(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102714596 A
(43)申请公布日 2012.10.03

(21)申请号 201180006557.0

(22)申请日 2011.01.17

(30)优先权数据
2010-012443 2010.01.22 JP

(85)PCT申请进入国家阶段日
2012.07.19

(86)PCT申请的申请数据
PCT/JP2011/051142 2011.01.17

(87)PCT申请的公布数据
WO2011/090178 EN 2011.07.28

(71)申请人 株式会社理光
地址 日本东京都大田区中马达一丁目3番6号

(72)发明人 太田广志

(74)专利代理机构 上海市华诚律师事务所 31210
代理人 肖华

(51)Int.Cl.
H04L 9/32(2006.01)
G06F 3/12(2006.01)
G06F 21/20(2006.01)
H04L 9/08(2006.01)
H04N 1/00(2006.01)

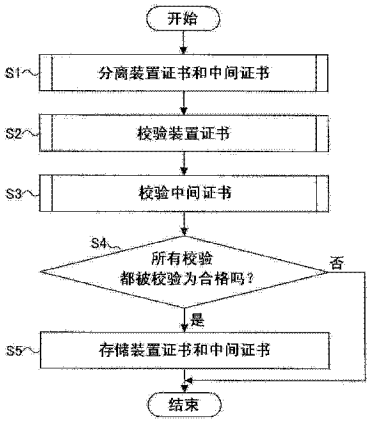
权利要求书 2 页 说明书 10 页 附图 17 页

(54)发明名称

电子装置及导入方法

(57)摘要

本发明公开了一种能够导入电子装置的装置证书以及签署装置证书的中间认证授权的中间证书的电子装置。所述电子装置包括通信单元；分离单元，被配置成分离通过通信单元从中间认证授权获取的中间证书和装置证书；装置证书验证单元，被配置成验证由分离单元分离的装置证书的有效性；中间证书验证单元，被配置成验证由分离单元分离的中间证书的有效性；以及导入单元，被配置成仅当装置证书和中间证书两者都被验证时，导入装置证书和中间证书。



CN 102714596 A

1. 一种电子装置，能够导入所述电子装置的装置证书以及签署所述装置证书的中间认证授权机构的中间证书，其特征在于，所述电子装置包括：

通信单元；

分离单元，被配置成分离通过所述通信单元从所述中间认证授权机构获取的所述中间证书和所述装置证书；

装置证书验证单元，被配置成验证由所述分离单元分离的所述装置证书的有效性；

中间证书验证单元，被配置成验证由所述分离单元分离的所述中间证书的有效性；

导入单元，被配置成仅当所述装置证书和所述中间证书两者都被验证时，导入所述装置证书和所述中间证书。

2. 根据权利要求 1 所述的电子装置，其特征在于，所述装置证书验证单元被配置成通过验证所述装置证书的格式，验证所述装置证书和获取所述装置证书的所述电子装置的名称之间的匹配，以及验证所述装置证书的有效期限来验证所述装置证书的所述有效性。

3. 根据权利要求 1 所述的电子装置，其特征在于，所述中间证书验证单元被配置成通过验证所述中间证书和所述装置证书的链以及验证所述中间证书的有效期限来验证所述中间证书的所述有效性。

4. 根据权利要求 1 所述的电子装置，其特征在于，所述导入单元同时导入所述装置证书和所述中间证书。

5. 根据权利要求 1 所述的电子装置，其特征在于，当延长所述中间证书的有效期限时，所述导入单元仅导入所述中间证书以便更新所述中间证书。

6. 根据权利要求 1 所述的电子装置，其特征在于，进一步包括配置成显示所述装置证书和所述中间证书的详细信息的单元。

7. 一种借助于电子装置的导入方法，所述电子装置能够导入所述电子装置的装置证书以及签署所述装置证书的中间认证授权机构的中间证书，其特征在于，所述方法包括以下步骤：

分离通过通信单元从所述中间认证授权机构获取的所述中间证书和所述装置证书；

验证由所述分离步骤分离的所述装置证书的有效性；

验证由所述分离步骤分离的所述中间证书的有效性；以及

仅当所述装置证书和所述中间证书两者都被验证时，导入所述装置证书和所述中间证书。

8. 根据权利要求 7 所述的导入方法，其特征在于，验证所述装置证书的所述有效性的步骤包括验证所述装置证书的格式，验证所述装置证书和获取所述装置证书的所述电子装置的名称之间的匹配，以及验证所述装置证书的有效期限。

9. 根据权利要求 7 所述的导入方法，其特征在于，验证所述中间证书的所述有效性的步骤包括验证所述中间证书和所述装置证书的链以及验证所述中间证书的有效期限。

10. 根据权利要求 7 所述的导入方法，其特征在于，所述装置证书和所述中间证书在所述导入步骤同时被导入。

11. 根据权利要求 7 所述的导入方法，其特征在于，当延长所述中间证书的有效期限时，在所述导入步骤中仅导入所述中间证书以便更新所述中间证书。

12. 根据权利要求 7 所述的导入方法，其特征在于，进一步包括显示所述装置证书和所

述中间证书的详细信息的步骤。

电子装置及导入方法

技术领域

[0001] 本发明涉及一种电子装置，例如，包括复印机，打印机，传真机以及具有如复印，打印或通信的多种功能的多功能外设（简称为“MFP”）的图像形成装置；图像读取装置（也被称为“扫描装置”）；以及包括个人电脑（PC）的信息处理装置。

背景技术

[0002] 在包括例如数字复印机；打印机；传真机；包括具有如复印，打印或通信的多个功能的 MFP 的图像形成装置；图像读取装置；或 PC 的网络中使用电子证书的认证系统中，通过在网络上设置的根认证授权机构（Root CA）来直接签署最终的电子证书（电子证书包括服务器证书，用户证书以及装置证书）以便验证电子证书的有效性的方案被广泛地使用。

[0003] 如上所述的验证系统变得更加普遍，但是，由于有限数量的根认证授权机构通过直接签署大量的电子证书来执行验证，导致验证系统的处理负荷增加。

[0004] 考虑到这些，开发了这样一种方案，其中除了根认证授权机构还提供了中间认证授权机构，并且中间认证授权机构签署最终的电子证书以便验证有效性。

[0005] 例如，安全超文本传输协议（在下文中简称为“HTTPS”）系统是利用使用电子证书的认证系统的典型实例。在这个系统中，为了验证服务器证书，该服务器证书是通过网络上的根认证授权机构和中间认证授权机构以多级式已经被签署的最终的电子证书，在网络上的 HTTPS 服务器导入中间认证授权机构的电子证书（以下简称为“中间证书”）作为服务器证书并且将中间证书返还给网络上的客户端设备。

[0006] 此外，在上述系统中，为了将中间证书与服务器证书返还给客户端设备，还开发了一种将成对的服务器证书和和中间证书返还给 HTTPS 服务器或者客户端设备的方法。

[0007] 传统地，当使用中间证书时，已经有一种验证证书的技术，它在公开密钥证书是通过不同的认证授权机构发布的情况下，通过利用公开密钥证书的分层结构来减少用户的验证处理（例如，参见专利文献 1）。

[0008] 【专利文献 1】

[0009] 日本专利申请公开公报 NO.H10-215245

[0010] 然而在传统技术中，当将中间证书导入到电子装置中时，中间证书本身的导入必须在使用证书的通信路径上被实现。因此，就有一个问题，当导入中间证书时，如果无效的电子证书被导入，那么引进中间证书的通信就不能被执行。

发明内容

[0011] 考虑到上述要点得到本发明，并且本发明的至少一个实施例的目的是通过通信路径可靠地实现远程导入中间证书。

[0012] 根据本发明的一方面，提供一种能够导入电子装置的装置证书以及签署装置证书的中间认证授权机构的中间证书的电子装置。该电子装置包括通信单元；分离单元，被配置成分离通过通信单元从中间认证授权机构获取的中间证书和装置证书；装置证书验证单

元，被配置成验证通过分离单元分离的装置证书的有效性；中间证书验证单元，被配置成验证通过分离单元分离的中间证书的有效性；以及导入单元，被配置成仅当装置证书和中间证书两者都被验证时导入装置证书和中间证书。

[0013] 根据本发明的另一方面，提供一种通过能够导入电子装置的装置证书以及签署装置证书的中间认证授权机构的中间证书的电子装置的导入方法。该方法包括分离通过通信单元从中间认证授权机构获取的中间证书和装置证书的步骤；验证通过分离步骤分离的装置证书的有效性的步骤；验证通过分离步骤分离的中间证书的有效性的步骤；以及仅当装置证书和中间证书两者都被验证时导入装置证书和中间证书的步骤。

附图说明

[0014] 图 1 是显示图 2 中所示的多功能外设的功能的主要配置的框图；

[0015] 图 2 是显示使用作为本发明的电子装置的一个实施例的多功能外设的网络系统的配置的框图；

[0016] 图 3 是显示装置证书和中间证书之间的链结构的实施例的图；

[0017] 图 4 是显示由如图 1 所示的多功能外设的证书管理器在装置内部管理的证书的状态的实例的图；

[0018] 图 5 是显示将装置证书和中间证书同时导入到如图 2 中所示的网络系统的多功能外设中的处理的时序图；

[0019] 图 6 是显示图 5 中的后续处理的时序图；

[0020] 图 7 是显示将装置证书和中间证书同时导入到如图 1 中所示的多功能外设中的处理的流程图；

[0021] 图 8 是显示用于分离图 7 中所示的装置证书和中间证书的处理的具体处理的流程图；

[0022] 图 9 是显示图 7 中所示的装置证书的验证处理的具体处理的流程图；

[0023] 图 10 是显示图 7 中所示的中间证书的验证处理的具体处理的流程图；

[0024] 图 11 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设中的操作中显示的装置证书屏幕的实例的图；

[0025] 图 12 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设中的操作中显示的证书项目内容输入屏幕的实例的图；

[0026] 图 13 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设中的操作中显示的消息屏幕的实例的图；

[0027] 图 14 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设中的操作中显示的证书详细信息屏幕的实例的图；

[0028] 图 15 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设中的操作中显示的装置证书导入屏幕的实例的图；

[0029] 图 16 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设中的操作中显示的另一个消息屏幕的实例的图；

[0030] 图 17 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设中的操作中显示的错误消息屏幕的实例的图；以及

[0031] 图 18 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设中的操作中显示的另一个证书详细信息屏幕的实例的图。

具体实施方式

[0032] 下面通过参考附图具体描述本发明的实施例。

[0033] [实施例]

[0034] 图 2 是显示使用作为本发明的电子装置的一个实施例的多功能外设的网络系统的配置的框图。

[0035] 这个网络系统的多功能外设(MFP)1 是具有包括扫描功能,复印功能,打印机功能以及通信功能的多种功能的图像形成装置。该多功能外设 1 能够通过局域网(LAN)8 与例如作为多个计算机的第一到第三 PC 的 PC2 通信。

[0036] 此外,证书提供服务器 5 用于将装置证书通过互联网 6 和防火墙 7 发送给多功能外设 1。

[0037] 该证书提供服务器 5 是通过证书提供公司维护的服务器。

[0038] 此外,在互联网 6 上,具有鉴别根认证授权机构 3 本身的有效性的根认证授权机构(Root CA)3,以及例如第一到第三中间认证授权机构的多个中间认证授权机构 4。中间认证授权机构 4 的有效性通过由根认证授权机构 3 的认证而被认证。

[0039] 在图 2 中,多功能外设 1,根认证授权机构 3 以及证书提供服务器 5 中的每一个都只有一个。但是,多功能外设 1,根认证授权机构 3 以及证书提供服务器 5 中的每一个都可以有多个。此外,PC2 和中间认证授权机构 4 的数量不限于 3 个,而可以是更多个。

[0040] 在 PC2 中,预先安装根认证授权机构 3 的电子证书。根认证授权机构 3 的有效性可以通过这些电子证书被验证。

[0041] 证书提供服务器 5 存储例如第一到第三中间认证授权机构的中间认证授权机构 4 的中间证书。证书提供服务器 5 具有这样的功能 :响应于签署通过包括多功能外设 1 和 PC2 的用户请求的装置证书的请求,通过利用中间认证授权机构 4 应用签名。当有来自用户的签署装置证书的请求时,证书提供服务器 5 将通过利用认证授权机构中间认证授权机构 4 已经签署的一对装置证书和应用签名的中间认证授权机构 4 的中间证书返还给用户的多功能外设 1 和 PC 2。

[0042] 在这个实施例中,展示了在使用证书提供公司的证书提供服务器 5 的情况下的网络系统。然而,中间认证授权机构可以被设置在办公室中操作的网络环境中,并且证书签署方法可以在另一个阶段执行。

[0043] 图 1 是显示图 2 中所示的多功能外设 1 的功能的主要配置的框图。

[0044] 该多功能外设 1 具有当导入中间证书时,中间证书可以通过通信路径被远程地可靠地导入的特点。

[0045] 该多功能外设 1 包括通过由 CPU,ROM 和 RAM 形成的微型计算机实现的控制器 10。

[0046] 控制器 10 的网络接口(I/F)11 对应于通过 LAN 8 从包括例如第一到第三 PC 的 PC 2 和如图 2 中所示的证书提供服务器 5 的远程装置接收网络访问的通信单元。

[0047] 例如 HTTP (S) 服务器的网络服务器 12 允许通过 LAN8 利用来自远程装置的浏览器执行各种处理。

[0048] 网络应用 15 可以利用浏览器通过 LAN 8 从远程装置导入各种各样的信息。例如，网络应用 15 能够从证书提供服务器 5 导入多功能外设 1 的装置证书以及相对于装置证书的中间证书。

[0049] 安全管理服务 16 由证书管理器 17，证书利用管理器 18 以及证书验证器 19 形成，并且执行该多功能外设 1 的装置证书的管理服务的处理。

[0050] 证书管理器 17 管理装置证书和中间证书的状态。证书管理器 17 将装置证书和中间证书存储到证书存储区域 20 中并且从证书存储区域 20 删除装置证书和中间证书。

[0051] 证书利用管理器 18 可以管理通过这样方式利用的证书，该方式通过利用装置证书和中间证书的认证客户端 13 以及利用证书的应用 14 来利用。

[0052] 当导入装置证书或者中间证书时，证书验证器 19 验证装置证书和中间证书的有效性。

[0053] 在上述的有效性的验证中，可以验证以下内容。

[0054] 1、证书的格式是否被建立为证书的验证(验证证书的格式)。

[0055] 2、证书的链是否被建立的验证(中间证书与装置证书的链的验证)。

[0056] 3、证书是否在有效期限内的验证(证书的有效期限的验证)。

[0057] 4、证书的公用名是否匹配用于通信的主机名的验证(与获取装置证书的自身装置的名称的匹配的验证)。

[0058] 认证客户端 13 是利用证书的应用 14 中的一个。例如，有 HTTP(S) 服务器，IEEE802.1X 认证客户端等等作为认证客户端 13。实际上可以有利用证书的其他的应用。那些利用证书的应用依赖于利用证书的应用的协议以及实现能够改变证书的处理。

[0059] 例如，在 IEEE802.1X 认证客户端中，服务器侧不是作为能够利用中间证书的方式实现的。因此，这种中间证书不是在多功能外设 1 中操作的设置是可能的。

[0060] 证书存储区域 20 是包括秘密密钥区域 21 和公开密钥区域 22 的记录设备。为了保护秘密密钥区域 21 的秘密密钥，通过设置密码等，秘密密钥能够比公开密钥区域 22 的公开密钥更严格地处理。

[0061] 计时器 23 用于计算时间。计时器 23 能够通过利用 NTP (网络时间协议) 服务器等被设置在准确的时间。当前时间能够被用于判断证书的有效期限。

[0062] 操作显示部 24 根据控制器 10 的控制显示各种操作屏幕，接收相对于操作屏幕的各种信息项目的输入，以及将输入的信息输出到控制器 10。

[0063] 证书管理器 17 起将通过通信单元从中间认证授权机构获取的中间证书和装置证书分离的分离单元的功能，并且起仅当通过装置证书验证单元和中间证书验证单元验证有效性时导入装置证书和中间证书的导入单元的功能。

[0064] 此外，证书验证器 19 起用于验证分开的装置证书的有效性的装置证书验证单元的功能，并且起用于验证相对于装置证书的分开的中间证书的签名的有效性的中间证书验证单元的功能。

[0065] 对于验证，装置证书的有效性是通过验证装置证书的格式、验证装置证书与获取装置证书的自身装置的名称之间的匹配，以及验证装置证书的有效期限验证的。

[0066] 进一步的，中间证书的有效性是通过验证中间证书与装置证书的链，以及验证中间证书的有效期限被验证的。

[0067] 进一步的，证书管理器 17 还起到用于同时导入装置证书和中间证书的单元的功能，或者起到用汉语当延长中间证书的有效期限时，仅导入中间证书以更新中间证书的单元的功能。

[0068] 此外，证书管理器 17 还起到用于显示装置证书和中间证书的详细信息的单元的功能。

[0069] 接下来，描述装置证书和中间证书的链结构的实施例。

[0070] 图 3 是装置证书和中间证书的链结构的实施例的示意图；

[0071] 如图 2 中所示的根认证授权机构 3 的电子证书 30 以初始状态被导入到诸如第一到第三 PC 的每一个 PC 2 中。因此，根认证授权机构 3 的电子证书 30 不需要被验证。

[0072] 第一中间认证授权机构 4 的中间证书 31 通过根认证授权机构 3 被签署。因此具有根认证授权机构 3 的电子证书 30 的例如第一到第三 PC 的每个 PC 2 可以很容易地验证第一中间认证授权机构 4 的中间证书 31。上述情况也适用于第二中间认证授权机构 4 的中间证书 32 和第三中间认证授权机构 4 的中间证书 33。

[0073] 然而，多功能外设 1 的装置证书 34 不是通过根认证授权机构 3 被直接签署的。因此，为了验证多功能外设 1 的装置证书 34，需要第一中间认证授权机构 4 的中间证书 31。上述情况也适用于其它证书 35-37。

[0074] 接下来，图 4 是显示在装置内部通过多功能外设 1 的证书管理器 17 管理的证书的状态的实例的图。

[0075] 相对于装置证书和中间证书，可以执行各种操作，例如“删除”，“生成自身签名证书”，“请求”，“导入(不包括中间证书)”，“导入(包括中间证书)”，“取消请求”，“导入中间证书”以及“删除中间证书”。

[0076] 关于装置证书和中间证书，具有各种状态，例如“未导入(A)”，“请求(B)”，“已导入的(第一中间认证授权机构的)第一中间证书认证授权机构(C)”，“已导入的(第二中间认证授权机构的)第二中间证书(D)”，“已导入并请求的(第一中间认证授权机构的)第一中间证书(E)”，“已导入并请求的(第二中间认证授权机构的)第二中间证书(F)”。

[0077] 在中间证书已经被导入的情况下，当执行导入中间证书的操作时，现有的中间证书被重写。在中间证书已经被导入的情况下，当执行删除中间证书的操作时，现有的中间证书被删除，从而导致没有中间证书存在的状态。

[0078] 进一步的，有依赖于证书的状态不能被处理的操作。

[0079] 接下来，描述当将装置证书和中间证书导入到多功能外设 1 时执行的处理。

[0080] 图 5 和图 6 是显示当将装置证书和中间证书同时导入到如图 2 中所示的网络系统的多功能外设 1 中时进行的处理的时序图。

[0081] 注意图 5 至图 6 中圆圈内的符号 A 到 G 指示了从图 5 到图 6 中各自的连接目标。

[0082] 图 7 是显示当将装置证书和中间证书同时导入到如图 1 中所示的多功能外设 1 中时进行的主程序的处理的流程图。

[0083] 图 8 是显示用于分离图 7 中所示的装置证书和中间证书的处理的子程序处理的流程图。

[0084] 图 9 是显示用于验证图 7 中所示的装置证书的处理的子程序处理的流程图。

[0085] 图 10 是显示用于验证图 7 中所示的中间证书的处理的子程序处理的流程图。

[0086] 图 11 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设 1 中的操作中显示的装置证书屏幕的实例的图。

[0087] 图 12 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设 1 中的操作中显示的证书项目内容输入屏幕的实例的图。

[0088] 图 13 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设 1 中的操作中显示的消息屏幕的实例的图。

[0089] 图 14 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设 1 中的操作中显示的证书详细信息屏幕的实例的图。

[0090] 图 15 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设 1 中的操作中显示的装置证书导入屏幕的实例的图。

[0091] 图 16 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设 1 中的操作中显示的另一个消息屏幕的实例的图。

[0092] 图 17 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设 1 中的操作中显示的错误消息屏幕的实例的图。

[0093] 图 18 是显示将装置证书和中间证书导入到如图 1 中所示的多功能外设 1 中的操作中显示的另一个证书详细信息屏幕的实例的图。

[0094] 当在多功能外设 1 中新导入装置证书时，如图 5 中所示，用户 40 操作操作显示部 24 的浏览器 25 以便打开装置证书屏幕（a1）。然后，浏览器 25 发送装置证书屏幕显示请求给网络服务器 26 （a2）。网络服务器 26 然后发送装置证书屏幕显示请求到网络应用 15（a3）。网络应用 15 向安全管理服务 16 请求获取装置证书的列表（a4）。

[0095] 安全管理服务 16 从证书存储区域 20 获取装置证书信息（a5），基于装置证书信息生成装置证书的列表（a6），并且发送生成的列表给网络应用 15 （a7）。

[0096] 网络应用 15 将基于装置证书列表的装置证书屏幕发送给网络服务器 26 （a8），网络服务器 26 发送装置证书屏幕给浏览器 25 （a9），并且浏览器 25 显示如图 11 中所示的装置证书屏幕。

[0097] 在图 5 中，用户 40 选择用户 40 希望在浏览器 25 的装置证书屏幕上从装置证书列表新导入的装置证书，并且输入生成选定的装置证书的命令的请求（b1）。然后，浏览器 25 将该生成选定的装置证书的命令的请求发送给网络服务器 26（b2）。网络服务器 26 然后发送该生成命令的请求到网络应用 15 （b3）。

[0098] 网络应用 15 响应于生成命令的请求发送证书项目内容输入屏幕给网络服务器 26（b4）。网络服务器 26 发送证书项目内容输入屏幕给浏览器 25 （b5）。浏览器 25 然后显示如图 12 中所示的证书项目内容输入屏幕。

[0099] 在图 5 中，当用户 40 在浏览器 25 的证书项目内容输入屏幕上输入证书项目内容时（c1），浏览器 25 发送证书项目内容给网络服务器 26 （c2）。网络服务器 26 发送证书项目内容给网络应用 15 （c3）。网络应用 15 发送证书项目内容给安全管理服务 16 （c4）。安全管理服务 16 基于证书项目内容生成秘密密钥（c5）并且将秘密密钥存储在证书存储区域 20 的秘密密钥区域 21（c6），并且与执行重启的同时，发送成功的通知给网络应用 15（c7）。

[0100] 用这样的方式，当生成命令时生成秘密密钥，其中生成所述命令用于签署装置证书。这里，秘密密钥在多功能外设 1 的内部生成，然而，秘密密钥可以由外部导入。那时，通

过单独输入用于保护秘密密钥的密码信息等，安全性可以得到提高。

[0101] 网络应用 15 发送重启屏幕给网络服务器 26(c8)，并且网络服务器 26 发送重启屏幕给浏览器 25（c9)。浏览器 25 显示设置被重写的重启屏幕报告，如图 13 中所示。

[0102] 在图 5 中，用户 40 输入命令信息获取请求给浏览器 25(d1)。浏览器 25 发送命令信息获取请求给网络服务器 26（d2)。网络服务器 26 发送命令信息获取请求给网络应用 15（d3)。网络应用 15 发送命令信息获取请求给安全管理服务 16（d4)。安全管理服务 16 从证书存储区域 20 获取命令信息(d5)，从命令信息生成命令字符串(d6)，并且发送命令给网络应用 15（d7)。

[0103] 用这样的方式，为了给证书提供服务器 5 发送命令的内容，从装置证书的证书详细信息获取命令信息。

[0104] 网络应用 15 发送命令屏幕给网络服务器 26（d8)。网络服务器 26 发送命令屏幕给浏览器 25（d9)。浏览器 25 显示如图 14 中所示的证书详细信息屏幕。

[0105] 用这样的方式，装置证书屏幕被打开，证书被选中，并且生成命令。

[0106] 接下来，如图 6 中所示，当用户 40 给浏览器 25 签名请求的指令时(e1)，浏览器 25 发送签名请求和命令给证书提供服务器 5(e2)。从证书提供服务器 5 接收签署的装置证书和装置证书的中间证书(e3)，浏览器 25 显示如图 15 中所示的装置证书导入屏幕。

[0107] 在图 6 中，浏览器 25 发送导入装置证书，签署的装置证书和装置证书的中间证书的指令给网络服务器 26（e4)。网络服务器 26 然后发送导入装置证书，签署的装置证书和装置证书的中间证书的指令给网络应用 15（e5)。网络应用 15 然后发送导入装置证书，签署的装置证书和装置证书的中间证书的指令给安全管理服务 16(e6)，并且同时从网络服务器 26 的主机信息(e7)，并发送主机信息给安全管理服务 16（e8)。

[0108] 安全管理服务 16 分离装置证书和中间证书，验证每个装置证书和中间证书，并且在证书存储区域 20 中存储验证的装置证书和中间证书(e9)。

[0109] 在这个处理中，如图 7 的主程序所示，在步骤(如图中“S”所示)1 中证书管理器 17 分离装置证书和中间证书，在步骤 2 中证书验证器 19 执行装置证书的验证处理来验证装置证书的有效性，并且在步骤 3 中证书验证器 19 执行中间证书的验证处理来验证相对于装置证书的中间证书的签名的有效性，在步骤 4 中证书验证器 19 确定是否所有的装置证书和中间证书的验证都被验证是合格 (OK) 的(有效性的验证是合格的)；如果所有的验证都被验证是合格的，证书管理器 17 将装置证书和中间证书存储在证书存储区域 20 中，并且在步骤 5 中导入装置证书和中间证书，并且终止这个处理。

[0110] 此外，当在步骤 4 中装置证书和中间证书的任何验证都被验证为不合格(NG)时，生成错误通知并且终止这个处理。

[0111] 用这样的方式，在导入装置证书中，装置证书和中间证书被分开，执行每一个装置证书和中间证书的验证，并且仅当装置证书和中间证书两者都验证为合格时，装置证书和中间证书才被存储和导入。

[0112] 在导入这个实施例的装置证书中，装置证书和中间证书是在执行了装置证书和中间证书的验证之后才被存储。

[0113] 接下来，详细描述分离装置证书和中间证书的处理。

[0114] 在分离装置证书和中间证书的处理中，如图 8 的子程序所示，在步骤 11-15 中，证

书管理器 17 对于所有输入的证书重复以下的处理。步骤 12 中，证书管理器 17 确定装置证书是否是对应于存储的秘密密钥的公开密钥公开密钥。如果装置证书是对应于秘密密钥的公开密钥公开密钥，在步骤 13 中，证书管理器 17 将装置证书保持为装置证书。如果装置证书不是对应于秘密密钥的公开密钥公开密钥，在步骤 14 中，证书管理器 17 将证书保持为中间证书。当所有输入的证书被检查过时，处理进行到步骤 16。

[0115] 在步骤 16 中，要确定签署的装置证书是否被存储在证书存储区域 20 中。如果签署的装置证书被存储在证书存储区域 20 中，处理进行到步骤 17。如果签署的装置证书没被存储在证书存储区域 20 中，处理进行到步骤 19。

[0116] 在步骤 17 中，已经导入的装置证书从证书存储区域被获取，并且在步骤 18 中被保持（被重写）为装置证书。然后，处理进行到步骤 19。

[0117] 在步骤 19-22 的处理中，对于所有保持的中间证书的候选者重复进行以下处理。在步骤 20 中，确定装置证书或者中间证书是否被签署。如果装置证书或者中间证书被签署，在步骤 21 中证书被保持为中间证书。如果装置证书或者中间证书没有被签署，则执行对检查下一个候选者的处理。当所有的中间证书的候选者都被检查过时，处理进行到步骤 23。

[0118] 在步骤 23 中，形成装置证书和中间证书的列表，并且处理返回到图 1 中的主程序。

[0119] 用这样的方式，装置证书和中间证书能够被同时输入到相同的文本框。因此，为了知道哪一个是装置证书以及哪一个是中间证书，需要检查与秘密密钥的对应性。

[0120] 在那种情况下，就可以解释对应于秘密密钥的证书是装置证书，而没有对应于秘密密钥的证书是中间证书。

[0121] 因为有多个中间证书存在的可能性，所以中间证书的候选者一旦被检查就验证候选者通过链是否被连接到装置证书。

[0122] 这里，即使当有不是中间证书的候选者存在时，候选者还是被放在中间证书的列表中。

[0123] 在那种情况下，因为不能在中间证书的验证部执行验证，所以错误出现。

[0124] 接下来，详细地描述装置证书的验证处理。

[0125] 关于装置证书的验证处理，如图 9 中的子程序所示，证书验证器 19 在步骤 31 中确定装置证书的公开密钥公开密钥和秘密密钥的验证是否是合格（OK），在步骤 32 中确定装置证书的期限是否在有效期限内，以及在步骤 33 中确定装置证书和通信的主机部分是否匹配。如果所有上述的确定都是合格的（OK），则在步骤 34 中证书验证器 19 确定关于装置证书的验证是合格（OK）的，并且如果至少一个确定是不合格（NG），则在步骤 35 中证书验证器 19 确定关于装置证书的验证是不合格的（NG），并且处理返回到图 1 中的主程序。

[0126] 用这样的方式，在装置证书的验证中，装置证书的有效性通过装置证书的格式的验证，装置证书和获取装置证书的自身装置的名称之间的匹配的验证，以及装置证书的有效期限的验证而被验证。

[0127] 接下来，详细地描述中间证书的验证处理。

[0128] 对于中间证书的验证处理，如图 10 中的子程序所示，在步骤 41-44 的处理中，证书验证器 19 对所有列出的中间证书的候选者重复以下的处理。在步骤 42 中证书验证器 19 执行确定与装置证书或者一级以下的中间证书的链是否被验证为合格（OK）的处理，在步骤

43 中确定中间证书的时间是否是在有效期限以内，以便对所有输入的中间证书的候选者进行检查。如果所有确定都是合格（OK）的，在步骤 45 中，中间证书的验证被确定为合格（OK），并且如果至少一个确定是不合格（NG）的，则在步骤 46 中，中间证书的验证被确定为不合格（NG），并且处理返回到图 1 中的主程序。

[0129] 用这样的方式，在中间证书的验证中，执行与装置证书的链的验证。如果有多个中间证书，则执行多个链的验证。

[0130] 这里，即使当有不是中间证书的候选者存在时，候选者还是在中间证书的列表中。因此，当包括不是中间证书的候选者时，全部的候选者被作为不合格（NG）处理。

[0131] 用这样的方式，在中间证书的验证中，通过验证与装置证书的链和验证中间证书的有效期限来验证中间证书的有效性。

[0132] 接下来，在图 6 中，当装置证书和中间证书已经被成功导入时，安全管理服务 16 将向网络应用 15 报告导入的成功（e10）。网络应用 15 执行重启，并且同时发送重启屏幕给网络服务器 26（e11）。网络服务器 26 发送重启屏幕给浏览器 25（e12）。浏览器 25 显示如图 16 中所示的屏幕。

[0133] 如果装置证书和中间证书不能被导入，安全管理服务 16 向网络应用 15 报告错误（e13）。网络应用 15 发送错误通知屏幕给网络服务器 26（e14）。网络服务器 26 发送错误通知屏幕给浏览器 25（e15）。浏览器 25 显示如图 17 中所示的错误通知屏幕。

[0134] 在上述的导入处理中，当已经有已被导入并正被请求的装置证书时，导入的装置证书和中间证书，以及正被请求的命令可以通过如图 18 中所示的证书详细信息屏幕被同时显示。

[0135] 在这个实施例中，命令被发送到证书提供服务器，并且在接收中间证书和通过中间认证授权机构签署的装置证书的基础上，装置证书和中间证书被验证和导入。这里，装置证书和中间证书可能同时或者分别被导入。

[0136] 要注意的是，当装置证书和中间证书被分别导入时，依赖于浏览器的实现和设置，浏览器的警报（指示证书的签署不能被验证）可以被显示直至中间证书被导入。

[0137] 更进一步地，在这个实施例中已经描述了导入文本格式的证书的情况的实例，但是文件可以被直接发送以便被导入。

[0138] 根据这个实施例，当将中间证书远程地导入到电子装置时，为通信执行最小需要的验证，例如与存储在电子装置中的电子证书的签名匹配。因此，可以通过通信路径将中间证书远程可靠地导入到电子装置中。

[0139] 更进一步地，可以避免影响通信的问题，例如中间证书的文件的破损。

[0140] 此外，通过不将与装置证书没有关系的中间证书相关联，可以避免例如在通信和通信停止时发出警报的问题。

[0141] 此外，由于中间证书的文件的有限期间的截止时间，不会显示警报。

[0142] 更进一步地，由于证书的通用名和主机间的不匹配，不会显示警报。

[0143] 更进一步地，从装置证书被导入时起直至当中间证书被导入时的期间内，不会显示警报。

[0144] 更进一步地，当中间证书的有效期限被延长时，仅仅是中间证书需要被更新。因此，可以减少管理操作。

[0145] 此外，可以很容易的检查中间证书和装置证书之间的关联。因此，可以减少管理操作。

[0146] 根据本发明的电子装置可以应用于一般的电子装置，例如数码复印机；打印机；传真机；包括具有例如复印，打印或通信的多个功能的 MFP 的图像形成装置；图像读取装置；或 PC。

[0147] 根据本发明的至少一个实施例，本发明的电子装置可以通过通信路径可靠地远程导入中间证书。

[0148] 本发明不局限于上述的实施例，在不超出本发明的范围内可以做出变化和修改。

[0149] 本申请是基于申请日为 2010 年 1 月 22 日在日本专利局提交的日本在先专利申请 NO. 2010-012443，其全部内容通过引用而结合在本文中。

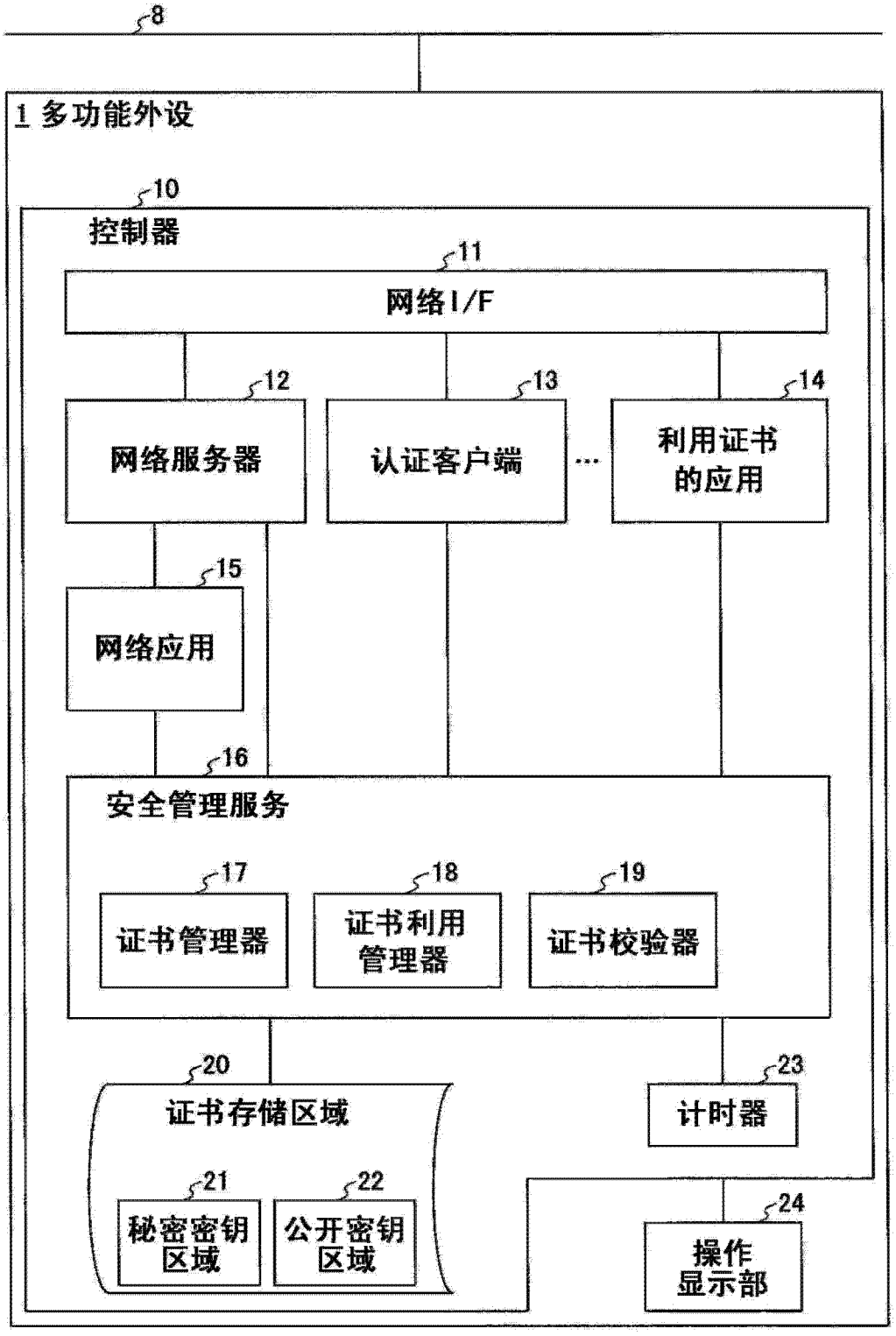

8
1 多功能外设
10
控制器
11
网络I/F
12
网络服务器
13
认证客户端
14
利用证书的应用
15
网络应用
16
安全管理服务
17
证书管理器
18
证书利用管理器
19
证书校验器
20
证书存储区域
21
秘密密钥区域
22
公开密钥区域
23
计时器
24
操作显示部

图 1

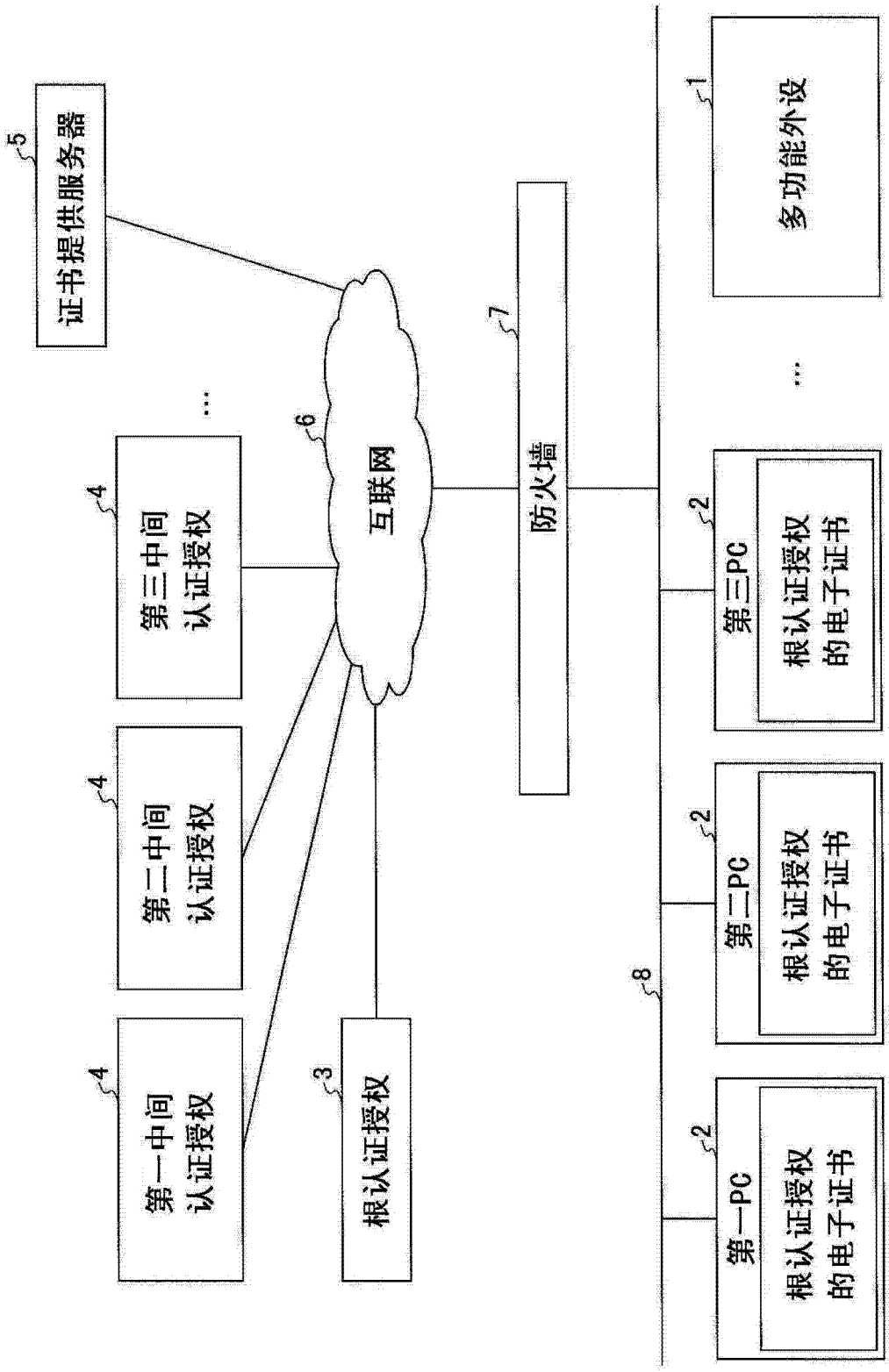

证书提供服务器
5
互联网
6
防火墙
7
多功能外设
1
第三中间
认证授权
4
第二中间
认证授权
4
第一中间
认证授权
4
根认证授权
3
第三PC
根认证授权
的电子证书
2
第二PC
根认证授权
的电子证书
2
第一PC
根认证授权
的电子证书
2
8

图 2

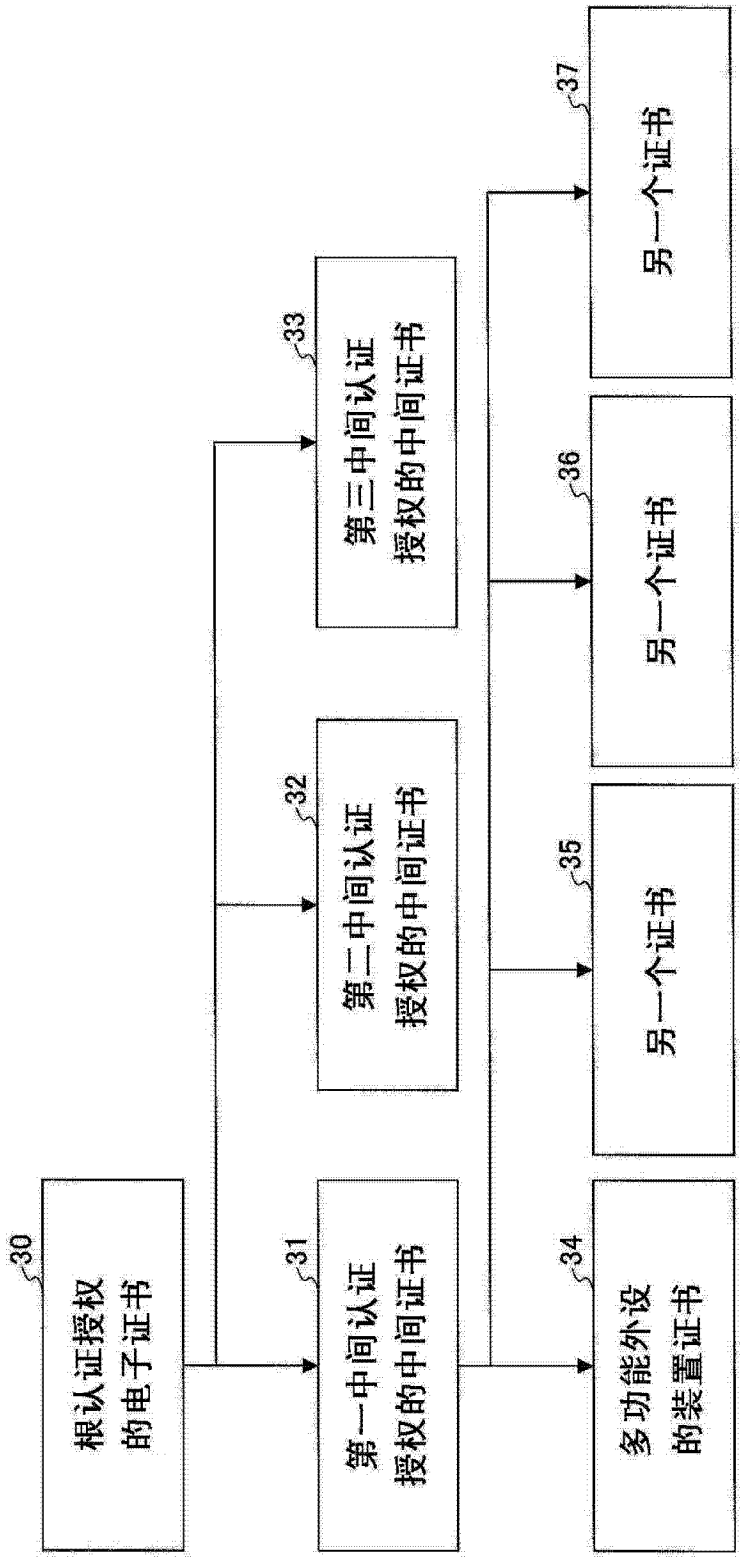
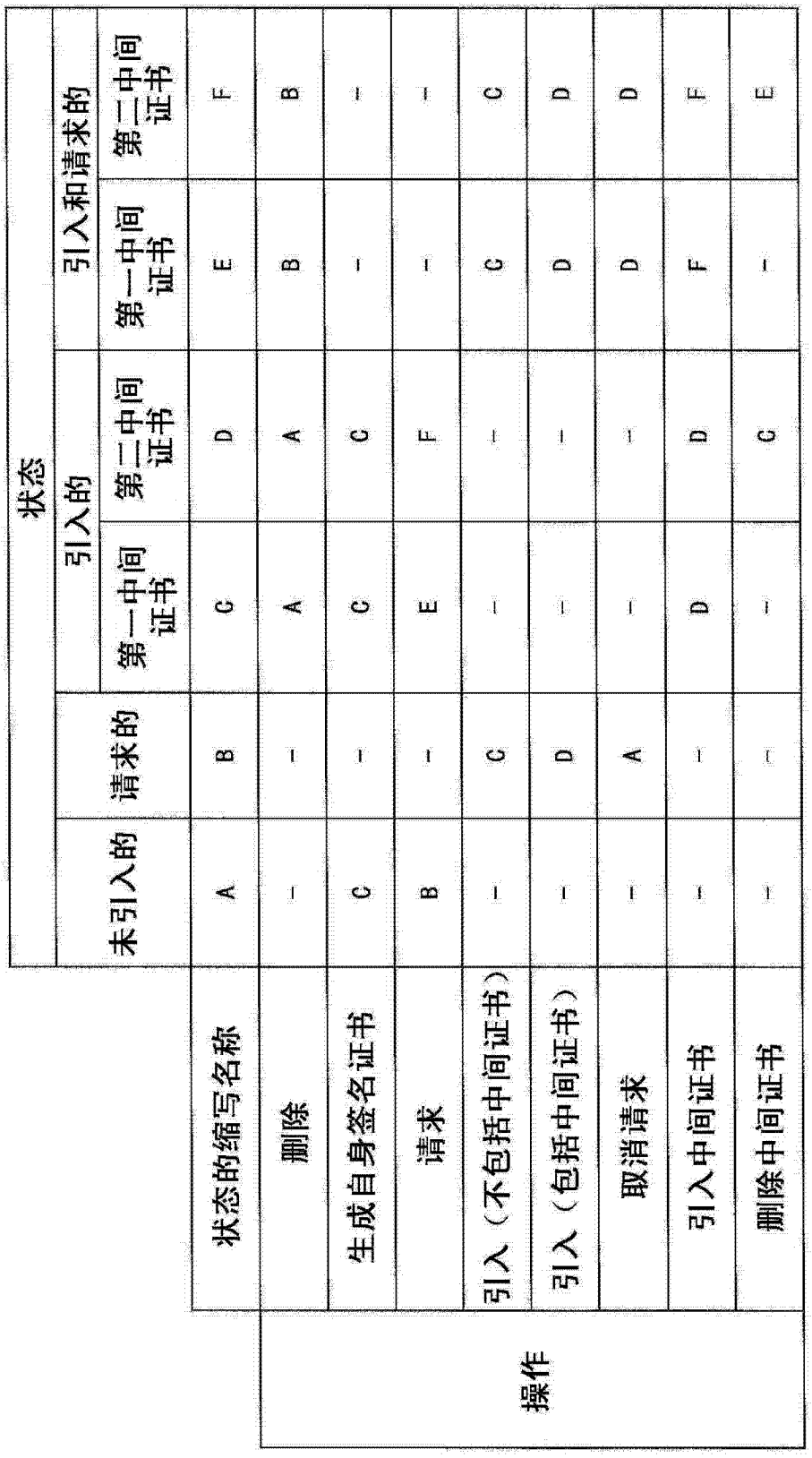

30
根认证授权的电子证书
31
第一中间认证授权的中间证书
32
第二中间认证授权的中间证书
33
第三中间认证授权的中间证书
34
多功能外设的装置证书
35
另一个证书
36
另一个证书
37
另一个证书

图 3



操作	状态的缩写名称	状态					
		未引入的	请求的	引入的		引入和请求的	
				第一中间证书	第二中间证书	第一中间证书	第二中间证书
删除		A	B	C	D	E	F
		-	-	A	A	B	B
生成自身签名证书		C	-	C	C	-	-
请求		B	-	E	F	-	-
引入（不包括中间证书）		-	C	-	-	C	C
引入（包括中间证书）		-	D	-	-	D	D
取消请求		-	A	-	-	D	D
引入中间证书		-	-	D	D	F	F
删除中间证书		-	-	-	C	-	E

图 4

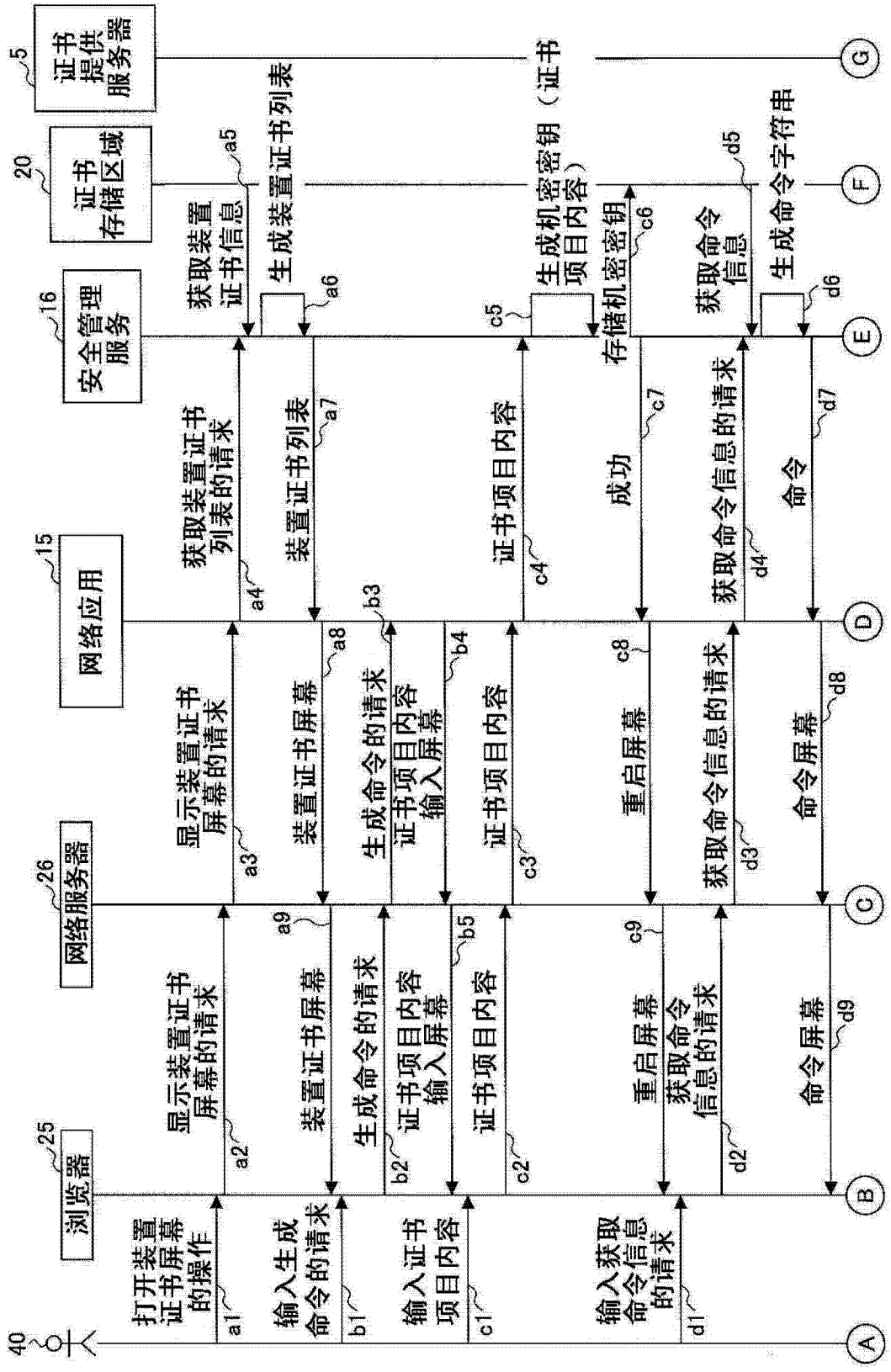

40
浏览器
25
网络服务器
26
网络应用
15
安全管理服务
16
证书存储区域
20
证书提供服务器
5
打开装置证书屏幕的操作
a1
显示装置证书屏幕的请求
a2
显示装置证书屏幕的请求
a3
获取装置证书列表的请求
a4
获取装置证书信息
a5
生成装置证书列表
a6
装置证书列表
a7
装置证书屏幕
a8
装置证书屏幕
a9
输入生成命令的请求
b1
生成命令的请求
b2
生成命令的请求
b3
证书项目内容输入屏幕
b4
证书项目内容输入屏幕
b5
输入证书项目内容
c1
证书项目内容
c2
证书项目内容
c3
证书项目内容
c4
生成机密密钥（证书项目内容）
c5
存储机密密钥
c6
成功
c7
重启屏幕
c8
重启屏幕
c9
输入获取命令信息的请求
d1
获取命令信息的请求
d2
获取命令信息的请求
d3
获取命令信息的请求
d4
获取命令信息
d5
生成命令字符串
d6
命令
d7
命令屏幕
d8
命令屏幕
d9
A
B
C
D
E
F
G

图 5

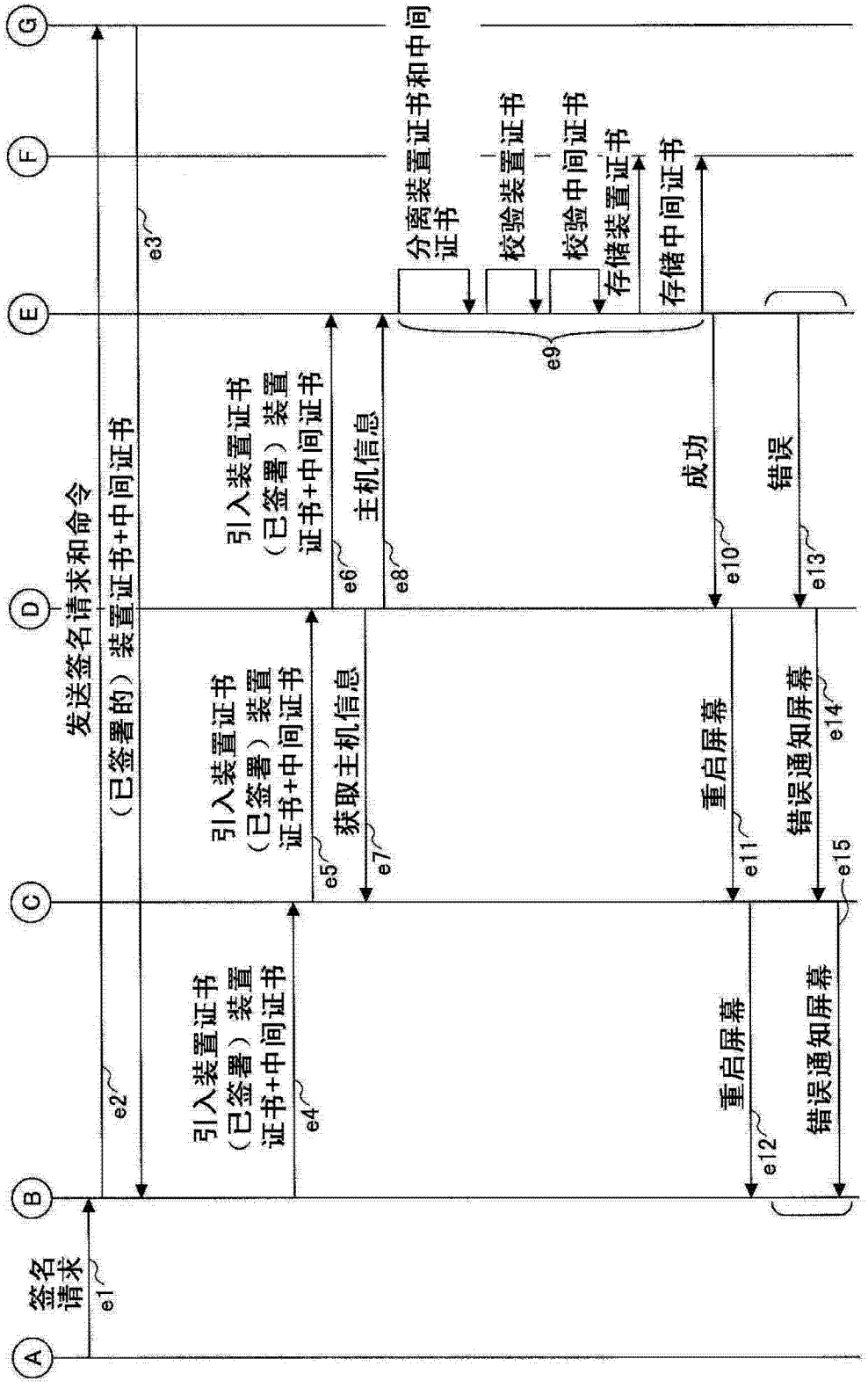

A
B
C
D
E
F
G
签名请求
e1
发送签名请求和命令
（已签署的）装置证书+中间证书
e2
e3
引入装置证书
（已签署）装置
证书+中间证书
e4
引入装置证书
（已签署）装置
证书+中间证书
e5
获取主机信息
e7
引入装置证书
（已签署）装置
证书+中间证书
e6
主机信息
e8
分离装置证书和中间证书
校验装置证书
校验中间证书
存储装置证书
存储中间证书
e9
成功
e10
重启屏幕
e11
重启屏幕
e12
错误
e13
错误通知屏幕
e14
错误通知屏幕
e15

图 6

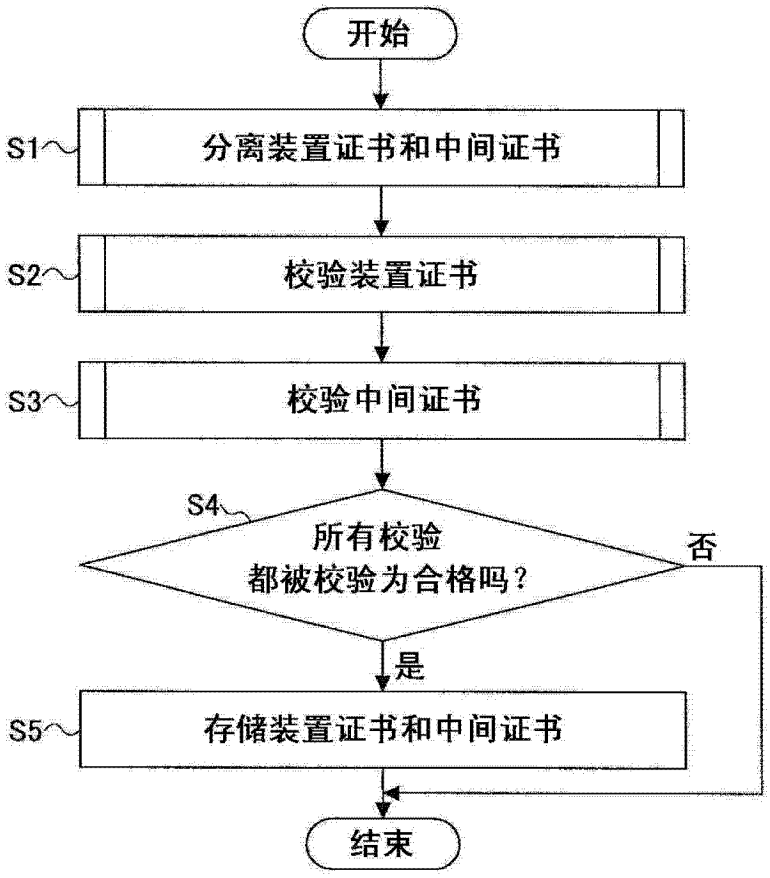

开始
S1
分离装置证书和中间证书
S2
校验装置证书
S3
校验中间证书
S4
所有校验
都被校验为合格吗？
否
是
S5
存储装置证书和中间证书
结束

图 7

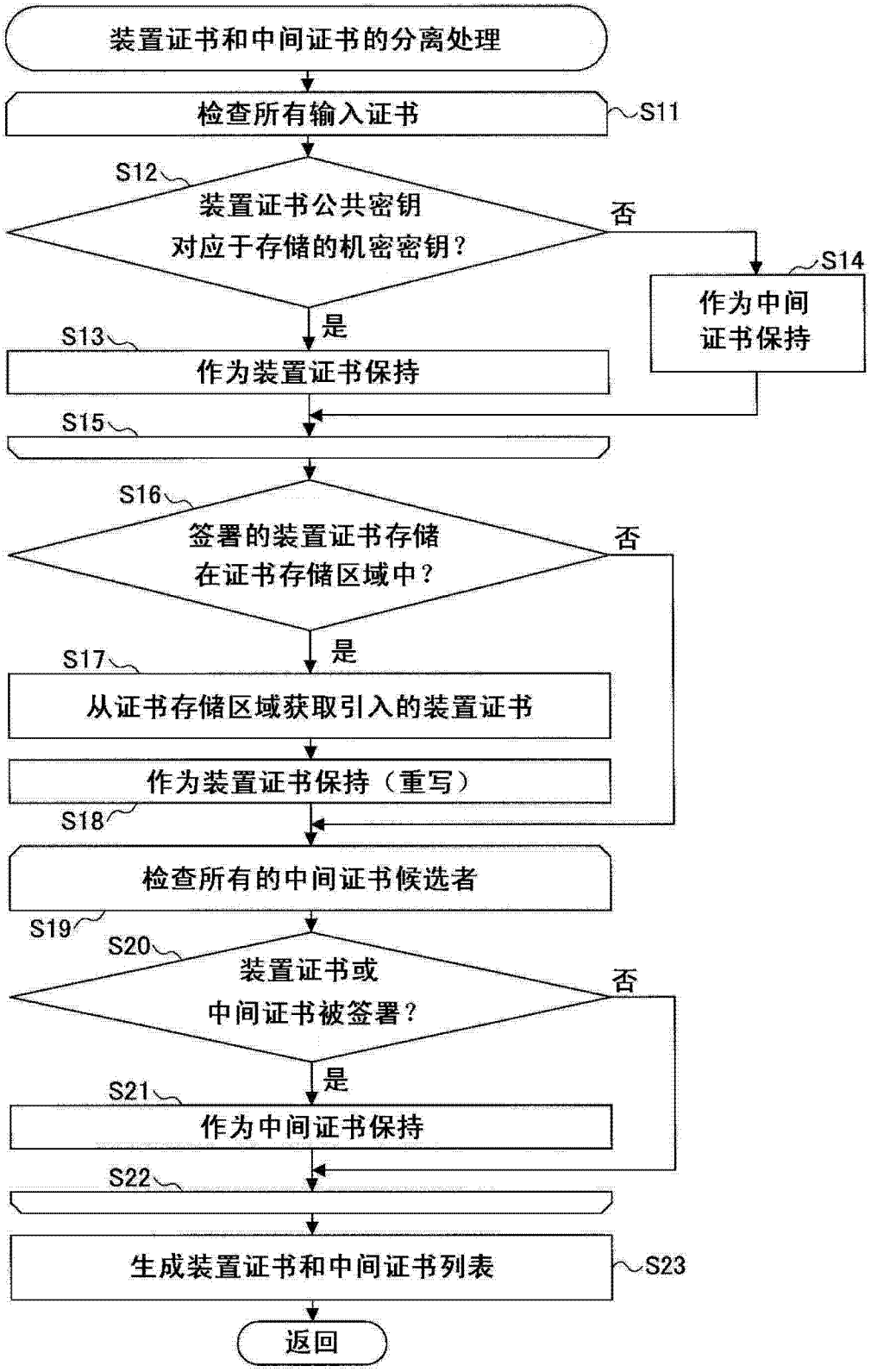

装置证书和中间证书的分离处理
检查所有输入证书
S11
S12
装置证书公共密钥
对应于存储的机密密钥？
否
S14
作为中间
证书保持
是
S13
作为装置证书保持
S15
S16
签署的装置证书存储
在证书存储区域中？
否
是
S17
从证书存储区域获取引入的装置证书
作为装置证书保持（重写）
S18
检查所有的中间证书候选者
S19
S20
装置证书或
中间证书被签署？
否
是
S21
作为中间证书保持
S22
生成装置证书和中间证书列表
S23
返回

图 8

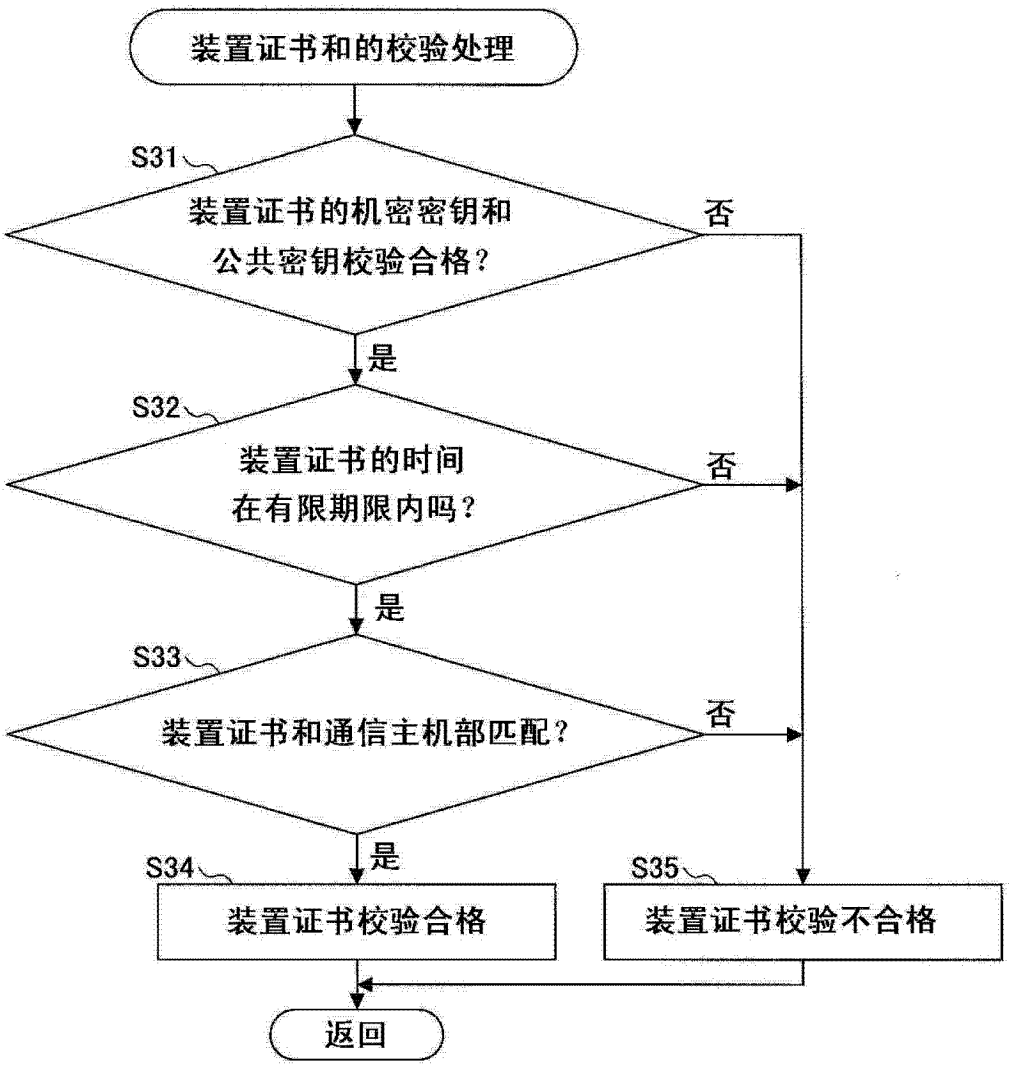

装置证书和的校验处理
S31
装置证书的机密密钥和
公共密钥校验合格？
否
是
S32
装置证书的时间
在有限期限内吗？
否
是
S33
装置证书和通信主机部匹配？
否
是
S34
装置证书校验合格
S35
装置证书校验不合格
返回

图 9

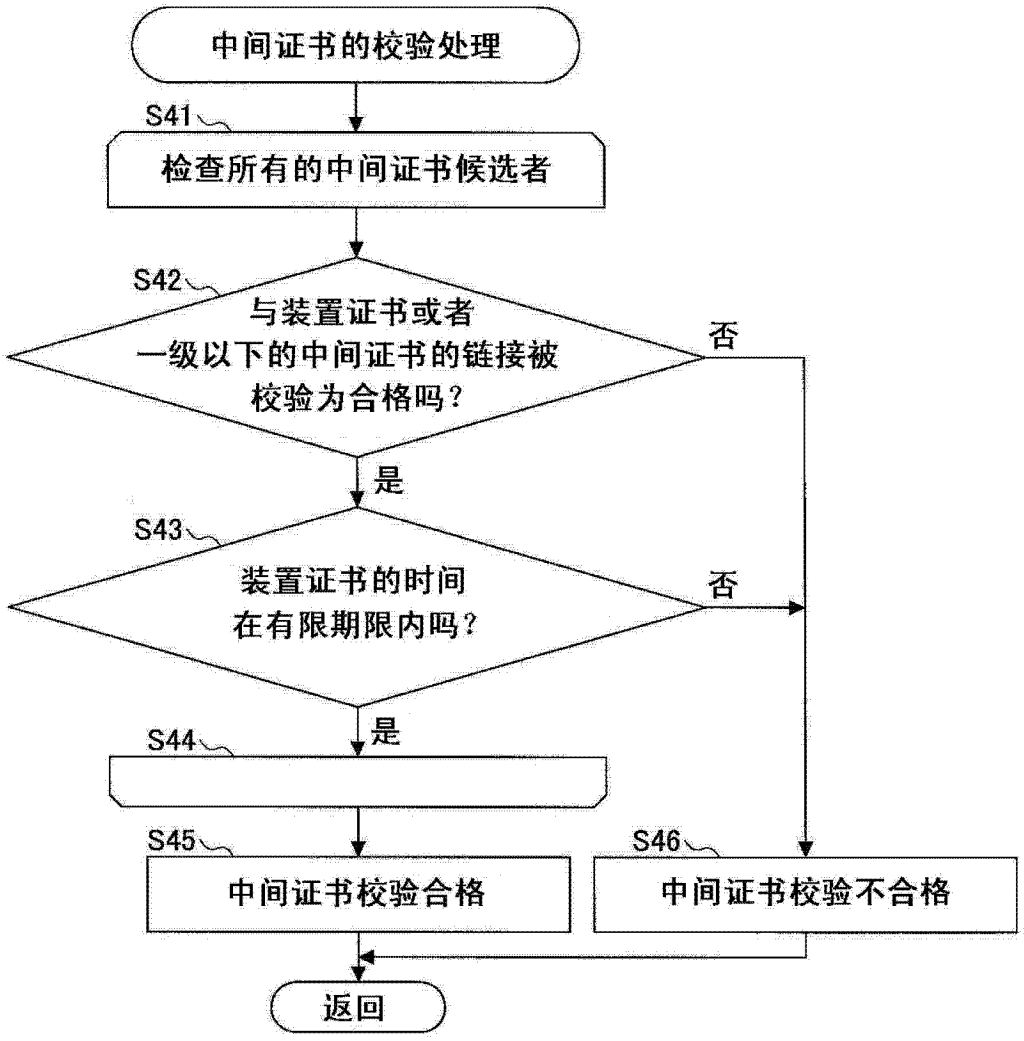

中间证书的校验处理
S41
检查所有的中间证书候选者
S42
与装置证书或者
一级以下的中间证书的链接被
校验为合格吗？
否
是
S43
装置证书的时间
在有限期限内吗？
否
是
S44
S45
中间证书校验合格
S46
中间证书校验不合格
返回

图 10

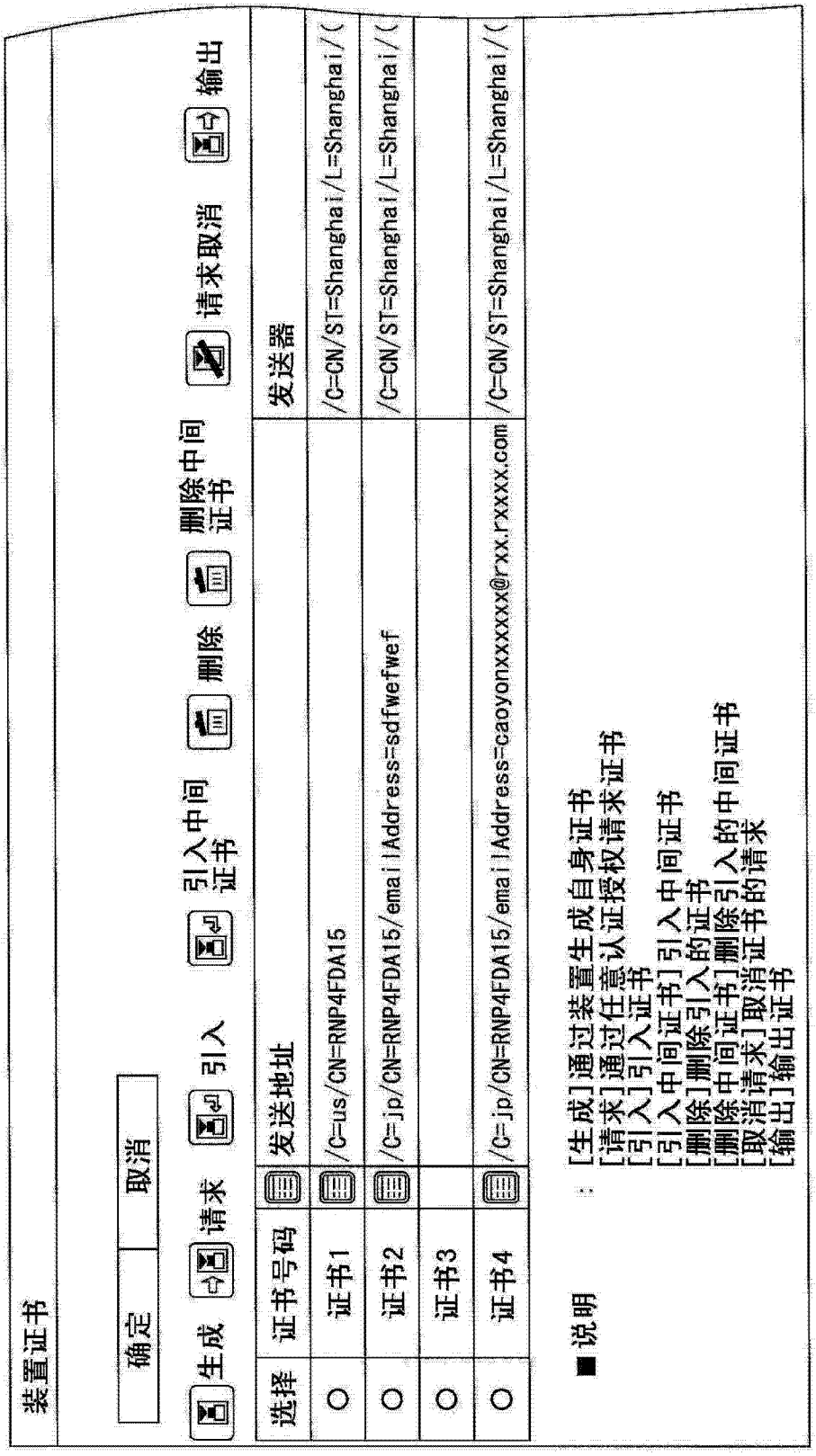

装置证书
确定
取消
生成
请求
引入
引入中间证书
删除
删除中间证书
请求取消
输出
选择
证书号码
发送地址
发送器
证书1
/C=us/CN=RNP4FDA15
/C=CN/ST=Shanghai/L=Shanghai/(
证书2
/C=jp/CN=RNP4FDA15/emailAddress=sdfwefwef
/C=CN/ST=Shanghai/L=Shanghai/(
证书3
证书4
/C=jp/CN=RNP4FDA15/emailAddress=caoyonxxxxxx@rxx.rxxxx.com
/C=CN/ST=Shanghai/L=Shanghai/(
■说明
[生成]通过装置生成自身证书
[请求]通过任意认证授权请求证书
[引入]引入证书
[引入中间证书]引入中间证书
[删除]删除引入的证书
[删除中间证书]删除引入的中间证书
[取消请求]取消证书的请求
[输出]输出证书

图 11

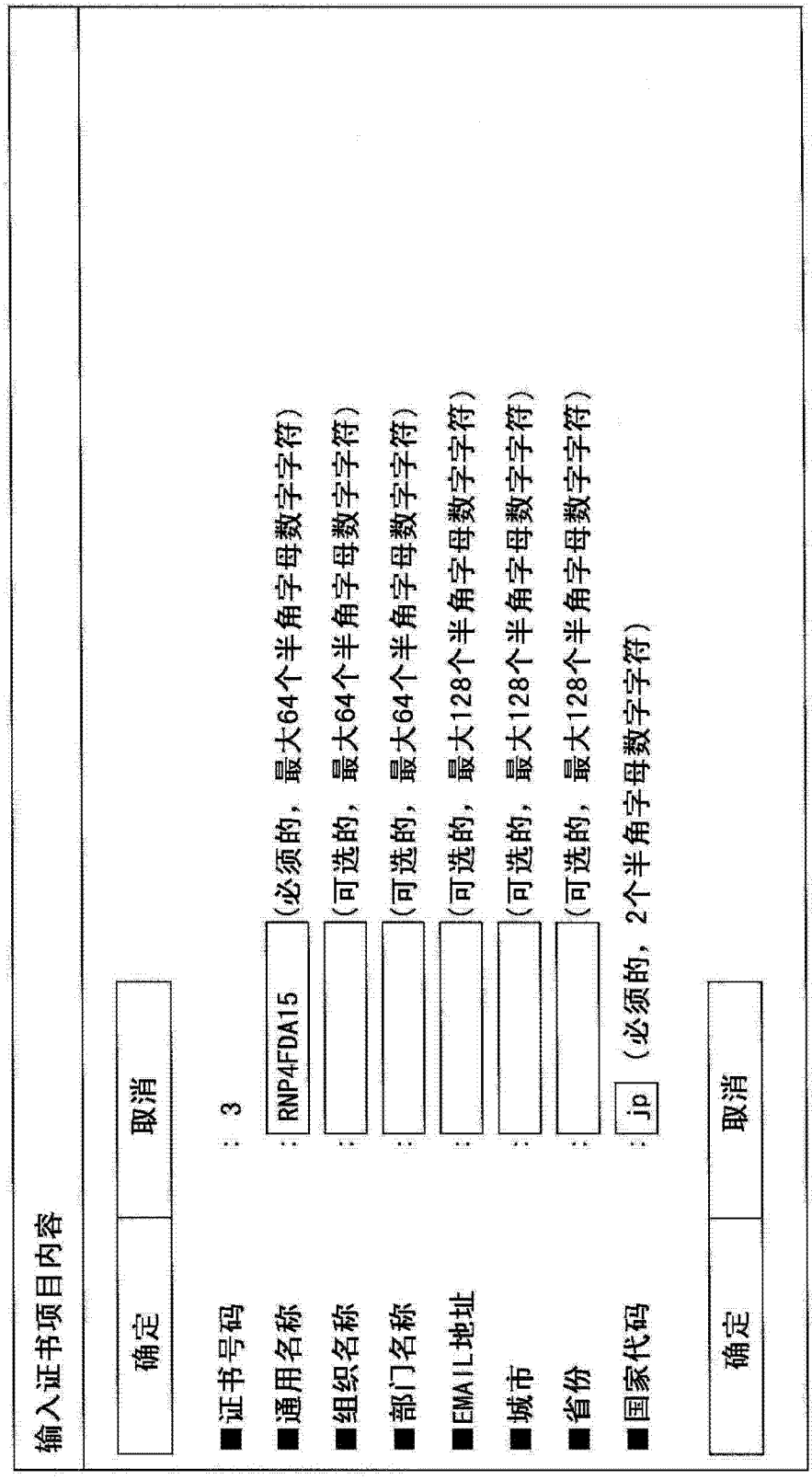

输入证书项目内容
确定
取消
■证书号码 : 3
■通用名称 : RNP4FDA15 (必须的，最大64个半角字母数字字符)
■组织名称 : (可选的，最大64个半角字母数字字符)
■部门名称 : (可选的，最大64个半角字母数字字符)
■EMAIL地址 : (可选的，最大128个半角字母数字字符)
■城市 : (可选的，最大128个半角字母数字字符)
■省份 : (可选的，最大128个半角字母数字字符)
■国家代码 : jp (必须的，2个半角字母数字字符)
确定
取消

图 12

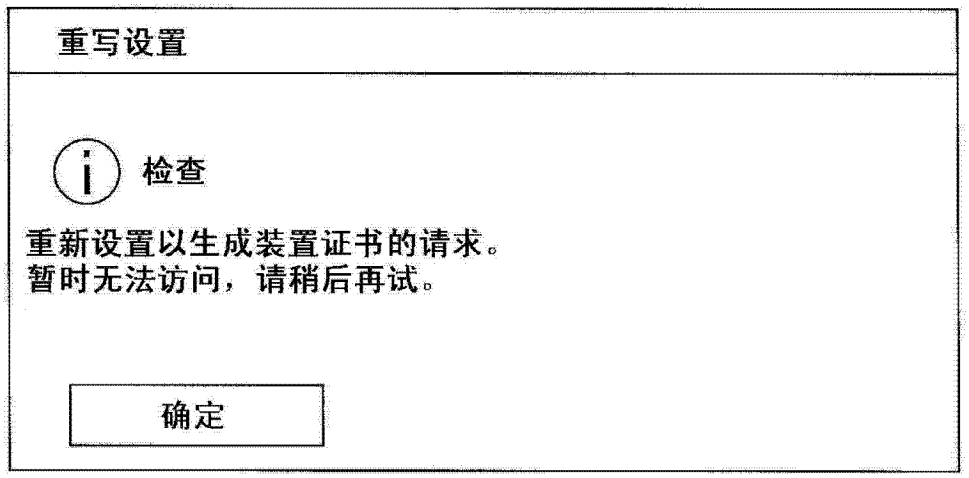


图 13

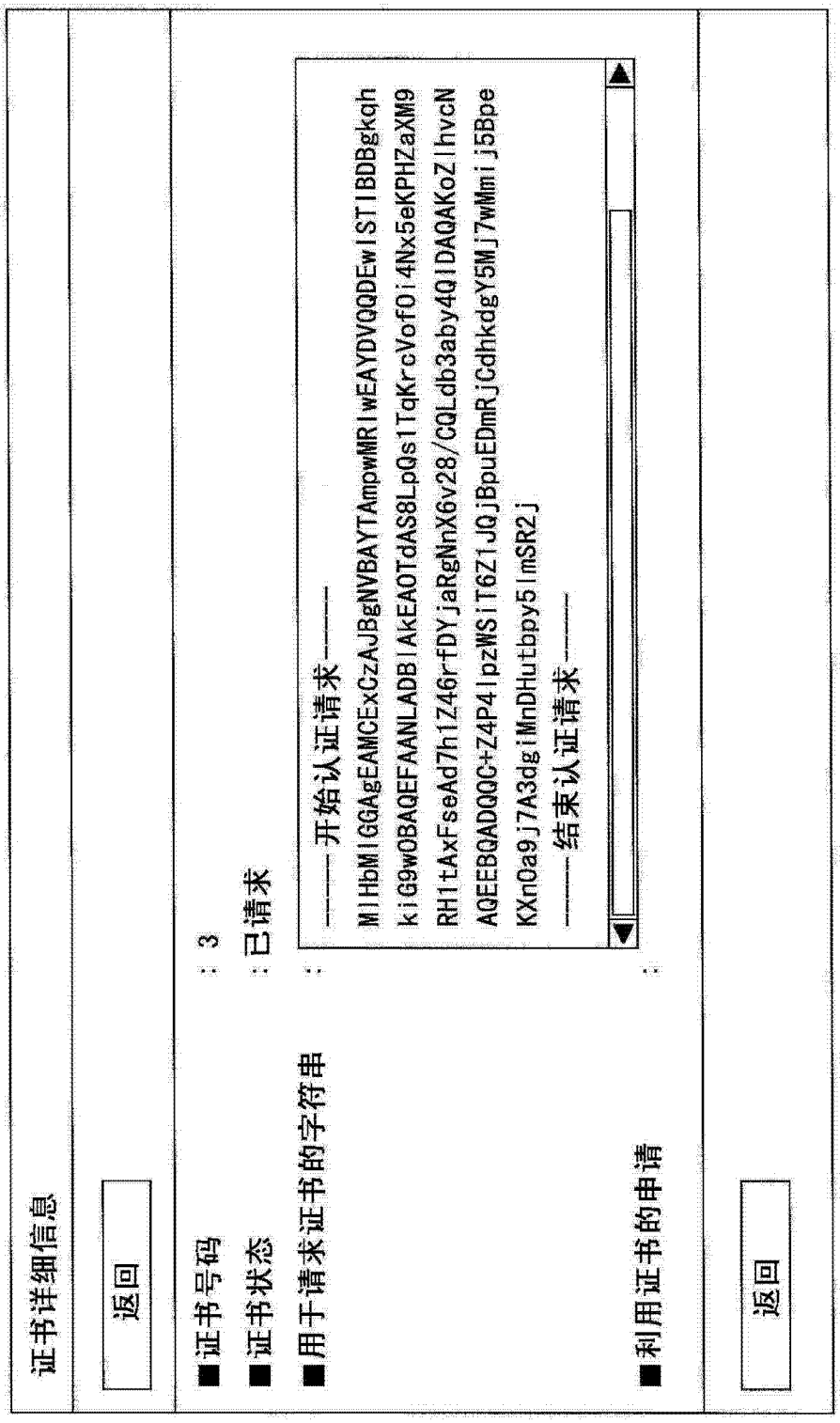

证书详细信息
返回
■证书号码 : 3
■证书状态 : 已请求
■用于请求证书的字符串 :
-----开始认证请求-----
MIHbMIGGAgEAMCExCzAJBgNVBAYTAmpwMRIwEAYDVQQDEwlSTIBDBgkqh
kiG9w0BAQEFAANLADBIAkEAOTdAS8LpQs1TqKrcVofOi4Nx5eKPHZaXM9
RH1tAxFseAd7h1Z46rfDYjaRgNnX6v28/CQLdb3aby4QIDAQAKoZIhvcN
AQEEBQADQQC+Z4P4IpzWSiT6Z1JQjBpuEDmRjCdhkdgY5MJ7wMmi j5Bpe
KXnOa9j7A3dgiMnDHutbpy5ImSR2j
-----结束认证请求-----
■利用证书的申请 :
返回

图 14

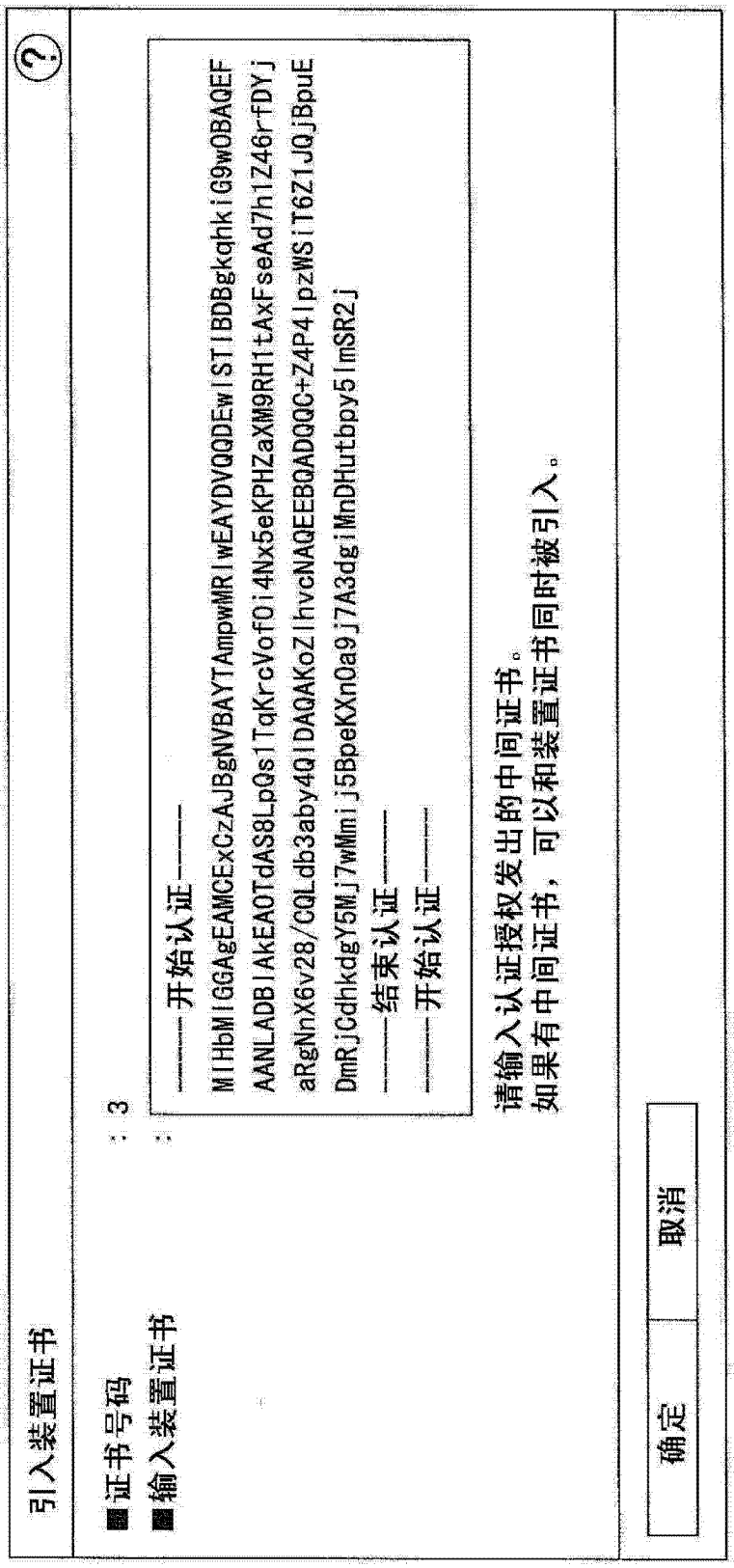

引入装置证书
?
■证书号码 : 3
■输入装置证书 :
-----开始认证-----
MIHbMIGGAgEAMCExCzAJBgNVBAYTAmpwMRIwEAYDVQQDEwlSTIBDBgkqhkiG9w0BAQEF
AANLADBIAkEA0TdAS8LpQs1TqKrcVofOi4Nx5eKPHZaXM9RH1tAxFseAd7h1Z46rfDYj
aRgNnX6v28/CQLdb3aby4QIDAQAKoZIhvcNAQEEBQADQQC+Z4P4IpzWSiT6Z1JQjBpuE
DmRjCdhkdgY5Mj7wMmij5BpeKXn0a9j7A3dgiMnDHutbpy5lmSR2j
-----结束认证-----
-----开始认证-----
请输入认证授权发出的中间证书。
如果有中间证书，可以和装置证书同时被引入。
确定
取消

图 15

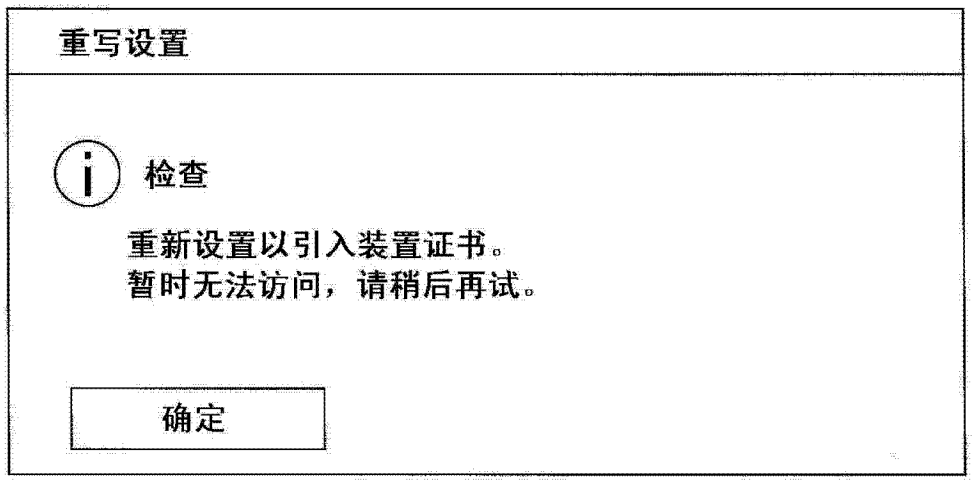

重写设置
检查
重新设置以引入装置证书。
暂时无法访问，请稍后再试。
确定

图 16

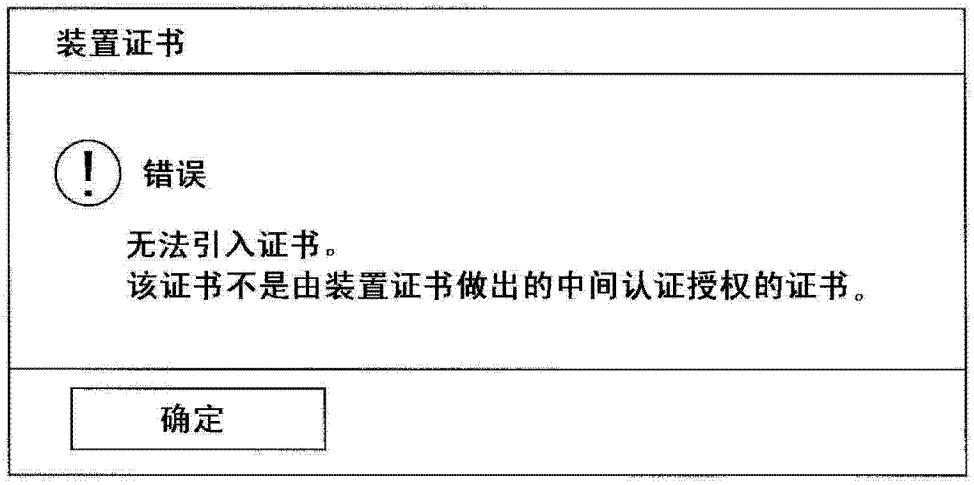

装置证书
错误
无法引入证书。
该证书不是由装置证书做出的中间认证授权的证书。
确定

图 17

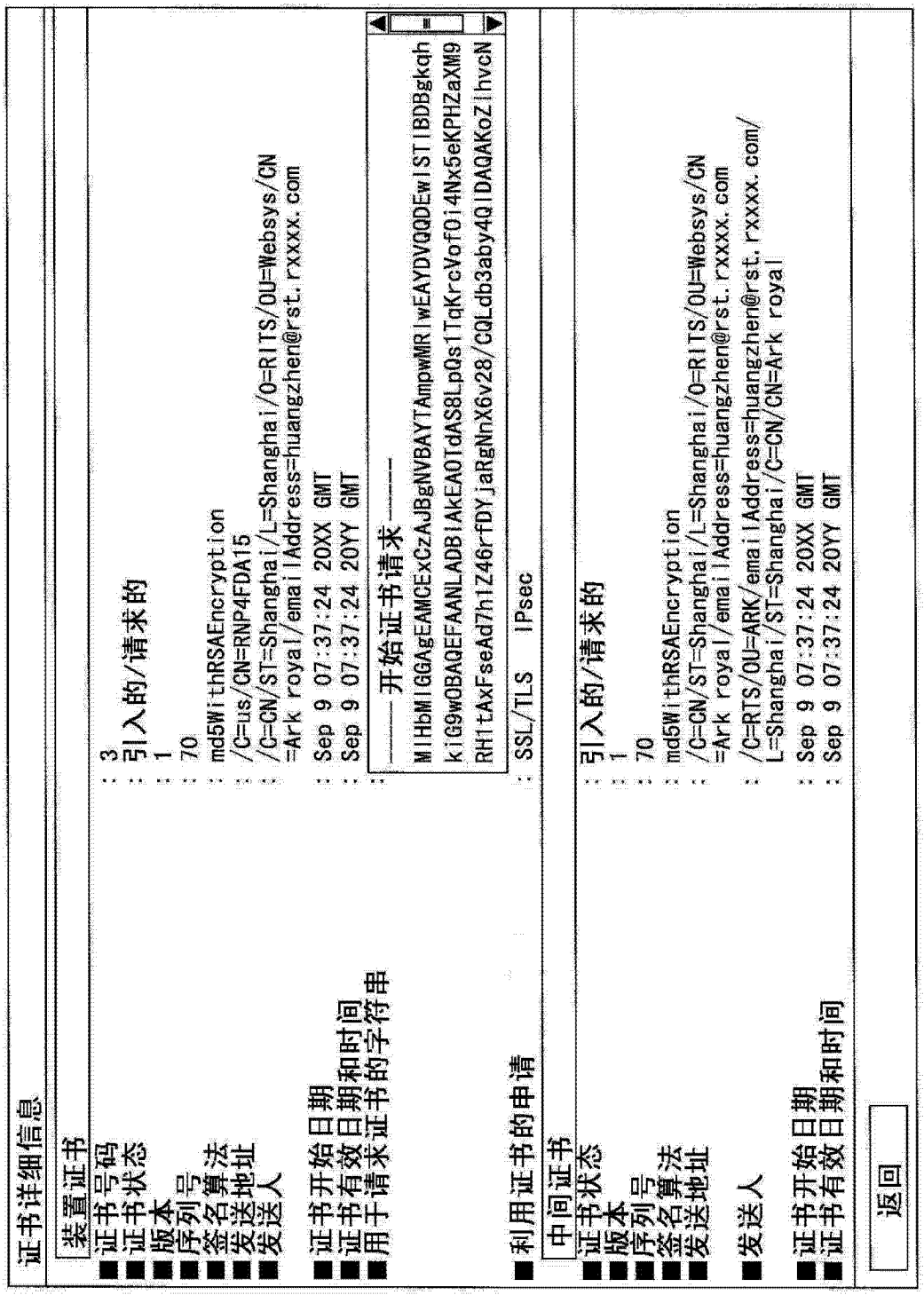

证书详细信息
装置证书
■证书号码 : 3
■证书状态 : 引入的/请求的
■版本 : 1
■序列号 : 70
■签名算法 : md5WithRSAEncryption
■发送地址 : /C=us/CN=RNP4FDA15
■发送人 : /C=CN/ST=Shanghai/L=Shanghai/O=RITS/OU=Websys/CN
=Ark royal/emailAddress=huangzhen@rst.rxxxx.com
■证书开始日期 : Sep 9 07:37:24 20XX GMT
■证书有效日期和时间 : Sep 9 07:37:24 20YY GMT
■用于请求证书的字符串 : -----开始证书请求-----
MIHbMIGGAgEAMCExCzAJBgNVBAYTAmpwMRIwEAYDVQQDEwlSTIBDBgkqh
kiG9w0BAQEFAANLADBIAkEA0IdAS8LpQs1TqKrcVofOi4Nx5eKPHZaXM9
RH1tAxFseAd7h1Z46rfDYjaRgNnX6v28/CQLdb3aby4QIDAQAKoZIhvcN
■利用证书的申请 : SSL/TLS IPsec
中间证书
■证书状态 : 引入的/请求的
■版本 : 1
■序列号 : 70
■签名算法 : md5WithRSAEncryption
■发送地址 : /C=CN/ST=Shanghai/L=Shanghai/O=RITS/OU=Websys/CN
=Ark royal/emailAddress=huangzhen@rst.rxxxx.com
■发送人 : /C=RTS/OU=ARK/emailAddress=huangzhen@rst.rxxxx.com/
L=Shanghai/ST=Shanghai/C=CN/CN=Ark royal
■证书开始日期 : Sep 9 07:37:24 20XX GMT
■证书有效日期和时间 : Sep 9 07:37:24 20YY GMT
返回

图 18