US 20130110919A1

(19) **United States**

(12) **Patent Application Publication**

An et al.

(10) **Pub. No.: US 2013/0110919 A1**

(43) **Pub. Date: May 2, 2013**

(54) **METHOD FOR CREATING/ISSUING ELECTRONIC DOCUMENT DISTRIBUTION CERTIFICATE, METHOD FOR VERIFYING ELECTRONIC DOCUMENT DISTRIBUTION CERTIFICATE, AND SYSTEM FOR DISTRIBUTING ELECTRONIC DOCUMENT**

(75) Inventors: **Dae Seob An**, Seoul (KR); **Jung Gu Lee**, Seoul (KR); **Seong Pil Kong**, Seongnam-si (KR); **Yeong Cheol Lim**, Seoul (KR)

(73) Assignee: **NATIONAL IT INDUSTRY PROMOTION AGENCY**, Seoul (KR)

(21) Appl. No.: **13/808,573**

(22) PCT Filed: **Jul. 8, 2011**

(86) PCT No.: **PCT/KR2011/005039**

§ 371 (c)(1),
(2), (4) Date: **Jan. 4, 2013**

(30) **Foreign Application Priority Data**

Jul. 8, 2010 (KR) 10-2010-0065985
Dec. 21, 2010 (KR) 10-2010-0131935
Dec. 21, 2010 (KR) 10-2010-0131936
Jul. 7, 2011 (KR) 10-2011-0067188

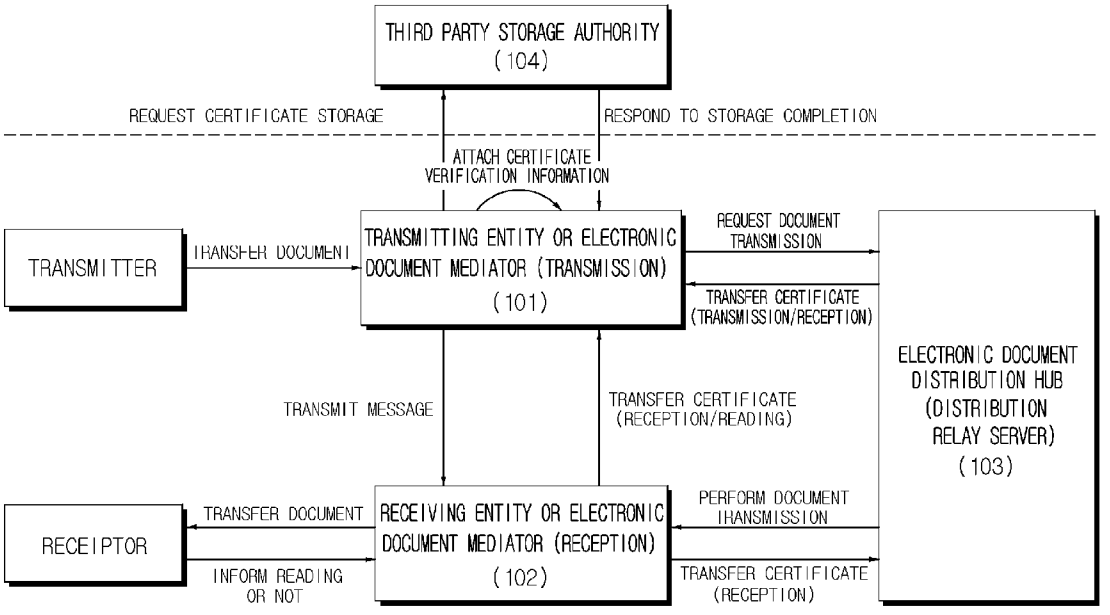
Publication Classification

(51) **Int. Cl.**
H04L 29/06 (2006.01)

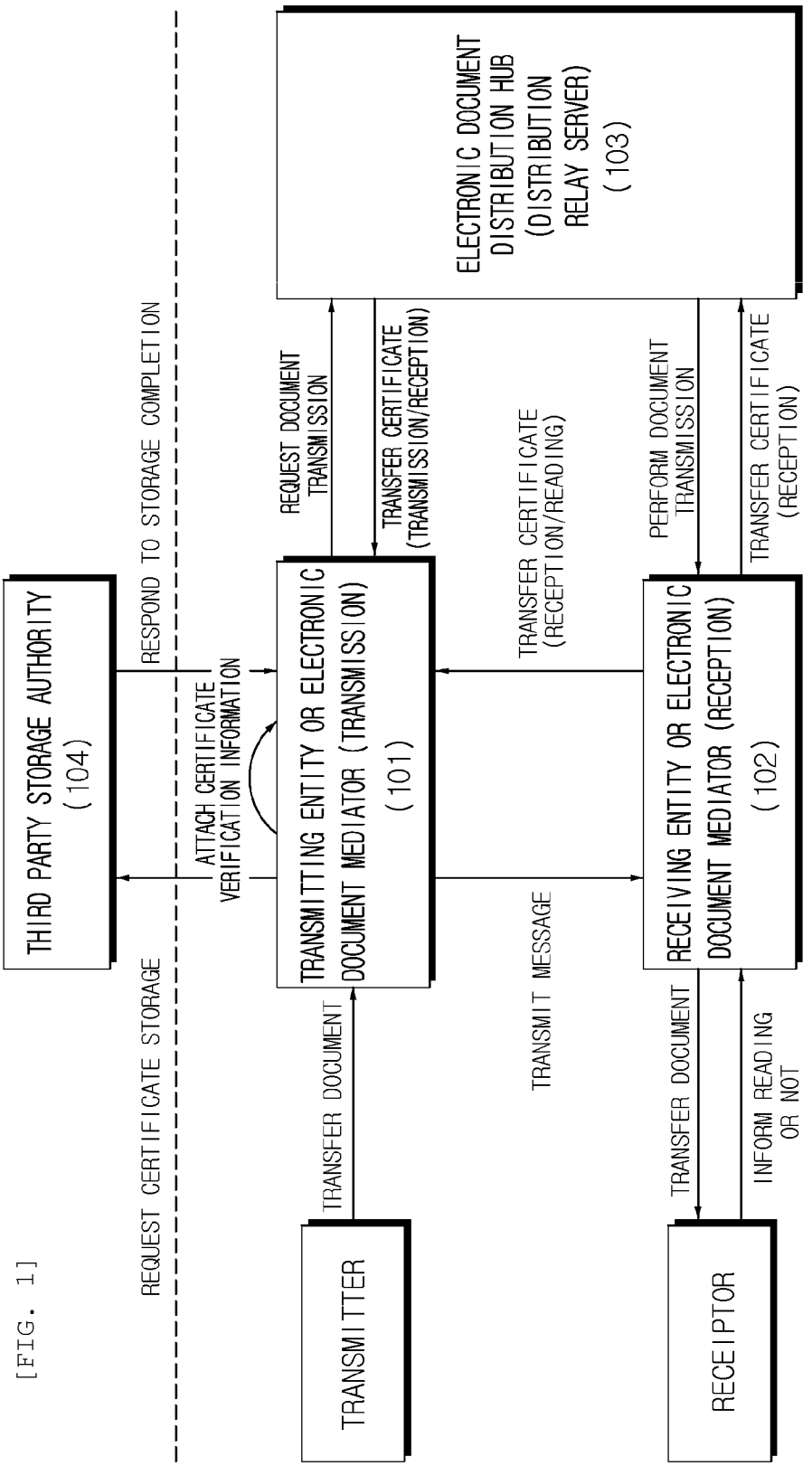
(52) **U.S. Cl.**
CPC ***H04L 63/0823*** (2013.01)
USPC **709/203**

(57) **ABSTRACT**

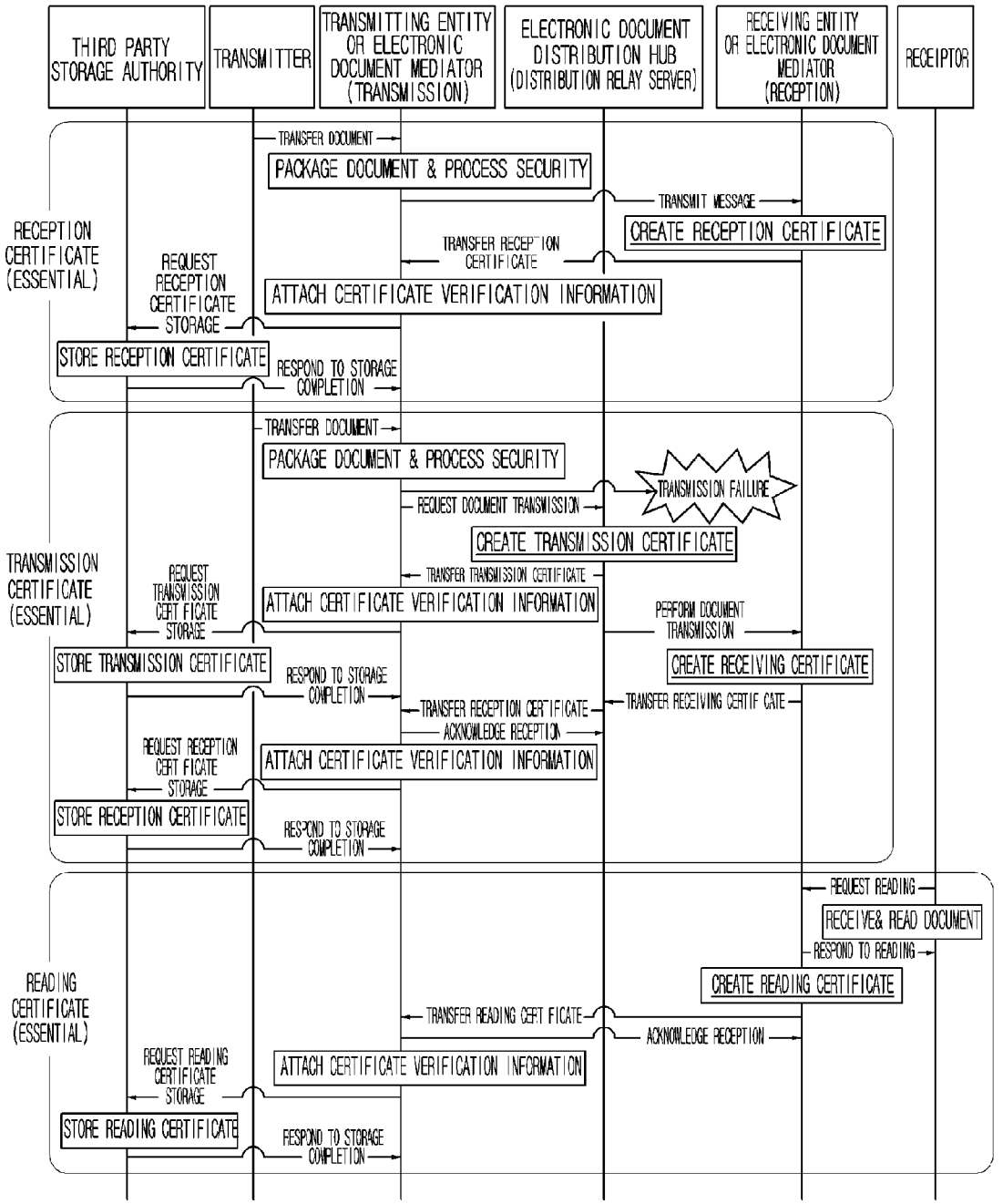
The present invention relates to creating, distributing, and storing a distribution certificate in an electronic document distribution system which is based on a public electronic address, and particularly to a method for creating/issuing an electronic document distribution certificate, a method for verifying an electronic document distribution certificate, and a system for distributing an electronic document, which makes it possible to provide a transparent and efficient issuing service and to raise the distribution reliability of electronic documents due to the security of the compatibility of the certificate.



[FIG. 1]


THIRD PARTY STORAGE AUTHORITY
(104)
REQUEST CERTIFICATE STORAGE
RESPOND TO STORAGE COMPLETION
ATTACH CERTIFICATE VERIFICATION INFORMATION
TRANSMITTING ENTITY OR ELECTRONIC DOCUMENT MEDIATOR (TRANSMISSION)
(101)
REQUEST DOCUMENT TRANSMISSION
TRANSFER CERTIFICATE (TRANSMISSION/RECEPTION)
ELECTRONIC DOCUMENT DISTRIBUTION HUB (DISTRIBUTION RELAY SERVER)
(103)
TRANSFER CERTIFICATE (RECEPTION/READING)
PERFORM DOCUMENT TRANSMISSION
TRANSFER CERTIFICATE (RECEPTION)
RECEIVING ENTITY OR ELECTRONIC DOCUMENT MEDIATOR (RECEPTION)
(102)
TRANSFER DOCUMENT
TRANSMIT MESSAGE
TRANSFER DOCUMENT
INFORM READING OR NOT
TRANSMITTER
RECEIPTOR

[FIG. 2]


THIRD PARTY STORAGE AUTHORITY
TRANSMITTER
TRANSMITTING ENTITY OR ELECTRONIC DOCUMENT MEDIATOR (TRANSMISSION)
ELECTRONIC DOCUMENT DISTRIBUTION HUB (DISTRIBUTION RELAY SERVER)
RECEIVING ENTITY OR ELECTRONIC DOCUMENT MEDIATOR (RECEPTION)
RECEIPTOR
TRANSFER DOCUMENT
PACKAGE DOCUMENT & PROCESS SECURITY
TRANSMIT MESSAGE
CREATE RECEPTION CERTIFICATE
RECEPTION CERTIFICATE (ESSENTIAL)
TRANSFER RECEPTION CERTIFICATE
REQUEST RECEPTION CERTIFICATE STORAGE
ATTACH CERTIFICATE VERIFICATION INFORMATION
STORE RECEPTION CERTIFICATE
RESPOND TO STORAGE COMPLETION
TRANSFER DOCUMENT
PACKAGE DOCUMENT & PROCESS SECURITY
TRANSMISSION FAILURE
REQUEST DOCUMENT TRANSMISSION
CREATE TRANSMISSION CERTIFICATE
TRANSMISSION CERTIFICATE (ESSENTIAL)
TRANSFER TRANSMISSION CERTIFICATE
REQUEST TRANSMISSION CERTIFICATE STORAGE
ATTACH CERTIFICATE VERIFICATION INFORMATION
PERFORM DOCUMENT TRANSMISSION
STORE TRANSMISSION CERTIFICATE
RESPOND TO STORAGE COMPLETION
CREATE RECEIVING CERTIFICATE
TRANSFER RECEPTION CERTIFICATE
TRANSFER RECEIVING CERTIF CATE
ACKNOWLEDGE RECEPTION
REQUEST RECEPTION CERTIFICATE STORAGE
ATTACH CERTIFICATE VERIFICATION INFORMATION
STORE RECEPTION CERTIFICATE
RESPOND TO STORAGE COMPLETION
REQUEST READING
RECEIVE& READ DOCUMENT
RESPOND TO READING
READING CERTIFICATE (ESSENTIAL)
CREATE READING CERTIFICATE
TRANSFER READING CERTIFICATE
ACKNOWLEDGE RECEPTION
REQUEST READING CERTIFICATE STORAGE
ATTACH CERTIFICATE VERIFICATION INFORMATION
STORE READING CERTIFICATE
RESPOND TO STORAGE COMPLETION

METHOD FOR CREATING/ISSUING ELECTRONIC DOCUMENT DISTRIBUTION CERTIFICATE, METHOD FOR VERIFYING ELECTRONIC DOCUMENT DISTRIBUTION CERTIFICATE, AND SYSTEM FOR DISTRIBUTING ELECTRONIC DOCUMENT

TECHNICAL FIELD

[0001] The present invention relates to a method for creating/issuing an electronic document distribution certificate capable of providing a transparent and efficient issuing service and enhancing reliability of distribution of the electronic document due to compatibility guarantee of a certificate, in creating, distributing, and storing a distribution certificate within a system for distributing an electronic document based on a certified electronic address, a method for verifying an electronic document distribution certificate, and a system for distributing an electronic document.

BACKGROUND ART

[0002] Generally, an electronic document distribution has limitedly been conducted only within a specific industrial group or a community based on individual inherent regulations of enterprises/organizations.

[0003] There are disadvantages in that e-mail has been used as an auxiliary means between individuals and between individuals and enterprises/organizations without a concept of trusted electronic distribution or one-line communications may be made only by a method of accessing individuals, individual businesses, small-scale enterprises to large-scale enterprises.

[0004] Therefore, enterprises holding a predetermined scale of distribution system and individuals, individual businesses, and small-scale enterprises need to build an electronic document distribution based infrastructure capable of guaranteeing reliability of distribution.

DETAILED DESCRIPTION OF THE INVENTION

Technical Problem

[0005] The present invention has been made in an effort to provide a method for creating/issuing an electronic document distribution certificate capable of providing a transparent and efficient issuing service and enhancing reliability of distribution of the electronic document due to compatibility guarantee of a certificate, in creating, distributing, and storing a distribution certificate within a system for distributing an electronic document based on a certified electronic address. Further, the present invention has been made in an effort to provide a method for verifying a distribution certificate helping to correctly utilize a certificate by defining a standardized verifying method of a distribution certificate. In addition, the present invention has been made in an effort to provide a system for distributing an electronic document capable of guaranteeing reliability of distribution.

Technical Solution

[0006] An exemplary embodiment of the present invention provides a method of creating/issuing a distribution certificate in a system for distributing an electronic document including transmitting and receiving entities and a distribution hub, the method including: (a) transmitting, by a transmitting entity, a distribution message including a transmitter's electronic document to a receiving entity; (b) creating, by a receiving entity, a reception certificate by acquiring essential information after receiving the distribution message; (c) transmitting, by the receiving entity, the created reception certificate to the transmitting entity; (d) completing, by the transmitting entity, verification for the received reception certificate and then, attaching verification information on an electronic signature certificate of the reception certificate to the reception certificate; and (e) transmitting, by the transmitting entity, the reception certificate to a third party storage authority and requesting the storage thereto.

[0007] Another exemplary embodiment of the present invention provides a method for verifying a distribution certificate created/issued in a system for distributing an electronic document including transmitting and receiving entities and a distribution hub, the method including: verifying whether a format of a distribution certificate observes constraints of a predefined structure and value; verifying whether transmitting, receiving, and reading date and time of a distribution message that are established in a distribution certificate, an issuance date of a distribution certificate, a verification time of a certification, and an effect expiration date of a certificate are ordered; verifying an electronic signature attached to the distribution certificate; and verifying validity of a certificate in which an electronic signature is written in the distribution certificate and verifying identity with information on an issuer of the distribution certificate.

[0008] Yet another exemplary embodiment of the present invention provides a system for distributing an electronic document, including: transmitting and receiving entities that distribute an electronic document through a distribution messaging server transmitting and receiving a message based on an electronic document and issuing and managing a distribution certificate for message transmission and reception; a distribution hub that registers/manages the electronic addresses of the transmitting and receiving entities, sets an electronic document distribution path between the transmitting and receiving entities, performs message transmission when errors are created during an electronic document distribution process between the transmitting and receiving entities, and issues the distribution certificate; and a trusted third party storage authority that receives and stores the distribution certificate; wherein the distribution certificate includes a reception certificate for non-repudiation for the fact that a receive entity receives a message, a transmission certificate for verifying a transmission try of the transmit entity, and a reading certificate for non-repudiation for the fact that a receiptor reads the received message.

Advantageous Effects

[0009] As set forth above, according to the exemplary embodiments of the present invention, it is possible to provide the transparent and efficient issuance service, in creating, distributing, and storing the distribution certificate within the system for distributing an electronic document based on the certified electronic address.

[0010] According to the exemplary embodiments of the present invention, it is possible to enhance the reliability of distribution of the electronic document by guaranteeing the compatibility in the certificate within a system for distributing an electronic document based on a certified electronic address.

[0011] According to the exemplary embodiments of the present invention, it is possible to provide the method for

verifying a distribution certificate helping to correctly utilize a certificate by defining the standardized verifying method for the distribution certificate.

BRIEF DESCRIPTION OF DRAWINGS

[0012] FIG. **1** is a diagram for describing creation and issuance of a distribution certification according to an exemplary embodiment of the present invention.

[0013] FIG. **2** is a diagram illustrating a process for creating and issuing a distribution certificate according to an exemplary embodiment of the present invention.

BEST MODE

[0014] A method for creating/issuing an electronic document distribution certificate, a method for verifying an electronic document distribution certificate, and a system for distributing an electronic document according to exemplary embodiments of the present invention will be described below with reference to the accompanying drawings and Tables.

[0015] A method for creating an electronic document distribution certificate according to an exemplary embodiment of the present invention includes: (a) transmitting, by a transmitting entity, a distribution message including a transmitter's electronic document to a receiving entity; (b) receiving, by the receiving entity, the distribution message and acquiring essential information to create a reception certificate; (c) transmitting, by the receiving entity, the created reception certificate to the transmitting entity; (d) completing, by the transmitting entity, verification on the received reception certificate and then, attaching verification information on an electronic signature certificate of the reception certificate to the reception certificate; and (e) transmitting, by the transmitting entity, the reception certificate to a third party storage authority to request the storage.

[0016] A method for verifying an electronic document distribution certificate according to another exemplary embodiment of the present invention includes: verifying whether a format of the distribution certificate observes constraints of predefined structures and values; verifying whether transmitting, receiving, and reading date and time of a distribution message that are established in a distribution certificate, an issuance date of a distribution certificate, a verification time of a certification, and an effect expiration date of a certificate are ordered; verifying an electronic signature attached to the distribution certificate; and verifying validity of an authentication certificate that an electronic signature is written in the distribution certificate and verifying identity with information on an issuer of the distribution certificate.

[0017] A system for distributing an electronic document according to yet another exemplary embodiment of the preset invention includes: transmitting and receiving entities that distribute an electronic document through a distribution messaging server transmitting and receiving a message based on an electronic address and issuing and managing a distribution certificate for message transmission and reception; a distribution hub that registers/manages the electronic addresses of the transmitting and receiving entities, sets an electronic document distribution path between the transmitting and receiving entities, performs message transmission when errors are created during an electronic document distribution process between the transmitting and receiving entities, and issues the distribution certificate; and a trusted third party storage authority that receives and stores the distribution certificate, wherein the distribution certificate includes a reception certificate for non-repudiation for the fact that a receiving entity receives a message, a transmission certificate for verifying a transmission try of the transmitting entity, and a reading certificate for non-repudiation for the fact that a receptor reads the received message.

[0018] The method for creating an electronic document distribution certificate, the method for verifying an electronic document distribution certificate, and the system for distributing an electronic document according to the exemplary embodiments of the present invention having the foregoing configuration will be described in detail with reference to FIGS. **1** and **2**.

[0019] [Model for Creating and Issuing Electronic Document Distribution Certificate]

[0020] FIG. **1** illustrates components for creating and issuing a distribution certificate according to an exemplary embodiment of the present invention and each component will be described with reference to the following ① to ④

[0021] ① A transmitting entity (or transmitting electronic document mediator, hereinafter, referred to as transmitting entity **101**): basically transmits a transmitter's electronic document to a receiving entity or if necessary, requests a transmission to a distribution relay server. The transmitting entity serves to verify the distribution certificate received from the receiving entity or the distribution relay server and then, attach the verification information to the distribution certificate to be stored in a third party storage authority, in connection with the distribution certificate.

[0022] ② A receiving entity (or receiving electronic document mediator, hereinafter, referred to as receiving entity **102**): basically, transfers the electronic document received from the transmitting entity or the distribution relay server to a receiptor). The receiving entity serves to create the reception certificate as soon as receiving the electronic document from the transmitting entity or the distribution relay server and transmit the created certificate to the transmitting entity or the distribution relay server as a response message or create a reading certificate immediately after the receiptor reads the electronic document and transfer the created reading certificate to the transmitting entity, in connection with the distribution certificate.

[0023] ③ An electronic document distribution hub (or distribution relay server **103**): basically, transfers an electronic document receiving a transmission request from the transmitting entity to the receiving entity. The electronic document distribution hub serves to create the transmission certificate as soon as receiving the transmission request of the electronic document from the transmitting entity so as to be transmitted to the transmitting entity or transfer the electronic document to the receiving entity and then, transfer the reception certificate received as a response to the transmission certificate to the transmitting entity, in connection with the distribution certificate.

[0024] ④ A third party storage authority (certified electronic document storage authority **104**) serves to safely store the distribution certificate as a trusted authority. Hereinafter, in describing the present invention, reference numerals of FIG. **1** will be omitted.

[Type and Process of Electronic Document Distribution Certificate]

[0025] The essential information required to create the electronic document distribution certificate according to the present invention is as the following Table 1.

TABLE 1

Type	Purpose	Creation Subject/Time	Essential information
Reception certificate	Non-repudiation for message receiving fact of receiving entity	Receiving entity/immediately after reception	Document information, transmitter, receiptor, transmitter transmitting time, receiptor receiving time
Transmission certificate	Verification for transmission try of transmitting entity	Distribution relay server/immediately after reception of transmission request message	Document information, transmitter, receiptor, transmitter transmission requesting time
Reading Certificate	Non-repudiation for fact that receiptor reads received message	Receiving entity/immediately after being read by receiptor	Document information, transmitter, receiptor, transmitter transmitting time, receiptor receiving time, receiptor reading time

[0026] A method for acquiring essential information on the electronic document distribution certificate according to the present invention is as the following Table 2.

TABLE 2

Type	Essential information	Method for acquiring information
Reception certificate	Document information, transmitter, receiptor, transmitter transmitting time	Use the sensitive field value of the distribution message and the SOAP message within the distribution linkage message transmitted by the transmitting entity
	Receiptor receiving time	Use the receiving time of the distribution messaging server of the receiving entity
Transmission certificate	Document information, transmitter, receiptor	Use the sensitive field value of the distribution message within the distribution linkage message transmitted by the transmitting entity
	Transmitter transmission requesting time	Use the receiving time of the distribution relay server
Reading Certificate	Document information, transmitter, receiptor, transmitter transmitting time	Use the sensitive field value of the distribution message and the SOAP message within the distribution linkage message transmitted by the transmitting entity
	Receiptor receiving time	Use the receiving time of the distribution messaging server by the receiving entity
	Receiptor reading time	Use the response time of the receiving entity for the document information request of the receiptor

[0027] ※ The system time of the distribution messaging server and the distribution relay server needs to be periodically synchronized with the time of externally authorized institution.

[0028] All of the processes involved in the electronic document distribution certificate according to the present invention are illustrated in FIG. **2**.

[0029] The reception certificate is an electronic document distribution certificate created for verifying the fact that the electronic document distribution message is received from the transmitting entity and the processes involved in the reception certificate are as the following Table 3.

TABLE 3

No.	Process Name
1	The transmitting entity transmits the distribution message including the transmitter's electronic document to the receiving entity
2	The receiving entity receives the distribution message and then, immediately receives the essential information to create the reception certificate
3	The receiving entity transmits the created reception certificate to the transmitting entity
4	The transmitting entity completes verification for the reception certificate and then, attaches the verification information on the electronic signature certificate of the reception certificate to the reception certificate
5	The transmitting entity transmits and stores the reception certificate to the certified electronic document storage authority.

[0030] When the transmitting entity tries the distribution message transmission to the receiving entity but fails in the distribution message transmission, and thus requests the transmission of the corresponding message to the distribution relay server, the transmission certificate is created by the distribution relay server for verifying the fact that the transmitting entity makes the transmission request and transmitted to the transmitting entity. The process involved in the transmission certificate is as the following Table 4.

TABLE 4

No.	Process Name
1	The transmitting entity transmits the distribution message to the receiving entity.
2	When the distribution message transmission fails, the transmitting entity requests the distribution message transmission to the distribution relay server.
3	The distribution relay server creates the transmission certificate for the requested transmission.
4	The distribution relay server transmits the transmission certificate to the transmitting entity.

TABLE 4-continued

No.	Process Name
5	The transmitting entity completes verification for the transmission certificate and then, attaches the verification information on the electronic signature certificate of the transmission certificate to the transmission certificate.
6	The transmitting entity stores the transmission certificate in the certified electronic document storage authority.
7	The distribution relay server transfers the distribution message to the receiving entity.
8	The receiving entity creates the reception certificate immediately after the reception of the electronic document.
9	The receiving entity transmits the reception certificate to the distribution relay server
10	The distribution relay server transfers the reception certificate to the transmitting entity.
11	The transmitting entity completes the verification for the reception certificate and then, attaches the verification information on the electronic signature certificate of the reception certificate to the reception certificate
12	The transmitting entity transmits and stores the reception certificate to the certified electronic document storage authority.

[0031] The reading certificate is a certificate that is created by the receiving entity and is transmitted to the transmitting entity so as to verify that the receiptor reads the message received from the transmitting entity by the receiving entity and the process involved in the reading certificate is as the following Table 5.

TABLE 5

No.	Process Name
1	The receiptor requests the reading of the distribution message to the receiving entity to read the distribution message received as a response.
2	The receiving entity creates the reading certificate.
3	The receiving entity completes the verification for the reading certificate and then, attaches the verification information on the electronic signature certificate of the reading certificate to the reading certificate.
4	The transmitting entity transmits and stores the reading certificate to the certified electronic document authority.

[Basic Preconditions and Considerations Involved in Issuance and Verification of Distribution Certificate]

[0032] The basic preconditions and considerations involved in the issuance and verification of the distribution certificate are as the following ① to ⑨.

[0033] ① The distribution certificate is created and verified by the distribution messaging server and the distribution relay server of the transmitting and receiving entities.

[0034] ② In the present invention, the distribution certificate is electronically signed and created only based on an NPKI certificate.

[0035] ③ The corresponding distribution certificate is created based on the distribution message. Even though at least two electronic documents are included in a single distribution message, only one distribution certificate created.

[0036] ④ The distribution certificate needs to be allocated with an ID that can identify the distribution message and an electronic document identifier or an electronic document name that can identify the electronic document within the distribution message.

[0037] ⑤ A serial number of the distribution certificate is created by individual transmitting and receiving entities and thus uses a random number of 32 bytes so as to allocate uniqueness.

[0038] ⑥ Update and revocation of the distribution certificate is not defined in terms of characteristics of the distribution system.

[0039] ⑦ The distribution messaging server needs to maintain the synchronization with the visual information of the external trusted institution at all times, thereby guaranteeing the reliability of the visual information within the distribution certificate.

[0040] ⑧ The policies of the distribution certificate use only an object identifier (OID) and a name that are defined in the present technology standard.

[0041] ⑨ The transmitting entity verifies the received distribution certificate and then, attaches the verification information on the signature certificate of the distribution certificate to the distribution certificate.

[Structure of Electronic Document Distribution Certificate]

[0042] The electronic document distribution certificate is created by the transmitting and receiving entities and electronically signed by using the NPKI certificate of the transmitting and receiving entities. The basic structure of the electronic document distribution certificate uses a SignedData structure of a CMS standard to use the same content identifier as the certificate of the certified electronic document authority.

[0043] ContentType of the electronic document distribution certificate is as the following Table 6.

TABLE 6

```
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 }
```

[0044] A basic field of the electronic document distribution certificate is as the following Table 7.

TABLE 7

```
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 }
```

[0045] The detailed contents of the basic field of the foregoing distribution certificate are the following to.

[0046] ① Version, Version

[0047] A version of the structure of the electronic document distribution certificate is represented. For the electronic document distribution certificate, the version is set to be v9 and uses a distributionInfos type of a target field.

TABLE 8

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

[0048] ② SerialNumber, Serial Number

[0049] The identification information of the electronic document distribution certificate is represented.

[0050] The serial number of the electronic document distribution certificate uses a random number of 32 bytes so as to be created as a unique amount of integer value. In order to process the electronic document distribution certificate, there is a need to process a serial number of 32 bytes.

TABLE 9

```
SerialNumber ::= INTEGER
```

[0051] ③ Issuer, Issuer of Certificate

[0052] A subject issuing the electronic document distribution certificate is represented.

[0053] When the value of the present field is created, a directoryName field having a GeneralName structure is necessarily used and the receiving entity or the distribution relay server extracts a subjectDN value of the certificate in which the electronic document distribution certificate is electronically signed so as to be set as it is.

TABLE 10

```
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)) }
```

[0054] ④ DataOfIssue, Issuance Date of Certificate

[0055] The time when the electronic document distribution certificate is issued is represented.

[0056] The dataOfIssue uses a GeneralizedTime format.

[0057] ⑤ DataOfExpire, Effect Expiration Date of Certificate

[0058] The time when the electronic document distribution certificate expires is represented.

[0059] The dataOfExpire of the electronic document distribution certificate is in the future, as compared with the dataOfIssue and needs to be set to have a sufficient spare in consideration of a period required to verify the distribution fact.

TABLE 11

```
DateOfExpiration ::= GeneralizedTime
```

[0060] ⑥ Policy, Certificate Policy

[0061] The policy of the electronic document distribution certificate is represented.

[0062] The present field is configured of Qualifier information for representing a policy OID according to types of electronic document distribution certificates and types of electronic document distribution certificates. It is to be noted that only userNotice is used as the Qualifier information and cPSuri is not used. The types of electronic document distribution certificates are displayed using an explicitText field that is lower than the userNotice field and a format thereof needs to use BMPString.

TABLE 12

```
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)) }
```

[0063] The policy OID within the electronic document distribution certificate follows the types of certificates and needs to use only the values designated in the present invention.

[0064] The OID and the Qualifier information according to the type of the electronic document distribution certificate are as follows.

TABLE 13

Type of Certificate	Policy OID	Qualifier
Transmission certificate	1.2.410.200032.6.1	"Transmission certificate"
Reception certificate	1.2.410.200032.6.2	"Reception certificate"
Reading certificate	1.2.410.200032.6.3	"Reading certificate"

[0065] ⑦ RequestInfo, Certificate Request Message Information

[0066] The present field is set to be null.

TABLE 14

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

[0067] ⑧ Target, Object to Certify

[0068] The present field includes the contents to be verified.

[0069] The present field needs to set the information on the distribution message by necessarily using the lower distributionInfos field.

TABLE 15

```
TargetToCertify ::= CHOICE {
        opRecord                [0] EXPLICIT
OperationRecord,
        orgAndIssued            [1] EXPLICIT
OriginalAndIssuedDocumentInfo,
        dataHash                [2] EXPLICIT HashedDataInfo
        distributionInfos       [10] EXPLICIT
DistributionInfos }
DistributionInfos ::= SEQUENCE OF DistributionInfo
DistributionInfo ::= SEQUENCE {
        senderAdd               UTF8String,
        receiptorAdd            UTF8String,
        dateOfSend              GeneralizedTime,
        dateOfReceive           [0] EXPLICIT
GeneralizedTime OPTIONAL,
        dateOfReceiveConfirm    [1] EXPLICIT
GeneralizedTime OPTIONAL,
        distributionId          UTF8String,
        numberOfFiles           INTEGER,
        distributedFileInfos    DistributedFileInfos }
```

[0070] 1) SenderAdd, Transmitter's Certified Electronic Address

[0071] The certified electronic address of the transmitter transmitting the electronic document distribution message is represented.

[0072] 2) ReceiverAdd, Receiptor's Certified Electronic Address

[0073] The certified electronic address of the receiptor receiving the electronic document distribution message is represented.

[0074] 3) DateOfsend, Transmitting Date and Time

[0075] The time when the distribution message is transmitted by the transmitter is represented.

[0076] The transmitting date and time of the reception certificate and the reading certificate means the time when the transmitting entity transmits the distribution message and the value of the TimeStamp field that is included in the SOAP message within the "message transmission" distribution linkage message is represented in the GeneralizedTime format.

[0077] It is to be noted that the transmitting date and time of the transmission certificate means the time when the transmitting entity requests the transmission of the distribution message to the distribution relay server and uses the time when the distribution relay server receives the "message transmission request" distribution message, unlike other distribution certificates using time values within the distribution linkage message. In connection with the time field, only the present field is included in the transmission certificate and the receiving date and time field and the reading date and time field are not created.

[0078] 4) DateOfReceive, Receiving Date and Time

[0079] The time when the receiptor receives the distribution message is represented.

[0080] The receiving date and time is a field that is created only in the reception certificate and the reading certificate and is set as the time when the distribution messaging server of the receiving entity receives the "message transmission" distribution message.

[0081] The receiving date and time is after the transmitting date and time and is equal to or earlier than the time when the certificate is created.

[0082] 5) DateOfReceiveConfirm, Reading Date and Time

[0083] The time when the receiptor reads the electronic document after receiving the electronic document is represented.

[0084] The reading date and time is a field that is created only in the reading certificate and is set as the time when the distribution messaging server of the receiving entity responds to the receiptor's "message detailed information request". The time needs to be equal to a value of a TimeStamp field included in the SOAP message within the distribution linkage message responding to the receiptor by the receiving entity represented in the GeneralizedTime format.

[0085] The reading date and time needs to be equal to or earlier than the time when the certificate is created and is equal to or later than the receiving date and time.

[0086] 6) DistributionId, Distribution Identification Value

[0087] An identification value for the distribution message is represented.

[0088] An identifier of the distribution message that is the issuance object of the electronic document distribution certificate is set as it is.

[0089] 7) NumberOfFiles, The Number of Distribution Files

[0090] The number of electronic document files attached to the distribution message is represented.

[0091] The number of electronic document files attached to the actual distribution message is set.

[0092] 8) DistributedFileInfos, Distribution Document Information

[0093] The distribution message may be attached with at least one electronic document file and sets the information on the individual files using a DistributedFile structure.

TABLE 16

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

TABLE 16-continued

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

[0094] 9) FileHashedData, File Hash Information

[0095] Hash values of individual electronic document files attached to the distribution message are represented.

[0096] The individual electronic document file is set in a hashedData field after a hash value is created using a hash algorithm of a hashAlg field.

[0097] 10) Filed, File Identification Value

[0098] Identifiers of individual electronic document files attached to the distribution message are represented. The file identification value is not present within the distribution message and a Content-ID value of the individual electronic document file attached to the overall distribution linkage message configured of a Multi Part message in an MIME format is set as it is.

[0099] The field may be selectively used, but when the file name field is not used, is necessarily used and it is recommended that the file identification value field be used.

[0100] When there are both the file identification value field and the file name field at the time of the verification of the distribution certificate, the distribution certificate is compared with the electronic document file and verified by preferentially using the file identification value field.

[0101] 11) FileName, File Name

[0102] The file names of the individual electronic document files attached to the distribution message are represented.

[0103] When the file identification value field is not created, the file name field is necessarily created and as a value, the Content-ID value of the individual electronic document file attached to the overall distribution linkage message configured of the Multi Part message in the MIME format is set as it is. When the file identification value field is created, the file name field may be omitted and the value capable of auxiliarily identifying the electronic document file is set at the time of the creation of the file identification value field.

[0104] The electronic document distribution certificate profile is as the following Table 17.

TABLE 17

Basic field	Content	Peculiar Matters
version	Version	v9
serialNumber	Serial Number	Random number of 32 bytes
issuer	Certificate Issuer	subject DN of signature certificate
dateOfIssue	Issuance date of certificate	GeneralizedTime
dateOfExpire	Effect expiration date of certificate	GeneralizedTime
policy	Certificate policy	OID: 1.2.410.200032.6.1 (Transmission): 1.2.410.200032.6.2 (Reception): 1.2.410.200032.6.3 (Reading)

TABLE 17-continued

Basic field	Content	Peculiar Matters
requestInfo	Certificate request message information	null
target	Verification object	Use of distributionInfos structure
senderAdd	Transmitter's certified electronic address	UTF8String
receiptorAdd	Receiptor's certified electronic address	UTF8String
dateOfSend	Transmitting date and time	GeneralizedTime, necessary
dateOfReceive	Receiving date and time	GeneralizedTime, selection
dateOfReceiveConfirm	Receiving acknowledgement date and time	GeneralizedTime, selection
distributionId	Distribution identifier	UTF8String
numberOfFiles	The number of transmission files	
distributedFileInfos	Transmission file information	At least one DistributedFile
DistributedFile		
fileHashedData	File hash value	SHA256
fileId	File ID	One of two fields, that is, fileId and filename is essential
fileName	File name	

[0105] Considerations associated with the electronic document distribution certificate profile are as the following ① to ③.

[0106] ① At the time of electronic signature, a public key encryption algorithm uses RSA and a hash algorithm uses SHA256

[0107] ② The electronic signature certificate is necessarily included in signedData

[0108] ③ Only one signerInfo is included in a signerInfos field.

[Method for Verifying Electronic Document Distribution Certificate

[0109] The distribution message transmitting entity needs to perform the verification on the certificate as soon as receiving the electronic document distribution certificate.

[0110] The process of verifying distribution certificate is largely divided into the validity verification of the certificate and the content verification of the certificate. The validity verification of the certificate is a process of confirming whether conditions for obtaining an effect as the certificate are satisfied and the content verification of the certificate is a process of confirming the fact by comparing with the distribution message to be verified through the certificate. Therefore, the content verification of the certificate is not the verification for the certificate but may be considered to be performed to confirm whether the distribution fact is truth.

[0111] The validity verification of the electronic document distribution certificate is performed by the processes of ① verifying the certificate format, ② visually verifying certificate, ③ verifying the certificate electronic signature, and ④ verifying the signature certificate and the content verification

of the certificate is performed by ⑤ the process of comparing and verifying the distribution message.

[0112] ① Verification of Certificate Format

[0113] The verification of the certificate format is a process of confirming whether the format of the distribution certificate to be verified observes the constraints of the structure and value defined in the present standard and the following 1) to 7) matters are basically confirmed at the time of verifying the certificate format.

[0114] 1) Does the overall structure of the distribution certificate meet the signedData format and observe a rule on whether the lower field defined in the present standard is created?

[0115] 2) Is the version to be set to v9?

[0116] 3) Is the serial number created as the positive integer value by using the random number of 32 bytes?

[0117] 4) Is the certificate issuer set by using the dirctroyName field of the GeneralName structure?

[0118] 5) Are the issuance date of the certificate and the effect expiration date of the certificate set by using the GeneralizedTime format?

[0119] 6) Is the certificate policy created by using the structure and values of the lower field defined in the present standard?

[0120] 7) Is the verification object field created by using the distributionInfos field and does the verification object field observe a rule on whether the lower field according to the types of certificates proposed in the certificate policy is created?

[0121] ② Certificate Visual Verification

[0122] The certificate visual verification is a process of confirming whether the values of each visual field set in the distribution certificate are normal at the verification reference time. That is, it is confirmed that the values of each visual field set in the distribution certificate meets the rule of the following Table 18 unlike those at the verification reference time, during the present process.

TABLE 18

Transmitting date and time < receiving date and time ≦ reading date and time ≦ issuance date of certificate ≦ certificate verification time ≦ effect expiration date of certificate

[0123] ③ Verification of Certificate Electronic Signature

[0124] The verification of the electronic signature is a process of verifying the electronic signature attached to the distribution certificate for integrity guarantee and non-repudiation for the contents to be verified by the distribution certificate and follows the method for verifying an electronic signature for the signedData of a general CMS.

[0125] ④ Verification of Signature Certificate

[0126] The verification of the signature certificate is a process of verifying the validity of the certificate in which the distribution certificate is electronically signed and the identity with the issuer information of the distribution certificate.

[0127] The validity verification of the electronic signature certificate is a process that is generally included in the process of verifying the electronic signature as a part thereof and is performed by the processes of verifying an available period of the certificate, verifying the revocation, and verifying a path with the upper CA certificates, and the like. This is verified based on "technology standard [KCAC.TS.CERTVAL] of verifying authorized certificate path" of the authorized certificate system.

[0128] If the validity verification of the electronic signature certificate succeeds, the comparison and verification with the issuer information of the distribution certificate needs to be performed. The issuer information of the distribution certificate is formed to set a subject DN value of the electronic signature certificate as it is and therefore, two values are extracted to perform the comparison and verification on whether the two values coincide with each other.

[0129] ⑤ Comparison and Verification of Distribution Message

[0130] The process of comparing and verifying a distribution message is not a process of verifying the validity of the distribution certificate but is a process of confirming whether the distribution fact is truth by comparing and verifying the information of the distribution message included in the distribution certificate with that of the actual distribution message.

[0131] When the transmitting entity transmits the distribution message or receives the distribution certificate after the transmission request, it is to be necessarily confirmed that the corresponding distribution certificate includes the information on the distribution message transmitted by the transmitting entity, by performing the comparison and verification of the present distribution message.

[0132] At the time of the comparison and verification of the distribution message, the following matters are basically confirmed.

[0133] Do the transmitter's certificated electronic address and the receiptor's certified electronic address correspond to the distribution message?

[0134] Does the transmitting date and time of the reception certificate and the reading certificate coincide with a value of TimeStamp field included in the SOAP message within the "message transmission" distribution linkage message?

[0135] Is the transmitting date and time of the transmission certificate the reasonable time for the distribution relay server to receive the "message transmission request" distribution message?

[0136] Is the receiving date and time of the reception certificate and the reading certificate for the "message transmission" distribution message directly transmitted to the receiving entity by the transmitting entity the reasonable time for the distribution messaging server of the receiving entity to receive the "message transmission" distribution message?

[0137] Is the receiving date and time of the reception certificate and the reading certificate for the "message transmission request" distribution message requested to the distribution relay server by the transmitting entity the reasonable time for the distribution messaging server of the receiving entity to receive the "message transmission" distribution message? (however, correspond to only to the case in which the transmitting entity can know the time when the distribution relay server transfers the distribution message to the receiving entity).

[0138] Does the reading date and time of the reading certificate coincide with the value of the TimeStamp field included in the SOAP message within the distribution linkage message responding to the "message detailed information request" of the receiptor by the

receiving entity (however, corresponding to only the case in which the transmitting entity can know the value of the corresponding TimeStamp field).

[0139] Does the distribution identification value coincide with the identifier of the distribution message that is the issuance object of the distribution certificate?

[0140] Is the number of distribution files equal to the number of electronic document files attached to the actual distribution message?

[0141] Do all of the file identification values or the file names of the individual files included in the distribution document information coincide with the Content-ID values of the electronic document file attached to the actual distribution message?

[0142] Does all of the file hash information of the individual files included in the distribution document information coincide with the values obtained by hashing the electronic document files attached to the actual distribution message?

[0143] [Long-Term Verification Information of Electronic Signature]

[0144] When the verification for the issued distribution certificate is completed in consideration of the importance of the distribution certificate, the distribution certificate is registered and stored in the certified electronic document authority, which provides only the long-term guarantee function for the storage time and integrity of the distribution certificate but cannot guarantee the long period of time for the validity of the electronic signature certificate of the issuance time of the distribution certificate after the available period of the electronic signature certificate expires. That is, after the valid period of the electronic signature certificate expires, the validity guarantee of the distribution certificate is not permitted. In order to solve the problem, it is possible to verify the distribution certificate even after the available period of the certificate in which the distribution certificate is electronically signed expires, by storing the verification information that can confirm that the corresponding electronic signature certificate is valid at the time when the distribution certificate is issued together with the distribution certificate.

[0145] ① Acquisition of Verification Information of Electronic Signature Certificate

[0146] The transmitting entity collects CRL and ARL and an upper CA certificate and a Root CA certificate for verifying the revocation of the electronic signature certificate and the path so as to perform the process of "5.2.4 verification of signature certificate" among the processes of verifying the validity of the received distribution certificate. It is possible to guarantee the validity of the electronic signature certificate at the time of the issuance of the distribution certificate by storing the corresponding data in the certified electronic document authority together with the distribution certificate, such that the validity of the distribution certificate is guaranteed.

[0147] ② Storage of Verification Information of Electronic Signature Certificate

[0148] The transmitting entity includes the CRL and the ARL and the upper CA certificate and the Root CA certificate that are used for verification in a certificates field and a crls field within the signedData structure of the distribution certificate after the verification for the electronic signature certificate succeeds. Precautions need to perform only the work including each information in the corresponding field regardless of an order of including each information. Since the certificates field and the crls field are not the electronic signature object information of the signedData, the verification for the distribution certificate still succeeds even after the corresponding work is performed.

TABLE 19

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

[0149] ③ Storage in Certificated Electronic Document Authority

[0150] The transmitting entity stores the distribution certificate in which the verification information of the electronic signature certificate is included in the certified electronic document authority, such that the long-term verification for the distribution certificate can be performed.

1. A method for creating/issuing a distribution certificate in a system for distributing an electronic document including transmitting and receiving entities and a distribution hub, the method comprising:

(a) transmitting, by a transmitting entity, a distribution message including a transmitter's electronic document to a receiving entity;

(b) creating, by a receiving entity, a reception certificate by acquiring essential information after receiving the distribution message;

(c) transmitting, by the receiving entity, the created reception certificate to the transmitting entity;

(d) completing, by the transmitting entity, verification for the received reception certificate and then, attaching verification information on an electronic signature certificate of the reception certificate to the reception certificate; and

(e) transmitting, by the transmitting entity, the reception certificate to a third party storage authority and requesting the storage thereto.

2. The method of claim **1**, wherein in the step (b), when the receiving entity creates the reception certificate, the essential information includes electronic document information, a transmitter, a receiptor, a transmitter transmitting time, and a receiptor receiving time.

3. The method of claim **1**, further comprising:

in the step (a), when the transmitting entity tries the transmission of the distribution message to the receiving entity but fails in the transmission of the distribution message,

(a1) requesting, by the transmitting entity, the transmission of the distribution message to a distribution relay server of the distribution hub;

(a2) creating, by the distribution relay server, the transmission certificate for the requested transmission;

(a3) transmitting, by the distribution relay server, the transmission certificate to the transmitting entity;

(a4) completing, by the transmitting entity, the verification for the received reception certificate and then, attaching the verification information on the electronic signature certificate of the reception certificate to the reception certificate; and

(a5) transmitting, by the transmitting entity, the reception certificate to the third party storage authority and requesting the storage thereto;

(a6) transmitting, by the distribution relay server, the distribution message to the receiving entity;

(a7) creating, by the receiving entity, the reception certificate immediately after receiving the electronic document;

(a8) transmitting, by the receiving entity, the reception certificate to the distribution relay server;

(a9) transmitting, by the distribution relay server, the reception certificate to the transmitting entity; and

(a10) performing, by the transmitting entity, steps (d) and (e) in order.

4. The method of claim **3**, wherein in the step (a2), when the distribution relay server creates the transmission certificate, the essential information includes electronic document information, a transmitter, a receiptor, and a transmitter transmitting request time.

5. The method of claim **1**, further comprising:

after the step (e),

(f1) reading, by the receiptor, the distribution message received by requesting the reading of the distribution message to the receiving entity;

(f2) creating, by the receiving entity, a reading certificate;

(f3) completing the verification for the received reading certificate and then, attaching the verification information on the electronic signature certificate of the reading certificate to the reading certificate; and

(f4) transmitting, by the transmitting entity, the reading certificate to the third party storage authority and requesting the storage thereto.

6. The method of claim **3**, further comprising:

after the step (a 10),

(a11) reading, by the receiptor, the distribution message received by requesting the reading of the distribution message to the receiving entity;

(a12) creating, by the receiving entity, the reading certificate;

(a13) completing the verification for the received reading certificate and then, attaching the verification information on the electronic signature certificate of the reading certificate to the reading certificate; and

(a14) transmitting, by the transmitting entity, the reading certificate to the third party storage authority and requesting the storage thereto.

7. The method of claim **5**, wherein when the receiving entity creates the reading certificate, the necessary information includes electronic document information, a transmitter, a receiptor, a transmitter transmitting time, a receiptor receiving time, and a receiptor reading time.

8. A method of verifying a distribution certificate created/issued in a system for distributing an electronic document including transmitting and receiving entities and a distribution hub, the method comprising:

verifying whether a format of a distribution certificate observes constraints of a predefined structure and value;

verifying whether transmitting, receiving, and reading date and time of a distribution message that are established in a distribution certificate, an issuance date of a distribution certificate, a verification time of a certification, and an effect expiration date of a certificate are ordered;

verifying an electronic signature attached to the distribution certificate; and

verifying validity of a certificate in which an electronic signature is written in the distribution certificate and verifying identity with information on an issuer of the distribution certificate.

9. The method of claim **8**, further comprising:

comparing and verifying information of the distribution message included in the distribution certificate with an actual distribution message.

10. The method of claim **9**, wherein the comparing and verifying includes:

confirming whether a transmitter certified electronic address and a receiptor certified electronic address included in the distribution certificate coincide with the transmitter certified electronic address and the receiptor certified electronic address of the actual distribution message; and

confirming whether the number of distribution files included in the distribution certificate is equal to the number of electronic document files attached to the actual distribution message.

11. The method of claim **9**, wherein the comparing and verifying includes:

when the distribution certificate is a reception certificate or a reading certificate, confirming whether the transmitting date and time included in the distribution certificate coincides with a value of a TimeStamp field included in a SOAP message within a "message transmission" distribution message; and

when the distribution certificate is a transmission certificate, confirming whether the transmitting date and time included in the distribution certificate is a reasonable time for a distribution relay server to receive a "message transmission request" distribution message.

12. The method of claim **9**, wherein the comparing and verifying includes:

when the distribution certificate is the receiving certificate or the reading certificate for the "message transmission" distribution message directly transmitted to the receiving entity by the transmitting entity, confirming whether the receiving date and time of the distribution certificate is the reasonable time for the distribution messaging server of the receiving entity to receive the "message transmission" distribution message; and

when the distribution certificate is the receiving certificate or the reading certificate for the "message transmission request" distribution message requested to the distribution relay server of the distribution hub by the transmitting entity, confirming whether the receiving date and time of the distribution certificate is the reasonable time for the distribution message server of the receiving entity to receive the "message transmission" distribution message.

13. The method of claim **9**, wherein the comparing and verifying includes:

when the distribution certificate is the reading certificate, confirming whether the reading date and time of the distribution certificate coincides with the TimeStamp field value included in the SOAP message within a distribution linkage message that the receiving entity responds to a "message detailed information request" of the receiptor.

14. The method of claim **9**, wherein the comparing and verifying includes:

confirming whether a distribution identification value included in the distribution certificate coincides with an identifier of the distribution message that is an issuance object of the distribution certificate;

confirming whether all of the file identification values or file identification names of individual files included in the distribution document information of the distribution certificate coincide with Content-ID values of an electronic document file attached to the actual distribution message; and

confirming whether all of the file hash information of the individual files included in the distribution document information of the distribution certificate coincides with the values obtained by hashing the electronic document files attached to the actual distribution message.

15. A system for distributing an electronic document, comprising:

transmitting and receiving entities that distribute an electronic document through a distribution messaging server transmitting and receiving a message based on an electronic document and issuing and managing a distribution certificate for message transmission and reception;

a distribution hub that registers/manages the electronic addresses of the transmitting and receiving entities, sets an electronic document distribution path between the transmitting and receiving entities, performs message transmission when errors are created during an electronic document distribution process between the transmitting and receiving entities, and issues the distribution certificate; and

a trusted third party storage authority that receives and stores the distribution certificate;

wherein the distribution certificate includes a reception certificate for non-repudiation for the fact that a receiving entity receives a message, a transmission certificate for verifying a transmission try of the transmit entity, and a reading certificate for non-repudiation for the fact that a receiptor reads the received message.

16. The system of claim **15**, wherein the distribution certificate includes:

a version of a distribution certificate structure, identification information of the distribution certificate, a subject issuing the distribution certificate, an issuance date of the distribution certificate, an effect expiration date of the distribution certificate, a policy of the distribution certificate, distribution certificate request message information, and a verification object.

17. The system of claim **16**, wherein the verification object includes:

a transmitter's certified electronic address through which a distribution message is transmitted, a receiptor's certified electronic address through which the distribution message is received, a time when the transmitter transmits the distribution message, a time when the receiptor receives the distribution message, a time when the receiptor receives and reads the electronic document, an identification value for the distribution message, the number of electronic document files attached to the distribution message, information on each of the electronic documents attached to the distribution message, a hash value of the individual electronic document file attached to the distribution message, an identifier of the individual electronic document file attached to the distribution message, and a file name of the individual electronic document file attached to the distribution message.

* * * * *