[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 17/60
H04L 9/00

[12] 发明专利说明书

专利号 ZL 03141296.3

[45] 授权公告日 2005 年 12 月 14 日

[11] 授权公告号 CN 1231862C

[22] 申请日 2003.6.12 [21] 申请号 03141296.3

[30] 优先权

[32] 2002.6.12 [33] JP [31] 170798/02

[32] 2003.5.7 [33] JP [31] 128549/03

[71] 专利权人 株式会社日立制作所

地址 日本东京都

[72] 发明人 锻忠司 藤城孝宏 熊谷洋子
羽根慎吾 长野裕美

审查员 解 欣

[74] 专利代理机构 中国专利代理(香港)有限公司

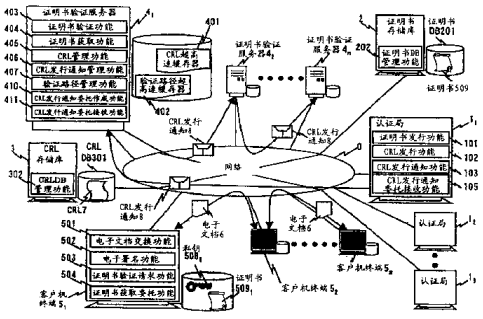
代理人 马铁良 王忠忠

权利要求书 3 页 说明书 19 页 附图 7 页

[54] 发明名称 具有 CRL 发行通知功能的认证基础结构系统

[57] 摘要

为使证明书的有效性判定处理高速化而超高速缓存 CRL 后，在认证局紧急发行了 CRL 的场合下，由于超高速缓存的上述 CRL 不是最新的，因而证明书的有效性验证结果的精度得不到保证。为此，由于在发行了上述 CRL 的场合下，从上述认证局向上述证明书验证服务器发送 CRL 发行通知，而且接收到该 CRL 发行通知的上述证明书验证服务器超高速缓存最新的上述 CRL，因而可以保证证明书有效性验证结果的精度。



ISSN1008-4274

1. 一种认证基础结构系统，其特征在于：具备

认证局，其具备有发行证明书的证明书发行单元和发行 CRL 的 CRL 发行单元；

CRL 存储库，其具备有寄存由上述认证局发行的上述 CRL 的 CRL 寄存单元；

证明书验证服务器，其具备有验证上述证明书有效性的证明书有效性验证单元和对从上述 CRL 存储库获取的上述 CRL 进行超高速缓存的 CRL 超高速缓存单元，

上述认证局具备 CRL 发行通知发送单元，其在发行了上述 CRL 的场合下，将通知「CRL 已发行」事实的 CRL 发行通知发送到上述证明书验证服务器，

上述证明书验证服务器具备 CRL 发行通知接收单元，其从上述认证局接收上述 CRL 发行通知。

2. 权利要求 1 中记载的认证基础结构系统，其特征在于：

上述证明书验证服务器的上述 CRL 超高速缓存单元在由上述 CRL 发行通知接收单元接收到上述 CRL 发行通知的场合下，从上述 CRL 存储库获取上述认证局新发行的上述 CRL。

3. 权利要求 1 或 2 中记载的认证基础结构系统，其特征在于：

上述证明书验证服务器具备 CRL 发行通知发送单元，其在发现上述 CRL 是新发行的场合下，对预先登录的其它证明书验证服务器通知「CRL 已发行」的事实。

4. 一种认证局，其特征在于：

具备发行证明书的证明书发行单元；发行 CRL 的 CRL 发行单元，

具备 CRL 发行通知发送单元，其在发行上述 CRL 的同时，向上述证明书验证服务器发送通知「CRL 已发行」事实的 CRL 发行通知。

5. 一种证明书验证服务器，其特征在于：具备

验证证明书有效性的证明书有效性验证单元；对 CRL 进行超高速缓存的 CRL 超高速缓存单元，具备接收通知 CRL 已发行的 CRL 发行通知的 CRL 发行通知接收单元。

6. 权利要求 5 中记载的证明书验证服务器，其特征在于：

上述证明书验证服务器的上述 CRL 超高速缓存单元在由上述 CRL

发行通知接收单元接收到上述 CRL 发行通知的场合下，获取新发行的上述 CRL。

7. 权利要求 5 或 6 中记载的证明书验证服务器，其特征在于：具备

CRL 发行通知发送单元，其在发现上述 CRL 是新发行的场合下，对预先登录的其它证明书验证服务器通知「CRL 已发行」的事实。

8. 权利要求 1 中记载的认证基础结构系统，其中

上述证明书验证服务器具备作成 CRL 发行通知委托消息的 CRL 发行通知委托作成单元，

上述认证局具备接收上述 CRL 发行通知委托消息的 CRL 发行通知委托接收单元，

上述认证局的上述 CRL 发行通知发送单元对于对该认证局发送了上述 CRL 发行通知委托消息的证明书验证服务器发送上述 CRL 发行通知。

9. 权利要求 8 中记载的认证基础结构系统，其中

上述证明书验证服务器具备

CRL 发行通知委托接收单元，其从其它证明书验证服务器接收上述 CRL 发行通知委托消息；

CRL 发行通知管理单元，其在接收到上述 CRL 发行通知的场合下，对发送了上述 CRL 发行通知委托消息的证明书验证服务器转送上述 CRL 发行通知。

10. 权利要求 4 中记载的认证局，其中

具备接收 CRL 发行通知委托消息的 CRL 发行通知委托接收单元，

上述 CRL 发行通知发送单元将上述 CRL 发行通知发送到所接收的上述 CRL 发行通知委托消息的发送源。

11. 权利要求 5 中记载的证明书验证服务器，具备

作成 CRL 发行通知委托消息的 CRL 发行通知委托作成单元。

12. 权利要求 11 中记载的证明书验证服务器，具备

CRL 发行通知委托接收单元，其从其它证明书验证服务器接收上述 CRL 发行通知委托消息；

CRL 发行通知管理单元，其在接收到上述 CRL 发行通知的场合下，对发送了上述 CRL 发行通知委托消息的证明书验证服务器转送上述

CRL 发行通知。

13. 一种具备有寄存认证局发行的 CRL 的 CRL 寄存单元的 CRL 存储库装置，具备

在上述 CRL 寄存单元寄存了新的 CRL 后，发送 CRL 发行通知的 CRL 发行通知发送单元。

14. 权利要求 13 中记载的 CRL 存储库装置，其中

具备接收 CRL 发行通知委托消息的 CRL 发行通知委托接收单元，

上述 CRL 发行通知发送单元将上述 CRL 发行通知发送到所接收的上述 CRL 发行通知委托消息的发送源。

具有CRL发行通知功能的认证基础结构系统

技术领域

本发明涉及由发行公钥证明书失效列表的认证局、验证公钥证明书有效性的证明书验证服务器、利用上述证明书验证服务器的客户机组成的认证基础结构系统。

现有技术

从政府认证基础结构（以下记述为GPKI）开始，为确认电子文档的作成者，而且为保证该电子文档不被改动，利用了公钥认证基础结构（Public Key Infrastructure，以下记述为PKI）的系统正得到普及（比如参照非专利文献1）。在利用了PKI的系统中，利用只有实施电子署名者（以下记述为署名者）持有的被称为私钥（Private key）的密钥对电子文档实施电子署名。在接收到实施了电子署名的电子文档的场合下，通过验证上述电子署名，来确认电子文档的作成者及确认该电子文档未被改动。

在要求高可靠性的用途中，为进行电子署名验证，不仅要利用上述署名者的公钥证明书（以下记述为证明书）中包含的被称为公钥的密钥来验证该电子署名，还有必要确认上述署名者的证明书对于电子署名验证者（以下记述为验证者）是否是有效的证明书。在验证上述署名者的证明书对于上述验证者是否有效时，有必要进行（1）认证路径的构筑，（2）认证路径的验证的处理。

所谓认证路径是从上述验证者至上述署名者的可靠性链条，作为证明书的链路表现出来。尤其是，在认证局之间相互发行证明书的场合下，发行称为相互认证证明书的特殊证明书。在从认证局1_1至认证局1_9的这9个认证局具有图2所示的相互认证关系的场合下，从持有认证局1_2所发行的证明书的验证者至持有认证局1_1所发行的证明书的署名者的验证路径成为一种呈第1为相互认证证明书9_{18}、第2为相互认证证明书9_{68}、第3为相互认证证明书9_{46}、第4为相互认证证明书9_{24}、最后是验证者的证明书的顺序的证明书链路。对于验证如此构筑的验证路径的方法，在上述非专利文献1中有详细记述。

此外在上述GPKI规格书中，作为验证证明书有效性的模式，记载

有终端实体模式、证明书验证服务器模式。（比如参照非专利文献 2.）上述证明书验证服务器模式为验证证明书的有效性，利用了提供代替客户机在线确认证明书有效性的功能的证明书验证服务器。

上述证明书验证服务器模式与上述终端实体模式相比，具有以下优点。首先，在上述证明书验证服务器模式中，由于不必在客户机中实装构筑上述认证路径的认证路径构筑功能，因而可以缩小客户机的署名验证程序。此外由于客户机相信上述证明书验证服务器的判定结果，因而只需变更上述证明书验证服务器的设定，便可灵活地对应系统结构的变化。根据上述非专利文献 2，在判定证明书是否失效中，利用上述认证局所发行的证明书失效列表（Certificate Revocation List，以下记述为 CRL）及 OCSP 对应符。

由于每当进行验证时从上述认证局获取上述 CRL 这种方法效率不良，因而在专利文献 1 中披露了一种上述证明书验证服务器对上述证明书及上述 CRL 和上述验证路径进行超高速缓存，由此使证明书的有效性判定处理高速化的方法。

不过，为验证电子署名或构筑验证路径，有必要获得署名者的证明书。获得署名者的证明书的方法可大致分为两类。

其一是只从署名者发送附加电子署名的电子文档，另外获取该署名者的证明书的方法。比如与附加电子署名的电子文档一道，通知表示用于验证该电子署名的证明书的寄存场所的 URL 的方法等。在该方法中，上述验证者有必要访问上述证明书的寄存场所（以下记述为证明书存储库）等，获得该证明书。另一种是署名者在发送带有电子署名的电子文档的同时，还附加用于验证该电子署名的证明书来发送的方法。

[专利文献 1]

特开 2002-72876 号公报

[非专利文献 1]

ITU, ITU-T Recommendation X.509 “Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks”, ITU, 2000 年 3 月, p.7-53

[非专利文献 2]

「政府认证基础结构（GPKI）政府认证基础结构相互运用性规格

书」p.18-20，27-29，[online]，平成13年4月25日，基本问题专门部认可，[2003年3月14日检索]，因特网<URL: http://www.soumu.go.jp/gyoukan/kanri/010514_2.pdf>

发明将要解决的课题

为使证明书的有效性判定处理高速化而对上述CRL进行超高速缓存后，在上述认证局紧急发行了上述CRL的场合下，被超高速缓存的上述CRL便不再是最新的。专利文献1中未涉及该点。

解决上述课题的方法之一是一种为能在紧急发行了上述CRL的场合下也能正确地进行有效性验证，上述证明书验证服务器定期访问上述CRL的寄存场所（以下称为CRL存储库），确认上述CRL是否被更新的方法。上述方法还分为上述证明书验证服务器本身通过网络进行确认的方式和在上述CRL存储库内导入CRL发行确认软件来进行确认的方式这2种。

为利用定期确认上述CRL是否被更新的方法，提高上述证明书的有效性验证结果的精度，有必要尽量缩短上述确认的间隔。但在上述证明书验证服务器本身通过网络进行确认的方式中，存在着缩短上述确认间隔后，网络负荷将增大的课题。

另一方面，在上述CRL存储库内导入用于进行确认的CRL发行确认软件的方式的场合下，如果上述CRL存储库的经营者与上述证明书验证服务器的经营者相异，则存在着上述CRL发行确认软件的安装得不到许可，不能进行上述确认的课题。

此外，在存在多个上述证明书验证服务器的环境下，如果所有的上述证明书验证服务器未利用被导入上述CRL存储库的上述CRL发行确认软件，则所有的上述证明书验证服务器便不能在相同精度下进行证明书有效性验证，因而在欲增减运作中的上述证明书验证服务器数量的场合下，便有必要变更上述CRL发行确认软件的设定，然而如果上述CRL存储库的经营者与上述证明书验证服务器的经营者相异，则难以灵活地变更上述证明书验证服务器的数量，这也是一个课题。

此外，即使对上述验证路径进行了超高速缓存，在由上述认证局废弃了旧的相互认证证明书，发行了新的相互认证证明书的场合下，有必要构筑包含新的相互认证证明书的验证路径。

此外在存在多个上述证明书验证服务器的环境下，即使在多个上

述证明书验证服务器验证出同一上述证明书有效性的场合下，各上述证明书验证服务器仍需进行上述认证路径的构筑及上述 CRL 的获取等，因而存在着对特定的上述 CRL 存储库及上述证明书存储库的访问集中，或网络负荷增大的可能性。专利文献 1 中对此未做涉及。

此外在另外获取上述证明书的方法中，存在着上述客户机为向上述证明书验证服务器委托上述证明书的有效性验证，必须首先访问上述证明书存储库，以获取上述证明书的课题。

因此，需要推出解决上述各课题的新方法。

发明内容

本发明的特征在于，其认证基础结构系统由以下部分构成：认证局，其具备有发行上述证明书的证明书发行单元、发行上述 CRL 的 CRL 发行单元；证明书存储库，其具备有寄存由上述认证局发行的上述证明书的证明书寄存单元；CRL 存储库，其具备有寄存由上述认证局发行的上述 CRL 的 CRL 寄存单元；证明书验证服务器，其具备有验证上述证明书有效性的证明书有效性验证单元、对从上述 CRL 存储库获取的上述 CRL 进行超高速缓存的 CRL 超高速缓存单元、对为上述证明书有效性验证单元验证上述证明书的有效性而构筑的验证路径进行超高速缓存的验证路径超高速缓存单元；客户机，其具备有验证电子署名的电子署名验证单元、向上述证明书验证服务器委托上述证明书的有效性验证的证明书有效性验证委托单元，在该认证基础结构系统中，上述认证局中设有 CRL 发行通知发送单元，其在发行上述 CRL 的同时，向上述证明书验证服务器发送通知「上述 CRL 已发行」事实的 CRL 发行通知，上述证明书验证服务器中设有 CRL 发行通知接收单元，其从上述认证局接收上述 CRL 发行通知。

此外本发明的特征在于：上述证明书验证服务器的上述 CRL 超高速缓存单元在由上述 CRL 发行通知接收单元接收到上述 CRL 发行通知的场合下，从上述 CRL 存储库获取由上述认证局新发行的上述 CRL。

此外本发明的特征在于：上述证明书验证服务器中设有 CRL 发行通知发送单元，其在发现上述 CRL 是新发行的场合下，对预先登录的其它证明书验证服务器通知「CRL 已发行」的事实。

此外本发明的特征在于：上述认证局中设有证明书发行通知发送单元，其在由上述证明书发行单元发行了上述证明书的场合下，向上

述证明书验证服务器发送通知「证明书已发行」的事实的证明书发行通知，上述证明书验证服务器中设有接收上述证明书发行通知的证明书发行通知接收单元，上述证明书有效性验证单元在由上述证明书发行通知接收单元接收到上述证明书发行通知的场合下，作成包含新发行的上述证明书的上述验证路径，上述验证路径超高速缓存单元对该验证路径进行超高速缓存。

此外本发明的特征在于：在上述证明书验证服务器中设有验证路径发送单元，其在构筑了上述验证路径的场合下，将该验证路径发送到预先登录的其它证明书验证服务器，上述验证路径超高速缓存单元在从其它证明书验证服务器接收到上述验证路径的场合下，对该验证路径进行超高速缓存。

此外本发明的特征在于：上述客户机中设有证明书获取委托单元，其向上述证明书验证服务器委托为验证上述电子署名所必需的上述证明书的获取，上述证明书验证服务器中设有证明书获取单元，其从上述证明书存储库获取从上述客户机请求了获取的上述证明书，而且在由上述证明书验证单元判定出该证明书有效的场合下，向上述客户机发送该证明书。

此外本发明的特征在于：在上述证明书验证服务器中设有作成「委托上述 CRL 发行通知的发送」的消息的单元，在上述认证局中设有接收上述 CRL 发行通知委托消息的单元，此外上述认证局的上述 CRL 发行通知发送单元对于对该认证局发送了上述 CRL 发行通知委托消息的证明书验证服务器发送上述 CRL 发行通知。

此外本发明的特征在于：在上述 CRL 存储库中具备有 CRL 发行通知发送单元，其在发现了在上述 CRL 寄存库寄存了新的 CRL 的场合下，发送「CRL 已发行」的 CRL 发行通知；CRL 发行通知委托接收单元，其接收「委托上述 CRL 发行通知的发送」的 CRL 发行通知委托消息。

此外本发明的特征在于：CRL 发行确认软件实现监视 CRL 的发行，在发行了新 CRL 的场合下，发送 CRL 发行通知的单元，实现接收 CRL 发行通知委托消息的单元，上述 CRL 发行通知发送单元将上述 CRL 发行通知发送到所接收的上述 CRL 发行通知委托消息的发送源。

此外本发明的特征在于：上述证明书验证服务器中设有接收由上述 CRL 发行通知委托作成单元作成的 CRL 发行通知委托消息的单元。

附图说明

图 1 是表示应用了本发明一实施方式的带有电子署名的电子文档交换系统的系统结构的附图.

图 2 是表示图 1 的带有电子署名的电子文档交换系统中，认证局 1 之间的相互认证关系的附图.

图 3 是表示图 1 的带有电子署名的电子文档交换系统中，发行了 CRL7 的场合下的动作的附图.

图 4 是表示图 1 的带有电子署名的电子文档交换系统中，证明书 509 与电子文档一同发送的场合下，客户机终端 5 收发电子文档 6 时的动作的附图.

图 5 是表示图 1 的带有电子署名的电子文档交换系统中，证明书 509 未与电子文档一同发送的场合下，客户机终端 5 收发电子文档 6 时的动作的附图.

图 6 是表示 CRL 发行通知发送目标列表 104 与 CRL 发行通知转送目标列表 408 的一例的附图.

图 7 是表示图 1 的带有电子署名的电子文档交换系统中，证明书验证服务器 4 向认证局 1 委托 CRL 发行通知 8 的发送的场合下的动作的附图.

图 8 是表示 CRL 发行通知委托消息 10 的一例的附图.

图 9 是表示图 1 所示的认证局 1、证明书存储库 2、CRL 存储库 3、证明书验证服务器 4、客户机终端 5 的各硬件结构例的附图.

符号说明

0...网络，1、1_1～1_n...认证局，2...证明书存储库，3...CRL 存储库，4、4_1～4_n...证明书验证服务器，5、5_1～5_n...客户机终端，6...电子文档，7...CRL，8...CRL 发行通知，9...相互认证证明书，10...CRL 发行通知委托消息，91...CPU，92...存储器，93...外部存储装置，94...读取装置，95...通信装置，96...输入装置，97...输出装置，98...接口，99...存储媒体，104...CRL 发行通知发送目标列表，408...CRL 发行通知转送目标列表，409...验证路径发送目标列表，508、508_1～508_n...私钥，509、509_1～509_n...证明书.

实施方式

以下利用附图对本发明的实施方式作以说明. 此外本发明并不受

此限定。

图 1 是表示作为本发明实施例的带有电子署名的电子文档交换系统的一种构成的附图。从认证局 1_1 至认证局 1_9 这 9 个认证局（以下统一记述为认证局 1）、证明书存储库 2、CRL 存储库 3、从证明书验证服务器 4_1 至证明书验证服务器 4_n 的 n 个证明书验证服务器（以下统一记述为证明书验证服务器 4）、向上述证明书验证服务器 4 委托证明书的有效性验证的从客户机终端 5_1 至客户机终端 5_m 的 m 个客户机终端(以下统一记述为客户机终端 5）通过网络 0 连接。

上述认证局 1 具备向上述客户机终端 5 发行证明书 509，并将该证明书 509 的副本寄存到上述证明书存储库 2 的证明书发行功能 101、发行作为失效的上述证明书 509 的列表的 CRL7，并将该 CRL7 寄存到上述 CRL 存储库的 CRL 发行功能 102、将通知发行了上述 CRL7 的 CRL 发行通知 8 发送到上述证明书验证服务器 4 的 CRL 发行通知功能 103、接收「委托上述 CRL 发行通知 8 的发送」的 CRL 发行通知委托消息 10 的 CRL 发行通知委托接收功能 105。

此外从认证局 1_1 至认证局 1_9 的上述认证局 1 相互发行相互认证证明书 9，具有如图 2 所示的相互认证关系。

上述证明书存储库 2 具备保持上述证明书 509 的证明书 DB201、从上述认证局 1 接收上述证明书 509，并将该证明书 509 寄存到上述证明书 DB201，此外从上述证明书 DB201 检索指定的上述证明书 509 并返回的证明书 DB 管理功能 202。

上述 CRL 存储库 3 具备保持上述 CRL7 的 CRLDB301、从上述认证局 1 接收上述 CRL7，并将该 CRL 寄存到上述 CRLDB301，此外从上述 CRLDB301 检索指定的上述 CRL7 并返回的证明书 DB 管理功能 302。

上述证明书验证服务器 4 具备:

对上述 CRL7 超高速缓存的 CRL 超高速缓存器 401;

对用于验证上述证明书 509 的有效性的验证路径进行超高速缓存的验证路径超高速缓存器 402;

接收来自上述客户机终端 5 的请求，验证证明书有效性的证明书验证功能 403;

接收来自上述客户机终端 5 的请求，从上述证明书存储库 2 获取上述证明书 509，通过上述证明书验证功能 403 来验证该证明书 509

的有效性，在该证明书 509 有效的场合下，返回上述客户机终端 5 的证明书获取功能 404;

从上述 CRL 存储库 3 获取上述 CRL7，并将该 CRL7 寄存到上述 CRL 超高速缓存器 401 的 CRL 管理功能 405;

从上述认证局 1 接收上述 CRL 发行通知 8，在从上述认证局 1 接收到上述 CRL 发行通知 8 的场合下，向预先登录的或者通过发送上述 CRL 发行通知委托消息 10 来委托了该 CRL 发行通知 8 的转送的其它证明书验证服务器 4 转送该 CRL 发行通知 8 的 CRL 发行通知管理功能 406;

在上述验证路径超高速缓存器 402 内对上述证明书验证功能 403 所作成的上述验证路径进行超高速缓存，并将该验证路径向预先登录的其它证明书验证服务器 4 发送，此外在上述验证路径超高速缓存器 402 内对从其它证明书验证服务器 4 接收的上述验证路径进行超高速缓存的验证路径管理功能 407;

作成对上述认证局 1 委托上述 CRL 发行通知 8 的发送的 CRL 发行通知委托消息 10 的 CRL 发行通知委托作成功能 410;

从其它证明书验证服务器 4 接收上述 CRL 发行通知委托消息 10 的 CRL 发行通知委托接收功能 411。

上述客户机终端 5 具备:

与其它客户机终端 5 交换电子文档 6 的电子文档交换功能 501;

在上述电子文档 6 上进行电子署名，并验证在从其它客户机终端 5 接收的上述电子文档 6 上进行的电子署名的电子署名功能 502;

向上述证明书验证服务器 4 请求上述证明书 509 的有效性验证，并从上述证明书验证服务器 4 接收上述证明书 509 的有效性验证结果的证明书验证请求功能 503;

在上述电子文档 6 上并非附加上述证明书 509 而是附加了表示上述证明书 509 的寄存场所的 URL 的场合下，为获取在该 URL 中寄存的上述证明书 509，向上述证明书验证服务器 4 发送该证明书识别信息，并从上述证明书验证服务器 4 接收该证明书 509 的证明书获取委托功能 506;

上述电子署名作成功能 502 所利用的私钥 508;

由上述认证局 1 发行的上述证明书 509。

上述客户机终端 5_1 的上述证明书 509_1 由上述认证局 1_1 发行，上述

客户机终端 5_2 的上述证明书 509_2 由上述认证局 1_2 发行。

在本实施例中，上述证明书验证请求功能 503 与上述证明书获取委托功能 506 所利用的上述证明书验证服务器 4 利用从上述证明书验证服务器 4_1 至上述证明书验证服务器 4_n 的上述证明书验证服务器 4 中预定的特定的上述证明书验证服务器 4。

比如客户机终端 5_2 利用上述证明书验证服务器 4_1。

图 1 所示的认证局 1、证明书存储库 2、CRL 存储库 3、证明书验证服务器 4、客户机终端 5 各装置可通过在一般电子计算机中由 CPU91 实行被装入存储器 92 的规定程序来实现，该计算机如图 9 所示具备有：CPU91、存储器 92、硬盘等外部存储装置 93、从 CD-ROM 等具有移动性的存储媒体 99 读取信息的读取装置 94、用于通过网络与其它装置进行通信的通信装置 95、键盘及鼠标等输入装置 96、监视器及打印机等输出装置 97、进行这些各装置之间的数据收发的接口 98。

即，证明书发行功能 101、CRL 发行功能 102、CRL 发行通知功能 103、CRL 发行通知委托接收功能 105、证明书 DB 管理功能 202、CRLDB 管理功能 302、证明书验证功能 403、证明书获取功能 404、CRL 管理功能 405、CRL 发行通知管理功能 406、验证路径管理功能 407、CRL 发行通知委托作成功能 410、CRL 发行通知委托接收功能 411、电子文档交换功能 501、电子署名功能 502、证明书验证请求功能 503、证明书获取委托功能 504 可以作为基于 CPU91 实行规定的程序的过程来实现。此外证明书 DB201、CRLDB301、CRL 超高速缓存器 401、验证路径超高速缓存器 402 可通过 CPU91 利用存储器 92 及外部存储装置 63 来实现。

用于实现上述各装置的规定程序可通过读取装置 94 从电子计算机可利用的存储媒体 99 被导入这种电子计算机，或者也可以通过通信装置 96，并通过网络或在网络上传播的载波等电子计算机可利用的通信媒体被从其它服务器导入。

在导入时，可以在暂时寄存到外部存储装置 93 后，由此装入存储器 92，由 CPU91 实行，或者也可以不寄存到外部存储装置 93，而直接装入存储器 92，由 CPU91 实行。

接下来，对图 1 的电子署名利用系统的动作，结合附图，对上述证明书验证服务器 4 对上述认证局 1 委托上述 CRL 发行通知 8 的发送

场合下的动作作以说明。

图 7 表示在图 1 的电子署名利用系统中，上述证明书验证服务器 4 对上述认证局 1 委托上述 CRL 发行通知 8 的发送场合下的上述证明书验证服务器 4 及上述认证局 1 的动作。

在上述证明书验证服务器 4 中，上述 CRL 发行通知委托作成功能 410 作成上述 CRL 发行通知委托消息 10（步骤 7101），发送到上述认证局 1（步骤 7102）。

图 8(a)例示的 CRL 发行通知委托消息 10 由「委托上述 CRL 发行通知 8 的发送」消息和作为成为上述 CRL 发行通知 8 的发送目标的网络 0 上的地址的主机名来构成。

在上述认证局 1 中，上述 CRL 发行通知委托接收功能 105 接收到上述 CRL 发行通知委托消息 10（步骤 7201）后，将发送了该 CRL 发行通知委托消息 10 的上述证明书验证服务器 4 的主机名追加到 CRL 发行通知发送目标列表 104（步骤 7202）。

在从上述证明书验证服务器 4_1 向上述证明书验证服务器 4_2 委托上述 CRL 发行通知 8 的转送的场合下，首先，上述证明书验证服务器 4_1 的上述 CRL 发行通知委托作成功能 410 作成上述 CRL 发行通知委托消息 10，发送到上述证明书验证服务器 4_2。

上述证明书验证服务器 4_2 的 CRL 发行通知委托接收功能 411 接收该 CRL 发行通知委托消息 10，将作为发送源的上述证明书验证服务器 4 的主机名追加到 CRL 发行通知转送目标列表 408。

上述证明书验证服务器 4 在对上述认证局 1 委托停止上述 CRL 发行通知 8 的发送的场合下，将图 8(b)例示的 CRL 发行通知委托消息 10 发送到上述认证局 1。

图 8(b)的 CRL 发行通知委托消息 10 由「委托停止上述 CRL 发行通知 8 的发送」消息和上述 CRL 发行通知 8 的发送目标的主机名来构成。

上述认证局 1 接收到图 8(b)的 CRL 发行通知委托消息 10 后，将所记载的上述证明书验证服务器 4 的主机名从 CRL 发行通知转送目标列表 408 删除。

上述证明书验证服务器 4 在向其它的证明书验证服务器 4 委托转送上述 CRL 发行通知 8 或委托停止转送的场合下，将上述 CRL 发行通

知委托消息 10 发送到委托目标的证明书验证服务器 4。

接下来，利用附图，对在图 1 的电子署名利用系统中，发行了上述 CRL7 的场合下的上述认证局 1、上述 CRL 存储库 3、上述证明书验证服务器 4 的动作作以说明。

图 3 是表示在图 1 的电子署名利用系统中，发行了上述 CRL7 的场合下的上述认证局 1、上述 CRL 存储库 3、上述证明书验证服务器 4 的动作的附图。

首先，对上述认证局 1 的动作作以说明。

上述认证局 1 中，上述 CRL 发行功能 102 作成上述 CRL7（步骤 3101）后，该 CRL 发行功能 102 将该 CRL7 发送到上述 CRL 存储库 3（步骤 3102）。

接下来，上述 CRL 发行通知功能 103 作成上述 CRL 发行通知 8，向预定的或者通过发送上述 CRL 发行通知委托消息 10 而委托了该 CRL 发行通知 8 的发送的上述证明书验证服务器 4 发送（步骤 3103）。

此外在本实施例中，认证局 1 将上述 CRL 发行通知 8 发送到在 CRL 发行通知发送目标列表 104 中记载了主机名的上述证明书验证服务器 4。

图 6(a)是上述认证局 1 所管理的 CRL 发行通知发送目标列表 104 一例，上述证明书验证服务器 4_1 的主机名及上述证明书验证服务器 4_n 的主机名被记载于内。

这样，上述认证局 1 的上述 CRL 发行通知功能 103 将上述 CRL 发行通知 8 发送到上述证明书验证服务器 4_1 及上述证明书验证服务器 4_n。

接下来，对上述 CRL 存储库 3 的动作作以说明。

上述 CRL 存储库 3 的上述 CRLDB 管理功能 302 等待来自上述认证局 1 或上述证明书验证服务器 4 的访问，当从上述认证局 1 接收上述 CRL7（步骤 3301）后，将该 CRL7 寄存到上述 CRLDB301（步骤 3302），再次等待来自上述认证局 1 或上述证明书验证服务器 4 的访问。

另一方面，从上述证明书验证服务器 4 接收到发送上述 CRL7 的委托（步骤 3303）后，从上述 CRLDB301 检索该 CRL7（步骤 3304），将该 CRL7 发送到上述证明书验证服务器 4（步骤 3305），再次等待来自上述认证局 1 或上述证明书验证服务器 4 的访问。

接下来，对上述证明书验证服务器 4 的动作作以说明。

这里，根据从上述认证局 1 接收上述 CRL 发行通知 8 的上述证明书验证服务器 4_1 的动作，对上述证明书验证服务器 4 的动作作以说明。

首先，在上述证明书验证服务器 4_1 中，上述 CRL 发行通知管理功能 406 从上述认证局 1 或其它证明书验证服务器 4 接收到上述 CRL 发行通知 8（步骤 3401）后，首先调查是否已经接收过该 CRL 发行通知 8（步骤 3402），在已经接收过该 CRL 发行通知 8 的场合下，就此结束处理。

另一方面，在首次接收到上述 CRL 发行通知 8 的场合下，上述 CRL 管理功能 405 访问上述 CRL 存储库 3（步骤 3403），获取上述 CRL7（步骤 3404），由上述 CRL 超高速缓存器 401 进行超高速缓存（步骤 3405）。

接下来，上述 CRL 发行通知管理功能 406 向预先登录的或者通过发送上述 CRL 发行通知委托消息 10 而委托了该 CRL 发行通知 8 的转送的其它证明书验证服务器 4 转送上述 CRL 发行通知 8（步骤 3406）。

上述证明书验证服务器 4 利用称为 CRL 发行通知转送目标列表 408 的列表，对转送上述 CRL 发行通知 6 的上述证明书验证服务器 4 进行管理。

图 6(b) 是上述证明书验证服务器 4_1 所管理的上述 CRL 发行通知转送目标列表 408 一例，上述证明书验证服务器 4_2 的主机名和上述证明书验证服务器 4_3 的主机名及上述证明书验证服务器 4_n 的主机名被记载于内。

这样，上述 CRL 发行通知管理功能 406 将上述 CRL 发行通知 6 转送到上述证明书验证服务器 4_2 和上述证明书验证服务器 4_3 及上述证明书验证服务器 4_n。

此外在本实施例中，从上述证明书验证服务器 4_1 至上述证明书验证服务器 4_n 的各主机名始终被记载于由从上述证明书验证服务器 4_1 至上述证明书验证服务器 4_n 的证明书验证服务器 4 各自保持的上述 CRL 发行通知转送目标列表 408 的任意一个。

这样，如果某一个上述证明书验证服务器 4 从上述认证局 1 接收到上述 CRL 发行通知 6，则从上述证明书验证服务器 4_1 至上述证明书验证服务器 4_n 的所有证明书验证服务器 4 便可接收上述 CRL 发行通知 6。

在新追加上述证明书验证服务器 4 的场合下，如果在由从上述证

明书验证服务器 4_1 至上述证明书验证服务器 4_n 的证明书验证服务器 4 各自保持的上述 CRL 发行通知转送目标列表 408 的任意一个中追加该证明书验证服务器 4 的主机名，则不必再变更上述 CRL 发行通知发送目标列表 104。

以上是发行了上述CRL7的场合下的图1的电子署名利用系统的动作。

接下来，利用附图对在图 1 的带有电子署名的电子文档交换系统中，从上述客户机终端 5_1 向上述客户机终端 5_2 发送上述电子文档 6 的场合下的动作作以说明。

此外在本实施例中，具有用于验证被施加于上述电子文档 6 的电子署名的上述证明书 509 被附加于上述电子文档 6 的场合及未被附加于上述电子文档 6 的场合这两种场合，首先，对用于验证被施加于上述电子文档 6 的电子署名的上述证明书 509 被附加于上述电子文档 6 的场合作以说明。

图 4 是表示在图 1 的带有电子署名的电子文档交换系统中，用于验证被施加于上述电子文档 6 的电子署名的上述证明书 509 被附加于上述电子文档 6 的场合下，从上述客户机终端 5_1 向上述客户机终端 5_2 发送上述电子文档 6 时的上述客户机终端 5_1、上述客户机终端 5_2、上述证明书验证服务器 4_1、上述证明书验证服务器 4_2 的动作的附图。

首先，对上述客户机终端 5_1 的动作作以说明。

上述客户机终端 5_1 中，上述电子文档交换功能 501 作成向上述客户机终端 5_2 发送的上述电子文档 6（步骤 4501）后，上述电子署名功能 502 利用上述私钥 508_1，对该电子文档 6 施加电子署名（步骤 4502）。

接下来，上述电子文档交换功能 501 将被施加了电子署名的上述电子文档 6 与上述证明书 509_1 一同发送到上述客户机终端 5_2（步骤 4503）。

接下来对上述客户机终端 5_2 的动作作以说明。

上述客户机终端 5_2 接收到上述电子文档 6（步骤 4511）后，为验证与上述电子文档 6 一同发送来的上述证明书 509_1 的有效性，上述证明书有效性确认功能 503 向上述证明书验证服务器 4_1 委托该证明书 509_1 的有效性验证（步骤 4512），从上述证明书验证服务器 4_1 接收有效性验证的结果（步骤 4513）。

这里，在作为上述有效性验证的结果，上述证明书 509_1 对上述客户机终端 5_2 无效的场合下，结束处理。

另一方面，在作为上述有效性验证的结果，上述证明书 509_1 对上述客户机终端 5_2 有效的场合下，上述电子署名功能 503 从上述证明书 509_1 取出公钥，验证被施加于上述电子文档 6 的电子署名（步骤 4515）。这里，在判定出上述电子署名不正确的场合下，结束处理。

另一方面，在判定出上述电子署名正确的场合下，保存上述电子署名 6（步骤 4516）。

接下来，对上述证明书验证服务器 4 的动作作以说明。

首先，在上述客户机终端 5_2 向上述证明书验证服务器 4_1 委托上述证明书 509_1 的有效性验证（步骤 4401）后，上述证明书验证功能 403 确认从上述客户机终端 5_2 至上述客户机终端 5_1 的验证路径是否存在于上述验证路径超高速缓存器 402（步骤 4402）。

这里，在上述验证路径超高速缓存器 402 中存在该验证路径的场合下，进入步骤 4404。另一方面，在上述验证路径超高速缓存器 402 中不存在该验证路径的场合下，构筑该验证路径（步骤 4403），进入步骤 4404。

在步骤 4404，上述证明书验证 403 从上述 CRL 超高速缓存器 401 取出上述 CRL7，判定上述验证路径是否有效。接下来将判定结果发送到上述客户机终端 5_2（步骤 4405）。

这里，在上述验证路径并非是在步骤 4403 新构筑的场合下，结束处理。另一方面，在上述验证路径是在步骤 4403 新构筑的场合下，向在验证路径发送目标列表 409 中记载了主机名的上述证明书验证服务器 4 发送该验证路径（步骤 4407），结束处理。

上述验证路径发送目标列表 409 是一种记载了发送新构筑的上述验证路径的上述证明书验证服务器 4 的主机名的列表，在本实施例中，在上述验证路径发送目标列表 409 中也利用上述 CRL 发行通知转送目标列表 408。

因此，在步骤 4407 中，上述验证路径被发送到上述证明书验证服务器 4_2、上述证明书验证服务器 4_3、上述证明书验证服务器 4_n。

此外在本实施例中，虽然在上述 CRL 发行通知转送目标列表 408 与上述验证路径发送目标列表 409 中使用同一列表，但本发明并非受

此限定，也可以各自利用不同的列表。

另一方面，上述证明书验证服务器 4_2、上述证明书验证服务器 4_3、上述证明书验证服务器 4_n从上述证明书验证服务器 4_1接收到上述验证路径（步骤 4411）后，上述验证路径管理功能 407 确认该验证路径是否被超高速缓存于上述验证路径超高速缓存器 402（步骤 4412）。

这里，如果上述验证路径被超高速缓存于上述验证路径超高速缓存器 402，不进行任何动作，结束处理。另一方面，如果上述验证路径未被超高速缓存于上述验证路径超高速缓存器 402，则将该验证路径超高速缓存到上述验证路径超高速缓存器 402（步骤 4413），向在验证路径发送目标列表 409 中记载了主机名的上述证明书验证服务器 4 发送该验证路径（步骤 4414），结束处理。

此外虽然在本实施例中，上述证明书验证服务器 4 的上述验证路径管理功能 407 对验证路径进行收发或进行超高速缓存，但本发明并非受此限定，也可以对可唯一识别上述验证路径的验证路径信息进行收发或进行超高速缓存，必要时可由该验证路径信息构成对应的验证路径。

以上所述是在用于验证被施加于上述电子文档 6 的电子署名的上述证明书 509 被附加于上述电子文档 6 的场合下，从上述客户机终端 5_1向上述客户机终端 5_2发送上述电子文档 6 时的图 1 的带有电子署名的电子文档交换系统的动作。

接下来，利用附图，对在用于验证被施加于上述电子文档 6 的电子署名的上述证明书 509 被附加于上述电子文档 6 的场合下，从上述客户机终端 5_1向上述客户机终端 5_2发送上述电子文档 6 时的图 1 的带有电子署名的电子文档交换系统的动作作以说明。

图 5 是表示在图 1 的带有电子署名的电子文档交换系统中，用于验证被施加于上述电子文档 6 的电子署名的上述证明书 509 被附加于上述电子文档 6 的场合下，从上述客户机终端 5_1向上述客户机终端 5_2发送上述电子文档 6 时的上述客户机终端 5_1、上述客户机终端 5_2、上述证明书验证服务器 4、上述证明书存储库 2 的动作的附图。

首先，对上述客户机终端 5_1的动作作以说明。

上述客户机终端 5_1中，上述电子文档交换功能 501 作成向上述客户机终端 5_2发送的上述电子文档 6（步骤 5501）后，上述电子署名功

能 502 利用上述私钥 508_1，对该电子文档 6 施加电子署名（步骤 5502）。

接下来，上述电子文档交换功能 501 将被施加了电子署名的上述电子文档 6 与表示了上述证明书 509_1 的寄存场所的 URL 一同发送到上述客户机终端 5_2（步骤 5503）。

虽然在本实施例中，与上述电子文档 6 一同发送表示了上述证明书 509 的寄存场所的 URL，但本发明并非受此限定，也可以发送记载于上述证明书 509 的信息的一部分。

接下来对上述客户机终端 5_2 的动作作以说明。

上述客户机终端 5_2 接收到上述电子文档 6（步骤 5511）后，上述证明书获取委托功能 504 向上述证明书验证服务器 4_1 委托获取与同上述电子文档 6 一道发送来的上述 URL 对应的上述证明书 509_1（步骤 5512），从上述证明书验证服务器 4_1 接收委托结果（步骤 5513）。

这里，在上述委托结果中未包含上述证明书 509_1 的场合下，即在上述证明书验证服务器 4_1 判断出上述 URL 所表示的上述证明书 509_1 对上述客户机终端 5_2 无效的场合下，结束处理。另一方面，在上述委托结果中包含上述证明书 509_1 的场合下，上述电子署名功能 503 从上述证明书 509_1 取出公钥，验证被施加于上述电子文档 6 的电子署名（步骤 5515）。这里，在判定出上述电子署名不正确的场合下，结束处理。另一方面，在判定出上述电子署名正确的场合下，保存上述电子署名 6（步骤 5516），结束处理。

接下来对上述证明书验证服务器 4 的动作作以说明。

上述证明书验证服务器 4_1 的上述证明书获取功能 404 从上述客户机终端 5_2 接收到获取上述证明书 509_1 的委托后（步骤 5401），利用从上述客户机终端 5_2 发送的上述 URL，访问上述证明书存储库 2（步骤 5402），获取上述证明书 509_1（步骤 5403）。

接下来，由上述证明书验证功能 403，判定上述证明书 509_1 对上述客户机终端 5_2 是否是有效的证明书（步骤 5404）。

这里，上述证明书验证功能 403 的动作与从图 4 的步骤 4402 至步骤 4409 的动作相同，省略说明。

在根据上述判定，判定出上述证明书 509_1 对上述客户机终端 5_2 是有效的证明书的场合下，作成包含该证明书 509_1 的委托结果（步骤 5405），发送到上述客户机终端 5_2（步骤 5407）。另一方面，在判定

出上述证明书 509_1 对上述客户机终端 5_2 不是有效的证明书的场合下，作成表示「非有效」事实的委托结果（步骤 5406），发送到上述客户机终端 5_2（步骤 5407）。

接下来对上述证明书存储库 2 的动作作以说明。

上述证明书存储库 2 的上述证明书 DB 管理功能 202 从上述证明书验证服务器 4_1 接收到发送上述证明书 509_1 的委托（步骤 5201）后，从上述证明书 DB201 检索该证明书 509_1（步骤 5202），将该证明书 509_1 发送到上述证明书验证服务器 4（步骤 5203）。

以上所述是在用于验证被施加于上述电子文档 6 的电子署名的上述证明书 509 被附加于上述电子文档 6 的场合下，从上述客户机终端 5_1 向上述客户机终端 5_2 发送上述电子文档 6 时的图 1 的带有电子署名的电子文档交换系统的动作。

这样，在本实施例的带有电子署名的电子文档交换系统中，在上述认证局 1 发行上述 CRL7 时，将上述 CRL 发行通知 8 发送到在上述 CRL 发行通知发送目标列表 104 中记载了主机名的上述证明书验证服务器 4，由此将已发行了上述 CRL7 的事实通知到上述证明书验证服务器 4，而且接收到上述 CRL 发行通知 8 的上述证明书验证服务器 4 从上述 CRL 存储库 3 获取上述 CRL7，并予以超高速缓存。

因此，即使在上述认证局 1 紧急发行了上述 CRL7 的场合下，由于上述证明书验证服务器 4 所超高速缓存的 CRL 是最新的，因而可保证上述证明书 590 的有效性验证结果的精度。

此外，在本实施例的带有电子署名的电子文档交换系统中，接收到上述 CRL 发行通知 8 的上述证明书验证服务器 4 将该 CRL 发行通知 8 转送到在上述 CRL 发行通知转送目标列表 408 中记载了主机名的其它证明书验证服务器 4。

因此，即使在新追加了证明书验证服务器 4 的场合下，只需在上述证明书验证服务器 4 的上述 CRL 发行通知转送目标列表 408 中记载新的证明书验证服务器 4 的主机名，便可接收上述 CRL 发行通知 8，不必变更上述认证局 1 侧的设定。

在本实施例的带有电子署名的电子文档交换系统中，在上述证明书验证服务器 4 从其它证明书验证服务器 4 接收到上述验证路径的场合下，对该验证路径进行超高速缓存，而且在上述证明书验证服务器 4

构筑了新的验证路径的场合下，将该新的验证路径发送到在上述验证路径发送目标列表 409 中记载了主机名的其它证明书验证服务器 4。

因此，由于可以在多个上述证明书验证服务器 4 之间共享验证路径，因而可以防止对上述证明书存储库 2 及上述 CRL 存储库 3 的访问集中或网络负荷的增大。

此外在本实施例的带有电子署名的电子文档交换系统中，上述客户机终端 5 在接收到表示了上述证明书 509 的寄存场所的 URL 的场合下，不访问上述证明书存储库 2，而向上述证明书验证服务器 4 委托获取上述证明书 509，而且只有在从上述证明书存储库 2 获取的上述证明书 509 对于上述客户机终端 5 是有效的证明书的场合下，上述证明书验证服务器 4 才将上述证明书 509 返回上述客户机终端 5。

因此，在上述客户机终端 5 中，不必实装访问上述证明书存储库 2 的功能。

此外虽然在本实施例中，在上述 CRL 发行通知 8 中，只记载「CRL 已发行」的通知，但本发明并非受此限定。

比如，在上述 CRL 发行通知 8 中，可包含新发行的上述 CRL7 自身，或也可以包含以前发行的 CRL7 与新发行的 CRL7 的差异信息。此外也可以包含新失效的证明书 509 的识别信息一览。

通过在上述 CRL 发行通知 8 中，包含新发行的上述 CRL7 自身、以前发行的 CRL7 与新发行的 CRL7 的差异信息、新失效的证明书 509 的识别信息一览，可以省略接收了该 CRL 发行通知 8 的上述证明书验证服务器 4 访问上述 CRL 存储库 3，并获取新发行的 CRL7 的处理。

此外虽然在本实施例中，上述 CRL 发行通知 8 的发送及上述 CRL 发行通知委托消息 10 的接收由上述认证局 1 进行，但本发明并非受此限定。比如，也可以由上述 CRL 存储库 3 进行上述 CRL 发行通知 8 的发送及上述 CRL 发行通知委托消息 10 的接收。

或者也可在 CRL 存储库 3 中导入实现监视上述 CRL7 的发行，在确认出发行了新 CRL7 的场合下发送上述 CRL 发行通知 8 的功能的 CRL 发行确认软件，并由该 CRL 发行确认软件实现上述 CRL 发行通知委托接收功能，上述 CRL 发行通知发送功能向所接收的上述 CRL 发行通知委托消息的发送源发送上述 CRL 发行通知。

通过利用上述 CRL 发行确认软件，还可以利用没有上述 CRL 发行

通知发送功能的上述认证局 1 及上述 CRL 存储库 3。此外如果上述 CRL 发行通知委托接收功能管理上述 CRL 发行通知的发送目标，即使上述 CRL 存储库的经营者与上述证明书验证服务器的经营者相异，也可灵活地变更上述证明书验证服务器的数量。

根据本实施例，由于上述 CRL 发行通知只在上述认证局发行了上述 CRL 时从该认证局对上述证明书验证服务器进行，因而不必每隔一定时间确认是否发行了上述 CRL，网络 0 中的负荷较小即可。

此外由于上述 CRL 发行通知 8 由上述认证局 1 处理，因而即使上述 CRL 存储库 3 与上述证明书验证服务器 4 的经营者相异，也可进行高精度的证明书有效性验证。

此外由于上述证明书验证服务器 4 可以通过发送上述 CRL 发行通知委托消息 10 来委托上述 CRL 发行通知 8 的发送，因而即使上述 CRL 存储库 3 的经营者与上述证明书验证服务器 4 的经营者相异，也可灵活地变更上述证明书验证服务器 4 的数量。

此外在上述证明书验证服务器发现发行了新的 CRL 的场合下，该证明书验证服务器将发行了新的上述 CRL 的事实通知到其它的证明书验证服务器。

由于在欲变更所发送的上述证明书验证服务器的场合下，变更该证明书验证服务器的设定即可，因而即使上述 CRL 存储库的经营者与上述证明书验证服务器的经营者相异，也可灵活地变更上述证明书验证服务器的数量。

此外由于上述证明书验证服务器在新构筑了验证路径的场合下，将该验证路径也转送到其它证明书验证服务器，共享验证路径，因而可抑制对特定的上述 CRL 存储库及上述证明书存储库的访问集中及网络负荷。

此外由于在利用了另外获取上述证明书的方法的场合下同样，上述客户机不访问上述证明书存储库并获取上述证明书，而向上述证明书验证服务器委托获取上述证明书并验证该证明书的有效性，因而不必在客户机中实装访问上述证明书存储库并获取上述证明书的功能。

发明效果

因而根据本发明，可以在高精度而且低负荷下可靠地进行上述证明书的有效性验证。

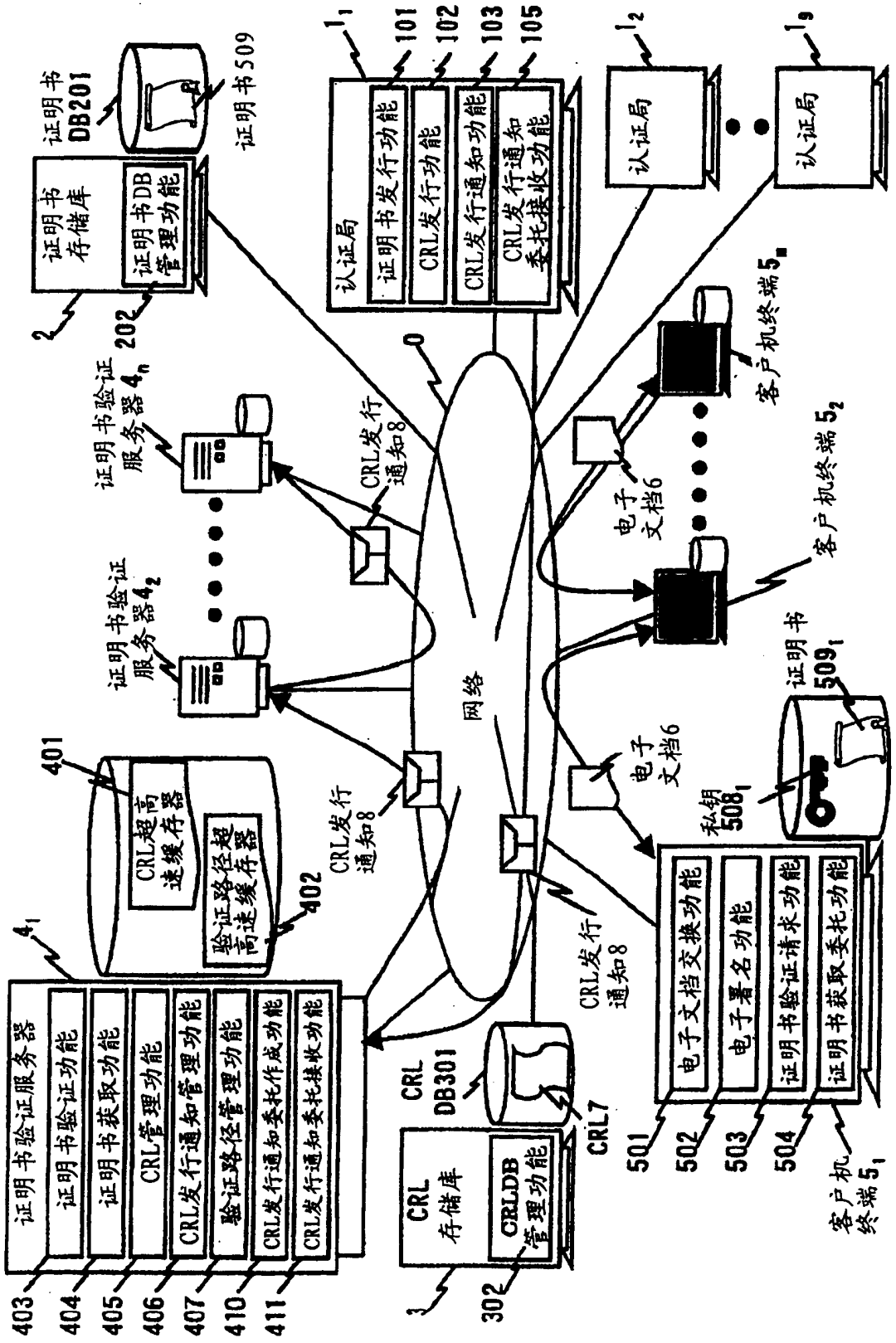

证明书验证服务器
证明书验证功能
证明书获取功能
CRL管理功能
CRL发行通知管理功能
验证路径管理功能
CRL发行通知委托作成功能
CRL发行通知委托接收功能
403
404
405
406
407
410
411
401
CRL超高速缓存器
验证路径超高速缓存器
402
证明书验证服务器 4n
证明书验证服务器 42
证明书存储库
证明书DB管理功能
2
证明书DB201
202
证明书509
CRL存储库
CRL管理功能
3
CRL DB301
302
CRL7
网络
CRL发行通知8
CRL发行通知8
CRL发行通知8
0
认证局
证明书发行功能
CRL发行功能
CRL发行通知功能
CRL发行通知委托接收功能
101
102
103
105
认证局
认证局
客户机终端 5n
客户机终端 52
客户机终端 51
电子文档6
电子文档6
证明书 5091
私钥 5081
电子文档交换功能
电子署名功能
证明书验证请求功能
证明书获取委托功能
501
502
503
504

图 1

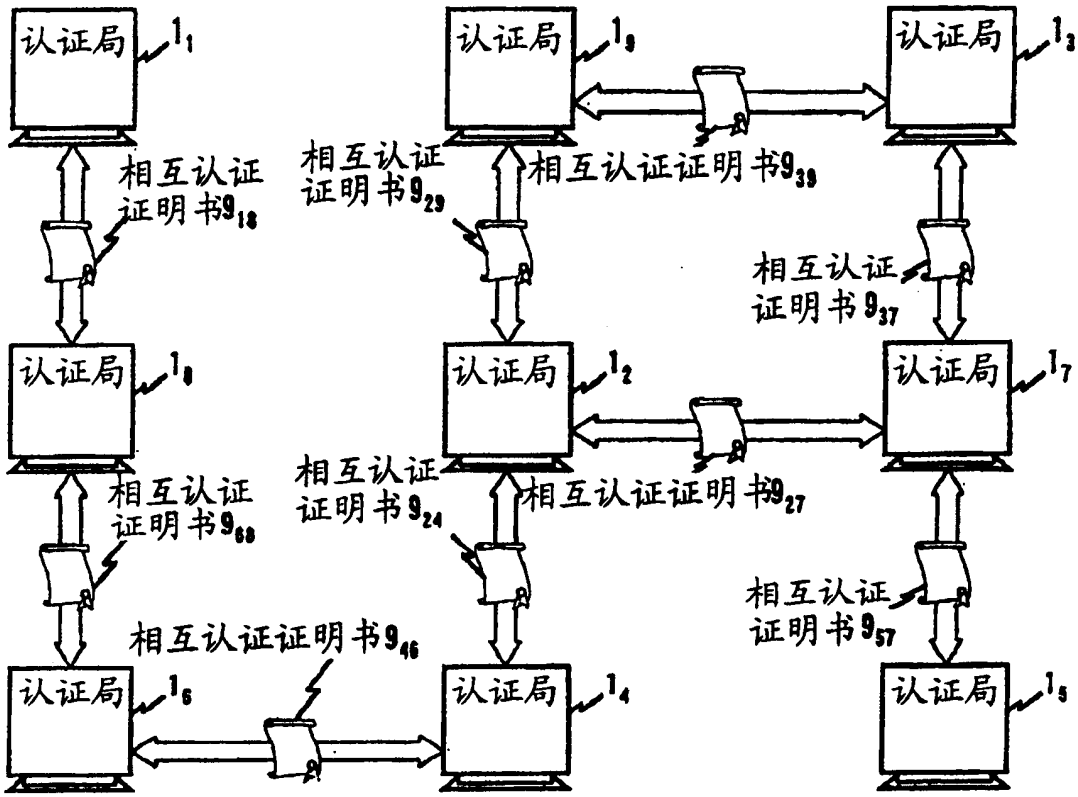

认证局 1_1
认证局 1_9
认证局 1_3
相互认证证明书 9_{18}
相互认证证明书 9_{29}
相互认证证明书 9_{39}
相互认证证明书 9_{37}
认证局 1_8
认证局 1_2
认证局 1_7
相互认证证明书 9_{68}
相互认证证明书 9_{24}
相互认证证明书 9_{27}
相互认证证明书 9_{57}
相互认证证明书 9_{46}
认证局 1_6
认证局 1_4
认证局 1_5

图 2

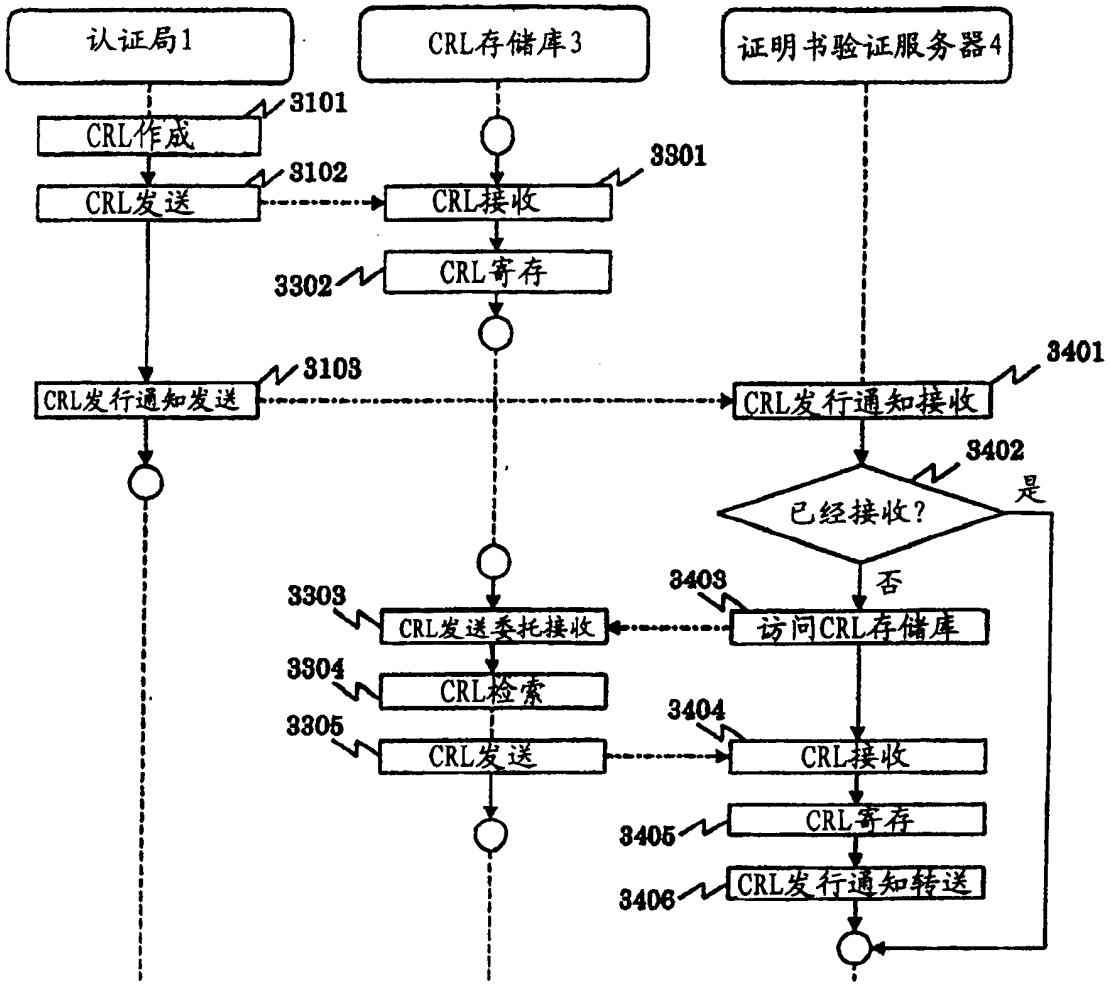

认证局1
CRL存储库3
证明书验证服务器4
3101
CRL作成
3102
CRL发送
3301
CRL接收
3302
CRL寄存
3103
CRL发行通知发送
3401
CRL发行通知接收
3402
已经接收?
是
否
3303
CRL发送委托接收
3403
访问CRL存储库
3304
CRL检索
3305
CRL发送
3404
CRL接收
3405
CRL寄存
3406
CRL发行通知转送

图 3

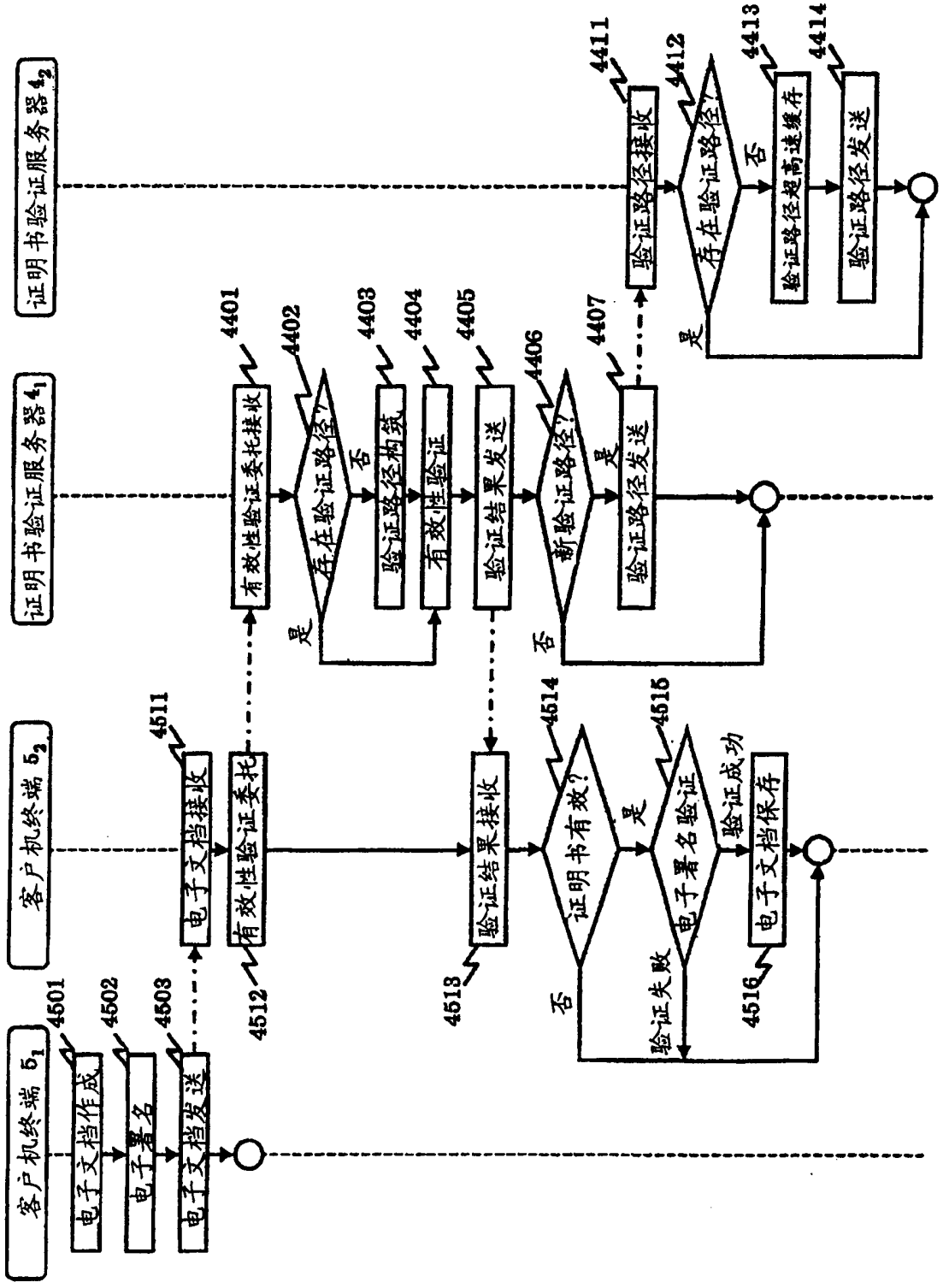

客户机终端 5₁
电子文档作成
电子署名
电子文档发送
4501
4502
4503
客户机终端 5₂
电子文档接收
有效性验证委托
4511
4512
证明书验证服务器 4₁
有效性验证委托接收
存在验证路径?
验证路径构筑
有效性验证
验证结果发送
新验证路径?
验证路径发送
4401
4402
4403
4404
4405
4406
4407
证明书验证服务器 4₂
验证路径接收
存在验证路径?
验证路径超高速缓存
验证路径发送
4411
4412
4413
4414
验证结果接收
证明书有效?
电子署名验证
验证成功
电子文档保存
4513
4514
4515
4516
是
否
验证失败

图 4

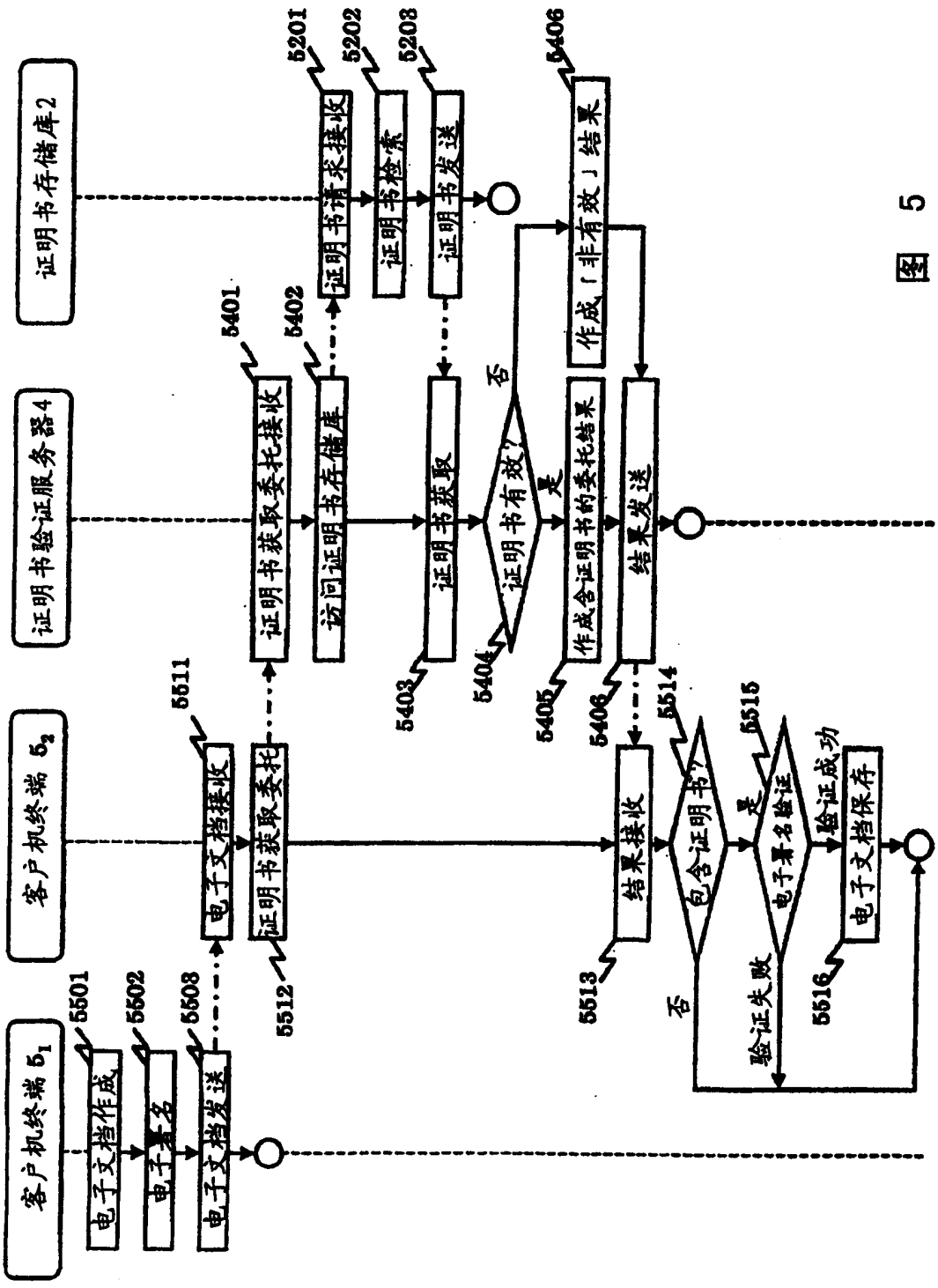

客户机终端 5_1
客户机终端 5_2
证明书验证服务器4
证明书存储库2
电子文档作成
电子签名
电子文档发送
电子文档接收
证明书获取委托
证明书获取委托接收
访问证明书存储库
证明书获取
证明书有效?
作成含证明书的委托结果
结果发送
证明书请求接收
证明书检索
证明书发送
作成「非有效」结果
结果接收
包含证明书?
电子署名验证
验证成功
电子文档保存
验证失败
否
是
5501
5502
5503
5511
5512
5401
5402
5403
5404
5405
5406
5513
5514
5515
5516
5201
5202
5203

图 5

(a)CRL发行通知发送目标列表104

证明书验证服务器4_1的主机名	cvs1.va.co.jp
证明书验证服务器4_n的主机名	cvs1.certvalidation.com

(b)CRL发行通知转送目标列表408

证明书验证服务器4_2的主机名	cvs.cvs.org
证明书验证服务器4_3的主机名	cvs.certvalidation.co.jp
证明书验证服务器4_n的主机名	cvs1.certvalidation.com

图 6

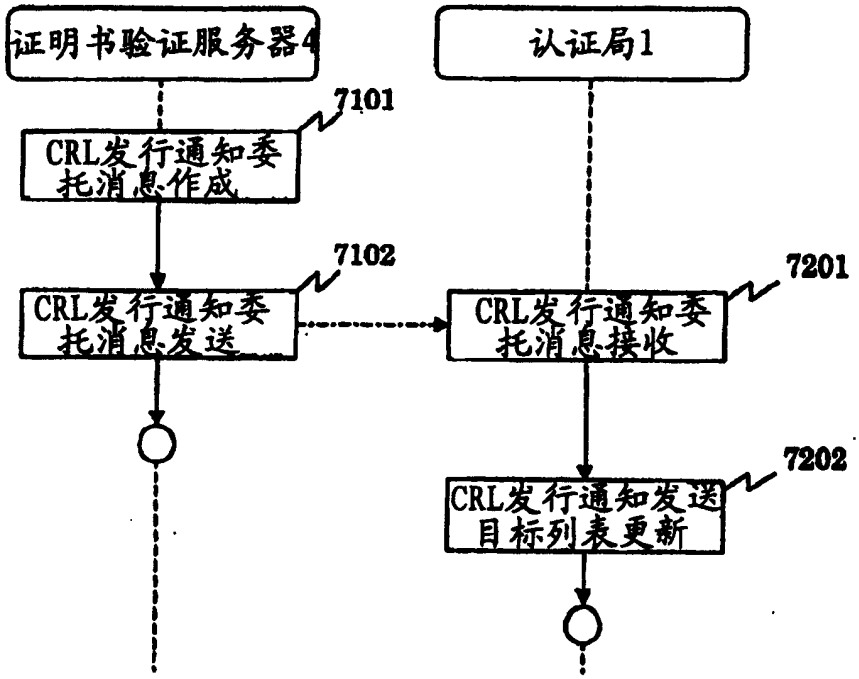


图 7

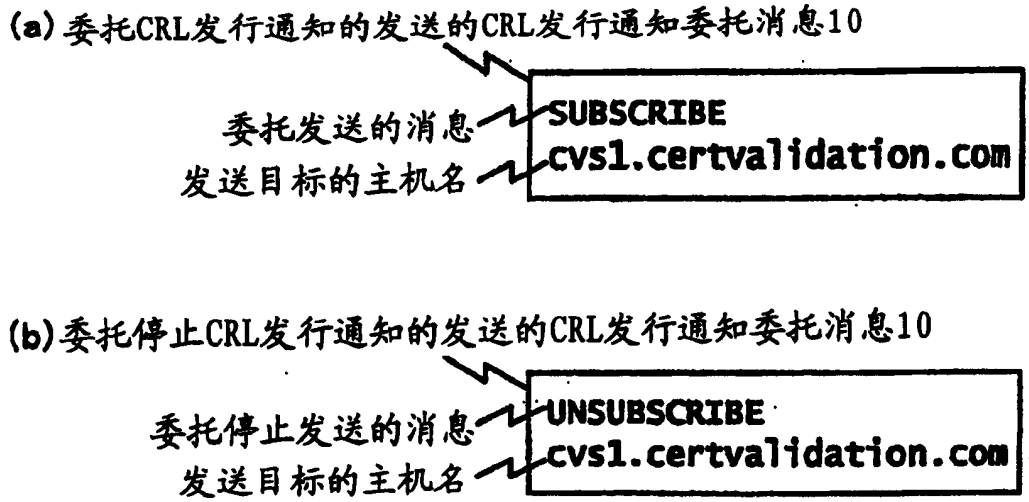

(a)委托CRL发行通知的发送的CRL发行通知委托消息10
委托发送的消息
发送目标的主机名
SUBSCRIBE
cvs1.certvalidation.com
(b)委托停止CRL发行通知的发送的CRL发行通知委托消息10
委托停止发送的消息
发送目标的主机名
UNSUBSCRIBE
cvs1.certvalidation.com

图 8

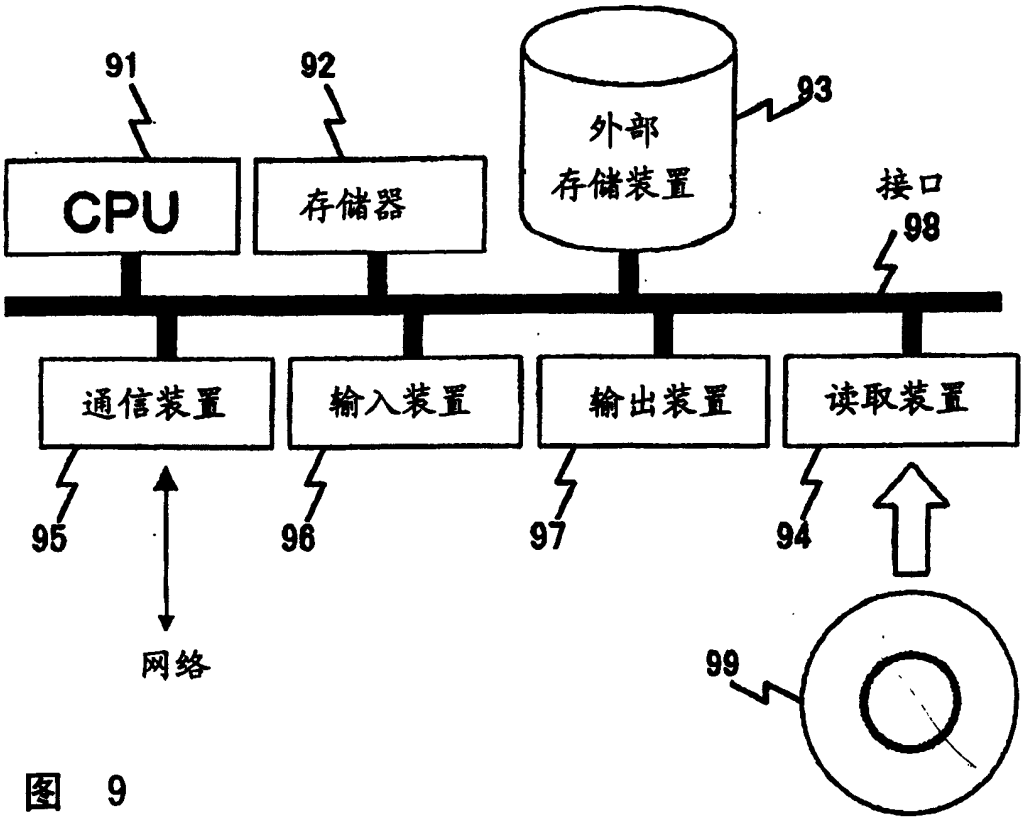

91
92
93
外部
存储装置
CPU
存储器
接口
98
通信装置
输入装置
输出装置
读取装置
95
96
97
94
网络
99

图 9