[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200780040018.2

[43] 公开日 2009 年 9 月 9 日

[11] 公开号 CN 101529797A

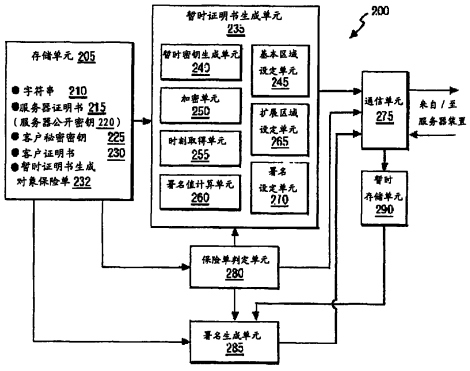
[22] 申请日 2007.10.24
[21] 申请号 200780040018.2
[30] 优先权
[32] 2006.10.27 [33] JP [31] 293253/2006
[86] 国际申请 PCT/JP2007/070706 2007.10.24
[87] 国际公布 WO2008/050792 日 2008.5.2
[85] 进入国家阶段日期 2009.4.27
[71] 申请人 国际商业机器公司
地址 美国纽约
[72] 发明人 冈本康介 宫本隆志
[74] 专利代理机构 北京市柳沈律师事务所
代理人 黄小临
权利要求书 7 页 说明书 19 页 附图 6 页

[54] 发明名称

用于使用包含个人信息的电子证明书来认证通信对方的系统、装置、方法和程序

[57] 摘要

本发明提供一种用于使用包含个人信息的电子证明书来认证通信对方的技术。 客户装置若从服务器装置接收电子证明书的请求，则从存储单元读取包含个人信息的客户证明书和服务器装置的服务器公开密钥，使用服务器公开密钥对客户证明书进行加密。 客户装置还在电子证明书的基本区域设定用于表示该电子证明书为暂时数字证明的规定事项，并在电子证明书的扩展区域设定被加密的客户证明书，从而生成暂时电子证明书。 然后，客户装置将暂时电子证明书发送到服务器装置。



1. 一种认证方法，使用包含个人信息的电子证明书来认证通信对方，

在客户装置中包括:

从服务器装置接收电子证明书的请求的步骤;

响应于所述请求的接收，从存储单元读取包含个人信息的客户证明书和所述服务器装置的服务器公开密钥的步骤;

使用所述服务器公开密钥，对所述客户证明书进行加密的步骤;

在所述服务器装置所支持的格式的电子证明书的第 1 区域设定用于表示该电子证明书为暂时电子证明书的判定信息，并且在第 2 区域设定被加密的所述客户证明书，从而生成所述暂时电子证明书的步骤；以及

将所述暂时电子证明书发送到服务器装置的步骤，

在所述服务器装置中包括:

接收电子证明书的步骤;

从接收的所述电子证明书的所述第 1 区域取出所述判定信息的步骤;

判定所述判定信息是否表示接收的所述电子证明书为所述暂时电子证明书的步骤;

在判定为接收的所述电子证明书是所述暂时电子证明书的情况下，

从所述暂时电子证明书的所述第 2 区域取出被加密的所述客户证明书的步骤;

使用与所述服务器公开密钥对应的服务器秘密密钥对取出的所述客户证明书进行解密的步骤；以及

使用解密的所述客户证明书来认证所述客户装置的步骤。

2. 如权利要求 1 所述的认证方法，其中

在所述服务器装置中，包括:

判定为接收的所述电子证明书不是所述暂时电子证明书的情况下，使用接收的所述电子证明书来认证所述客户装置的步骤。

3. 如权利要求 1 所述的认证方法，其中

包含所述个人信息的客户证明书是通过公共个人认证服务所发行的所述客户装置的电子证明书。

4. 如权利要求 1 所述的认证方法，其中

所述服务器装置所支持的电子证明书的格式是 X.509。

5. 如权利要求 1 所述的认证方法，其中

所述第 1 区域是 X.509 证明书的基本区域，所述第 2 区域是所述 X.509 证明书的扩展区域。

6. 如权利要求 1 所述的认证方法，其中

所述服务器装置所支持的格式的电子证明书的第 1 区域是 X.509 证明书的扩展区域，作为表示电子证明书是暂时电子证明的所述判定信息而利用证明书保险单。

7. 如权利要求 1 所述的认证方法，其中

在所述客户装置中接收的所述电子证明书的请求是 SSL（Secure Socket Layer）或者 TLS（Transport Layer Security）的 Hand Shake 协议的 Certificate Request 消息。

8. 如权利要求 1 所述的认证方法，其中

在所述客户装置中，包括:

在所述第 2 区域还设定规定的字符串和署名值的步骤，所述署名值是使用与在所述客户证明书中记载的客户公开密钥对应的客户秘密密钥，对该规定的字符串的散列值进行加密的值，

在所述服务器装置中，还包括:

在判定为接收的所述电子证明书是所述暂时电子证明书的情况下，通过将根据在所述暂时电子证明书的所述第 2 区域中记载的所述规定的字符串所求出的散列值、与使用从所述客户证明书中取出的所述客户公开密钥对在所述暂时电子证明书的所述第 2 区域中记载的所述署名值进行解密的值进行比较，从而确认通信对方是所述客户证明书的所有者本人的步骤。

9. 如权利要求 1 所述的认证方法，其中

在所述客户装置中，包括:

取得在所述客户装置上的当前时刻的步骤；以及

还在所述第 2 区域设定规定的字符串、表示所述当前时刻的署名时刻以及署名值的步骤，所述署名值是使用与在所述客户证明书中包含的客户公开密钥对应的客户秘密密钥，对所述规定的字符串和所述署名时刻的散列值进行加密的值，

在所述服务器装置中，还包括:

在判定为接收的所述电子证明书是所述暂时电子证明书的情况下，通过将在所述暂时电子证明书的所述第 2 区域中记载的所述规定的字符串和所述署名时刻、与使用从所述客户证明书中取出的所述客户公开密钥对在所述暂时电子证明书的所述第 2 区域中记载的所述署名值进行解密的值进行比较，从而确认通信对方是所述客户证明书的所有者本人的步骤。

10. 如权利要求 9 所述的认证方法，其中

在所述服务器装置中，还包括:

在判定为接收的所述电子证明书是所述暂时电子证明书的情况下，取得在所述服务器装置上的当前时刻的步骤；以及

判断该当前时刻和从所述暂时电子证明书的所述第 2 区域中取出的所述署名时刻之差是否在容许范围内的步骤。

11. 一种用于认证通信对方的方法，是在客户装置中执行的、使用包含个人信息的电子证明书来认证通信对方的方法，所述用于认证通信对方的方法包括:

从服务器装置接收电子证明书的请求的步骤;

响应于所述请求的接收，从存储单元读取包含个人信息的客户证明书和所述服务器装置的服务器公开密钥的步骤;

使用所述服务器公开密钥，对所述客户证明书进行加密的步骤;

在所述服务器装置所支持的格式的电子证明书的第 1 区域设定用于表示该电子证明书为暂时电子证明书的判定信息，并且在第 2 区域设定被加密的所述客户证明书，从而生成所述暂时电子证明书的步骤；以及

将所述暂时电子证明书发送到所述服务器装置的步骤。

12. 一种用于认证通信对方的方法，是在服务器装置中执行的、使用包含个人信息的电子证明书来认证通信对方的方法，所述用于认证通信对方的方法包括:

对客户装置请求客户证明书的步骤;

从所述客户装置接收该客户装置的电子证明书的步骤;

从接收的所述电子证明书的第 1 区域取出判定信息的步骤;

判定所述判定信息是否表示接收的所述电子证明书为包含个人信息的暂时电子证明书的步骤;

在判定为接收的所述电子证明书不是所述暂时电子证明书的情况下，使

用接收的所述电子证明书来认证所述客户装置的步骤;

在判定为接收的所述电子证明书是所述暂时电子证明书的情况下,

从接收的所述电子证明书的第 2 区域取出使用所述服务器装置的服务器公开密钥被加密的客户证明书的步骤;

使用与所述服务器公开密钥对应的服务器秘密密钥对加密的所述客户证明书进行解密的步骤;以及

使用解密的所述客户证明书来认证所述客户装置的步骤。

13. 一种系统,使用包含个人信息的电子证明书来认证通信对方,所述系统包括客户装置和服务器装置,

所述客户装置包括:

接收单元,从服务器装置接收电子证明书的请求;

存储单元,存储包含个人信息的客户证明书和所述服务器装置的服务器公开密钥;

加密单元,响应于所述请求的接收,使用从所述存储单元读取的所述服务器公开密钥,对所述客户证明书进行加密;

生成单元,在所述服务器装置所支持的格式的电子证明书的第 1 区域设定用于表示该电子证明书为暂时电子证明书的判定信息,并且在第 2 区域设定被加密的所述客户证明书,从而生成所述暂时电子证明书;以及

发送单元,将所述暂时电子证明书发送到所述服务器装置,

所述服务器装置包括:

存储单元,存储与所述服务器公开密钥对应的服务器秘密密钥;

接收单元,接收电子证明书;

判定单元,判定从接收的所述电子证明书的所述第 1 区域取出的所述判定信息是否表示接收的所述电子证明书为暂时电子证明书;

解密单元,响应于所述判定单元判定为是暂时电子证明书,从接收的所述电子证明书的所述第 2 区域取出被加密的所述客户证明书,并使用从所述存储单元读取的服务器秘密密钥对该客户证明书进行解密;以及

认证单元,在所述判定单元判定为接收的所述电子证明书是暂时电子证明书的情况下,使用通过所述解密单元解密的所述客户证明书来认证客户装置。

14. 一种客户装置,用于使用包含个人信息的电子证明书来认证通信对

方，所述客户装置包括:

接收单元，从服务器装置接收电子证明书的请求;

存储单元，存储包含个人信息的客户证明书和所述服务器装置的服务器公开密钥;

加密单元，响应于所述请求的接收，使用从所述存储单元读取的所述服务器公开密钥，对所述客户证明书进行加密;

生成单元，在所述服务器装置所支持的格式的电子证明书的第 1 区域设定用于表示该电子证明书为暂时电子证明书的判定信息，并且在第 2 区域设定被加密的所述客户证明书，从而生成所述暂时电子证明书；以及

发送单元，将所述暂时电子证明书发送到所述服务器装置。

15. 一种服务器装置，用于使用包含个人信息的电子证明书来认证通信对方，所述服务器装置包括:

存储单元，存储与服务器公开密钥对应的服务器秘密密钥;

接收单元，从客户装置接收电子证明书;

判定单元，判定从接收的所述电子证明书的第 1 区域取出的判定信息是否表示接收的所述电子证明书为暂时电子证明书;

解密单元，响应于所述判定单元判定为是暂时电子证明书，从接收的所述电子证明书的第 2 区域取出被加密的客户证明书，并使用从所述存储单元读取的服务器秘密密钥进行解密；以及

认证单元，在所述判定单元判定为接收的所述电子证明书不是所述暂时电子证明书的情况下，使用接收的所述电子证明书来认证所述客户装置，而在所述判定单元判定为是暂时电子证明书的情况下，使用通过所述解密单元解密的所述客户证明书来认证所述客户。

16. 一种程序，用于使用包含个人信息的电子证明书来认证通信对方，

所述程序使客户装置执行以下步骤:

从服务器装置接收电子证明书的请求的步骤;

响应于所述请求的接收，从存储单元读取包含个人信息的客户证明书和所述服务器装置的服务器公开密钥的步骤;

使用所述服务器公开密钥，对所述客户证明书进行加密的步骤;

在所述服务器装置所支持的格式的电子证明书的第 1 区域设定用于表示该电子证明书为暂时电子证明书的判定信息，并且在第 2 区域设定被加密的

所述客户证明书，从而生成暂时电子证明书的步骤；以及

将所述暂时电子证明书发送到服务器装置的步骤，

所述程序还使所述服务器装置执行以下步骤：

接收电子证明书的步骤；

从接收的所述电子证明书的所述第 1 区域取出所述判定信息的步骤；

判定所述判定信息是否表示接收的所述电子证明书为所述暂时电子证明书的步骤；

在判定为接收的所述电子证明书是所述暂时电子证明书的情况下，

从接收的所述暂时电子证明书的所述第 2 区域取出被加密的所述客户证明书的步骤；

使用与所述服务器公开密钥对应的服务器秘密密钥对取出的所述客户证明书进行解密的步骤；以及

使用解密的所述客户证明书来认证所述客户装置的步骤。

17. 一种用于认证通信对方的程序，使用包含个人信息的电子证明书来认证通信对方，

所述程序使客户装置执行以下步骤：

从服务器装置接收电子证明书的请求的步骤；

响应于所述请求的接收，从存储单元读取包含个人信息的客户证明书和所述服务器装置的服务器公开密钥的步骤；

使用所述服务器公开密钥，对所述客户证明书进行加密的步骤；

在所述服务器装置所支持的格式的电子证明书的第 1 区域设定用于表示该电子证明书为暂时电子证明书的判定信息，并且在第 2 区域设定被加密的所述客户证明书，从而生成暂时电子证明书的步骤；以及

将所述暂时电子证明书发送到所述服务器装置的步骤。

18. 一种用于认证通信对方的程序，使用包含个人信息的电子证明书来认证通信对方，

所述程序使服务器装置执行以下步骤：

对客户装置请求客户证明书的步骤；

从所述客户装置接收该客户装置的电子证明书的步骤；

从接收的所述电子证明书的第 1 区域取出判定信息的步骤；

判定所述判定信息是否表示接收的所述电子证明书为包含所述个人信息

的暂时电子证明书的步骤;

在判定为接收的所述电子证明书不是所述暂时电子证明书的情况下，使用接收的所述电子证明书来认证所述客户装置的步骤;

在判定为接收的所述电子证明书是所述暂时电子证明书的情况下，

从接收的所述暂时电子证明书的第 2 区域取出使用所述服务器装置的服务器公开密钥被加密的客户证明书的步骤;

使用与所述服务器公开密钥对应的服务器秘密密钥对加密的所述客户证明书进行解密的步骤; 以及

使用解密的所述客户证明书来认证所述客户装置的步骤。

用于使用包含个人信息的电子证明书来认证通信对方的系统、装置、方法和程序

技术领域

本发明涉及使用了电子证明书的通信对方的认证，特别涉及使用包含个人信息的电子证明书来认证通信对方的技术。

背景技术

以往，在电子商务或在线银行等的要求安全的通信的服务器-客户型数据通信中，广泛地利用 SSL（Secure Socket Layer）以及它的后继技术的作为 RFC2246 而以 IETF（Internet Engineering Task Force）标准化的 TLS（Transport Layer Security）。

在 SSL/TLS 的 Hand shake Protocol 中，在加密通信的开始之前，在服务器-客户之间进行用于开始加密通信所需的各种参数的协商。在 Hand shake Protocol 中，最初进行对方的认证，之后根据在客户和服务器两者可共同利用的压缩/加密算法来决定最佳算法的利用。若基于 Hand shake Protocol 的协商正常地结束，则之后在服务器-客户之间开始加密通信。

其中，以服务器装置认证客户装置的情况为例子说明在 Hand Shake Protocol 中的对方认证。在利用公开密钥加密方式的 Hand Shake Protocol 的对方认证中，响应于来自服务器装置的 Certificate Request 消息，客户装置将自身的电子证明书包含在 Client Certicicate 消息的主体中发送到服务器装置。接受到电子证明书的服务器装置使用所保有的来源（route）认证台（C（A））的密钥来确认其合法性。除了公开密钥之外，在电子证明书中还记载了与该公开密钥对应的秘密密钥的所有者（电子证明书的发行对方）信息、公开密钥的有效期限等的书籍信息。因此，服务器装置参照有关书籍信息来确认客户装置为合适的通信对方的情况。

接着，客户装置通过客户装置的秘密密钥对作为 Hand shake Protocol 的开始消息的 Client Hello 消息开始到 Client Key Exchange 消息为止的通信内容的摘要进行加密从而生成署名，并将其包含在 Certificate Verify 消息的主体中

发送到服务器装置中。服务器装置通过在客户装置的电子证明书中记载的公开密钥对包含在 Certificate Verify 消息的主体中的信息进行解密，从而确认当前的通信对方是电子证明书的所有者本人的情况（参照非专利文献 1）。

这样，SSL/TLS 提供的对方认证的功能是非常严谨的，在他人的冒充或篡改成为重大问题的电子政府、电子自治体中，可称为最佳的认证方式。但是，作为电子政府/电子自治体的基础，近年来，开始了公共个人认证服务（参照非专利文献 2）。公共个人认证服务是指，都道府县的长官发行行政机关所提供的、在利用电子申请/申报服务时可使用的电子证明书的服务。电子证明书的发行对于在全国各地居住的人都以便宜的费用进行。因此，期望将通过公共个人认证服务所发行的电子证明书作为 SSL/TLS 的客户证明书来使用。

非专利文献 1：T.Dierks,E.Rescorla,"The TransportLayer Security(TLS)Protocol",[online],平成 16 年 4 月、RFC 4346、[检索平成 18 年 9 月 22 日]、因特网〈URL: http://www.ietf.org/rfc/rfc4346.txt〉

非专利文献 2: "公的個人認証サービス　ポータルサイト"、[online]、平成 16 年 1 月 29 日（开设网站）、公的個人認証サービス都道府県協議会、[检索平成 18 年 9 月 22 日]、因特网〈URL: http://www.jpki.go.jp/ index1.html〉

发明要解决的课题

但是，在通过公共个人认证服务所发行的电子证明书中，记录在居民户口簿上的姓名、地址、出生年月日、性别作为公开密钥的所有者信息而记载。因此，若将其作为 SSL/TLS 的客户证明书来使用，则由于如上所述那样在 SSL/TLS 中在加密通信的开始之前进行对方认证，所以姓名、地址等个人信息不会被加密而直接发送。此外，作为电子证明书的标准，有 ITU（International Telecommunication Union）建议的 X.509。X.509 是在 SSL/TLS 中也采用并已经成为标准规格，但在该规格中没有嵌入可安全地发送记载信息的结构。

因此，本发明的目的在于，提供一种通信对方的认证方法、装置、系统以及程序，其在使用了包含个人信息的电子证明书的通信对方的认证中，防止窃听等的对个人信息的非法访问。本发明的另一目的在于，在使用了包含个人信息的电子证明书的安全的通信对方的认证中，维持了与以往的通信对方的认证方法的互换性。

用于解决课题的手段

为达到上述目的的本发明通过如下所述那样的使用包括个人信息的电子证明书来认证通信对方的方法实现。该方法从客户装置从服务器装置接收电子证明书的请求开始。响应于请求的接收，客户装置从存储单元读取包含个人信息的客户证明书和服务器装置的服务器公开密钥，并使用服务器公开密钥，对包括个人信息的客户证明书进行加密。然后，客户装置在服务器装置所支持的格式的电子证明书的第 1 区域设定用于表示该电子证明书为暂时电子证明书的判定信息，并且在第 2 区域设定被加密的客户证明书，从而生成暂时电子证明书。若生成暂时电子证明书，则客户装置将其发送到服务器装置。

响应于电子证明书的接收，服务器装置从接收的电子证明书的第 1 区域取出判定信息。然后，服务器装置判定判定信息是否表示接收的电子证明书为暂时电子证明书。在判定为接收的电子证明书不是暂时电子证明书的情况下，服务器装置使用接收的电子证明书来认证客户装置。另一方面，在判定为接收的电子证明书是暂时电子证明书的情况下，服务器装置使用在暂时电子证明书的第 2 区域中记载的客户证明书来认证客户装置。在后者的情况下，服务器装置作为前处理，从第 2 区域取出被加密的客户证明书，使用与服务器公开密钥对应的服务器秘密密钥对取出的客户证明书进行解密。

在客户证明书中包含的个人信息是姓名、地址、出生年月日、性别、公司名称、邮件地址等，可确定个人的任意信息。包含个人信息的客户证明书可以是通过公共个人认证服务所发行的客户的电子证明书。此时，在电子证明书中，作为与在该电子证明书中记载的公开密钥对应的秘密密钥的所有者信息，记载了在居民户口簿中记载的姓名、地址、出生年月日、性别。

服务器装置所支持的电子证明书的格式可以是 X.509。优选地，第 1 区域是 X.509 证明书的基本区域，第 2 区域是 X.509 证明书的扩展区域。代替地，也可以是服务器装置所支持的格式的电子证明书的第 1 区域是 X.509 证明书的扩展区域，作为表示电子证明书是暂时电子证明的所述判定信息而利用证明书保险单（policy）。此外，在客户装置中接收的电子证明书的请求可以是 SSL（Secure Socket Layer）或者 TLS（Transport Layer Security）的 Hand Shake Protocol 的 Certificate Request 消息。

此外，客户装置还可以在电子证明书的第 2 区域追加设定规定的字符串

和署名值，所述署名值是使用与在客户证明书中包含的客户公开密钥对应的客户秘密密钥，对该规定的字符串的散列值进行加密的值。此时，服务器装置将判定为接收的电子证明书是暂时电子证明书作为条件，进一步求出在暂时电子证明书的第 2 区域中记载的字符串的散列值。此外，服务器装置使用在客户证明书中记载的客户公开密钥对在暂时电子证明书的第 2 区域中记载的署名值进行解密。然后，通过判定这两个值是否一致，服务器装置确认通信对方是否为客户证明书的所有者本人。

代替地，客户装置还可以在电子证明书的第 2 区域追加设定规定的字符串、表示当前时刻的署名时刻以及署名值，所述署名值是使用与在客户证明书中包含的客户公开密钥对应的客户秘密密钥，对规定的字符串和署名时刻的散列值进行加密的值。当前时刻是署名时在客户装置上取得。此时，服务器装置将判定为接收的电子证明书是暂时电子证明书作为条件，进一步求出在暂时电子证明书的第 2 区域中记载的规定的字符串和署名时刻的散列值。此外，服务器装置使用在客户证明书中记载的客户公开密钥对在暂时电子证明书的第 2 区域中记载的署名值进行解密。然后，通过判定这两个值是否一致，服务器装置确认通信对方是否为客户证明书的所有者本人。

优选地，服务器装置将接收的电子证明书是暂时电子证明书作为条件，在服务器装置上取得当前时刻。然后，服务器装置为了禁止在过去使用的本人确认信息的再次利用，求出当前时刻和在暂时电子证明书的第 2 区域中记载的署名时刻之间的差，并判断求出的差是否在容许范围之内。

以上，作为在包括客户装置和服务器装置的系统中的、用于认证通信对方的方法来说明了本发明，但本发明还能够作为用于认证通信对方的系统或者使该系统执行上述方法的程序来掌握。此外，本发明还能够作为在客户装置或服务器装置中的、用于认证通信对方的方法或者使客户装置或者服务器装置执行该各种方法的程序来掌握。进而，本发明还能够作为用于认证通信对方的客户装置或者服务器装置来掌握。

发明效果

根据本发明，在使用了包含个人信息的电子证明书的通信对方的认证中，防止了窃听等的对个人信息的非法访问。此外，若使用本发明的通信对方的认证技术，还能够维持与以往的通信对方的认证方法的互换性。

附图说明

图 1 表示本发明的一实施方式的用于认证通信对方的系统 100 的结构的一例。

图 2 是表示本发明的一实施方式的客户装置 200 的功能结构的一例。

图 3（a）是表示 X.509 证明书的格式，（b）是表示本发明的实施方式的包含个人信息的客户证明书的一例，（c）是表示本发明的实施方式的暂时电子证明书的一例。

图 4 是表示本发明的一实施方式的服务器装置 400 的功能结构的一例。

图 5（a）是表示在本发明的实施方式的客户装置 200 中的、用于进行通过服务器装置 400 的通信对方认证的处理流程的一例的流程图，（b）是表示本发明的实施方式的暂时电子证明书生成处理的流程的一例的流程图，（c）是表示本发明的实施方式的本人确认信息生成的处理流程的一例的流程图。

图 6（a）是表示在本发明的实施方式的服务器装置 400 中的、用于进行通信对方认证的处理流程的一例的流程图，（b）是表示本发明的实施方式的电子证明书验证的处理流程的一例的流程图，（c）是表示本发明的实施方式的暂时电子证明书验证的处理流程的一例的流程图。

图 7 是表示本发明的实施方式的客户装置 200 以及服务器装置 400 的硬件结构的一例。

具体实施方式

以下，基于附图详细说明用于实施本发明的优选方式，但以下的实施方式并不是限定关于权利要求范围的发明，此外，并不限定在实施方式中说明的特征的组合的全部对于发明的解决手段所必需的。另外，通过实施方式的全部说明，对相同的要素赋予相同的标号。

图 1 是本发明的一实施方式的用于认证通信对方的系统 100 的结构的一例。本实施方式的用于认证通信对方的系统 100 的目的在于，在客户装置 200 响应于来自服务器装置 400 的电子证明书的请求而发送包含自身的个人信息的电子证明书的情况下，防止窃听等对个人信息的非法访问的同时维持与以往的通信对方的认证方法之间的互换性。另外，在本实施方式中，以往的通信对方的认证方法基于 SSL/TLS 的 Handshake Protocol。

用于认证通信对方的系统 100 包括：请求与服务器装置 400 之间的通信

的客户装置200以及为了认证通信对方而请求电子证明书的服务器装置400。客户装置200和服务器装置400是通过因特网等的网络300连接。另外，设为客户装置200预先取得了包含个人信息的客户的电子证明书作为证明自身的电子证明书。

在利用了SSL/TLS的通信中，通信对方的认证是在基于Handshake Protocol的手续的初期进行。服务器装置400首先将包含服务器证明书的Server Certificate消息发送到客户装置200。在服务器证明书中包含基于公开密钥加密方式的服务器的公开密钥。因此，客户装置200在该时刻取得服务器公开密钥。接着，服务器装置400对客户装置200发送Clienet Certificate消息，并对客户装置200请求电子证明书。接收了请求的客户装置200从自身的存储单元读取包含个人信息的客户证明书和服务器装置400的服务器公开密钥，并为了防止对个人信息的非法访问而通过服务器公开密钥对客户证明书进行加密。

被加密的客户证明书在这个状态下在服务器装置400中不被识别为电子证明书。因此，客户装置200生成基于服务器装置400所支持的电子证明书的格式的暂时电子证明书。SSL/TLS作为电子证明书的格式而采用X.509。在X.509中存在多个版本，在当前利用最多的版本3中，除了设置了记载发行者信息或公开密钥等的基本事项的基本区域之外，还新设置了可记载独立信息的扩展区域。因此，客户装置200在X.509证明书的基本区域或者扩展区域设定用于表示该电子证明书为暂时电子证明书的判定信息，此外，通过在X.509证明书的扩展区域设定被加密的客户证明书，从而生成暂时电子证明书。然后，客户装置200在Client Certificate消息中包含暂时电子证明书后发送到服务器装置400。

服务器装置400从客户装置接收包含了暂时电子证明书的Client Certificate消息，并从暂时电子证明书的基本区域或扩展区域取出判定信息。然后，服务器装置400判定判定信息是否表示接收的电子证明书为暂时电子证明书。在判定为接收的电子证明书不是暂时电子证明书的情况下，服务器装置400使用接收的电子证明书来认证客户装置。另一方面，在判定为接收的电子证明书是暂时电子证明书的情况下，服务器装置400从暂时电子证明书的扩展区域取出被加密的客户证明书，通过与服务器公开密钥对应的服务器秘密密钥对其进行解密。然后，服务器装置400使用解密的客户证明书来

认证客户装置。

如上所述，由于客户装置200在服务器装置400所支持的格式的电子证明书中设定用于证明自身的真的电子证明书，所以能够对包含个人信息的客户证明书进行加密而发送，防止了第三者对个人信息的非法访问。此外，由于服务器装置400根据在规定的区域中记载的判定信息来判定接收的电子证明书是否为暂时电子证明书，所以能够根据判定结果来改变应作为用于对方认证的电子证明书的对象，维持了与以往的通信对方的认证方法之间的互换性。

图2是表示本发明的一实施方式的客户装置200的功能结构的一例。客户装置200包括：存储单元205、暂时证明书生成单元235、保险单判定单元280、署名生成单元285以及通信单元275。暂时证明书生成单元235具有生成基于服务器装置400所支持的电子证明书的格式的暂时证明书的功能，并包括：暂时密钥生成单元240、基本区域设定单元245、加密单元250、时刻取得单元255、署名值计算单元260、扩展区域设定单元265以及署名设定单元270。存储单元205存储：包含预先取得的个人信息的客户证明书230；与在该客户证明书230中记载的基于公开密钥加密方式的客户公开密钥对应的客户秘密密钥225；从服务器装置取得的服务器证明书215；规定的字符串210；以及暂时证明书生成对象保险单一览232。

其中，参照图3（a）说明在SSL/TLS中采用的X.509版本3的电子证明书的格式。X.509证明书由大致分为基本区域和扩展区域的两个区域构成。在基本区域中，设定了X.509的版本、证明书的序列号、在证明书的署名上使用的散列/算法以及公开密钥算法（署名方式）、作为证明书的发行者的发行者信息、包含在该基本区域中设定的公开密钥的有效期限以及与它对应的秘密密钥的所有者信息的书籍信息、公开密钥信息。此外，在扩展区域中，可分别任意设定从X.509版本2追加的认证台固有识别信息以及所有者固有识别信息、从X.509版本3追加的扩展型、扩展值以及临界比特（critical bit）的三个组的集合。另外，在扩展型中，除了在X.509版本3中决定的标准的扩展型之外，还可以嵌入独立的新的扩展型。

在X.509证明书中，还赋予了认证台的署名，该认证台的署名是通过认证台的秘密密钥对散列值进行加密的署名，所述散列值是对在基本区域和扩展区域中设定的信息进行散列处理而得到。电子证明书的接收者通过使用认

证台的来源证明书来验证认证台的署名，从而能够确认电子证明书的有效性。即，通过判定对在基本区域和扩展区域中设定的信息进行散列处理而得到的散列值、和使用在认证台的来源证明书中记载的来源公开密钥而解密的认证台的署名是否一致，从而能够确认署名确实通过认证台赋予了的情况以及在基本区域和扩展区域中记载的信息没有受到损伤和篡改的情况。另外，来源证明书是指，发行电子证明书的认证台为了证明其合法性而自己署名发行的电子证明书。

如上所述那样在利用了 SSL/TLS 的通信的认证处理中，存储单元 205 中存储的服务器证明书 220 是从服务器装置 400 发送到客户装置 200 的证明书。因此，本实施方式的服务器证明书 220 是基于 X.509 格式。此外， 在存储单元 205 中存储的包含个人信息的客户证明书 230 在本实施方式中设为是通过公共个人认证服务而发行的证明书。图 3（b）表示通过公共个人认证服务所发行的基于 X.509 格式的客户证明书的一例。在客户证明书的基本区域中，记载了参照图 3（a）而说明那样的信息。另一方面，在客户证明书 230 的扩展区域中，独立地记载了在居民户口簿上记载的姓名、出生年月日、性别、地址。同样在扩展区域中记载的证明书保险单是用于规定证明书的目的和利用用途的单子。其中，表示该证明书是通过公共个人认证服务而发行的信息以 Object Identifier（OID）格式记载。OID 是国际性地注册并且由标准机关承认的被特别格式化的号码，是表示以 ISO 标准注册的特定的对象或对象组。

此外，对客户证明书 230 赋予的署名值 B 是通过都道府县长官而施加的署名。

另外，在公共个人认证服务中，为了防止他人的非法使用，电子证明书和与该电子证明书证明的公开密钥对应的秘密密钥存储在用户的 IC 卡中。因此，在图 2 中表示用于生成暂时证明书所需的信息全部被存储在同一个存储单元 205 中，但客户证明书 230 以及客户秘密密钥 225 实际上存储在 IC 卡中，通过 IC 卡读写器读取。在存储单元 205 中存储的规定的字符串是预先与服务器装置 400 之间规定的字符串，是适合作为署名利用的任意的字符串。此外，在存储单元 205 中存储的暂时证明书生成对象保险单一览 232 是可在包含个人信息的电子证明书中设定的证明书保险单的一览。本实施方式的暂时证明书生成对象保险单一览 232 列表了用于表示是通过公共个人认证服务而发行的证明书保险单。

通信单元（接收单元）275 从服务器装置 400 接收电子证明书的请求，并对保险单判定单元 280 通知消息的接收。保险单判定单元 280 响应于电子证明书的请求的通知，从存储单元 205 读取客户证明书 230 和暂时证明书生成对象保险单一览 232。然后，保险单判定单元 280 判定在客户证明书 230 的扩展区域中记载的证明书保险单是否为在暂时证明书生成对象保险单一览 232 中列表的证明书保险单。

在客户证明书 230 的证明书保险单在暂时证明书生成对象保险单一览 232 中列表的情况下，保险单判定单元 280 对暂时证明书生成单元 235 委托暂时电子证明书的生成。在客户证明书 230 的证明书保险单没有在暂时证明书生成对象保险单一览 232 中列表的情况下，即客户证明书 230 不包含个人信息的情况下，保险单判定单元 280 将从存储单元 205 读取的客户证明书 230 经由通信单元（发送单元）275 原样发送到服务器装置 400。另外，由于本实施方式的客户证明书 230 包含个人信息，所以保险单判定单元 280 对暂时证明书生成单元 235 委托暂时电子证明书的生成。

暂时证明书生成单元 235 响应于来自保险单判定单元 280 的委托，如下开始基于服务器装置 400 所支持的电子证明书的格式，即在本实施方式中是基于 X.509 的暂时电子证明书的生成。由于暂时密钥生成单元 240 用于暂时电子证明书的生成，所以生成基于公开密钥加密方式的一组密钥，即生成暂时公开密钥和与它对应的暂时秘密密钥。基本区域设定单元 245 设定暂时电子证明书的基本区域。作为一例，基本区域设定单元 245 从存储单元 205 读取在服务器证明书 215 中记载的所有者信息，并将其复制到暂时电子证明书的发行者信息的字段中。这样，能够对接收到暂时电子证明书的服务器装置 400 表示该电子证明书是暂时电子证明书的情况。

代替地，也可以利用表示电子证明书为暂时电子证明书的证明书保险单。电子证明书的基本区域的发行者信息的字段或电子证明书的扩展区域的证明书保险单的字段，一般是用于识别电子证明书的种类的目的所使用的字段。因此，在将这些字段用于记载表示电子证明书为暂时电子证明书的信息的情况下，不会像利用独立定义的字段的情况那样电子证明书的内容对第三者意思不明确。基本区域设定单元 245 还在所有者信息的字段设定自身的信息，进而在公开密钥的字段设定暂时密钥生成单元 240 生成的暂时公开密钥。对于基本区域的其他字段，分别设定任意适当的值。

加密单元 250 从存储单元 205 读取在客户证明书 230 以及服务器证明书 215 中记载的服务器公开密钥 220，并使用服务器公开密钥 220 对客户认证书 230 进行加密。时刻取得单元 255 取得在客户装置 200 上的当前时刻。署名值计算单元 260 从存储单元 205 读取字符串 210，并将通过时刻取得单元 255 所取得的当前时刻和字符串作为署名对象，计算署名值。即，署名值计算单元 260 使用散列函数对当前时刻和字符串 210 进行散列处理，并使用在存储单元 205 中存储的客户秘密密钥 225 对得到的散列值进行加密。

用于署名值计算的散列函数也可以预先与服务器装置 400 之间规定，也可以是与用于客户证明书 230 的署名的散列函数相同的函数。此外，也可以利用暂时电子证明书的扩展区域将利用的散列函数信息通知到服务器装置 400。此外，署名值计算单元 260 也可以仅将从存储单元 205 读取的字符串 210 作为署名对象。

扩展区域设定单元 265 在暂时电子证明书的扩展区域设定通过加密单元 250 加密的客户证明书 230。扩展区域设定单元 265 还可以作为本人确认信息而在暂时电子证明书的扩展区域追加设定从存储单元 205 读取的字符串 210、通过时刻取得单元 255 取得的当前时刻（以下，称为“署名时刻”）以及通过署名值计算单元 260 计算的署名值。此外，署名设定单元 270 对暂时电子证明书施以署名。即，署名设定单元 270 在暂时电子证明书中设定使用在服务器证明书 215 中记载的服务器公开密钥 220 对散列值进行加密的署名值，该散列值是对在基本区域和扩展区域中设定的信息进行散列处理而得到的值。

图 3（c）表示通过暂时证明书生成单元 235 所生成的暂时电子证明书的一例。如上所述那样，在本实施方式的暂时电子证明书的发行者信息字段中，记载了表示该电子证明书是暂时数字证明的判定信息（在本实施方式中是服务器装置 400 的信息）。此外，在暂时电子证明书的扩展区域中，记载了已经加密的客户证明书 230 和作为本人确认信息的字符串 210、署名时刻、署名值 C。此外，在暂时电子证明书中，赋予了使用服务器装置 400 的服务器公开密钥而计算的署名值 B。通信单元（发送单元）275 对服务器装置 400 发送通过暂时证明书生成单元 235 所生成的暂时电子证明书作为对于电子证明书的请求的响应。

暂时存储单元 290 暂时存储作为 SSL/TLS 的 Handshake Protocol 的开始

消息的 ClientHello 消息开始到 Client Key Exchange 消息为止的通信内容。署名生成单元 285 使用暂时存储单元 290 存储的上述信息，生成在服务器装置 400 确认通过通信单元（发送单元）275 发送的电子证明书确实是通过客户装置 200 发送的情况时可使用的署名。即，署名生成单元 285 通过从暂时存储单元 290 读取上述通信内容后对其进行散列处理而求出散列值，并通过与在发送它的电子证明书中记载的公开密钥对应的秘密密钥对其进行加密，从而生成署名。然后，署名生成单元 285 将生成的署名与电子证明书一同或者在电子证明书的发送之后，经由通信单元（发送单元）275 而发送到服务器装置 400。

如上所述，根据本发明的实施方式的客户装置 200，由于利用电子证明书的扩展区域而在服务器装置 400 所支持的格式的电子证明书内设定证明自身的真的电子证明书，所以能够以加密的状态发送包含个人信息的客户证明书，能够防止第三者对个人信息的非法访问。

图 4 是表示本发明的一实施方式的服务器装置 400 的功能结构的一例。服务器装置 400 包括：通信单元 405、暂时存储单元 410、判定单元 415、解密单元 420、存储单元 425 以及认证单元 430。存储单元 425 存储服务器秘密密钥 430 和已委托证明书一览 435。其中，服务器秘密密钥 430 是与在发送到客户装置 200 的服务器证明书 215 中记载的服务器公开密钥 220 对应的秘密密钥。此外，已委托证明书一览 435 是多个认证台的来源证明书的一览，假设来源证明书的合法性在服务器装置 400 中是已经确认的。认证单元 430 具有认证通信对方的功能，其包括证明书验证单元 435 和本人确认单元 440。本人确认单元 440 具有用于确认电子证明书确实是从本人发送的功能，其包括署名验证单元 445 和时刻验证单元 450。

通信单元 405 作为对于电子证明书的请求的响应，从客户装置 200 接收电子证明书。接收的电子证明书被存储在暂时存储单元 410 中。判定单元 415 从暂时存储单元 410 读取在电子证明书中记载的判定信息，即在本实施方式中是在电子证明书的基本区域中记载的发行者信息，并判定判定信息是否表示接收的电子证明书为暂时电子证明书。在表示接收的电子证明书是暂时电子证明书的情况下，即在本实施方式中发行者信息表示服务器装置 400 本身的情况下，判定单元 415 将判定结果通知到解密单元 420 和认证单元 430。另一方面，在不表示接收的电子证明书是暂时电子证明书的情况下，判定单

元 415 将判定结果仅通知到认证单元 430。

解密单元 420 响应于接收的电子证明书是暂时电子证明书的通知，从暂时存储单元 410 读取在接收的电子证明书的扩展区域中记载的被加密的客户证明书 230。然后，解密单元 420 使用在存储单元 425 中存储的对应的服务器秘密密钥 430 对读取的客户证明书 230 进行解密。被解密的客户证明书 230 之后被交给认证单元 430。

在判定单元 415 判定为接收的电子证明书不是暂时电子证明书的情况下，认证单元 430 使用接收的电子证明书和与该电子证明书一同或者在该电子证明书之后从客户装置 200 发送的署名，认证客户装置 200。另一方面，在判定单元 415 判定为接收的电子证明书是暂时电子证明书的情况下，认证单元 430 使用解密的客户证明书 230 和在该暂时电子证明书的扩展区域中设定的署名，认证客户装置 200。认证单元 430 的认证处理是响应于来自判定单元 415 的判定结果的通知而开始，进行证明书验证单元 435 和本人确认单元 440 的处理。

与判定单元 415 的判定结果无关，电子证明书的验证方法基本相同。因此在以下，以验证包含个人信息的客户证明书 230 的情况为例子来说明证明书验证单元 435 的处理。另外，在将包含个人信息的客户证明书 230 设为验证对象的情况下，也可以将后述的本人确认单元 440 的处理成功作为条件。

证明书验证单元 435 从解密单元 420 接收被解密的客户证明书 230，并进行电子证明书的验证，即对客户证明书 230 赋予的署名的验证和在客户证明书 230 中记载的书籍信息的确认。署名的验证如下那样进行。首先，参照在客户证明书 230 中记载的发行者信息，从在存储单元 425 中存储的已委托证明书一览 435 中检索对应的认证台（在本实施方式中是都道府县长官）的来源认证书。接着，使用在来源证明书中记载的来源公开密钥对在客户证明书 230 中赋予的署名进行解密。然后，将其与对在客户证明书 230 的基本区域和扩展区域中记载的信息进行散列处理而得到的散列值进行比较，判定是否一致。在两个一致的情况下，验证成功。另外，可通过在客户证明书 230 中记载的署名方式来确认用于署名的算法。

接着，在客户证明书 230 中记载的书籍信息的确认中，作为一例包括客户证明书 230 的有效期限和失效的确认，还有参照了所有者信息或个人信息的通信对方的确认。其中，说明确认客户证明书的失效的方法。在认证台将

电子证明书的失效通知到用户的方法有两种，一种是定期地公开失效的证明书的列表的 Certificate Revocation List（CRL）方法，一种是保持了证明书的失效信息的服务器回答来自客户的证明书的失效信息的查询的 Online Certificate Status Protocol（OCSP）方法。在公共个人认证服务中采用前面的方法，因此在本实施方式中，认证书验证单元 435 对认证台请求 CRL，通过判定在接收的 CRL 中是否列表了客户证明书来确认失效。另外，上述参照了的个人信息的通信对方的确认仅限于将包含个人信息的客户证明书 230 作为验证对象的情况。

本人确认单元 440 确认验证对象的电子证明书确实由客户证明书 230 的所有者发送的情况。在判定单元 415 判定了接收的电子证明书是暂时电子证明书的情况下，署名验证单元 445 从暂时存储单元 410 读取在暂时电子证明书的扩展区域中记载的本人确认信息，并进行署名的验证。如下那样进行使用了本人确认信息的署名的验证。首先，使用预先在与客户装置 200 之间制定的散列函数对在本人确认信息中包含的字符串 210 和署名时刻进行散列处理，从而得到散列值。接着，使用在解密的客户证明书 230 中记载的客户公开密钥对在本人确认信息中包含的署名值 C 进行解密。最后，比较解密的署名值 C 和上述散列值。若两者一致，则称为客户证明书 230 确实是由客户证明书 230 的所有者发送的证明书。

另一方面，在判定单元 415 判定为接收的电子证明书不是暂时电子证明书的情况下，署名验证单元 445 对与电子证明书一同或者在电子证明书的接收之后从客户装置 200 发送的署名进行验证处理。在客户装置 200 的功能结构的说明中，如上所述那样在 SSL/TLS 的 Handshake Protocol 中的对方认证中，作为本人确认信息，利用作为 Handshake Protocol 的开始消息的 ClientHello 消息开始到 Client Key Exchange 消息为止的通信内容。然后，将通过与在电子证明书中记载的公开密钥对应的秘密密钥对该通信内容的散列值进行加密而计算的署名值加入到在 ClientCertificate 消息之后发送的 CertificateVerify 消息的主体后从客户装置 200 发送。

其中，在接收的电子证明书原样成为验证对象的情况下，署名验证单元 445 如下那样进行署名验证。在通信单元 405 中若从客户装置 200 接收 CertificateVerify 消息，则署名验证单元 445 经由暂时存储单元 410 读取在 CertificateVerify 消息主体中包含的署名值。然后，署名验证单元 445 通过在

从客户装置 200 接收的电子证明书中记载的公开密钥对署名值进行解密。此外，暂时存储单元 410 暂时存储从 ClientHello 消息开始到 Client Key Exchange 消息为止的通信内容。其中，署名验证单元 445 从暂时存储单元 410 读取这些通信内容从而求出散列值，并与解密的署名值进行比较。若两者一致，则称为接收的电子证明书确实是由该电子证明书的所有者发送的证明书。

另外，在本实施方式中，由于维持与以往的通信对方的认证方法，即 SSL/TLS 的 Handshake Protocol 中的对方认证之间的互换性，所以即使在将暂时电子证明书发送到服务器装置 400 的情况下，也设为客户装置 200 生成 CertificateVerify 消息而发送到服务器装置 400。此时使用的客户的秘密密钥是与在暂时电子证明书中记载的暂时公开密钥对应的暂时秘密密钥。其中，服务器装置 400 无需验证在 CertificateVerify 消息主体中包含的署名。

在暂时电子证明书的扩展区域中还记载署名时刻的情况下，本人确认单元 440 也可以确认在暂时电子证明书的扩展区域中记载的本人确认信息不是再利用的信息。此时，时刻验证单元 450 首先取得在服务器装置 400 上的当前时刻。然后，计算当前时刻和在暂时电子证明书的扩展区域中记载的署名时刻之差，并判定求出的差是否在容许范围内。在容许范围内的情况下，称为本人确认信息不是再利用的信息。这样，通过在署名中包含署名时刻来禁止本人确认信息的再利用，从而能够防止窃听暂时电子证明书而窃取了本人确认信息的第三者生成假的暂时电子证明书。

如上所述，根据本发明的实施方式的服务器装置 400，由于在从客户装置 200 接收到电子证明书的情况下，首先使用在电子证明书的规定区域中记载的判定信息来判定接收的电子证明书是否为暂时电子证明书，所以可根据判定结果来改变应作为用于对方认证的电子证明书的对象。即，根据本发明的实施方式的服务器装置 400，可处理被加密的电子证明书和普通的没有加密的电子证明书的两种证明书，可维持与以往的通信对方的认证方法之间的互换性。

接着，参照图 5 的流程图，说明本实施方式的客户装置 200 的动作。图 5（a）是表示响应于来自服务器装置 400 的电子证明书的请求而发送电子证明书为止的客户装置 200 的处理的流程。若从服务器装置 400 接收用于认证客户装置 200 的电子证明书的请求（步骤 500），则客户装置 200 从存储单元 205 读取应发送到服务器装置 400 的客户证明书 230 和暂时证明书生成对

象保险单一览232（步骤503）。然后，客户装置200从客户证明书230的扩展区域取出证明书保险单（步骤 506），并判断读取的证明书保险单是否在暂时证明书生成对象保险单一览232中列表（步骤509）。

在取出的证明书保险单在暂时证明书生成对象保险单一览232中列表的情况下（步骤 509: 是），开始用于生成暂时电子证明书的前准备。即，客户装置200首先从存储单元205读取服务器证明书215（步骤512），并从读取的服务器证明书 215 取出所有者信息和服务器公开密钥（步骤 515）。此外，客户装置 200 为了用于暂时电子证明书而生成基于公开密钥方式的一组密钥，即暂时公开密钥和暂时秘密密钥（步骤518）。

若前准备结束，则客户装置200使用准备的信息而生成基于服务器装置400所支持的电子证明书的格式的暂时电子证明书（步骤521）。暂时电子证明书的生成方法在后面叙述。若将生成的暂时电子证明书发送到服务器装置400（步骤524），则客户装置200使用与在暂时电子证明书中记载的暂时公开密钥对应的暂时秘密密钥生成署名，并将其发送到服务器装置 400（步骤527）。

另一方面，在步骤509为否的情况下，即在取出的证明书保险单没有在暂时证明书生成对象保险单一览232中列表而在客户证明书230中没有包含个人信息的情况下，客户装置200将从存储单元205读取的客户证明书230原样发送到服务器装置400（步骤530）。然后，客户装置200使用与在客户证明书 230 中记载的客户公开密钥对应的客户秘密密钥生成署名，并将其发送到服务器装置400（步骤536）。步骤527或者步骤533的后处理结束。

参照图5（b）说明暂时电子说明书生成处理的流程。客户装置200首先使用在图5（a）的步骤515以及518中准备的信息，进行暂时电子证明书的基本区域的设定（步骤 540）。即，在发行者信息的字段设定用于表示服务器装置 400 的所有者信息，还在公开密钥信息的字段设定暂时公开密钥。对于其他字段，分别设定任意合适的值。接着，客户装置200使用在图5（a）的步骤 515 所取得的服务器公开密钥，对包含个人信息的客户证明书进行加密（步骤 545）。此外，客户装置 200 为了表示客户证明书确实是由其所有者发送的情况而生成本人确认信息（步骤 550）。本人确认信息的生成方法在后面叙述。然后，客户装置200在暂时电子证明书的扩展区域设定已加密的客户证明书和本人确认信息（步骤 555）。最后，客户装置 200 使用服务

器公开密钥220对暂时电子证明书施以署名（步骤560）。然后，处理结束。

参照图5（c）说明本人确认信息的生成方法的处理流程。客户装置200从存储单元205读取预先在与服务器装置400之间制定的字符串(步骤570)。接着，客户装置200取得客户装置200上的当前时刻（步骤575）。然后，将读取的字符串和当前时刻作为署名对象，使用与在客户证明书230中记载的客户公开密钥对应的客户秘密密钥计算署名值（步骤580）。然后，处理结束。

接着，参照图6的流程图，说明本实施方式的服务器装置400的动作。图6（a）表示服务器装置400的处理流程的概要。服务器装置400为了认证作为通信对方的客户装置200，对客户装置200发送电子证明书的请求（步骤600）。若从客户装置200接收电子证明书（步骤603），服务器装置400验证该证明书（步骤606）。接着，服务器装置400从客户装置200接收署名（步骤609）。服务器装置400验证署名，并确认接收的电子证明书确实是从该电子证明书的所有者发送的情况（步骤612）。然后，处理结束。

参照图6（b）说明服务器装置400验证电子证明书的处理流程。首先，电子证明书400从接收的电子证明书的基本区域取出发行者信息(步骤615)，并判定接收的电子证明书是否为暂时电子证明书（步骤620）。在判定为是暂时电子说明书的情况下（步骤620：是），服务器装置400验证暂时电子证明书（步骤625）。暂时电子证明书的验证在后面叙述。在步骤630中，在暂时电子证明书的验证成功的情况下，服务器装置400将在暂时电子证明书内包含的客户证明书230识别为用于认证客户装置200的验证对象（步骤635）。另一方面，在判定为接收的电子证明书不是暂时电子证明书的情况下（步骤620：否），服务器装置400将接收的电子证明书本身识别为用于认证客户装置200的验证对象（步骤637）。

然后，处理从步骤635或步骤637进入步骤640，服务器装置400验证对验证对象的证明书施以的署名（步骤640）。在步骤640中验证成功的情况下，服务器装置400根据在验证对象的证明书中记载的有效期限验证证明书还有效的情况（步骤645）。在步骤645中验证成功的情况下，服务器装置400与验证对象的证明书的发行者进行通信，验证证明书没有失效（步骤650）。在步骤650中验证成功的情况下，服务器装置400参照在验证对象的证明书中记载的所有者信息，验证客户装置200是合适的通信对方（步骤

652）。在步骤 652 中的验证的成功表示电子证明书的验证的成功。另外，验证的顺序并不限定于如图 6（b）所示的顺序。

在步骤 630 中暂时电子证明书的验证失败的情况下，或者在步骤 640、645、650 以及 652 的任一个步骤中验证失败的情况下，处理进至步骤 660，将验证失败的情况通知到客户装置 200。为了通知验证的失败，在 SSL/TLS 中利用 Alert Protocol。例如，在到了证明书的有效期限的情况下，将 Certificate_expired 消息发送到客户装置 200。此外，在证明书失效的情况下，将 Certificate_revoked 消息发送到客户装置 200。

参照图 6(c)说明服务器装置 400 的暂时电子证明书的验证处理的流程。首先，服务器装置 400 从暂时电子证明书的扩展区域取出被加密的客户证明书 230（步骤 665），并使用从存储单元 425 读取的服务器秘密密钥 430 对客户证明书 230 进行解密（步骤 670）。接着，服务器装置 400 从暂时电子证明书的扩展区域取出作为本人确认信息而记载的署名对象，即字符串和署名时刻（步骤 675），并使用规定的散列函数求出署名对象的散列值。服务器装置 400 还从暂时电子证明书的扩展区域取出作为本人确认信息而记载的署名值（步骤 680）。服务器装置 400 使用在解密的客户证明书中记载的客户公开密钥对取出的署名值进行解密，将其与散列值进行比较从而验证署名（步骤 685）。

在步骤 690 中验证成功的情况下，即可确认客户证明书 230 确实是从客户证明书 230 的所有者发送的情况下，服务器装置 400 还取得服务器装置 400 上的当前时刻（步骤 695）。然后，服务器装置 400 计算取得的当前时刻和在暂时电子证明书的扩展区域中记载的署名时刻之差（步骤 700）。在计算的差在容许范围内的情况下（步骤 705: 是），即可确认在暂时电子证明书的扩展区域中记载的本人确认信息不是再利用的信息的情况下，服务器装置 400 保存验证成功（步骤 710）。在步骤 740 中署名验证失败的情况下或者在步骤 705 中计算的差不在容许范围内的情况下，服务器装置 400 保存验证失败（步骤 715）。然后，处理结束。

图 7 是表示本实施方式的客户装置 200 的硬件结构的一例。图 7 也是服务器装置 400 的硬件结构的一例。以下，作为客户装置 200 的硬件结构说明图 7。客户装置 200 包括：CPU 周边单元，包含通过主控制器 715 而相互连接的 CPU710 以及 RAM730；输入输出单元，包含通过输入输出控制器 735

而连接到主控制器 715 的卡总线控制器 740 以及连接到卡总线控制器 740 的 IC 卡读写器 745、通信接口 770、硬盘驱动 760 以及 CD-ROM 驱动 760；以及传统（legacy）输入输出单元，包含连接到输入输出控制器 735 的超 I/O 控制器 780 以及连接到超 I/O 控制器 780 的软磁盘驱动 790、闪速 ROM800 以及键盘鼠标控制器 810。

主控制器 715 将以高转速访问 RAM730 的 CPU710 与 RAM730 连接。CPU710 基于存储在硬盘的程序而动作，进行各个部分的控制。本发明的实施方式的用于认证通信对方的客户装置 200 用的程序存储在硬盘中，并使用 RAM730 而由 CPU710 执行。客户装置 200 用的程序使客户装置 200 作为存储单元 205、保险单判定单元 280、署名生成单元 285、暂时存储单元 290、暂时证明生成单元 235，即作为暂时密钥生成单元 240、基本区域设定单元 245、加密单元 250、时刻取得单元 255、署名值计算单元 260、扩展区域设定单元 265 以及署名设定单元 270 以及通信单元 275 起作用。由于其具体的功能和动作与使用图 2 和图 5 说明的相同，所以省略说明。

另一方面，在本发明的实施方式的服务器装置 400 用的程序使服务器装置 400 作为通信单元 405、暂时存储单元 410、判定单元 415、解密单元 420、存储单元 425 以及认证单元 430，即作为证明书验证单元 435 以及包含署名验证单元 445 和时刻验证单元 450 的本人确认单元 440 起作用。由于其具体的功能和动作与使用图 4 和图 6 说明的相同，所以省略说明。另外，本发明的实施方式的客户装置 200 用和服务器装置 400 用的程序可存储在可通过计算机读取的介质中。可通过计算机读取的介质包含用于命令执行系统、装置或设备或者与它们相关的程序，可以是可存储、通信、传播、或者传输的任意的装置。介质可以是电性的、磁性的、光学的、电磁的、红外线或者半导体系统（或者，装置或设备）或者传播介质。在计算机可读取的介质的例子中，包含半导体或者固态存储装置、磁盘、可装卸的计算机软盘、随机存取存储器（RAM）、只读存储器（ROM）、硬磁盘以及光盘。在当前时刻的光盘的例子中，包含只读光盘存储器（CD-ROM）、读写光盘（CD-R/W）以及 DVD。

输入输出控制器 735 将作为比较高速的输入输出装置的卡总线控制器 740 和连接到卡总线控制器 740 的 IC 卡读写器 745、通信接口 770、硬盘驱动 750 和 CD-ROM 驱动 760 与主控制器 715 连接。通信接口 770 经由网络与

服务器装置 400 等的外部装置进行通信。

此外，在输入输出控制器 735 上，连接了软磁盘驱动 790 或键盘鼠标控制器 810 等比较低速的输入输出装置、以及闪速 ROM800。闪速 ROM800 存储在客户装置 200 起动时 CPU710 执行的多功能程序或依赖于客户装置 200 的硬件的程序等。软磁盘驱动 790 从软磁盘读取程序或数据，并经由 RAM730 提供给超 I/O 控制器 735。超 I/O 控制器 735 连接软磁盘或例如并行端口、串行端口、键盘端口、鼠标端口等而连接各种输入输出装置。

以上，使用实施方式说明了本发明，但本发明的技术范围并不限定于在上述实施方式中记载的范围中。本领域的技术人员应该理解可对上述实施方式施加各种变更或改良。因此，那些进行了变更或改良的方式也应该包含在本发明的技术范围中。

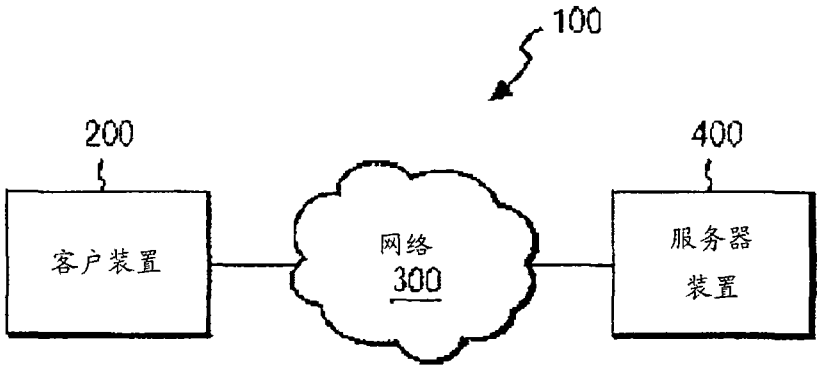

100
200
400
客户装置
网络
300
服务器
装置

图 1

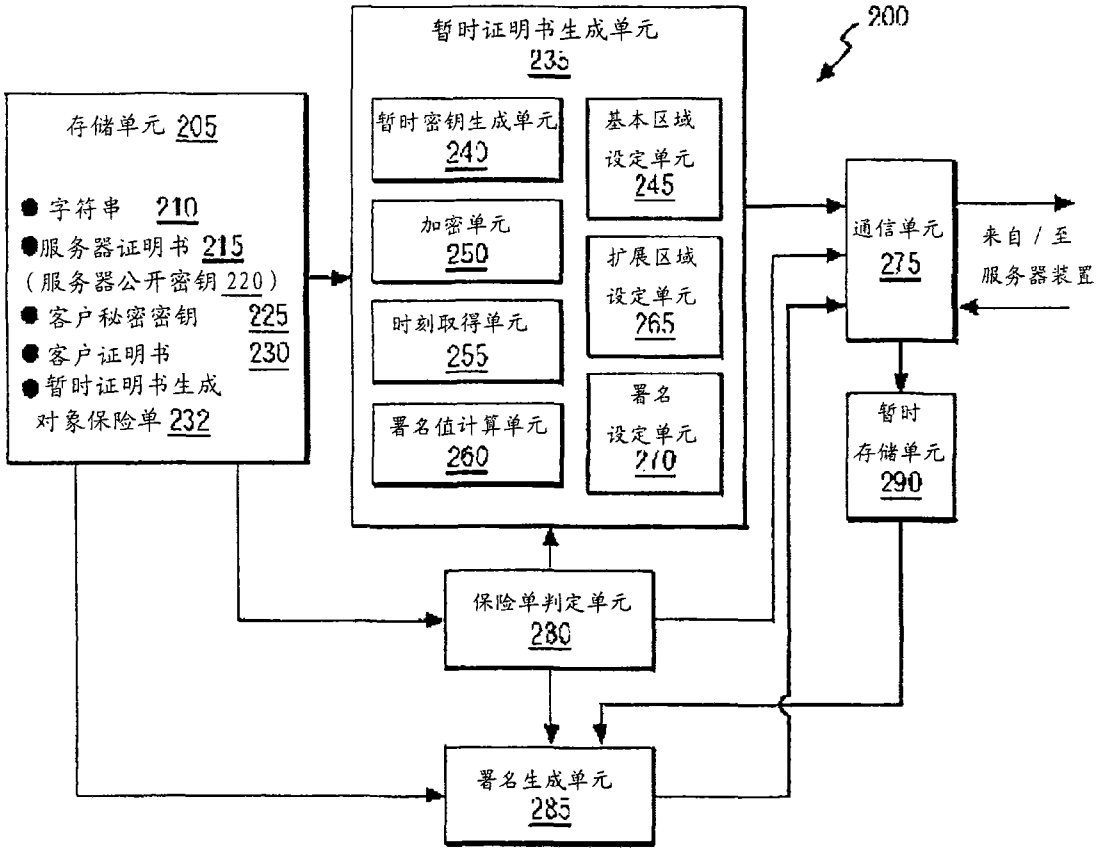

200
暂时证明书生成单元
235
存储单元 205
● 字符串 210
●服务器证明书 215
（服务器公开密钥 220）
● 客户秘密密钥 225
● 客户证明书 230
●暂时证明书生成
对象保险单 232
暂时密钥生成单元
240
加密单元
250
时刻取得单元
255
署名值计算单元
260
基本区域
设定单元
245
扩展区域
设定单元
265
署名
设定单元
270
通信单元
275
来自 / 至
服务器装置
暂时
存储单元
290
保险单判定单元
280
署名生成单元
285

图 2

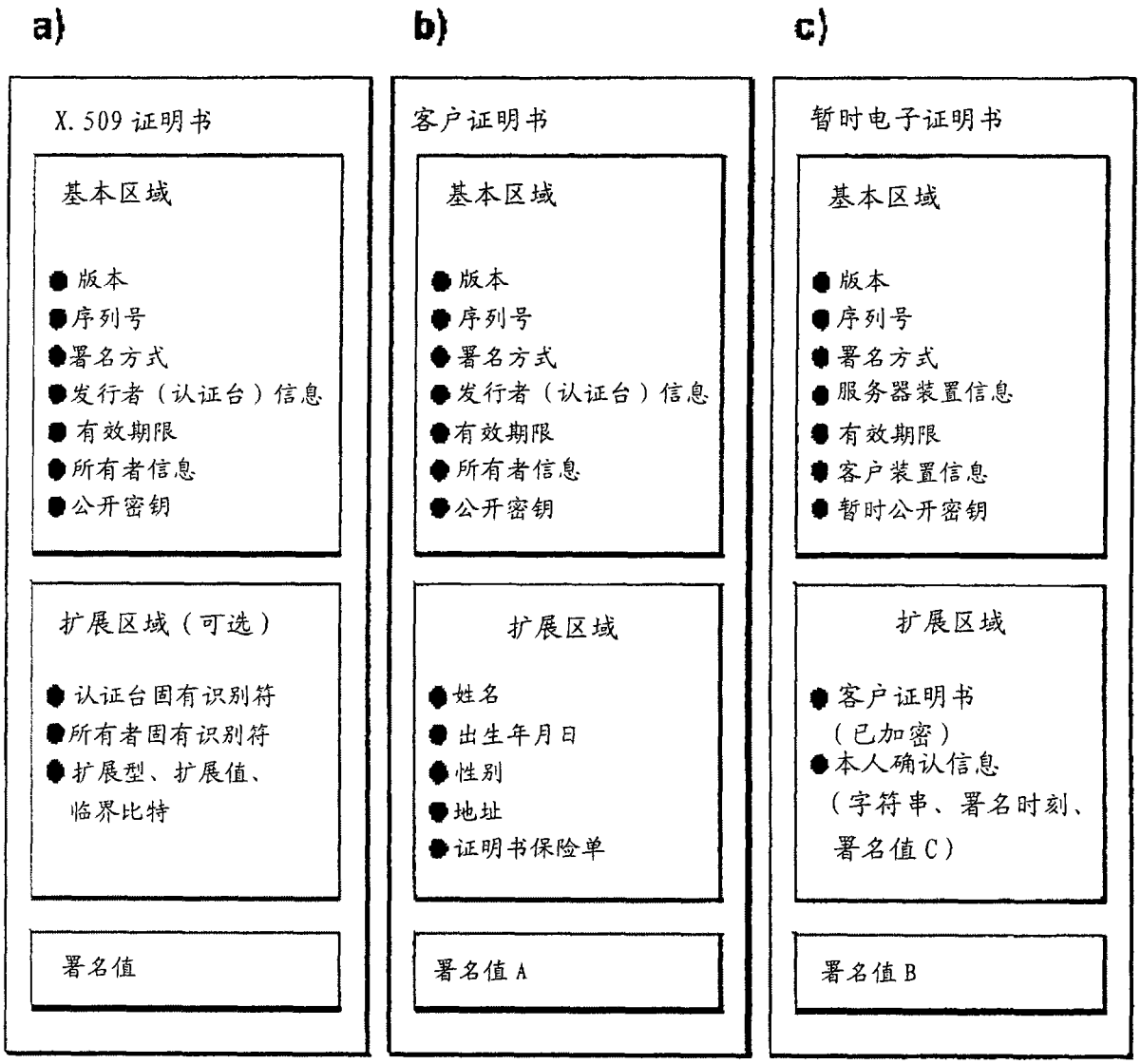

a)
X.509 证明书
基本区域
● 版本
● 序列号
● 署名方式
● 发行者（认证台）信息
● 有效期限
● 所有者信息
● 公开密钥
扩展区域（可选）
● 认证台固有识别符
● 所有者固有识别符
● 扩展型、扩展值、临界比特
署名值
b)
客户证明书
基本区域
● 版本
● 序列号
● 署名方式
● 发行者（认证台）信息
● 有效期限
● 所有者信息
● 公开密钥
扩展区域
● 姓名
● 出生年月日
● 性别
● 地址
● 证明书保险单
署名值 A
c)
暂时电子证明书
基本区域
● 版本
● 序列号
● 署名方式
● 服务器装置信息
● 有效期限
● 客户装置信息
● 暂时公开密钥
扩展区域
● 客户证明书（已加密）
● 本人确认信息（字符串、署名时刻、署名值 C）
署名值 B

图 3

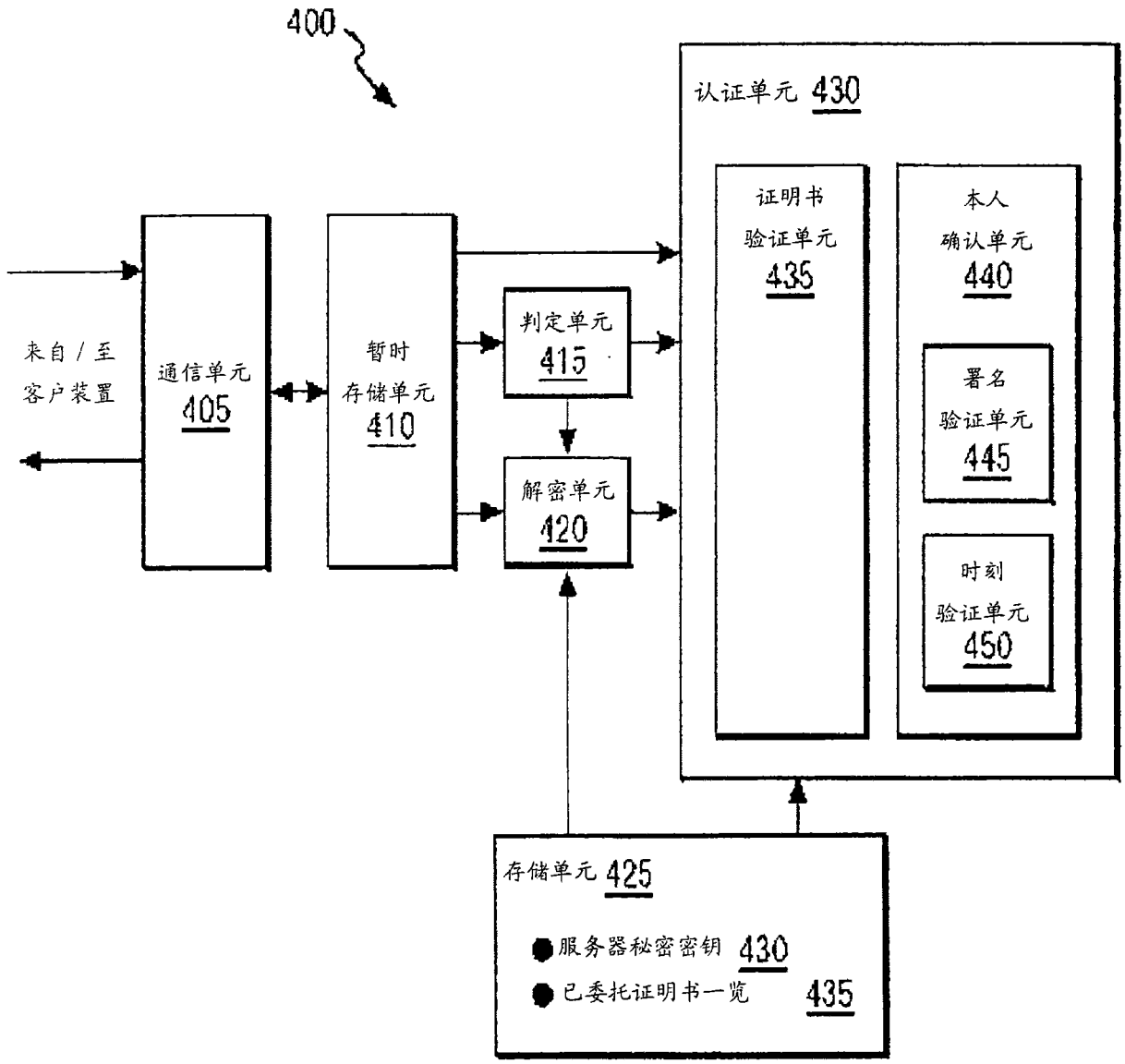

400
认证单元 430
证明书
验证单元
435
本人
确认单元
440
署名
验证单元
445
时刻
验证单元
450
来自 / 至
客户装置
通信单元
405
暂时
存储单元
410
判定单元
415
解密单元
420
存储单元 425
服务器秘密密钥 430
已委托证明书一览 435

图 4

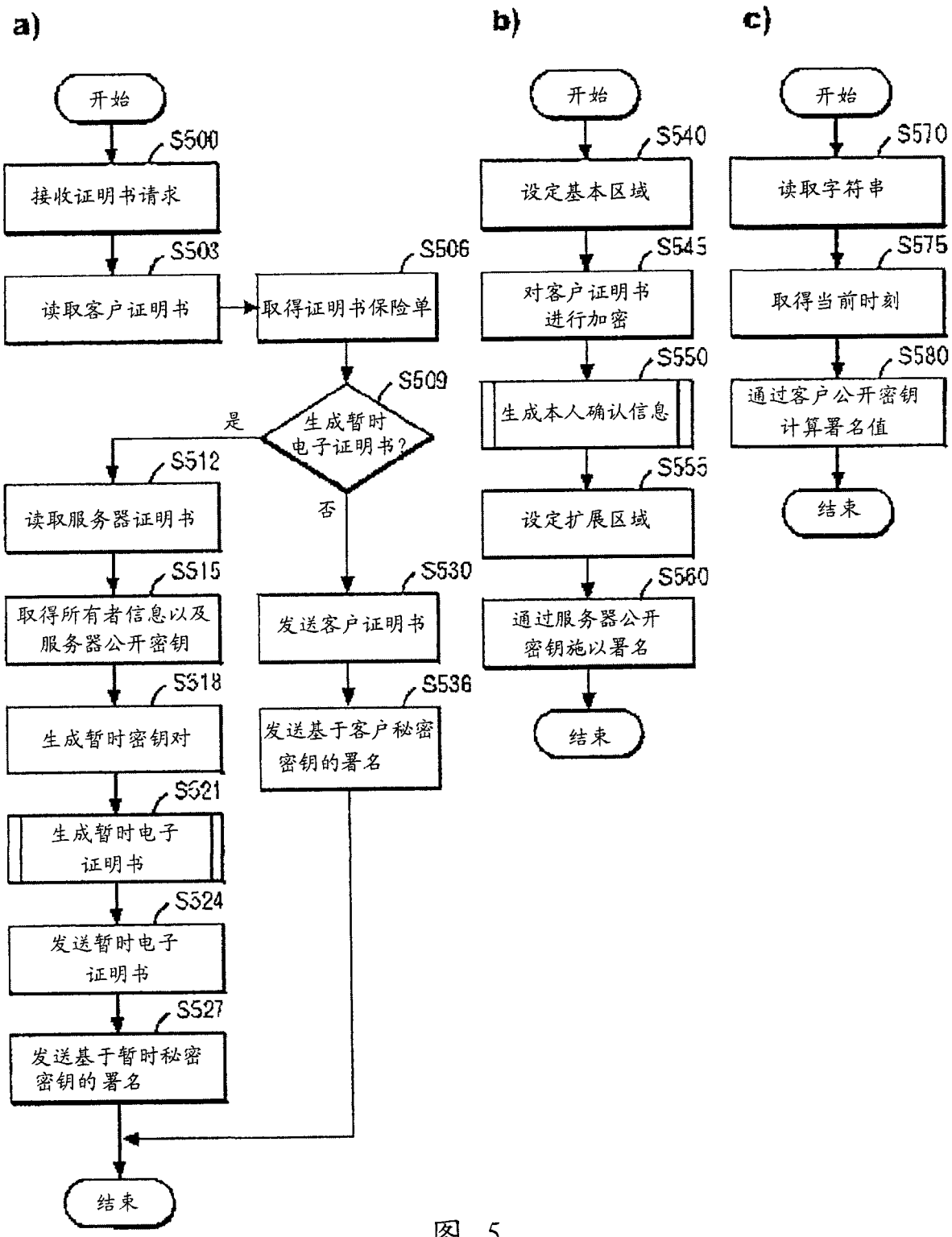

a)
开始
S500
接收证明书请求
S503
读取客户证明书
S506
取得证明书保险单
S509
生成暂时电子证明书?
是
否
S512
读取服务器证明书
S515
取得所有者信息以及服务器公开密钥
S518
生成暂时密钥对
S521
生成暂时电子证明书
S524
发送暂时电子证明书
S527
发送基于暂时秘密密钥的署名
S530
发送客户证明书
S536
发送基于客户秘密密钥的署名
结束
b)
开始
S540
设定基本区域
S545
对客户证明书进行加密
S550
生成本人确认信息
S555
设定扩展区域
S560
通过服务器公开密钥施以署名
结束
c)
开始
S570
读取字符串
S575
取得当前时刻
S580
通过客户公开密钥计算署名值
结束

图 5

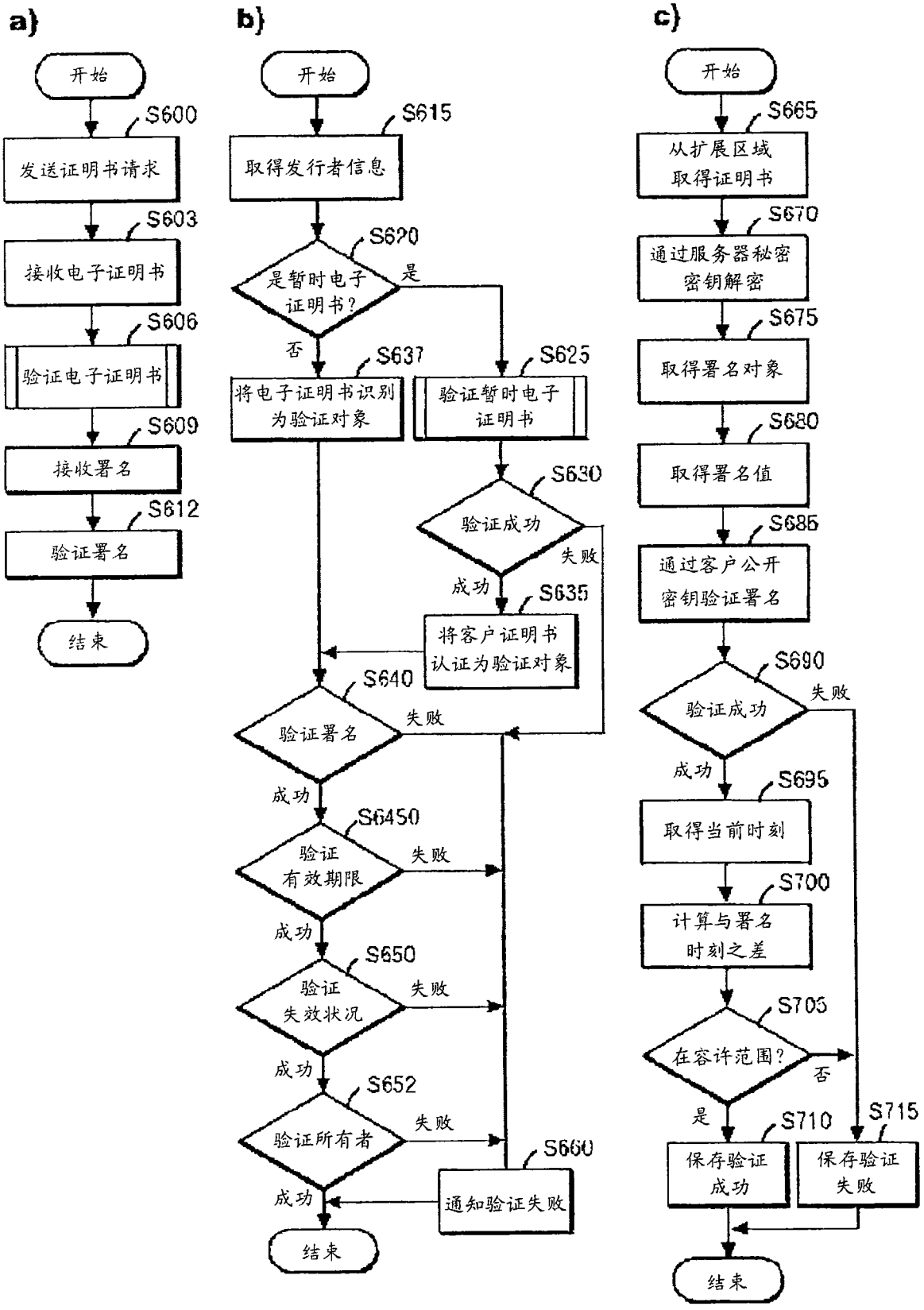

a)
开始
S600
发送证明书请求
S603
接收电子证明书
S606
验证电子证明书
S609
接收署名
S612
验证署名
结束
b)
开始
S615
取得发行者信息
S620
是暂时电子证明书?
是
否
S637
将电子证明书识别为验证对象
S625
验证暂时电子证明书
S630
验证成功
失败
成功
S635
将客户证明书认证为验证对象
S640
验证署名
失败
成功
S6450
验证有效期限
失败
成功
S650
验证失效状况
失败
成功
S652
验证所有者
失败
成功
S660
通知验证失败
结束
c)
开始
S665
从扩展区域取得证明书
S670
通过服务器秘密密钥解密
S675
取得署名对象
S680
取得署名值
S685
通过客户公开密钥验证署名
S690
验证成功
失败
成功
S695
取得当前时刻
S700
计算与署名时刻之差
S705
在容许范围?
否
是
S710
保存验证成功
S715
保存验证失败
结束

图 6

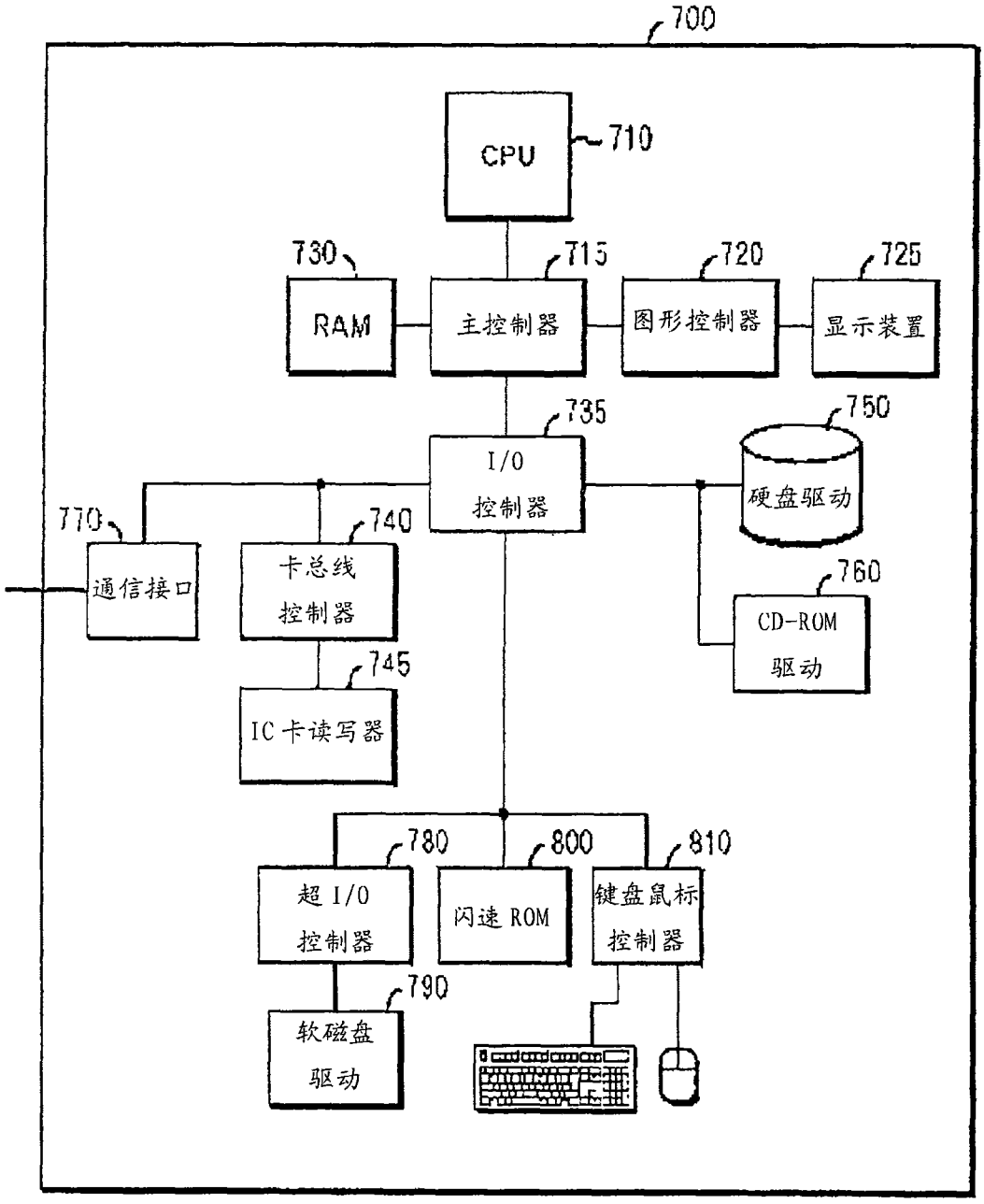

700
CPU
710
730
RAM
715
主控制器
720
图形控制器
725
显示装置
735
I/O
控制器
750
硬盘驱动
770
通信接口
740
卡总线
控制器
760
CD-ROM
驱动
745
IC卡读写器
780
超I/O
控制器
800
闪速ROM
810
键盘鼠标
控制器
790
软磁盘
驱动

图 7