内容

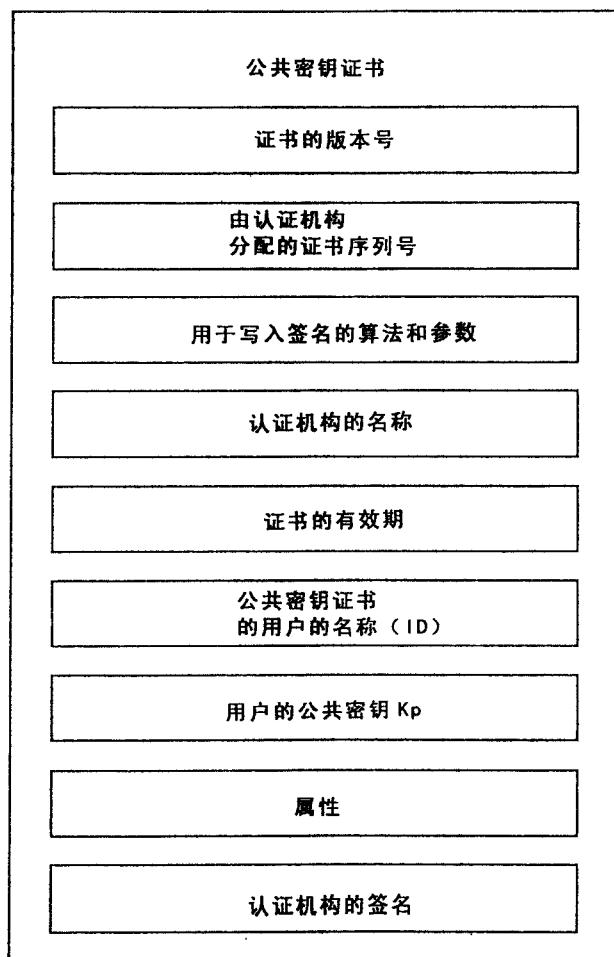
图 67

图 68

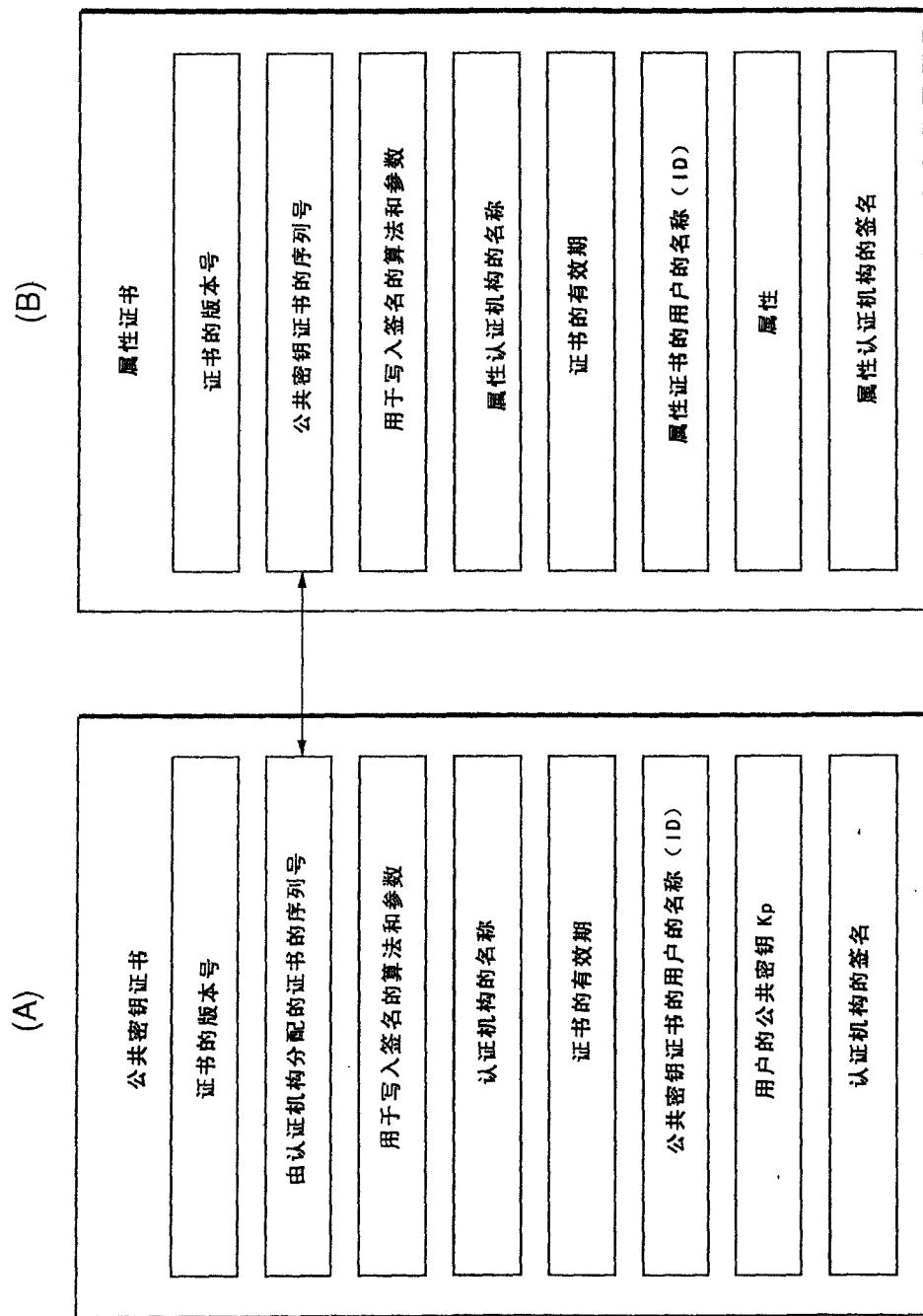


图 69

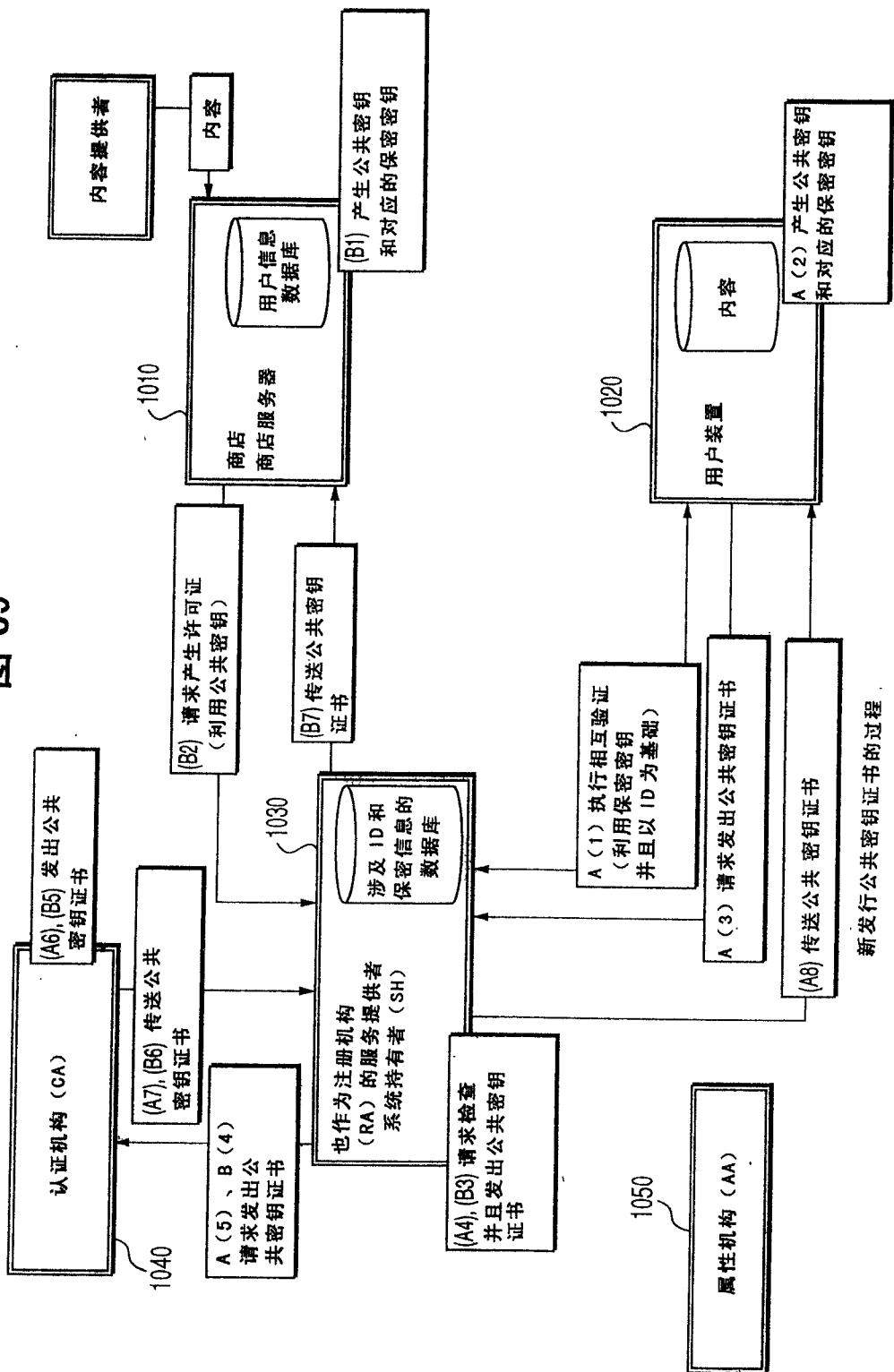


图 70

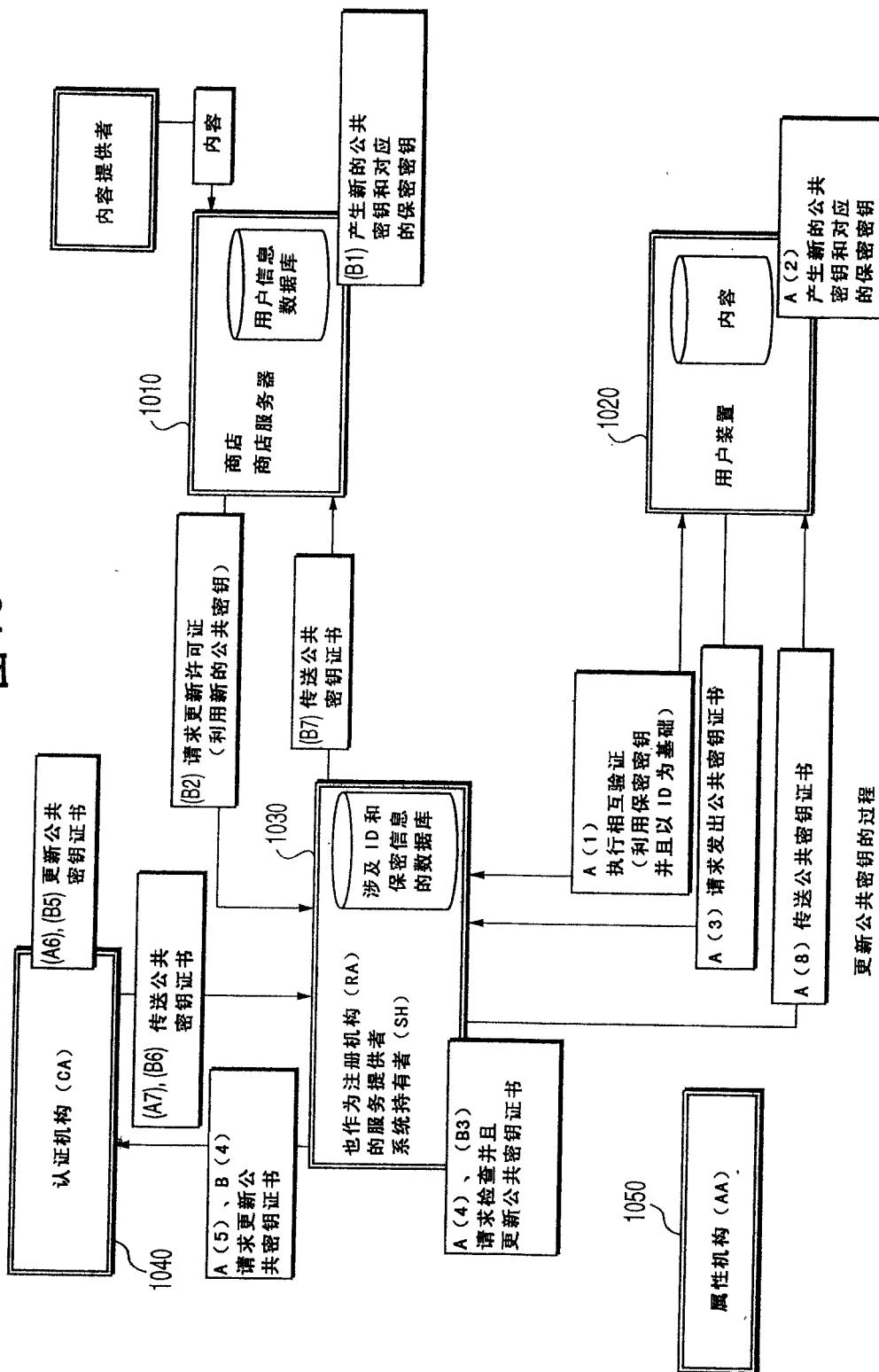


图 71

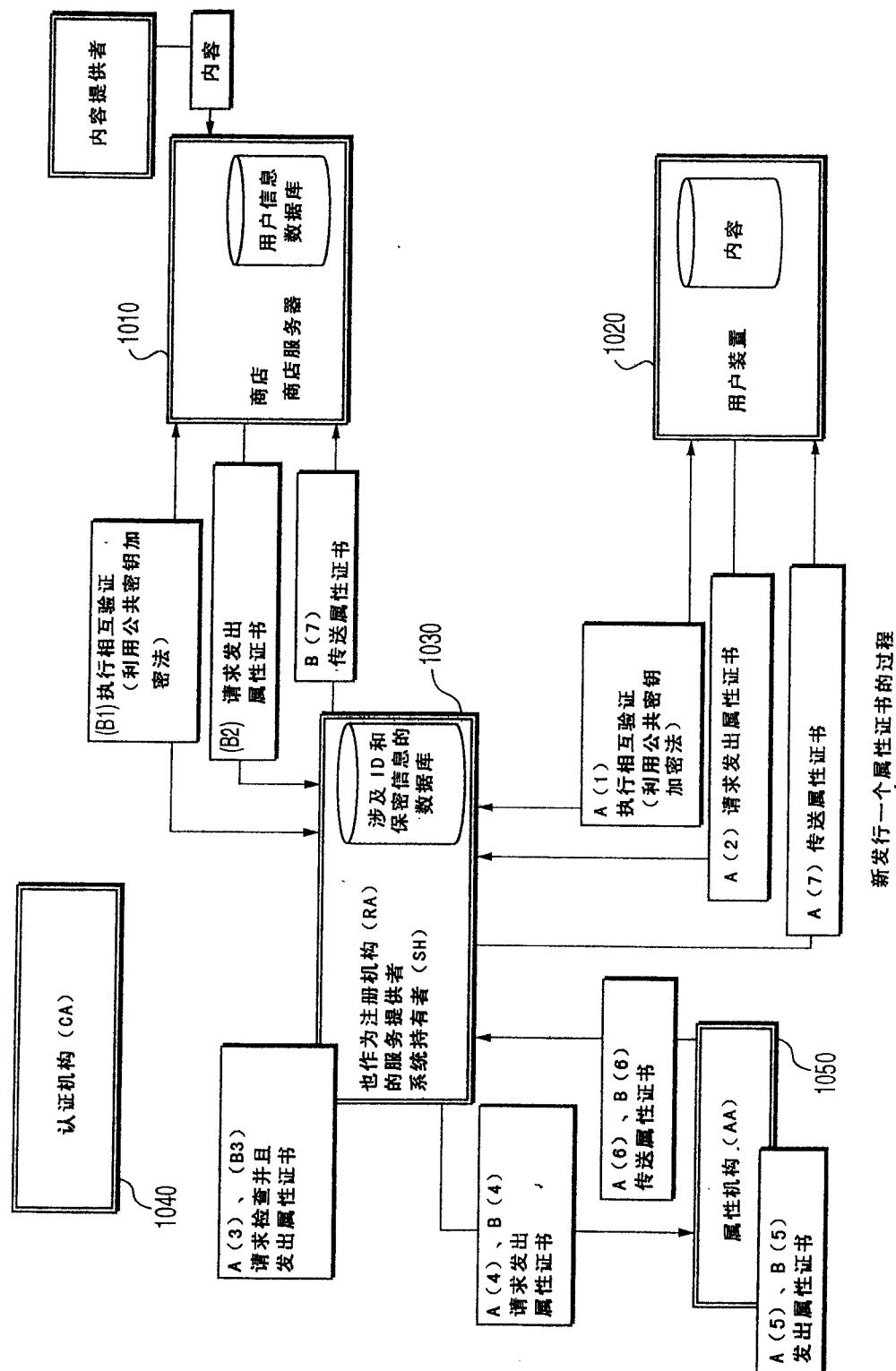


图 72

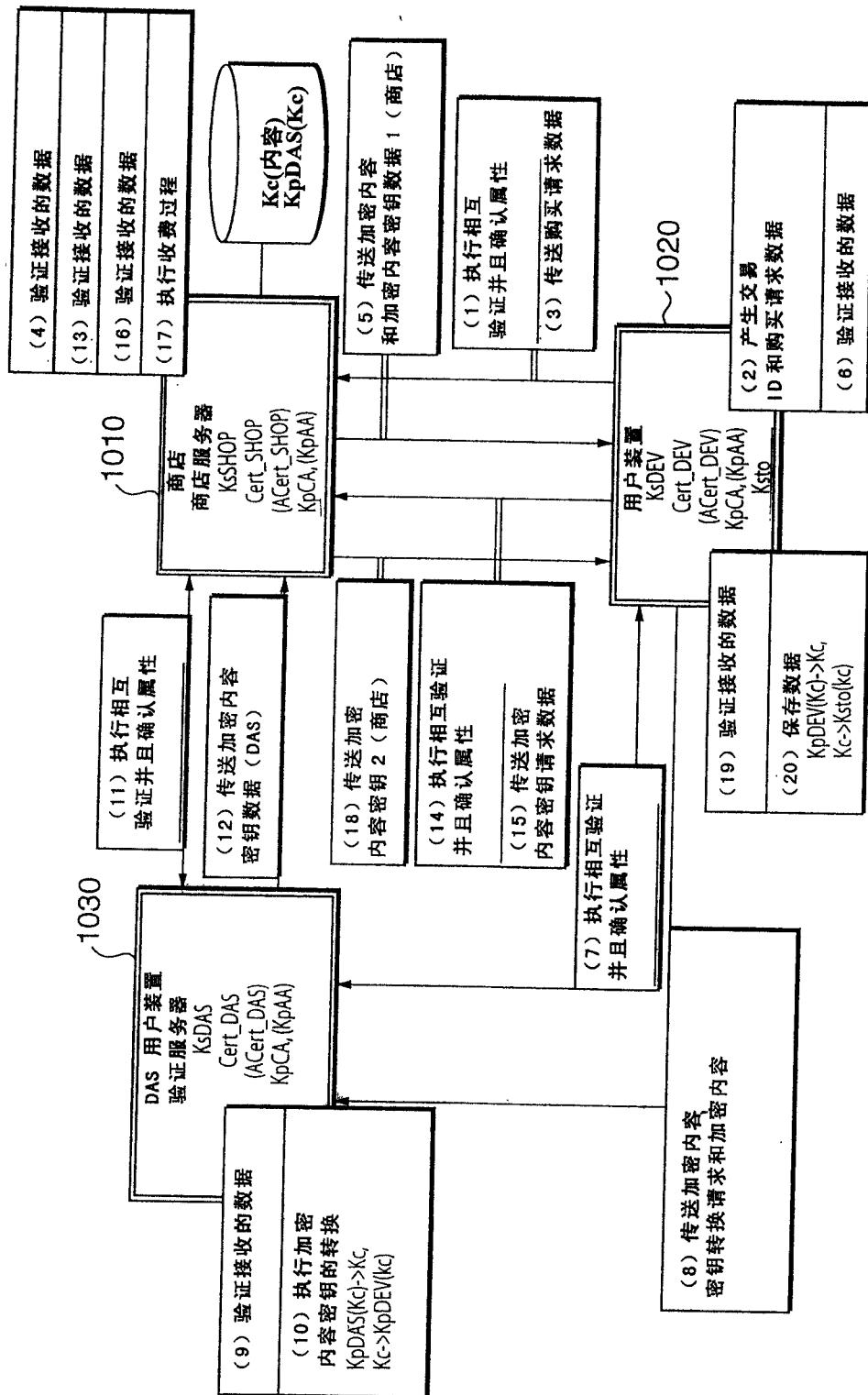


图 73

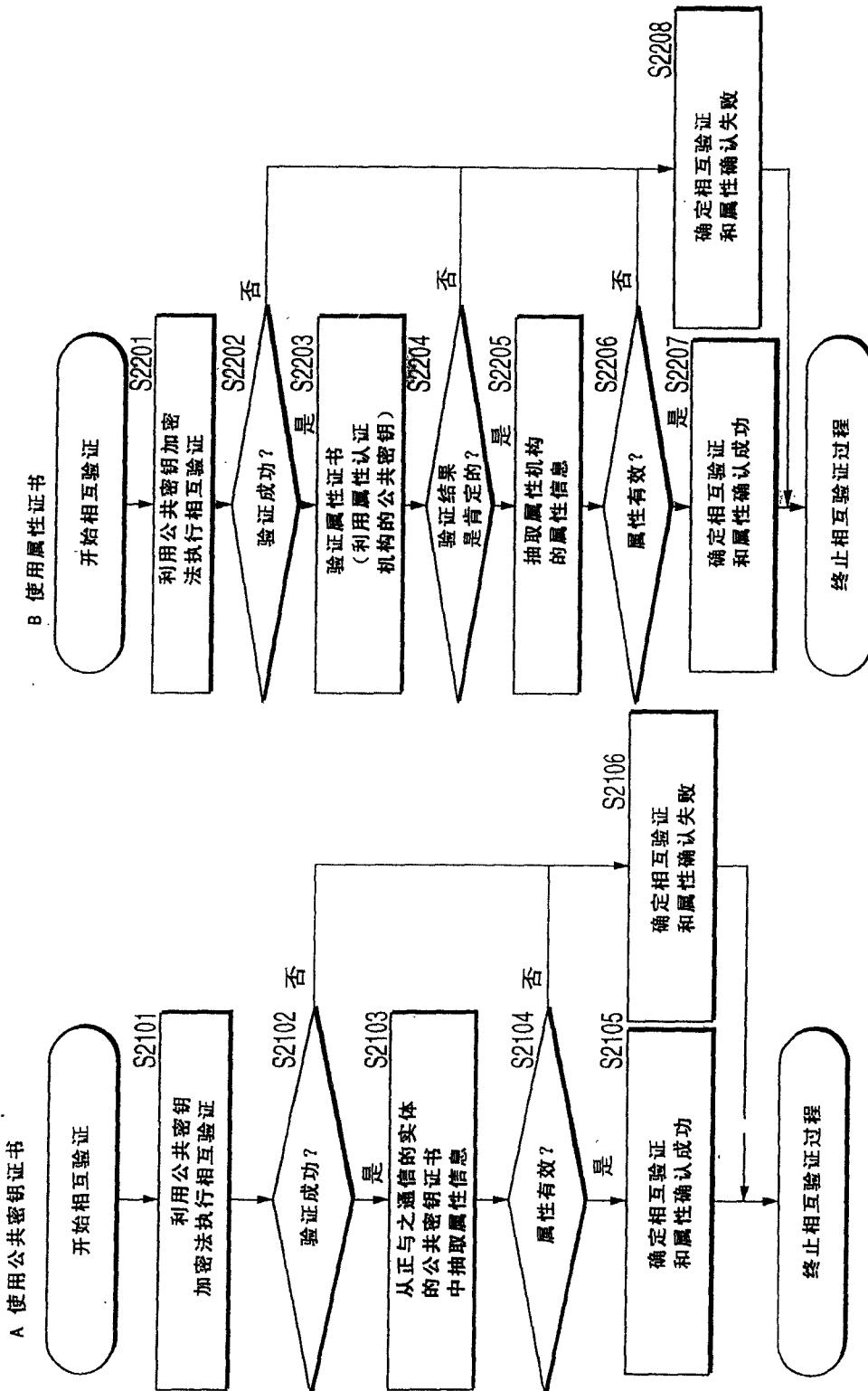


图 74

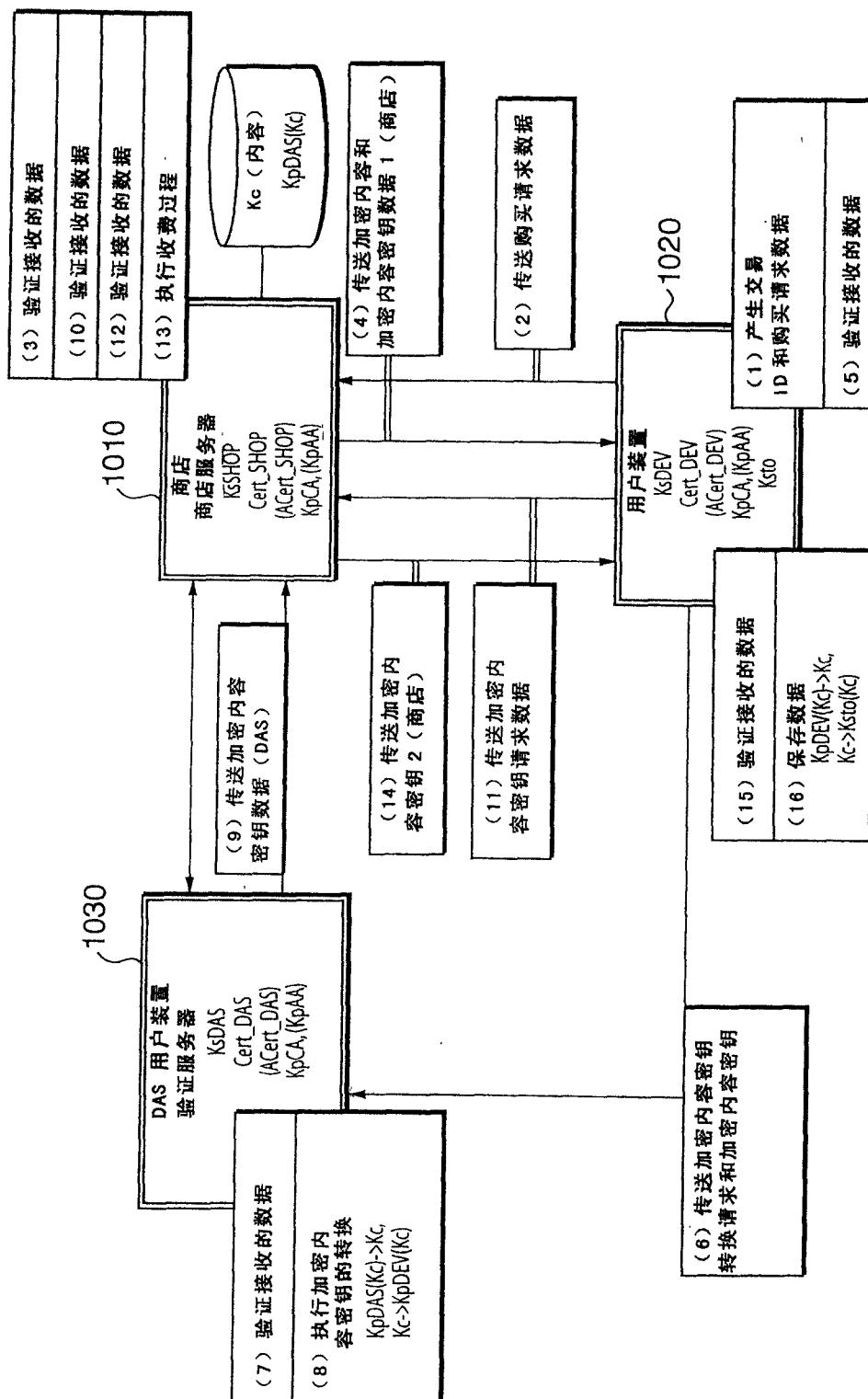


图 75

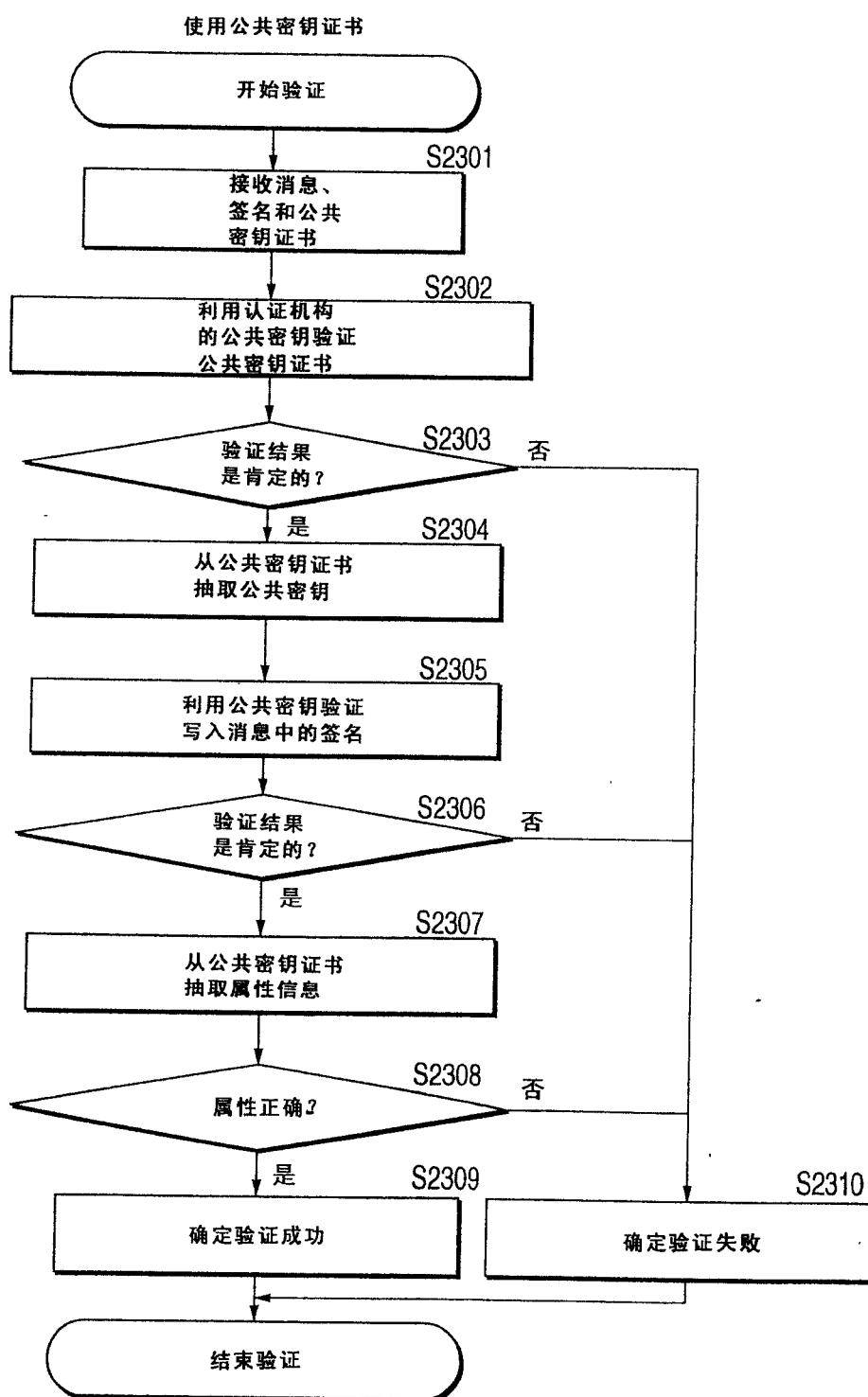


图 76

