(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 103080958 A
(43)申请公布日 2013.05.01

(21)申请号 201180035945.1
(22)申请日 2011.07.08
(30)优先权数据
10-2010-0065985 2010.07.08 KR
10-2010-0131936 2010.12.21 KR
10-2010-0131935 2010.12.21 KR
10-2011-0067188 2011.07.07 KR
(85)PCT申请进入国家阶段日
2013.01.22
(86)PCT申请的申请数据
PCT/KR2011/005039 2011.07.08
(87)PCT申请的公布数据
WO2012/005555 KO 2012.01.12

(71)申请人 情报通信产业振兴院
地址 韩国首尔
(72)发明人 安大燮 李重九 孔圣弼 林映哲
(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 余刚 吴孟秋

(51)Int.Cl.
G06Q 10/10(2012.01)
H04L 12/58(2006.01)

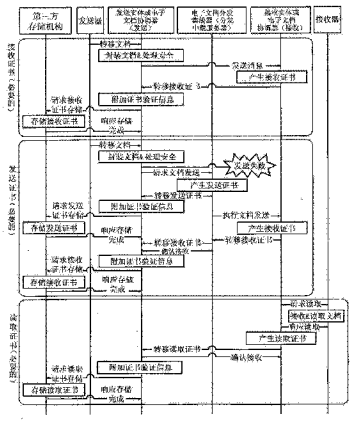
权利要求书3页 说明书18页 附图2页

(54)发明名称

用于产生/发行电子文档分发证书的方法、用于验证电子文档分发证书的方法以及用于分发电子文档的系统

(57)摘要

本发明涉及在基于公共电子地址的电子文档分发系统中产生、分发和存储分发证书，尤其是涉及一种用于产生/发行电子文档分发证书的方法、验证电子文档分发证书的方法以及用于分发电子文档的系统，该系统可以提供透明且有效的发行服务，而且由于该证书兼容的安全性而能够提高电子文档的分发可靠性。根据本发明的优选实施方式，上述用于产生/发行电子文档分发证书的方法涉及在包括发送和接收对象以及分发集线器的电子文档分发系统中产生/发行分发证书的方法，并且包括如下步骤：通过发送对象将包括发送器的电子文档的分发消息发送至接收对象；接收分发消息，获得必要信息并通过接收对象产生接收证书；通过接收对象将所产生的接收证书发送至发送对象；在完成接收证书的验证之后，通过发送对象添加关于所接收的接收证书的电子签名证书的验证信息至接收证书；以及通过发送对象将接收证书发送至第三方存储机构并请求第三方存储机构存储接收证书。



CN 103080958 A

1. 一种用于在分发电子文档的系统中产生 / 发行分发证书的方法，所述系统包括发送实体和接收实体以及分发集线器，该方法包括 ：

（a）通过发送实体，将包括发送器的电子文档的分发消息发送至接收实体 ；

（b）通过接收实体接，在接收所述分发消息后通过获取必要信息而产生接收证书 ；

（c）通过所述接收实体将所产生的接收证书发送至所述发送实体 ；

（d）通过所述发送实体完成对所接收的接收证书的验证，然后，将关于所述接收证书的电子签名证书的验证信息附加至所述接收证书 ；以及

（e）通过所述发送实体将所述接收证书发送至第三方存储机构并请求向其存储。

2. 根据权利要求 1 所述的方法，其中，在所述步骤（b）中，当所述接收实体产生所述接收证书时，所述必要信息包括电子文档信息、发送器、接收器、发送器发送时间以及接收器接收时间。

3. 根据权利要求 1 所述的方法，进一步包括 ：

在所述步骤（a）中，当所述发送实体试图将所述分发消息发送至所述接收实体但却在所述分发消息的发送中失败时，

（a1）通过所述发送实体请求将所述分发消息发送至所述分发集线器的分发中继服务器 ；

（a2）通过所述分发中继服务器对所请求的发送产生所述发送证书 ；

（a3）通过所述分发中继服务器将所述发送证书发送至所述发送实体 ；

（a4）通过所述发送实体完成对所接收的接收证书的验证，然后将关于所述接收证书的所述电子签名证书的验证信息附加至所述接收证书 ；并且

（a5）通过所述发送实体将所述接收证书发送至所述第三方存储机构并向其请求存储 ；

（a6）通过所述分发中继服务器将所述分发消息发送至所述接收实体 ；

（a7）通过所述接收实体在接收所述电子文档之后立即产生所述接收证书 ；

（a8）通过所述接收实体将所述接收证书发送至所述分发中继服务器 ；

（a9）通过所述分发中继服务器将所述接收证书发送至所述发送实体 ；以及

（a10）通过所述接收实体依次执行步骤（d）和（e）。

4. 根据权利要求 3 所述的方法，其中，在所述步骤（a2）中，当所述分发中继服务器产生所述发送证书时，所述必要信息包括电子文档信息、发送器、接收器和发送器发送请求时间。

5. 根据权利要求 1 所述的方法，进一步包括 ：

在所述步骤（e）之后，

（f1）通过所述接收器读取通过向所述接收实体请求所述分发消息的读取而接收的所述分发消息 ；

（f2）通过所述接收实体产生读取证书 ；

（f3）完成对所接收的读取证书的验证，然后将关于所述读取证书的所述电子签名证书的验证信息附加至所述读取证书 ；以及

（f4）通过所述发送实体将所述读取证书发送至所述第三方存储机构并向其请求存储。

6. 根据权利要求 3 所述的方法，进一步包括 ：

在所述步骤(a10)之后,

(a11)通过所述接收器读取通过向所述接收实体请求所述分发消息的读取而接收的所述分发消息;

(a12)通过所述接收实体产生所述读取证书;

(a13)完成对所接收的读取证书的验证,然后将关于所述读取证书的所述电子签名证书的验证信息附加至所述读取证书;以及

(a14)通过所述发送实体将所述读取证书发送至所述第三方存储机构并向其请求存储。

7. 根据权利要求 5 或 6 所述的方法,其中,当所述接收实体产生所述读取证书时,所述必需信息包括电子文档信息、发送器、接收器、发送器发送时间、接收器接收时间以及接收器读取时间。

8. 一种验证在用于分发电子文档的系统中产生 / 发行的分发证书的方法,所述系统包括发送实体和接收实体以及分发集线器,所述方法包括:

验证分发证书的格式是否遵循预定义的结构和值的约束;

验证在分发证书中建立的分发消息的发送、接收和读取的日期和时间、分发证书的发行日期、证书的验证时间和证书的有效截止日期是否顺序排列;

验证附加至所述分发证书的电子签名;以及

验证在所述分发证书中写有电子签名的证书的有效性并验证与关于所述分发证书的发行方的信息的一致性。

9. 根据权利要求 8 所述的方法,进一步包括:

将包括在所述分发证书中的所述分发消息的信息与实际的分发消息进行比较和验证。

10. 根据权利要求 9 所述的方法,其中,所述比较和验证包括:

确认包括在所述分发证书中的发送器的认证电子地址和接收器的认证电子地址是否与所述实际分发消息的发送器的认证电子地址和接收器的认证电子地址一致;以及

确认包括在所述分发证书中的分发文件的数量是否等于附加至所述实际分发消息的电子文档文件的数量。

11. 根据权利要求 9 所述的方法,其中,所述比较和验证包括:

当所述分发证书是接收证书或读取证书时,确认包括在所述分发证书中的所述发送日期和时间是否与在“消息发送”分发消息内的 SOAP 消息中包括的 TimeStamp 字段的值一致;以及

当所述分发证书是发送证书时,确认包括在所述分发证书中的所述发送日期和时间对于分发中继服务器接收“消息发送请求”分发消息来说是否是合理的时间。

12. 根据权利要求 9 所述的方法,其中,所述比较和验证包括:

当所述分发证书是用于被所述发送实体直接发送至所述接收实体的所述“消息发送”分发消息的所述接收证书或所述读取证书时,确认所述分发证书的所述接收日期和时间对于所述接收实体的所述分发消息服务器接收所述“消息发送”分发消息来说是否是合理的时间;以及

当所述分发证书是所述接收证书或所述读取证书时,其中所述接收证书或所述读取证书用于通过所述发送实体请求至所述分发集线器的所述分发中继服务器的所述“消息发送

请求”分发消息，确认所述分发证书的所述接收日期和时间对于所述接收实体的所述分发消息服务器接收所述“消息发送”分发消息来说是否是合理的时间。

13. 根据权利要求 9 所述的方法，其中，所述比较和验证包括：

当所述分发证书是所述读取证书时，确认所述分发证书的所述读取日期和时间是否与在所述接收实体响应所述接收器的“消息详细信息请求”的分发链接消息内的所述 SOAP 消息中包括的所述 TimeStamp 字段值相一致。

14. 根据权利要求 9 所述的方法，其中，所述比较和验证包括：

确认包括在所述分发证书中的发送标识值是否与作为所述分发证书的发行对象的所述分发消息的标识符相一致；

确认在所述分发证书的所述分发文档信息中包括的各个文件的全部文件标识值或文件标识名称是否与附加至所述实际分发消息的电子文档文件的 Content-ID 值相一致；以及

确认在所述分发证书的所述分发文档信息中包括的所述各个文件的全部文件散列信息是否与通过对附加至所述实际分发消息的所述电子文档文件进行散列而获得的值相一致。

15. 一种用于分发电子文档的系统，包括：

发送实体和接收实体，通过分发消息服务器分发电子文档，所述分发消息服务器发送和接收基于电子文档的消息并发行和管理用于消息发送和接收的分发证书；

分发集线器，注册 / 管理所述发送实体和接收实体的电子地址，在所述发送实体和接收实体之间设置电子文档分发路径，当在所述发送实体和接收实体之间进行电子文档分发处理中产生错误时执行消息发送，并且发行所述分发证书；以及

可信第三方存储机构，接收并存储所述分发证书；

其中，所述分发证书包括用于认可接收实体接收消息的事实的接收证书、用于验证所述发送实体的发送尝试的发送证书、以及用于认可接收器读取所接收的消息的事实的读取证书。

16. 根据权利要求 15 所述的系统，其中，所述分发证书包括：

分发证书结构的版本、所述分发证书的识别信息、发行所述分发证书的主体、所述分发证书的发行日期、所述分发证书的有效截止日期、所述分发证书的策略、分发证书请求消息信息以及验证对象。

17. 根据权利要求 16 所述的系统，其中，所述验证对象包括：

通过其发送分发消息的发送器的认证电子地址、通过其接受所述分发消息的接收器的认证电子地址、所述发送器发送所述分发消息的时间、所述接收器接收所述分发消息的时间、所述接收器接收和读取所述电子文档的时间、所述分发消息的标识值、附加至所述分发消息的电子文档文件的数量、关于附加至所述分发消息的每一个所述电子文档的信息、附加至所述分发消息的各个所述电子文档文件的散列值、附加至所述分发消息的各个所述电子文档文件的标识符、以及附加至所述分发消息的各个所述电子文档文件的文件名称。

用于产生 / 发行电子文档分发证书的方法、用于验证电子文档分发证书的方法以及用于分发电子文档的系统

技术领域

[0001] 本发明涉及用于在基于认证电子地址分发电子文档的系统内产生、分发和存储分发证书时，能够提供透明有效的发行服务并且由于保证了证书的兼容性而增强电子文档分发的可靠性的产生 / 发行电子文档分发证书的方法、用于验证电子文档分发证书的方法以及用于分发电子文档的系统。

背景技术

[0002] 通常，电子文档分发（distribution）仅仅基于企业 / 组织的个体的固有规则在特定的产业集团或团体内有限地进行。

[0003] 存在以下缺点：电子邮件已经在个人之间以及个人和企业 / 组织之间用作辅助手段而没有可信电子分发的概念，或者仅通过访问个人、单个业务、小规模企业至大规模企业的方法进行一线通信。

[0004] 所以，保持预定规模的分发系统的企业、以及个人（individual）、单个业务（individual business）和小规模企业需要建立基于能够保证分发可靠性的基础设施的电子文档分发。

发明内容

[0005] [技术问题]

[0006] 本发明致力于提供一种用于在基于认证电子地址分发电子文档的系统内产生、分发和存储分发证书时，能够提供透明有效的发行服务并且由于保证了证书的兼容性而增强电子文档分发的可靠性的产生（create，创建）/ 发行（issue）电子文档分发证书的方法。进一步地，本发明致力于提供一种验证分发证书的方法，通过定义分发证书的标准验证方法来帮助正确地利用证书。此外，本发明还致力于提供一种能够保证分发可靠性的用于分发电子文档的系统。

[0007] [技术方案]

[0008] 本发明的示例性实施方式提供了一种用于在分发电子文档的系统中产生 / 发行分发证书的方法，其中该系统包括发送实体和接收实体（transmitting and receiving entities）以及分发集线器（distribution hub），该方法包括：（a）通过发送实体，将包括发送器的电子文档的分发消息发送至接收实体；（b）在由接收实体接收分发消息之后，通过获取必要信息而产生接收证书；（c）所述接收实体将所产生的接收证书发送至发送实体；（d）发送实体完成对接收的接收证书的验证，然后，将关于接收证书的电子签名证书的验证信息附加至接收证书；以及（e）发送实体将接收证书发送至第三方存储机构并请求向其存储。

[0009] 本发明的另一个示例性实施方式提供了一种验证在用于分发电子文档的系统中产生 / 发行分发证书的方法，其中该系统包括发送和接收实体以及分发集线器，该方法包

括：验证分发证书的格式是否遵循(observe)预定义的结构和值的约束(constraint)；验证在分发证书中建立的分发消息的发送、接收和读取日期和时间、分发证书的发行日期、证书的验证时间和证书的有效截止日期是否顺序排列；验证附加至分发证书的电子签名；以及验证在分发证书中写有电子签名的证书的有效性并验证和与分发证书的发行方相关的信息的一致性。

[0010] 本发明的再一个示例性实施方式提供了一种用于分发电子文档的系统，包括：发送和接收实体，其通过分发消息服务器(distribution messaging server)分发电子文档，分发消息服务器发送和接收基于电子文档的消息并发行和管理用于消息发送和接收的分发证书；分发集线器，其注册 / 管理发送和接收实体的电子地址，在发送和接收实体之间设置电子文档分发路径，当在发送和接收实体之间进行电子文档分发处理中产生错误时执行消息发送，并且发行分发证书；以及可信第三方存储机构，其接收并存储分发证书；其中，分发证书包括用于认可(non-repudiation)接收实体接收消息的接收证书、用于验证发送实体的发送尝试的发送证书，以及用于认可接收器读取所接收的消息的读取证书。

[0011] [有益效果]

[0012] 正如以上所述，根据本发明的示例性实施方式，在用于基于认证电子地址分发电子文档的系统中产生、分发并存储分发证书时，能够提供透明且有效的发行服务。

[0013] 根据本发明的示例性实施方式，在用于基于认证电子地址分发电子文档的系统内通过保证证书的兼容性，能够增强电子文档的分发可靠性。

[0014] 根据本发明的示例性实施方式，提供用于验证分发证书的方法，通过定义分发证书的标准验证方法，有助于正确地利用证书。

附图说明

[0015] 图 1 是描述根据本发明的示例性实施方式的分发证书的产生和发行的图；

[0016] 图 2 是示出根据本发明的示例性实施方式的用于产生和发行分发证书的处理的图。

具体实施方式

[0017] 以下参照附图和表格描述根据本发明示例性实施方式的用于产生 / 发行电子文档分发证书的方法、用于验证电子文档分发证书的方法和用于分发电子文档文件的系统。

[0018] 根据本发明示例性实施方式的用于产生电子文档分发证书的方法包括：(a)通过发送实体，将包括发送器的电子文档文件的分发消息发送至接收实体；(b)由接收实体接收该分发消息并获得必要信息以产生接收证书；(c)由接收实体将所产生的接收证书发送至发送实体；(d)由发送实体对所接收的接收证书完成验证，然后将关于接收证书的电子签名证书的验证信息附加在接收证书上；以及(e)由发送实体将接收证书发送至第三方存储机构以请求存储。

[0019] 根据本发明的另一个示例性实施方式，用于验证电子文档分发证书的方法包括：验证分发证书的格式是否遵循了预定义的结构和值的约束；验证在分发证书中建立的分发消息的发送、接收以及读取日期和时间、分发证书的发行日期、证书的验证时间以及证书的有效截止日期是否顺序排列；验证附加到分发证书的电子签名；以及验证分发证书中写有

电子签名的认证证书的有效性并验证和有关分发证书的发行商的信息的一致性。

[0020] 根据本发明的再一个示例性实施方式，用于分发电子文档文件的系统包括：发送和接收实体，其通过分发消息服务器来分发电子文档文件，该分发消息服务器基于电子地址发送和接收消息并发行和管理用于消息发送和接收的分发证书；分发集线器，其注册/管理发送和接收实体的电子地址，在发送和接收实体之间设置电子文档文件分发路径，当在发送实体和接收实体间的电子文档文件分发处理期间产生错误时执行消息发送，并发行该分发证书；以及可信的第三方存储机构，其接收并存储分发证书，其中，该分发证书包括用于对接收实体接收消息这个事实认可的接收证书、用于验证发送实体的发送尝试的发送证书，以及用于对接收器读取所接收的消息这个事实认可的读取证书。

[0021] 将参照图1和2将详细描述根据具有前述配置的本发明的示例性实施方式的用于产生电子文档分发证书的方法、用于验证电子文档分发证书的方法以及用于分发电子文档文件的系统。

[0022] [用于产生并发行电子文档分发证书的模型]

[0023] 图1示出了根据本发明示例性实施方式的用于产生并发行分发证书的组成，并且将参照以下①至④对每一个组成进行描述：

[0024] ①发送实体(或者发送电子文档文件协调器(mediator)，在下文中称之为发送实体101)：主要是将发送器的电子文档文件发送至接收实体或者如果必要的话，请求发送至分发中继服务器(distribution relay server)。发送实体用于对从接收实体或分发中继服务器接收的分发证书进行验证，然后将验证信息附加至分发证书，以和分发证书一起存储在第三方存储机构(third party storage authority)中。

[0025] ②接收实体(或者接收电子文档文件协调器，在下文中称之为接收实体102)：主要是将从发送实体或分发中继服务器接收的电子文档文件转移至接收器。该接收实体用于一旦从发送实体或分发中继服务器接收到电子文档文件就产生接收证书，并且将产生的证书作为响应消息而发送至发送实体或分发中继服务器，或者在接收器读取电子文档文件之后立即产生读取证书并将产生的读取证书和分发证书一起转移至发送实体。

[0026] ③电子文档文件分发集线器(或者分发中继服务器103)：主要是将从发送实体接收发送请求的电子文档文件转移至接收实体。电子文档文件分发集线器用于一旦从发送实体接收到电子文档的发送请求就产生发送证书以发送至发送实体，或者将电子文档文件转移至接收实体，然后将作为对发送证书的响应所接收的接收证书和分发证书一起转移至发送实体。

[0027] ④第三方存储机构(认证的电子文档存储机构104)作为可信机构(trusted authority)用于安全地存储分发证书。在下文中，在描述本发明时，将省略图1中的参考标号。

[0028] [电子文档分发证书的类型和处理]

[0029] 要产生根据本发明的电子文档分发证书所需的必要信息如以下表格1所示。

[0030] 表格1

[0031]

类型	目的	产生主体/时间	必要信息
接收证书	对接收实体的消息接收事实的认可	接收实体/接收之后立即	文档信息、发送器、接收器、发送器发送时间、接收器接收时间
发送证书	对发送实体的发送尝试的验证	分发中继服务器 / 接收发送请求消息之后立即	文档信息、发送器、接收器、发送器发送请求时间
读取证书	对接收器读取所接收的消息的实施的认可	接收实体/被接收器读取之后立即	文档信息、发送器、接收器、发送器发送时间、接收器接收时间、接收器读取时间

[0032] 在根据本发明的获取关于电子文档分发证书的必要信息的方法如以下表格 2 所示。

[0033] 表格 2

[0034]

类型	必要信息	获取信息的方法
接收证书	文档信息、发送器、接收器、发送器发送时间	在由发送实体发送的分发链接消息中使用分发消息和 SOAP 消息的敏感字段值
	接收器接收时间	使用接收实体的分发消息服务器的接收时间
发送证书	文档信息、发送器、接收器	在由发送实体发送的分发链接消息中使用分发消息的敏感字段值（sensitive field value）
	发送器发送请求时间	使用分发中继服务器的接收时间
读取证书	文档信息、发送器、接收器、发送器发送时间	在由发送实体发送的分发链接消息中使用分发消息和 SOAP 消息的敏感字段值
	接收器接收时间	由接收实体使用分发消息服务器的接收时间
	接收器读取时间	使用用于接收器的文档信息请求的接收实体的响应时间

[0035] ※分发消息服务器和分发中继服务器的系统时间需要和外部授权机构（authorized institution）的时间定期同步。

[0036] 在图 2 中示出了根据本发明的电子文档分发证书中所涉及的全部处理。

[0037] 接收证书是用于验证从发送实体接收到电子文档分发消息的事实所产生的电子文档分发证书，并且接收证书中所涉及的处理如以下表格 3 所示。

[0038] 表格 3

[0039]

编号	处理名称
1	发送实体将包括发送器的电子文档的分发消息发送至接收实体
2	接收实体接收分发消息，然后立即接收必要信息以产生接收证书
3	接收实体把产生的接收证书发送至发送实体
4	发送实体完成对接收证书的验证，然后将关于接收证书的电子签名证书的验证信息附加到接收证书上
5	发送实体将接收证书发送并存储到认证的电子文档存储机构

[0040] 当发送实体试图将分发消息发送至接收实体但却在分发消息发送中失败、并且由此请求将相应的消息发送至分发中继服务器时，发送证书由分发中继服务器产生，用于验证发送实体做出了发送请求并被发送至发送实体的事实。发送证书中涉及的处理如表格 4 所示。

[0041] 表格 4

[0042]

编号	处理名称
1	发送实体将分发消息发送至接收实体。
2	当分发消息发送失败时，发送实体请求将分发消息发送至分发中继服务器。
3	分发中继服务器对所请求的发送产生发送证书。
4	分发中继服务器将发送证书发送至发送实体。
5	发送实体完成对发送证书的验证，然后将关于发送证书的电子签名证书的验证信息附加至发送证书。
6	发送实体将发送证书存储在认证的电子文档存储机构中。
7	分发中继服务器将分发消息转移至接收实体。
8	接收实体在收到电子文档文件之后立即产生接收证书。
9	接收实体将接收证书发送至分发中继服务器。
10	分发中继服务器将接收证书转移至发送实体。
11	发送实体完成对接收证书的验证，然后将关于接收证书的电子签名证书的验证信息附加至接收证书。
12	发送实体将接收证书发送并存储至认证的电子文档存储机构。

[0043]

[0044] 读取证书是由接收实体产生的证书并被发送至发送实体以验证接收器读取通过接收实体从发送实体接收的消息，并且读取证书所涉及的处理如表格 5 所示。

[0045] 表格 5

[0046]

编号	处理名称
1	接收器向接收实体请求分发消息的读取，以读取作为响应所接收的分发消息 。
2	接收实体产生读取证书。
3	接收实体完成读取证书的验证，然后将关于读取证书的电子签名证书的验证信息附加至读取证书。
4	发送实体将读取证书发送并存储至认证的电子文档机构。

[0047] [在分发证书的发行和验证中所涉及的基本的前提和考虑]

[0048] 在分发证书的发行和验证中所涉及的基本的前提和考虑如以下①至⑨。

[0049] ①分发证书由发送和接收实体的分发中继服务器和分发消息服务器产生并验证。

[0050] ②在本发明中，分发证书被电子签名并仅基于 NPKI 证书而产生。

[0051] ③基于分发消息产生对应的分发证书。即使在单个分发消息中包括至少两个电子文档，也仅产生一个分发证书。

[0052] ④分发证书需要被分配能够识别分发消息的 ID 和能够在分发消息内识别电子文档文件的电子文档标识符或电子文档名称。

[0053] ⑤通过单独的发送和接收实体来产生分发证书的序列号，由此使用 32 个字节的随机数从而予以唯一地分配。

[0054] ⑥没有根据分发系统的特点定义分发证书的更新和撤回。

[0055] ⑦分发消息服务器需要和外部可信机构的可视信息一直保持同步，由此保证了分发证书内可视信息的可靠性。

[0056] ⑧分发证书的策略仅使用在本技术标准中定义的对象标识符（OID）和名称。

[0057] ⑨发送实体验证所接收的分发证书，然后将与分发证书的签名证书相关的验证信息附加到分发证书上。

[0058] [电子文档分发证书的结构]

[0059] 通过发送和接收实体产生电子文档分发证书，并使用发送和接收实体的 NPKI 证书予以电子签名。电子文档分发证书的基本结构使用 CMS 标准的 SignedData 结构以使用与认证的电子文档机构（certified electronic document authority）的证书相同的内容标识符。

[0060] 电子文档分发证书的 ContentType 如以下表格 6 所示。

[0061] [表格 6]

[0062]

```
id-kiec-arcCertReseponse OBJECT IDENTIFIER ::= { iso(1) member-body(2)
korea(410) kiec(200032) certificate(2) 2 }
ARCCertResponse ::= CHOICE {
        arcCertInfo             [0] EXPLICIT ARCCertInfo,
        arcErrorNotice          [1] EXPLICIT ARCErrorNotice }
```

[0063] 电子文档分发证书的基本字段如以下表格 7 所示。

[0064] [表格 7]

[0065]

```
ARCCertInfo ::= SEQUENCE {
        version             [0] EXPLICIT ARCVersion DEFAULT v1,
        serialNumber        SerialNumber,
        issuer              GeneralNames,
        dateOfIssue         GeneralizedTime,
        dateOfExpire        DateOfExpiration,
        policy              ARCCertificatePolicies,
        requestInfo         RequestInfo,
        target              TargetToCertify,
        extionsions         [1] EXPLICIT Extensions OPTIONAL }
```

[0066] 上述分发证书的基本字段的详细内容为以下①至⑧。

[0067] ① Version,版本

[0068] 表示电子文档分发证书的结构的版本。对于电子文档分发证书,版本设为 v9,并使用 distributionlnfos 类型的目标字段。

[0069] [表格 8]

[0070]

```
ARCVersion ::= INTEGER {v1(1), v2(2), v9(9)}
```

[0071] ② SerialNumber,序列号

[0072] 表示电子文档分发证书的识别信息。

[0073] 电子文档分发证书的序列号使用 32 个字节的随机数以产生为唯一数量的整数值。为了处理电子文档分发证书,有必要处理 32 个字节的序列号。

[0074] [表格 9]

[0075]

```
SerialNumber ::= INTEGER
```

[0076] ③ Issuer,证书的发行方

[0077] 表示发行电子文档分发证书的主体 (subject)。

[0078] 当产生本字段的值时,必须使用具有 GeneralName 结构的 directoryName 字段,并且接收实体或分发中继服务器提取其中电子文档分发证书被电子签名的证书的 subjectDN 值,以被原样设置。

[0079] [表格 10]

[0080]

```
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
        otherName                       [0] OtherName,
        rfc822Name                      [1] IA5String,
        dNSName                         [2] IA5String,
        x400Address                     [3] ORAddress,
        directoryName                   [4] Name,
        ediPartyName                    [5] EDIPartyName,
        uniformResourceIdentifier       [6] IA5String,
        iPAddress                       [7] OCTET STRING,
        registeredID                    [8] OBJECT IDENTIFIER }

Name ::= CHOICE {
        RDNSequence }

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {
        type            AttributeType,
        value           AttributeValue }

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType

DirectoryString ::= CHOICE {
        teletexString           TeletexString (SIZE (1..MAX)),
        printableString         PrintableString (SIZE (1..MAX)),
        universalString         UniversalString (SIZE (1..MAX)),
        utf8String              UTF8String (SIZE (1..MAX)),
        bmpString               BMPString (SIZE (1..MAX)) }
```

[0081]

[0082] ④ DataOflssue，证书的发行日期

[0083] 表示发行电子文档分发证书的时间。

[0084] dataOflssue 使用 GeneralizedTime 格式。

[0085] ⑤ dataOfExpire，证书的有效截止日期

[0086] 表示电子文档分发证书的截止时间。

[0087] 在将来，电子文档分发证书的 dataOfExpire 将与 dataOflssue 比较，并且考虑到验证分发事实所需的时间而需要设置有足够的裕量。

[0088] [表格 11]

[0089]

```
DateOfExpiration ::= GeneralizedTime
```

[0090] ⑥ Policy，证书策略 (Certificate policy)

[0091] 表示电子文档分发证书的策略。

[0092] 本字段由用于表示根据电子文档分发证书的类型的 Qualifier 信息和电子文档分发证书的类型构成。

[0093] 注意：只有 userNotice 用作 Qualifier 信息，而并没有使用 cPSuri。使用低于 userNotice 字段的 explicitText 字段来显示电子文档分发证书的类型并且它的格式需要使用 BMPString。

[0094] [表格 12]

[0095]

```
ARCCertificatePolicies ::= SEQUENCE SIZE   (1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
        policyIdentifier          CertPolicyId,
        policyQualifiers           SEQUENCE SIZE (1..MAX) OF

PolicyQualifierInfo OPTIONAL }

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
        policyQualifierId          PolicyQualifierId,
        qualifier                  ANY DEFINED BY policyQualifierId }

PolicyQualifierId ::= OBJECT IDENTIFIER ( id-qt-cps | id-qt-unotice )

Qualifier ::= CHOICE {
        cPSuri                CPSuri,
        userNotice             UserNotice }

UserNotice ::= SEQUENCE {
        noticeRef             NoticeReference OPTIONAL,
        explicitText          DisplayText OPTIONAL}

NoticeReference ::= SEQUENCE {
        organization           DisplayText,
        noticeNumbers          SEQUENCE OF INTEGER }

DisplayText ::= CHOICE {
        ia5String             IA5String(SIZE (1..200)),
        visibleString         VisibleString(SIZE (1..200)),
        bmpString             BMPString(SIZE (1..200)),
        utf8String            UTF8String(SIZE (1..200)) }
```

[0096] 在电子文档分发证书内的策略 OID 跟随证书的类型并且需要仅使用本发明指定的数值。

[0097] 根据电子文档分发证书的类型的 OID 和 Qualifier 信息如下。

[0098] [表格 13]

[0099]

证书类型	策略 OID	Qualifier
发送证书	1.2.410.200032.6.1	“发送证书”
接收证书	1.2.410.200032.6.2	“接收证书”
读取证书	1.2.410.200032.6.3	“读取证书”

[0100] ⑦ RequestInfo，证书请求消息信息

[0101] 本字段设置为空(null)。

[0102] [表格 14]

[0103]

```
RequestInfo ::= CHOICE {
        arcCertRequest          ARCCertRequest,
        null                    NULL }
```

[0104] ⑧ Target，要证明的对象

[0105] 本字段包括要验证的内容。

[0106] 本字段必须通过使用低级(lower)distributionInfos 字段设置关于分发消息的信息。

[0107] [表格 15]

[0108]

```
TargetToCertify ::= CHOICE {
        opRecord                [0] EXPLICIT
OperationRecord,
        orgAndIssued            [1] EXPLICIT
OriginalAndIssuedDocumentInfo,
        dataHash                [2] EXPLICIT HashedDataInfo
        distributionInfos       [10] EXPLICIT
DistributionInfos }

DistributionInfos ::= SEQUENCE OF DistributionInfo

DistributionInfo ::= SEQUENCE {
```

[0109]

```
        senderAdd                UTF8String,
        receiptorAdd             UTF8String,
        dateOfSend               GeneralizedTime,
        dateOfReceive            [0] EXPLICIT
GeneralizedTime OPTIONAL,
        dateOfReceiveConfirm     [1] EXPLICIT
GeneralizedTime OPTIONAL,
        distributionId           UTF8String,
        numberOfFiles            INTEGER,
        distributedFileInfos     DistributedFileInfos }
```

[0110] 1）SenderAdd，发送器的认证电子地址

[0111] 表示发送电子文档分发消息的发送器的认证电子地址。

[0112] 2）ReceiverAdd，接收器的认证电子地址

[0113] 表示接收电子文档分发消息的接收器的认证电子地址。

[0114] 3）DateOfsend，发送日期和时间

[0115] 表示发送器发送分发消息的时间。

[0116] 接收证书和读取证书的发送日期和时间是指发送实体发送分发消息的时间，并且在“消息发送”分发链接消息内的 SOAP 消息中包括的 TimeStamp 字段的值以 GeneralizedTime 格式表示。

[0117] 应注意，发送证书的发送日期和时间是指发送实体请求将分发消息发送至分发中继服务器的时间并且与其它使用分发链接消息内的时间值的分发证书不同，使用分发中继服务器接收“消息发送请求”分发消息时的时间。和时间字段一起，仅有本字段包括在发送证书内，并且不产生接收日期和时间字段以及读取日期和时间字段。

[0118] 4）DateOfReceive，接收日期和时间

[0119] 表示接收器接收分发消息的时间。

[0120] 接收日期和时间是仅在接收证书和读取证书中产生的字段并且被设置为接收实体的分发消息服务器接收“消息发送”分发消息的时间。

[0121] 接收日期和时间在发送日期和时间之后并且等于或早于产生证书的时间。

[0122] 5）DateOfReceiveConfirm，读取日期和时间

[0123] 表示接收器在接收电子文档文件之后读取该电子文档文件的时间。

[0124] 读取日期和时间是仅在读取证书中产生的字段，并且设置为接收实体的分发消息服务器响应接收器的“消息详细信息请求”的时间。该时间需要等于 TimeStamp 字段的值，其中 TimeStamp 字段包括在通过接收实体响应于接收器的分发链接消息内的 SOAP 消息中并且以 GeneralizedTime 格式表示。

[0125] 读取日期和时间需要等于或早于产生证书的时间，并且等于或晚于接收日期和时间。

[0126] 6）DistributionId，分发标识值

[0127] 表示用于分发消息的标识值。

[0128] 将作为电子文档分发证书的发行对象的分发消息的标识符原样设置。

[0129] 7）NumberOfFiles，分发文件数量

[0130] 表示附加至分发消息的电子文档文件的数量。

[0131] 设置附加至实际分发消息的电子文档文件的数量。

[0132] 8)DistributedFileInfos,分发文件信息

[0133] 分发消息可以附加有至少一个电子文档文件并且使用 DistributedFile 结构设置关于各个文件的信息。

[0134] [表格 16]

[0135]

```
DistributedFileInfos ::= SEQUENCE OF DistributedFile

DistributedFile ::= SEQUENCE {
        fileHashedData          HashedDataInfo,
        fileId                  [0] EXPLICIT UTF8String OPTIONAL,
        fileName                [1] EXPLICIT UTF8String OPTIONAL }

HashedDataInfo ::= SEQUENCE {
        hashAlg                  HashAlgorithm,
        hashedData               BIT STRING }

HashAlgorithm ::= AlgorithmIdentifier
```

[0136] 9)FileHashedData,文件散列信息(File hash information)

[0137] 表示附加至分发消息的各个电子文档文件的散列值。

[0138] 在使用 hashAlg 字段的散列算法产生散列值之后,将各个电子文档文件在 hashedData 字段内设置。

[0139] 10)Filed,文件标识值

[0140] 表示附加至分发消息的各个电子文档文件的标识符。

[0141] 在分发消息内不存在文件标识值,并且将附加至由 Multi Part 消息以 MIME 格式构成的全部分发链接消息的各个电子文档文件的 Content-ID 值原样设置。

[0142] 可以选择性地使用该字段,但是当未使用文件名称字段时必须使用该字段,并且推荐使用文件标识值字段。

[0143] 当验证分发证书时存在文件标识值字段和文件名称字段两者时,将分发证书与电子文档文件相比较并优先使用文件标识值字段进行验证。

[0144] 11)FileName,文件名称

[0145] 表示附加至分发消息的各个电子文档文件的文件名称。

[0146] 当没有产生文件标识值时,必须产生文件名称字段并且作为一个值,将附加至由 Multi Part 消息以 MIME 格式构成的整个分发链接消息的各个电子文档文件的 Content-ID 值原样设置。当产生文件标识值字段时,可以省略文件名称字段,并且在产生文件标识值字段时设置能够辅助识别电子文档文件的值。

[0147] 电子文档分发证书特征(profile)如以下表格 17 所示。

[0148] [表格 17]

[0149]

基本字段	内容	特有事项（Peculiar Matter）
version	版本	v9
serialNumber	序列号	32 字节的随机数
issuer	证书发行方	签名证书的主体 DN
dateOfIssue	证书的发行日期	GeneralizedTime
dateOfExpire	证书的有效截止日期	GeneralizedTime
policy	证书策略	OID： 1.2.410.200032.6.1 (发送) ：1.2.410.200032.6.2 (接收) ：1.2.410.200032.6.3 (读取)

[0150]

requestInfo	证书请求消息信息	空
target	验证对象	distributionInfos 结构的使用
senderAdd	发送器的认证电子地址	UTF8String
receiptorAdd	接收器的认证电子地址	UTF8String
dateOfSend	发送日期和时间	GeneralizedTime, 必需的
dateOfReceive	接收日期和时间	GeneralizedTime, 选择
dateOfReceiveConfirm	接收确认日期和时间	GeneralizedTime, 选择
distributionId	分发标识符	UTF8String
numberOfFiles	发送文件的数量	
distributedFileInfos	发送文件信息	至少一个 DistributedFile
DistributedFile		
fileHashedData	文件散列值	SHA256
fileId	文件 ID	两个字段之一，即 fileId 和 filename 是必须的
fileName	文件名称	

[0151] 与电子文档分发证书特征相关联的考虑如以下①至③。

[0152] ①在电子签名时，公共密匙加密算法使用 RSA 并且散列算法使用 SHA256

[0153] ②电子签名证书必须包括在 signedData 中

[0154] ③仅有一个 signerInfo 包括在 signerInfo 字段中。

[0155] [验证电子文档分发证书的方法]

[0156] 分发消息发送实体一旦接收到电子文档分发证书就需要对证书执行验证。

[0157] 验证分发证书的处理大体上分成证书的有效性验证和证书的内容验证。证书的有效性验证是确认是否满足有效获得证书的条件的处理，并且证书的内容验证是确认通过与要由证书验证的分发消息相比较的事实的处理。因此，证书的内容验证不是对证书的验证而是可以认为是要进行确认分发事实是否是真的。

[0158] 电子文档分发证书的有效性验证通过以下处理来执行 :①验证证书格式，②可视化验证证书，③验证证书电子签名，以及④验证签名证书，并且通过⑤比较和验证分发消息的处理来执行证书的内容验证。

[0159] ①证书格式的验证

[0160] 证书格式的验证是确认要验证的分发证书的格式是否遵循本标准中定义的结构和值的约束的处理，而且在验证证书格式的时候，基本上验证以下 1）至 7）事项。

[0161] 1）分发证书的整个结构是否满足 signedData 格式以及是否遵循有关是否产生了在本标准中定义的较低级的字段的规则？

[0162] 2）版本将被设置为 v9 吗？

[0163] 3）序列号是通过使用 32 字节的随机数产生为正整数值的吗？

[0164] 4）证书发行方是通过使用 GeneralName 结构的 dirctroyName 字段设置的吗？

[0165] 5）证书的发行日期和证书的有效截止日期是通过使用 GeneralizedTime 格式设置的吗？

[0166] 6)证书策略是通过使用本标准中定义的低级字段(lower field)的结构和值所产生的吗？

[0167] 7）验证对象字段是通过使用 distributionInfos 字段产生的吗？并且验证对象字段遵循有关是否产生了依据在证书策略中所提出的证书类型的低级字段的规则了吗？

[0168] ②证书可视化验证

[0169] 证书可视化验证是确认在分发证书中设置的每一个可视化字段的值在验证参考时间是否是正常的处理。也就是说，确认在本处理期间，不同于在验证参考时间的那些情况，在分发证书中设置的各个可视化字段的值满足以下表格 18 的规则。

[0170] [表格 18]

[0171]

发送日期和时间 < 接收日期和时间≤ 读取日期和时间 ≤ 证书的发行日期≤ 证书验证时间 ≤ 证书的有效截止日期

[0172] ③证书电子签名的验证

[0173] 电子签名的验证是验证附加至分发证书的电子签名以用于完整保证并认可由分发证书验证的内容的处理，并且遵循用于验证通常 CMS 的 signedData 的电子签名的方法。

[0174] ④签名证书的验证

[0175] 签名证书的验证是验证其中分发证书被电子签名的证书的有效性以及与分发证书的发行方信息的同一性的处理。

[0176] 电子签名证书的有效性验证是通常包括在验证电子签名的处理中作为其一部分的处理，并且通过验证证书的可用时段、验证撤回、以及用上级 CA 证书验证路径等处理来执行。这基于授权证书系统的“验证授权证书路径的技术标准 [KCAC.TS.CERTVAL]”予以验证。

[0177] 如果电子签名证书的有效性验证成功，则需要执行与分发证书的发行方信息的比较和验证。形成分发证书的发行方信息以将电子签名证书的主体 DN 值原样设置，因此，提取两个值以执行关于该两个值是否彼此相一致的比较和验证。

[0178] ⑤分发消息的比较和验证

[0179] 比较和验证分发消息的处理并不是验证分发证书的有效性的处理，而是通过将包括在分发证书中的分发消息的信息与实际分发消息的信息相比较和验证来确认分发事实

是否是真实的处理。

[0180] 当发送实体发送分发消息或者在发送请求之后接收分发证书时，有必要通过对本分发消息执行比较和验证来确认：对应的分发证书包括与由发送实体发送的分发消息相关的信息。

[0181] 在比较和验证分发消息时，主要确认以下事项。

[0182] - 发送器的认证电子地址和接收器的认证电子地址对应于分发消息吗？

[0183] - 接收证书和读取证书的发送日期和时间与在“消息发送”分发链接消息内的 SOAP 消息中包括的 TimeStamp 字段的值一致吗？

[0184] - 发送证书的发送日期和时间对于分发中继服务器接收“消息发送请求”分发消息来说是合理的时间吗？

[0185] - 通过发送实体直接发送至接收实体的“消息发送”分发消息的接收证书和读取证书的接收日期和时间对于接收实体的分发消息服务器接收“消息发送”分发消息来说是合理的时间吗？

[0186] - 由发送实体请求至分发中继服务器的“消息发送请求”分发消息的接收证书和读取证书的接收日期和时间对于接收实体的分发消息服务器接收“消息发送”分发消息来说是合理的时间吗？（然而，仅仅对应于这种情况，其中发送实体能够知道分发中继服务器把分发消息转移至接收实体时的时间）。

[0187] - 读取证书的读取日期和时间与在通过接收实体响应于接收器的“消息详细信息请求”的分发链接消息内的 SOAP 消息中包括的 TimeStamp 字段的值是一致的吗？（然而，仅仅对应于这种情况，其中发送实体能够知道相应 TimeStamp 字段的值）。

[0188] - 分发标识值与作为分发证书的发行对象的分发消息的标识符是一致的吗？

[0189] - 分发文件的数量等于附加至实际分发消息的电子文档文件的数量吗？

[0190] - 包括在分发文档信息中的各个文件的文件标识值或文件名称全部与附加至实际分发消息的电子文档文件的 Content-ID 值是一致的吗？

[0191] - 包括在分发文档信息中的各个文件的所有文件散列信息与通过散列被附加至实际分发消息的电子文档文件所获得的值一致吗？

[0192] [电子签名的长期验证信息]

[0193] 当考虑到分发证书的重要性而完成对所发行的分发证书的验证时，将分发证书注册并存储在认证的电子文档机构中，该认证的电子文档机构仅对于分发证书的存储时间和完整性提供长期保证功能，但在电子签名证书的可用时段期满之后并不能保证在分发证书的发行时间的电子签名证书的长期有效性。也就是说，在电子签名证书的有效期期满之后，不允许分发证书的有效性保证。为了解决这个问题，通过连同分发证书一起存储能够确认在分发证书发行时对应的电子签名证书是有效的验证信息，即使在分发证书被电子签名的证书的可用时段期满之后，也能验证分发证书。

[0194] ①电子签名证书的验证信息的获取

[0195] 发送实体收集 CRL 和 ARL 和上级 CA 证书以及 Root CA 证书，用于验证电子签名证书的撤回和路径，从而执行验证接收的分发证书有效性的处理中的“5.2.4 签名证书的验证”处理。可以通过在认证的电子文档机构中连同分发证书一起存储对应的数据而在分发证书的发行时间保证电子签名证书的有效性，从而保证分发证书的有效性。

[0196] ②电子签名证书的验证信息的存储

[0197] 发送实体包括在对电子签名证书验证成功之后用于在分发证书的 signedData 结构内的 certificates 字段和 crls 字段中验证的 CRL 和 ARL 和上级 CA 证书以及 Root CA 证书。注意仅需要执行包括在相应字段中的每一个信息的工作，而与包括每一个信息的顺序无关。由于 certificates 字段和 crls 字段不是 signedData 的电子签名对象信息，所以，即使在执行相应的工作之后，对分发证书的验证仍然成功。

[0198] [表格 19]

[0199]

```
SignedData ::= SEQUENCE {
        version                 CMSVersion,
        digestAlgorithms        DigestAlgorithmIdentifiers,
        encapContentInfo        EncapsulatedContentInfo,
        certificates            [0] IMPLICIT CertificateSet OPTIONAL,
        crls                    [1] IMPLICIT
RevocationInfoChoices OPTIONAL,
        signerInfosSignerInfos }
```

[0200] ③在认证的电子文档机构中存储

[0201] 发送实体将包括电子签名证书的验证信息的分发证书存储在认证的电子文档机构中，使得能够执行分发证书的长期验证。

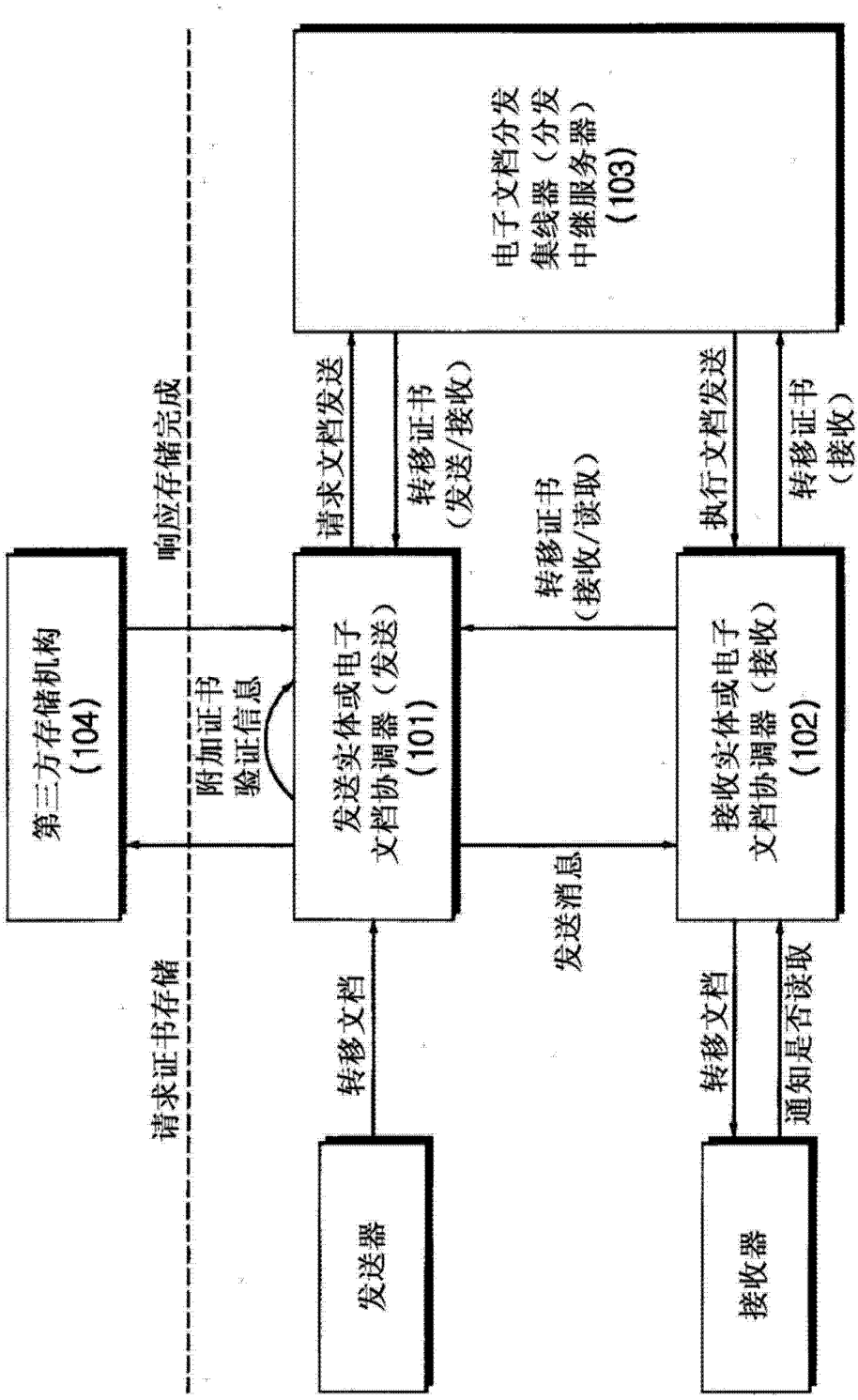

电子文档分发
集线器（分发
中继服务器）
(103)
请求文档发送
转移证书
（发送/接收）
转移证书
（接收/读取）
执行文档发送
转移证书
（接收）
响应存储完成
第三方存储机构
(104)
附加证书
验证信息
发送实体或电子
文档协调器（发送）
(101)
接收实体或电子
文档协调器（接收）
(102)
发送消息
请求证书存储
转移文档
转移文档
通知是否读取
发送器
接收器

图 1

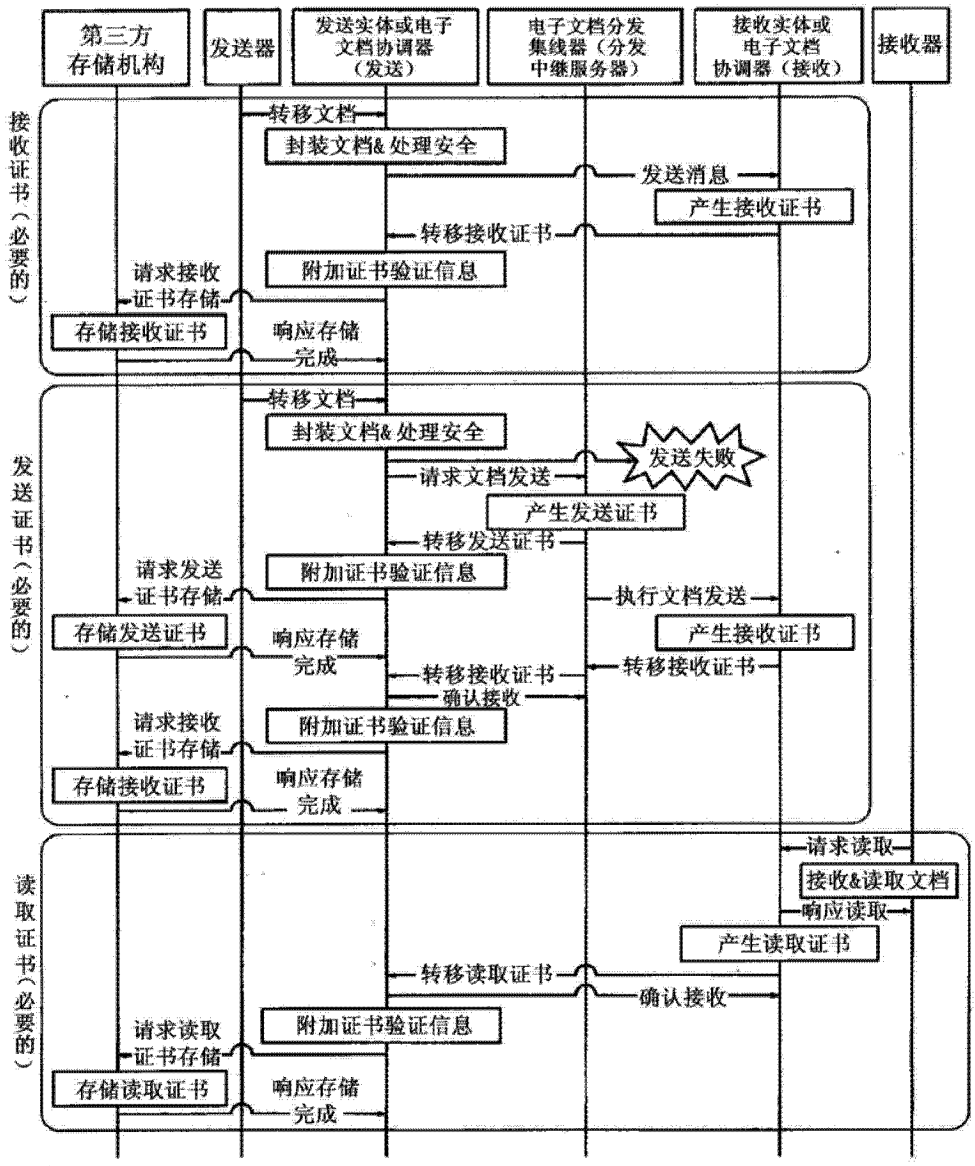

第三方
存储机构
发送器
发送实体或电子
文档协调器
（发送）
电子文档分发
集线器（分发
中继服务器）
接收实体或
电子文档
协调器（接收）
接收器
接收证书（必要的）
转移文档
封装文档& 处理安全
发送消息
产生接收证书
转移接收证书
附加证书验证信息
请求接收
证书存储
存储接收证书
响应存储
完成
发送证书（必要的）
转移文档
封装文档& 处理安全
发送失败
请求文档发送
产生发送证书
转移发送证书
附加证书验证信息
请求发送
证书存储
执行文档发送
存储发送证书
响应存储
完成
产生接收证书
转移接收证书
转移接收证书
确认接收
附加证书验证信息
请求接收
证书存储
存储接收证书
响应存储
完成
读取证书（必要的）
请求读取
接收&读取文档
响应读取
产生读取证书
转移读取证书
确认接收
附加证书验证信息
请求读取
证书存储
存储读取证书
响应存储
完成

图 2