[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 19/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 02129771.1

[45] 授权公告日 2008 年 10 月 29 日

[11] 授权公告号 CN 100429666C

[22] 申请日 1998.12.4 [21] 申请号 02129771.1
分案原申请号 98122775.9
[30] 优先权
[32] 1997.12.5 [33] JP [31] 352243/1997
[73] 专利权人 株式会社日立制作所
地址 日本东京
[72] 发明人 广田纯子 武内敏 山部浩一
[56] 参考文献
CN1220430A 1999.6.23
审查员 高琛颢

[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 吴丽丽

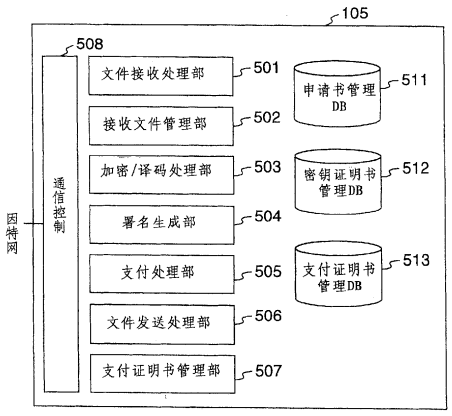
权利要求书 1 页 说明书 22 页 附图 15 页

[54] 发明名称

文件发送系统及方法

[57] 摘要

支付接收服务器根据来自于申请人装置的用费支付委托，对金融机关服务器进行申请人的支付信用查询。 在判断申请人的支付有保证时，支付接收服务器即给申请人装置发送电子支付证明书。 附有支付证明书的文件从申请人装置或其代理人装置经通信网络发送给文件接收服务器。 文件接收服务器在接收文件本身之前，从发送文件的装置接收对此文件施加单向函数所得的压缩数据，并把这一接收时刻作为接收此文件的日期与时刻。



1.一种文件接收系统，其特征在于，此系统包括

通信网络，

与此通信网络连接来发送文件的装置，及

与此通信网络连接并经由此通信网络接收前述文件且包含有存储装置的文件接收服务器，

所述文件发送装置将对所述文件施加单向函数后所得的第一压缩数据经前述网络发送给前述文件接收服务器；

前述文件接收服务器将所接收的前述压缩数据以及前述的第一压缩数据的接收时间存储于前述存储装置中；

前述文件发送装置在所述第一压缩数据发送后将上述文件的非压缩数据通过所述网络发送给前述文件接收服务器；

前述文件接收服务器把对所接收的前述非压缩数据施加单向函数后所得的第二压缩数据与前述第一压缩数据比较，在得到此第一与第二压缩数据相一致的比较结果时，把所述第一压缩数据的接收时间确定为前述文件的接收时间。

文件发送系统及方法

本申请是申请号为 98122775.9、申请日为 1998 年 12 月 4 日、发明名称为“文件发送系统和方法”的发明专利申请的分案申请。

技术领域

本发明涉及通过电子数据发送/接收各类文件，伴随此种文件的发送/接收进行费用支付以及进行这种支付接收的文件发送系统与方法。

技术背景

近年来，在因特网之类的开放网络环境中，已可进行文件数据的接收与发送以及贸易等，预计将来的形式将更会多种多样。例如现在向专利局提出专利申请文件等时，申请人已可通过拨号直接接通专利局的服务器来发送提出的文件数据。而在将来，申请人则可能经由因特网与专利局连接。另一方面，对于不动产登记或商业登记，或是由相应机关从事的户口卡和其它证明的发行业务，则要有由申请人直接向登记单位或相应机关提交文件（各种申请书）的手续。但是，即使是后述这类业务，将来也很有可能通过因特网执行。

于是，在通过因特网等通信提交电子式文件的情况下，伴随这类文件的提出，需要支付手续费。相对于专利局、登记所或是机关那样的官方公共机构提交文件时，多取购入印花票与收讫标签等，将其贴于前述文件上提交的形式。在通信中，进行文件提出时需有某种手续费的支付机构。例如日本的专利局的电子申请系统中，首先由文件提出者将若干金额存入预交户头。而在专利局一方的电子申请系统接收申请时，就从该预交户头中划拨必要的金额。

另一方面，在所谓电子购物的贸易中，可经由因特网购入种种商品。它的支付可从信用卡或银行户头进行划拨。具体地说，购物者经通信将信用卡或银行户头的帐号发送出，而在售货一方则据此帐号从信用卡或银行户头划拨预定的金额。此外，近年来还提出了称作 SET（安全电子

交易）的因特网的电子结帐方式。有关 SET，例如可参看“SET Secure Electronic Transaction Specification Book I: Business Description”, Version 1.0, March 31, 1997。

通过因特网等通信提交电子文件时需支付手续费时，在如上述的日本专利局的电子申请系统之类装置从预交户头划拨方式下，提交文件者必须设置预交户头这一点是不方便的。在不动产等的申请中，这类文件的提出者通常一生中也只办理一次这样的手续。因而难怪申请人把设置预交户口视为麻烦的事情。

作为不依赖预交户头的支付方法有从信用卡或银行户口划拨的方法。这时需使从申请者指定的信用卡或银行户头所作的划拨处理与经由通信进行文件提出的接收处理分别进行。从而有可能发生在文件提交之后，由于户头中预存的金额不足需划拨的金额而不能划拨的情形。

若是根据上述 SET 的协议，则能在因特网上进行电子结帐。这时的购物者与货款的支付者是同一个人，是以在提出商品购入的同时进行结帐为前提。因此，对于专利局、登记所或是某种机关那样的公共机构所适用的贴付印花票或收讫标签的手续便不熟悉了。这样的手续，有时是由文件申请者的代理人代替申请者进行文件的发送。这就是说，附到文件上的证明书或印花票等应由文件的申请者支付其费用，而另一方面文件则是由代理人提出。由于费用的支付者和文件的提交者不同，这时文件的提交手续和相关的关系就不能进行 SET 的协议进行支付手续。如果文件提交的费用的支付是同文件的提交本身无关的进行，则在费用的支付中可以使用 SET 的协议。但在这种情况下费用的支付手续与文件的提交手续有关系时，那就要费工夫的。

再有，在提交各类文件时，有时需要明确规定提交的日期时间。由通信来提交文件时，当通信线路状态恶劣时，就会产生重新发送的必要，会产生文件提交时间不明确的不便情形。特别是在把开始发送文件的时刻作为文件提交的时刻时的情形，在开始发送而确保提交的日期和时刻后，由于会发生再发送，之后会发送其它内容的文件，当这份文件是在前述的提交日子时刻提交时，便有可能发生滥用主张的恶果。于是需要

有合理地确定通信中提交文件之际的提交时刻的结构。

发明内容

本发明的目的在于提供使经由通信网络来发送电子文件和交纳其手续费两者能方便进行的文件发送系统与方法。

根据上述目的，可以在经由因特网等通信提交电子文件之际有需要支付手续费时，不必要设置预交户口这类的特别户头，也不必要从信用卡或银行户头由另外的步骤来进行划拨处理，而且即使是费用支付者与文件提交者不同时，也能恰当地进行文件的提交及其费用的支付。

本发明的另一个目的在于提供于通信中提交电子文件时，具有不允许滥用，能合理地确定提出日期与时刻的结构的文件发送系统与方法。

一种文件接收系统，其特征在于，此系统包括

通信网络，

与此通信网络连接来发送文件的装置，及

与此通信网络连接并经由此通信网络接收前述文件且包含有存储装置的文件接收服务器，

所述文件发送装置将对所述文件施加单向函数后所得的第一压缩数据经前述网络发送给前述文件接收服务器；

前述文件接收服务器将所接收的前述压缩数据以及前述的第一压缩数据的接收时间存储于前述存储装置中；

前述文件发送装置在所述第一压缩数据发送后将上述文件的非压缩数据通过所述网络发送给前述文件接收服务器；

前述文件接收服务器把对所接收的前述非压缩数据施加单向函数后所得的第二压缩数据与前述第一压缩数据比较，在得到此第一与第二压缩数据相一致的比较结果时，把所述第一压缩数据的接收时间确定为前述文件的接收时间。

根据本发明的一种实施形式，提供了经由网络从申请人装置相对于文件接收服务器发送文件的文件发送系统，其中，在前述网络上连接有支付接收服务器；前述申请人装置具有相对于此支付接收服务器指定支付金额，委托其进行费用支付的装置；此支付接收服务器具有：根据来

自前述申请人装置的对费用支付的委托，实施相对于金融机关的支付的信用查询的装置，和根据此信用查询判明前述申请人的费用支付有保证时，将表示该费用支付得到保证为宗旨的支付证明书制成不能改动形式发送给前述申请人装置的装置；前述申请人装置具有将前述支付证明书附于发送的文件中作为附有不能改动形式的支付证明书的文件发送给前述文件接收服务器的装置；此文件接收服务器具有在确认由前述申请人装置送来的支付证明书为未曾使用的之后，将附有此支付证明书的文件加以保管的装置。

根据本发明的另一种实施形式，提供了经由网络从申请人装置，通过代理人装置代理，相对于文件接收服务器发送文件的文件发送系统，其中，在前述网络上连接有支付接收服务器；前述申请人装置具有相对于此支付接收服务器指定支付金额且委托其进行费用支付的装置；此支付接收服务器具有：根据来自前述申请人装置的对费用支付的委托，实施相对于金融机关的支付的信用查询的装置，和根据此信用查询判明前述申请人的费用支付有保证时，将显示该费用支付得到保证为宗旨的支付证明书制成不能改动形式发送给前述申请人装置的装置；前述申请人装置具有将前述支付证明书附于发送的文件中作为附有不能改动形式的支付证明书的文件发送给前述代理人装置的装置；前述代理人装置具有将接收的附有支付证明书的文件发送给前述文件接收服务器的装置；此文件接收服务器具有在确认由前述申请人装置送来的支付证明书为未曾使用的之后将附有此支付证明书的文件加以保管的装置。

根据本发明的又一种实施形式，提供了经由网络从申请人装置相对于文件接收服务器发送文件的文件发送系统中，伴随文件发送接收费用支付的支付接收服务器，它包括有：根据来自前述申请人装置的对费用支付的委托，实施相对于金融机关的支付的信用查询的装置；和根据此信用查询判明前述申请人的费用支付有保证时，将显示该费用支付得到保证为宗旨的支付证明书制成不能改动形式发送给前述申请人装置的装置。

根据本发明的再一种实施形式，提供了经由网络从预定的装置相对

于文件接收服务器发送文件的文件发送系统，此系统包括：由前述发送文件的预定装置对欲发送的文件数据作单向函数变换取得压缩数据，并将此压缩数据以不可改动形式发送给前述文件接收服务器的装置；由前述文件接收服务器存储所接收的压缩数据之后，将票据发送给前述发送文件装置的装置；在前述发送文件装置接收至票据时进行将欲发送的文件数据发送给前述文件接收服务器的装置，在前述文件接收服务器接收到全部前述文件数据后，把对此文件数据施加单向数据取得的压缩数据与前述存储的压缩数据相比较，来确认这些压缩数据是否一致的装置。

根据本发明的又一实施形式，提供了经由网络从申请从装置相对于文件接收服务器发送文件的文件发送方法，此方法包括下述步骤：在前述网络上连接支付接收服务器的同时，由前述申请人装置相对于前述支付接收服务器指定支付金额且委托其进行费用支付的步骤；由前述支付接收服务器根据来自前述申请人装置的对费用支付的委托，实施相对于金融机关的支付的信用查询的步骤；根据此信用查询判明前述申请人的费用支付保证时，将显示该费用支付得到保证为宗旨的支付证明书制成不能改动形式发送给前述申请人装置的步骤；由前述申请人装置将前述支付证明书附于应发送的文件中作为附有不能改动形式的支付证明书的文件发送给前述文件接收服务器的步骤；由前述文件接收服务器在确认由前述申请人装置送来的支付证明书为未曾使用之后，将附有此支付证明书的文件加以保管的步骤。

根据本发明的再一种实施形式，提供了经由网络从预定的装置相对于文件接收服务器发送文件的文件发送方法，此方法包括下述步骤：由前述发送文件的预定装置对欲发送的文件数据施加单向函数变换取得压缩数据，并将此压缩数据以不可改动形式发送给前述文件接收服务器的步骤；在前述文件接收服务器存储所接收的压缩数据之后，将票据发送给前述发送文件装置的步骤；在前述发送文件装置接收到票据后进行将欲发送的文件数据发送给前述文件接收服务器的步骤；在前述文件接收服务器接收到全部前述文件数据后，把对此文件数据施加单向函数变换取得的数据与前述存储的压缩数据相比较，来确认这些数据一致的步

骤。

根据本发明的实施例，在经由因特网等通信进行电子文件的提交而需支付费用时，若相对于支付接收服务器提出支付的委托时，此支付接收服务器则实施信用查询，在费用的支付有保证时，即发放旨在表明具有不可改动形式的支付证明书，这样，就可不必设置预交户头之类的特别户头，也不存在在从信用卡或银行户头上由另外方面进行划拨处理时而未曾划拨的情形，此外，即使费用支付者与进行文件提交者不同时，也能够恰当地进行文件的提交及其费用的支付。

再者，提供了这样的结构，使得在发送文件之前是将所发送的文件用单向函数压缩成的压缩数据来发送，然后与相对于实际发送的文件由相同单向函数压缩成的压缩数据进行比较确认，这样，在由通信进行电子文件的提交时，就不会发生滥用，而能合理地确定提交的日期与时刻。

附图说明

图 1 是本发明的实施例的文件发送系统的总图。

图 2 是图 1 中所示文件接收服务器与支付接收服务器的内部结构图。

图 3 是图 1 所示认证局的结构图。

图 4 是图 1 所示代理人装置的结构图。

图 5 是图 1 所示申请人装置的结构图。

图 6 示明图 1 所示实施例的系统中所用支付证明书的内容。

图 7 示明图 1 所示实施例的系统中所用支付证明书管理 DB 的内容。

图 8 示明图 1 所示实施例的系统从文件接收服务器发送给代理人装置的票据的内容。

图 9 示明图 1 所示实施例的系统所用接收管理 DB 的内容。

图 10 是示明图 1 所示实施例的系统中从代理人装置到申请人装置的文件发送流程的流程图。

图 11 是示明图 1 所示实施例中接收从代理人装置发送给申请人装置的数据的申请人装置处理流程的流程图；

图 12 是示明图 1 所示实施例中申请人的费用支付处理流程的流程图。

图 13 是示明图 1 所示实施例中支付接收服务器的支付接收处理流程的流程图。

图 14 是示明图 1 所示实施例中从申请人装置向代理人装置发送文件流程的流程图。

图 15 是图 1 所示实施例中从申请人接收数据的代理人装置的处理流程的流程图。

图 16 是图 1 所示实施例中从代理人装置向文件接收服务器发送附有支付证明书的文件的处理流程的流程图。

图 17 是图 1 所示实施例中表明文件接收服务器的票据发放处理流程的流程图。

图 18 是图 1 所示实施例中表明文件接收服务器的文件接收处理流程的流程图。

图 19 概示图 1 所示实施例中文件接收服务器的文件接收日期与时刻确定的时间图。

具体实施方式

下面根据附图说明本发明的实施例。

图 1 是本发明一实施例的文件发送系统的总图。在因特网 110 上连接有文件接收服务器 101、支付接收服务器 102、认证局 103、代理人装置 104、申请人装置 105、金融机关服务器 106 以及金融机关认证局 107。此 101～107 的装置各为计算机节点。

现在概述图 1 的系统中的处理流程。为简化说明，加密/译码处理或数字署名处理都予除去（关于它们将在以后参照流程图证明）。

申请人装置 105 是支付规定费用并提交文件的申请人操作的装置，代理人装置 104 是代理该申请人进行文件提交（实际的文件发送）的由代理人操作的装置。提交的文件首先由代理人根据申请人的委托通过代理人装置 104 制成。制成的文件数据发送给申请人装置 105。申请人确认接收的文件数据的内容后即保存该文件数据。此外，申请人从申请人

装置 105 连接到支付接收服务器 102，进行费用支付处理。

支付接收服务器 102 是伴随文件的提交进行有关费用支付处理的服务器。在收到申请人装置 105 的用费支付处理要求时，与金融机关服务器 106 相连接对相应申请人实施信用查询后，将支付证明书返送给申请人装置 105。支付证明书是证明申请人进行了费用支付（或已保证进行的支付预约）的数据，是相当于印花票或收讫标签的数据，详述于后。支付证明书在本实施例中由文件接收服务器 101 与支付接收服务器 102 两者能共同访问的支付证明书管理 DB 管理。申请人从申请人装置 105 接收其支付证明书，将支付证明书附于所保存的文件数据中发送给代理人装置 104。代理人通过代理人装置 104 接收此数据后即加以保管。在以后的任意时期中，代理人可把该数据发送给文件接收服务器 101。

文件接收服务器 101 是接收代理人装置 104 发送来的电子式的提交文件的服务器。文件接收服务器 101 接收由代理人发送的数据（于文件数据中附有支附证明书的数据），验证支付证明书，保管文件数据。所谓支付证明书的验证是向支付证明书 DB 查询此支付证明书是否是未曾使用过的，如果是未曾使用的，文件接收服务器 101 便进行使用结束的处理。

认证局 103 是发放用于进行申请人或代理人认证的证明书的认证机构。金融机关服务器 106 是设有申请人户头的金融机关的服务器。金融机关认证局 107 是发放用来进行具有此户头的申请人认证的证明书的认证机构。

图 2 示明图 1 的文件接收服务器 101 与支付接收服务器 102 的内部结构。

文件接收服务器 101 包括票据发放处理部 211、文件接收处理部 212、署名生成部 213、加密/译码处理部 214 以及通信控制部 215。支付接收服务器 102 包括支付接收处理部 211、署名生成部 222、加密/译码处理部 223、支付证明书生成管理部 224、SET 处理部 225 以及通信控制部 226。此外，作为文件接收服务器 101 与支付接收服务器 102 两方能共同访问的 DB，配备有接收管理 DB231、密钥与证明书管理 DB232、

申请人与代理人管理 DB233 以及支付证明书管理 DB234。

文件接收服务器 101 通过因特网 110（图 1）接收代理人装置 104 发送来的文件。文件接收处理部 212 则进行这种文件的接收处理（详见图 18 的说明）。票据发放处理部 211 在进行文件接收处理时，于接收到实际文件数据之前进行票据的发放处理（详见图 17 的说明）。票据的发放用于确定文件接收服务器 101 的文件提出日期与时刻的处理。这就是说，从代理人装置 104 将文件发送给文件接收服务器 101 之际，若把实际要发送的文件作为数据原样发送时，需要很长的时间。因此，容易产生再发送的必要性。这将使此种文件提交的时刻变得不明确，而且会出现滥用文件提交时刻不明确的问题，因此进行下述①～④中的处理。

①首先由代理人装置 104 将实际欲发送的数据由单向函数例如散列函数压缩，求得信息提要，将此信息提要发送给文件接收服务器 101（具体地说，附有证明书进行加密通信）。

②在文件接收服务器 101 中，经票据发行处理部 211 的票据发放处理（图 17），取得新的接收编号。然后，文件接收服务器 101 使此接收编号与该信息提要相对应进行存储，并在同时将此接收编号发送给代理人装置。用来发送此接收编号的数据便是票据。如以后所述，这时的文件接收服务器 101 便确定与此信息提要相对应的文件接收的日期与时刻。

③代理人装置 104 在根据票据接收到接收信号后，即附上此接收编号作为实际发送的数据发送给文件接收服务器 101。

④在文件接收服务器 101 中，当从代理人装置 104 接收到全部数据后，由单向函数（同①中所用的函数）压缩这种数据求得信息提要，来确认其是否与②中存储的信息提要一致。如果一致，则从票据发行时由代理人装置 104 实际发送后，实际接收到的便是目的数据。如果不一致，则发送的可能是别的数据。

图 8 示明了本实施例的系统中，从文件接收服务器 101 发送给代理人装置 104 的票据内容。接收编号 801 是从代理人装置 104 发送文件时

对应于此文件的发送，文件接收服务器 101 新分配的编号。发送者信息 802 是对发送此文件的送信者（代理人）特定的种种信息。接收日期与时刻 803 是文件接收服务器 101 接收信息提要结束的日期与时刻。有效期限 804 表示的是此票据的有效期限。从代理人装置 104 发送文件时，即使发生再发送的问题，也可只把发送该文件的那段充分的时间取作有效期限（也可取从票据发行时起的一段预定时间）。为了防止文件发送的极端过迟才确定了有效期限 804。署名 805 是相对于 801～804 的数据附加文件接收服务器 101 的电子署名。

图 9 示明本实施例的系统中所用图 1 的接收管理 DB231 的内容。文件接收服务器 101 在上述②的票据发放处理（图 17）中取得新的接收编号时，在此接收管理 DB231 上即取得新的接收编号，并确保与所接收编号相对应的 1 行的区域。在接收编号 901、发送者信息 902、接收日期与时刻 903 以及有效期限 904 中，存储有与设定在发送票据（图 8）中的信息 801～804 相同的内容。在信息提要 905 与发送者证明书 906 中存储有上述①中由代理人装置 104 发送来的信息。此外，票据管理信息 907 存储有此票据使用与否的标记信息，且令初始值为“未使用”。文件的内容 908 是存储从代理人装置 104 送来的文件中全部数据的区域。在上述④中确认信息提要是一致时，文件接收服务器 101 在票据管理信息 907“使用完毕”时，即把接收的文件数据存储于文件内容 908 中。

再回到图 2，继续说明文件接收服务器 101 的结构。署名生成部 213 与加密/译码处理部 214 用于在进行文件接收处理中给发送数据附上署名，以及用于进行加密/译码处理。通信控制部 215 进行和因特网 110 之间的通信控制。

支付接收服务器 102 从申请人接收费用支付。在此实施例系统中，申请人从申请人装置 105 连接到支付接收服务器 102，从而进行费用支付处理。在图 2 中，支付接收处理部 221 进行接收申请人费用支付要求的处理（由图 13 作详细说明），将表明申请人已进行了费用支付（或已保证支付）的支付证明书发放给申请人。支付证明书起到印花票，收

讫标签或代用券与商品券之类的作用。支付证明书的发放，是就申请人而言相对于金融机关在执行支付信用查询与支付预约时所发放的。因此，文件接收服务器 101 与支付接收服务器 102 的管理机关必然可以相应申请人的户头上划拨支付证明书所发放的金额。支付证明书与预先交费不同，它首先不必开设预交户口。支付证明书如同印花票那样，可用于别的文件中或是赠与他人。

图 6 中示明本实施例的系统中所用支付证明书的内容。支付证明书包括管理编号 601、支付金额 602、申请人信息 603、有效期限 604 以及支付接收服务器 102 的署名 605。管理编号 601 是支付证明书固有的管理编号。支付金额 602 是指定申请人支付的金额的信息。申请人信息 603 是具体规定提出支付请求并接收相应支付证明书的申请人的信息。有效期限 604 是此支付证明书的有效期限。署名 605 是发放此支付证明书的支付接收服务器 102 的署名，由此保证此支付证明书确实是从支付接收服务器 102 所发放的。这些信息 604～605 是在相对于支付接收服务器 102，在此即为费用支付人也即申请人，发放上述支付证明书时设定的。

图 7 示明本实施例的系统中所用图 1 的支付证明书管理 DB234 的内容。支付接收服务器 102 由此支付证明书管理 DB 管理所发放的支付证明书。在支付证明书管理 DB234 的 701～705 中，存储有发放的支付证明书 601～605 的信息。使用状态 706 是表明此支付证明书是否使用过的标志。当文件服务接收器 101 接收文件时，由附于此文件上的支付证明书的管理编号 601 来检索支付证明书管理 DB234，搜索相对应的入口。如果此入口的使用状态 706 为“未使用”时，由于此支付证明书亦处在未使用情形，则令此使用状态 706 为“使用完毕”。这相当于确认已贴附有印花票或收讫标签等。当再次发送使用同一支付证明书的文件时，由于使用状态 706 为“使用完毕”，则可确认费用的支付没有保证。

由于是用图 7 所示的支付证明书管理 DB234 来管理支付证明书，既使支付费用的申请人和实际进行文件发送的代理人不是同一人时，也可完成相应的手续。此外，支付证明书也可以转让给他人来使用。

再次返回图 2 继续说明支付接收服务器 102 的结构。署名生成部

222 与加密/译码处理部 223，用于在进行支付接收处理时给传输数据上附上署名，以及用于进行加密/译码。支付证明书生成管理部 224 生成图 6 所示的支付证明书，由图 7 所示的支付证明书管理 DB234 进行此支付证明书的管理处理。SET 处理部 225 在从支付接收服务器 102 相对于金融机关服务器 106 执行申请人的信用查询时，进行遵照 SET 协议的处理。通信控制部 226 进行与因特网 110 之间的通信控制。

有关由文件接收服务器 101 和支付服务器 102 两方共同访问的 DB 即接收管理 DB231 与支付证明书管理 DB234，已由图 9 与图 7 说明。密钥与证明书管理 DB232，是用来管理文件接收服务器 101 与支付服务器 102 的私有密钥与公开密钥以及由认证局 103、107 发放的证明书、进行认证时所用的认证局 103、107 的公开密钥，还有通信对方的公开密钥等的 DB。申请人与代理管理 DB233 是用来管理有关与文件接收服务器 101 和支付接收服务器 102 相连接的申请人或代理人的信息的 DB。

在此实施例中，文件接收服务器 101 与支付接收服务器 102 是分别设置而共同使用同一个 DB230 的，但也可取不用共同的 DB 而是完全分开的 DB 的结构。这时的支付管理 DB231 可由文件接收服务器 101 管理。在这种情形下，文件接收服务器 101 可对支付证明书管理 DB234 进行访问，要求使检索入口的使用状态 706 从“未使用”变更到“使用完毕”的情形代之以文件接收服务器 101 相对于支付接收服务器使该入口的使用状态从“未使用”变更到“使用完毕”。相反，文件接收服务器 101 与支付接收服务器 102 也可包括 DB203 而在一台装置上构成。这时的通信控制部 215 与 226、署名生成部 213 与 222 以及加密/译码处理部 214 与 223 也可具有共同的结构。

图 3 示明图 1 所示认证局 103 的结构。认证局 103 包括证明书发放处理部 301、证明书管理部 302、通信控制部 304 及以证明书管理 DB311。认证局 103 首先是发放证明书给代理人或申请人。

图 4 示明图 1 所示代理人装置 104 的结构。代理人装置 104 包括申请书编辑部 401、署名生成部 402、加密/译码处理部 403、文件发送处理部 404、文件接收处理部 405、通信控制部 406、申请书管理 DB411

以及密钥与证明书管理 DB412。

申请书编辑部 401 是代理人用来制成发送的文件的编辑程序。文件输送处理部 404 进行把文件发送给申请人装置 105 的处理（由图 10 详释）或是进行把附有支付证明书的文件发送给文件接收服务器 101 的处理（由图 16 详释）。署名生成部 402 与加密/译码处理部 403 是在把署名附于发送/接收的数据上时，以及在进行加密/译码处理时使用。通信控制部 406 进行与因特网 110 之间的通信控制。

申请书管理 DB411 是把代理人用申请书编辑部 401 制成的文件或由申请人装置 105 送来的附有支付证明书的文件加以保存、管理的 DB。密钥与证明书管理 DB412 是用来管理代理人装置 104 的私有密钥、公开密钥以及认证局 103 与 107 发放的证明书、进行认证时所用的认证局 103、107 的公开密钥以及通信对方的公开密钥等的 DB。

图 5 示明图 1 中所示申请人装置 105 的结构。申请人装置 105 包括文件接收处理部 501、接收文件管理部 502、加密/译码处理部 503、署名生成部 504、支付处理部 505、文件发送处理部 506、支付证明书管理部 507、通信控制部 508、申请书管理 DB511、密钥与证明书管理 DB512 以及支付证明书管理 DB513。

文件接收处理部 501 进行从代理人发送来的文件的接收处理（详释于图 11 中）。接收文件管理部 502 将接收的文件在申请书管理 DB231 中加以保存并管理。支付处理部 505 与支付接收服务器 100 连接，进行手续费的支付处理（详释于图 12 中）。文件输送处理部 506 相对于代理人进行附有支付证明书的文件等的发送处理（详释于图 14 中）。署名生成部 504 与加密/译码处理部 503 用于在将署名附于发送数据上时，以及进行加密/译码处理时。支付证明书管理部 507 对支付接收服务器 102 发放的支付证明书由支付证明书管理 DB513 进行管理处理。通信控制部 508 进行与因特网之间的通信控制。

申请书管理 DB511 是对代理人发送来的文件等进行保存与管理的 DB。密钥与证明书管理 DB512 是管理申请人装置 105 的私有密钥与公开密钥以认证局 103 与 107 发行的证明书、进行认证时所用的认证局 103

与 107 的公开密钥及通信对象的公开密钥等的 DB。支付证明书管理 DB513 是保存与管理支付接收服务器 102 发放的支付证明书，它的结构与图 7 所示的支付接收服务器 102 的支付证明书管理 DB234 相同。但是，此支付证明书管理 DB513 是管理申请人所接收的支付证明书，而使用状态 706 则表明此申请人使用与否的信息。

下面，参照图 10－图 18 的流程图及图 19 的时间图详细说明图 1 的系统的各处理。

图 10 是示明从代理人装置 104 到申请人装置 105 的文件发送流的流程图。此流程的处理主要是由图 4 所示的文件处理部 404 所进行的处理。首先由代理人根据申请人委托用图 4 所示的申请书编辑部 401 制成文件。在步骤 1001 相对于所发送的文件实施代理人的电子署名。具体地说，由单向函数（散列函数等）压缩文件数据，然后将此压缩数据（信息提示）用代理人的私有密钥加密得到的署名数据附于原始的文件数据上，制成附有代理人署名的文件。随后于步骤 1002 形成使附有代理人署名的文件加密的共用密钥，由此共用密钥使代理人署名的文件加密。再于步骤 1003 用申请人的公开密钥使上述共用密钥加密。在步骤 1004，将已加密的附有代理人署名的文件与共用密钥同代理人的证明书一起发送给申请人装置 105，结束处理。

首先从认证局 103 取得代理人的证明书。所谓代理人的证明书是使代理人的公开密钥与有关此代理人的种种信息相连系，并对于此连系的数据由认证局 103 的私有密钥附上署名的数据。认证局 103 在接收代理人的证明书发放委托时，进行此代理人的身分确认后，发放证明书。当把此证明书附于代理人装置 104 发送的数据上，即可由此证明书验证此数据确实为该代理人关来的数据，亦能从此证明书取得对此代理人的公开密钥或代理人特别规定的种种信息。同样，申请人也是首先从认证局预先取得证明书。

图 11 示明根据图 10 的处理，接收从代理人装置 104 发送给申请人装置 105 数据的，申请人装置 105 的处理流程。这一处理主要是由图 5 的文件接收处理部 501 进行的处理。首先，于步骤 1101 验证接收数据

中代理的证明书，同时用申请人的私有密钥使接收数据中的加密的共用密钥译码。在步骤1102，用译码后的共用密钥对附有代理的署名的文件译码。于步骤1103用代理人的公开密钥验证附有此代理人署名的文件的署名。这一验证是用来确认，由代理人公开密钥使署名数据译码的值，是否等于由单向函数（采用与图10的步骤1001所用的相同的函数）压缩的压缩数据（信息提要）。如果验证的结果是恰当的署名（步骤1104中的“否”），则于步骤1105保管附有此代理人署名的文件。如果验证的结果不是恰当的署名（步骤1104中的“是”），则申请人便于步骤1106中报告申请文件被改动并结束此处理。

图12是示明申请人费用支付处理的流程的流程图。这项处理主要是由图5的支付处理部505进行的处理。首先于步骤1201中从申请人装置105连接上支付接收服务器102，确定并输送支付的金额。在步骤1202，将申请人的证明书（从认证局103取得的证明书）出示给支付接收服务器102。步骤1203是支付接收服务器102方向的处理，由图13于以后说明。在步骤1203之后，从支付接收服务器102发送由申请人的公开密钥加密的共用密钥与由此共用密钥加密的支付证明书（图6）。在步骤1204，由申请人的私有密钥使从支付接收服务器102发送的已加密的共用密钥译码。在步骤1205，采用已译码的共用密钥使加密的支付证明书译码。在步骤1206，将译码的支付证明书保管于支付证明书管理DB513（图7）中，结束处理。

图13是示明图12的步骤1203的处理即支付接收服务器中支付接收处理流程的流程图。这一处理主要是由图2中支付接收处理部221进行的处理。首先于步骤1301中，验证申请人送来的证明书，取得申请人的公开密钥。其次于步骤1302中，例如采用SET的协议，相对于金融机实施来自申请人信用查询。具体地说，向图1的金融机关服务器106发送特定的申请人与划拨的金额的信息，确保从此申请人的户头应划拨下的金额。

在对金融机关实施支付信用查询时，为了需要相对金融机关证明使用支付接收服务器102的机关本身，此使用支付接收服务器102的机关

需预先从金融机关认证局 107 取得证明书。同时，由于此支付信用查询也应进行有关进行划拨的申请人的认证（必须确认是否确实是来自此申请人的划拨委托），申请人首先也应从金融认证局 107 领得证明书，同时在步骤 1202 将此金融机关的证明书发送给支付接收服务器 102。此支付接收服务器 102 在步骤 1302 实施信用查询时，需附上此申请人的金融机关的证明书实施信用查询。

作为步骤 1302 的信用查询的结果，在步骤 1303 如果能确保上述所划拨的金额部分的划拨范围便进行步骤 1304。如果信用查询结果存在某些问题便结束处理。在步骤 1304，取得新发行的支付证明书的管理编号，具体上是由图 7 所示结构的支付证明书管理 DB234 来确保新规定的管理编号 1 行部分的区域。在步骤 1305，从申请人的证明书提取表征申请人的信息。在步骤 1306，对管理编号、支付金额、表征申请人的信息以及有效期效等相连接的数据实施电子署名，制成支付证明书（图 6）。具体地说，由单向函数压缩上述关联的数据，把由支付接收服务器 102 的私有密钥加密此压缩数据的署名数据附于原始的相关数据上，制成支付证明书。

在步骤 1307，将此制成的支付证明书中所含信息记录于支付证明书管理 DB234（图 7）。然后于步骤 1308 生成支付证明书加密用的共用密钥，用此共用密钥使支付证明书加密，再于步骤 1309 由申请人的公开密钥使前述共用密钥加密。于步骤 1301，将加密的共用密钥与由此共用密钥加密的支付证明书发送给申请人装置 105，结束处理。

图 14 是表示从申请人装置 105 向代理人装置 104 进行文件发送的流程的流程图。主要由图 5 的文件发送处理部 506 进行处理。

首先在步骤 1401，取出由图 11 的步骤 1105 保管的附有代理人署名的文件。在步骤 1402，对于含有附有代理署名的文件及支付证明书的数据实施申请人电子署名，称其为附有支付证明书的文件。另外，此处使用的支付证明书，在由图 7 的结构中由支付证明书管理 DB513 管理的支付证明书中，使使用状况 706 为“未使用”的。

其次，在步骤 1403 中，生成共用密钥，用该共用密钥将附有支付

证明书文件加密。在步骤1404，使用代理人的公开密钥，将前述共用密钥加密。在步骤1405，将加密后的共用密钥和用该共用密钥加密的附有支付证明书的文件发送给代理人装置104。

图15示明接收由图14的申请人发送的数据的代理人装置104的处理流程图。此项处理主要是由图4所示文件接收处理部405的处理。首先于步骤1501用代理人的私有密钥将接收数据中的加密共用密钥译码。在步骤1502，用译码的共用密钥使附有支付证明书的文件译码。在步骤1503，用申请人的公开密钥验证添加在附有此支付证明书文件上申请人的电子署名。具体地说，进行处理来确认，由申请人公开密钥译码的署名数据的值是否等于由单向函数（与图14步骤1402的署名中所用的相同的函数）压缩附有支付证明书的文件所得的压缩数据。

在步骤1504，如果验正的结果是恰当的署名，则进行步骤1506。在步骤1506，用支付接收服务器102的公开密钥来验证包括在附有支付证明书文件中的支付证明书中的电子署名。这项验证是进行处理以确认：由支付接收服务器102的公开密钥将署名数据译码的值，是否等于由单向函数（与图13的步骤1306的署名中所用的相同的函数）压缩与支付证明书中包括的管理编号、支付金额、表征申请人的信息以及有效期限相连接的数据而得到的数据。

在步骤1507，如果验证的结果是恰当的署名，则进到步骤1509。于步骤1509，用代理人的私有密钥验证附有支付证明书的文件中所含附有代理人署名的文件中的代理人署名。在步骤1510，如果验证结果是恰当的署名，则于步骤1512中保管附有支付证明书的文件，结束处理。如果在步骤1504、1507、1510任一个之中的验证结果表明是署名不恰，则向代理人报告在步骤1505、1508、1511中改动了文件。

图16示明从代理人装置104向文件接收服务器101发送处理附有支附证明书的文件的流程。这项处理主要是由图4中的文件发送处理部404进行的处理。首先于步骤1601由单向函数压缩欲发送的附有支付证明书的文件，生成压缩数据（信息提要）。然后于步骤1602生成共用密钥，由此共用密钥使上述信息提要加密。在步骤1604，将代理人证明

书加到由加密的共用密钥和由此共用密钥加密的信息提要中，发送给文件接收服务器 101。由于信息提要的发送时间比与之相应的整个文件的发送时间短，因而可以减少因通信线路不良带来的恶劣影响的可能性。

步骤 1605 是文件接收服务器 101 这一方的票据发放处理，由图 17 在以后说明。在步骤 1605 之后，从文件接收服务器 101 来发送由代理人公开密钥加密的共用密钥（由文件接收服务器 101 方面生成的密钥）和由此共用密钥加密的票据（图 8）。

在步骤 1606，用代理人的私有密钥将文件接收服务器 101 送来的加密的共用密钥译码。在步骤 1607，用文件接收服务器 101 的公开密钥来验证附于票据（图 8）上的电子署名。在步骤 1609，如果验证的结果表明是恰当的署名，由于能确保文件接收服务器 101 的接收的或提交的日期与时刻，便进行步骤 1611。在步骤 1609，如果署名不恰，则向代理人报告在步骤 1610 中票据有了改动，结束此处理。

如果接收到正确的票据，则于步骤 1611 生成共用密钥，而在步骤 1612 由此共用密钥将附有支付证明书的文件加密。随后于步骤 1614，由文件接收服务器 101 的公开密钥将上述共用密钥加密。再在步骤 1615 将此加密的共用密钥以及由此共用密钥加密的票据和附有支付证明书的文件发送给文件接收服务器 101。步骤 1616 是文件接收服务器 101 一方的处理，由图 18 于以后说明。步骤 1616 之后，由文件接收服务器 101 发送由代理人的公开密钥加密的共用密钥和由此共用密钥加密的接收确认书。

在步骤 1617，由代理人的私有密钥使由文件接收服务器 101 发送的加密的共用密钥译码。在步骤 1618，用译码的共用密钥使编码化的接收确认书译码。在步骤 1619，验证添加到接收确认书上的文件接收服务器 101 的电子署名。在步骤 1620，如果验证结果表明署名恰当，则于步骤 1622 保管此接收确认书，结束处理。在步骤 1620，如果验证结果表明署名不恰，则向代理人报告于步骤 1620 中改动了某些数据，结束处理。

图 17 是表明图 16 的步骤 1605 的处理即文件接收服务器 101 的票

据发放处理的流程。这项处理主要是由图 2 的票据发行处理部 211 进行的处理。首先于步骤 1701，用文件接收服务器 101 的私有密钥使代理人发送来的共用密钥译码。随之于步骤 1702，用此共用密钥使信息提要译码。再于步骤 1703 取得新的接收编号，将此接收编号 901、有关代理人（发送者）的信息 902、接收的日期与时刻 903、有效期效 904、信息提要 905 及代理人的证明书 906 保存于接收管理 DB231（图 9）中。此外，有关代理人的信息设定为从代理人发送来的数据中所包含的代理人证明书中抽取出的信息。有效期限设定为在现在的时间上加上预定时间而得到的时间。票据的管理信息 907 初始化为“未使用”。

在步骤 1704 生成连接接收编号 801、有关代理人的信息 802、接收的日期与时刻 803 以及有效期效 804 的数据，对此连接数据实施电子署名 805。附有此电子署名的数据即票据（图 8）。具体地说，用单向函数（图 16 的步骤 1601 或 1608 中所用的同一函数）压缩上述连接数据，把由文件接收服务器 101 的私有密钥加密此压缩数据而成的署名数据，相对于原来的连接数据制成票据（图 8），然后于步骤 1705 生成共用密钥，由此共用密钥使上述票据加密。在步骤 1707 把加密的共用密钥以及为此共用密钥编码化的票据发送给代理人，结束此处理。

图 18 示明图 16 的步骤 1616 的处理即文件接收服务器 101 中的文件接收处理流程。这项处理主要是由图 2 的文件接收处理部 212 进行的处理。首先于步骤 1801 用文件接收服务器 101 的私有密钥使由代理人发送来的共用密钥译码。随后在步骤 1802，用已译码的共用密钥，使票据和附有支付证明书的文件译码。然后于步骤 1803，验证附于票据上的电子署名以及有效期限。验证的结果，当于步骤 1804 中署名恰当且在有效期限内时，进行步骤 1806。当署名不恰或超过有效期限，则于步骤 1805 表明票据不当，结束处理。

在步骤 1806，用代理人装置 104 所用的单向函数（图 16 的步骤 1601 或 1608 中所用的同一函数），将代理人送来的附有支付证明书的文件压缩，生成信息提要。于步骤 1807，从代理人送来的票据中提取接收编号。然后，参照接收管理 DB231（图 9），取出对应于此接收编号的票

据，索求的信息提要，与步骤 1806 生成的信息提要比较。比较的结果据步骤 1808 是同一时，由于能确切地认定在票据索取时欲发送的内容和发送来的相同，便进到步骤 1810。当于步骤 1808 中比较的结果不同时，由于在票据索取时输送了与欲发送的内容有别的内容，在步骤 1809 进行数据不一致的显示，结束此处理。

在步骤 1810，从支付证明书管理 DB234（图 7）中检索支付证明书中所包括的管理编号的数据，验证其使用状况 706 是否为“未使用”。在步骤 1811，在“未使用”时，即由步骤 1813 将支付证明书管理 DB234 中相应于该管理编号的支付证明书的使用状况 706 变更为“使用完毕”。其次，于步骤 1814，将该接收编号的票据的管理信息 907 变更为“使用完毕”。再于步骤 1815，保管附有支付证明书的文件。文件的保管通过存储于图 9 的接收管理 DB231 的文件的内容 908 进行。

在步骤 1816，制成包含接收编号等接收信息的接收确认书，进行电子署名。在步骤 1817，生成共用密钥，由此共用密钥使上述附有电子署名的接收确认书加密。于步骤 1818，由代理人的公开密钥使上述共用密钥加密。在步骤 1819，将加密的共用密钥以及由此共用密钥加密了的附有电子署名的接收确认书发送给代理人，结束此处理。

根据上述实施形式的系统，申请人取得支付证明书，而代理人能将此支付证明书附于提交文件上发送给文件接收服务器。支付证明书能像印花票、收讫标签、货币代用券或商品券那样地作用，由于附有支付接收服务器的署名，不容易改动。实际的结帐则可用任意哪一种形式进行。在支付信用查询的阶段，由于保证了可以进行划拨，在文件接收服务器一方必然能征收到费用。同时，申请人将支付证明书附于文件上，并于其全部材料上附有署名发送给代理人，因而这成为表明了申请人对该文件内容了解的一种意志，使以后的代理人也不能改动此文件。

在确定文件提交时刻之中，首先用单向函数压缩提交者发送的文件数据而求得信息提要，把它与证明书一道发送给文件接收服务器，由文件接收服务器存储此信息提要，返回票据。然后，在由提交者发送全部文件数据时，求出此信息提要，与票据发放时存储的信息提要比较，以

确认从一开始送出的预定文件已送出，由此可把票据发放时刻视作为文件提交的时刻。

图 19 示明能由两个代理人装置分别将各自的电子文件基本上同时送到文件接收服务器 101 中时，确定文件接收时间的情形。

图中，首先由代理人装置 104 将电子文件 A 的信息提要 A 发送给文件接收服务器 101。文件接收服务器 101 接收到信息提要 A 后，按图 17 的步骤 1701～1702 使此信息提要译码，于步骤 1703 确定文件 A 的接收编号同时确定文件 A 的接收日期与时刻。这一处理即图 19 的步骤 1901。

另一方面，比信息提要稍晚，代理人装置 104'将电子文件 B 的信息提要 B 发送给文件服务器 101。同样，文件接收服务器 101 在接收到信息提要 B 后，于步骤 1902 确定文件 B 的接收编号同时确定文件 B 的接收日期与时刻。

其次，代理人装置 104'将附有支付证明书的文件 B 发送给文件接收服务器 101，然后由代理装置 104 将附有支付证明书的文件 A 发送给文件接收服务器 101。如果文件 A 与 B 中任一个都是合理的文件时，文件接收服务器 101 便给代理人装置 104 与 104'发放文件接收确认书。

从图 19 可知，从代理人装置 104 向文件接收服务器 101 的信息提要 A 的发送，要比从代理人装置 104'的信息提要 B 的发送快，但文件 A 的发送则比文件 B 的发送慢。这时，给以文件 A 由步骤 1901 确定的接收日期与时刻，给以文件 B 由步骤 1902 确定的接收日期与时刻。这就是说，文件 A 的接收日期与时刻比文件 B 的早。若是文件 A 与 B 为同一内容的专利申请说明书，假定文件接收服务器 101 是专利局，则专利局将决定文件 A 这一方为最前的专利申请。

在上述的实施例中说明的是代理人代理申请者进行文件提交的例子，但申请人也可不经由代理人而对文件接收服务器直接进行文件的发送。

另外，在上述实施例中，是以采用 SET 为例说明支付方式，但也可采用SET之外 的支付方式，例如不使用SET的信用卡的支付方式等。

再者，此述实施例中，申请人与手续费支付人虽为同一人，但本发明也适用于申请人与支付人为不同的情形。这时，支付人的计算机即支付人装置可以由与图 5 所示申请人装置 105 相同的结构实现。支付人装置接收申请人手续费的支付委托，对支付接收服务器 102 提出支付处理要求。支付接收服务器 102 在实施支付人的信用查询后给支付人发送支付证明书。此支付证明书从支付人装置转送给申请人装置 105。

本发明适用于经由因特网将文件发送给专利局、登记所或是机关等公用机构等的情形。此外也能用于所谓的电子购物等。

图 1

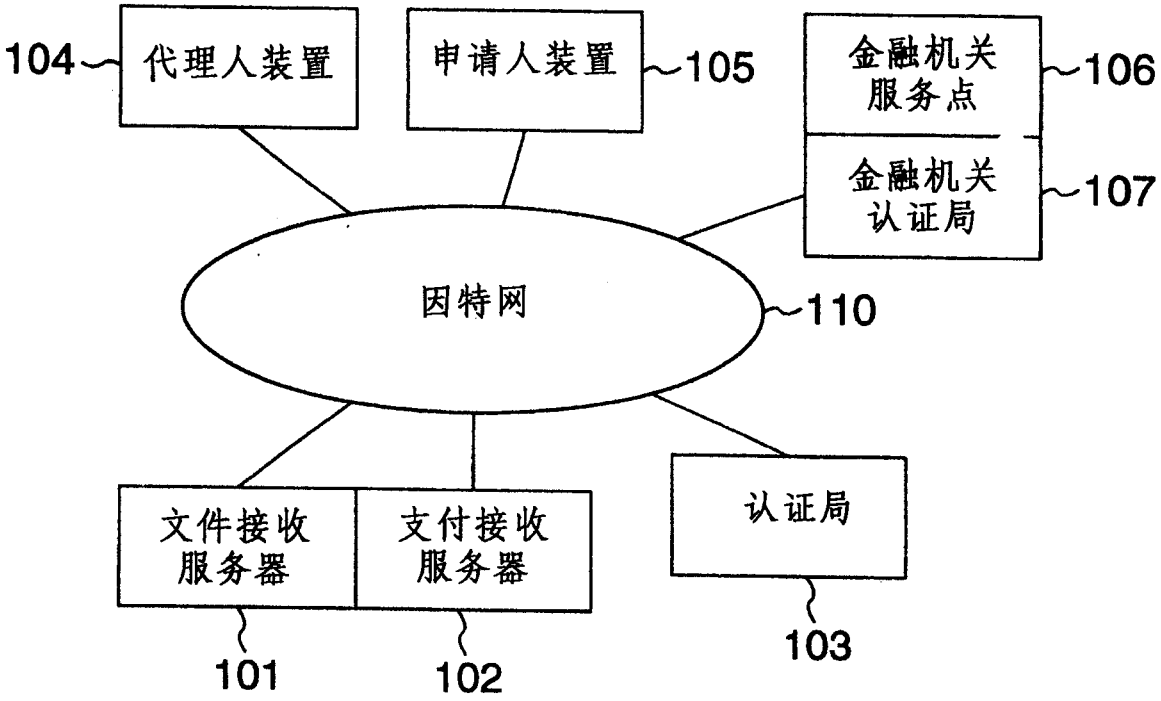

104
代理人装置
申请人装置
105
金融机关
服务点
106
金融机关
认证局
107
因特网
110
文件接收
服务器
支付接收
服务器
认证局
101
102
103

图 2

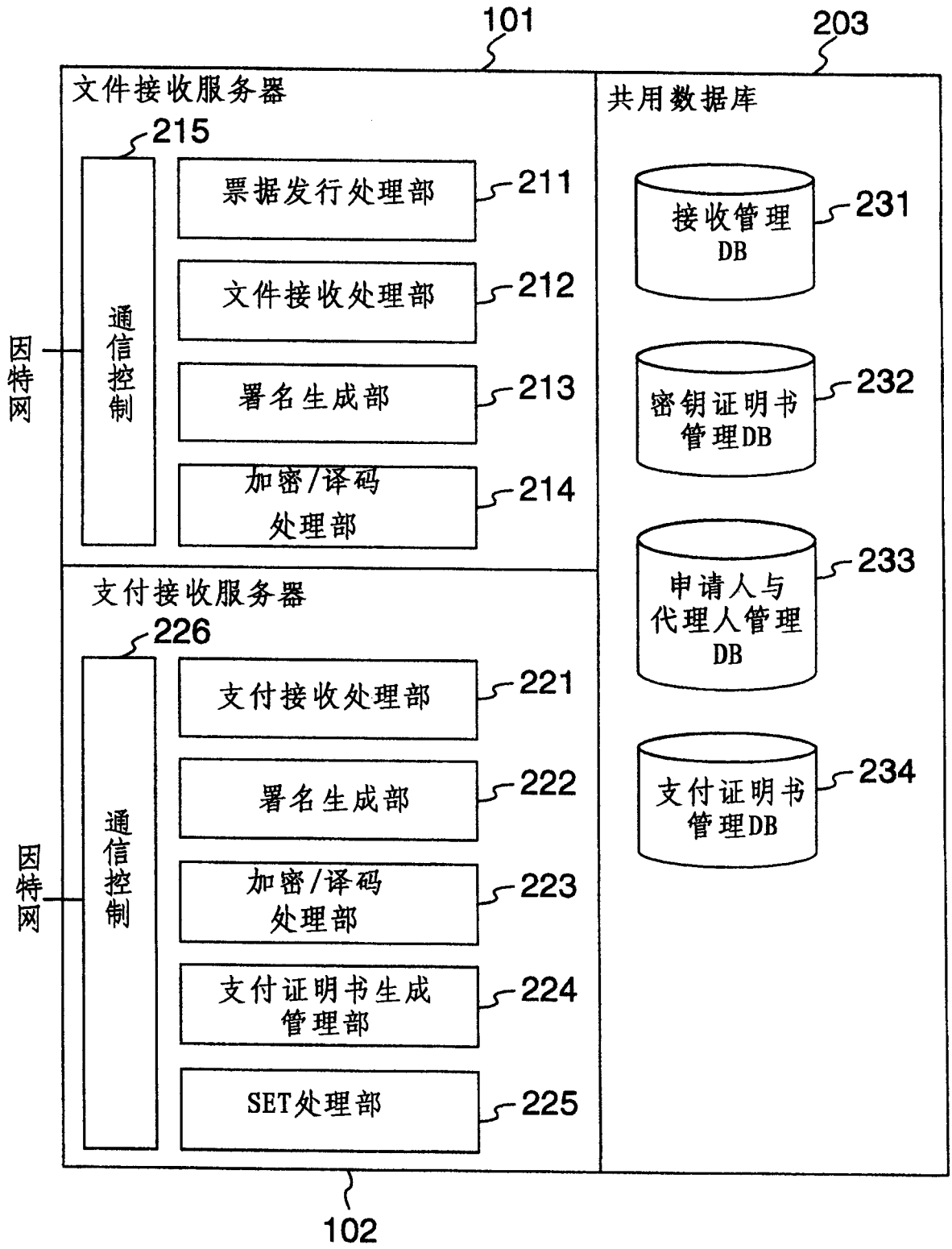

101
203
文件接收服务器
共用数据库
215
票据发行处理部
211
文件接收处理部
212
署名生成部
213
加密/译码处理部
214
通信控制
因特网
接收管理DB
231
密钥证明书管理DB
232
申请人与代理人管理DB
233
支付证明书管理DB
234
支付接收服务器
226
支付接收处理部
221
署名生成部
222
加密/译码处理部
223
支付证明书生成管理部
224
SET处理部
225
通信控制
因特网
102

图 3

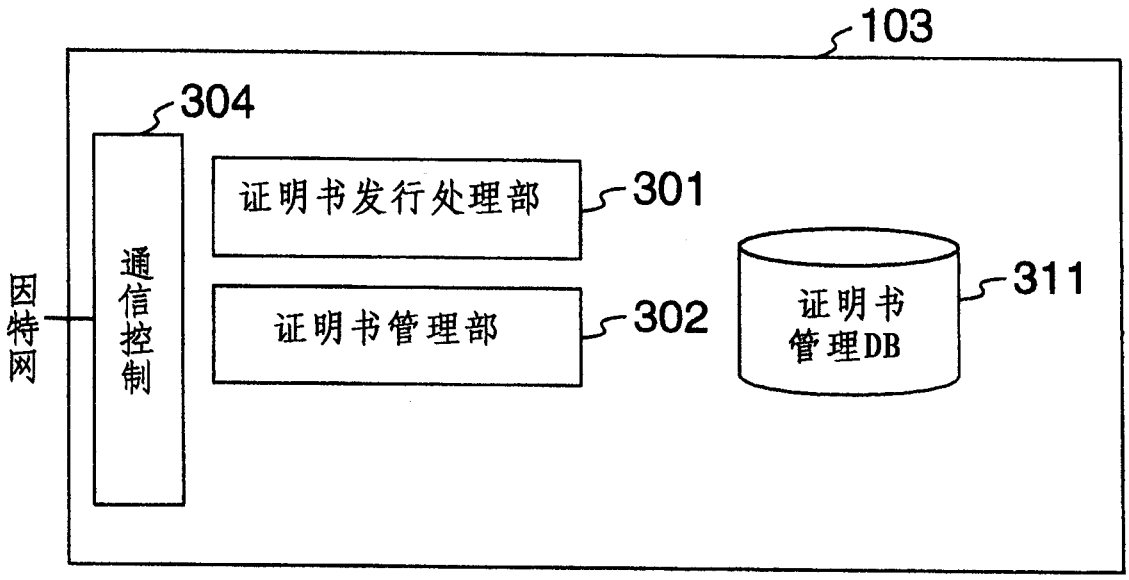

103
304
通信控制
因特网
证明书发行处理部
301
证明书管理部
302
证明书管理DB
311

图 4

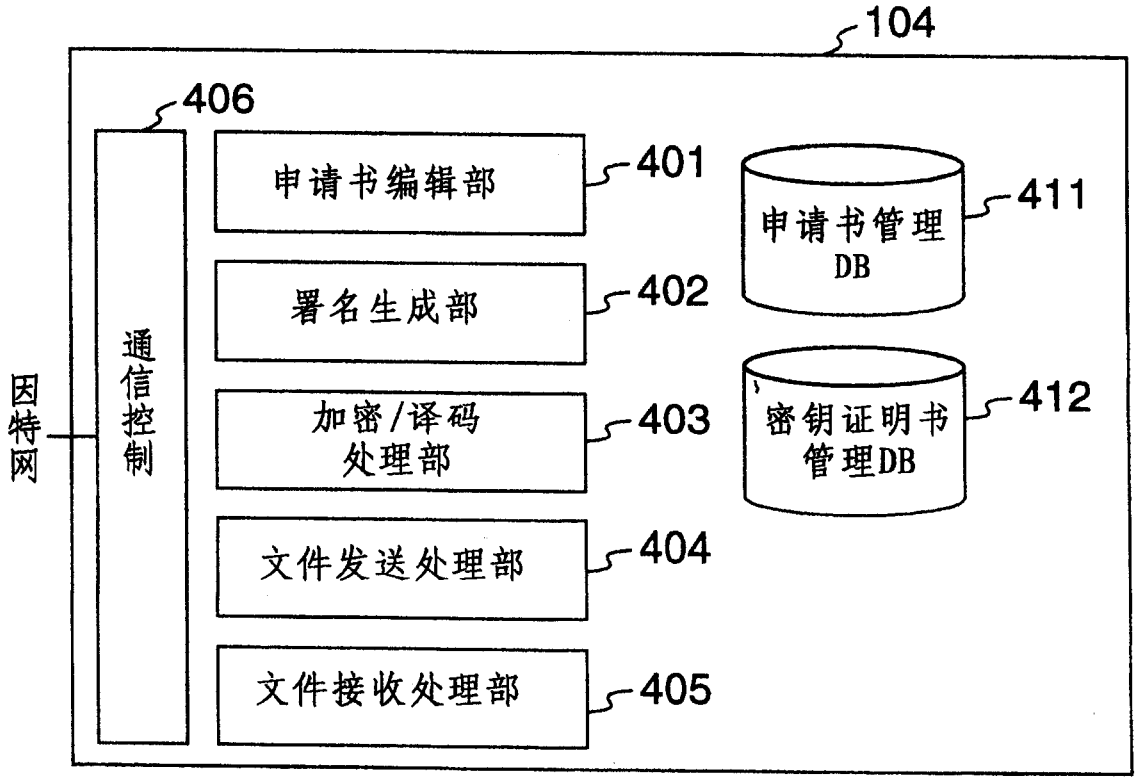

104
406
通信控制
因特网
申请书编辑部
401
署名生成部
402
加密/译码处理部
403
文件发送处理部
404
文件接收处理部
405
申请书管理DB
411
密钥证明书管理DB
412

图 5

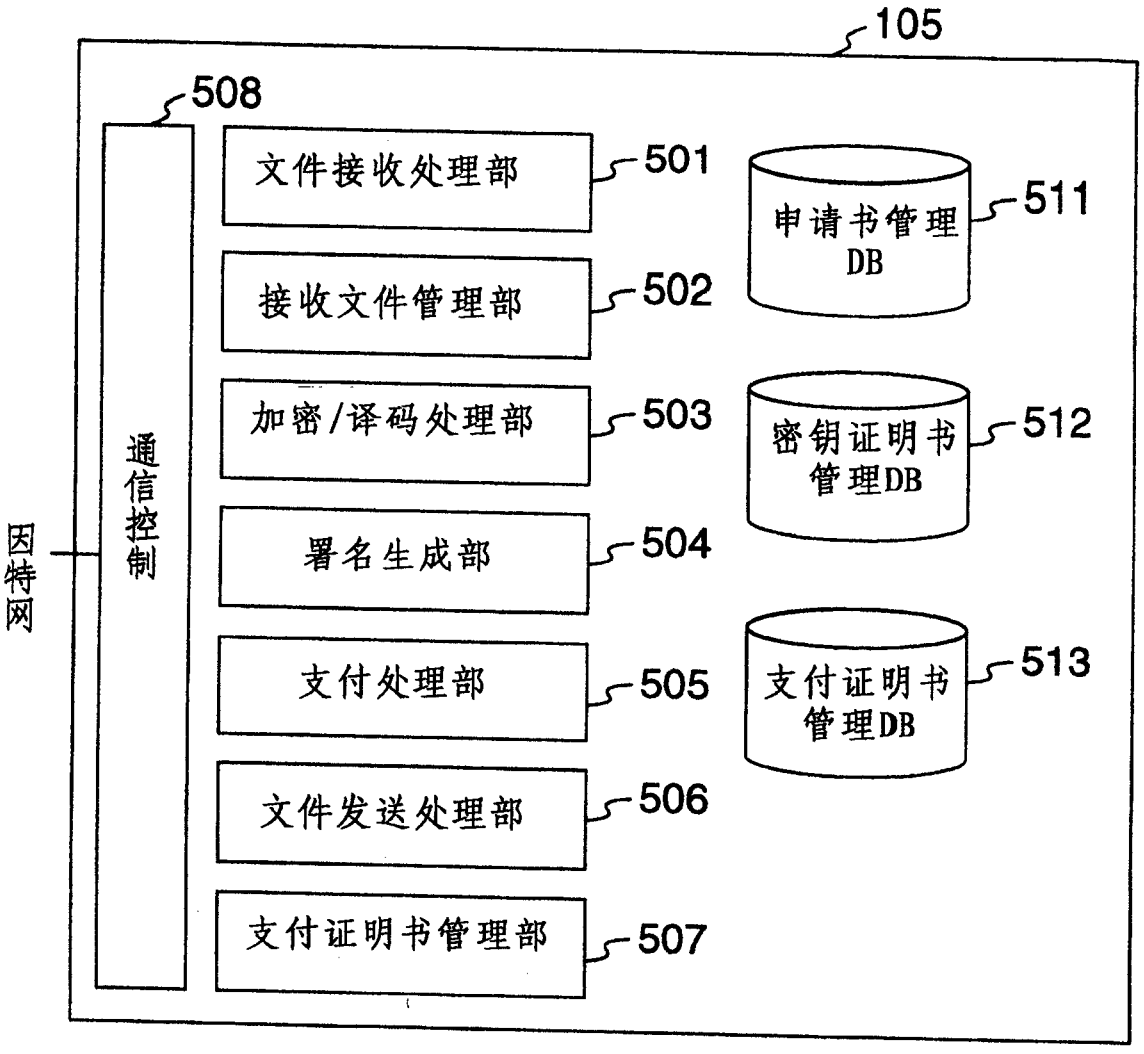

105
508
通信控制
因特网
文件接收处理部
501
接收文件管理部
502
加密/译码处理部
503
署名生成部
504
支付处理部
505
文件发送处理部
506
支付证明书管理部
507
申请书管理DB
511
密钥证明书管理DB
512
支付证明书管理DB
513

图 6

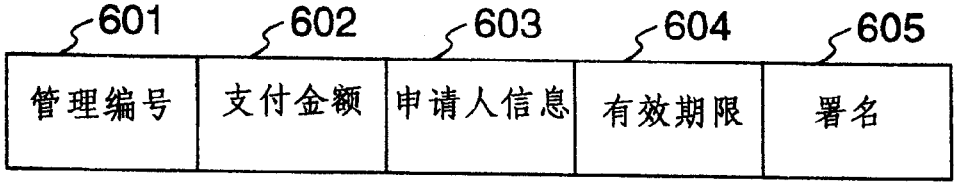

601
602
603
604
605
管理编号
支付金额
申请人信息
有效期限
署名

图 7

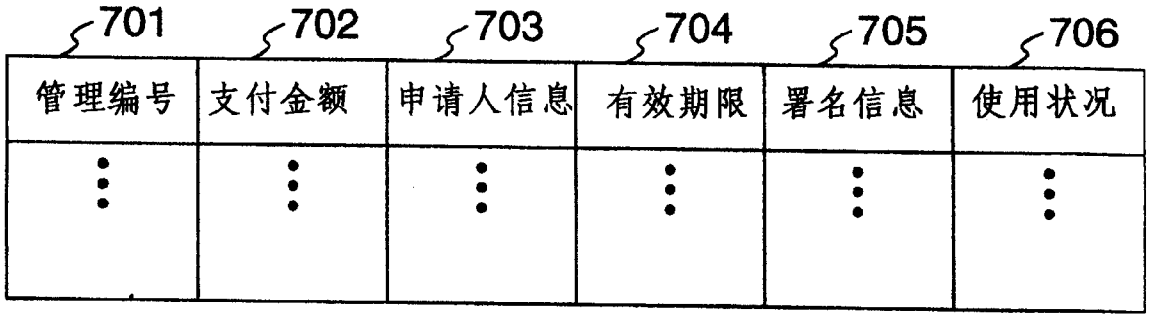

701
702
703
704
705
706
管理编号
支付金额
申请人信息
有效期限
署名信息
使用状况

图 8

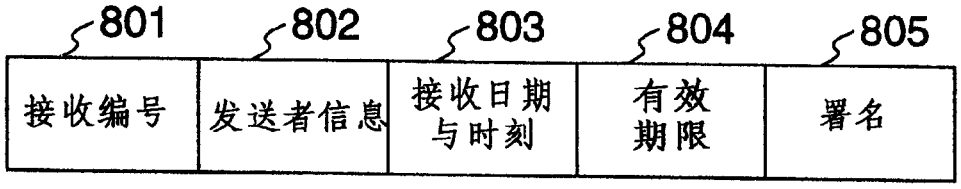

801
802
803
804
805
接收编号
发送者信息
接收日期与时刻
有效期限
署名

图 9

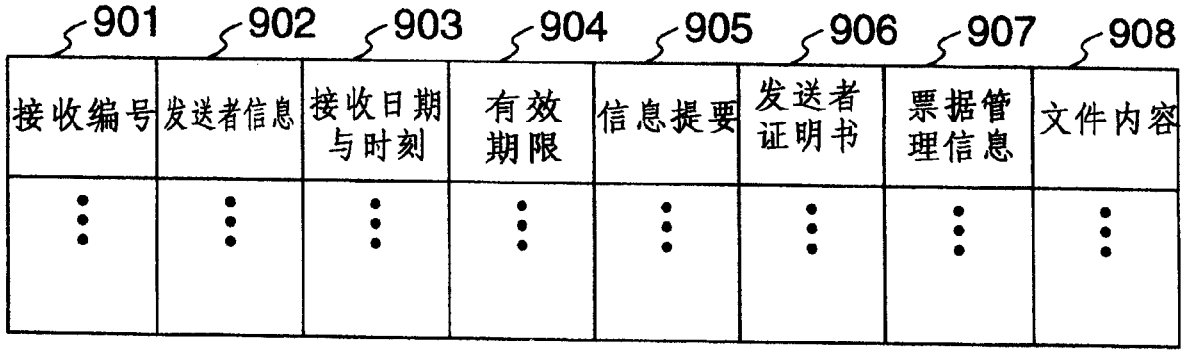

901
902
903
904
905
906
907
908
接收编号
发送者信息
接收日期与时刻
有效期限
信息提要
发送者证明书
票据管理信息
文件内容

图 10

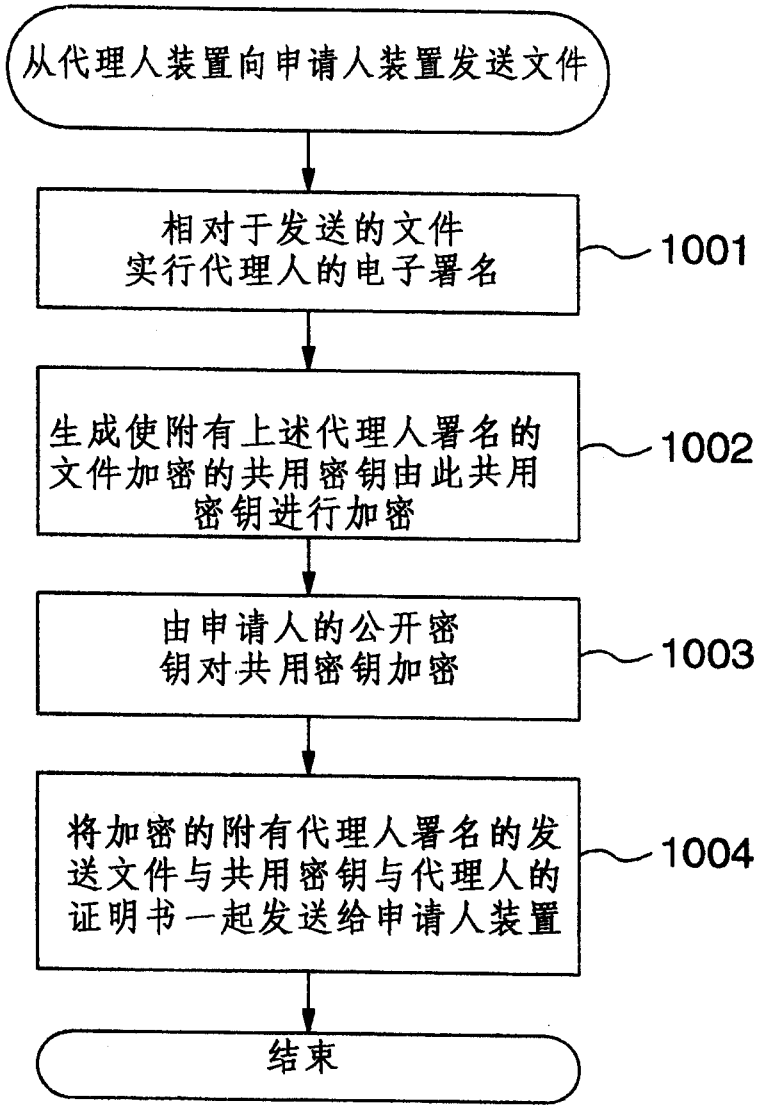

从代理人装置向申请人装置发送文件
相对于发送的文件
实行代理人的电子署名
1001
生成使附有上述代理人署名的
文件加密的共用密钥由此共用
密钥进行加密
1002
由申请人的公开密
钥对共用密钥加密
1003
将加密的附有代理人署名的发
送文件与共用密钥与代理人的
证明书一起发送给申请人装置
1004
结束

图 11

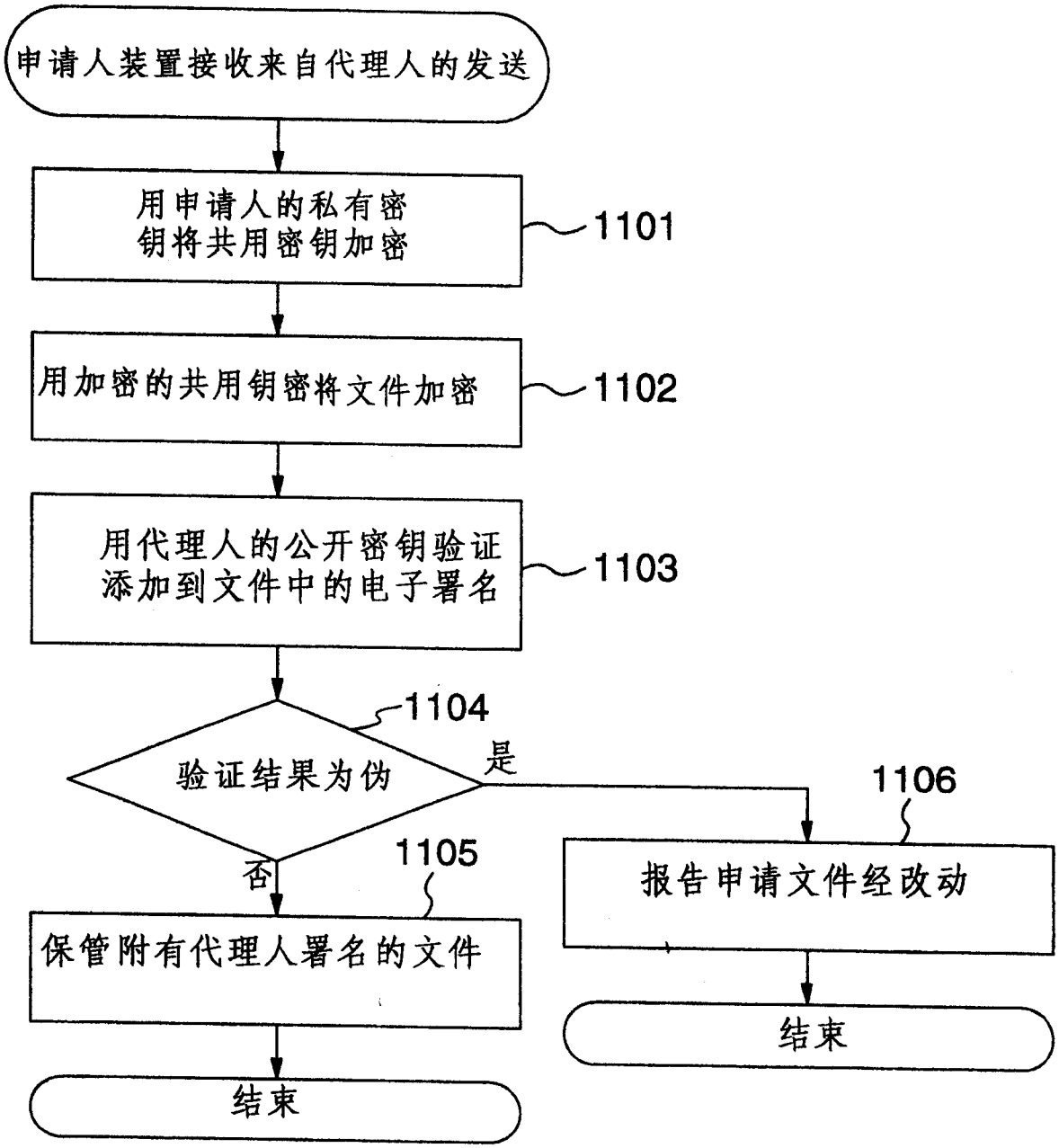

申请人装置接收来自代理人的发送
用申请人的私有密钥将共用密钥加密
1101
用加密的共用钥密将文件加密
1102
用代理人的公开密钥验证添加到文件中的电子署名
1103
1104
验证结果为伪
是
否
1105
1106
保管附有代理人署名的文件
报告申请文件经改动
结束
结束

图 12

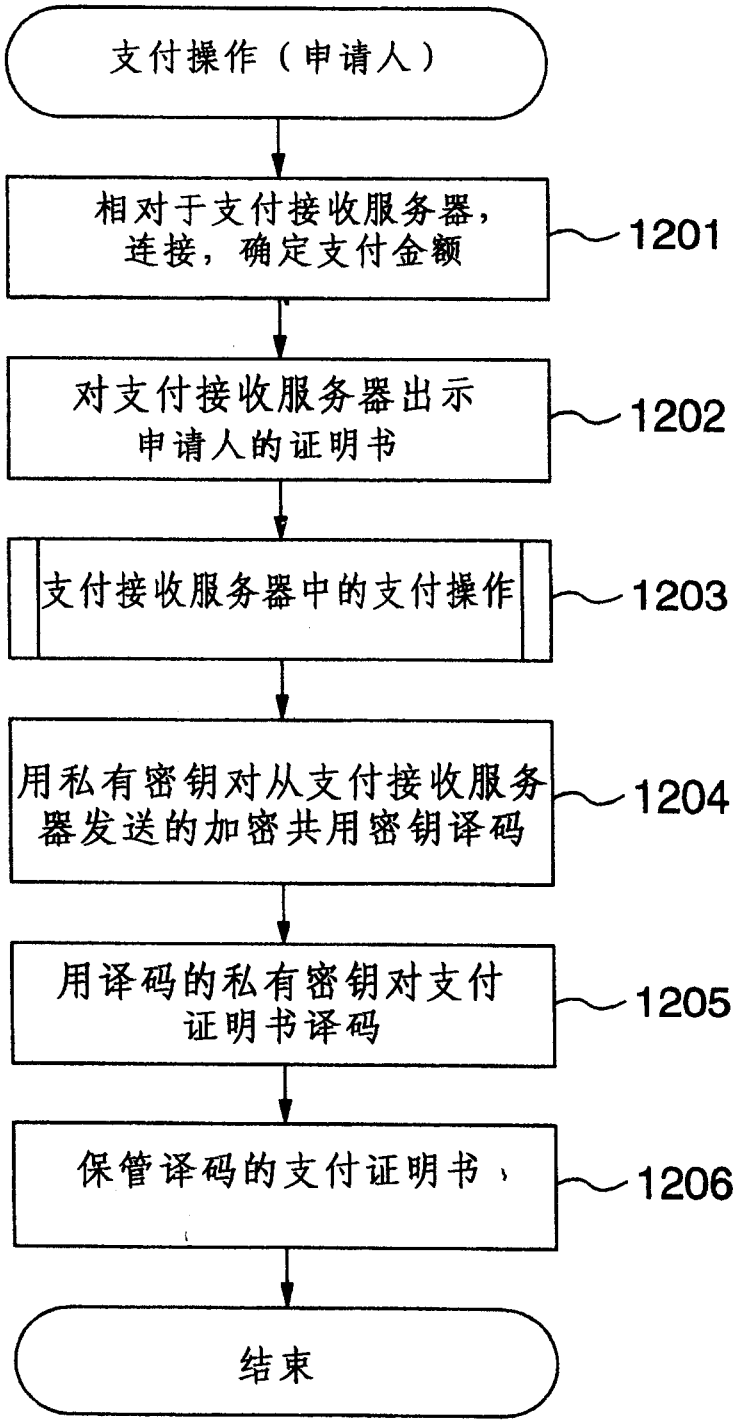

支付操作（申请人）
相对于支付接收服务器，连接，确定支付金额
1201
对支付接收服务器出示申请人的证明书
1202
支付接收服务器中的支付操作
1203
用私有密钥对从支付接收服务器发送的加密共用密钥译码
1204
用译码的私有密钥对支付证明书译码
1205
保管译码的支付证明书，
1206
结束

图 13

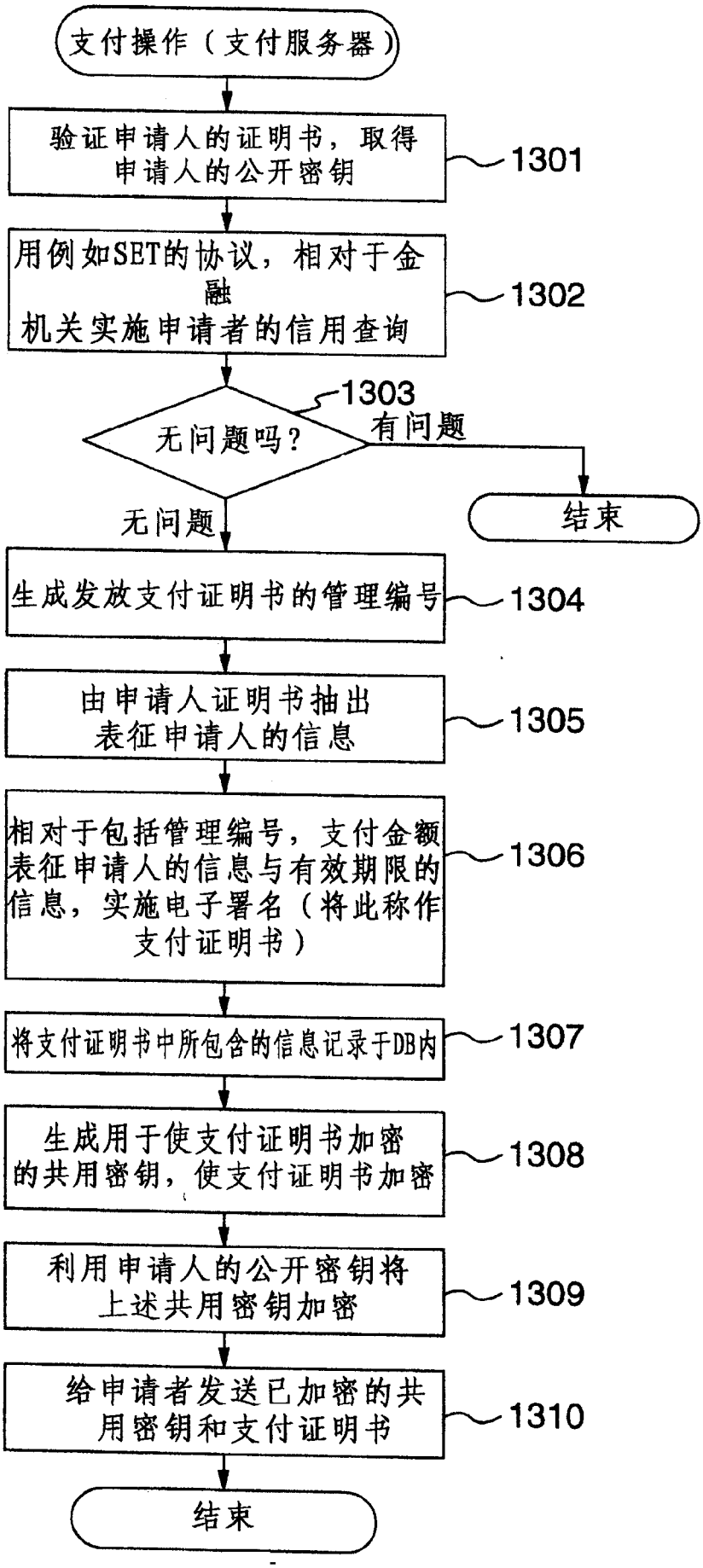

支付操作（支付服务器）
验证申请人的证明书，取得申请人的公开密钥
1301
用例如SET的协议，相对于金融机关实施申请者的信用查询
1302
1303
无问题吗？
有问题
结束
无问题
生成发放支付证明书的管理编号
1304
由申请人证明书抽出表征申请人的信息
1305
相对于包括管理编号，支付金额表征申请人的信息与有效期限的信息，实施电子署名（将此称作支付证明书）
1306
将支付证明书中所包含的信息记录于DB内
1307
生成用于使支付证明书加密的共用密钥，使支付证明书加密
1308
利用申请人的公开密钥将上述共用密钥加密
1309
给申请者发送已加密的共用密钥和支付证明书
1310
结束

图 14

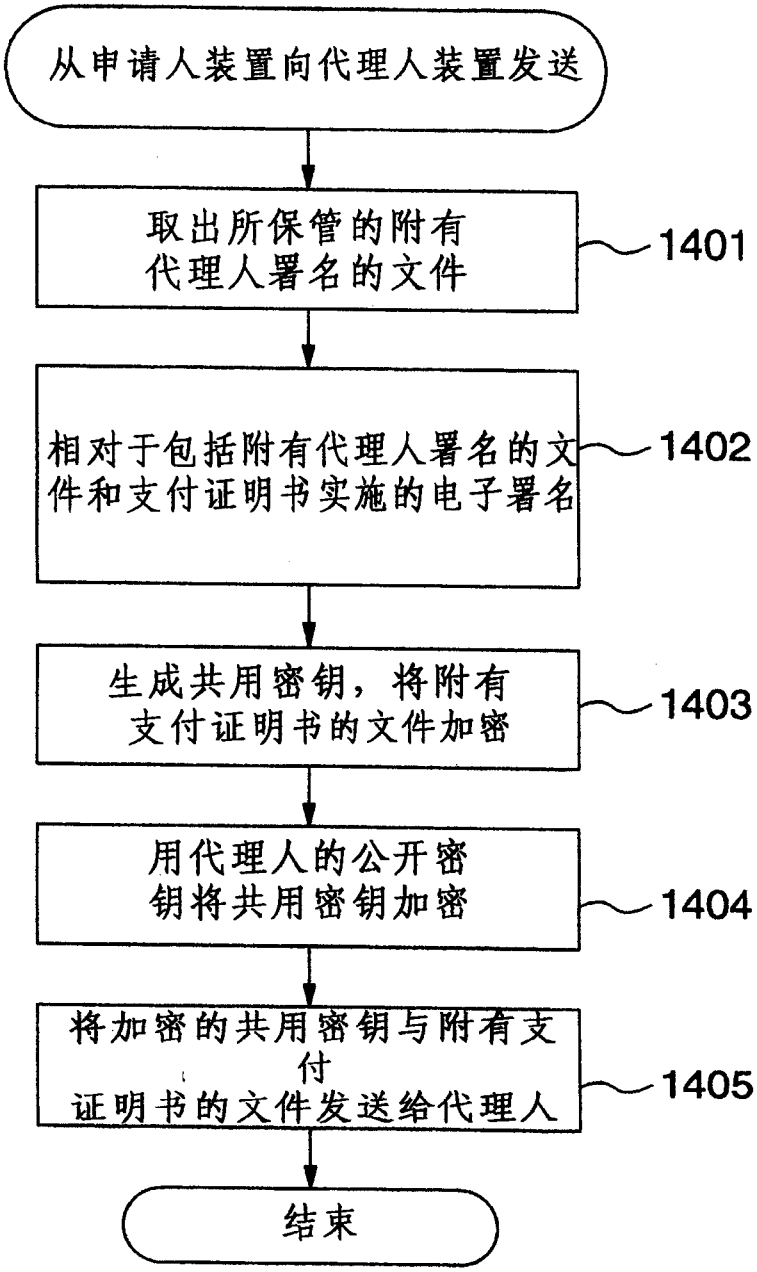

从申请人装置向代理人装置发送
取出所保管的附有代理人署名的文件
1401
相对于包括附有代理人署名的文件和支付证明书实施的电子署名
1402
生成共用密钥，将附有支付证明书的文件加密
1403
用代理人的公开密钥将共用密钥加密
1404
将加密的共用密钥与附有支付证明书的文件发送给代理人
1405
结束

图 15

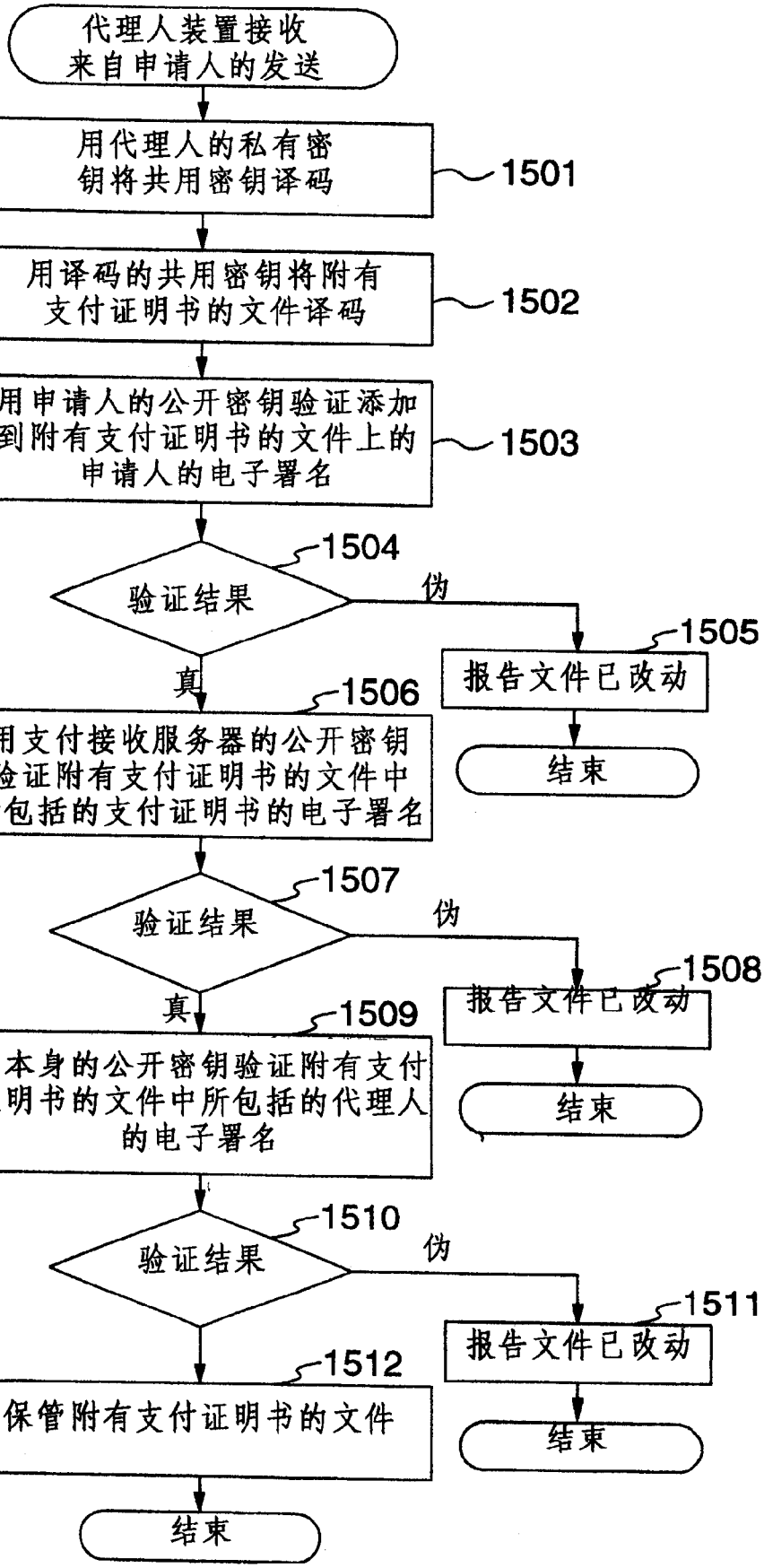

代理人装置接收
来自申请人的发送
用代理人的私有密
钥将共用密钥译码
1501
用译码的共用密钥将附有
支付证明书的文件译码
1502
用申请人的公开密钥验证添加
到附有支付证明书的文件上的
申请人的电子署名
1503
1504
验证结果
伪
1505
报告文件已改动
结束
真
1506
用支付接收服务器的公开密钥
验证附有支付证明书的文件中
所包括的支付证明书的电子署名
1507
验证结果
伪
1508
报告文件已改动
结束
真
1509
用本身的公开密钥验证附有支付
证明书的文件中所包括的代理人
的电子署名
1510
验证结果
伪
1511
报告文件已改动
结束
1512
保管附有支付证明书的文件
结束

图 16

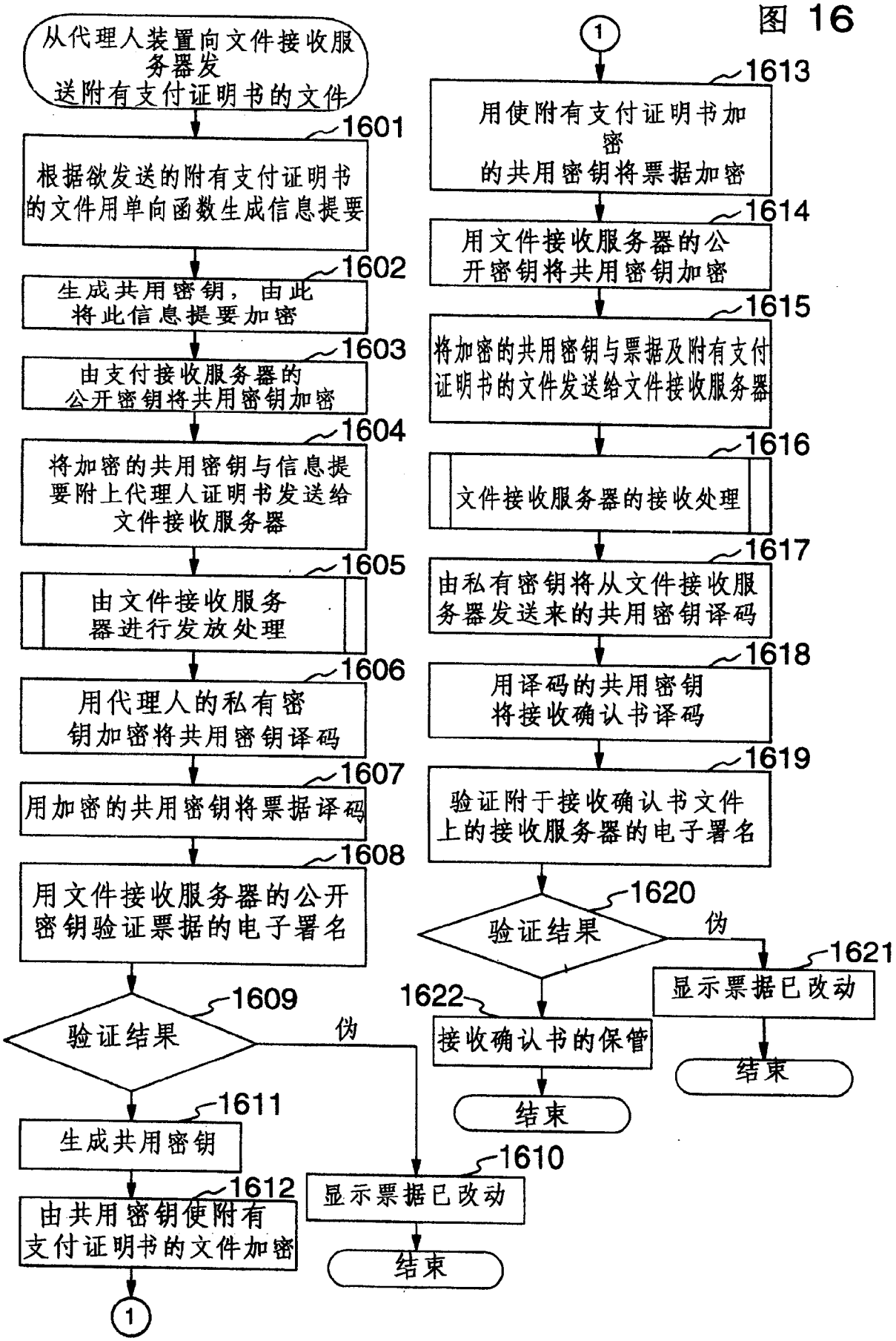

从代理人装置向文件接收服务器发送附有支付证明书的文件
1601
根据欲发送的附有支付证明书的文件用单向函数生成信息提要
1602
生成共用密钥，由此将此信息提要加密
1603
由支付接收服务器的公开密钥将共用密钥加密
1604
将加密的共用密钥与信息提要附上代理人证明书发送给文件接收服务器
1605
由文件接收服务器进行发放处理
1606
用代理人的私有密钥加密将共用密钥译码
1607
用加密的共用密钥将票据译码
1608
用文件接收服务器的公开密钥验证票据的电子署名
1609
验证结果
伪
1610
显示票据已改动
结束
1611
生成共用密钥
1612
由共用密钥使附有支付证明书的文件加密
1
1
1613
用使附有支付证明书加密的共用密钥将票据加密
1614
用文件接收服务器的公开密钥将共用密钥加密
1615
将加密的共用密钥与票据及附有支付证明书的文件发送给文件接收服务器
1616
文件接收服务器的接收处理
1617
由私有密钥将从文件接收服务器发送来的共用密钥译码
1618
用译码的共用密钥将接收确认书译码
1619
验证附于接收确认书文件上的接收服务器的电子署名
1620
验证结果
伪
1621
显示票据已改动
结束
1622
接收确认书的保管
结束

图 17

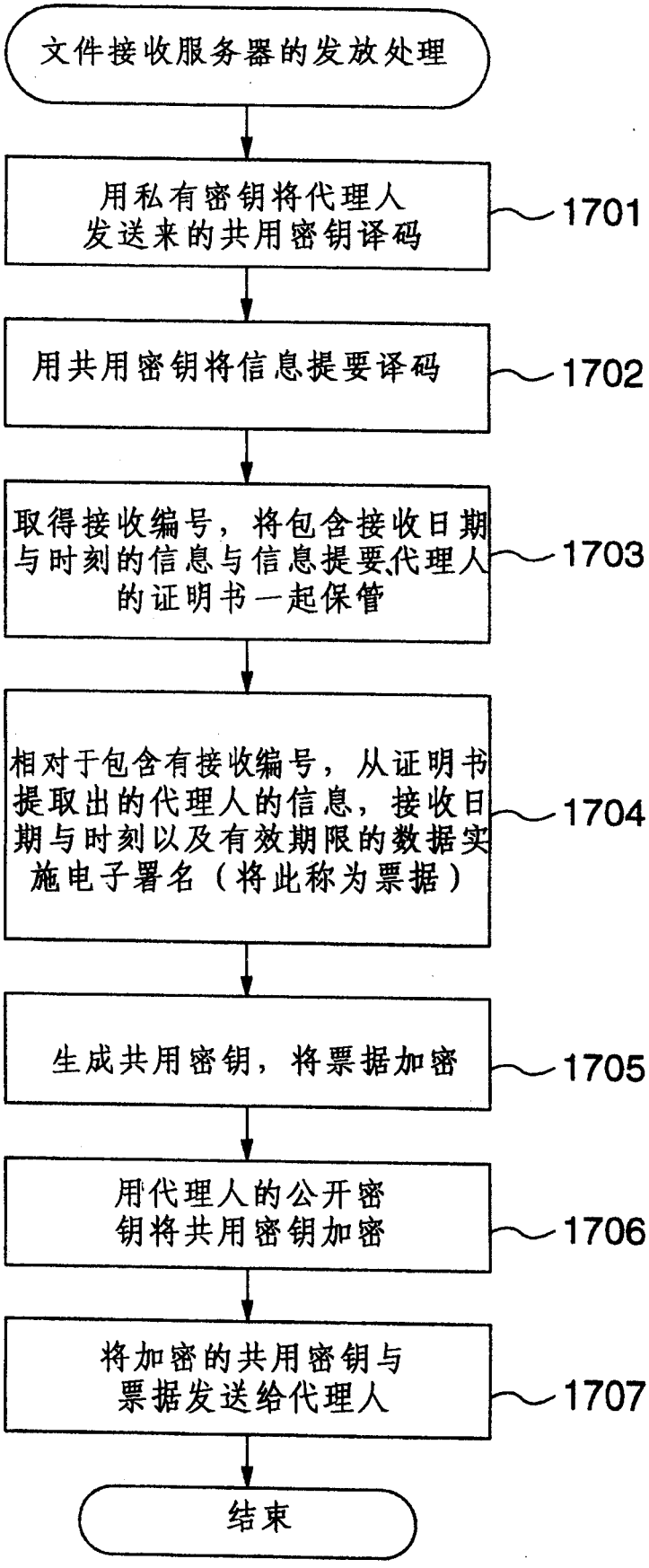

文件接收服务器的发放处理
用私有密钥将代理人发送来的共用密钥译码
1701
用共用密钥将信息提要译码
1702
取得接收编号，将包含接收日期与时刻的信息与信息提要代理人的证明书一起保管
1703
相对于包含有接收编号，从证明书提取出的代理人的信息，接收日期与时刻以及有效期限的数据实施电子署名（将此称为票据）
1704
生成共用密钥，将票据加密
1705
用代理人的公开密钥将共用密钥加密
1706
将加密的共用密钥与票据发送给代理人
1707
结束

图18

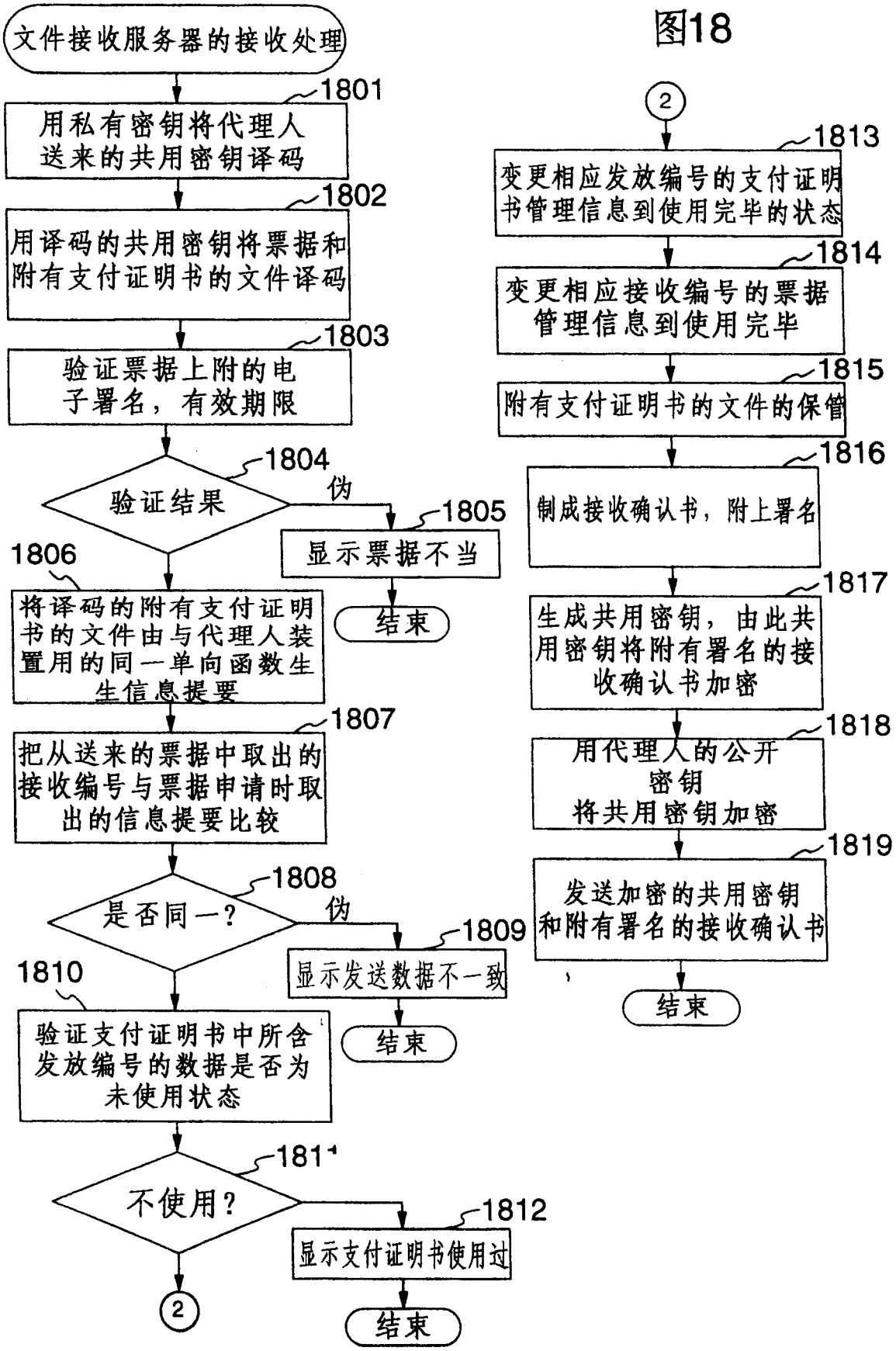
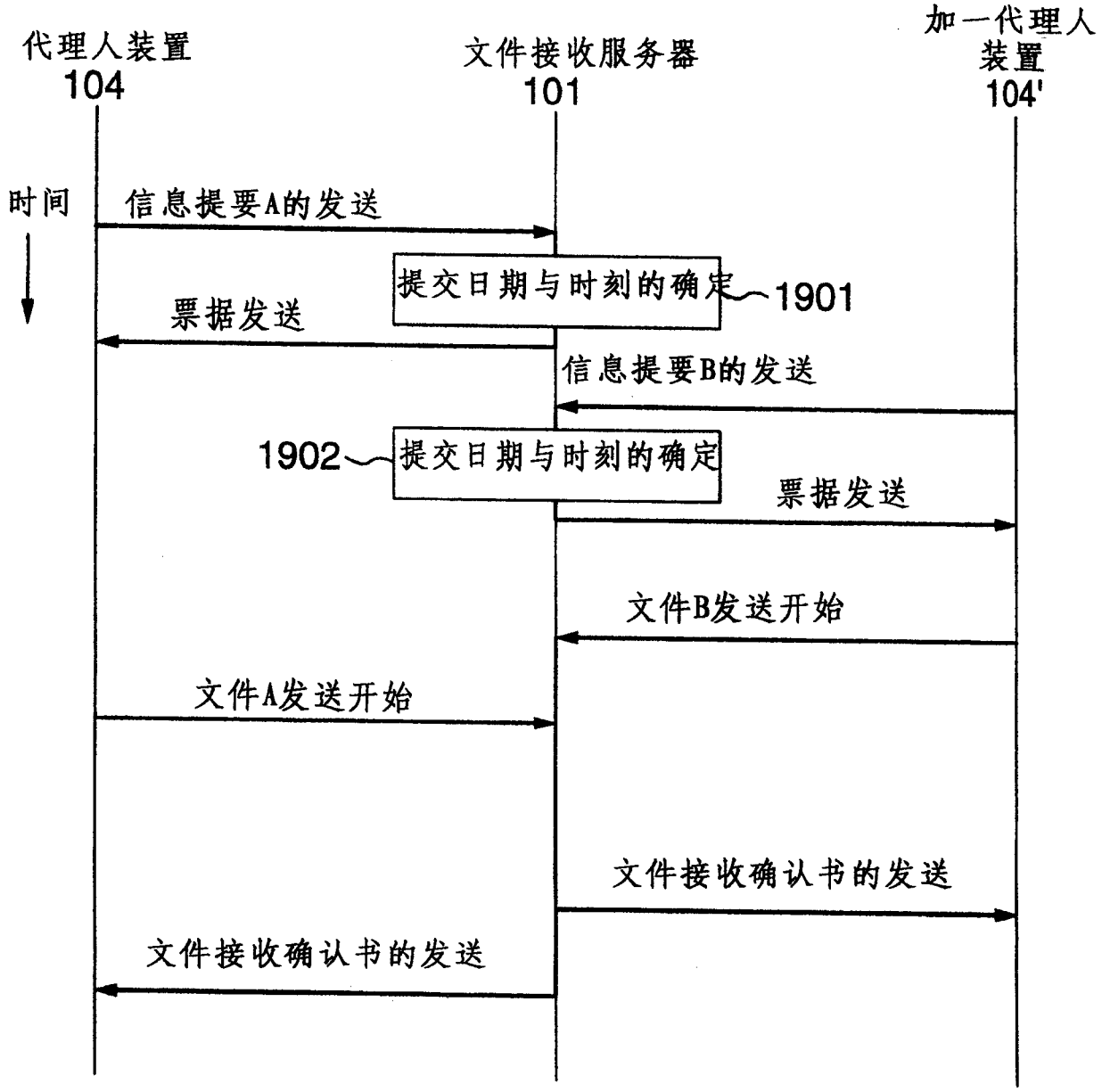

文件接收服务器的接收处理
1801
用私有密钥将代理人送来的共用密钥译码
1802
用译码的共用密钥将票据和附有支付证明书的文件译码
1803
验证票据上附的电子署名，有效期限
1804
验证结果
伪
1805
显示票据不当
结束
1806
将译码的附有支付证明书的文件由与代理人装置用的同一单向函数生生信息提要
1807
把从送来的票据中取出的接收编号与票据申请时取出的信息提要比较
1808
是否同一？
伪
1809
显示发送数据不一致
结束
1810
验证支付证明书中所含发放编号的数据是否为未使用状态
1811
不使用？
1812
显示支付证明书使用过
结束
2
2
1813
变更相应发放编号的支付证明书管理信息到使用完毕的状态
1814
变更相应接收编号的票据管理信息到使用完毕
1815
附有支付证明书的文件的保管
1816
制成接收确认书，附上署名
1817
生成共用密钥，由此共用密钥将附有署名的接收确认书加密
1818
用代理人的公开密钥将共用密钥加密
1819
发送加密的共用密钥和附有署名的接收确认书
结束

图 19


代理人装置
104
文件接收服务器
101
加一代理人
装置
104'
时间
信息提要A的发送
提交日期与时刻的确定
1901
票据发送
信息提要B的发送
1902
提交日期与时刻的确定
票据发送
文件B发送开始
文件A发送开始
文件接收确认书的发送
文件接收确认书的发送