159159

[Description]

[Invention Title]

ELECTRONIC DOCUMENT DISTRIBUTION SYSTEM AND ELECTRONIC DOCUMENT DISTRIBUTION METHOD

[Technical Field]

The present invention relates to an electronic document distribution system and an electronic document distribution method that can construct an electronic document distribution system for providing not only enterprise/institutions, but also individuals and small companies with reliability.

[Background Art]

Generally, the electronic document distribution has been restrictively performed only in a specific industrial group or community based on an individual unique regulation of corporations/institutions.

Further, there are problems in that an email is used as an assistant means between general individuals or between an individual and an enterprise/institution without considering a concept of a reliable electronic distribution, or online communication is performed only when the individual, an individual business, or a small company access to an web site of the enterprise.

Therefore, it is expected that not only the enterprise that can possess a predetermined size of

distribution system, but also the individuals, the individual business, or the small company may build an electronic document distribution based infra that guarantees the reliability of the distribution.

[Disclosure]

[Technical Problems]

The present invention makes an effort to provide an electronic document distribution system and an electronic document distribution method that allow not only the corporation/institution that can possess a predetermined size of distribution system, but also the individuals and the small company to establish reliability.

[Technical Solution]

An electronic document distribution system according to an exemplary embodiment of the present invention includes: a transceiving entity that transmits and receives a message based on an electronic mailing address and distributes the electronic document through a distribution messaging server that issues and manages a distribution certificate for message transmission/reception, a distribution hub that registers/manages the electronic mailing address of the transceiving entity, sets an electronic document distribution route between the transceiving entities, provides a standard form of the electronic document to the transceiving entity, transmits

the message by proxy when an error occurs in the process of distribution the electronic document between the transceiving entities and issues a distribution certificate; and a reliable third party storing institution that receives and stores the distribution certificate.

In an electronic document distribution system according to an exemplay embodiment of the present invention, a method of distributing an electronic document in an electronic document distribution system including a transceiving entity and a distribution hub include: (a) a step of allowing a transmitting entity to acquire physical address information corresponding to address information of a receiving entity and then transmit a message with an attached electronic document to the physical address, (b) a step of allowing the receiving entity that receives the message to issue a reception certificate or an error certificate in accordance with compatibility verification result for a received message and the transmitting entity and deliver the certificate to the transceiving entity; and (c) a step of allowing a transmitting entity that transmits the message to the receiving entity but fails the transmission to request the distribution hub to transmit the message by proxy and allowing the distribution hub that receives request to transmit a message by proxy to issue the transmission certificate to deliver the certificate to

the transmitting entity and transmit the message to the receiving entity and then perform the step (b).

[Advantageous Effects]

The present invention with the above-mentioned configuration and method may build an electronic document distribution system that allows not only the corporation/institution, but also the individuals and the small company to establish reliability.

[Description of Drawings]

Fig. 1 is a view illustrating a configuration example of an electronic document distribution system according to an exemplary embodiment of the present invention.

Fig. 2 is a view illustrating a distribution messaging server of Fig. 1.

Fig. 3 is a view illustrating a distribution client of Fig. 1.

Fig. 4 is a view illustrating an address directory server of Fig. 1.

Fig. 5 is a view illustrating an electronic document form register of Fig. 1.

Fig. 6 is a view illustrating a distribution relay server of Fig. 1.

Fig. 7 is a view illustrating an externally connected gateway of Fig. 1.

Fig. 8 is a view illustrating an effective range of a

certified electronic mailing address in the electron document distribution system of Fig. 1.

Fig. 9 is a view illustrating an application/issuance, and operation system of the certified electronic mailing address according to an exemplary embodiment of the present invention.

Figs. 10 to 13 are views illustrating a message security when the electronic document is distributed in the exemplary embodiment of the present invention.

Figs. 14 to 17 are views illustrating a message transceiving processor in the exemplary embodiment of the present invention.

Fig. 18 is a view illustrating a physical address obtaining process according to an exemplary embodiment of the present invention.

Figs. 19 to 21 are views illustrating a distribution relay supporting process according to an exemplary embodiment of the present invention.

Figs. 22 to 24 are views illustrating a managing process such as certified electronic mailing address registration according to an exemplary embodiment of the present invention.

Figs. 25 and 26 are views illustrating an electronic document format application process according to an exemplary embodiment of the present invention.

Figs. 27 to 29 are views illustrating a spam message processing process according to an exemplary embodiment of the present invention.

Figs. 30 and 31 are conceptual views of an electronic document reading service according to an exemplary embodiment of the present invention.

Fig. 32 is a conceptual view of an externally connected gateway server according to an exemplary embodiment of the present invention.

Fig. 33 is a view illustrating a process of distributing an electronic document that is connected to an external system in the exemplary embodiment of the present invention.

Figs. 34 to 38 are views illustrating a configuration of a communication protocol for operating components so as to be linked to each other in order to distribute the electronic document under the electronic document distribution system according to an exemplary embodiment of the present invention.

Figs. 39 to 43 are views illustrating an error processing method under the electronic document distribution system according to an exemplary embodiment of the present invention.

Figs. 44 to 51 are views illustrating a linkage interface between a distribution messaging server and an

address directory server in the electronic document distribution system according to the exemplary embodiment of the present invention.

Figs. 52 to 63 are views illustrating a linkage interface between distribution messaging servers in the electronic document distribution system according to the exemplary embodiment of the present invention.

Figs. 64 to 78 are views illustrating a linkage interface between a distribution client and a distribution messaging server in the electronic document distribution system according to the exemplary embodiment of the present invention.

Figs. 79 to 81 are views illustrating a linkage interface between a distribution messaging server and a distribution relay server in the electronic document distribution system according to the exemplary embodiment of the present invention.

Fig. 82 is a view illustrating a process that authenticates the distribution messaging server system so as to be registered as a certified electronic mailing address according to another exemplary embodiment of the present invention.

Fig. 83 is a view illustrating a process that reports a spam message at an electronic document distribution hub when a transceiving entity servers as a receiver according

to another exemplary embodiment of the present invention.

Fig. 84 is a view illustrating a process that checks whether to refuse to receive a communication party in real time basis when a transceiving entity servers as a receiver according to another exemplary embodiment of the present invention.

Fig. 85 is a view illustrating a process that periodically checks whether to refuse to receive a communication party in real time basis when a transceiving entity servers as a receiver according to another exemplary embodiment of the present invention.

Figs. 86 to 100 are views illustrating a distribution messaging server system according to another exemplary embodiment of the present invention.

Figs. 101 to 105 are views illustrating a distribution protocol which is applied to the electronic document distribution system and method according to another exemplary embodiment of the present invention.

Figs. 106 and 107 are views illustrating an electronic document form register according to another exemplary embodiment of the present invention.

Fig. 108 is a view illustrating electronic document packaging which is applied to the electronic document distribution system and method according to another exemplary embodiment of the present invention.

Figs. 109 to 114 are views illustrating a distribution client application according to another exemplary embodiment of the present invention.

Fig. 115 is a view illustrating a system where the address directory server issues an electronic mailing address according to yet another exemplary embodiment of the present invention.

Fig. 116 is a view illustrating a process where the address directory server issues an electronic mailing address according to yet another exemplary embodiment of the present invention.

Figs. 117 and 118 are views illustrating an example of a process that searches address information through the address directory server according to yet another exemplary embodiment of the present invention.

Fig. 119A is a view illustrating a postal distribution system of Table 37, Fig. 119B is a view illustrating an e-mail distribution system of Table 37, Fig. 119C is a view illustrating an electronic document interchange (EDI) distribution system of Table 37, and Fig. 119D is a view illustrating a work related system distribution system of Table 37.

Fig. 120A is a view illustrating an automatic processing method of Table 38 and Fig. 120B is a view illustrating a semi-automatic processing method of Table 38.

Fig. 121A is a view illustrating a web method of Table 39 and Fig. 121B is a view illustrating an application method of Table 39.

[Best Mode]

Hereinafter, an electronic document distribution system and an electronic document distribution method according to an exemplary embodiment of the present invention will be described with reference to the accompanying drawings and Tables.

Fig. 1 illustrates a configuration example of an electronic document distribution system according to an exemplary embodiment of the present invention.

Referring to Fig. 1, an electronic document distribution system according to an exemplary embodiment of the present invention includes a transceiving entity 101 that distributes an electronic document through a distribution messaging server that transmits/receives a message based on an electronic mailing address and issues and manages a distribution certificate for the message transmission/reception, an electronic document distribution hub 102 that registers/manages the electronic mailing address of the transceiving entity 101, sets a distribution path of the electronic document between the transceiving entities 101, provides a standard form of the electronic document to the transceiving entity 101, and sends a

message by proxy for the transceiving entity and issues a distribution certificate when an error occurs in a process of the distribution of the electronic document between the transceiving entities 101, and a reliable third party storing institution (certified electronic document storage) 103 that receives and stores the distribution certificate.

The distribution messaging server of the transceiving entity 101 stores the transmitted/received message in a message box together with state information for every user and store the message transmission and reception record in a media which cannot be edit and deleted for a predetermined period and issues a distribution certificate for the transmission and reception of the message to request the third party storing institution to store the distribution certificate. The distribution messaging server is connected with the address directory server to allow the transceiving entity 101 to use functions of registering, searching, editing, and deleting the electronic mailing address. Further, the distribution messaging server transfers messages which have been stored for a predetermined time or longer to an external storage device so as to be stored.

The electronic mailing address includes a user identification mark of the transceiving entity 101 which is issued through the address directory server of the

electronic document distribution hub 102, an additional identification which is a unique value autonomously given by the transceiving entity 101 if necessary and a unique value in the transceiving entity 101, and a separation symbol which is located between the user identification mark and the additional identification mark.

The electronic document distribution hub 102 includes an electronic document form register. The electronic document form register performs the management including registration, deletion, and edition of information of the electronic document standard form. Further, the electronic document form register additionally classifies the electronic document standard form in accordance with a context and performs management including registration and edition of a context in which the electronic document standard form is used.

The electronic document distribution hub 102 includes a distribution relay server that sends a message by proxy and issues a distribution certificate when error occurs during the process of distributing the electronic document between the transceiving entities 101. When the distribution relay server is requested by the transceiving entity 101 to send the message, the distribution relay server issues a transmission certificate to the transceiving entity 101 that requests to send the message

after sending the message by proxy. If the requested message sending is failed, the distribution relay server sends an error message to the transceiving entity 101 that requests to send the message.

The electronic document distribution hub 102 includes an externally connected gateway server for connection with an external system. The externally connected gateway server includes a distribution messaging server that transmits/receives a message based on an electronic mailing address. The externally connected gateway server provides an transmission/reception electronic mailing address verifying/transforming function between the connected external system and the electronic document distribution system, a message verifying/transforming function between the connected external system and the electronic document distribution system, a verifying/transforming function of security which is applied to an electronic document between the connected external system and the electronic document distribution system, and a function that verifies and transforms a compatibility of the electronic document between the connected external system and the electronic document distribution system.

An electronic document distribution system with the above-described configuration and an electronic document distribution method using the same according to exemplary

embodiments of the present invention will be described in detail with reference to Figs. 1 to 118. In the detailed description of the present invention, reference numerals of Fig. 1 will be omitted.

[Structure of electronic document distribution system]

In order to guarantee reliability and stability in distribution of an electronic document, the electronic document distribution system according to the present invention distribution needs to satisfy the following requirements (1) to (7).

(1) A transceiving entity and a sender/receiver that participate in the distribution system need to transmit/receive an electronic document using a predetermined method and agree with a service level agreement (SLA) of a management institution or an electronic document provider.

(2) Identification of the transceiving entity and a certified sender/receiver that participates in the distribution system is allowed and denial of the electronic document distribution action needs to be prevented.

(3) A certified electronic address which is information for discriminating the transceiving entity and a certified sender/receiver in the distribution system

needs to be given in the unit of a corporate or an individual and registered and managed by a registered institution.

(4) When the electronic document is distributed in the distribution system, the distribution certificate needs to be generated and sent and stored into a transmitting entity which participates in the distribution action and a third party storing institution.

(5) Even though all electronic document distribution actions are performed based on a P2P (peer to peer) communication, a system that supports the distribution when the communication is failed due to various environmental factors needs to be provided.

(6) Not only the exchange of the electronic documents between the parties in the distribution system, but also various additional services such as an electronic document reading service need to be supported.

(7) A gateway that supports to connect with an external system other than the distribution system needs to be provided.

The electronic document distribution system according to the present invention is performed based on a certified electronic mailing address and P2P communication that transmits/receives the electronic document between the transceiving entities having a distribution messaging

server.

A structure of the electronic document distribution system according to the present invention is illustrated in Fig. 1 and components in the system will be described in the following Tables 1 and 2. Further, a main process will be described in the following Table 3.

[Table 1]

No.	Name of entity	Description
1	Transceiving entity	A corporate or an institution that includes a system required to distribute an electronic document such as a distribution messaging server to participate in the distribution of the electronic document in a distribution system in accordance with a predetermined method. This is a general concept including an electronic document provider.
2	Electronic document provider	A third party institution which is authenticated in order to provide an electronic document distribution service to a sender/receiver that does not have a system required to distribute an electronic document such as a distribution messaging server

3	Electronic document distribution hub	Which commonly refers to a system that supports the distribution of the electronic document between the transceiver entities and performs the address management, a path setting, an error or security processing, and connection to the outside.
4	Sender/receiver	Which is a basic unit of the distribution of the electronic document and is a general concept including an end user who actually transmits and receives an electronic document. General concept including a certified sender/receiver.
5	Certified sender/receiver	A sender/receiver who becomes a member of the electronic document provider and gets a certified electronic mailing address to use the electronic document distribution service.
6	Third party storing institution	A corporate body which is designated by a secretary of The Ministry of Knowledge Economy to store or verify an electronic document on behalf of the other party or performs a job related with the electronic document

[Table 2]

No.	Name of	Description

	entity	
1	Distribution messaging server	A messaging system that distributes the electronic document by proxy for a sender/receiver in a predetermined method and is provided in a transceiving entity or an electronic document provider.
2	Distribution client	Which commonly refers to an application which is used by the sender/receiver to distribute the electronic document and provides a function of editing a message and transceiving a message through a distribution messaging server(for example, outlook or a web mail client)
3	Address directory server	A system that registers and manages a certified electronic mailing address of a transceiving entity and a sender/receiver who participate in the certified electronic mailing address based electronic document distribution system and provides address information required for transceiving.
4	Electronic document form register	A system that registers, manages, and provides a standard form of an electronic document to be structuralized such as an order sheet, an invoice, or a tax voucher so that the

		transceiving entity may openly use the standard form.
5	Distribution relay server	A system that transmits a message by proxy instead of the transceiving entity when an error occurs during the process of distributing the electronic document between the transceiving entities
6	Externally connected gateway server	A system that serves as a reliable path to connect the distribution system to the external system
7	NTP server	Which is a Network Time Protocol server that serves to send a time to a system that requests a time in the distribution system
8	Registration agency system	A system that allows a registration agent to apply and register a certified electronic mailing address

[Table 3]

No.	Name of process	Description
1	Transceiving of Message	An action that transmits and receives a message (including an electronic document) between the transceiving entities and

		transmits and receives a message through a distribution messaging server in the transceiving entity and a distribution certificate including distribution certified information
2	Acquiring of Physical address	An action that inquires an address directory server in an electronic document distribution hub in order to obtain a physical address corresponding to a certified electronic mailing address of a receiver and receives a physical address prior to sending the electronic document
3	Supporting of distribution relay	A process that is performed by a distribution relay server to send an electronic document by proxy when the distribution of the electronic document is not good between the transceiving entities due to various errors such as a network error or a receiver system error
4	Storing of distribution certificate	An action that stores the distribution certificate received by a transmitting entity in a predetermined determined third party storing institution (storing a message if necessary)

5	Management such as registration of certified electronic mailing address	A process that registers and changes the certified electronic mailing address of the transceiving entity or a certified sender/receiver
6	Applying of electronic document form	A process that uses an electronic document registered in an electronic document form register by a distribution client
7	Processing of spam message	A process that reports and processes an improper behavior of a specific sender/receiver in the distribution system such as spam mailing
8	Processing of error	An action that analyzes causes of various failures of the electronic document distribution in the distribution system and copes with and supplements the failures

[Component of electronic document distribution system]

(1) Distribution messaging server

The distribution messaging server is a messaging system provided in the transceiving entity and plays a core role in the electronic document distribution. The distribution messaging server needs to physically have one electronic mailing address (IP address), but issue and manage a plurality of user accounts for a lower-level user. In order to manage the user accounts, the distribution messaging server needs to manage a message box for every user account. The distribution messaging server has a responsibility to safely and reliably manage the accounts and the message boxes of the users.

A functional concept of the distribution messaging server is as illustrated in Fig. 2 and the functions thereof will be described in the following Table 4.

[Table 4]

No.	Name of function	Description
1	Transmitting and receiving of message	- transmits and receives a message in accordance with a distribution protocol
2	Managing of message box	- stores a transmitted/received message in a message box in accordance with a user account

	for every user	or an internal identifier - manages the transmitted document stored in the message box as status information in the following six steps 1) in the process of transmitting: a state when no reply is received from a receiver after sending a document 2) completely transmit: a state when a "reception certificate" has been received from the distribution messaging server of the receiver 3) commissioned transmission: a state when the transmission is commissioned to the distribution relay server after the failure of the transmission 4) transmission failure: when a SOAP Fault message is returned due to an error occurring in the distribution messaging server of the receiver or a network error occurs in the transceiving process. 5) reading failure: when an error occurs while a receiver reads the message 6) completely read: a state when a "read certificate" has been received from the

		distribution messaging server of the receiver - manages received document stored in the message box as state information in the following four steps 1) verification error: an error occurs while verifying a basic structure of the received message 2) before the reception confirmation: before a receiver of the document reads a list of received documents 3) reception confirmation: a receiver of the document reads the list of the received documents 4) reading confirmation: a receiver of the document reads the details of the received documents - if the receiver requests the deletion, the corresponding received document needs to be physically deleted. - the transmission message, reception certificate, and reading certificate in the message box need to have related information so as to be related with each other.

3	Managing of transmission /reception record	- distribution messaging server needs to store the transmission/reception record in a medium, which is not allowed to edit and delete the transmission/reception record for a predetermined period of time. - transmission/reception record information to be stored 1) transmission record: message id, connected message id, transmitter, receiver, transmission time, hash value for the transmitted document 2) reception record : transmitter, receiver (including a user account), reception time, hash value for the received document
4	Supplementing of message	- needs to perform message security functions (digital signature, signature verification, encryption/decoding) which are suggested by the distribution protocol
5	Message packaging and verification processing	- a document to be transmitted needs to be packaged in a message structure defined by the distribution protocol before transmitting the document. - a received document needs to be verified and parsed by a message structure defined by the

		distribution protocol after receiving the document and required information needs to be extracted.
6	Issuing and managing of distribution certificate	- the distribution messaging server should issue a distribution certificate in order to evidence the transmission/reception of the document and manage the distribution certificate. - request the third party storing institution to store the distribution certificate as soon as the issued distribution certificate is received. - record information of distribution certificate: distribution certificate id, issuance time, related message id, an original of the distribution certificate (optional), or registration certificate of the third party storing institution received after storing the distribution certificate in the third party storing institution - see a technical standard of "electronic document distribution certificate"

7	Connecting with address directory server	- needs to register address information supplied from the address directory server and manage the address information in accordance with a searching process - needs to have a client function which can call a service provided by the address directory server - needs to provide a service client function that remotely calls a function of registering, editing, deleting the address information provided by the address directory server
8	Connecting with third party storing institution	- the distribution messaging server sends a storing request message to the distribution messaging server which is provided outside the third party storing institution in order to request to store the distribution certificate. - distribution messaging server of the third party storing institution calls a storing request client to the third party storing institution in order to store the distribution certificate in the third party storing institution - calls the storing request client at the time when the distribution messaging server of the

		third party storing institution directly generates the distribution certificate - the storing request client requests the third party storing institution to store the distribution certificate in accordance with a connection interface standard of the third party storing institution.
9	Internal system connection interface	- needs to provide functions which are directly connected to a corporate internal system if the distribution messaging server is the corporate internal system rather than the distribution client
10	Managing of distribution client	- manages a user account related with the distribution client or manages a user authentication or environmental information
11	Managing of additional function	- records and statistic information related with the message distribution - system management: system monitoring - environmental information management: needs to provide environmental information for entire distribution messaging server and environment setting function for individual users - manages a document form
12	Storing and	- functions as a system that transfers messages

	managing of message	which have been stored for one year or longer to an external storage device in order to automatically store the messages

In addition to the functions described in Table 4, the following (1) to (4) principles need to be observed in the server system management in order to improve the reliability of the distribution messaging server.

(1) A system manager cannot see or voluntarily delete a message box of an individual.

(2) The record information related to the server system management cannot be voluntarily deleted and stored in a unchangeable medium for 10 years or longer.

(3) The system manager cannot voluntarily change a basic function of an authenticated distribution messaging server solution.

(4) An operation guideline related with the system management needs to be created and the management needs to be performed in accordance with the guideline.

(2) Distribution client

The distribution client is an application that provides an UI (user interface) such as transmission and reception of a message, read and management of a received electronic document on behalf of the senders/receivers who

participate in the distribution system. The distribution client cannot independently transmit/receive the document and needs to be inevitably connected with the distribution messaging server.

The distribution client requests to send a message through the distribution messaging server or inquires the message received through the distribution messaging server. The distribution messaging server manages the message box for every user account. The distribution client needs to access to only a message which is stored in its own account among the received documents by checking the user account information.

The distribution client may be implemented as a C/S type application or a web type screen in accordance with a request of the transceiving entity.

A functional concept of the distribution client is as illustrated in Fig. 3 and the functions thereof will be described in the following Table 5.

[Table 5]

No.	Name of function	Description

1	User authentication	- the distribution client needs to receive login session information from the distribution messaging server after checking a user account. - a user authentication method of the distribution client includes 1) user authentication based on a certificate and 2) user authentication based on ID/PW. - when the authentication is operated based on ID/PW, a security policy for the password needs to be enforced. For example, changing a password in the unit of a week, combination of difficult character/number, prohibition of changing IP address
2	Generating of message	- the distribution client needs to provide a user interface that is capable of creating a new message - items other than a value which is set in advance by the environmental information among basic information required to send a message so as to be input - a main text of the message is not a critical item and the main text can be selectively and additionally created.

3	Inquiring of message list and reading of detailed contents	- the distribution client needs to provide a function of inquiring a list of the messages corresponding to the user account. - needs to provide a function of reading detail information of the message including an attached document
4	Managing of message folder	- the distribution client needs to notify a status of the transmitted/received message based on the message box of the distribution messaging server to the user in accordance with the status information provided by the distribution messaging server. - a function that provides temporary storage box or a deleted message box or a function of allowing a user to directly define and manage a message folder is optionally provided.
5	Managing of basic information and environmental information	- the distribution client needs to provide a function of managing necessary environmental information related with the message transmission/reception. - the distribution client needs to be synchronized with the environmental information which is managed by the distribution messaging server. Additionally, the

		distribution client provides a function of setting and managing individual environmental information of the distribution messaging server. - management of additional information on a system environment of the distribution client is defined in accordance with the development range of the application to be provided.
6	Creating of document	- a function of calling a registered electronic document form to create an electronic document
7	Request to transmit message and get received message	- the distribution client performs a message transmitting function and a received message importing function through a connected interface with the distribution messaging server based on user account information.
8	Security processing of message	- need to perform a security processing for a message such as digital signature or encryption/decoding
9	Registering and searching of document form	- a function of registering an electronic document form disposed in the electronic document form register or the outside as a distribution client - a function of searching an electronic document form in the distribution client

10	Managing of address book	- a function of managing a frequently used certified electronic mailing address - selectively perform a function of automatically registering and managing the certified electronic mailing address through a received message
11	Connecting with in-corporate system	- a connection function such as a function of registering the electronic document in the message in a group ware or job related system in the corporate
12	Storing and managing of message	- a function of transferring a message whose politically set storage time limit has been passed to an external storage device in order to store the message - in this case, related information such as distribution certificate and log information needs to be comprehensively stored in order to understand a context related with the message.
13	Reporting of spam	- a function of reporting a message which is received with an improper purpose such as spam
14	Supporting to read document	- selective function of sending only an authority to store and read the electronic document in a system of the transmitting entity or the third party storing institution

		- the receiver has only a reading authority and cannot download the electronic document but can only read the electronic document

(3) Address directory server

The address directory server is a system that manages the transmitting/receiving entity and address information of certified sender/receiver and provides a physical address.

The address directory server provides the basic functions such as the following functions (1) and (2):

(1) managing and providing a physical address (IP address) of the distribution messaging server of a receiving entity

(2) managing function such as registering and editing information of certified electronic address

Additionally, the address directory server basically has a function of managing white-list information and accepts a report on a spam message from the user and manages blacklist information based the report.

The address directory server provides information related to the certified electronic address to the transceiving entity or the certified sender/receiver through a web portal screen and the distribution messaging server and the related applications may use the services

provided by the address directory server through the connected interface.

A functional concept of the address directory server is as illustrated in Fig. 4 and the functions thereof will be described in the following Table 6.

[Table 6]

No.	Name of function	Description
1	Managing of certified electronic mailing address	- managing such as new registration and change of certified electronic mailing address of the transceiving entity and certified sender/receiver - read information of transceiving entity having certified electronic mailing address and record information
2	Managing of spam report	- a function of accepting a report of a spam received from the distribution client and notifying the result
3	Managing of white/black list	- creating and managing/storing white-list which is a list of certified electronic mailing addresses - a function of accepting and processing a request to search the whitelist

		- management such as creating and editing a black list for the certified electronic mailing address which is improperly used such as a spam - a function of searching the blacklist
4	Searching address information and communicating physical address	- a function of accepting and returning a physical address request of the certified electronic mailing address requested by the distribution messaging server - a function of searching record information related therewith
5	Managing of web portal	- provides a user interface related with the address management - provides a system manager interface related with the address management - manages system environmental information of the address directory server - manages various statistic information related with the address

(4) Electronic document form register

The electronic document form register is a system that is provided by the electronic document distribution

hub so as to be automatically processed or utilize an e-Form type electronic document using a predetermined standard electronic document between the transceiver entities.

The electronic document form register provides a server engine that manages the electronic document form, an interface that provides a function that allows the distribution client to search and download the electronic document form, and a web portal interface.

A functional concept of the electronic document form register is as illustrated in Fig. 5 and the functions thereof will be described in the following Table 7.

[Table 7]

No.	Name of function	Description
1	Managing of electronic document form	- manage to register and delete the electronic document form and edit information - notifies details related with the registration/deletion of the electronic document
2	Managing to search and receive	- provide a function of searching an electronic document form - receive or download the searched electronic

	electronic document	document form
3	Electronic document form connection interface	- provide a function of searching and downloading the electronic document while being directly connected with the distribution client
4	Managing of context	- additionally classify the electronic document forms in accordance with the context because different forms may be used in accordance with the context of the country or the industry even though the name of the corresponding electronic document form is same - manages to register and edit the context of a country, a region, an industry, a corporate, or a process in which the electronic document form may be used
5	Function of examining and evaluating electronic document form	- standby after the user submits the electronic document form for registration - a process that formally registers or returns the electronic document form after evaluation of an evaluator * additionally notify an electronic document form and a submitting method

6	Managing of web portal	- provide a user interface related with the electronic document management - provide a system manager interface related with the electronic document management - manage the system environmental information of an electronic document form register server - manage various statistic information of the electronic document form register

(5) Distribution relay server

The distribution relay server is a system which is provided in the electronic document distribution hub to send a message by proxy for the transmitting entity when an error occurs during the electronic document distribution process between the transceiving entities in the distribution system.

The distribution relay server has a function therein as a distribution messaging server so as to provide a basic electronic document transceiving service. Further, the distribution relay server provides the distribution messaging server with a unique service of the distribution relay server such as relay request accepting and error message transmission through a connection interface in the case of final failure .

A functional concept of the distribution relay server

is as illustrated in Fig. 6 and the functions thereof will be described in the following Table 8.

[Table 8]

No.	Name of function	Description
1	Message routing information processing	A function of setting a route for the distribution messaging server in the transceiving entity
2	Reprocessing operation in the case of transmission error	A function of resending a message if an error occurs when the message is sent to the receiving entity
3	Issuing of transmission certificate	A function of issuing the transmission certificate to a transmitting entity that requests to send a message
4	Transmitting of error message at the time of transmission failure	A function of sending an error message to the transmitting entity when the requested message sending is failed

5	Requesting to relay electronic document	A function of receiving a request to relay a message in a state connected with the distribution messaging server
6	Managing of records/statistic information	A function of storing and processing record or statistic information related with the message distribution relay
7	Monitoring of relay situation	A function of providing a distribution relay situation for the transceiving entity and monitoring a relay situation by a system manager

(6) Externally connected gateway server

The externally connected gateway server is a system which serves as a reliable channel in order to connect an external system which is already operated or hardly included in the distribution system with the distribution system.

In the case of a public sector, civil affair documents are electronically distributed through public information sharing center or electronic document distribution supporting center. As a channel to connect with the systems, the externally connected gateway server

may be used. The externally connected gateway server may serve as a channel to connect with other external systems in addition to the public sector.

A functional concept of the externally connected gateway server is as illustrated in Fig. 7 and the functions thereof will be described in the following Table 9.

[Table 9]

No.	Name of function	Description
1	Distribution messaging server module	Use a part of functions of the distribution messaging server
2	Verification/conversion module	A verification/transformation module corresponding to individual connected external systems
3	Electronic mailing address verification/transformation	A function of verifying and transforming a transmitting/receiving address between the distribution system and the externally connected system
4	Message package	A function of verifying and transforming a message package between the distribution

	verification/transformation	system and the externally connected system
5	Electronic document security verification/transformation	A function of verifying and transforming a security applied to the electronic document between the distribution system and the externally connected system
6	Document compatibility verification/transformation	A function of verifying a compatibility of the electronic document between the distribution system and the externally connected system and transforming the electronic document therebetween
7	System management	System management of externally connected gateway server
8	Inquiring of statistic information	A function of inquiring statistic information related with the usage of the externally connected gateway

(7) Certified electronic mailing address

The transceiving entity and a certified sender/receiver that participate in the distribution system need to receive a unique certified electronic mailing address.

The certified electronic mailing address is

configured by combination of sharp [#], numbers [0 to 9], hyphen [-], and period [.].

A configuration system of the certified electronic mailing address will be described in the following Table 10.

[Table 10]

Classification	certified electronic mailing address		Contents
	identifier	User identification	
Personal purpose	#	000-0000-0000	Numbers which is randomly applied to an applicant to be combined by 13 digits symbols formed of numbers and hyphens
Other purpose		000-00-00000	A business registration number or a unique registration number which is combined by 12 digits symbols formed of numbers and hyphens

The principles related with the configuration system of the certified electronic mailing address are as the following (1) to (3):

(1) As a front part of "#", an additional user identification configured by the combination of characters

[A-Z][a-z], Korean alphabet [completed Korean alphabet, 2,350 letters], numbers [0-9], hyphen [-], and period [.] may be selectively used for the convenience of the user. In this case, the additional user identification may be managed by the electronic document distribution messaging server.

(2) The additional user identification of the certified electronic mailing address should not start or end with the hyphen or the period and the length thereof is set to be 30 byte or shorter.

(3) As the additional user identification of the certified electronic mailing address, combination of characters and numbers which may destroy social customs or public morals or the other restricted symbols determined by a head of a management agency may not be used.

A correlation relationship between the certified electronic mailing address and an IP address which is an actual physical address (actual physical address of the distribution message server) is managed only by the address directory server. The certified electronic mailing address and the actual physical address of the distribution message server have the relationship of 1:1 or N:1. Therefore, one certified electronic mailing address does not have plural physical addresses.

A corporate/organization/personal next to "#" should have a legal responsibility of receiving the information (document) of the certified electronic mailing address. Further, the distribution according to the additional user identification is divided for the convenience of the corporate/organization/personal. Therefore, the transceiving entity should have the responsibility of the distribution according to the additional user identification. In this case, the transceiving entity needs to prepare a policy and management know-how of the user authentication corresponding to the additional user identification and thoroughly manage the user authentication in accordance with the know-how. Further, the transceiving entity needs to include the contents of the certified electronic mailing address with an internal identifier when the transceiving entity enters into an agreement with the management agency about the SLA before participating in the distribution system.

An effective range of the certified electronic mailing address in the distribution system will be illustrated in Fig. 8.

The additional user identification needs to be a unique value in the transceiving entity. The individual transceiving entity is basically responsible for applying the additional user identification. Further, the

transceiving entity is responsible for distribution of the electronic document in accordance with the additional user identification. Therefore, if a problem occurs, the transceiving entity needs to solve the problem. The additional user identification is not included in the effective range of the distribution system, but may be defined by the SLA with the management agency.

The additional user identification is used to distribute the electronic document for the convenience of the operation of the corporation and is used only for internal information of the corporation without being registered in the address directory server.

As other example of the certified electronic mailing address as described above, the following structure may be allowed.

Certified electronic mailing address = ID + separation symbol + registrant

Here, the "ID" is configured by the combination of English (or Korean alphabet or numbers), hyphen [-], and period [.], the "separation symbol" is #, and the "registrant" is configured by the combination of English (or Korean alphabet or numbers) and period [.].

"swconvergence#mke.go.kr" is an example of the certified electronic mailing address. In the above example, "swconvergence" indicates a name of the department of a

government agency, "mke" indicates the government agency, "go" indicates an attribute, and "kr" indicates a country.

An application/issuance and operation system of the certified electronic mailing address is illustrated in Fig. 9 and configuration related thereto will be described in the following Table 11.

[Table 11]

Configuration	**Role**
Management agency (comprehensively manage certified electronic mailing address)	- the management agency manages the information of the certified electronic mailing address in a restricted sense as a supreme main agent of management of the certified electronic mailing address - manage to issue and change a unique certified electronic mailing address ID for the transceiving entity and the certified sender/receiver
Registration agency	- an agency that is commissioned by a management institution to apply and examine the certified electronic mailing address
transceiving entity	- most basic unit of the certified electronic mailing address (registration address) in a restricted sense - in the case of corporate/organization, issues

	and manages a user account or additional user identification for a plurality of users as a lower level of one certified electronic mailing address and guarantees the exclusiveness
(certified or internal) sender/receiver	- an actual user who participates in the electronic document distribution - the certified sender/receiver has the certified electronic mailing address with the user account which is opened through the electronic document provider and is a transceiving unit having a legal responsibility - an internal sender/receiver is a transceiving unit which is managed by the additional user identification in the transceiving entity having a legal responsibility for the transmission and reception but does not have a legal responsibility and is not registered in the electronic mailing address directory server

(8) Electronic document information package

An electronic document information package is required to support to automatically register or process an electronic document in a corporate internal system such as a group ware by clearly describing metadata for the

electronic document included in the message.

The electronic document information package is not an essential element for the message distribution. Therefore, the electronic document information package may be selectively used for a necessary task. However, if the electronic document information package is used, the following requirements (1) and (2) need to be observed.

(1) The electronic document information package needs to be sent as a separate file format from the electronic document included in the message.

(2) The electronic document information package needs to be provided as an XML file format.

The metadata of the electronic document information package will be described in the following Table 12.

[Table 12]

No.	Meta information	Required/optional	Description
1	Name of electronic document	required	File name of the electronic document included in the message
2	Electronic document	required	Unique identifier that identifies the electronic document

	identifier		
3	Classification of electronic document type	required	Identifier distinguishing whether the corresponding electronic document is an electronic document which is registered in the electronic document form register or an electronic document which is used in a corporate/organization, or its own electronic document 0: an electronic document which is registered in the electronic document form register 1 :an electronic document which is commonly used in a corporate/organization 2: an electronic document which is autonomously used
4	Identifier of electronic document type	optional	Identifier that identifies the type of the document when the classification of the electronic document type is 0 or 1
5	Signature value of	optional	Digital signature value for the electronic document

	electronic document		
6	Other information	optional	Other information related with the electronic document

[Message security]

One of the most important parts in the distribution system is security of the sending message which requires (1) prevention of denial of the transmission/reception, (2) guarantee of integrity for the sending message, (3) authentication for a sending party, and (4) guarantee of confidentiality for the sending message. Among these, (1) to (3) are supported by the digital signature of the sender for the sending message and (4) is provided by encrypting the transmission message.

A security which is applied when the electronic document is distributed between the distribution messaging servers, which is the basic of the distribution system, supports the message digital signature and the encryption as illustrated in Fig. 10. The network encryption needs to be applied to each section in order to secure the sending.

The digital signature for the contents is a unique part for every application. The description thereof will be omitted. In this invention, basically, the encryption is performed with a public key of a receiver. If there is

no authentication certificate of the receiver, or the receiver is an internal receiver, only the encryption of the receiving entity may be selected. Further, during the message sending, the message is sent to the distribution messaging server together with the authentication information on the message. In this case, the distribution messaging server mainly uses authenticate information to authenticate the client. Further, the distribution messaging server adopts various authenticating methods such as IP/PW based authentication, token information based authentication by SSO (single sign on) in addition to the authentication certificate based digital signature in order to authenticate the distribution client.

Hereinafter, a digital signature method will be described in detail.

When the distribution messaging server is connected with the other system (other distribution messaging server, the address directory server, or the distribution relay server), the digital signature needs to be performed based on its own certificate. All distribution messages for connecting the components in the distribution system are basically digitally signed. However, the digital signature between the distribution client and the distribution messaging server is optional and the digital signature is applied to only a user authentication method based on the

certificate. In this case, the distribution messaging server is responsible for the user authentication, the integrity, and the prevention of the denial of the transmission/reception for the distribution message with the distribution client.

Hereinafter, the encryption method will be described in detail.

An attached document in the distribution system may be sent after the sender selects the encryption in order to secure the document, which is performed for the confidentiality of the document but is different from the network encryption. Therefore, after applying the network encryption, the distribution document may be additionally encrypted.

Sections to be encrypted may be (1) from the distribution client of the transmitter to the distribution messaging server of the receiver or (2) from the distribution client of the transmitter to the distribution client of the receiver as illustrated in Fig. 10. If the receiver is a certified sender/receiver and the certificate is registered in the address directory server, the encryption is performed in the section (2) from the transmitter to the receiver. Otherwise, the encryption is performed in the section (1) from the transmitter to the receiving entity.

When the attached document is encrypted, the transmitter needs to encrypt the document so as to decode the document in three steps of the distribution messaging server of the transmitter, the distribution messaging server of the receiver, and the distribution client of the receiver if the encryption is maintained in the section (1) from the transmitter to the receiving entity. If the encryption is maintained in the section (2) from the transmitter to the receiving entity, the transmitter needs to encrypt the document so as to decode the distribution messaging server of the transmitter and the distribution messaging server of the receiver.

If the attached electronic document is encrypted, the distribution messaging servers of the transmitting entity and the receiving entity store the electronic document in an encrypted state in order to manage the record. Therefore, if the sender/receiver wants to verify the distribution certificate based on the decoded document, the electronic document is decoded to verify the distribution certificate. For this reason, the distribution messaging server needs to continuously manage a private key of a revocated certificate and a password for accessing to the private key.

Hereinafter, an outline of the encryption in the encryption method will be described.

If the transmitter determines that the confidentiality of the message which is distributing in the distribution is assured, the following encrypting process needs to be observed.

As a ciphertext, an Enveloped-data content type which is represented by a ContentInfor structure which is suggested by IETF RFC 3852 "CMS(Cryptographic Message Syntax)" which are used in and outside the country as a standard is used.

※RFC 3852 CMS

1) IETF is a main agent which defines a standard of an internet operation protocol such as TCP/IP. IETF is supervised by IAB (Internet Architecture Board, a surveillance body of the internet society for technical improvement of Internet). The members of IETF are selected from individuals or members of an organization of the Internet Society. The standards created in IETF are represented in a RFC type and many PKI based solutions (various authenticating systems, a time stamp, or a size of a third party storing institution) in and outside the country are made based on the RFC standard document.

2) The CMS(Cryptographic Message Syntax) is created based on "PKCS#7 v1.5" first created by RSA corporation. RFC2630 is created with the RFC standard standardized by IETF. In the first PKCS#7, only key transfer (a symmetric

key used for encryption is delivered to the other party using the RSA) method is provided. In contrast, in the CMS of RFC2630, key agreement (a method that delivers the key using a DH algorithm) is added.

3) Thereafter, RFC3369 in which the algorithm part is separated and various key management methods are applied is established in 2002. However, various problems of RFC3369 are reported and thus a finally corrected version is RFC3852 which is applied in this invention.

As an additional application standard, an algorithm which is used in Content Encryption (an electronic tax invoice package which will be actually transmitted) at the time of creating the ciphertext or a parameter corresponding to the algorithm follow IETF RFC 3370 "Cryptographic Message Syntax(CMS) Algorithm" and IETF RFC 4010 "Use of the SEED Encryption Algorithm in Cryptographic Message Syntax(CMS)".

Hereinafter, encryption target data in the encryption method will be described.

Referring to Fig. 11, the encryption target of a message to be delivered are the following (1) and (2).

(1) Distribution information which is input in a second MIME

(2) A <text> region of the message body in which an actual content of a main text is input and an attached

document

The Text in the message body and the attached document are separately encrypted and included in a corresponding position.

A first encryption target is the content of the main text which will be delivered to the receiver and has a value in the <Text> section in the XML body.

Next, a configuring method of the target data will be described. The data follows ASN.1 Basic Encoding Rules (BER) and observes Distinguished Encoding Rules (DER).

[Table 13]

MainText ::= OCTET STRING

MainText of Table 13 is the content of a text type main text.

Second or later encryption target data is attached document which is attached to a third MIME or later. The second or later encryption target data is separately encrypted in the unit of the attached document and then input in the corresponding MIME.

Next, a configuring method of target data will be described. The data follows ASN.1 Basic Encoding Rules (BER) and observes Distinguished Encoding Rules (DER), which is similar to the first encryption method.

[Table 14]

```
AttachedDoc ::= URL
```

AttachedDoc in Table 14 is a binary type attached document.

Hereinafter, an encryption process and structure in the encryption method will be described.

The following Table 15 describes a configuration of EnvelopedData of RFC 3852.

[Table 15]

```
EnvelopedData ::= SEQUENCE {
version CMSversion,
originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
recipientInfos RecipientInfos,
encryptedContentInfo EncryptedContentInfo,
unprotectedAttrs [1] IMPLICIT UnprotectedAttributes
OPTIONAL }
```

In Table 15, version follows a configuration of a syntax version number of RFC 3852.

OriginatorInfo is not used because a key management algorithm is not used and CRL does not need to be sent

(defined in RFC 3852)

Since a currently available algorithm of an encryption certificate is RSA, a key (content-encryption key) which is decoded by the receiver through KeyTransRecipientInfo of RecipientInfos is delivered.

In encryptedContentInfo, MainText or AttachedDoc which is encrypted based on an algorithm of Algorithm Identifier defined therein is input.

Since unprotectedAttrs is not separately used in this version, a value may be inserted for the purpose of the management at the transmitter side but the receiver does not need to decode or use this value.

Main parts for creating EnvelopedData of RFC3852 will be described in the following (1) and (2).

(1) Creating of EncryptedContentInfo

[Table 16]

```
EncryptedContentInfo ::= SEQUENCE {
contentType ContentType,
contentEncryptionAlgorithm
ContentEncryptionAlgorithmIdentifier,
encryptedContent [0] IMPLICIT EncryptedContent OPTIONAL }
```

- id-data (an identifier -OID - information indicating which information is encrypted data) is input as

ContentType.

- Symmetric key algorithm information which is actually used for encryption is input as contentEncryptionAlgorithm.

- An input of the encryptedContent is OCTET STRING (Binary value) obtained by encrypting a DER encoded value of the TaxInvoicePackage defined above in accordance with an algorithm method defined in contentEncryptionAlgorithm.

(2) Creating of RecepientInfo

[Table 17]

```
RecipientInfos ::= SET SIZE (1..MAX) OF RecipientInfo
RecipientInfo ::= CHOICE {
ktri KeyTransRecipientInfo,
kari [1] KeyAgreeRecipientInfo,
kekri [2] KEKRecipientInfo,
pwri [3] PasswordRecipientInfo,
ori [4] OtherRecipientInfo }
```

-The encryption is required for the transmitting entity and the receiving entity. The receiver performs the encryption only when the receiver has a certificate. Therefore, actual RecipientInfos has at least two or at most 3 lower level RecipientInfos.

- Since the encryption certificate uses RSA, the

encryption certificate is configured only by ktri (a method that sends a symmetric key that uses RSA public key of the other party to encrypt data).

Hereinafter, OID definition for message in the encryption method will be described.

Object Identifier for configuring a message is as following (1) and (2).

(1) EnvelopedData Type: a format that actually transmits data in RFC3852 CMS is a structure called as ContentInfo and EnvelopedData Type is information input in ContentType so as to check which data is in the structure.

[Table 18]

- id-envelopedData - OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 3 }

(2) ContentType of EncryptedContentInfo: information which is input in ContentType so as to check which data is in EncryptedContentInfo structure in which encrypted data is input.

[Table 19]

```
- id-data
- OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs7(7) 1 }
```

Hereinafter, the encryption algorithm in the encryption method will be described.

The algorithm used for encryption is mainly divided into two.

(1) a symmetric key algorithm used to directly encrypt target data

(2) a public key algorithm which transmits the symmetric key so as to be decoded only by the receiver

Since a certificate to be used is an encryption certificate of a GPKI or NPKI system, the public key algorithm uses a RSM based algorithm. Further, for the symmetric key algorithm, one of the following three symmetric key encryption algorithms (SEED, ARIA, and 3DES) should be selected.

The transmitter may support only one of the symmetric key encryption algorithms, but the receiver needs to support all of three algorhtims.

(1) asymmetric key algorithm (RSA): which is randomly generated to be used to safely encrypt symmetric key information in which data is encrypted to transmit to the other party and examples thereof will be described in the

following Table 20.

[Table 20]

RSA Encryption - rsaEncryption - OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }

(2) symmetric key algorithm (SEED, ARIA, 3DES): which is randomly generated to be used to actually encrypt transmitting data and examples thereof will be described in the following Table 21.

[Table 21]

Triple-DES CBC - des-ede3-cbc - OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) encryptionAlgorithm(3) 7 } - Parameter of algorithm is surely presented and parameters must have CBCParameter. or SEED CBC - id-seedCBC - OBJECT IDENTIFIER ::= { iso(1) member-body(2) korea(410)

kisa(200004) algorithm(1) seedCBC(4)

- Parameter of algorithm is surely presented and parameters must have SeedCBCParameter.

or

ARIA CBC

- id-aria128-cbc OBJECT IDENTIFIER ::=
{ iso(1) member-body(2) korea(410) gcma(100001) gpki-alg(1)
aria128-cbc(20) }
- id-aria192-cbc OBJECT IDENTIFIER ::=
{ iso(1) member-body(2) korea(410) gcma(100001) gpki-alg(1)
aria192-cbc(21) }
- id-aria256-cbc OBJECT IDENTIFIER ::=
{ iso(1) member-body(2) korea(410) gcma(100001) gpki-alg(1)
aria256-cbc(22) }

Parameter of algorithm is surely presented and parameters must have ARIACBCParameter.

ARIACBCParameter::= ARIAIV -- Initialization Vector

ARIAIV ::= OCTET STRING(SIZE(16))

Hereinafter, acquisition and verification of encryption certificate in the encryption method will be described.

In order to create a ciphertext, a certificate of a receiver side that decodes actual data needs to be acquired. In order to acquire the certificate, the transmitter needs to be connected to the address directory server so as to acquire a certificate for a receiver (or receiving entity). In this case, depending on whether the acquired certificate is a certificate of the receiving entity or a certificate of a certified receiver, a section in which the confidentiality is maintained is varied.

If the transmitter selects the encryption for the transmission message, the transmitter performs the encryption based on the acquired receiver (or receiving entity) certificate and transmits a message to the receiver. Even when an error occurs during the message transmission so that the distribution relay hub is requested to transmit the message, the message is transmitted without changing the encrypted contents.

Hereinafter, a configuration of EnvelopedData in the encryption method will be described.

Fig. 12 illustrates an encrypted body which will be actually transmitted to the receiver and thus a connection relationshpe between actual values may be understood more clearly.

- ContentInfo: which is represented in RFC 3852 and is a container in which SignedData, EnvelopedData,

EncryptedData of component data of RFC 3852 are input. contentType of the structure indicates which type of information is content. In this invention, an identifier (Object Identifier) which is called as id-envelopedData needs to be inserted.

- EnvelopedData: A structure for delivering encryption information (see the above description)

- EncryptedContentInfo: A structure that stores encrypted information. contentType of the structure indicates which type of information is encryptedContent. In this invention, an identifier (Object Identifier) which is called as id-data needs to be inserted. In contentEncryptionAlgorithm, an identifier (OID) for one of SEED, ARIA, and 3DES needs to be inserted. Further, a randomly created secrete key is used to input data encrypted by the algorithm in encryptedContent as OCTET STRING (binary data).

- RecipientInfo: A structure that allows a receiver to select which method is used to decode. In this invention, KeyTransRecipientInfo needs to be used.

- KeyTransRecipientInfo: a structure which is used to encrypt and deliver a random secrete key obtained by encrypting the above-mentioned encryptedContent using a public key of the receiver so as to allow the receiver to

decode. The encrypted secrete key is input in encryptedKey, RecipientIdentifier which is information indicating whose public key is used and KeyEncryptionAlgorithmIdentifier which is algorithm information which is used to encrypt the secrete key are included.

Hereinafter, a decoding method will be described.

A receiver who receives an encrypted electronic document decodes the encrypted body and the attached document in accordance with a procedure described with reference to Fig. 12. The receiver decodes the encrypted body and the attached document to acquire a plain text type body and attached document.

-First step: EnvelopedData structure is extracted from the ciphertext to be read out.

-Second step: Decoding information structure (RecipientInfo) is extracted from EnvelopedData structure and then encrypted symmetric key information (KeyTransRecipientInfo) is acquired from the extracted decoding information structure.

-Third step: a receiver acquires a symmetric key used to encrypt the body and the attached document by decoding encryptedKey extracted from encrypted symmetric key information through a private key (which may be mapped to a public key of the certificate) of the receiver.

-Fourth step: an encrypted structure of the body or

the attached document is acquired from EnvelopedData structure extracted in the first step.

-Fifth step: the encrypted body or attached document extracted in the fourth step is decoded using the symmetric key acquired in the third step.

-Sixth step: finally decoded body and attached document are acquired.

[Network security]

In order to keep a confidentiality of the message distributed between the transmitter and the receiver, SSL (Secure Sockets Layer) is applied to all sections of the electronic document distribution (between the distribution client and the distribution messaging server of the messaging transmitter, between the distribution messaging servers of the transmitter and the receiver, and between the distribution messaging server and the distribution client of the receiver) for the network security.

[Message transceiving process]

Various task processes are present between the interested parties in the distribution system and between the systems. There is a most basic message transceiving process in the distribution system and various processes are provided to support the basic message transceiving process.

The message transceiving process is a process that directly sends and receives a message between the transmitter and the receiver and exchanges the document with the other party likes mail or e-mail.

In order to transmit/receive the message between the transmitter and the receiver, a process in four steps of (1) acquiring a physical address and security information for the receiver, (2) sending the message and confirming the sending, (3) confirming the reception of a receiver of a task, and (4) issuing and storing a distribution certificate are provided. In this case, in the process for the distribution certificate, a flow of the detailed process may be changed depending on a content to be evidenced. A basic flow thereof is illustrated in Fig. 14 and described in detail in the following Table 22.

[Table 22]

No.	Name of process	Description
1	Acquiring physical address and security information	◆ the transmitting entity requests the address directory server for physical address information to which a message is actually delivered and security information (if a reception encryption for the transmission

	for receiver	message is necessary) based on the address information of an opposing party and acquires the information ◆ in this process, the address directory server checks whether a requested certified electronic mailing address of the receiving entity is on the blacklist or the white-list (if the electronic mailing address is on the blacklist, message sending error is notified to the transmitting entity) ◆ the distribution messaging server of the transmitting entity requests the address directory server for the physical address and the security information of the receiver and then receives the physical address and the security information
2	Transceiving message and confirming sending	◆ the transmitting entity packages the message in accordance with the technical standard and then performs digital signature based on the certificate of the distribution messaging server ◆ the distribution messaging server sends a packaged and digitally signed message to the physical address which is acquired in advance

		◆ the distribution messaging server of the receiving entity who receives the message verifies a basic packaging structure of the message, a validity of the digital signature, and the compatibility to the transmitter and then creates a reception certificate or an error message for confirming the reception◆ the distribution messaging server of the receiving entity sends a created reception certificate to the transmitting entity ◆ the distribution messaging server of the transmitting entity receives the reception certificate and 1) verifies a compatibility of the reception certificate, 2) attaches the verified information to the reception certificate, and 3) autonomously stores the reception certificate and requests the third party storing institution to store the reception certificate ◆ the sending and the confirmation of the sending are performed by synchronous message processing

3	Confirming reception of receiver of task	◆ if the transmitter requests a reading certificate of the receiving entity at the time of sending the message, the receiving entity creates a reading certificate that evidence the reading confirmation at the time of reading the message and sends the reading certificate to the transmitting entity ◆ if the receiving entity transmits the reading certificate to the transmitting entity, the transmitting entity that receives the reading certificate 1) verifies a compatibility of the reading certificate, 2) attaches the verified information to the reading certificate, and 3) autonomously stores the reading certificate and requests the third party storing institution to store the reading certificate
4	Issuing and storing distribution certificate	◆ when the distribution is evidenced in every step, the transmitting entity receives certificates for the reception, reading, and transmission in accordance with the steps from the receiving entity or the distribution relay server and stores the certificates in the third party storing institution to establish a legal basis

The message transceiving process is divided into a transmitting process and a receiving process. Further, the transmitting process is divided into a synchronous transmission and an asynchronous transmission depending on the connection method between the distribution client and the distribution messaging server.

Hereinafter, the synchronous message transceiving process will be described with reference to Fig. 15 and Table 23.

When the distribution client of the transmitting entity requests the distribution messaging server to transmit a message, the synchronous message transceiving process is a process that transmits a message to the distribution messaging server of the receiving entity in real time basis and synchronously receives a reply therefor from the distribution messaging server of the transmitter. According to the synchronous process, the distribution client instantly checks the result of the transmission so that the definition of the task process may be simplified.

The synchronous message transceiving process will be described in detail in the following Table 23.

[Table 23]

No.	Name of	Description

	process	
1	Acquiring physical address and security information for receiver	◆ similar to the above-described message transceiving process. See a physical address acquiring process as for the detailed process.
2	Transceiving message and confirming transmission	◆ the distribution client of the transmitting entity cerates and attaches a document, sets a transmitting target and transmitting method (encryption or reception of the reading certificate), and requests the distribution messaging server of the transmitting entity to transmit the message. The distribution client waits the response without disconnecting the communication ◆ the distribution messaging server of the transmitting entity receives the message and then transmits the message to the distribution messaging server of the receiving entity ◆ the distribution messaging server of the transmitting entity receives a response message for the transmission from the receiving entity

		(for this process, see the process of transmitting a message and confirming the transmission in the above-described message transceiving process) ◆ the distribution messaging server of the transmitting entity synchronously returns the received response message through the communication section connected to the distribution client.
3	Confirming reception of receiver of task	◆ similar to the above-described message transceiving process
4	Issuing and storing distribution certificate	◆ similar to the above-described message transceiving process

Hereinafter, the asynchronous message transceiving process will be described with reference to Fig. 16 and Table 24.

When the distribution client of the transmitting entity requests the distribution messaging server to

transmit a message, the asynchronous transmitting process verifies only the validity of the transmission request to the distribution messaging server and then returns a reception confirming message for the request to the distribution client. The message is transmitted to the distribution messaging server of the receiving entity in real time basis and the response therefor is synchronously received through the distribution messaging server of the transmitting entity.

The asynchronous process is used when it takes time to transmit the message so that the client cannot wait the response for example, when a quantity of the message to be transmitted is large or a plurality of receivers are designated for one message.

The asynchronous message transceiving process will be described in detail in the following Table 24.

[Table 24]

No.	Name of process	Description
1	Acquiring physical address and security	◆ similar to the above-described message transceiving process. See a physical address acquiring process as for the detailed process.

	information for receiver	
2	Request to transmit message	◆ the distribution client of the transmitting entity cerates and attaches a document, sets a transmitting target and transmitting method (encryption or reception of the reading certificate), and requests the distribution messaging server of the transmitting entity to transmit the message. ◆ the distribution messaging server of the transmitting entity receives the message and verify the validity of the transmitting request, synchronously returns the reception confirmation for the transmitting request and then completes the communication
3	Transmit message to receiver	◆ the distribution messaging server of the transmitting entity searches the transmitting request message received from the distribution client and then transmits the transmitting request message to the receiver ◆ the distribution messaging server of the transmitting entity synchronously receives the response message (reception certificate or

		error message) for the transmission from the receiver and then stores the response message in a receiving box of the distribution client which requests the transmission at first
4	Receives transmission result	◆ the distribution client accesses to the distribution messaging server and requests received message Get in order to get the received message thereto ◆ if a response message is transmitted from the receiving entity, the distribution client receives the response message
5	Confirming reception of receiver of task	◆ similar to the above-described message transceiving process
6	Issuing and storing distribution certificate	◆ similar to the above-described message transceiving process

Hereinafter, a message receiving process will be described in detail.

A process in which a document receiver receives a message through the distribution client is illustrated in Fig. 17 and the process will be described in the following Table 25. When the distribution messaging server of the receiver receives the message from the transmitter, the distribution messaging server sends a reception certificate as a response thereof and stores the document in a message box of a final receiver.

The distribution client frequently requests a list of the received messages to the distribution messaging server. If there is a newly received message, the distribution client receives a list of the received message as a response message and gets the received document through a message that requests detained information.

[Table 25]

No.	Name of process	Description
1	Receive message	◆ when receiving a message, the receiving entity returns a response message for the received message to the transmitting entity, and stores the received message in a mail box of the corresponding user

2	Get list of received messages	◆ the distribution client of the receiving entity passes through the authentication and requests the received document to the distribution messaging server ◆ the distribution messaging server of the receiving entity delivers the list of the received documents stored in the mail box of the user who requests the received document to the distribution client as a synchronous response
3	Get received document	◆ if the receiver requests to read detailed information of the message from the list of the received messages, the distribution client requests the distribution messaging server system to deliver the detailed information including the attached document of the corresponding message ◆ the distribution messaging server of the receiving entity delivers the detailed information of the received document stored in the mail box and the original of the attached document to the distribution client as a synchronous response

4	Send reading certificate (optional process)	◆ if an initial transmitter requests the reading confirmation of a person in charge of reception, the distribution messaging server of the receiver transmits a message including the reading certificate to the transmitter of the corresponding message at the time when the user request the detailed information for the received document ◆ if the attached document is encrypted, the reading certificate is generated at the time when the user decodes the attached document and then delivers the read status to the distribution messaging server rather than at the time when the detailed information is received and then transmitted to the distribution messaging server of the transmitter. In this case, if an error occurs in the process of the decoding, the status information on the error is delivered and the distribution messaging server of the receiving entity delivers a decoding error message to the sender instead of the reading certificate ◆ the distribution messaging server of the receiving entity receives a reception response

		message for the sent reading certificate message (or error message) from the distribution messaging server of the transmitting entity

[Physical address acquiring process]

The transmitting entity which participates in the distribution system needs to know physical actual address information based on the certified electronic mailing address before sending a message to the other party. Further, in order to encrypt a document to be additionally attached, the transmitting entity needs to know public key information of the receiver in the address directory server.

Essential steps of acquiring a physical address of the certified electronic mailing address are as follows 1) to 4):

1) the transmitting entity inquires the address directory server in order to obtain physical address information and security information based on the address information of the receiving entity

2) the address directory server receives/verifies the inquiry of the transmitting entity and then processes the inquiry

3) the transmitting entity set a route based on the received physical address to transmit a message to the

receiving entity

4) the distribution messaging server of the receiving entity receives the message to internally distribute the message in accordance with the user account or the internal identifier

Further, a method of acquiring the physical address of the certified electronic mailing address in the distribution system are classified into the following two methods (1) and (2).

(1) a method that requests the address directory server to search to get the physical address and the receiver public key at a time when the distribution client inputs the address information of the receiver: 1) in order to check previously the validity of the certified electronic mailing address, 2) when the message encryption is required between the distribution client and the distribution messaging server (transmitting entity)

(2) a method where the distribution messaging server gets the physical address from the address directory server after the distribution client requests the distribution messaging server to transmit the message.

A process of acquiring the physical address of the certified electronic mailing address and the security information is illustrated in Fig. 19.

[Distribution relay supporting process]

The distribution system basically performs the direct communication (P2P) between the transmitting entity and the receiving entity. However, additionally, if failure occurs in the message distribution due to the error of the network and the distribution messaging server of the receiving entity, a relay process that relays/performs by proxy the distribution for the purpose of the convenience of the user and the smooth support of the distribution is provided.

When the sending is failed due to the error occurring in the process of sending the message from the transmitting entity to the receiving entity, the distribution relay server in the electronic document distribution hub commissions/sends the message by proxy for the transmitting entity to evidence the sending of the transmitting entity and lessen the systematic load of the transmitting entity.

Fig. 23 illustrates a basic flow thereof and Fig. 24 illustrates a process where the distribution relay server relays the message.

The following Table 26 describes the steps of the distribution relay process.

[Table 26]

No.	Name of	Description

	process	
1	Requesting to transmit message by proxy	◆ transmitting entity sends the message to the receiving entity after packaging and security processing ◆ when the sending is finally failed due to the error occurring during the transmission, the transmitting entity requests the distribution relay server to send the message by proxy ◆ the distribution relay server that accepts the sending request synchronously issues and sends the transmission certificate to the transmitting entity
2	Relaying message commission	◆ the distribution relay server transmits the message which is requested to be relayed. When the transmission is failed, the distribution relay server tries to retransmit at a predetermined interval (the resending time and interval are determined in accordance with the policy of the distribution relay server) ◆ if the distribution relay server finally fails the transmission, the distribution relay server transmits the transmission failure message to the transmitting entity that

		requests the relay of the message.
3	Issuing reception and reading certificate	◆ after the receiving entity successfully receives the message, the receiving entity transmits the reception certificate to the distribution relay server ◆ after the receiver reads the electronic document, the receiving entity directly transmits the transmitting entity not through the distribution relay server

[Storing process of distribution certificate]

As a result related with all distributing actions performed in the distribution system, the distribution certificate is inevitably created to be stored in the third party storing institution. This is because it is possible to establish legal presumption by storing the distribution certificate having distribution evidence in the third storing institute which is legally recognized.

The process of storing the distribution certificate is a separate process from the electronic document distribution but is a supporting process that evidences the fact of the distributing action. Therefore, all the distribution messaging servers need to become a member of a

specific third party storing institution that is capable of receiving and storing the distribution certificate in advance.

Further, if the transmitting entity wants the certification for contents of the electronic document, the entity message in addition to the distribution certificate may be stored in the third party storing institution.

The third party storing institution needs to include the following two additional systems (1) and (2) in order to receive and store the distribution certificate.

(1) distribution messaging server of third party storing institution provider: a system required to transceive the distribution certificate with the distribution messaging server in the distribution system

(2) third party storing institution connected client module: a module that communicates with a third party storing institution connection interface in order to store the distribution certificate received in the third party institution through the distribution messaging server of the third party storing institution provider

However, if the third party storing institution provider also serves as the electronic document provider, the distribution messaging may not be additionally necessary.

Fig. 28 illustrates a process of storing the

distribution between the transceiving entity and the third storing institution provider and the steps of the distribution certificate storing process will be described in the following Table 27.

[Table 27]

No.	Name of process
1	The distribution messaging server of the transmitter receives the distribution certificate from the distribution messaging server of the receiver ◆ when the reception certificate is received from the receiving distribution messaging server or the transmission certificate is received from the relay hub, the distribution certificate is received as the response message ◆ when the reading certificate is received from the receiving distribution messaging server or the reception certificate is received from the relay hub, the distribution certificate is received as a request message
2	- if the received distribution certificate is verified so that the validity is confirmed, the distribution certificate and the verification information of the certificate are sent to the distribution messaging server of a previously set third party storing institution.

	- if the distribution certificate is not valid, the verification error message of the distribution certificate is notified to the distribution messaging server of the receiver to request for resending ◆ if the distribution certificate is received as the response message, the verification error message is sent as the response message thereof (synchronously) ◆ if the distribution certificate is received as the response message, the verification error message is sent as a new request message (asynchronously) ◆ if the verification error message of the distribution certificate is received, the distribution certificate is resent as a new request message or a certification issuance failure message is sent (asynchronously) ◆ if a valid distribution certificate is not received, the transmission of the electronic document is considered to be failed and the electronic document needs to be resent
3	If the distribution messaging server of the third party storing institution receives a message of the third party storing institution storing request, the distribution messaging server of the third party storing institution calls the storage request client in order to store the distribution certificate and the verification information

	(if the third party storing institution also serves as the electronic document provider, the distribution messaging server directly calls the third party storing institution storage request client (local storage request))
4	The distribution certificate storage request client requests third party storing institution to store the distribution certificate and the verification information in accordance with the connection interface standard of the third party storing institution

[Management process such as registration of certified electronic mailing address]

The transceiving entities needs to apply and register the certified electronic mailing address in order to participate in the distribution system and a registration agency and a management agency needs to register and manage the information related to the certified electronic mailing address. The certified electronic mailing address management process includes a management process such as registration, change, and deletion related with the certified electronic mailing address and a blacklist/whitelist management process.

The management agency allows the certified electronic mailing address registration agency to manage the certified

electronic mailing address in order to efficiently manage the certified electronic mailing address.

The registration agency performs the following tasks (1) to (4).

(1) examination task such as identification of an applicant of the certified electronic mailing address

(2) registration information changing task of the registrant of the certified electronic mailing address

(3) task support such as cancellation of the registration of the certified electronic mailing address

(4) other task related with the management of the certified electronic mailing address

The management agency may select any of the third party storing institution who satisfies requirements and the electronic document provider as the registration agency.

Hereinafter, a process of registering the certified electronic mailing address will be described.

A corporate/institution/individual which wants to participate in the distribution system needs to apply the certified electronic mailing address and the registration agency examines and processes the applied information and notifies the result. The related process is illustrated in Fig. 22.

Hereinafter, a process of changing the registration information of the certified electronic mailing address

will be described.

Even though the information related with the certified electronic mailing address which has been already registered may be changed due to various reasons, the identity needs to be maintained so that the electronic mailing address and the information of the owner are not changed.

An authority for changing the information related with the certified electronic mailing address is delegated to the registration agency to be processed. In this case, the record information concerning the change of the information needs to be stored in accordance with the service level agreement (SLA) between the management agency and the registration agency.

The process related therewith is illustrated in Fig. 23. Referring to Fig. 23, the certified electronic mailing address may be changed only by the party concerned. In case of the individual, the certified electronic mailing address, the registration number, and the name cannot be changed. Therefore, the individual withdraws the certified electronic mailing address and then newly creates a new one. In case of corporate, the certified electronic mailing address cannot be changed. If a registration number (business license number) and a company name are changed, the certified electronic mailing address needs to be

changed with a new certificate which is received when the corresponding information is changed.

Fig. 24 illustrates a process of changing the registration agency. Referring to Fig. 24, if the registration agency is changed, 1) a withdrawal process from the existing registration agency and 2) a new registration process through a new registration agency need to be performed. In this case, it is required to request the address directory server to temporally hold the certified electronic mailing address. When all certified electronic addresses are withdrawn, the certified electronic mailing address is selectively temporally held so that the address directory server may maintain the certified electronic mailing address for a predetermined period when the registration agency is changed.

Hereinafter, a process of updating, suspending, and deleting the certified electronic mailing address will be described.

The certified electronic mailing address which has been already registered needs to be updated in accordance with a set usage term. After the registration of the certified electronic mailing address, the owner needs to update the certified electronic mailing address before the usage term set based on the service policy elapses. If the owner does not update the certified electronic mailing

address, the owner lost the ownership of the certified electronic mailing address and the certified electronic mailing address is automatically cancelled.

Further, even when the certified electronic mailing address has not been expired, if the registrant wants to stop using or cancel the electronic mailing address, a function for that needs to be provided.

[Electronic document form application process]

An object of this process is to increase the usage after distributing the message. According to this process, the electronic document included in the message is automatically or semiautomatically processed in the corporation internal system. The distribution messaging server exclusively transceives between the parties concerned and the distribution client provides an interface so that the sender/receiver easily uses the message to be transceived. In the subsequent steps, the electronic document in the message is utilized. The electronic document form register or the electronic document form provides a method that efficiently operates the electronic document utilizing step.

The type of documents which distributed according to the distribution system is not specifically limited. An image, an office document, or a motion picture may be

available. However, in order to increase the convenience of the user, a function of creating a document in the form of text is additionally suggested in the distribution system.

The additional function described above introduces an electronic document exchanging function so that document data is transceived based on the electronic document format appointed between the transceiving entities to automatically transform the electronic document which is received by the internal system of the receiving entity.

As for the form of the electronic document, the following two methods (1) and (2) are available.

(1) a method that utilizes an electronic document form register in the electronic document distribution hub. A standardized electronic document such as an electronic tax invoice is mainly used

(2) a method that shares an electronic document form obtained by the agreement between the transceiving entities. A nonstandaridized electronic document for which is specified to a specific corporate is mainly used

Hereinafter, the utilization of the electronic document form register will be described in detail as follows.

After searching an electronic document form registered in the electronic document form register, the

corporate, the organization, or the individual user registers the electronic document form for in the distribution client to use the electronic document form. The electronic document form register is used by the following two methods (1) and (2).

(1) a method that directly searches an electronic document in the electronic document form register to import the electronic document from the distribution client

(2) a method that searches an electronic document from an electronic document form register site and downloads the electronic document in a local PC, and then registers the electronic document in the distribution client to use the electronic document

Since the electronic document form register registers/utilizes the standardized electronic document form, the management agency needs to systematically operate/manage the electronic document form register and the electronic document form register may have the following standards (1) to (3).

(1) The user needs to apply through the electronic document form register site. The application needs to be performed according to the format and procedure provided from the site.

(2) The registered/applied electronic document needs

to be registered through the examination of the management agency.

(3) Individual electronic documents need to be classified based on a systematic context.

[Table 28]

Classification	Description	Remark
Region	Classify whether the electronic document is distributed internationally or in a specific region, or a specific country	
Sentence structure	Classify whether a sentence structure which is applied to the electronic document is EDIFACT basis, or XML basis, or an editorial format	
Industry	Used when the electronic document is applied only to a specific industry. For example, classify whether a purchase order is used in a trading part, or a manufacturing or a distribution or a logistics part	
Product	If the electronic document uses a format of a specific company product, classify whether the format is a PDF format or a	

	specific company e-Form format	
Corporate	Classify when the electronic document is used only in a specific corporate	
The other	When it is classified by other context other than the above classification	

Fig. 25 illustrates a basic flow of a process of utilizing the electronic document form register. Specifically, Fig. 25A illustrates that the electronic document form register is directly connected with the distribution client and Fig. 25B illustrates that the electronic document form register site is used.

In the following Table 29, a process of utilizing the form by being directly connected to the distribution client is described.

[Table 29]

No.	Classification	Description
1	Searching electronic document form	Directly searches the electronic document form in the electronic document form register from the distribution client
2	Importing form	When the form is searched, the form is imported to the distribution client
3	Registering form	The form which is imported to the

		distribution client is registered in the distribution client
4	Importing/creating electronic document form	The electronic document form which is registered in the distribution client is imported to create the electronic document and attach the electronic document to the message

In the following Table 30, a process of utilizing the electronic document form register site is described.

[Table 30]

No.	Classification	Description
1	Search electronic document form	Access to the electronic document form register site to search a necessary electronic document form
2	Store form in local PC	Download the searched form to store in a local PC
3	Register form	The form which is stored in the local PC is registered in the distribution client
4	Importing/creating electronic document form	The electronic document form which is registered in the distribution client is imported to create the electronic document and attach the electronic document to the

		message

Hereinafter, utilization of the agreed electronic document form will be described.

The agreed electronic document form is used in order to distribute the form specified to a specific corporation in a site which is operated by the corporation to do a business with the parties related with the specific corporation.

Fig. 26 illustrates a procedure of using the agreed electronic document form and the process related with Fig. 26 will be described in the following Table 31.

[Table 31]

No.	Classification	Description
1	Distributing of electronic document form	A corporation A distributes an electronic document form which may be processed in its own system in a web site which is operated by itself to support to be utilized by a business partner
2	Storing of form in local PC	A corporation B2 downloads the form from the web site to store the form in a local PC
3	Registering of	The form stored in the local PC is

	form	registered in a distribution client of a corporation B
4	Importing/creating of electronic document form	The electronic document form which is registered in the distribution client is imported to create the electronic document and attach the electronic document to a message
5	Transmitting of message	Transmit a message through a distribution messaging server
6	Automatic/semiautomatic processing of attached document	The electronic document which is attached to the received message is transformed to be automatically or semiautomatically registered in an internal system of the corporation A

[Spam message processing process]

In the distribution system, the transmitter performs the transmission through a certified distribution messaging server and the receiver performs the reception therethrough. Therefore, if a spam mail is transmitted, the distribution system has an infrastructure that holds the transmitter responsible.

However, a specific transmitter may establish a user account in the electronic document provider and transmits a

commercial message using the user account. The current authentication method may authentify only technical contents of a system so that it is difficult to eradicate the spam message at the initial stage.

In order to block the distribution of the spam message, the distribution system provides a whitelist based on the authentication list management or the blackilist having malicious intention such as a spam to enhance the safety and the reliability of the distribution system.

A function of reporting the spam message and confirming a transmitting party is an essential function. Therefore, all distribution messaging servers necessarily build the function.

Hereinafter, a method of reporting the spam message will be described.

Steps of a reporting procedure of the spam message will be described in the following Table 32.

[Table 32]

No.	Name of process
1	If a receiver determines that a message is a spam message at the timing of receiving the message, the receiver reports the message as a received message to the address directory server through the distributing messaging server

2	The address directory server that receives a report for the spam message from the distribution messaging server returns a confirmation message indicating that the report is received
3	The management agency which is a principal agent managing the address directory server analyzes the message and searches for the transmitter to examine and determine whether to add the certified electronic mailing address of the transmitter to the blacklist
4	If it is finally confirmed as an object of the blacklist, the address directory server adds the certified electronic mailing address to the blacklist and then notifies the transmitter the contents of addition to the blacklist
5	The address directory server transmits the result for the request of the spam message to a reporter (receiver) of the spam

If the receiver determines that the received message is a spam message, the receiver reports the spam message to the address directory server by the process illustrated in Fig. 27.

Roles of the whitelist and the blacklist are as follows:

(1) whitelist: records only information for a

messaging server which is authenticated by the transmitting distribution messaging server and formally registered

(2) blacklist: if an address of the transmitter is registered as a spam sender, the sender is registered as the blacklist

If the spam address which is registered in the blacklist through the same distribution messaging server is repeatedly generated, the management agency determines to cancel the authentication of the distribution messaging server, the authentication is cancelled, and deletes the spam address from the whitelist.

Hereinafter, a processing method when the spam message is received will be described.

When the message is received, the receiving entity checks the whitelist and the blacklist of the address directory server in order to confirm whether the transmitting party is a reliable and legal user and then determines whether to deny the reception.

The transmitter may be checked 1) in real time basis at the time of receiving the message or checked by a periodic checking method that manages as a cache in the distribution messaging server system of the receiver.

(1) A real time checking process: the receiving entity determines whether the address of the transmitting entity is registered in the whitelist and the blacklist in

the address directory server at the time of receiving the message and then determines whether to deny the reception.

[Table 33]

No.	Name of process
1	When the message is received, the distribution messaging server of the receiver delivers a checking request message to the address directory server in order to check whether the transmitter is a legal user
2	The address directory server checks whether the address information of the requested user is included in the whitelist
3	If the address is not included in the whitelist, the address directory server immediately returns the result message indicating the user is not a registered user to a checking requestor. If the address is included in the white list, the address directory server checks whether the address is registered in the blacklist
4	The address directory server returns a result message indicating whether to be registered in the blacklist to the checking requestor
5	If the receiver receives a result message indicating the transmitter is not the legal user (not in the whitelist or registered in the blacklist) from the address directory

	server, the receiver autonomously processes the received message as a spam message and then records and stores the processed result message received from the address directory server and the spam message reception records
6	The processing records for the spam message is necessarily stored for one month or longer so that the legitimacy of the reception denial against the transmitter is checked

Fig. 28 illustrates a process of checking the spam message in realtime basis.

(2) A periodic checking process: the receiver periodically receives the whitelist and the blacklist from the address directory server and autonomously manages and determines whether the address of the transmitter is registered in the whitelist and the blacklist based thereon and then determines whether to deny the reception of the message.

[Table 34]

No.	Name of process
1	The distribution messaging server of the receiving entity requests the latest whitelist and blacklist to the address directory server in advance and autonomously manages. In

	this case, the distribution messaging server transmits automatic notification request when the list is changed (when the automatic notification of the changed matter is requested, periodically requests the address directory server in order to import the latest list so that an interval of list information is at most one day)
2	The address directory server broadcasts details of the change to a user who requests the changing notification when the whitelist and the blacklist are changed
3	The distribution messaging server that receives the changed matter modifies the information of the list which is autonomously managed to synchronize the information
4	When the message is received, the receiver checks the list which is autonomously managed in order to check whether the transmitter is a legal user to the address directory server
5	If the transmitter is not determined to be a legal user (not in the whitelist or registered in the blacklist) as a result of checking the list which is autonomously managed, the receivers processes the received message as a spam message and then records and stores the spam message reception records
6	The processing records for the spam message is necessarily stored for one month or longer so that the legitimacy of

	the reception denial against the transmitter is checked

Fig. 29 illustrates a periodical checking process in order to manage the spam message between the distribution messaging server and the address directory server.

[Error processing process]

Types of error occurring in the distribution system are classified into the following (1) and (2).

(1) error occurrence of synchronous response: in the case of an error for the synchronous response, the requestor is waiting until the processing result for the request message is received so that the requestor immediately notices the error

(2) error occurrence of asynchronous response: the requestor transmits the request contents and the processing result for the request will be received later so that additional error processing is required

Hereinafter, a synchronous error processing method will be described.

Since all errors for synchronous transmission may be immediadetly checked by the transmitter, basically the message is retransmitted. The retransmitting method is determined in accordance with the system policy of the corporate or the institution which participate in the

distribution system. However, basically, if the identical message is transmitted, an identical MessageId value is set to transmit the message.

Types of synchronous error processing are as follows (1) to (4):

(1) Request message transmission failure: a transmission error occurs in the process of transmitting a message by the transmitter so that the request message is not transmitted to the receiver. The transmitter notices the transmission failure by the timeout for the trial of the transmission or a network error message.

(2) Response message reception failure: Even though the transmitter normally transmits the message, an error occurs in the process of receiving a response message from the receiver. The response message reception failure is not discriminated from (1) "request message transmission failure" so that the error is processed by the same method, but the processing method is different because t he receiver normally receives the request message.

(3) Error message reception: Even though the transmitter normally transmits the message, an error occurs in the process of processing the message by the receiver. In this case, the processing method of the transmitter may be varied depending on the types of the error message.

(4) Three stage synchronous error: The message

distribution between three entities in which the distribution client is connected with the other distribution messaging server, address directory server, and distribution relay hub through the distribution messaging server supports a synchronous connection method among the connection types in order to immediately check the final result. In this process, if an error occurs in a step of connecting the distribution messaging server and the receiver, the distribution messaging server promptly occurs an error and then transmits the error to the distribution messaging server as a response message.

Hereinafter, asynchronous error processing method will be described.

The message distribution between three entities in which the distribution client is connected with the other distribution messaging server, address directory server, and distribution relay server through the distribution messaging server may support the connection in the asynchronous method such that the distribution client independently operates in accordance with the situation of the final receiver.

The transmitter may not immediately check the final error for the asynchronous transmission, which is different from the synchronous transmission. Therefore, an error message is generated for the distribution client at the

time of finally checking the error so as to allow the distribution client to receive the error message.

[Electronic document reading service]

The electronic document reading service is a service that provides an electronic document which is stored in a transmitter system or the third party storing institution to be read rather than directly exchanges the electronic document between the transmitter and the receiver.

The electronic document reading service uses the existing distribution system as it is. In this case, the transmitter transmits not a message including the electronic document but a message including a reading authority that reads the electronic document stored in the transmitter system or the third party storing institution to the receiver.

The procedure related therewith is as follows.

(1) acquisition of public key of receiver

(2) storage of electronic document

(3) creation of certificate to which security such as reading authority and DRM is applied

(4) transmission of certificate of reading authority and confirmation of transmission

(5) reading of electronic document by receiver

(6) issuance and storage of distribution (reading)

certificate or reading evidence

The electronic document reading service may be classified into a method where the transmitter uses its own system and a method where the transmitter uses a third party.

Fig. 30 illustrates a flow that the transmitter uses the electronic document reading service utilizing the own system and the procedure illustrated in Fig. 30 will be described in the following Table 35.

[Table 35]

No.	Name of process	Description
1	acquisition of public key of receiving entity certificate	Acquire a public key of the receiving entity certificate which is required to create the electronic document reading authority from the address directory server
2	storage of electronic document and creation of reading authority	Store the electronic document in its own system of the transmitting entity

3	creation of certificate to which security such as reading authority and DRM is applied	Create an authority of reading the stored electronic document and a reading authority certificate to which the security such as DRM is applied
3	Transmission of reading authority	Send the certificate including the reading authority to the receiving entity
4	Reading of electronic document	The receiver of the receiving entity accesses to an electronic document reading system with the reading authority to read the electronic document
5	Storage of distribution (reading) certificate	When the receiver of the receiving entity reads the electronic document, the transmitting entity creates the distribution (reading) certificate and stores the certificate in the third party storing institution

In order to provide the above-described service, the transmitter needs to include a system that is capable of providing an electronic document reading service in addition to the distribution system.

Fig. 31 illustrates a flow where the transmitting entity utilizes the third party to use the electronic document reading service and the procedure illustrated in Fig. 31 will be described in Table 36.

[Table 36]

No.	Name of process	Description
1	Acquisition of public key of receiving entity certificate	Acquire a public key of the receiving entity certificate required to create the electronic document reading authority from the address directory server
2	Storage of electronic document and request of reading service	The transmitting entity stores and requests the electronic document in third party storing institution, and requests the reading service therefor (write the certified electronic mailing address of the receiver)
3	Creation of certificate to which security such as reading authority and DRM are applied	Create a certificate of an authority of reading the requested electronic document stored in the third party storing institution and a certificate to which the security such as DRM is applied

4	Transmission of reading authority certificate	Transmit a certificate including a reading authority of the third party storing institution to the receiving entity
5	Reading of electronic document	The receiver of the receiving entity accesses to the third party storing institution with the reading authority to read the electronic document
6	Storage of distribution (reading) certificate	When a receiver of the third party storing institution receiving entity reads the electronic document, create and store the distribution (reading) certificate
7	Transmission of distribution (reading) certificate	In addition, transmit the distribution (reading) certificate to the transmitting entity that requests the third party storing institution reading service

[Connection mwthod with system in corporation]

The corporation/institution internally creates and stores various electronic documents and exchanges the electronic document with the external corporation/institution by various methods.

The electronic document may be exchanged by off-line such as a postal mail or by an e-mail or job related system.

The distribution systems are connected to each other as illustrated in Table 37 and Fig. 119 when it is connected to the inside the corporation/institution.

[Table 37]

Classification	Description
Postal distribution system	- parties to a transaction transmit a document including an official document by mail - a person in charge of the corporation/institution receives the mail including the document including the official document - tear the mail to receive and register the document including the official document and receive internal approval - after the approval, the document is stored in the document box as a document format
	- (strength) 1) this system is used for a long time and thus very familiar method, 2) IT system cost is saved - (weakness) 1) it takes time to distribute the document, 2) service fee and document storing cost are required, 3) it takes time to search

E-mail distribution system	- parties to a transaction transmit the document including the official document by e-mail - a person in charge of the corporation/institution receives the e-mail including the document including the official document using an e-mail program - (in case of being linked with an internal system) the electronic document in the received message is semiautomatically registered and processed by the internal system - (if it is not connected with the internal system) the electronic document in the received message is stored in the local PC of a person in charge. Accesses to the internal system to register and process the stored electronic document
	- (strength) 1) easy to use, 2) widely used in the worldwide as an assistance of the task, 3) few or no cost - (weakness) 1)since the exchange is performed between the person in charge, additional task processing of the person in charge is required. Further, task failure may occur due to mistake or change of the person in charge 2)when a reception error is caused by the instability of e-mail protocol, a legal dispute may occur

	3)the corporation/institution cannot collectively manage the distributing documents so that the distributing document may be locally processed and managed by the person in charge 4) for one time usage as a simple assistance of the task. A concept for the storage/deletion is weak 5) the e-mail management by the individual has widely spread. Lack in managing principle and control of usage of the corporation e-mail. 6) automatized processing is not available due to the distribution of non-structurized document such as a word document (semiautomatic or manual processing)
Electronic document exchange (EDI) Distribution system	- the parties to a transaction transmit the electronic document through EDI - the receiver receives the electronic document through the EDI application - the received electronic document is automatically transformed and processed to be registered in the internal system - a person in charge of the corporation/institution checks and processes the electronic document registered in the internal system in accordance with the task

	- (strength) 1) the electronic document is automatically transformed and processed without intervention of a person so that the task efficiency is high, 2) correct transmission is available. If there is a dispute for the transmission error, the provider is responsible. - (weakness) 1) lots of initial investment cost is consumed and service fee is required in case of outsourcing. 2) it is required to agree with the party to a transaction for the task and document in advance, 3) only structurized (standardarized) document is distributed. Non-structurized document is not distributed
Task related system distribution system	- the parties to a transaction accesses to the web site which is operated by the receiver through a web browser by the user authentication such as a log-in process - the document is created and the file is attached in accordance with the procedure and the method provided in the web site - a person in charge of the corporation/institution checks the electronic document received by accessing to the task related system. However, since the task related system is the internal system, a specific processing is not required

	- (strength) 1) since the receiver automatically receives the electronic document, the task efficiency of the receiver is high, 2) the transmitter does not need to install additional program so that the distribution cost is not required - (weakness) 1) since the distribution system is mainly based on the receiver, the transmitter needs to access to the system which is operated by the receiver, which is inconvenient for the transmitter, 2) the electronic document remains only in the receiver's system so that if a dispute occurs in the future, the transmitter has a disadvantage

The distribution system based on the certified electronic address may be connected with the internal of the corporation/institution by the following method.

Hereinafter, a method that is linked with an internal system will be described.

A method that is linked with the internal system is mainly used when the corporation or institution installs the distribution messaging server and develops the distribution client in the internal system as system integration (SI). The details will be described in the following Table 38 and the drawing thereof is illustrated in Fig. 120.

[Table 38]

Classification	Description
Automatic processing method	- share user authentication system which is used in the corporation internal system - the electronic document uses a standard electronic document form or an agreed electronic document form - a distribution document processing program is required to automatically process a message which is transmitted at a specific certified electronic mailing address (parsing of the electronic document in the message or verification of suitability) - send and register the electronic document into the internal system in accordance with the certified electronic mailing address
Semi-automatic processing method	- share user authentication system which is used in the corporation internal system - an connection system with the internal system such as an electronic linkage system needs to be already built in the distribution client - a person in charge of the corporation/institution semi-automatically registers the electronic document in accordance with the contents of the distribution client

Hereinafter, a method that is not linked with the internal system will be described.

A method that is not linked with the internal system is suitable for a certified sender/receiver that receives a user account from the electronic document provider to use the user account and is a method that uses a web type distribution client provided by the electronic document provider or installs a distribution client application distributed by the electronic document provider in the local PC to use the distribution client application. The details will be described in the following Table 39 and the drawing is illustrated in Fig. 121.

[Table 39]

Classification	Description
Web method	- become a member of a web site which is operated by the electronic document provider to secure the user account - access to the distribution messaging server based on the web site. Store the electronic document in the received message in the local PC - if a small corporation has a corporation internal

	system, the electronic document stored in the local PC is registered and stored in the internal system
Application method	- the electronic document provider distributes a distribution client install file - the sender/receiver installs the distribution client application in the local PC - access to the distribution messaging server using the distribution client application. Store the electronic document in the received message in the local PC - if a small corporation has a corporation internal system, the electronic document stored in the local PC is registered and stored in the internal system

According to the web method, the user access and process to a web site, the individual user does not needs to install a program in the local PC.

According to the application method, the individual user downloads the install program and installs the program in the local PC to access to the distribution messaging server to use the program.

[Linkage method with external system]

The distribution system has a distribution network based on its own system and the Internet. The electronic

document may be distributed in the distribution system so that there may be a restriction. The distribution system includes an externally connected gateway server in order to distribute the electronic document to a system which is not directly connected thereto.

A basic conceptual view of the extenerally connected gateway server is illustrated in Fig. 32.

The externally connected gateway server serves as a stopover. One includes a distribution messaging server for the distribution system and the other one includes adaptors for connection with the external system.

As described above, in order to be connected with the external system, a task factor and a technical factor need to be considered.

The task factor is an agreement for a task procedure or method related with the connection between the parties. The management agency and the externally connected system management agency need to make the service level agreement (SLA) with each other.

The technical factor refers to a technique factor related with the user authentication, messaging, and the message format which are required for the connection.

The technical principal for the connection with the external system may be summarized as the following (1) to (6).

(1) (Address) The transmitter needs to write an address of the stopover and an address of the final destination.

(2) (User authentication) The transmitter needs to provide user information so that the external system authenticates the transmitter. If the transmitter has become a member of the external system in advance, the authentication identifier of the external system may be used.

(3) (Message disassemble & assemble) The received message is disassembled to be assembled as a message which is compatible with the external system.

(4) (Message security) The encryption or the security such as DRM which is applied to the message needs to be verified/transformed.

(5) (Metadata information) Message and electronic document related information which are included in the message need to be verified/transformed.

(6) (Identification for externally connected system) An external system which is connected with the distribution system may be added or changed. Information on the external system is managed by the address directory server and the distribution messaging server inquires to the address directory server to process the information if necessary.

A procedure of distributing the electronic document in connection with the external system is illustrated in Fig. 33.

In the electronic document distribution system and and electronic document distribution method according to the exemplary embodiment of the present invention as described above, in order to distribute the electronic document, components such as a distribution messaging server, a distribution client, and a distribution relay server are required and these components need to be connected with each other in an overall flow of the electronic document distribution. Therefore, the components operate so as to be connected with each other, a communication protocol, a message exchanging method, and a connected message structure for the connection need to be defined.

Hereinafter, a common base communication protocol and the message exchanging method for the connection between the components are defined and a message structure in accordance with the connection type are defined as a standard to be suggested. Therefore, the present invention allows the smooth connection between the components built under the different circumstances, and by a different development method and interoperation.

[Base communication protocol for connection]

Under the electronic document distribution system based on the certified electronic address, in the electronic document distribution connection interface which is required to distribute the information and the electronic document between the components, the distribution connected message is based on "ebXML Message Services v2.0 standard" (hereinafter, referred to as ebMS) and is hierarchically extended to be defined as a more generalized form. The ebXML based structure is configured by components such as SOAP, SOAP with Attachment, Security, and Reliability which are independent but have a close relationship. "base communication protocol for connection" (hereinafter, base communication protocol) defines elements required in the distribution system based on these basic elements and configured to be a form in which the elements are organically recombined.

The base communication protocol is configured by packaging that forms a message, message envelope configuration, message security, and message transception that transmits and receives a message.

Hereinafter, the message packaging in the base protocol configuration will be described.

The entire message structure of the distribution connection message applies the ebMS v2.0 standard. The

message defined in the base communication protocol has two logical MIME Parts.

A first MIME Part is referred to as a header container and includes a SOAP message. The SOAP message is configured by a Header and a Body.

Second or subsequent MIME Parts are referred to as a payload container and include an application level message and an attached document.

The first MIME Part will be described in detail below. In this part, common information for distributing a message (routing related information of a message, a SOAP message exchanging pattern, digital signature, error information, and position information of data which is added at a second time) is described.

The second MIME Part attaches requests for every connection interface and a response message. In accordance with a type of the connection interface, the presence of a third or subsequent MIME Parts is determined. When the electronic document or the certificate is delivered using the distribution system, the second MIME is included in the third MIME Part.

A basic configuration of the distribution connection message is illustrated in Fig. 34. Referring to Fig. 34, (1) "SOAP-ENV: Header" is configured by MesageHeader and Signature information accordance with the distribution

protocol standard, (2) "SOAP-ENV: BODY" includes Mainfest component information and user login information defined by the distribution protocol standard, (3) "sending container #1 (payload container #1)" includes the request message and the response message. Detailed contents of a business document are defined in accordance with the type of the connection interface, and the presence of request, response, or error message, and (4) in "sending container #2 (payload container #2)", documents to be attached in accordance with the type of the connection interface is sequentially input from the payload container #2.

The distribution connection message needs to observe the standard such as Simple Object Access Protocol(SOAP) 1.1 and SOAP Messages with Attachment.

In Fig. 34, all components of the MIME header of the distribution connection message need to comply with the SOAP Messages with Attachments standard. Additionally, Content-Type MIME Header in the message necessarily has an identical type attribute to a MIME media type of the MIME body part including the SOAP message document. The MIME type of the SOAP message according to the SOAP standard needs to have a "text/xml" value. A route part needs to include Content-ID MIME Header having a structure based on [RFC2045] and a start parameter (optional in [RFC2387])

needs to be always present in addition to an essential parameter for a Multipart/Related media type. An example of the MIME Header of multipart/related message package will be described in the following Table 40.

[Table 40]

```
Content-Type: multipart/related; type="text/xml";
boundary="boundaryValue";
start=messagepackage-123@example.com


--boundaryValue
Content-ID: <messagepackage-123@example.com>
```

Referring to Fig. 34, the first MIME Part header container needs to include the SOAP message. MIME Content-Type header of the header container needs to have a "text/xml" value in accordance with the SOAP standard. The Content-Type header needs to include a "charset" attribute and an example thereof will be described in Table 41. A MIME charset attribute is used to discriminate a character group which is used to create the SOAP message. The MIME charset attribute value and an encoding declaration of the SOAP message located in the header container match with each other and the value thereof needs to be UTF-8. An example of the header container will be described in the

following Table 42.

[Table 41]

Content-Type: text/xml; charset="UTF-8"

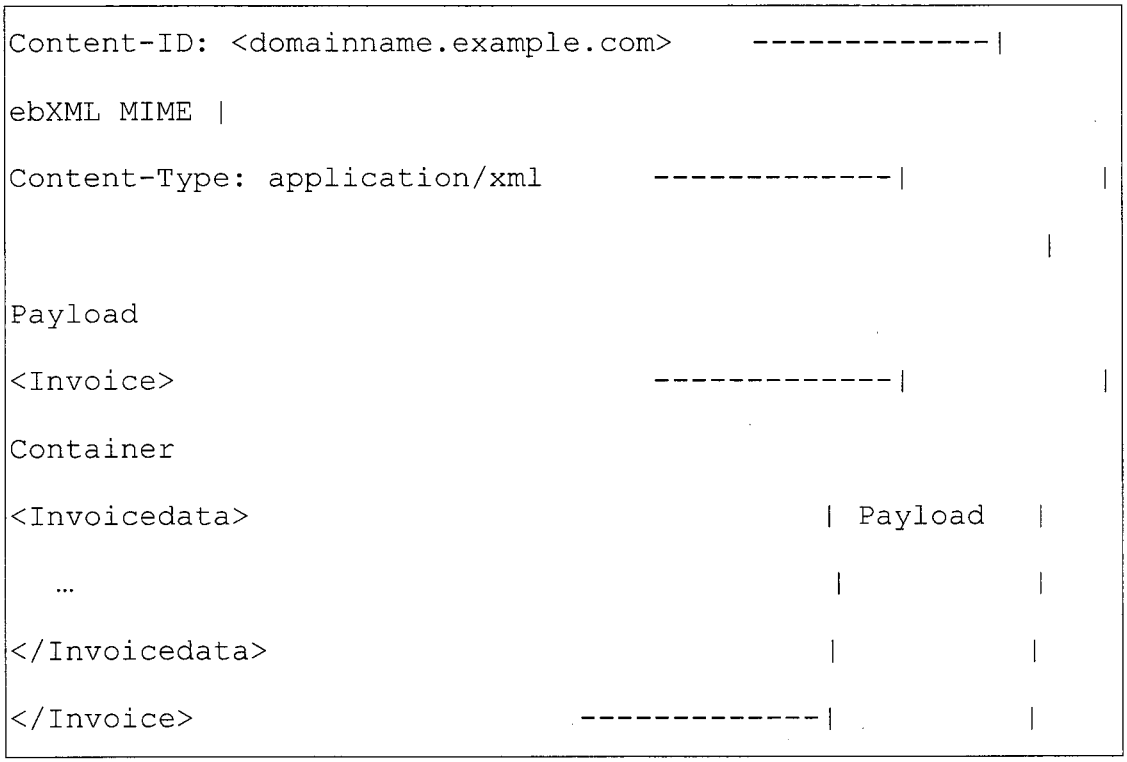
[Table 42]

Ctent-ID: <messagepackage-123@example.com> ---| Header Content-Type: text/xml; charset="UTF-8" . | | <SOAP:Envelope -- |SOAP Message | xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"> | | <SOAP:Header> | | … | | </SOAP:Header> | | <SOAP:Body> | | … | | </SOAP:Body> | | </SOAP:Envelope> --| | |

Referring to Fig. 34, the number of payload

containers may be varied depending on the types of connection interface. Each of the payload containers may be referred by a Manifest element in the SOAP Body in accordance with the ebMS standard. An example thereof will be described in the following Table 43.

[Table 43]



Referring to Fig. 34, in addition to the MIME Header defined as an essential element in this invention, MIME Headers may be added for convenience sake. In this case, the added MIME Header needs to be an item which is clearly described in [RFC2045]. However, the added MIME Header does not need to be noticed or analyzed by a side that does

not add the MIME header.

Hereinafter, the message envelope configuration in the base protocol configuration will be described.

Contents of all extension elements need to be limited to an available name space based on the SOAP standard. The contents of all ebXML SOAP extension elements defined in this invention need to be limited to ebXML SOAP Envelope extension name space. The declarations of the name space may be included in the SOAP Envelop, Header, or Body elements or directly included in each SOAP extension element.

The SOAP Envelop declares various Namespaces in the SOAP message as a Root item of the SOAP message. The Namespaces to be declared are as follows.

[Table 44]

Item	**Namespace URL**
SOAP	http://schemas.xmlsoap.org/soap/envelope/
Digital Signature	http://www.w3.org/2000/09/xmldsig#
Xlink	http://www.w3.org/1999/xlink
Xsi	http://www.w3.org/2001/XMLSchema-instance

A schema structure of the message envelope is

illustrated in Table 35 and an example of the message envelope will be described in the following Table 45.

[Table 45]

```
<SOAP:Envelope
xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
  http://www.oasis-open.org/committees/ebxml-
msg/schema/envelope.xsd">
 <SOAP:Header
xmlns:eb="http://www.oasis-open.org/committees/ebxml-
msg/schema/msg-header-2_0.xsd"

xsi:schemaLocation="http://www.oasis-
open.org/committees/ebxml-msg/schema/msg- header-2_0.xsd
   http://www.oasis-open.org/committees/ebxml-msg/schema/msg-
header-2_0.xsd">
   <eb:MessageHeader ...>
      ...
   </eb:MessageHeader>
  </SOAP:Header>
  <SOAP:Body
```

```
xmlns:eb="http://www.oasis-open.org/committees/ebxml-
msg/schema/msg-header-2_0.xsd"

xsi:schemaLocation="http://www.oasis-
open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
   http://www.oasis-open.org/committees/ebxml-msg/schema/msg-
header-2_0.xsd">
   <eb:Manifest eb:version="2.0">
      ...
   </eb:Manifest>
  </SOAP:Body>
</SOAP:Envelope>
```

The SOAP Header element includes extension elements (1) to (4) as a first child element of the Envelop element.

(1) MessageHeader: An essential element including routing information (To/From) of a message and other context information concerning the message

(2) SyncReply: An element indicating that a method of transceiving a message is synchronous

(3) Signature: an element indicating a digital signature value for the SOAP message and the attached document

(4) ErrorList: An element in which details of the error is input when an error occurs in the process of

processing a message such as Message syntax verification, and message digital signature verification to return the error message

The SOAP Body element includes an extension element such as Manifest as a second child element of the SOAP Envelope. Manifest is an element indicating data which is located in a different position such as a payload container or a web.

The Manifest element requires referring the payload container. The Manifest element is a complex element configured by one or more Reference elements. Each of the Reference elements is included as a part of payload document(s) contained in the payload container or discriminates data related with a message which is a distant resource which is accessible by a URL. It is suggested not to load payload data in the SOAP Body. A purpose of the Manifest is as follows (1) and (2).

(1) allow a specific payload related with the ebXML message to be easily and directly accessed

(2) To determine whether the application processes the payload without parshing

The Manifest element has the following attributes and elements (1) to (3).

(1) One id attribute

(2) One version attribute

(3) one or more Reference elements

The Reference element is a complex element configured by the following subelements (1) and (2).

(1) 0 or more Schema elements: information concerning schema(s) that defines an instant document discriminated from a parent Reference element

(2) 0 or more Description elements: description for a payload objecte referenced by the parent Reference elements

The Reference element is a simple link of [XLINK]. XLINK is a current candidate recommendation (CR) of W3C. Here, XLINK is provided in order to clarify the description of associated relationship. XLINK process or engine is not necessarily used but may be useful depending on the implementation requirements. The Reference element includes the following attribute contents (1) to (5) in addition to the contents of the above-mentioned elements.

(1) id: XML ID for Reference element

(2) xlink-type: this attribute defines the element as a XLINK simple link. This attribute has a fixed value of "simple"

(3) xlink:href: this essential attribute is a URI value of the referenced payload object. This attribute is based on the simple link of [XLINK] specification

(4) xlink:role: this attribute discriminates the payload object or a resource that describes the purpose of

the payload object. If this attribute is present, this attribute needs to have an available URI value based on the [XLINK] specification

(5) Other effective name space attributes may be present. A receiving MSH may ignore an external name space attributes other than the attributes defined above

If reference items have schema(s) that describes the reference items (for example, XML Schema, DTD or Database Schema), the Schema elements needs to be present as child elements of the Reference element. This is used to discriminate the schema from the version and defines the payload object which is discriminated by the parent Reference element. The Schema element has the following attributes (1) and (2).

(1) location: essential URI of schema

(2) version: version identifier of schema

If the xlink:href attribute includes an URI which is content id(URI scheme "cid"), the MIME having the content-id needs to be expressed in the payload container of the message. Otherwise, an error having MimeProbem as errorCode and Error as severity needs to be transmitted to the transmitting party. If the xml:href attribute does not include an URI which is the content id(URI scheme "cid"), the URI is not interpreted and thus it is determined whether to transmit an error depending on the

implementation. If it is determined to transmit the error, an error having MimeProbem as errorCode and Error as severity needs to be transmitted to the transmitting party.

The following Table 46 represents a typical Mainfest of the message having one payload MIME body part.

[Table 46]

```
<eb:Manifest eb:id="Manifest" eb:version="2.0">
  <eb:Reference eb:id="pay01" xlink:href="cid:payload-1"
xlink:role="http://regrep.
org/gci/purchaseOrder">
    <eb:Schema
eb:location="http://regrep.org/gci/purchaseOrder/po.xsd"
eb:version
="2.0"/>
    <eb:Description xml:lang="en-US">Purchase Order for 100,000
widgets</eb:
Description>
  </eb:Reference>
</eb:Manifest>
```

Hereinafter, detailed components of the message in the base protocol configuration will be described.

The MessageHeader element is an essential element which is expressed in all ebXML messages and expressed as a

child element of the SOAP Header element. The MessageHeader element is a complex element configured by the following subelements.

An element structure of the MessageHeader will be described in the following Table 47.

[Table 47]

Name of item	Description			Number of repetition	Type	Length
From	■ message transmitting and transceiving entity information			1..1		
	PartyId	type	■ fixed as 'ecf_cd'			
		■ code identifying transmitter ■ authentication number in case of distribution messaging server ■ set self-management number in case of distribution client ■ set entity code value in		1..1	S	13

		case of address directory server, and distribution relay server			
	Role	■ serve as transmitter ■ fixed as 'sender'	1..1	S	Up to 256
To	■ message receiving and transceiving entity information		1..1		
	PartyId	■ type: ■ fixed as 'ecf_cd'	1..1	S	13
		■ code discriminating receiver ■ authentication number in case of distribution messaging server ■ set self-management number in case of distribution client ■ set entity code value in case of address directory server and distribution relay server	1..1	S	13
	Role	■ serves as receiver ■ fixed as 'receiver'	1..1	S	Up to 256

CPAId	■ ID of business cooperation protocol ■ set code value depending on type of connection interface		1..1	S	Up to 256
ConversationId	■ transceiving transaction identifier		1..1	S	Up to 256
Service	■ identifier of business service defined in business cooperation protocol		1..1	S	Up to 256
Action	■ identifier of specific task process in Service ■ unique value in Service		1..1	S	Up to 256
MessageData	■ data for discriminating message		1..1		
	MessageId	■ unique identifier of one message	1..1	S	Up to 256
	Timestamp	■ message creating time ■ UTC type ■ ex> 2008-07-31T06:29:39.724Z	1..1	S	24
	RefToMessageId	■ existed Only in response message ■ MessageId of request message	0..1	S	Up to 256

Other	■ extension element depending on type of interface ■ name of element has different name depending on the interface ■ refer to connection interface (chapters 5, 6, 7, and 8) for details	0..1		

A schema structure of MessageHeader is illustrated in Fig. 36 and an item code table of MessageHeader will be described in the following Table 48 and a Service/Action item per business will be described in the following Table 49.

[Table 48]

Item of identification code	Code value	Definition of code value
PartyId	ads	Address directory server entity code
	ech	distribution relay server entity code
CPAId	urn:ads-and-ecm-cpa	When connection interface between distribution messaging

		server and address directory server is used
	urn:ecm-and-ecm-cpa	When connection interface between distribution messaging servers is used
	urn:ecm-and-ecc-cpa	When connection interface between distribution client and distribution messaging server is used
	urn:ech-and-ecm-cpa	When connection interface between distribution messaging server and distribution relay server is used

[Table 49]

Item	Service	Action	Definition
When connection interface between distribution messaging server and address directory server is used	urn:ads-service	request	Request
		response	response
When connection interface	urn:ecm-	request	request

between distribution messaging servers is used	service	response	response
When connection interface between and distribution client and distribution messaging server is used	urn:ecc-service	request	request
		response	response
When connection interface between distribution messaging server and distribution relay server is used	urn:ech-service	request	request
		response	response

Examples of the MessageHeader will be described in Table 50.

[Table 50]

```
<eb:MessageHeader SOAP:mustUnderstand="1"
eb:id="MessageHeader" eb:version="2.0">
  <eb:From>
   <eb:PartyId eb:type="ecf_cd">1234567</eb:PartyId>
   <eb:Role>sender</eb:Role>
  </eb:From>
  <eb:To>
   <eb:PartyId eb:type="ecf_cd">4567899</eb:PartyId>
   <eb:Role>receiver</eb:Role>
 </eb:To>
  <eb:CPAId>urn:ecm-and-ecm-cpa</eb:CPAId>
<eb:ConversationId>urn:ecm-and-ecm-
cpa:0210050643</eb:ConversationId>
  <eb:Service>urn:ecm-service</eb:Service>
  <eb:Action>request</eb:Action>
  <eb:MessageData>
<eb:MessageId>20110210-170644Z-00057@127.0.0.18d1f96bf-9cd6-
4049-9fdb-a6c0ed9af467</eb:MessageId>
   <eb:Timestamp>2011-02-10T08:06:44.810Z</eb:Timestamp>
  </eb:MessageData>
  <eb:DuplicateElimination></eb:DuplicateElimination>
</eb:MessageHeader>
```

If SyncReply is present, the SyncReply indicates a synchronous transmission and has the following attributes

(1) to (4).

(1) id attribute

(2) version attribute

(3) SOAP actor attribute (necessarily has "http://schemas.xmlsoap.org/soap/actor/next" value)

(4) SOAP mustUnderstand attribute

An example of SyncReply element will be described in the following table 51.

[Table 51]

```
<eb:SyncReply eb:id="3833kkj9" eb:version="2.0"
SOAP:mustUnderstand="1"
 SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
```

The distribution connection message needs to be digitally signed in order to cope with various dangerous elements which may occur in the process of transceiving. Therefore, the Signature element needs to be present as a child element of the SOAP Header.

Entire SOAP message and a message and attached document contained in the payload container in the distribution connection message need to be a target of the digital signature. Signature target information is digested to be included in the digital signature information.

A process of performing the digital signature in accordance with [XMLDSIG] standard is as follows (1) to (4).

(1) Create a SignedInfo element having SignatureMethod, CanonicalizationMethod, and Reference elements and an essential payload object in the SOAP Envelope as defined in [XMLDSIG]

- A first Reference item at a lowerlevel of SignedInfo has the entire SOAP message as a target so that "" is described in the URI value.

- From a second Reference item, it is described repeatedly as many as the number of payload containers. In this case, the URI value describes a content ID value defined in the MIME Header of the attached document. (a target of Digest is a Content part excluding the Mime Header)

(2) After canonicalization, calculate SignatureValue of SignedInfo based on an algorithm designated in the SignedInfo as designated in [XMLDSIG]

(3) Create signature element including SignedInfo, KeyInfo, and SignatureValue elements as designated in [XMLDSIG]

(4) The Signature of the SOAP Header is included in the SOAP Header element

Algorithm information which is used at the time of digital signature is as follows. The algorithm basically

follows an algorithm part (6.0 Algorithms) of W3C "XML-Signature Syntax and Processing" (RFC3275). Further, in order to support a domestic unique algorithm, an algorithm defined in TTAS.IF-RFC3075 "XML-Signature Syntax and Processing" (Telecommunications Technology Association, 2004) is used.

Next, an algorithm list used in the distribution protocol will be described. In order to minimize ambiguity in the process of creating and verifying of the digital signature at the time of transceiving a message, the use of the algorithm other than the listed following (1) to (5) is restricted.

(1) Digital signature Namespace

[Table 52]

<... xmlns:ds="http://www.w3.org/2000/09/xmldsig#" ... >

(2) Hash (Digest)

;An algorithm used to reduce data observes a related regulation of a certified authentication system.

[Table 53]

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

```
or
<ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256/>
```

(3) Digital signature (Signature)

;An algorithm used to perform digital signature of the message observes a related regulation of a certified authentication system.

[Table 54]

```
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
or
<ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
```

(4) Canonicalization

;Due to characteristics of XML which can physically variously express logically identical document, the digital signature value may be different for the same document. In order to prevent the above phenomenon, the canonicalization process needs to be performed. In the canonicalization, a canonical XML in which comments are omitted is used.

[Table 55]

```
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
```

(5) Transform

;even though there are various transform algorithms as an algorithm that passes through a process of processing and selecting data to be signed among the entire XML data, only three algorithms may be used among the various transform algorithms. A first algorithm is Enveloped Signature transformation since the digital signature observes the form included in the target of the signature, a second algorithm is the above-described Canonicalization, and a third algorithm is Xpath filtering that selects signature target information.

[Table 56]

```
<Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
and
<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
and
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-
19991116">
<ds:XPath>not(ancestor-or-
self::node()[@SOAP:actor=&quot;urn:oasis:names:tc:ebxml-
msg:actor:nextMSH&quot;]
    | ancestor-or-self::node()[@SOAP:actor=
&quot;http://schemas.xmlsoap.org/soap/
actor/next&quot;])
  </ds:XPath>
</ds:Transform>
```

A structure of the digital signature syntax is illustrated in Fig. 37 and an example of the digitally signed message will be described in the following Table 57.

[Table 57]

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:eb="http://www.oasis-open.org/committees/ebxml-
msg/schema/msg-header-2_0.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope
/
http://www.oasis-open.org/committees/ebxml-
msg/schema/envelope.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-
header-2_0.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-
header-2_0.xsd">
  <SOAP:Header>
   <eb:MessageHeader eb:id="..." eb:version="2.0"
SOAP:mustUnderstand="1">
   ...
   </eb:MessageHeader>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
     <CanonicalizationMethod
      Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
```

```
    <SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa
-sha256"/>
    <Reference URI="">
     <Transforms>
      <Transform
     Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
    <Transform Algorithm="http://www.w3.org/TR/1999/REC-
xpath-19991116">
     <XPath> not(ancestor-or-self::node()[@SOAP:actor=
       &amp;quot;urn:oasis:names:tc:ebxml-
msg:actor:nextMSH&amp;quot;]
       | ancestor-or-self::node()[@SOAP:actor=
"http://schemas.xmlsoap.org/
soap/actor
/next"])
     </XPath>
    </Transform>
    <Transform Algorithm="http://www.w3.org/TR/2001/REC-
xml-c14n-20010315"/>
    </Transforms>
    <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```
    <DigestValue>...</DigestValue>
   </Reference>
   <Reference URI="cid://blahblahblah/">
    <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <DigestValue>...</DigestValue>
   </Reference>
  </SignedInfo>
  <SignatureValue>...</SignatureValue>
  <KeyInfo>...</KeyInfo>
 </Signature>
</SOAP:Header>
<SOAP:Body>
 <eb:Manifest eb:id="Mani01" eb:version="2.0">
  <eb:Reference xlink:href="cid://blahblahblah/"
xlink:role="http://ebxml.org/gci
/invoice">
   <eb:Schema eb:version="2.0"

eb:location="http://ebxml.org/gci/busdocs/invoice.dtd"/>
  </eb:Reference>
 </eb:Manifest>
</SOAP:Body>
</SOAP:Envelope>
```

When an error occurs in the process of communication protocol processing process such as message syntax verification or message digital signature verification, the ErrorList element is created in the lowerlevel of the Header and is synchronously returned to the transmitter. When the ErrorList element is generated, RefToMessageId is necessarily present in the MessageHeader elemet and RefToMessageId needs to designate the MessageID of a message in which error occurs.

The ErrorList element has the following attributes (1) to (5).

(1) id attribute

(2) SOAP mustUnderstand attribute

(3) version attribute

(4) highestSeverity attribute

(5) one or more Error elements

If there is no error to be reported, the ErrorList element should not be present. A structure of ErrorList is illustrated in Fig. 38.

The highestSeverity attribute indicates a most serious status of all Error elements. Specifically, if an Error element set the severity as Error, the highestSeverity is set to be Error. Otherwise, the highestSeverity is set as Warning.

The Error element has the following attributes (1) to

(6).

(1) id attribute

; The id attribute serves to uniquely discriminate an ErrorList element in the document.

(2) codeContext attribute

; The codeContext attribute represents a name space or a schema of the errorCodes and should be an URI. A default value of this attribute is urn:oasis:names:tc:ebxml-msg:service:errors. If there is no default value in this attribute, the implementation of the specification indicates that errorCodes is used.

(3) errorCode attribute

; An essential errorCode attribute indicates an essence of an error of a message having an error.

(4) severity attribute

; The severity attribute which is an essential attribute indicates a severity of the error. An effective value is Warning and Error. Warning indicates that other messages in the process of the conversation are normally created regardless of the error. Error indicates that no recovery error is present in the message and other messages are not created in the process of the conversation any more.

(5) location attribute

; The location attribute indicates a message part in which an error is present. If the error is present in

ebXML element and the element is "well-formed", the contents of the location attribute needs to be [Xpointer].

(6) Description attribute

; Contents of the Description element provides a descriptive explanation of the error by a language defined in a xml:lang attribute. Generally, this message is generated by software that verifies XML parser or the message. This means that the content is defined by a seller or a developer of software that creates the Error element.

An example of ErrorList will be described in the following Table 58.

[Table 58]

```
<eb:ErrorList eb:id="3490sdo", eb:highestSeverity="error"
eb:version="2.0" SOAP:mustUnderstand="1">
  <eb:Error eb:errorCode="SecurityFailure"
eb:severity="Error"eb:location="URI_of_ds
:Signature">
   <eb:Description xml:lang="en-US">Validation of signature
failed<eb:Description>
  </eb:Error>
  <eb:Error ...> ... </eb:Error>
</eb:ErrorList>
```

If an error occurs in the process of transceiving a message based on the distribution protocol, a transceiving entity that notices the error needs to report the error to the other party. Errors to be reported include a message structure error, a messaging error, and a security error.

Errors related with a data communication protocol such as HTTP and Socket which belongs to a lower layer than the distribution protocol defined in this invention needs to be found and reported by a standard mechanism supported by the data communication protocol and do not use the error reporting mechanism defined in this invention.

An error code is classified by an error target and error type and details thereof will be described in the following Table 59.

[Table 59]

Error code	Contents	Detailed description
ValueNotRecognized	Element contents or attribute value is not recognized	Even though the document is well formed and effective, a value of element/attribute is unrecornized and thus a value which is used by the ebXML message service is included.

NotSupported	Element or attribute is not supported	Even though the document is well formed and effective and the element or the attribute follows a regulation or restriction of this specification, the document is not supported by the sbXML message service that is capable of processing the message
Inconsistent	Element contents or attribute value is inconsistent with other element or attribute	Even though the document is well formed and effective and follows a regulation or restriction of this specification, the contents of the element and the attribute do not match with the element or the attribute.
OtherXml	Other error in element contents or attribute value	Even though the document is well formed and effective, the contents of the element or the attribute value do not follow a regulation or restriction of this specification and do not belong to other error codes. Contents of Error element need to be used to indicate the essence of the

		problem.
DeliveryFailure	Message transmission failure	The received message is approximately or surely sent to a next destination. If the severity is set as Warning, a possibility that the message is delivered is low
TimeToLiveExpired	Expiration of time when message is present	Even though the message is received, the message is received at a time when a time restricted by TimeToLive of the MessageHeader element has elapsed.
SecurityFailure	Message security check failure	Verification of the signature of the party who sends a message or checking an authority or real name is failed.
Unknown	Unknown error	An error which does not belong to any kinds of error occurs. The content of the Error element is used to indicate the essence of the problem.

Hereinafter, a message transmitting method through the HTTP in the HTTP binding method will be described.

An example of HTTP binding will be described in the following Table 60.

[Table 60]

```
POST /servlet/ebXMLhandler HTTP/1.1
Host: www.example2.com
SOAPAction: "ebXML"
Content-type: multipart/related; boundary="BoundarY";
type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"

xmlns:eb="http://www.oasis-open.org/committees/ebxml-
msg/schema/msg-header-2_0.xsd"

xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope
/
  http://www.oasis-open.org/committees/ebxml-
```

```
msg/schema/envelope.xsd
  http://www.oasis-open.org/committees/ebxml-msg/schema/msg-
header-2_0.xsd
  http://www.oasis-open.org/committees/ebxml-msg/schema/msg-
header-2_0.xsd">
 <SOAP:Header>
  <eb:MessageHeader SOAP:mustUnderstand="1"
eb:version="2.0">
   <eb:From>
    <eb:PartyId eb:type="ecf_cd">123456789</eb:PartyId>
    <eb:Role>sender</eb:Role>
   </eb:From>
   <eb:To>
    <eb:PartyId eb:type="ecf_cd">912345678</eb:PartyId>
    <eb:Role>receiver</eb:Role>
   </eb:To>
   <eb:CPAId>urn:ecm-and-ecm-cpa</eb:CPAId>
   <eb:ConversationId>20001209-133003-
28572</eb:ConversationId>
   <eb:Service>>urn:ecm-service</eb:Service>
   <eb:Action>request</eb:Action>
   <eb:MessageData>
    <eb:MessageId>20001209-133003-
28572@example.com</eb:MessageId>
```

```
    <eb:Timestamp>2001-02-15T11:12:12.724Z</eb:Timestamp>
   </eb:MessageData>
  </eb:MessageHeader>
 </SOAP:Header>
 <SOAP:Body>
  <eb:Manifest eb:version="2.0">
   <eb:Reference
xlink:href="cid:ebxmlpayload111@example.com"
     xlink:role="XLinkRole" xlink:type="simple">
    <eb:Description xml:lang="en-US">Purchase Order
1</eb:Description>
   </eb:Reference>
  </eb:Manifest>
 </SOAP:Body>
</SOAP:Envelope>


--BoundarY
Content-ID: <ebxmlpayload111@example.com>
Content-Type: text/xml


<?xml version="1.0" encoding="UTF-8"?>
<purchase_order>
 <po_number>1</po_number>
 <part_number>123</part_number>
```

```
<price currency="USD">500.00</price>
</purchase_order>--BoundarY--
```

Hereinafter, an HTTP response code in the HTTP binding method will be described.

In the invention, in order to return the response code of the HTTP level, an HTTP response code defined in [RFC2616] needs to be used. Main response codes will be described in the following Table 61.

[Table 61]

State code	Related message	Meaning
200	OK	Request is successfully performed
400	Bad Request	Request has grammatical problem
401	Unauthorized	Client tries to access to a page that requires an approval without having proper approval
404	Not Found	No content is found in this address
500	Internal Server Error	Request is not normally processed due to error in server
503	Service Unavailable	Server currently cannot process requests due to excessive requests which exceeds available limit

Hereinafter, an HTTP sending security method in the HTTP binding method will be described.

The transmission between distribution messaging server and distribution messaging server in the distribution system or the sending between the distribution messaging server and the distribution client need to be processed using HTTP/S(Secure Hypertext Transfer Protocol) that necessarily uses SSL (Secure Socket Layer) V3.0 for the network sending security.

A type of error occurring in the distribution system according to the present invention is largely classified into error occurrence for the synchronous response and error occurrence for the asynchronous response.

In the case of the error for the synchronous response, the requester waits until the processing result for the request message is received so that the requester immediately recognizes the error. In contrast, in the case of the error for the asynchronous response, the requester receives the processing result later after delivering request contents only so that additional error processing is required.

Hereinafter, a synchronous error processing method in the error processing method will be described.

All message distribution between a distribution two

entities of messaging server, other distribution messaging server, the address directory server, the distribution client, and the distribution relay server is a synchronous distribution. Further, the message distribution between three entities in which the distribution client is connected to the other distribution messaging server, the address directory server, and the distribution relay server through the distribution messaging server through the distribution messaging server is synchronously or asynchronously connected in accordance with the connection type.

All errors for the synchronous transmission may be immediately checked by the transmitter so that the message is basically retransmitted. The retransmission method is determined in accordance with a policy of the system of the corporation or the institution which participates in the distribution system. However, basically, the identifical message is transmitted again by setting the same MessageId value.

By transmitting the message with the same MessageId, not only when the error occurs at the time of sending, but also when an error occurs in the process of synchronously sending the response message after the receiver successfully receives the message, the redundancy message is noticed so as to prevent the same request from being

redundantly processed.

The transmitter and the receiver of the synchronous error may be the distribution messaging server, the address directory server, the distribution client, and the distribution relay server in accordance with the connection type.

(1) error message sending failure: the sending error occurs when the transmitter sends a message so that the request message is not delivered to the receiver. The transmitter recognizes the sending failure by timeout or network error message for the trial of the transmission. Fig. 39 illustrates a process when the request message transmission is failed and the processing procedure is as follow 1) to 3).

1) The sending error occurs in the process of the sending by the message transmitter. In most cases, this error is caused by the network error

2) If the transmitter receives an error message such as an HTTP error, the transmitter requests needs to resend the same message

3) Only when the reception confirmation message is received from the receiver, the transmitter recognizes that the sending is successful

(2) response message reception failure: Even though the transmitter normally transmits a message, an error

occurs when the response message is received from the receiver. In the position of the transmitter, the response message reception failure is not discriminated from the (1) request message transmission failure so that the error is processed by the same method. However, since the receiver normally receives the request message, the processing method is different from the transmitter's processing method. Fig. 40 illustrates a process related with the response message reception failure and the processing procedure will be described as follows 1) to 3).

1) Even though the message is normally delivered to the receiver, when the transmitter does not receive a reception confirmation message from the receiver

2) In this case, the transmitter recognizes as the transmission failure error and retransmits the identical message to the receiver with the identical MessageId

3) If the MessageId of the received document is identical to the previously received message, the receiver sends a reception confirmation message indicating redundant reception and internally processes the message

(3) Error message reception : Even though the transmitter normally sends a message, an error occurs while the receiver who receives the sent message processes the message. In this case, the processing method of the transmitter is varied depending on the type of the error

message. The error type on the communication protocol refers to the above-described "ErrorList" item. Further, the error occurring in the process of the internal processing on the request message for every connection interface refers to the message structure of the connection interface is referred. Fig. 41 illustrates a process related with the reception of the error message and the processing procedure is as follows 1) to 3).

1) Even though the message which is sent to the receiver is correctly delivered, when the error message is received due to the error of the transmission message

2) In this case, generally, the transmitter recreates the request message and then resends the message. However, the message processing may be varied depending on the error type

3) when the transmitter resends the request message, the MessageId of the message to be sent does not need to be identical to the previous message and differently processed in accordance with the task situation.

(4) three stage synchronous error : the message distribution between three entities in which the distribution client is connected to the other distribution messaging server, the address directory server, and the distribution relay server through the distribution messaging server supports a synchronous connection method

among the connection methods in order to immediately check the final result. During this process, if an error occurs in the connection step between the distribution messaging server and the receiver, the distribution messaging server immediately generates an error and then delivers the error to other distribution messaging server as a response message. Fig. 42 illustrates a process related with the three stage synchronous error and the processing procedure is as follows 1) to 3).

1) Even though the transmission is successful in the process where the distribution client transmits a message in connection with the distribution messaging server, an error occurs in the process of transmitting a message to a receiver next to the distribution messaging server (the addres directory server, other distribution messaging server, or the distribution relay server)

2) In this case, the error refers to all errors that occur during the synchronous sending between the distribution messaging server and the receiver

3) the distribution messaging server generates an error message for the distribution client at the time when the distribution messaging server notices the error and delivers the error message to the distribution client as a response message

The error message created by the distribution

messaging server is configured in the structure of the following Table 62.

[Table 62]

Name of item		Description	Number of repetition	Type	Length
Content		■ Root element			
	DocType	■ type of distribution message - failure: 9	1..1	Integer	1
	Sender	■ receiver of request message certified electronic mailing address	1..1	String	Up to 128
	Receiver	■ transmitter of request message certified certified electronic mailing address	1..1	String	Up to 128
	RefIdentifier	■ unique identification value of request message	1..1	String	36
	Identifier	■ unique identification value of error message	1..1	String	36

		created in UUID type			
	ErrorCode	■ corresponding error code	1..1	Integer	4

Hereinafter, the asynchronous error processing method in the error processing method will be described.

The message distribution between three entites in which the distribution client is connected to the other distribution messaging server, the address directory server, and the distribution relay server through the distribution messaging server supports an asynchronous connection method among the connection methods adapted to situation of final receiver.

The final error for the asynchronous transmission may not be immediately checked by the transmitter, which is different from the synchronous transmission. Therefore, the distribution messaging server generates an error message for the distribution client at the time when the distribution messaging server finally checks the error and allows the distribution client to receive the error message.

Fig. 43 illustrates a process related with the asynchronous error processing method and the processing method is as follows 1) to 4).

1) Even though the transmission is successful in the process where the distribution client transmits a message

in connection with the distribution messaging server, an error occurs in the process of transmitting a message to a receiver next to the distribution messaging server (the addres directory server, other distribution messaging server, or the distribution relay server)

2) In this case, the error refers to all errors that occur during the synchronous transmission between the distribution messaging server and the receiver

3) the distribution messaging server generates an error message for the distribution client at the time of finally recognizing the error after the retrial and then delivers the error message to the mail box of the distribution client

4) the distribution client notices the error for the previous request message by the error message which is received in its mail box in the process of requesting the reception message to the distribution messaging server

The error message generated by the distribution messaging server is configured by the structure of the following Table 63.

[Table 63]

Name of item	Description	Number of	Type	Length

			repetition		
Content		■ Root element			
	DocType	■ type of distribution message - failure: 9	1..1	Integer	1
	Sender	■ receiver of request message certified electronic mailing address	1..1	String	Up to 128
	Receiver	■ transmitter of request message certified electronic mailing address	1..1	String	Up to 128
	RefIdentifier	■ unique identification value of request message	1..1	String	36
	Identifier	■ unique identification value of error message created in UUID type	1..1	String	36
	ErrorCode	■ corresponding error code	1..1	Integer	4

[Connection interface between distribution messaging server and address directory server]

The address directory server is a system that manages a certified electronic mailing address which is very basic in the distribution system and is inevitably necessary in the electronic document distribution.

The connection interface between the distribution messaging server and the address directory server are largely divided into two functions. A first function is an interface related with a registration task of the certified electronic mailing address of the registration agency and a second function is an interface related with a task of physical address inquiring/response with the distribution messaging server and reporting the spam.

The interface for the registration task of the certified electronic mailing address with the registration agency may be separated. However, the electronic document provider or the third party storing institution server is the registration agency so that the interface function is inserted in the distribution messaging server.

In this case, in the distribution messaging server provided in the transceiving entity, the connection interface related with the registration of the certified electronic mailing address is not inserted.

The interface function between the distribution messaging server and the address directory server will be described in the following Table 64.

[Table 64]

Classification of Interface		Description of interface	Remark
Address Management	Register certified electronic mailing address (when address of certified sender/receiver is registered)	□ interface of registering certified electronic mailing address information of a certified sender/receiver who transmits/receives a document through the electronic document provider in the address directory server □ if the requested certified electronic mailing address is not unique in the address directory server, the registration is failed	Requester is electronic document provider
	Change certified electronic mailing address information	□ interface that requests the address directory server to change the information and receives the result when information concerning certified electronic mailing address (for example, security	

		information or ID) is changed	
	Delete certified electronic mailing address	□ interface that requests the address directory server to delete the address and receives the result when the certified electronic mailing address registered in the address directory server is not used any more	
Address search	Search physical address information	□ interface that requests the address directory server to search the security information (certificate) of the user corresponding to the certified electronic mailing address information and physical address information and then receives the result	Requester is electronic document provider and transceiving entity
Blacklist management	Report spam message	□ interface that reports the spam message to the address directory server and then receives the reception as a result	

		□ address directory server notifies the reporter and the spam sending party of the final processing result for the reported spam message (whether to be confirmed as a spam message) using "message transmitting interface"	
notification	Notify whitelist	□ interface that transmits whitelist from the address directory server to the transceiving entity	
	Notify blacklist	□ interface that transmits blacklist from the address directory server to the transceiving entity	

Details of the interfaces between the distribution messaging server and the address directory server will be described below.

First, common facts of the interfaces between the distribution messaging server and the address directory server are as follows (1) and (2).

(1) Extension of MessageHeader of request message

The digital signature information of the transmitting entity needs to be delivered so as to be included in a SOAP message of the first MIME Part of the request message which is transmitted from the distribution messaging server of the transmitting entity to the address directory server. Further, additional information (CorpNum, RValue) of the transmitting entity which is required for the address directory server to verify whether an owner of the certificate used for the digital signature of the SOAP message matches with the transmitting entity (VID verification) is also delivered to be included therein.

The additional information of the transmitting entity needs to be located at a lower level of the MessageHeader element in the SOAP message of the request message as an extension element (any ##other position).

The extension element structure will be described in the following Table 65 and an example of the extension element will be described in the following Table 66.

[Table 65]

Name of item	Description	Number of repe	Type	Length

			titi on		
Extension		■ Extension element	1..1		
	CorpNum	■ business registration No. of provider or transceiving entity	1..1	Strin g	10
	RValue	■ Rvalue extracted from private key of certificate of provider or transceiving entity ■ RValue is encoded by Base64 to be input	1..1	Strin g	28

[Table 66]

```
<eb:MessageHeader SOAP:mustUnderstand="1"
eb:id="MessageHeader" eb:version="2.0">
 <eb:From>
    <eb:PartyId eb:type="ecf_cd">123456789</eb:PartyId>
    <eb:Role>sender</eb:Role>
   </eb:From>
   <eb:To>
    <eb:PartyId eb:type="ecf_cd">ads</eb:PartyId>
    <eb:Role>receiver</eb:Role>
   </eb:To>
   <eb:CPAId>urn:ads-and-ecm-cpa</eb:CPAId>
   <eb:ConversationId>20001209-133003-
```

```
28572</eb:ConversationId>
    <eb:Service>>urn:ads-service</eb:Service>
    <eb:Action>request</eb:Action>
 <eb:MessageData>

<eb:MessageId>20110210-170644Z-00057@127.0.0.18d1f96bf-9cd6-
4049-9fdb-a6c0ed9af46 7</eb:MessageId>
  <eb:Timestamp>2011-02-10T08:06:44.810Z</eb:Timestamp>
  </eb:MessageData>
  <eb:DuplicateElimination></eb:DuplicateElimination>
  <Extention>
   <CorpNum>2208203228</CorpNum>
   <RValue>asdfasdf</RValue>
  </Extention>
</eb:MessageHeader>
```

(2) Entire message structure

In the connection interface between the distribution messaging server and the address directory server, the SOAP message is located at the first MIME part of the message and the distribution message for the request and response is located at the second MIME Part.

The SOAP structure between the distribution messaging server and the address directory server is illustrated in Fig. 44.

Hereinafter, the registration of the certified electronic mailing address in the interface between the distribution messaging server and the address directory server will be described.

A message exchange flow related with the registration of the certified electronic mailing address is illustrated in Fig. 45.

The request distribution message structure will be described in the following Table 67 and an example of the message will be described in the following Table 68.

[Table 67]

Name of item		Description	Number of repetition	Type	Length
Request		■ request Root element			
	RegAddrReq	■ registration request element of certified electronic mailing address of certified sender/receiver			

		PeerCorpNum	■ business registration No. of transceiving entity	1..1	String	10
		PeerRegNum	■ authentication No. of transceiving entity	0..1	String	10
		Name	■ Name of member	1..1	String	70
		Type	■ membership type - personal: U - business: C	1..1	String	1
		IDN	■ Identification No. of member - personal: resident registration number - business: business registration No.	1..1	String	minimum 10 up to 13
		RAddress	■ certified electronic mailing address	1..1	String	minimum 1 up to 128
		Cert	■ certificate	0..1	Base64	-
		Representative	■ name of representative in case of business member	0..1	String	30

	Addr	■ personal or business address	0..1	String	256
	Tel	■ personal or business phone number (omitting -)	0..1	Integer	minimum 9 up to 12
	Fax	■ personal or business fax number	0..1	Integer	minimum 9 up to 12
	Mobile	■ personal or business mobile phone number (omitting -)	0..1	Integer	minimum 10 up to 12
	EMail	■ personal or business e-mail	0..1	String	256
	RegDate	■ registration date of certified electronic mailing address	0..1	Long	-
	EndDate	■ expiration date of certified electronic mailing address	0..1	Long	-
	ManagerName	■ name of manager of certified electronic mailing address	0..1	String	70
	ManagerAd	■ address of manager of	0..	String	256

		dr	certified electronic mailing address	1		
		ManagerEMail	■ email of manager of certified electronic mailing address	0..1	String	256
		ManagerTel	■ phone number of manager of certified electronic mailing address	0..1	Integer	minimum 9 up to 12
		ManagerMobile	■ mobile phone number of manager of certified electronic mailing address	0..1	Integer	minimum 10 up to 12

[Table 68]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
 <RegAddReq>
  <PeerCorpNum>1234567890</PeerCorpNum>
  <PeerRegNum>5555555555</PeerRegNum>
  <Name>Hong, Gildong</Name>
  <Type>U</Type>
  <IDN>1111112222222</IDN>
  <RAddress>#000-0000-0000</RAddress>
  <Cert>MIDJAHjhh46dhkfjsjfsj...</Cert>
  <Addr>Seoul</Addr>
  <Tel>021113333</Tel>
  <Mobile>0101112222</Mobile>
```

```
 </RegAddReq>
</Request>
```

A structure of the response distribution message will be described in the following Table 69 and an example of the message will be described in the following Table 70.

[Table 69]

Name of item		Description	Number of repetition	Type	Length
Response		■ Response Root element			
	RegAddrRes	■ registration agency (electronic document provider) member			

			registration response element			
		ResultCode	■ processing result - success: 1 - fail: 0	1..1	Boolean	-
		ErrorCode	■ error code (only when the processing result is failed (0), input corresponding error code)	0..1	String	256

[Table 70]

```
<Response xmlns="http://www.nipa.kr/eDocument_Circulation">
 <RegAddRes>
  <ResultCode>1</ResultCode>
 </RegAddRes>
</Response>
```

Hereinafter, an interface of changing the certified electronic mailing address information in the interface between the distribution messaging server and the address directory server will be described.

The interface of changing the certified electronic mailing address information is an interface that allows the electronic document provider to request the address

directory server to change the certified electronic mailing address information of the certified sender/receiver registered in the address directory server and receive the response. After transmitting the request message including the user information and the certified electronic mailing address information to be changed, the electronic document provider receives the changing result of the address directory server as a response message.

A message exchange flow related with the changing process of the certified electronic mailing address is illustrated in Fig. 46.

The request distribution message structure will be described in the following Table 71 and an example of the message will be described in the following Table 72.

[Table 71]

Name of item	Description	Number of repetition	Type	Length
Request	■ request Root element			

ModAddrReq		■ registration request element of certified electronic mailing address of certified sender/receiver			
	PeerCorpNum	■ business registration No. of transceiving entity	1..1	String	10
	PeerRegNum	■ authentication No. of transceiving entity	0..1	String	10
	Name	■ Name of member	0..1	String	70
	Type	■ membership type - personal: U - business: C	0..1	String	1
	IDN	■ Identification No. of member - personal: regident registration number - business: business registration No.	0..1	String	minimum 10 up to 13
	RAddress	■ certified electronic mailing address	1..1	String	minimum 1 up to 128
	Cert	■ certificate	0..	Base6	-

			1	4	
Representative	■ name of representative in case of business member	0..1	String	30
Addr	■ personal or business address	0..1	String	256
Tel	■ personal or business phone number (omitting -)	0..1	Integer	minimum 9 up to 12
Fax	■ personal or business fax number	0..1	Integer	minimum 9 up to 12
Mobile	■ personal or business mobile phone number (omitting -)	0..1	Integer	minumum 10 up to 12
EMail	■ personal or business e-mail	0..1	String	256
RegDate	■ registration date of certified electronic mailing address	0..1	Long	-
EndDate	■ expiration date of certified electronic mailing address	0..1	Long	-
ManagerNam	■ name of manager of	0..	Strin	70

		e	certified electronic mailing address	1	g	
		ManagerAddr	■ address of manager of certified electronic mailing address	0..1	String	256
		ManagerEMail	■ email of manager of certified electronic mailing address	0..1	String	256
		ManagerTel	■ phone number of manager of certified electronic mailing address	0..1	Integer	minumum 9 up to 12
		ManagerMobile	■ mobile phone number of manager of certified electronic mailing address	0..1	Integer	minumum 10 up to 12

[Table 72]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
 <ModAddrReq>
  <PeerCorpNum>1234567890</PeerCorpNum>
  <PeerRegNum>5555555555</PeerRegNum>
  <Name>Hong, Gildong</Name>
  <Type>U</Type>
  <IDN>1111112222222</IDN>
  <RAddress>#000-0000-0000</RAddress>
```

```
  <Cert>MIDJAHjhh46dhkfjsjfsj...</Cert>
  <Addr>Seoul</Addr>
  <Tel>021113333</Tel>
  <Mobile>0101112222</Mobile>
 </ModAddrReq>
</Request>
```

A structure of the response distribution message will be described in the following Table 73 and an example of the message will be described in the following Table 74.

[Table 73]

Name of item		Description	Number of repetition	Type	Length
Response		■ Response Root element			
	ModAddrRes	■ member modification response element of electronic document provoder			

		ResultCode	■ processing result - success: 1 - fail	1..1	Boolean	-
		ErrorCode	■ error code (only when the processing result is failed (0), input corresponding error code)	0..1	String	256

In Fig. 73, if the ResultCode is input as failure (0), an error code corresponding to a cause of the error is input as ErrorCode

[Table 74]

```
<Response xmlns="http://www.nipa.kr/eDocument_Circulation">
 <ModAddrRes>
  <ResultCode>1</ResultCode>
 </ModAddrRes>
</Response>
```

Hereinafter, an interface of deleting the the certified electronic mailing address information in the interface between the distribution messaging server and the address directory server will be described.

The interface of deleting the certified electronic

mailing address information is an interface that allows the electronic document provider to request the address directory server to delete the certified electronic mailing address information of the certified sender/receiver registered in the address directory server and receive the response. After transmitting the request message including the user information and the certified electronic mailing address information to be deleted, the electronic document provider receives the deleting result of the address directory server as a response message.

A message exchange flow related with the deleting process of the certified electronic mailing address is illustrated in Fig. 47.

The request distribution message structure will be described in the following Table 75 and an example of the message will be described in the following Table 76.

[Table 75]

Name of item	Description	Number of repetitio	Type	Length

			n		
Request		■ request Root element			
	DelAddrReq	■ deleting request element of certified electronic mailing address of member			
		Name	■ name of member	1..1	String	Up to 70
		IDN	■ Identification No. of member - personal: regident registration number - business: business registration No.	1..1	String	Minimum 10 Up to 13
		RAddress	■ certified electronic mailing address	1..1	String	minimum 1 up to 128

[Table 76]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
 <DelAddrReq>
  <Name>Hong, Gildong</Name>
  <IDN>1111112222222</IDN>
  <RAddress>#000-0000-0000</RAddress>
```

```
</DelAddrReq>
</Request>
```

A structure of the response distribution message will be described in the following Table 77 and an example of the message will be described in the following Table 78.

[Table 77]

Name of item			Description	Number of repetition	Type	Length
Response			■ Response Root element			
	DelAddrRes		■ member deleting response element of electronic document provider			
		ResultCode	■ processing result - success: 1 - fail: 0	1..1	Boolean	-
		RAddress	■ certified electronic	0..∞	String	minimum

			mailing address			1 up to 128
		ErrorCode	■ error code (only when the processing result is failed (0), input corresponding error code)	0..1	String	256

In Fig. 77, if the ResultCode is input as failure (0), an error code corresponding to a cause of the error is input as ErrorCode.

[Table 78]

```
<Response xmlns="http://www.nipa.kr/eDocument_Circulation">
 <DelAddrRes>
  <ResultCode>1</ResultCode>
 </DelAddrRes>
</Response>
```

Hereinafter, an interface of searching physical address information in the interface between the distribution messaging server and the address directory will be described.

The interface of searching physical address

information is an interface that allows the electronic document provider or the transceiving entity to request the address directory server to request physical address information corresponding the certified electronic mailing address information of the receiver of the electronic document and certificate information for message secure processing and receive the response. After transmitting the request message including the certified electronic mailing address of the receiver of the electronic document and request of the certificate, the electronic document provider receives the physical address information (IP address or Domain address) of the receiver of the electronic document and the certificate information from the address directory server as a response message.

A message exchange flow related with the searching process of the physical address information is illustrated in Fig. 48.

The request distribution message structure will be described in the following Table 79 and an example of the message will be described in the following Table 80.

[Table 79]

Name of item	Description	Number	Type	Length

			of repetition		
Request		■ request Root element			
	SchAddrReq	■ searching request element of certified electronic mailing address			
		ReqInfo	■ request certified electronic mailing address information element	1..∞		
		RAddress	■ certified electronic mailing address	1..1	String	Up to 128
		IsCert	■ request of certificate - request: 1 - no request: 0	1..1	Integer	1

[Table 80]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
 <SchAddrReq>
  <ReqInfo>
   <RAddress>#000-0000-0000</RAddress>
   <IsCert>0</IsCert>
  </ReqInfo>
```

```
</SchAddrReq>
</Request>
```

A structure of the response distribution message will be described in the following Table 81 and an example of the message will be described in the following Table 82.

[Table 81]

Name of item	Description	Number of repetition	Type	Length
Response	■ Response Root element			
SchAddrRes	■ searching response element of certified electronic mailing address			
ResultCode	■ processing result - success: 1 - fail: 0	1..1	Boolean	-

		ResultData	■ result list	0..∞		
		RAddress	■ certified electronic mailing address	0..∞	String	minimum 1 maximum 128
		IsExist	■ existence of address information (Attribute) - existed: 1 - not existed: 0	1..1	Integer	1
		Endpoint	■ physical address of certified electronic mailing address	0..1	String	maximum 256
		PeerRegNum	■ authentication number of transceiving entity	0..1	String	10
		Cert	■ public key of receiver	0..1	Base64	-
		PeerCert	■ public key of transceiving entity	0..1	Base64	-
		ErrorCode	■ error code (only when the processing result is failed (0), input corresponding error code)	0..1	String	256

[Table 82]

```
<Response xmlns="http://www.nipa.kr/eDocument_Circulation">
 <SchAddrRes>
  <ResultCode>1</ResultCode>
  <ResultData>
   <RAddress IsExist="1">#000-0000-0000</RAddress>
   <Endpoint>http://111.111.111.111:8080/imxs/msh</Endpoint>
   <Cert>MFJIFDjfksdfjsl...</Cert>
  </ResultData>
 </SchAddrRes>
</Response>
```

Hereinafter, an interface of reporting a spam message in the interface between the distribution messaging server and the address directory will be described.

The interface of reporting a spam message is an interface that allows the electronic document provider or the transceiving entity to report the spam message to the address directory server. After transmitting the request message including the certified electronic mailing address of the spam transmitter and spam message information, the interface receives whether to accept the spam report from the address directory server as a response message. If the determination regarding whether the reported spam message is a spam is completed, the address directory server notifies the processing result using the "message sending"

interface of the connection interface between the distribution messaging servers.

A message exchange flow related with the reporting and accepting process of the spam message is illustrated in Fig. 49.

The request distribution message structure will be described in the following Table 83 and an example of the message will be described in the following Table 84.

[Table 83]

Name of item	Description	Number of repetition	Type	Length
Request	■ request Root element			
ReportSpamReq	■ spam report request element			
ReportRAdderss	■ certified electronic mailing address of reporter	1..1	String	Up to 128
SpamRAdderss	■ certified electronic mailing address of spam	1..1	String	Up to 128

			transmitter			
		ContentsPid	■ reference ID of content ID sent by spam transmitter (MIME Part cid of spam reporting message)	1..1	String	Up to 256
		AttacheFileInfo	■ attached document information sent by spam transmitter	0..*		
			FilePid	■ reference ID of attached document information sent by spam transmitter (MIME Part cid of spam reporting message)	1..1	String	Up to 256
			FileName	■ reference name of attached document information sent by spam transmitter	1..1	String	Up to 256
		SpamPeerCorpNum	■ business number of distribution messaging server operator that is used by spam user	1..1	String	Up to 10

[Table 84]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
 <ReportSpamReq>
  <ReportRAddress>#000-0000-0000</ReportRAddress>
  <SpamRAddress>#000-0000-0000</SpamRAddress>
  <ContentsPid>cid-1</ContentsPid>
  <AttacheFileInfo>
   <FilePid>cid-2</FilePid>
   <FileName>License.txt</FileName>
  </AttacheFileInfo>
  <SpamPeerCorpNum>1234567890</SpamPeerCorpNum>
 </ReportSpamReq>
</Request>
```

A structure of the response distribution message will be described in the following Table 85 and an example of the message will be described in the following Table 86.

[Table 85]

Name of item	Description	Number of repetition	Type	Length

Response			■ Response Root element			
	ReportSpamRes		■ spam report response element			
		ResultCode	■ processing result - success: 1 - fail: 0	1..1	Boolean	-
		RAddress	■ certified electronic mailing address of spam transmitter	0..1	String	minimum 1 up to 128
		ErrorCode	■ error code (only when the processing result is failed (0), input corresponding error code)	0..1	String	256

In Table 85, it is noted that ResultCode is a simple acception processing result for the spam reporting message.

[Table 86]

```
<Response xmlns="http://www.nipa.kr/eDocument_Circulation">
 <ReportSpamRes>
  <ResultCode>1</ResultCode>
  <RAddress>#spammer. individual</RAddress>
 </ReportSpamRes>
```

```
</Response>
```

Hereinafter, an interface of notifying a whitelist in the interface between the distribution messaging server and the address directory will be described.

The interface of notifying a whitelist is an interface that notifies the wihtelist (list of the transceiving entities and certified electronic mailing addresses of the sender/receiver that participate in the distribution system) to the transceiving entity.

A message exchange flow related with the whitelist notification is illustrated in Fig. 50.

The request distribution message structure will be described in the following Table 87 and an example of the message will be described in the following Table 88.

[Table 87]

Name of item	Description	Number of repetiti	Type	Length

				on		
Request			■ request Root element			
	BroadcastWlistReq		■ whitelist notifying request element			
		PeerInfo	■ transceiving entity information	1..∞		
			Name	■ real name of registrant (individual: name institution: business name)	1..1	String	Up to 128
			PeerCorpNum	■ business number of operator of belonged distribution messaging server	1..1	String	Up to 128
			CorpType	■ (general corporation:C, ASP business:A)	1..1	String	Up to 256
			RAddress	■ certified electronic mailing address	1..∞	String	minimum 1 up to 128
			Tel	■ Phone number (input without using '-')	0..1	Integer	minimum 9 up to 12

[Table 88]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
 <BoradcastWlistReq>
  <PeerInfo>
   <Name>Hong, Gildong</Name>
   <PeerCorpNum>22432456</PeerCorpNum>
   <CorpType>C</CorpType>
    <RAddress>#000-0000-0000</RAddress>
  </PeerInfo>
 </BroadcastWlistReq>
</Request>
```

A structure of the response distribution message will be described in the following Table 89 and an example of the message will be described in the following Table 90.

[Table 89]

Name of item		Description	Number of repetition	Type	Length
Response		■ Response Root element			
	BroadcastWlistRes	■ whitelist notifying response element			

		ResultCode	■ processing result - success: 1 - fail: 0	1..1	Boolean	-
		ErrorCode	■ error code (only when the processing result is failed (0), input corresponding error code)	0..1	String	256

In Table 89, it is noted that ResultCode is a simple acception processing result for the spam reporting message

[Table 90]

```
<Response xmlns="http://www.nipa.kr/eDocument_Circulation">
 <BroadcastWlistRes>
  <ResultCode>1</ResultCode>
 </BroadcastWlistRes>
</Response>
```

Hereinafter, an interface of notifying a blacklist in the interface between the distribution messaging server and the address directory server will be described.

The interface of notifying a blacklist (reception denial list) is an interface that notifies the blacklist to the transceiving entity. The notified blacklist is used to

manage the blacklist by the transceiving entity.

A message exchange flow related with the blacklist notification is illustrated in Fig. 51.

The request distribution message structure will be described in the following Table 91 and an example of the message will be described in the following Table 92.

[Table 91]

Name of item	Description	Number of repetition	Type	Length
Request	■ request Root element			
BroadcastBlistReq	■ blacklist notifying request element			
UserInfo	■ blacklist element	1..∞		
SpamPeerCorpNum	■ business number of operator of distribution messaging server that transmits spam	1..1	String	Up to 128
Name	■ real name of registrant (individual: name	0..1	String	Up to 128

				institution: business name)			
			RAddress	■ certified electronic mailing address	1..∞	String	minimum 1 up to 128
			Tel	■ Phone number (input without using '-')	0..1	Integer	minimum 9 up to 12

[Table 92]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
 <BoradcastBlistReq>
  <UserInfo>
   <SpamPeerCorpNum>32345633</SpamPeerCorpNum>
   <Name>Park, Insoo</Name>
   <RAddress>#000-0000-0000</RAddress>
  </UserInfo>
 </BroadcastBlistReq>
</Request>
```

A structure of the response distribution message will be described in the following Table 93 and an example of

the message will be described in the following Table 94.

[Table 93]

Name of item			Description	Number of repetition	Type	Length
Response			■ Response Root element			
	BroadcastBlistRes		■ spam report response element			
		ResultCode	■ processing result - success: 1 - fail: 0	1..1	Boolean	-
		ErrorCode	■ error code (only when the processing result is failed (0), input corresponding error code)	0..1	String	256

[Table 94]

```
<Response xmlns="http://www.nipa.kr/eDocument_Circulation">
 <BroadcastBlistRes>
  <ResultCode>1</ResultCode>
 </BroadcastBlistRes>
</Response>
```

[Connection interface between distribution messaging servers]

The distribution messaging server is basically connected with a distribution messaging server which is built by other transceiving entity or other electronic document provider in order to transmit/receive a message.

In addition to the above basic function, the distribution messaging server has a connection function that delivers the distribution certificate between the distribution messaging server of the third party storing institution provider and other messaging server in order to store the distribution certificate in the third party storing institution.

The connection interface between the distribution messaging servers is a protocol for transmitting/receiving a message and a distribution certificate between the messaging servers and classified by interfaces described in the following Table 95.

[Table 95]

Classification of Interface	Description of interface

Connection between distribution messaging server	message transmission	□ an interface that allows a distribution messaging server of a transmitter to transmit a message to a distribution messaging server of a receiver □ after receiving a message, the receiving distribution messaging server returns a reception certificate or an error message to the transmitting distribution messaging server as a response message
	distribution certificate delivery	□ an interface that allows a distribution messaging server of a message receiver to transmit a reading certificate to a distribution messaging server of a message transmitter □ when the message receiver reads the message, the receiving distribution messaging server transmits the reading certificate to the message transmitting messaging server □ the distribution messaging server that receives the distribution certificate returns a reception confirmation ACK or an error message as a response message

	Request to store distribution certificate	☐ an interface that allows a general distribution messaging server to request a distribution messaging server of a third party storing institution provider to store the distribution certificate ☐ the distribution messaging server built by the third party storing institution needs to built a service that receives the distribution certificate from the general distribution messaging server and store the distribution certificate in the third party storing institution ☐ general corporation/institution/personal distribution messaging server other than the third party storing institution provider does not build this service
	third party storing institution storing result delivery	☐ an interface that delivers the storage result (initial registration certificate) to a storing request distribution messaging server after the distribution messaging server of the third party storing institution provider stores the distribution certificate/distribution document

Details of the interfaces between the distribution messaging servers will be described below.

First, a common fact of the interfaces between the distribution messaging servers is as follows (1).

(1) Extension of MessageHeader of request and reponse message

The digital signature information of the transmitter needs to be delivered so as to be included in a SOAP message which is a first MIME Part of the message of the connection interface between the distribution messaging servers. Further, additional information (CorpNum, RValue) of the transmitter which is required to verify whether an owner of the certificate used for the digital signature of the SOAP message matches with the transmitter (VID verification) is also delivered to be included therein.

The additional information of the transmitter needs to be located at a lower level of the MessageHeader element in the SOAP message of the request and response message as an extension element (any ##other position).

The extension element structure will be described in the following Table 96 and a schema structure will be described in the following Table 97.

[Table 96]

Name of item		Description	Number of repetition	Type	Length
Extension		■ Extension element	1..1		
	CorpNum	■ business registration No. of transmitter	1..1	String	10
	RValue	■ RValue extracted from private key of transmitter certificate ■ RValue is encoded by Base64 to be input	1..1	String	28

[Table 97]

```
<eb:MessageHeader SOAP:mustUnderstand="1"
eb:id="MessageHeader" eb:version="2.0">
   <eb:From>
      <eb:PartyId eb:type="ecf_cd">123456789</eb:PartyId>
      <eb:Role>sender</eb:Role>
   </eb:From>
   <eb:To>
      <eb:PartyId eb:type="ecf_cd">567890123</eb:PartyId>
      <eb:Role>receiver</eb:Role>
    </eb:To>
```

```
    <eb:CPAId>urn:ecm-and-ecm-cpa</eb:CPAId>
    <eb:ConversationId>20001209-133003-
28572</eb:ConversationId>
    <eb:Service>>urn:ecm-service</eb:Service>
    <eb:Action>request</eb:Action>
   <eb:MessageData>

<eb:MessageId>20110210-170644Z-00057@127.0.0.18d1f96bf-9cd6-
4049-9fdb-a6c0ed9af46
7</eb:MessageId>
    <eb:Timestamp>2011-02-10T08:06:44.810Z</eb:Timestamp>
  </eb:MessageData>
  <eb:DuplicateElimination></eb:DuplicateElimination>
  <Extention>
   <CorpNum>2208203228</CorpNum>
  <RValue>asdfasdf</RValue>
 </Extention>
</eb:MessageHeader>
```

Hereinafter, a message transmitting interface in the interfaces between the distribution messaging servers will be described.

The message transmitting interface is used when one distribution messaging server transmits a message to the other distribution messaging server.

A message exchange flow in the message transmission is illustrated in Fig. 52.

A request format at the time of exchanging a message is illustrated in Fig. 53. In the entire message structure as illustrated in Fig. 53, a SOAP message is located in a first MIME Part, a request distribution message is located in a second MIME Part, and a document which is attached by the user is located in a third or subsequent MIME part.

The request distribution message structure will be described in the following Table 98 and an actual example will be described as follows.

[Table 98]

Name of item	Description	Number of repetition	Type	Length
Request	■ request Root element			
SendMsgReq	■ message transmitting request element			
DocType	■ type of distribution message - document: 0	1..1	Integer	1
Title	■ title of message	1..1	String	Up to

					256
	Text	■ body of message - may be encrypted as certificate of receiver by transmitter	0..1	String	-
	Sender	■ certified electronic mailing address of transmitter	1..1	String	Up to 128
	Receiver	■ certified electronic mailing address of receiver	1..1	String	Up to 128
	ReqConfirm	■ request reading certificate - unrequested: 0 - requested: 1	1..1	Integer	1
	IsEncrypted	■ encryption of message - plane text : 0 - cipertext : 1	1..1	Integer	1
	Identifier	■ unique identifier (UUID) of request distribution message	1..1	String	36

In Table 98, if the body is not necessary for the purpose of deliverying the document, the Text may be

omitted.

[Table 99]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
   <SendMsgReq>
        <DocType>0</DocType>
        <Title>document to be sent</Title>
        <Text>body of document to be sent</Text>
        <Sender>#000-0000-0000</Sender>
        <Receiver>#000-0000-0000</Receiver>
        <ReqConfirm>1</ReqConfirm>
        <IsEncrypted>0</IsEncrypted>
        <Identifier>b366ff65-16c8-4d9d-a0ba-
d76a2cc95ad2</Identifier>
   </SendMsgReq>
</Request>
```

A response format at the time of exchanging a message is illustrated in Fig. 54. In the entire message structure as illustrated in Fig. 54, a SOAP message is located in a first MIME Part, a response distribution message is located in a second MIME Part, and a reception certificate is located in a third MIME part. If an error occurs in the process of processing the request message, the third MIME Part is not generated.

The response distribution message structure will be described in the following Table 100 and an actual example will be described in the following Table 101.

[Table 100]

Name of item	Description	Number of repetition	Type	Length
Response	■ request Root element			
SendMsgRes	■ message transmitting response element			
DocType	■ type of distribution message - reception certificate : 1 - error : 9	1..1	Integer	1
RefIdentifier	■ unique identifier value (UUID) of request distribution message corresponding to response distribution message	1..1	String	36

		ErrorCode	■ error code (only when the type of distribution message is error (9), input corresponding error code)	0..1	String	256

In Table 100, if DocType is an error (9), the MIME Part 3 in which the reception certificate is located is not generated.

[Table 101]

```
<Response xmlns="http://www.nipa.kr/eDocument_Circulation">
  <SendMsgRes>
    <DocType>1</DocType>
    <RefIdentifier>b366ff65-16c8-4d9d-a0ba-
d76a2cc95ad2</Identifier>
  </SendMsgRes>
</Response>
```

Hereinafter, a distribution certificate delivering interface in the interface between the distribution messaging servers will be described.

The distribution certificate delivering interface is used when the distribution messaging server sends the

reading certificate to the other distribution messaging server. Further, the distribution certificate transmitting interface is used when the distribution relay server receives the request to send the electronic document, send the electronic document to the receiving distribution messaging server and then sends the received reception certificate to the sending request distribution messaging server as a response message.

A message exchanging flow related with the distribution certificate delivering processing is illustrated in Fig. 55.

A distribution certificate delivery request format is illustrated in Fig. 56. In the entire message structure as illustrated in Fig. 56, a SOAP message is located in a first MIME Part, a request distribution message is located in a second MIME Part, and a distribution certificate is located in a third MIME part.

The request distribution message structure will be described in the following Table 102 and an actual example will be described in the following Table 103.

[Table 102]

Name of item	Description	Number of	Type	Length

			repetition		
Request		■ request Root element			
	SendCertReq	■ distribution certificate delivering request element			
	DocType	■ type of distribution message - reception certificate: 1 - transmission certificate: 2 - reading certificate: 3	1..1	Integer	1
	Sender	■ certified electronic mailing address of transmitter of certificate	1..1	String	Up to 128
	Receiver	■ certified electronic mailing address of receiver	1..1	String	Up to 128
	Identifier	■ unique identifier (UUID) of request distribution message	1..1	String	36

		TargetIdentifier	■ unique identifier (UUID) of transmission request distribution message whose certificate needs to be issued	1..1	String	36

[Table 103]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
   <SendCertReq>
      <DocType>1</DocType>
      <Sender>#000-0000-0000</Sender>
      <Receiver>#000-0000-0000</Receiver>
      <Identifier>5347146a-3528-4469-8ef7-
9c346ab36d54</Identifier>
      <TargetIdentifier>b366ff65-16c8-4d9d-a0ba-
d76a2cc95ad2</TargetIdentifier>
   </SendCertReq>
</Request>
```

A distribution certificate transmission response format is illustrated in Fig. 57 (Fig. 57A illustrates the distribution certificate transmission response in case of being successful, Fig. 57B illustrates the distribution certificate transmission response in case of being failed).

In the entire message structure as illustrated in Fig. 57, if the processing for the request message is successful, only reception confirmation Acknowledgment SOAP message is located in a first MIME Part. In case of being an error, a SOAP message is located in the first MIME Part and error response message is located in a second MIME Part.

The response distribution message structure will be described in the following Table 104. Table 104 corresponds only when the processing result is failed.

[Table 104]

Name of item			Description	Number of repetition	Type	Length
Response			■ request Root element			
	SendCertRes		■ distribution certificate delivery response element			
		DocType	■ type of sending message - error : 9	1..1	Integer	1
		RefIdentifier	■ unique identifier (UUID) of request distribution message	1..1	String	36

			corresponding to response distribution message			
		ErrorCode	■ error code	1..1	String	256

Hereinafter, a distribution certificate storing request interface in the interface between the distribution messaging servers will be described.

The distribution certificate storing request interface is used when the distribution messaging server of the transceiving entity requests the distribution messaging server of the third party storing institution to store the distribution certificate in order to store the distribution certificate in the third party storing institution. In the response message in the interface, only reception confirmation information is included. An initial registration certificate which is issued as a result that the distribution certificate is stored in the third party storing institution is delivered to the storing request distribution messaging server using a "third party storing institution storing result delivering interface which will be described below.

A message exchanging flow related with the distribution certificate storing request processing is illustrated in Fig. 58.

A distribution certificate storing request format is illustrated in Fig. 59. In the entire message structure as illustrated in Fig. 59, a SOAP message is located in a first MIME Part, a request distribution message is located in a second MIME Part, and a distribution certificate is located in a third MIME part.

The request distribution message structure will be described in the following Table 105 and an actual example will be described in the following Table 106.

[Table 105]

Name of item	Description	Number of repetition	Type	Length
Request	■ request Root element			
RegCertReq	■ distribution certificate storing request element			
DocType	■ type of distribution message - reception certificate: 1 - transmission certificate: 2	1..1	Integer	1

			- reading certificate: 3			
		Sender	■ certified electronic mailing address of transmitter	1..1	String	Up to 128
		Receiver	■ certified electronic mailing address of receiver	1..1	String	Up to 128
		Identifier	■ unique identifier (UUID) of request distribution message	1..1	String	36

[Table 106]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
   <RegCertReq>
      <DocType>1</DocType>
      <Sender>#000-0000-0000</Sender>
      <Receiver>#000-0000-0000</Receiver>
      <Identifier>5347146a-3528-4469-8ef7-
9c346ab36d54</Identifier>
   </RegCertReq>
</Request>
```

A distribution certificate storing response format is illustrated in Fig. 60 (Fig. 60A illustrates the

distribution certificate storing response in case of being successful, Fig. 60B illustrates the distribution certificate storing response in case of being failed). In the entire message structure as illustrated in Fig. 60, if the processing for the request message is successful, only a reception confirmation Acknowledgment SOAP message is located in a first MIME Part. In case of being an error, a SOAP message is located in the first MIME Part and error response message is located in a second MIME Part.

The response distribution message structure will be described in the following Table 107. Table 107 corresponds only when the processing result is failed.

[Table 107]

Name of item	Description	Number of repetition	Type	Length
Response	■ request Root element			
RegCertRes	■ distribution certificate storing response element			
DocType	■ type of distribution message	1..1	Integer	1

			- error : 9			
		RefIdentifier	■ unique identifier (UUID) of request distribution message corresponding to response distribution message	1..1	String	36
		ErrorCode	■ error code	1..1	String	256

Hereinafter, a third party storing institution storing result delivering interface in the interface between the distribution messaging servers will be described.

The third party storing institution storing result delivering interface is used when the distribution messaging server of the third party storing institution provider stores the distribution certificate in the third party storing institution and then transmits the initial registration certificate which is received as the result to the distribution messaging server that requests to store the distribution certificate.

A message exchanging flow related with the third party storing institution storing result delivery processing is illustrated in Fig. 61.

A third party storing institution storing result

delivery format is illustrated in Fig. 62. In the entire message structure as illustrated in Fig. 62, a SOAP message is located in a first MIME Part, a request distribution message is located in a second MIME Part, and the first registration certificate is located in a third MIME part. If an error occurs in the process of storing the distribution certificate in the third party storing institution, the third MIME Part is not generated.

The request distribution message structure will be described in the following Table 108 and an actual example will be described in the following Table 109.

[Table 108]

Name of item		Description	Number of repetition	Type	Length
Request		■ request Root element			
	RegResultReq	■ third party storing institution storing result delivery processing request element			

		DocType	■ type of distribution message - initial registration certificate: 4 - error: 9	1..1	Integer	1
		Sender	■ certified electronic mailing address of transmitter	1..1	String	Up to 128
		Receiver	■ certified electronic mailing address of receiver	1..1	String	Up to 128
		Identifier	■ unique identifier (UUID) of request distribution message	0..1	String	Up to 128
		TargetIdentifier	■ unique identifier (UUID) of distribution certificate storing request distribution message which is a target of the request distribution messaging	1..1	String	Up to 128
		ErrorCode	■ error code (only when the type of	0..1	String	Up to

			distribution message is error (9), input corresponding error code)			256

In Table 108, if DocType is an error (9), the MIME Part 3 in which the initial registration certificate is located is not generated.

[Table 109]

```
-- successful
<Requuest xmlns="http://www.nipa.kr/eDocument_Circulation">
   <ReqResultReq>
      <DocType>4</DocType>
      <Sender>#000-0000-0000</Sender>
      <Receiver>#000-0000-0000</Receiver>
      <Identifier>dd27e2e2-4731-4da1-8043-
a250dcc8690c</Identifier>
      <TargetIdentifier>5347146a-3528-4469-8ef7-
9c346ab36d54</RefIdentifier>
   </regResultReq>
</Request>
```

```
-- error

<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
  <RegResultReq>
    <DocType>9</DocType>
    <Sender>#000-0000-0000</Sender>
    <Receiver>#000-0000-0000</Receiver>
    <TargetIdentifier>5347146a-3528-4469-8ef7-
9c346ab36d54</RefIdentifier>
    <ErrorCode>ERR-01-0001</ErrorCode>
  </RegResultReq>
</Request>
```

A third party storing institution storing result response format is illustrated in Fig. 63 (Fig. 63A illustrates the distribution certificate transmission response in case of being successful, Fig. 63B illustrates the distribution certificate transmission response in case of being failed). In the entire message structure as illustrated in Fig. 57, if the processing for the request message is successful, only a reception confirmation Acknowledgment SOAP message is located in a first MIME Part. In case of being an error, a SOAP message is located in the first MIME Part and error response message is located in a second MIME Part.

The response distribution message structure will be described in the following Table 110. Table 110 corresponds only when the processing result is failed.

[Table 110]

Name of item			Description	Number of repetition	Type	Length
Response			■ request Root element			
	RegResultRes		■ third party storing institution storing result delivery processing result element			
		DocType	■ type of distribution message - error : 9	1..1	Integer	1
		RefIdentifier	■ unique identifier (UUID) of request distribution message corresponding to response distribution message	1..1	String	36
		ErrorCode	■ error code	1..1	String	256

[Connection interface between distribution client and distribution messaging server]

The distribution messaging server needs to provide a basic document transceiving function to a user in connection with a system (distribution client) for a user (an internal sender/receiver or a certified sender/receiver) that requests actual electronic document distribution.

The connection interface between the distribution client and the distribution messaging server is a protocol that allows the distribution client to primarily communicate with the distribution messaging server in order to transmit and receive the electronic document and classified into interfaces as described in the following Table 111.

[Table 111]

Classification of Interface		Description of interface
Connection interface	Request to transmit message	□ an interface that allows a distribution client to request a distribution messaging server to transmit a message

between distribution client and distribution messaging server	Request message list	□ an interface for requesting a list of received message received in the distribution messaging server □ after authenticating the distribution client user, the distribution messaging server delivers the received message lists to the user
	Request details of message	□ an interface that allows the distribution client to request whole information for a specific received message to the user to the distribution messaging server □ after authenticating the distribution client user, the distribution messaging server delivers the whole information of the message requested by the user
	Report spam message	□ an interface that allows the distribution client to report a spam message □ after authenticating the distribution client user, the distribution messaging server delivers the contents reported by the user to the address directory server

	Search physical address information	□ an interface that allows the distribution client to search physical address information □ after authenticating the distribution client user, the distribution messaging server delivers the result of the request of the searching to the address directory server

Details of the interfaces between the distribution client and the distribution messaging server will be described below.

First, a common fact of the connection interfaces between the distribution client and the distribution messaging server is as follows (1).

(1) Extension of MessageHeader of request messages

The digital signature information of the user needs to be delivered so as to be included in a SOAP message which is a first MIME Part of a request message which is transmitted from the distribution client to the distribution messaging server. Further, additional user information (IDN, RValue) which is required for the distribution messaging server to verify whether an owner of the certificate used for the digital signature of the SOAP message matches with the corresponding user (VID

verification) is also delivered to be included therein.

Corresponding information needs to be located at a lower level of the MessageHeader element in the SOAP message of the request message as an extension element (any ##other position).

Further, individual authentication information for a plurality of internal users that uses the same certificate will be added.

The extension element structure will be described in the following Table 112 and an example of extension element will be described in the following Table 113.

[Table 112]

Name of item		Description	Number of repetition	Type	Length
UserInfo		■ Extension element	1..1		
	IDN	■ User identification No. - individual: resident registration number - business: business registration number	1..1	String	10

	RValue	■ RValue extracted from private key of user certificate ■ RValue is encoded by Base64 to be input	1..1	String	28
	Id	■ user ID registered in the distribution messaging server	0..1	String	Up to 20
	Password	■ user password registered in the distribution messaging server	0..1	String	8
	AuthType	■ authentication method of a plurality of internal users ■ method using ID, password is basically set to 0 ■ in order to authenticate the user using other method than the method using ID and password, AuthType value and lower extension element are autonomously defined to be used	1..1	Integer	1
	Any Extension	■ in order to authenticate the user using other method than the method using ID and	0..1	Any	-

		password, a new element is autonomously defined to be used■ ex> Token, Certificate			

[Table 113]

```
<eb:MessageHeader SOAP:mustUnderstand="1"
eb:id="MessageHeader" eb:version="2.0">
 <eb:From>
  <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-
cppa:partyid-type:duns">openAPI
_Sender</eb:PartyId>

<eb:Role>http://www.rosettanet.org/processes/3A4.xml#Buyer</
eb:Role>
 </eb:From>
 <eb:To>
 <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-
type:duns">openAPI_
Receiver</eb:PartyId>

<eb:Role>http://www.rosettanet.org/processes/3A4.xml#seller<
/eb:Role>
 </eb:To>
 <eb:CPAId>uri:openapi-and-openapi-cpa_mxs</eb:CPAId>
```

```
 <eb:ConversationId>uri:openapi-and-openapi-
cpa_mxs:0210050643</eb:ConversationId>
 <eb:Service>bpid:icann:rosettanet.org:3A4$2.0</eb:Service>
 <eb:Action>RequestRelaySend</eb:Action>
 <eb:MessageData>

<eb:MessageId>20110210-170644Z-00057@127.0.0.18d1f96bf-9cd6-
4049-9fdb-a6c0ed9af
467</eb:MessageId>
  <eb:Timestamp>2011-02-10T08:06:44.810Z</eb:Timestamp>
 </eb:MessageData>
 <eb:DuplicateElimination></eb:DuplicateElimination>
 <UserInfo>
  <IDN>2208203228</CorpNum>
  <RValue>asdfasdf</RValue>
  <Id>tester1</Id>
  <Password>test</Password>
  <AuthType>0</AuthType>
 </UserInfo>
</eb:MessageHeader>
```

Hereinafter, a message transmission request interface in a connection interface between the distribution client and the distribution messaging server will be described.

The message transmission request interface is used

when the distribution client transmits a message to the distribution messaging server in order to transmit a message through the distribution messaging server.

The message transmission processing flow of the distribution client is illustrated in Fig. 64.

A message transmission request format of the distribution client is illustrated in Fig. 65. In the entire message structure as illustrated in Fig. 65, a SOAP message is located in a first MIME Part and a request distribution message is located in a second MIME Part. If there is a document which is attached by the user, the document is located in a third or subsequent MIME part.

The request distribution message structure will be described in the following Table 114 and an actual example will be described in the following Table 115.

[Table 114]

Name of item		Description	Number of repetition	Type	Length
Request		■ request Root element			
	SendMsgReq	■ message transmitting request element			

		DocType	■ type of distribution message - document: 0	1..1	Integer	1
		Title	■ title of message	1..1	String	Up to 256
		Text	■ body of message - may be encrypted as certificate of receiver by transmitter	0..1	String	-
		Sender	■ certified electronic mailing address of transmitter	1..1	String	Up to 128
		Receiver	■ certified electronic mailing address of receiver	1..1	String	Up to 128
		ReqConfirm	■ request reading certificate - unrequested: 0 - requested: 1	1..1	Integer	1
		IsEncrypted	■ encryption of message - plane text : 0 - cipertext : 1	1..1	Integer	1
		Identifier	■ unique identifier (UUID) of request	1..1	String	36

			distribution message			

In Table 114, if the body is not necessary for the purpose of delivering the document, the Text may be omitted.

[Table 115]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
   <SendMsgReq>
       <DocType>0</DocType>
       <Title>document to be sent</Title>
       <Text>body of document to be sent</Text>
       <Sender>#000-0000-0000</Sender>
       <Receiver>#000-0000-0000</Receiver>
       <ReqConfirm>1</ReqConfirm>
       <IsEncrypted>1</IsEncrypted>
       <Identifier>b366ff65-16c8-4d9d-a0ba-
d76a2cc95ad2</Identifier>
    </SendMsgReq>
</Request>
```

A distribution client message transmission response format is illustrated in Fig. 66 (Fig. 66A illustrates the distribution certificate transmission response in case of being successful, Fig. 66B illustrates the distribution

certificate transmission response in case of being failed). In the entire message structure as illustrated in Fig. 66, if the processing for the request message is successful, only a reception confirmation Acknowledgment SOAP message is located in a first MIME Part. In case of being an error, a SOAP message is located in the first MIME Part and error response distribution message is located in a second MIME Part.

The response distribution message structure will be described in the following Table 116. Table 116 corresponds only when the processing result is failed.

[Table 116]

Name of item	Description	Number of repetition	Type	Length
Response	■ request Root element			
SendMsgRes	■ message transmission response element			
DocType	■ type of transmission message - error : 9	1..1	Integer	1

		RefIdentifier	■ unique identifier (UUID) of request distribution message corresponding to response distribution message	1..1	String	36
		ErrorCode	■ error code	1..1	String	256

Hereinafter, a message list request interface in the connection interface between the distribution client and the distribution messaging server will be described.

The message list request interface is used when the distribution client requests the list of the messages received in the distribution messaging server.

The message list processing flow of the distribution client is illustrarted in Fig. 67.

A message list request format of the distribution client is illustrated in Fig. 68. In the entire message structure as illustrated in Fig. 68, a SOAP message is located in a first MIME Part and a request distribution message is located in a second MIME Part.

The request distribution message structure will be described in the following Table 117 and an actual example will be described in the following Table 118.

[Table 117]

Name of item			Description	Number of repetition	Type	Length
Request			■ request Root element			
	MsgListReq		■ message list request element			
		Requester	■ certified electronic mailing address of requester	1..1	String	Up to 128
		MsgSize	■ number of lists of distribution messages	1..1	Integer	Up to 100

[Table 118]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
   <MsgListReq>
      <Requester>#000-0000-0000</Requester>
      <MsgSize>100</MsgSize>
   </MsgListReq>
</Request>
```

A message list response format of the distribution client is illustrated in Figure 67. In the entire message structure as illustrated in Figure 67, the SOAP message is

located in a first MIME Part and a response distribution message (list of distribution messages received in the distribution messaging server) is located in a second MIME Part.

The response distribution message structure will be described in the following Table 119 and an actual example will be described in the following Table 120.

[Table 119]

Name of item	Description	Number of repetition	Type	Length
Response	■ request Root element			
MsgListRes	■ message list response element			
ResultCode	■ processing result - successful: 1 - failed: 0	1..1	Boolean	-
ErrorCode	■ error code (input corresponding error code only when ResultCode is failed	0..1	Integer	1

		(0))			
List		■ received distribution message list	0..∞		
	DocType	■ type of distribution message - document: 0 - reception certificate: 1 - transmission certificate: 2 - reading certificate: 3 - storage certificate: 4 - error: 9	1..1	Integer	Up to 100
	Title	■ title of message	0..1	String	Up to 256
	Sender	■ certified electronic mailing address of transmitter	1..1	String	UP to 128
	Identifier	■ unique identifier	0..1	String	36

				(UUID) of distribution message			
			TargetIdentifier	■ when the type of distribution message is distribution certificate, unique identifier (UUID) of distribution message whose certificate is issued	0..1	String	36
			IsExistPayloads	■ presense of attached file - None: 0 - Present: 1	1..1	Integer	1
			IsEncrypted	■ encryption of message - planar text : 0 - ciphertext : 1	1..1	Integer	1
			SendDate	■ document transmission time	0..1	Long	-
			ReceiveDate	■ document reception time	0..1	Long	-

[Table 120]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
   <MsgListRes>
      <ResultCode>1</ResultCode>
      <List>
         <DocType>0</DocType>
         <Title>title of document</Title>
         <Sender>#000-0000-0000</Sender>
         <Identifier>e82fae92-981e-4d36-80b8-
ec16cb6b7993</Identifier>
         <IsExistPayloads>0</IsExistPayloads>
         <IsEncrypted>0</IsEncrypted>
         <SendDate>1286263498929</SendDate>
         <ReceiveDate>1286273498929</ReceiveDate>
      </List>
      <List>
         <DocType>9</DocType>
         <Sender>#000-0000-0000</Sender>
         <RefIdentifier>e82fae92-981e-4d36-80b8-
ec16cb6b7993</RefIdentifier>
         <IsExistPayloads>0</IsExistPayloads>
         <IsEncrypted>0</IsEncrypted>
      </List>
   </MsgListRes>
</Response>
```

Hereinafter, a message detailed information request interface in the connection interface between the distribution client and the distribution messaging server will be described.

The message detailed information request interface is used when the distribution client requests a specific message and an attached document received by the distribution messaging server.

The detailed information request processing flow of the distribution client is illustrated in Fig. 69.

A message detailed information request format of the distribution client is illustrated in Fig. 70. In the entire message structure as illustrated in Fig. 70, a SOAP message is located in a first MIME Part and a body of a request distribution message is located in a second MIME Part.

The request distribution message structure will be described in the following Table 121 and an actual example will be described in the following Table 122.

[Table 121]

Name of item	Description	Number of repeti	Type	Length

			tion		
Request		■ request Root element			
	MsgDetailReq	■ message detailed information request element			
		Requester	■ certified electronic mailing address of requester	1..1	String	Up to 128
		RefIdentifier	■ unique identifier (UUID) of distribution message to be requested	1..1	String	36

[Table 122]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
   <MsgDetailReq>
      <Requester>#000-0000-0000</Requester>
      <RefIdentifier>5f6d8126-a691-452b-b17a-
e3a8b8ce3ac5</RefIdentifier>
   </MsgDetailReq>
</Request>
```

A message detailed information response format is illustrated in Fig. 72. In the entire message structure as illustrated in Fig. 72, a SOAP message is located in a

first MIME Part and a response distribution message (detailed information of the distribution message) is located in a second MIME Part. If there is an attached document, the attached document is sequentially located in a third or subsequent MIME Part.

The response distribution message structure will be described in the following Table 123 and an actual example will be described in the following Table 124.

[Table 123]

Name of item	Description	Number of repetition	Type	Length
Response	■ request Root element			
MsgDetailRes	■ message detailed information response element			
DocType	■ type of distribution message - document: 0 - reception, transmission, reading	1..1	Integer	Up to 100

			certificate: 1, 2, 3 - storage certificate: 4 - error: 9			
		Title	■ message title	0..1	String	Up to 256
		Text	■ body of message	0..1	String	-
		Sender	■ certified electronic mailing address of transmitter	1..1	String	Up to 128
		Receiver	■ certified electronic mailing address of receiver	0..1	String	Up to 128
		ReqConfirm	■ request of reading certificate - unrequested: 0 - requested: 1	0..1	Integer	1
		IsEncrypted	■ encryption of message - planar text: 0 - ciphertext: 1	1..1	Integer	1
		Identifier	■ unique identifier (UUID) of distribution message	0..1	String	36
		TargetIdentifier	■ when the type of distribution message is	0..1	String	36

			distribution certificate, unique identifier (UUID) of distribution message whose certificate is issued			
		ErrorCode	■ error code (only when the type of distribution message is an error (9), input the corresponding error code)	0..1	Integer	1

[Table 124]

```
<Response xmlns="http://www.nipa.kr/eDocument_Circulation">
  <MsgDetailRes>
    <DocType>0</DocType>
    <Title>title of document</Title>
    <Text>body of document</Text>
    <Sender>#000-0000-0000</Sender>
    <Receiver>#000-0000-0000</Receiver>
    <ReqConfirm>1</ReqConfirm>
    <IsEncrypted>0</IsEncrypted>
    <Identifier>e82fae92-981e-4d36-80b8-
ec16cb6b7993</Identifier>
  </MsgDetailRes>
</Content>
```

Hereinafter, a spam message reporting interface in the connection interface between the distribution client and the distribution messaging server will be described.

The spam message reporting interface is used when the distribution client reports the spam message to the distribution messaging server. The distribution messaging server reports the spam message to the address directory server and then delivers the result to the distribution client.

The spam message report processing flow of the distribution client is illustrarted in Fig. 73.

A spam message reporting format of the distribution client is illustrated in Fig. 74. In the entire message structure as illustrated in Fig. 74, a SOAP message is located in a first MIME Part and a request distribution message is located in a second MIME Part.

The request distribution message structure will be described in the following Table 125 and an example of the message will be described in the following Table 126.

[Table 125]

Name of item	Description	Number of	Type	Length

			repetition		
Request		■ request Root element			
	ReportSpamReq	■ spam reporting request element			
	ReportRAddress	■ certified electronic mailing address of reporter	1..1	String	Up to 128
	SpamRAdderss	■ certified electronic mailing address of spam transmitter	1..1	String	Up to 128
	ContentsPid	■ reference ID of content file sent by spam transmitter(MIME Part cid of spam report message)	1..1	String	Up to 256
	AttacheFileInfo	■ information of attached document sent by spam transmitter			
	FilePid	■ reference ID of attached document sent by spam transmitter(MIME Part cid of spam report message)	1..1	String	Up to 256

[Table 126]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
  <ReportSpamReq>
    <ReportRAddress>#000-0000-0000</ReportRAddress>
    <SpamRAddress>#000-0000-0000</SpamRAddress>
    <ContentsPid>cid-1</ContentsPid>
    <AttacheFileInfo>
      <FilePid>cid-2</FilePid>
      <FileName>License.txt</FileName>
    </AttacheFileInfo>
    <SpamPeerCorpNum>1234567890</SpamPeerCorpNum>
  </ReportSpamReq>
</Request>
```

A spam message response format of the distribution client is illustrated in Fig. 75. In the entire message structure as illustrated in Fig. 75, the SOAP message is located in a first MIME Part and a response distribution message (list of distribution message received in the distribution messaging server) is located in a second MIME Part.

The response distribution message structure will be described in the following Table 127 and an example of the message will be described in the following Table 128.

[Table 127]

Name of item			Description	Number of repetition	Type	Length
Response			■ request Root element			
	ReportSpamRes		■ spam report response element	1..1		
		ResultCode	■ processing result - successful: 1 - failed: 0	1..1	Boolean	-
		RAddress	■ certified electronic mailing address of spam transmitter	0..1	String	minimum 1 up to 128
		ErrorCode	■ error code (input corresponding error code only when ResultCode is failed (0))	0..1	String	256

In Table 127, it is noted that ResultCode indicates a simple accepting result for the spam report message.

[Table 128]

```
<Response xmlns="http://www.nipa.kr/eDocument_Circulation">
  <ReportSpamRes>
    <ResultCode>1</ResultCode>
    <RAddress>#000-0000-0000</RAddress>
  </ReportSpamRes>
</Response>
```

Hereinafter, a physical address searching interface in the connection interface between the distribution client and the distribution messaging server will be described.

The physical address searching interface is used when the distribution client requests the distribution messaging server to search a physical address. The distribution messaging server searches the physical address and then delivers the result to the address directory server.

A message exchanging flow related with the physical address search processing is illustrated in Fig. 76.

A physical address searching request format is illustrated in Fig. 77. In the entire message structure as illustrated in Fig. 77, a SOAP message is located in a first MIME Part and a request distribution message is located in a second MIME Part.

The request distribution message structure will be described in the following Table 129 and a message example will be described in the following Table 130.

[Table 129]

Name of item	Description	Number of repetition	Type	Length
Request	■ request Root element			
SchAddrReq	■ search request element of certified electronic mailing address of a member			
ReqInfo	■ request certified electronic mailing address information element	1..∞		
RAddress	■ certified electronic mailing address	1..1	String	Up to 128
IsCert	■ request of certificate - requested: 1 - non requested: 0	1..1	Integer	1

[Table 130]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
  <SchAddrReq>
    <ReqInfo>
      <RAddress>#000-0000-0000</RAddress>
      <IsCert>0</IsCert>
    </ReqInfo>
  </SchAddrReq>
</Request>
```

A physical address searching response format is illustrated in Fig. 78. In the entire message structure as illustrated in Fig. 78, a SOAP message is located in a first MIME Part and a response distribution message (list of distribution messages received in the distribution messaging server) is located in a second MIME Part.

The response distribution message structure will be described in the following Table 131 and an actual example will be described in the following Table 132.

[Table 131]

Name of item	Description	Number of repetition	Type	Length

Response			■ request Root element			
	SchAddrRes		■ certified electronic mailing address searching response element			
		ResultCode	■ processing result - successful: 1 - failed: 0	1..1	Boolean	-
		ResultData	■ result list	0..∞		
		RAddress	■ certified electronic mailing address	1..1	String	Minimum 1 Up to 128
		IsExist	■ existence of address information (Attribute) - existed: 1 - not existed: 0	1..1	Integer	1
		Endpoint	■ physical address of certified electronic mailing address	0..1	String	Up to 256
		PeerRegNum	■ authentication No. of transceiving entity	0..1	String	10
		Cert	■ receiver certificate	0..1	Base64	-
		PeerCert	■ public key of transceiving	0..1	Base64	-

				entity			
			ErrorCode	■ error code (input corresponding error code only when ResultCode is failed (0))	0..1	String	256

It is noted that even when a search is normally performed for some or all of a plurality of RAddresses but when an error of non-existence of address occurs, ResultCode is input to be successful (1), which is different from the other interface.

* RAddress is described regardless of success (1)/failure (0) of ResultCode and whether RAddress is existed is input in IsExist which is attribute information

* Endpoint and Cert are input when a value of IsExist is existed (1)

* RAddress is not pharsed due to the error of the request message, RAddress may be omitted (as a result, Endpoint and Cert will be omitted)

* If ResultCode is input as failure (0), that is, other error than the error of non-existence of address occurs, ErrorCode inputs an error code corresponding to a cause of the error

[Table 132]

```
<Response xmlns="http://www.nipa.kr/eDocument_Circulation">
  <SchAddrRes>
    <ResultCode>1</ResultCode>
    <ResultData>
      <RAddress IsExist="1">#000-0000-0000</RAddress>

<Endpoint>http://111.111.111.111:8080/imxs/msh</Endpoint>
      <Cert>MFJIFDjfksdfjsl...</Cert>
    </ResultData>
  </SchAddrRes>
</Response>
```

[Connection interface between distribution messaging server and distribution relay server]

The distribution relay server is a system that sends an electronic document by proxy for the transmitting distribution messaging server when an error occurs in the process of directly sending the electronic document between the distribution messaging servers in the electronic document distribution system so that the sending is failed.

The distribution relay server is managed by National Industry Promotion Agency and all distribution messaging servers may be supported in connection with the distribution relay server when an error occurs in P2P distribution process.

The connection interface between the distribution messaging server and the distribution server is a protocol that allows the distribution messaging server to request the distribution relay server to transmit an electronic document and classified into an interface described in the following Table 133.

[Table 133]

Classification of Interface		Description of interface
Transmission by proxy	Request to transmit message	□ an interface that allows a distribution messaging server of a transmitter to request the distribution relay serve to transmit a transmission message by proxy when an error occurs in the process of transmitting a message due to a system or a network environment of the receiver □ distribution relay server returns a transmission certificate evidencing that the distribution messaging server of the transmitter tries to transmit as a response message

First, a common fact of the connection interfaces between the distribution messaging server and the

distribution relay server is as follows (1).

(1) Extension of MessageHeader of request messages

The digital signature information of the distribution messaging server needs to be delivered so as to be included in a SOAP message which is a first MIME Part of the connection interfaces between the distribution messaging server and the distribution relay server. Further, additional information (CorpNum, RValue) of the distribution messaging server which is required for the distribution messaging server to verify whether an owner of the certificate used for the digital signature of the SOAP message matches with the corresponding messaging server (VID verification) is also delivered to be included therein.

Additional information of the distribution messaging server needs to be located at a lower level of the MessageHeader element in the SOAP message as an extension element (any ##other position).

The extension element structure will be described in the following Table 134 and an example of extension element will be described in the following Table 135.

[Table 134]

Name of	Description	Number	Type	

item			of repetition		Length
Extension		■ Extension element	1..1		
	CorpNum	■ Business registration number of transmitter	1..1	String	10
	RValue	■ RValue extracted from private key of certificate of transmitter ■ RValue is encoded by Base64 to be input	1..1	String	28

[Table 135]

```
<eb:MessageHeader SOAP:mustUnderstand="1"
eb:id="MessageHeader" eb:version="2.0">
  <eb:From>
    <eb:PartyId eb:type="ecf_cd">123456789</eb:PartyId>
    <eb:Role>sender</eb:Role>
  </eb:From>
  <eb:To>
    <eb:PartyId eb:type="ecf_cd">ech</eb:PartyId>
    <eb:Role>receiver</eb:Role>
  </eb:To>
  <eb:CPAId>urn:ech-and-ecm-cpa</eb:CPAId>
```

```
  <eb:ConversationId>20001209-133003-
28572</eb:ConversationId>
  <eb:Service>>urn:ech-service</eb:Service>
   <eb:Action>request</eb:Action>
<eb:MessageData>

<eb:MessageId>20110210-170644Z-00057@127.0.0.18d1f96bf-9cd6-
4049-9fdb-a6c0ed9af46
7</eb:MessageId>
    <eb:Timestamp>2011-02-10T08:06:44.810Z</eb:Timestamp>
  </eb:MessageData>
  <eb:DuplicateElimination></eb:DuplicateElimination>
  <Extention>
    <CorpNum>2208203228</CorpNum>
    <RValue>asdfasdf</RValue>
  </Extention>
</eb:MessageHeader>
```

Hereinafter, a message transmission request interface in the connection interface between the distribution messaging server and the distribution relay server will be described.

The message transmission request interface is used to request the distribution relay server for the message transmission and issue the transmission certificate when a

reception error occurs at the other distribution messaging server in the process of transmitting a message from the distribution messaging server to the other distribution messaging server. The distribution relay server immediately returns the accepting result for the message transmission request of the distribution messaging server and transmits the reception certificate which is received after transmitting a message to the receiving distribution messaging server to the transmission request distribution messaging server using the above-described "distribution certificate transmission interface".

The message relay processing flow is illustrated in Fig. 79.

A message relay request message format is illustrated in Fig. 80. In the entire message structure as illustrated in Fig. 80, a SOAP message is located in a first MIME Part and a request distribution message is located in a second MIME Part. If there is a document which is attached by the user, the document is located in a third or subsequent MIME part.

The request distribution message structure will be described in the following Table 136 and an actual example will be described in the following Table 137.

[Table 136]

Name of item			Description	Number of repetition	Type	Length
Request			■ request Root element			
	SendMsgReq		■ message transmitting request element			
		DocType	■ type of distribution message - document: 0	1..1	Integer	1
		Title	■ title of message	1..1	String	Up to 256
		Text	■ body of message - may be encrypted as certificate of receiver by transmitter	0..1	String	-
		Sender	■ certified electronic mailing address of transmitter	1..1	String	Up to 128
		Receiver	■ certified electronic mailing address of receiver	1..1	String	Up to 128
		ReqConfirm	■ request reading certificate	1..1	Integer	1

			- unrequested: 0 - requested: 1			
		IsEncrypted	■ encryption of message - plane text : 0 - cipertext : 1	1..1	Integer	1
		Identifier	■ unique identifier (UUID) of request distribution message	1..1	String	36

In Table 136, if the body is not necessary for the purpose of delivering the document, the Text may be omitted.

[Table 137]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
  <SendMsgReq>
    <DocType>0</DocType>
    <Title>document to be sent</Title>
    <Text>body of document to be sent</Text>
    <Sender>#000-0000-0000</Sender>
    <Receiver>#000-0000-0000</Receiver>
    <ReqConfirm>1</ReqConfirm>
    <IsEncrypted>0</IsEncrypted>
    <Identifier>b366ff65-16c8-4d9d-a0ba-
d76a2cc95ad2</Identifier>
```

```
  </SendMsgReq>
</Request>
```

A message relay response message format is illustrated in Fig. 81. In the entire message structure as illustrated in Fig. 81, the SOAP message is located in a first MIME Part, a response distribution message is located in a second MIME Part, and a transmission certificate is located in a third MIME Part. If an error occurs in the process of processing the request message, the third MIME Part is not generated.

The response distribution message structure will be described in the following Table 138 and an actual example will be described in the following Table 139.

[Table 138]

Name of item		Description	Number of repetition	Type	Length
Response		■ request Root element			
	SendMsgRes	■ response for message transmission request			

		DocType	■ type of distribution message - transmission certificate: 2 - error: 9	1..1	Integer	1
		RefIdentifier	■ unique identifier (UUID) of request distribution message corresponding to response distribution message	1..1	String	36
		ErrorCode	■ error code (input corresponding error code only when a type of distribution message is an error (9))	0..1	String	256

In Table 138, if DocType is an error (9), the third MIME Part in which the transmission certificate is located is not generated.

[Table 139]

```
<Request xmlns="http://www.nipa.kr/eDocument_Circulation">
  <SendMsgRes>
    <DocType>2</DocType>
```

```
    <RefIdentifier>b366ff65-16c8-4d9d-a0ba-
d76a2cc95ad2</Identifier>
  </SendMsgRes>
</Request>
```

Hereinafter, another example of the electronic document distribution system and electronic document distribution method using the same according to the exemplary embodiment of the present invention as described above will be described in detail.

[Structure of electronic document distribution system and electronic document distribution process]

The electronic document is distributed based on P2P communication that allows corporation/institution that observes the standard for reliable distribution to directly transmit/receive the electronic document to each other. A basic element of the electronic document distribution system according to the present invention for performing the P2P communication is a distribution messaging server system based on the standard that supports the distribution between the address directory server that manages address information and each transceiving entity. If only the address directory server and the distribution messaging server system are provided, a basic structure that allows

the corporation or institution to distribute the electronic document is equipped. Further, a distribution certificate for certifying the document distribution between the senders/receivers is issued and is simultaneously stored in the third party storing institution (certified electronic document storing institution) to establish a legal basis for the distribution.

In addition to the basic element, the electronic document distribution system according to the present invention includes a distribution client application (APP) that suppies a user interface for document transceiving function so as to allow a general user (corporation/institution, individual) to easily distribute document, an electronic document form register that provides a standard document format in order to increase convenience of creating a document, and a public sector connection gateway for relaying an administrative institution with the electronic document as additional configuration elements.

A basic process that is performed in the above-mentioned electronic document distribution system will be described in the following Table 140.

[Table 140]

classification	process	remarks

Registration and management of address information	Registration of address information	Basic process
	Changing of address information	Basic process
	Searching of address information	Basic process
P2P document distribution between transceiving entities	Electronic document transmission and reception confirmation between transceiving entities	Basic process
	Electronic document transceiving request between actual user and distribution messaging server of transceiving entity	Basic process
	Request to issue distribution certificate and store in certified electronic document depository	Basic process
	Search and download	Selective process

	electronic document form between distribution client APP and electronic document form register	
	Request certified electronic document depository to store transmitted/received document	Selective process
Electronic document distribution between public sector/administrative sector and corporation/individual user	Document distribution via public connection gateway	Document is distributed by public connection gateway when public sector/administrative institution is hard to built distribution system in accordance with standard of distribution messaging server

[Component of electronic document distribution system]

The elements of the electronic document distribution system will be more systematically described below.

In order to establish the electronic document distribution, first "(1) a transceiving entity" which is a principal agent of the distribution needs to be present and the transceiving entity needs to include "(2) a distribution messaging server system" that observes the distribution messaging server standard in order to distribute the document. Further, "(3) an address directory server" which is a basic configuration of the electronic document distribution and registers and manages a certified electronic mailing address of the transceiving entity and a user needs to be present.

Based on the above basic configuration, "(4) a distribution client APP" is provided in order to provide a convenience of the distribution to the user and "(5) a public sector connection gateway" that supports to connect the administrative/public institution and "(6) an electronic document form register" that manages a form of the document are additionally provided.

Hereinafter, the above-mentioned components will be described in detail.

(1) transceiving entity

Among base infra components of the electronic document distribution, a unit which is a criterion of the distribution is the transceiving entity. The transceiving entity serves as a sender or a receiver in accordance with a role that participates in the distribution and these entities distribute the document (information) through the distribution messaging server system in accordance with a distribution protocol.

All transceiving entities that participate in the distribution build a distribution messaging server system that is capable of transceiving a document in accordance with the distribution messaging standard and then registers physical address information of the distribution messaging server system in the address directory server to create a base for participating in the electronic document distribution. In this case, each transceiving entity has an actual distribution user having at least one certified electronic mailing address at a lower level.

An entity that is recognized as a transceiving entity in the electronic document distribution is limited to an entity that builds a system observing the messaging server standard and then receives the authentication of standard compatibility and interoperability by National Industry Promotion Agency. In order to evidence the distribution,

(1) after distributing the electronic document through the authenticated transceiving entity, (2) the distribution certificate needs to be issued in accordance with the standard and stored in a third party storing institution.

In this case, the transceiving entity is classified into an entity that is responsible to directly transmit the electronic document as a legal owner and a person in charge for the electronic document and an entity that acts as a proxy for a user who is an actual owner and a person in charge of the distributing electronic document. In this case, if the owner of the electronic document is a transceiving entity that directly transmits the electronic document, only by receiving the authentication of the standard compatibility and the interoperability of the distribution messaging server system and stably storing the distribution certificate in the third party storing institution, the owner of the electronic document may participate in the distribution as the transceiving entity.

In contrast, if the transceiving entity is responsible to transmit the electronic document by proxy for the owner (user) of the electronic document as a third party, the transceiving entity needs to prove that the tranceiving entity stably and reliably manages the transmission message and manages and authenticates the user information. In order to secure the stability and

reliability of the third party distribution, temporally, the transceiving entity that performs the third party distribution is limited only to the third party storing institution provider.

(2) Distribution messaging server system

The distribution messaging server system needs to build a message transceiving function and a function of searching address information concerning a receiver and security related information in connection with the address directory server in order to distribute the electronic document (information) based on the distribution messaging server standard. The distribution messaging server system physically has one electronic mailing address (IP address) but may issue or manage a plurality of user account for lower level users and each user account has one certified electronic mailing address.

The distribution messaging server system needs to manage electronic document mail box for every user account in order to manage the user accounts and distribution messaging server system has responsibility for stable and reliable electronic document distribution as a representative for the user accounts.

In order to participate in the electronic document distribution as a transceiving entity, the distribution

messaging server system is authentified whether the requirements according to this invention are appropriately implemented and there is no problem in the interoperation with other solution.

The authentifying system that authenticates the standard compability and the interoperability for the distribution messaging server system manages the authenticated transceiving entity. Further, if the address directory server requests to confirm whether to be authentified in the process of registering the certificated electronic mailing address, the authentifying system returns the result.

The distribution messaging system is authenticated and registered by the certificated electronic mailing address in accordance with the following process as illustrated in Fig. 82.

First, a corporation/institution or an individual user which serves as a transceiving entity builds a distribution messaging server system in accordance with a technical standard.

Next, the standard compatibility and the interoperability of the built distribution messaging server system is authenticated by an automatic verifying equipment provided by an authentication test bed.

Next, the transceiving entity whose verification is

completed requests the authentication test bed for the authentication test.

Next, if the result of the authentication for the system in accordance with the test process of the authentication test bed is "pass", the transceiving entity prepare a next procedure for registering the certified electronic mailing address.

Next, the authentication test bed delivers information concerning the transceiving entity that passes the authentication examination to the address directory server and the address directory server utilizes the information as a condition of address registration.

Next, the transceiving entity requests the address directory server to issue a unique ID in order to register the authenticated distribution messaging server system.

Next, if the distribution messaging server system is completely registered in the address directory server, the distribution messaging server system may participate in the electronic document distribution.

Next, after completely authenticating the distribution messaging server system, the user account is open. In the case of representative certified electronic mailing address, the user account is requested to be registered in the certified electronic mailing address.

(3) Address directory server

In order to participate in reliable electronic document distribution, all users need to receive a unique electronic mailing address.

(4) Distribution client APP

The distribution client APP refers to an application that provides an UI such as document transmission and reception, received document reading, and management for the users who participate in the document distribution. The distribution client APP does not independently transmit/receive the document but needs to be connected with the distribution messaging server system.

A document which is created or attached by the distribution client APP is delivered to the users using the distribution messaging server system, the documents received through the distribution messaging server system are searched. If the distribution messaging server system manages the transceiving mail box through the user account, the distribution client APP may access to only the corresponding document among the received documents by checking the user account information.

The distribution client APP may be implemented as a C/S type application or a web type screen in accordance with the request of the user.

(5) Public sector connection gateway

An administrative or public institution which cannot accept the electronic document distribution performs a function that relays the administrative or public institution with a private enterprise, institution, or individuals under the electronic document distribution system through a public sector connection gateway.

(6) Electronic document form register

Users who wants to transmit an electronic document using the distribution messaging server system may directly create a document to be transmitted using Office tools. The electronic document form register is a system that support the management such as the registration and management of the document format, searching, reading, and downloading of the document format so as to be used by a user application such as the distribution client APP while registering and managing the standard document format so as to support to allow the user to easily create the electronic document.

The electronic document form register provides a server engine that manages the document standard format and a standard interface that allows a client application (APP) to search and download the document standard format and

then plugged-in an internal program to use the document standard format.

[Electronic document distribution method]

A whole process for distribution an electronic document in the electronic document distribution is largely divided into "(1) a prior preparation step before the distribution", "(2) an electronic document distribution step", "(3) an evidencing step for distribution". Hereinafter, the above-mentioned three steps will be described in detail. Further, a document transceiving method", "a distribution evidencing method", and "a spam message processing method" will be described in detail.

(1) Prior preparation step before distribution

-A manager of the electronic document form register registers a standard document form to be used using the electronic document form register.

-A transceiving participant determines whether to autonomously build a distribution messaging server system for reliable distribution or open a user account in a previously built distribution messaging server system to use the distribution messaging server system. If the distribution messaging server system is autonomously built for reliable distribution, a distribution messaging server

system for transceiving the electronic document is built and then an authentication test is performed for the standard compatibility and interoperability of the distribution messaging server system through an authentication institution. Thereafter, the transceiving participant accesses to the address directory server to apply and receive a transceiving entity ID for an authenticated distribution messaging server system, and then autonomously registers and manages an internal identifier for an internal actual user and plugs-in a standard document form creating function in the client application for a document creating function based on the standard document form (optional). In contrast, if a transceiving entity that includes a distribution messaging server system in which third party distribution is allowed is used, the transceiving participant requests to open a user account for a corporation/institution/individual through the distribution messaging server system and then registers certified electronic mailing address information for the user account in the address directory server. Thereafter, the transceiving participant plugs-ins a standard document format creating function in the client application in order for a general user to use the document creating function based on the standard document form (optional).

(2) Electronic document distribution step

o Document transmitter

- A document transmitter selects a document to be distributed or creates a document to be transmitted using a word processor.

- Address information of the other party who receives the document and a document to be delivered, whether to encrypt the document and whether to do digital signature is selected (encryption and the digital sigunature are performed on an attached delivery document rather than the transmission message and this processes are optional)

-The distribution client APP acquires physical address information and public key information for encryption based on a certified electronic mailing address of a receiving party in connection with the address directory server (optionally, if the distribution client APP does not acquire the physical address, the distribution messaging server performs this process)

- The distribution client APP requests the transmission to the distribution messaging server based on the address information of the receiver (both physical address information and the certified electronic mailing address are available)

o Distribution messaging server of transmitter

- If the transmission request message requested in the distribution client APP is not the physical address information for the receiver, the distribution messaging server inquires physical address information for a transceiving entity of the receiver based on the certified electronic mailing address to the address directory server.

- The electronic document is packaged as a message structure defined in a distribution protocol standard.

-Digital signature is performed on the message based on the certificate of the distribution messaging server of the transmitter.

- The message is sent the receiver based on the physical address information of terminal.

o Distribution messaging server of receiver

- After receiving a message, the message is verified and then a document is extracted from the message.

- The message including a reception certificate is sent to the transmitter as a synchronous response.

(3) Evidencing step for distribution

- A receiver creates a "reception certificate" at a time of receiving a document for confirmation of reception of the document and delivers the reception certificate to the transmitter. The transmitter that receives the reception certificate stores the reception certificate in

the third party storing institution.

If there is a request from a transmitter, the receiver delivers the received document to an actual person in charge of the document (user) and then creates a "reading certificate" at a time when the person in charge checks the received document to deliver the reading certificate to the transmitter. The document transmitter that receives the "reading certificate" stores the "reading certificate" in the third party storing institution (the reading certificate is issued only when there is a request from the transmitter).

-When the transmitter tries to deliver a document to the receiver but the trial is failed, the transmitter requests an electronic document distribution hub which is an objective third party in order to evidence the transmission trial and the electronic document distribution hub that receives the transmission request issues a "transmission certificate" in order to evident the reception of the transmission request and delivers the transmission certificate to a transmission requestor. The transmission requester who receives the transmission certificate stores the "transmission certificate" in the third party storing institution.

○ Document transceiving method

The transmitter and the receiver electronically distribute the document through the distribution messaging server system. The distribution messaging server system transmits/receives the electronic document in accordance with the distribution protocol. All messages are configured by combination of transmission and reception confirmation (or reception certificate) messages for reliable message distribution and the physical address information for the receiver is acquired through the address directory server.

○ Distribution verification method

"Distribution verifying" refers verification of events regarding transmission, reception, or reading related with the electronic document distribution using a reliable method. In this case, a certificate that is issued for an action related with the electronic document distribution is collectively referred to as a "distribution certificate".

The distribution messaging server system issues a distribution certificate at a time of transmission and reception in order to evidence the action for transmission and reception and stores the issued distribution certificate in the third party storing institution so as to be utilized as an evidential material for the distribution

action.

The distribution messaging server system evidences events for transmitting, receiving, and reading the electronic document and creates distribution certificates for the events. The distribution certificate includes identification information of the distribution certificate, creating time and expiring time of the distribution certificate, a policy of the distribution certificate, and a distribution evidencing target.

The distribution certificate for the transmission of the electronic document is created by the electronic document distribution hub and the distribution evidencing target includes identification information of a transmitter, identification information of a receiver, distribution identification information, document identification information, and an electronic document transmission request time.

The distribution certificate for the reception of the electronic document is created by a receiver who receives the electronic document and the distribution evidencing target includes identification information of a transmitter, identification information of a receiver, distribution identification information, document identification information, electronic document transmitting time, and an electronic document receiving time.

The distribution certificate for the reading of the electronic document is created by a user who checks the reception of the electronic document and the distribution evidencing target includes identification information of a transmitter, identification information of a receiver, distribution identification information, document identification information, electronic document transmitting time, an electronic document receiving time, and an electronic document checking time.

The distribution certificate created as described above is digitally signed by NPKI or GPKI certificate and the created distribution certificate is delivered to the electronic document transmitter. All distribution certificates are preferably stored in the third party storing institution.

○ Spam message processing method

The electronic document distribution has an infrastructure in which basically, the transmitter transmits the electronic document through a certified distribution messaging server system and a receiver also receives the electronic document based thereon so that the transmitter is responsible therefor. However, the spam transmitter may open a user account in the distribution messaging server system and transmit an electronic document

using the same. Further, a current authentication system authenticates only technical contents of the system. Therefore, if a spam transmitter builds a distribution messaging server system, technically authenticates the distribution messaging server system, and then uses the distribution messaging server system as a spam transmitting unit, it is difficult to block any attempt at an initial stage.

Therefore, in order to solve the above problems, in the standard document distribution infra according to the present invention, whitelist based on the authentication list management and blacklist system based on the spam target list management in accordance with the user reporting method are provided and a process that allows the receiver to deny the reception by this system is applied to prevent the spam message.

Functions of reporting the spam message and checking a transmitting party are essential and thus all distribution messaging servers need to necessarily build these functions.

If a receiver judges that the received message is a spam message, the receiver reports the spam message to the address directory server of the electronic document distribution hub in accordance with the process illustrated in Fig. 83 and a processing procedure related therewith is

as follows.

First, if the receiver judges that the message is a spam message at a time of receiving the message, the receiver reports the message to the address directory server through the distribution messaging server system as a spam message.

Next, the address director serve that accepts the report of the spam message from the distribution messaging server system returns a confirmation message indicating the acceptation.

Next, National IT Industry Promotion Institution that is a principal agent that manages the address directory server analyzes the message and investigates the transmitter to examine and determine whether to add the certified electronic mailing address of the transmitter as blacklist.

Next, if the transmitter is determined as a blacklist candidate, the address director server adds the corresponding certified electronic mailing address to the blacklist and then notifies the addition to the blacklist to the transmitter.

Next, the address directory server delivers the processing result for the spam message request to the spam reportor (receiver).

In the above-mentioned processing procedure, only

information for a messaging server system which is authenticated and formally registered is recorded in the whitelist. In contrast, when an address of the transmitter is registered as a spam transmitter, the address is registered in the blacklist. If the spam address which is registered in the blacklist through the same distribution messaging server system is repeatedly generated, the electronic document distribution hub determines whether to cancel the authentication for the corresponding messaging server system and then cancels the authentication and deletes the spam address from the whitelist.

When a message is received, the receiver checks the whitelist and the blacklist of the address directory server in order to confirm whether the transmitting party is a reliable and legal user to determine whether to deny the reception. A transmitter checking method includes a realtime checking method at the time of reception and a periodical checking method that checks the transmitter through a list which is managed in a type of cache in the distribution messaging server of the receiver.

In the process of checking the transmitter in realtime basis, as illustrated in Fig. 84, at a time when the receiver receives the message, it is determined whether the address of the transmitter is registered in the whitelist or blacklist in the address directory server and

then determines whether to deny the reception. The details of checking the transmitter in the realtime basis will be described below.

First, if a message is received, the distribution messaging server system of the receiver delivers a checking request message to the address directory server in order to check whether the transmitter is a legal user.

Next, the address directory server checks whether the address information of the requested user is included in the whitelist.

Next, if the address is not in the whitelist, the address directory server immediately returns a result message indicating that the requested user is non-registered user to the checking requester. If the address is included in the whitelist, the address directory server checks whether the corresponding address is registered in the blacklist.

Next, the address directory sserver returns a result message whether to be registered in the blacklist to the checking requester.

Next, if the receiver receives a result message indicating that the transmitter is not a legal user (not included in the whitelist or registered in the blacklist) from the address directory server, the receiver autonomously processes the received message as a spam

message and then records and stores the processing result message received from the address directory server and the reception records of spam message.

Next, the processing record of the spam message needs to be stored one month or longer so as to confirm the legitimacy of the reception denial against the corresponding transmitter.

Further, in the process of periodically checking the transmitter, as illustrated in Fig. 85, the receiver receives the whitelist and the blacklist from the address directory server in advance, autonomously manages the whitelist and the blacklist, and determines whether that the address of the transmitter is registered in the whitelist and the blacklist based thereon to determine whether to deny the reception of the message. The details of the process of periodically checking the transmitter will be described below.

First, the distribution messaging server system of the receiver requests a latest whitelist and a latest blacklist to the address directory server in advance and autonomously manages the whitelist and the blacklist. In this case, if the list is changed, whether to request the automatic notification is delivered. Even though the automatic notification of the changed matter of the list is requested, a request for importing a latest list in the

address directory server is periodically performed so that the difference of the list information is at most one day.

Next, if the whitelist and the blacklist are changed, the address directory server broadcasts the changed details to a user who requests the notification of the change.

Next, the distribution messaging server system of the user who receives the changed matters for the list modifies information of the list which is autonomously managed to synchronize the list.

Next, if the message is received, the receiver checks the list which is autonomously managed in order to check whether to be a legal user to the address directory server.

Next, if it is determined that the transitter is not a legal user (not included in the whitelist or registered in the blacklist) as a result of checing the list which is autonomously managed, the receiver autonomously processes the received message as a spam message and records and stores the receiving record of the spam message.

Next, the processing record for the spam message needs to be stored one month or longer so as to confirm the legitimacy of the reception denial against the corresponding transmitter.

[Distribution messaging server system]

Hereinafter, a distribution messaging server system

of the electronic document distribution system according to an exemplary embodiment of the present invention as described above will be described in detail.

The distribution messaging server system is largely configured by message transmission, message reception, mail box management of a received message, message security (user authentication, document encryption/decoding), transceiving record management, address directory server connection, message verification, an internal system connection interface, issuance and management of a distribution certificate, and connection of third party storing institution.

Fig. 86 illustrates a configuration of the distribution messaging server system. Referring to Fig. 86, components (1) to (9) of the distribution messaging server system will be described in detail as follows.

(1) Message transmission/reception

- A message is transmitted and received in accordance with a distribution protocol.

(2) Account (mailbox) management for every user

- A transmitted or received message is stored in a mailbox for every account in accordance with the user account or an internal identifier.

- For the transmitted document stored in the mail box, four stage status information including "in the process of transmitting", "transmission completed", "transmission failed", and "reception completed by a person in charge" is managed. In this case, a status of "in the process of transmitting" refers to a status when no response is received from the receiver after transmitting a document, a status of "transmission completed" refers to a status when the "reception certificate" is received from the distribution messaging server system of the receiver, a status of "transmission failed" refers to a status when SOAP Fault message is returned due to an error occurring inside of the receiving distribution messaging server system or a network error occurs in the transceiving process, and a status of "reception completed by a person in charge" refers to a status when the transmitting distribution messaging server system receives a "reading certificate" evidencing that the person in charge checks the document from the receiver.

- For the received document stored in the mailbox for every user account, four stage status information including "verification error", "before reception confirmation", "reception confirmation", and "reading confirmation" is managed. In this case, a status of "verification error"

refers to a status when an error occurs in verification of basic structure of received message, a status of "before reception confirmation" refers to a status before a person in charge of the received document reads a list of received documents in the mailbox, a status of "reception confirmation" refers to a status when the person in charge of the received document has read the list of the received document in the mailbox, and a status of "reading confirmation" refers to a status when the person in charge of the received document has read the details of the received document and the distribution messaging server system of the receiver issues a "reading certificate" at this time and then delivers the "reading certificate" to the transmitter.

- If deleting request is received from the reception user, the corresponding received document is physically deleted.

- In the mailbox, the transmitted document, reception confirmation message for transmission, and reception confirmation message of a person in charge of reception has connection information so as to be connected to each other.

(3) Address directory server connection

- The distribution messaging server system manages address information in accordance with the address

information registering and searching process provided by the address directory server.

- The distribution messaging server system includes a client function that is capable of calling a service provided by the address directory server. In other words, the distribution messaging server system provides a service client function that remotely calls the address information registering, searching, editing, and deleting functions provided by the address directory server.

(4) Message security (user authentication, document encryption/decoding)

- The distribution messaging server system basically performs the message security function (message digital signature, signature verification) suggested by the distribution protocol.

(5) Transmitting/receiving record management

- The distribution messaging server system necessarily stores/manages the transmitting/receiving records at least one year or longer.

- Information on the transmitting/receiving records to be stored includes a transmitting record and a receiving record. The transmitting record includes a message id, a related message id, a transmitter (including a user

account), a receiver, a transmitting time, and a hashed value for the transmitted document. The receiving record includes a transmitter, a receiver (including a user account), a reception time, and a hashed value for the received document.

(6) Distribution certificate issuance and management

- The distribution messaging server system issues and manages the distribution certificate so as to evidence the contents for the document transmitting and receiving event.

- The issued distribution certificate is requested to be stored in a third party storing institution as soon as the certificate is delivered so as to assure reliability.

- After issuing the distribution certificate, the distribution messaging server system manages the record of the distribution certificate stored in the third party storing institute. The issuing record of the distribution certificate includes a distribution certificate id, a distribution certificate issuing time, a related message id, an original of the distribution certificate (optional), and storage key information which is received after storing the distribution certificate in the third party storing institution.

(7) Message packaging process (Packaging, Parsing,

Extracting)

- The distribution messaging server system packages the transmitting document as a message structure defined in the distribution protocol before transmitting the transmitting document.

- The distribution messaging server system parses (syntactic analyzes) the received document by the message structure defined in the distribution protocol and extracts necessary information.

(8) Request to store distribution certificate

- In order to request to store the distribution certificate, a general transceiving entity transmits a third party storing institution storing request message to a distribution messaging server system of a third party storing institution (remote storing request).

- If the certificated electronic document depository storing request message is received, the distribution messaging server system of a third party storing institution calls a storing request client to store the distribution certificate in the third party storing institution.

- If the distribution messaging server system of the third party storing institution directly creates the distribution certificate, the distribution messaging server

system of the third party storing institution directly calls the storing request client of the third party storing institution (local storing request)

- The client for requesting to store the distribution certificate requests the third party storing institution to store the distribution certificate in accordance with the transceiving connection interface standard of the third party storing institution.

(9) Additional service

- The distribution messaging server system distributes the distribution client APP management and manages a version thereof.

- The distribution messaging server system performs the message distribution management (record or statistic information).

- The distribution messaging server system performs system management (system monitoring or environmental information).

- The distribution messaging server system performs document form management.

If the distribution messaging server system according to the present invention including the above-mentioned components (1) to (9) is applied to a third party storing institution as illustrated in Fig. 87, when the

distribution certificate is stored, the distribution certificate storing request module calls an connection interface client developed in accordance with a third party storing institution connection interface standard to request to store the distribution certificate.

If the distribution messaging server system according to the present invention including the above-mentioned components (1) to (9) is applied to a general transceiving entity (general business entity) as illustrated in Fig. 88, the distribution certificate is stored by a method that transmits a message requesting to store the distribution certificate to the distribution messaging server system of the third party storing institution provider and receives the processing result.

A process that directly distribute between a transmitter and a receiver using the distribution messaging server system according to the present invention including the above-mentioned components (1) to (9) is configured by four steps including "(1) acquiring physical information and security information for a receiver", "(2) transmitting a message and confirming the transmission", "(3) confirming reception of a task receiver", and "(4) issuing and storing a distribution certificate". The four steps will be described in detail with reference to Fig. 89.

(1) Acquisition of physical address and security information for a receiver

- A system of the transmitter requests the physical address information and the security information (if reception password for the transmission message is required) to which an actual message is delivered based on the address information of the other party to the address directory server to acquire the physical address information and the security information.

- After the distribution client APP requests the physical address information and the security information for the receiver to the address directory server, the physical address information of the receiver is delivered to the distribution messaging server.

- The Address information for the receiver may be acquired only using an id (for example, resident registration number or business registration number) for the user, which is available only when the receiver allows the transmitter to search the address information based on id.

If the transmitter already knows the physical address information and the security information of the receiver, this process may be omitted.

(2) Message transmission and transmission

confirmation

After packaging the message in accordance with the distribution protocol standard, the transmitter performs the digital signature based on the certificate of the distribution messaging server system.

- The distribution messaging server system transmits the message which is packaged in the previously acquired physical address and digitally signed.

- The distribution messaging server system that receives the message verifies a basic packaging structure, the validity of the digital signature and the suitability for the transmitter (refers to "2.4.6. Message verification" for details for the verification) and then creates a reception certificate for reception confirmation or an error message.

- The receiving distribution messaging server system transmits the created response message to the transmitter.

- The transmission and transmission confirmation processes are configured by synchronlus message processing.

(3) Comfirmation Reception of a task receiver

- If the transmitters requests a reading confirmation message of a person in charge of a task receiver at the time of transmitting a message, the receiver necessarily creates a reading certificate for evidencing the reading

confirmation of a person in charge to deliver the reading certificate to the transmitter at the time of confirming the reception of the message on business.

- If the receiver sends a reading certificate message for reading confirmation of a person in charge to the message transmitter, the message transmitter transmits synchronously the reception confirmation message.

(4) Issuance and storage of Distribution certificate

- If an evidence for the distribution for every step is required, the transmitter issues certificates for reception, reading, and transmission in accordance with the steps and stores the certificate in the third party storing institution to assure a ground of the legal evidence for the distribution.

The process of directly distributing the message between the transmitter and the receiver using the distribution messaging server system according to the present invention performs "(5) error processing" in addition to the above-mentioned "(1) acquiring physical address and security information for a receiver", "(2) transmitting a message and confirming the transmission", "(3) confirming reception of a task receiver", and "(4) issuing and storing a distribution certificate". Referring to Figs. 90 to 92, details an error processing function

will be described below.

(5) Error processing function

All message transceiving processes of the distribution messaging server system are based on synchronous process. Therefore, since all errors for the transmission are checked by the transmitter, basically the message is retransmitted. The same message is resent by setting the same MessageId value so that the receiver may notice the redundant message even when an error occurs in the process of transmitting the reception confirmation message after successfully receiving the message.

The distribution messaging server system follows the processing flowchart as illustrated in Fig. 90 even when the transmission of the request message is failed. In other words, when a transmission error occurs due to the network error in the process of transmitting the message by the message transmitter, if the transmitter receives an error message such as an HTTP error, the transmitter requests to retransmit the same message. Only when the transmitter receives the reception confirmation message, the transmitter recognizes that the transmission is successful.

The distribution messaging server system follows the processing flowchart as illustrated in Fig. 91 when the

reception of the response message is failed. In other words, even though the message is normally delivered to the receiver, if the transmitter does not receive the reception confirmation message from the receiver, the transmitter recognizes as transmission failure error and retransmits the same message to the receiver with the same MessageId. If the MessageId of the received document is identical to the previously received message, the receiver sends the reception confirmation message as redundancy reception and performs internal processing..

When the error message reception is failed, the distribution messaging server system follows the processing flowchart as illustrated in Fig. 92. In other words, even though the message which is transmitted from the transmitter to the receiver is correctly delivered, when an error message is received as a response due to the error of the transmission message, the transmitter differently processes the message in accordance with the type of the error. However, the MessageId of the message which is transmitted in accordance with the re-request does not need to be the same but may be varied depending on the business situation.

"(1) A message transceiving function", "(2) a received message mailbox managing function", "(3) a message security function", "(4) a transceiving record managing

function", "(5) an address directory server connecting function", "(6)a message verifying function", "(7) a internal system connecting interface function", and "(8) a distribution certificate issuing and managing function" which are essentially required in the distribution messaging server system according to the present invention as described above will be described in detail as follows.

(1) Message transceiving

A basic process of transceiving the message by the distribution messaging server system follows the "document transceiving method of the "electronic document distribution method" according to the present invention as described above. A message exchanging type which is a basis for transceiving the message is based on the synchronous response of the message distribution protocol and a configuration of a transmission message and a reception confirmation message, transmission message and a reception error message, a transmission message and a business response message (including a meaning of reception confirmation message) may be formed.

A message transceiving type includes two types including a combination of the transmitting and reception confirmation response messages and a combination of transmitting and business response messages.

A processing flow when the message transceiving type is the combination of the transmitting and reception confirmation response messages is illustrated in Fig. 93. The transmission message and the reception confirmation (or reception error) message is configured by the combination of SOAP (Simple Object Access Protocol) Request-Response and the transmission message and a response message thereof are connected by inserting the MessageId of the transmission message in a RefToMessageId of the response message to be sent and details thereof will be described with reference to [distribution protocol] which will be described below.

A processing flow when the message transceiving type is the combination of the transmitting and business response messages is illustrated in Fig. 94. The transmission message and the response message including the reception confirmation (or reception error) message is configured by the combination of SOAP Request-Response. After the receiver receives the message and then creates a response document which is processed on business in connection with the internal system in realtime basis, the response document and the reception confirmation ACK message are included in the response message to be delivered to the transmitter. The transmission message and a response message thereof are connected by inserting the

MessageId of the transmission message in a RefToMessageId of the response message to be sent and details thereof will be described with reference to [distribution protocol] which will be described below.

A structure of the transceived message has a MultiPart-MIME structure as illustrated in Fig. 95. A SOAP message is inserted in a first MIME Part and a document to be transmitted is inserted in a second or subsequent MIME part.

A SOAP Envelope configured by a SOAP header and a SOAP Body is inserted in the first MIME. Message header information for transceiving a message, digital signature, a reception confirmation message, a synchronous transmission mark, and an error message are inserted in the SOAP Header. Further, in the second MIME part, a document (information) to be delivered to the message receiver is inserted. If the reception confirmation message of a person in charge is delivered, the document is inserted in this position. In the third MIME Part, if there are two or more documents (information) to be delivered to the message receiver, the documents are sequentially inserted in the third or subsequent MIME part.

(2) Received message mailbox management

If a message is received, the distribution messaging

server system stores the received messages in the mailbox for every account. The reception message mailboxes are divided for one or more user accounts to store and manage the messages. The reception message mailbox needs to provide an interface that performs a required process in accordance with the request of the user (existence of the new received message, reading of the received message, downloading of the received message, and deletion of the received message) and returns the result in a standardized manner.

In order to qualify the user account managed by the distribution massaging server system as a certified electronic mailing address included in the electronic document distribution, the distribution messaging server system needs to satisfy certification requirements in order to have a reliable user account (the requirements will be defined by separate evaluation guideline and currently, it is recognized that only third party storing institution satisfies the certification requirements).

Therefore, a method of allowing an individual or a corporation (institution) to acquire the certified electronic mailing address in the electronic document distribution includes the following two methods. A first method is a method of autonomously building a distribution messaging server system and authenticating the distribution

messaging server system to register an acquired transceiving entity ID in the address directory server. A second method is a method of opening a mailbox in a transceiving entity that additionally satisfies the requirement to have a reliable user account in the authenticated distribution messaging server system to receive a user ID and then register the user ID in the address directory server.

(3) Message security

The security for the transmission message is divided into digital signature for securing integrity and encryption/decoding for securing confidentiality. The message which is transmitted through the distribution messaging server system is divided into a SOAP message and an attached document. In this case, the attached document is already encrypted in the distribution client APP and only header information for transceiving a message is included in the SOAP Envelope so that additional encrypting process is not performed in the distribution messaging server system but the digital signature process for preventing forgery is performed in the message transceiving process. The digital signature method and a detailed procedure refer [distribution protocol] which will be described below.

(4) Transceiving record management

The distribution messaging server system needs to manage transceiving record information in order to check the record when a conflict or an issue related to the transmission/reception is caused in the future. The record information may include not only information regarding the transceiving action but also actual transmission/reception document. If an actual document is stored in the third party storing institution, only the registration certificate received from the third party storing institution may be stored rather than an original of the document.

(5) Address directory server connection

The distribution messaging server system is connected with the address directory server using the service connection interface provided by the address directory server. The address directory server provides two kinds of address searching services, an address registering service, and an address changing service. The distribution messaging server system essentially provides function of a "searching service of physical address related to the certified electronic mailing address" among the address searching services.

In addition to the searching service, whether to use the address registering service and the address changing service is determined depending on whether to use the user account which is registered/managed at a lower level by the distribution messaging server system as a certified electronic mailing address of the corporation or individual. If the user account which is registered/managed by the distribution messaging server system is authenticated so as to be registered as the certified electronic mailing address, since the distribution messaging server system perfoms the registering and changing service for the certified electronc mailing address by proxy, the corresponding service of the address directory service is connected.

(6) Message verification

When the distribution messaging server system transmits/receives a message, the receiver verifies the validity of the message at the time of receiving the message, and likes the process illustrated in Fig. 96, after verifying the validity of the message, only when the message passes the verification, the receiver delivers the message reception confirmation message to the transmitter. Otherwise, the receiver transmits an error message for the received message.

Verification target: Schema verification of the received message (verifies whether the received message is correctly packaged in accordance with the distribution protocol), verification of integrity of message (digital signature value of the received message is verified so as to verify that the message is perfect without being forged), and message transmitter verification (it is verified whether owner of the certificate used for the digital signature is identical to the transmitter of the message in order to authenticate whether the transmitter who performs the digital signature on the message is identical to the transmitter represented on the message).

(7) Internal system connecting interface

The distribution messaging server system provides a standardized interface for transceiving in order to allow an internal system to transmit and receive a document through the distribution messaging server system. Details of the interface will be described with reference to [distribution client APP] which will be described below.

(8) Distribution certificate issuance and management

Basic conditions of the distribution certificate are that (1) the distribution certificate is created by the transmission and receiving distribution messaging server

system, (2) the distribution certificate is created by performing digital signature based on GPKI and NPKI certificates, and (3) the distribution certificate is created based on the electronic document distribution action (in this case, if one or more electronic documents are delivered while the electronic document is distributed once, one distribution certificate is created and an ID is assigned so as to identify the corresponding distribution in order to distribute one electronic document and the distribution certificate is created by the distribution based thereon).

When the distribution certificate is issued, it is considered that (1) since a serial number of the distribution certificate is created by individual transceiving entities, 20 byte random number is used in order to give an uniqueness, which is different from the standard of the existing certificate, (2) the update and revocation of the distribution certificate are not defined, (3) a system time of the distribution messaging server system that creates the distribution certificate and the distribution client APP always maintains the current time, and (4) the distribution certificate policy uses only OID and names defined in the technical standard.

The distribution certificate issuing process is illustrated in Fig. 97 and a type of the distribution

certificate and essential information required to create the distribution certificate are described in the following Table 141 and a method of acquiring the essential information of the distribution certificate will be described in the following Table 142.

[Table 141]

Type	Principal agent of creation/time	Purpose	Essential information
Reception certificate	Receiving distribution messaging server system/immediately after reception	Prevention of denial that the receiver receives the message	Document information, transmitter, receiver, transmitting time by transmitter, receiving time by receiver
Reading certificate	Receiving distribution messaging server system/immediately after being read	Prevention of denial that the receiver reads the	Document information, transmitter, receiver, transmitting

	by a person in charge	received message	time by transmitter, receiving time by receiver, reading time by receiver
Transmission certificate	Electronic document distribution hub/immediately after receiving a transmitting request message	Evidence of transmission trial of the transmitter	Document information, transmitter, receiver, transmission request time by transmitter

[Table 142]

type	Essential information	Creating method
Reception certificate	Document information, transmitter, receiver, transmitting time	Use field value in distribution message transmitted by the transmitter

	by transmitter	
	receiving time by receiver	Use time of receiving distribution messaging server system
Reading certificate	Document information, transmitter, receiver, transmitting time by transmitter	Use field value in distribution message transmitted by the transmitter
	receiving time by receiver, reading time by receiver	Use time in receiving distribution messaging server system
Transmission certificate	Document information, transmitter, receiver	Use field value in distribution message transmitted by the transmitter
	transmission request time by	Use time of electronic

	transmitter	document distribution hub system

The distribution certificate is created by the transceiving entity and digitally signed using the NPKI and GPKI certificates of the transceiving entity. As a basic structure of the distribution certificate, a SignedData structure of CMS standard is used and a contents identifier which is equal to the certificate is used.

contentType of the distribution certificate is as follows.

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 }

A basic field of the distribution certificate is as follows.

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
    }
```

Details of the basic field of the distribution certificate as described above will be described below.

(1) version

-version indicates a version of the structure of the distribution certificate. The version is set to v2 for the distribution certificate and dataHash is used in a target field.

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

(2) Serial Number

-Serial number indicates identification information of the distribution certificate. The distribution certificate is created by the transceiving entity that receives the electronic document so that an identification number of serial number style is useless. Further, when

the distribution client of the transceiving entity is reinstalled, it is difficult to maintain the serial number.

Therefore, the identification information of the distribution certificate uses 20 byte random number. Accordingly, in order to process the distribution certificate, it should be possible to process 20 byte random number.

SerialNumber ::= INTEGER

(3) Issuer, Issuer of certificate

- A certificate identification value of an issuer that issues the distribution certificate is input. A value of thie field needs to have the same value as SubjectName field in the certificate of a signing person who digitally signs the distribution certificate.

(4) dateOfIssue, Date of issuing certificate

- dateOfIssue indicates a time when the issuer issues the distribution certificate.

(5) dateOfExpire, Expiration date of certificate

- dateOfExpire refers to the expiration date of the distribution certificate.

(6) Policy, Certificate policy

- policy refers to the policy of the distribution certificate. A policy OID in all distribution certificates are varied in accordance with the type of the certificate and only a value that is stored in the technical standard is used.

- The distribution certificate has one OID in accordance with the type of the certificates in a lump.

- A Qualifier value is represented in UserNotice > ExplicitText > DisplyText as a UTF8String type and a specified sentence is used.

- Policy information represented in the following Table 143 is used in accordance with the type of the distribution certificates.

[Table 143]

Type of certificate	Policy OID	Qualifier
Transmission certificate	1.2.410.200032.2.?.1	Transmission certificate
Reception certificate	1.2.410.200032.2.?.2	Reception certificate

Reception confirmation certificate	1.2.410.200032.2.?.3	Reception confirmation certificate

(7) requestInfo, Certificate request message information

- This field is set to be null.

RequestInfo ::= CHOICE {

arcCertRequest ARCCertRequest,

null NULL }

(8) Target, Target of evidencing

- Hashed values of all distributed electronic documents are specified. This field necessarily uses distributionInfos method. The structure for opRecord and orgAndIssued, dataHash fields refers "certificate format and operating procedure technical standard" of the third party storing institution.

- Information on the distributed electronic document is included in a DistributionInfos field.

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             GeneralNames,
        receiverAdd           GeneralNames,
        dateOfSend            GeneralizedTime,
        dateOfReceive         [0] EXPLICIT
GeneralizedTime OPTIONAL,
        dateOfReceiveConfirm  [1] EXPLICIT
GeneralizedTime OPTIONAL,
        distributionId        INTEGER,
        numberOfFiles         INTEGER,
        distributedFileInfos  DistributedFileInfos}
```

(1)-1 senderAdd, certified electronic mailing address

- This field indicates a certified electronic mailing address of the transmitter.

(1)-2 receiverAdd, certified electronic mailing address of receiver

- This field indicates a certified electronic mailing address of the receiver.

(1)-3 dateOfSend, transmitting date and time

- This field indicates a time when the transmitter transmits the electronic document.

- In case of transmission certificate, dateOfSend specifies a time when the transmitter requests the transmission to the electronic document distribution hub.

- The transmission certificate includes only this field, but does not include dateOfReceive and dateOfReceiveConfirm.

(1)-4 dateOfReceive, receiving date and time

- This field indicates a time when the receiver receives the electronic document. This time needs to be equal to or prior to the time when the certificate is created. The reception certificate and the reading certificate need to include this field. In contrast, the transmission certificate does not include this field.

(1)-5 dateOfReceiveConfirm, reading date and time

- This field indicates a time when the receiver receives and checks the electronic document. This time needs to be equal to or later than the receiving date and time and equal to or prior to the time when the certificate is created. The reading certificate needs to include this field. In contrast, the transmission certificate and the reception certificate do not include this field.

(1)-6 distributionId, distribution identification value

- This field indicates an identification value for the distribution of the electronic document. In order to

create this field, 20 byte random number is created and used. This field value indicates an identification value which is assigned to the distribution message for the electronic document distribution.

(1)-7 numberOfFiles, number of distributed files

- One or more electronic documents may be delivered in the distribution and this field indicates a number of files which are delivered in one distribution.

(1)-8 distributedFileInfos, distribution document information

- One or more electronic documents may be delivered in the distribution and information for all documents to be delivered needs to be included in this field.

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

(1)-8-1 fileHashedData, file hashed information

- This field indicates a hashed value for a distributed and delivered electronic document.

(1)-8-2 fileId, file identification value

- When an identification value is assigned to the electronic document to be distributed, an identification

value for the corresponding document is designated. A file identification value is created by the transmitter and needs to be delivered together when the electronic document is delivered to the receiver. The receiver applies the delivered file identification value to this field.

- The transmitter creates this field using uuid method.

- This field may be selectively used but if the fileName field is not used, this field is necessarily used and use of field is recommended.

(1)-8-3 fileName, fine name

- This field indicates a file name of the electronic document to be distributed. A file name is designated by the transmitter and needs to be delivered together when the electronic document is delivered to the receiver. The receiver applies the delivered file identification value to this field.

- This field may be selectively used but if the fileID filed is not used, this field is necessarily used.

The consistency criteria related with the time information of the distribution certificate described above will be described in the following Table 144.

[Table 144]

Number	Field	Contents
1	dateOfSend	Transmitting date and time/transmitting request date and time
2	dateOfReceive	Receiving date and time
3	dateOfReceiveConfirm	Reading date and time
4	dateOfIssue	Certificate issuing date
5	dateOfExpirre	Expiration date of certificate

An order of time information is transmitting date and time < receiving date and time ≤ reading date and time ≤ issuing date of certificate < expiration date of certificate. When the distribution certificate is verified, the above order needs to be checked.

The verification of the distribution certificate includes verification of certificate structure, verification of digital signature of certificate, checking of main fields of certificate, and verification of consistency of time information of certificate.

Verification of certificate structure is a process of verifying whether the certificate is same as defined in ASN.1.

Verification of digital signature of certificate is a process of verifying the digital signature applied to the

distribution certificate.

Checking of main fields of certificate includes checking of a version field checking whether a version field value is v2, checking of a target field checking whether the target field is hashData, issuer information verification verifying whether DN of a certificate used for the digital signature is identical to DN of a basic field of the certificate, checking of requestInfo field checking whether a requestInfo field is Null, checking of extension field checking whether distributionInfos extension field is existed and critical is TRUE, checking of number of files checking whether a value of numberOfFiles field is equal to the number of DistributedFile in distributionInfos extension field, checking of target field hashed value checking whether the hashed value of the target field is equal to the hashed value of the distributionInfos extension field, and verification of consistency of time information verifying in accordance with the consistency verification criteria of the time information.

Verification of consistency of time information of certificate verifies based on consistency verification criteria of the time information of the distribution certificate.

In the meantime, the distribution certification refers to an action certificating the fact of transmission,

reception, and reception confirmation occurring in the process of distributing the electronic document using a reliable method. The distribution certification is performed in a separate application program but is not performed in a distribution certificate viewer and the distribution certification API. If the distribution certification is performed additionally to the verification of the distribution certificate, the followings will be performed.

- Verification of distribution certificate: the distribution certificate is verified.

- Checking of policy of distribution certificate: a distribution certificate policy OID and a Qualifier value for transmission, reception, and reception confirmation are checked.

- Checking of transmitter's address: Whether the address of the transceiving entity that transmits the electronic document is correct is checked.

- Checking of receiver's address: Whether the address of the transceiving entity that receives the electronic document is correct is checked.

- Checking of transmitting date and time: Whether the time when the transmitter transmits the electronic document is correct is checked.

- Checking of receiving date and time: Whether the

time when the receiver receives the electronic document is correct is checked.

- Checking of reception confirmation date and time: Whether the time when the receiver confirms the reception of the electronic document is correct is checked.

- Checking of distribution ID: Whether the distribution ID which is assigned to individual distribution cases is correct is checked. If the transmitter and the receiver separately store and manage the distribution IDs, the distribution IDs may be compared and managed.

- Checking of identifier or fine name of distribution file: Whether an ID or a name of the file to be distributed is correct is checked. If the transmitter and the receiver separately store and manage the file IDs and the file names, the file IDs and the file names may be compared and managed.

- Checking of hashed value of distribution file: Whether the hashed values of the files to be distributed are equal to the values of DistributedFile field of the extension field is checked. In this case, the hash algorithm which is designed in the distribution certificated is used to compare the hashed value and the field value.

In the meantime, a profile of the distribution certificate will be described in the following Table 145.

It should be considered to apply RSA 2048bit and SHA256 algorithms to the digital signature, necessarily include the certificate in the signedData structrure, and include only one signerInfor in signerInfos field.

[Table 145]

Basic field	contents	remarks
Version	Version	V2
serialNumber	Serial number	20 byte random number
dateOfIssue	Date of issuance	GeneralizedTime
dateOfExpire	Date of expiration of certificate	GeneralizedTime
Policy	Policy of certificate	OID: 1.2.410.200032.2.?.?
requestInfo	Certificate request message information	Null
Target	Evidencing target	Use distributionInfos structure
senderAdd	Certified	

	electronic mailing address of transmitter	
receiverAdd	Certified electronic mailing address of receiver	
dateOfSend	Date of transmission	GeneralizedTime, essential
dateOfReceive	Date of reception	GeneralizedTime, optional
dateOfReceiveConfirm	Date of reception confirmation	GeneralizedTime, optional
distributionId	Distribution identifier	20 byte random number
numberOfFiles	Number of distributed files	
distributedFileInfos	Distributed file information	One or more distributedFile
DistributedFile		
fileHashedData	File hashed	SHA256

	value	
fileId	File Id	One of fileID and filename is essential
filename	File name	

In the method that connects the distribution certificate with the third party storing institution as described above, the distribution certificate is requested to be stored in the third party storing institution as soon as the distribution certificate is issued so as to assure the reliability of the issued distribution certificate.

In the case of the distribution messaging server system of the third party storing institution provider, the distribution certificate storing process is illustrated in Fig. 98. The third party storing stitution connection module directly requests to directly store distribution certificate issued from the distribution messaging server system in the third party storing institution. The third party storing institution connection module is configured by a distribution certificate storing request module and a third party storing institution connection interface client module. The distribution certificate is stored in the third party storing institution in accordance with the existing third party storing institution connection interface module standard.

In the case of the distribution messaging server system of a general transceiving entity, the distribution certificate storing process is illustrated in Fig. 99. In order to request the third party storing institution providers to store the issued distribution certificate, a request message is delivered to the distribution messaging server system of the third party storing institution provider. The distribution messaging server system of the third party storing institution provider that receives the storing request from the outside requests to store the distribution certificate in the third party institution through the third party storing institution connection module. The third party storing institution connection module requests the third party storing institution to store the distribution certificate in accordance with the existing third party storing institution connection interface module standard.

The detailed processing that the transceiving entity stores the distribution certificate in the third party storing institution is illustrated in Fig. 100 and the details will be described below.

o Distribution certificate registrant

- When the distribution certificate is stored in the third party storing institution, a storing agent may be appointed by an agreement between the third party storing

institution provider and the transceiving entity. The storing agency stores the distribution certificate using certificate in the third party storing institution.

o Type of storing request process of third party storing institution

- The third party storing institution provider may provide at least one of synchronous processing and asynchronous processing and the distribution messaging server is connected in accordance with a method provided by the third party storing institution provider to be connected

- Case 1: A synchronous processing process (when a transmitter requests to store the distribution certificate, all processes of issuing the registration certificate after completely registering the distribution certificate in the third party storing institution are synchronously performed so that the distribution messaging server of the transmitter receives the registration certificate as a synchronous response message. Since the response message for the request is a final registration result of the third party storing institution, if an error for the storing request occurs, reprocessing is performed by the distribution messaging server of the transmitter)

- Case 2: An asynchronous processing process (if a transmitter requests the third party storing institution

distribution messaging server to store the distribution certificate, the third party storing institution distribution messaging server verifies the validity of the request message first and then accepts the storing request. The third party storing institution provider needs to deliver the registration certificate which is registered in the third party storing institution to be issued in accordance with the storing request message to the distribution messaging server of the transmitter which is a first storing requestor. Since the third party storing institution provider is responsible to register the registration certificate in the third party storing institution for the accepted storing request, if a storage error occurs, the reprocessing is also performed by the third party storing institution provider)

[Distribution protocol]

Hereinafter, a distribution protocol which is applied to the electronic document distribution system and method according to the exemplary embodiment of the present invention as described above will be described in detail.

In the description of the distribution protocol which is applied to the electronic document distribution system and method according to the exemplary embodiment of the present invention, "(1) message packaging", "(2) message

envelope configuration", and "(3) HTTP binding" will be described in this order.

(1) Message packaging

The message structure of the distribution protocol applies the ebMS v2.0 standard and has two logical MIME Parts.

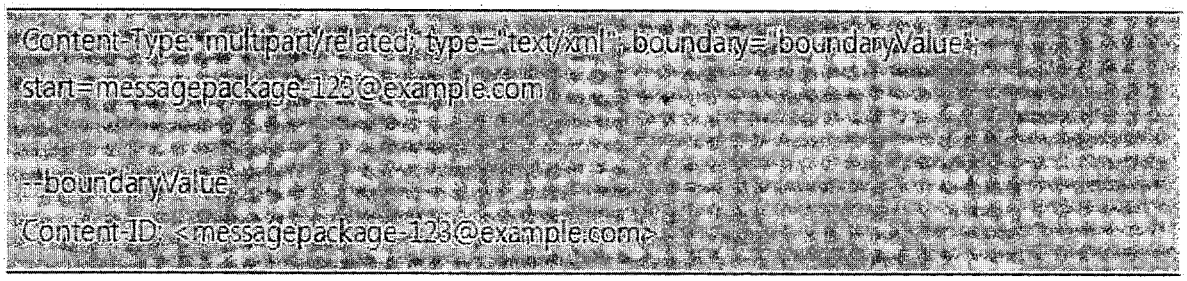
A first MIME Part includes a SOAP message and is referred to as a header container. The SOAP message is configured by a Header and a Body. A second MIME part is 0 or more additional MIME parts and is also called as a payload container. The second MIME part includes an application level attached document.

A basic structure of the distribution message is illustrated in Fig. 101 and observes the standard such as Simple Object Access Protocol (SOAP) 1.1 and, SOAP Messages with Attachment.

All components of the MIME header of the distribution message package observes the SOAP Messages with Attachments standard. Additionally, Content-Type MIME Header in the message package necessarily has an identical type attribute to a MIME media type of the MIME body part including the SOAP message document. The MIME type of the SOAP message according to the SOAP standard needs to have a "text/xml" value.

A root part needs to include Content-ID MIME Header having a structure based on [RFC2045] and a start parameter (optional in [RFC2387]) needs to be always present in addition to an essential parameter for a Multipart/Related media type. An example of the MIME Header of multipart/related message package will be described in the following Table 146.

[Table 146]



Hereinafter, in the description of the distribution message according to the present invention, a route Body part of the message package is defined as a Header container. The Header container includes one SOAP message as a MIME body part as defined in SOAP Messages with Attachment specification.

A MIME Content-Type header of the header container needs to have a "text/xml" value in accordance with the SOAP standard. The Content-Type header may include a "charset" attribute and an example thereof will be described in Table 147.

[Table 147]

```
Content-Type: text/xml; charset="UTF-8"
```

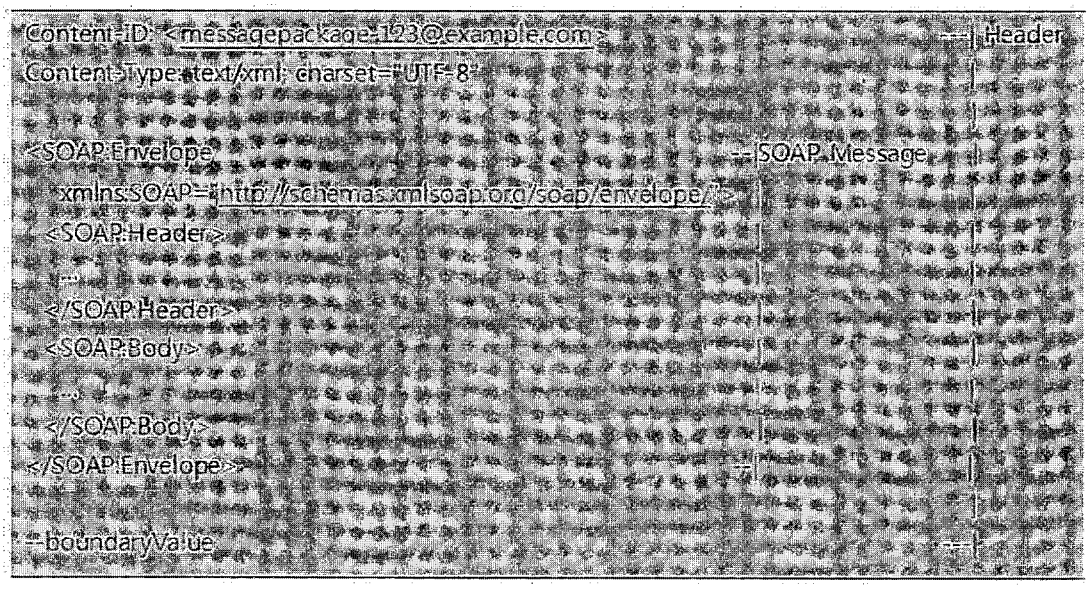
A MIME charset attribute is used to discriminate a character group which is used to create the SOAP message. Semantics of this attribute is described in "charset parameter / encoding consideration" of text/xml clearly expressed in [XMLMedia]. A list of effeceive values may be found in http://www.iana.org/.

If the MIME charset attribute include the Content-Type header, the MIME charset attribute needs to be equal to encoding declaratives of the SOAP message. Also, the MIME charset attribute does not include a value conflicting to the encoding when creating the SOAP message.

When this document is encoded, {UTF-8} is necessarily used to maximize compatibility. However, due to the processing rule defined for media types deducted from text/xml[XMLMedia], this MIME attribute does not have a default value.

An example of the header container will be described in the following Table 148.

[Table 148]



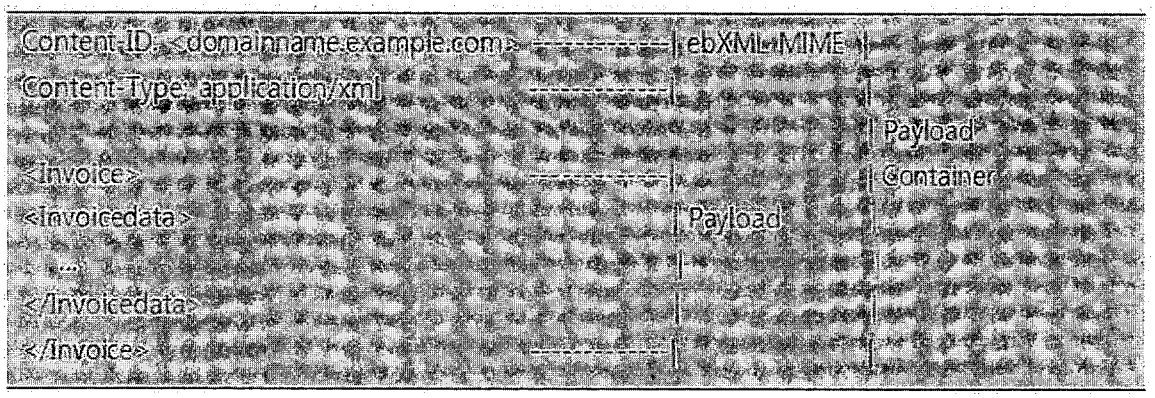
In accordance with SOAP Messages with Attachments standard, 0 or more payload container may be included in the message package. If the message package includes an application payload, the message package is necessarily included in the payload container.

If the message package does not include an application payload, the payload container is not represented. The contents of the payload contains are discriminated by ebXML message Manifest element in the SOAP Body.

The ebXML message service specification does not restrict the structure and the contents of the application payload. The payload may be a simple-plain-text object or an object of complicatedly overlapping several parts. The specification for the structure and the configuration of the payload object may be varied depending on how to define

the operation process or information exchange using ebXML message service. An example of the payload container will be described in the following Table 149.

[Table 149]



All MIME parts of the distribution message according to the present invention may include additional MIME headers based on the [RFC2045] standard. In the implementation, MIME headers which are not defined in this invention may be ignored and unidentified MIME headers should be ignored. For example, in the implementation, content-length may be included in the message. However, a receiver of a message including the content-length may ignore the content-length.

(2) Message envelope configuration

Contents of all extension elements need to be limited to an available name space based on the SOAP standard. The contents of all ebXML SOAP extension elements defined in

this invention need to be limited to ebXML SOAP Envelope extension name space. The declarations of the name space may be included in the SOAP Envelop, Header, or Body elements or directly included in each SOAP extension element.

The SOAP Envelop declares various Namespaces in the SOAP message as a Root item of the SOAP mesage. The Namespaces to be declared are as following Table 150.

[Table 150]

ITEM	Namespace URL
SOAP	http://schemas.xmlsoap.org/soap/envelope/
Digital Signature	http://www.w3.org/2000/09/xmldsig#
xlink	http://www.w3.org/1999/xlink
xsi	http://www.w3.org/2001/XMLSchema-instance

A schema structure of the message envelope is illustrated in Table 102 and an example of the message envelope will be described in the following Table 151.

[Table 151]

```
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
  http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
  <SOAP:Header
  xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
  xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
  http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
    <eb:MessageHeader ....>
      ....
    </eb:MessageHeader>
  </SOAP:Header>
  <SOAP:Body
  xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
  xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
  http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
    <eb:Manifest eb:version="2.0">
      ....
    </eb:Manifest>
  </SOAP:Body>
</SOAP:Envelope>
```

A SOAP Header element and a SOAP Body element which are child elements of the SOAP Envelope element will be described in detail in this order as follows.

The SOAP Header element is a first child element of the SOAP Envelope element and includes extension elements such as MessageHeader, SyncReply, Signature, and ErrorList.

MessageHeader is an essential element including routing information (To/From) of a message and other

context information concerning the message, SyncReply is an element indicating an essential transmission state to the next SOAP node, Signature is an element indicating digital signature based on [XMLDSIG] that signs data related with the message, and ErrorList is an element that has a list of errors reported for the previous message and used only when the error for the previous message is reported. Details of the elements of MessageHeader will be described below.

The MessageHeader element is an essential element which is expressed in all ebXML messages and expressed as a child element of the SOAP Header element. The MessageHeader element is a complex element configured by the following subelements. An element structure of the MessageHeader will be described in the following Table 152 and a schema structure of the MessageHeader is illustrated in Fig. 103.

[Table 152]

Name of item	Description	Number of repetition	Type	Length
From	■ message transmitting and transceiving entity information	1..1		

	PartyId	■ code identifying transmitter	1..1	S	13
	Role	■ serve as transmitter	1..1	S	Up to 256
To	■ message receiving and transceiving entity information		1..1		
	PartyId	■ code discriminating receiver	1..1	S	13
	Role	■ serves as receiver	1..1	S	Up to 256
CPAId	■ ID of business cooperation protocol		1..1	S	Up to 256
ConversationId	■ transceiving transaction identifier		1..1	S	Up to 256
Service	■ message service defined in CPA		1..1	S	Up to 256
Action	■ identifier of specific task process in Service ■ unique value in Service		1..1	S	Up to 256
	■ data for discriminating message		1..1		
	MessageId	■ unique identifier of one message	1..1	S	Up to 256

MessageData	Timestamp	■ message creating time ■ UTC type ■ ex> 2008-07-31T06:29:39.724Z	1..1	S	24
	RefToMessageId	■ Only response message ■ MessageId of request message	0..1	S	Up to 256

The SyncReply means a synchronous transmission and includes an id attribute, a version attribute, a SOAP actor attribute (necessarily has "http://schemas.xmlsoap.org/soap/actor/next" value), and an SOAP mustUnderstand attribute value. An example of SyncReply element will be described in the following Table 153.

[Table 153]

```
<eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
```

The Signature element needs to be present as a child element of the SOAP Header because the distribution message needs to be digitally signed in order to cope with the dangerous element mentioned above.

A process of performing the digital signature in accordance with [XMLDSIG] standard is as follows.

First, a SignedInfo element having SignatureMethod, CanonicalizationMethod, and Reference elements and an essential payload object in the SOAP Envelope is created as defined in [XMLDSIG].

Next, after canonicalization, SignatureValue of SignedInfo is calculated based on an algorithm designated in the SignedInfo as designated in [XMLDSIG].

Next, a signature element including SignedInfo, KeyInfo (recommended), and SignatureValue elements is created as designated in [XMLDSIG].

Next, the Signature element of the SOAP Header is included in the SOAP Header element.

Algorithm information which is used at the time of digital signature as described above is as follows. The algorithm basically follows an algorithm part (6.0 Algorithms) of W3C "XML-Signature Syntax and Processing" (RFC3275). Further, in order to support a domestic unique algorithm, an algorithm defined in TTAS.IF-RFC3075 "XML-Signature Syntax and Processing" (Telecommunications Technology Association, 2004) is used.

An algorithm list used in the distribution protocol according to the present invention includes digital

signature NameSpace, hash (Digest), digital signature (Signature), Canonicalization, and Transform. In order to minimize ambiguity in the process of creating and verifying the digital signature at the time of transmitting/receiving a message, algorithms other than the following list are not preferably used.

An example of the Namespace of the digital signature will be described in the following Table 154.

[Table 154]

<... xmlns:ds="http://www.w3.org/2000/09/xmldsig#" ... >

As an algorithm used to reduce data, SHA1 and SHA256 may be used and an example will be described in the following Table 155. In this case, the use of HA1 is restricted since 2012 when 'certificate cryptographic system sophistication' is entirely applied.

[Table 155]

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

or

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

An algorithm used for the digital signature of the message is RSAwithSHA1 and RSAwithSHA256 and an example will be described in the following Table 156. In this case, the use of RSAwithSHA1 is restricted since 2012 when 'certificate cryptographic system sophistication' is entirely applied.

[Table 156]

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/> or <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

Due to characteristics of XML which can physically variously express logically identical document, the digital signature value may be different for the same document. In order to prevent the above phenomenon, the canonicalization process needs to be performed. In the canonicalization, a canonical XML in which comments are omitted is used.

[Table 157]

<ds:CanonicalizationMetnod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>

Even though there are various transform algorithms as an algorithm that passes through a process of processing and selecting data to be signed among the entire XML data, only three algorithms may be used among the various transform algorithms. A first algorithm is Enveloped Signature transformation since the digital signature observes the form included in the target of the signature, a second algorithm is the above-described Canonicalization, and a third algorithm is Xpath filtering that selects signature target information. An example will be described in the following Table 158.

[Table 158]

```
<Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
and
<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
and
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-
19991116">
<ds:XPath>not(ancestor-or-
self::node()[@SOAP:actor=&amp;quot;urn:oasis:names:tc:ebxml-
```

```
msg:actor:nextMSH&amp;quot;]
    | ancestor-or-self::node()[@SOAP:actor=
&amp;quot;http://schemas.xmlsoap.org/soap/
actor/next&amp;quot;])
  </ds:XPath>
</ds:Transform>
```

A structure of the digital signature syntax is illustrated in Fig. 104 and an example of the digitally signed message as described above will be described in the following Table 159.

[Table 159]

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd ">
  <SOAP:Header>
    <eb:MessageHeader eb:id="..." eb:version="2.0" SOAP:mustUnderstand="1">
      ...
    </eb:MessageHeader>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
        <CanonicalizationMethod
          Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <Reference URI="">
```

```
<Transforms>
  <Transform
 Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
 <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
  <XPath> not(ancestor-or-self::node()[@SOAP:actor=
   &quot;urn:oasis:names:tc:ebxml-msg:actor:nextMSH&quot;]
   | ancestor-or-self::node()[@SOAP:actor=
   &quot;http://schemas.xmlsoap.org/soap/actor/next&quot;])
  </XPath>
 </Transform>
 <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
 </Transforms>
 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
 <DigestValue>...</DigestValue>
</Reference>
<Reference URI="cid://blahblahblah/">
 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
 <DigestValue>...</DigestValue>
 <Transforms>
  <Transform
 Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
 <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
  <XPath> not(ancestor-or-self::node()[@SOAP:actor=
   &quot;urn:oasis:names:tc:ebxml-msg:actor:nextMSH&quot;]
   | ancestor-or-self::node()[@SOAP:actor=
   &quot;http://schemas.xmlsoap.org/soap/actor/next&quot;])
  </XPath>
 </Transform>
 <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
 </Transforms>
 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
 <DigestValue>...</DigestValue>
</Reference>
<Reference URI="cid://blahblahblah/">
 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
 <DigestValue>...</DigestValue>
```

Only when an error occurs in the process of receiving

the message to process the message, the ErrorList is located in the lower level of the Header. When the ErrorList element is generated, RefToMessageId is necessarily present in the MessageHeader elemet and RefToMessageId needs to designate the MessageID of a message in which error occurs. The ErrorList element has attributes such as an id attribute, an OAP mustUnderstand attribute, a version attribute, a highestSeverity attribute, and one or more Error elements. A structure of ErrorList is illustrated in Fig. 105. In this case, if there is no error to be reported, the ErrorList element should not be present.

The highestSeverity attribute indicates a most serious status of all Error elements. Specifically, if an Error element set the severity as Error, the highestSeverity is set to be Error. Otherwise, the highestSeverity is set as Warning.

The Error element has an id attribute, a codeContext attribute, an errorCode attribute, a severity attribute, a location attribute, and a Description attribute.

The id attribute serves to uniquely discriminate an ErrorList element in the document.

The codeContext attribute represents a name space or a schema of the errorCodes and should be an URI. A default value of this attribute is urn:oasis:names:tc:ebxml-

msg:service:errors. If there is no default value in this attribute, the implementation of the specification indicates that errorCodes is used.

An errorCode attribute which is an essential attribute indicates an essence of an error of a message having an error. An effective value of the errorCode and the meaning of the code will be described below.

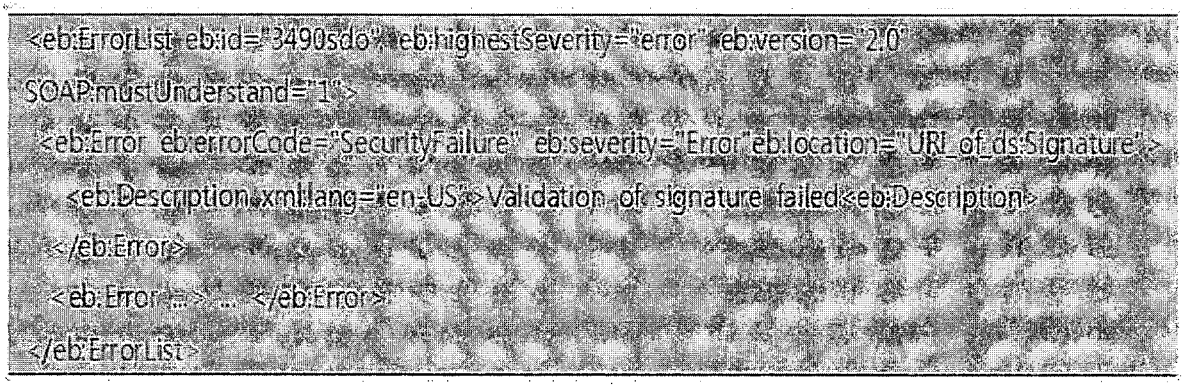
The severity attribute which is an essential attribute indicates a severity of the error. An effective value is Warning and Error. Warning indicates that other messages in the process of the conversation are normally created regardless of the error. Error indicates that no recovery error is present in the message and other messages are not created in the process of the conversation any more.

The location attribute indicates a message part in which an error is present. If the error is present in ebXML element and the element is "well-formed", the contents of the location attribute needs to be [Xpointer].

Contents of the Description attribute provides a descriptive explanation of the error by a language defined in a xml:lang attribute. Generally, this message is generated by software that verifies XML parser or the message. This means that the content is defined by a seller or a developer of software that creates the Error element.

An example of ErrorList will be described in the following Table 160.

[Table 160]



If an error occurs in the process of transceiving a message based on the distribution protocol, a transceiving entity that notices the error needs to report the error to the other party. Errors to be reported include a message structure error, a reliable messaging error, and a security error.

Errors related with a data communication protocol such as HTTP and Socket which belongs to a lower layer than the distribution protocol defined in this invention are found and reported by a standard mechanism supported by the data communication protocol and do not use the error reporting mechanism defined in this invention.

An error code is classified by an error target and error type and details thereof will be described in the

following Table 161.

[Table 161]

Error code	Contents	Detailed description
ValueNotRecognized	Element contents or attribute value is not recognized	Even though the document is well formed and effective, a value of element/attribute is unrecognized and thus a value which is used by the ebXML message service is included.
NotSupported	Element or attribute is not supported	Even though the document is well formed and effective and the element or the attribute follows a regulation or restriction of this specification, the document is not supported by the sbXML message service that is capable of processing the message
Inconsistent	Element contents or attribute value is inconsistent with other	Even though the document is well formed and effective and follows a regulation or restriction of this specification, the contents of the element and the attribute do not match with the other element or the attribute.

	element or attribute	
OtherXml	Other error in element contents or attribute value	Even though the document is well formed and effective, the contents of the element or the attribute value do not follow a regulation or restriction of this specification and do not belong to other error codes. Contents of Error element need to be used to indicate the essence of the problem.
DeliveryFailure	Message transmission failure	The received message is approximately or surely sent to a next destination. If the severity is set as Warning, a possibility that the message is delivered is low
TimeToLiveExpired	Expiration of time when message is present	Even though the message is received, the message is received at a time when a time restricted by TimeToLive of the MessageHeader element has elapsed.
SecurityFailu	Message security	Verification of the signature of the party who sends a message or checking

re	check failure	an authority or real name is failed.
Unknown	Unknown error	An error which does not belong to any kinds of error occurs. The content of the Error element is used to indicate the essence of the problem.

The SOAP Body element includes an extension element such as Manifest as a second child element of the SOAP Envelope. Manifest is an element indicating data which is located in a different position such as a payload container or a web.

The Manifest element is a complex element configured by one or more Reference elements. Each of the Reference elements is included as a part of payload document(s) contained in the payload container or discriminates data related with a message which is a distant resource which is accessible by a URL. It is suggested not to load payload data in the SOAP Body. A purpose of the Manifest is to allow a specific payload related with the ebXML message to be easily and directly accessed and to determine whether the application processes the payload without parsing.

The Manifest element has one id attribute, one version attribute, and one or more Reference elements.

The Reference element is a complex element configured

by subelements including 0 or more Schema elements and 0 or more Description elements. In this case, the 0 or more Schema elements are information concerning schema(s) that defines an instant document discriminated from a parent Reference element. Further, the 0 or more Description elements are description for a payload objects referenced by the parent Reference elements.

The Reference element is a simple link of [XLINK]. XLINK process or engine is not necessarily used but may be useful depending on the implementation requirements. The Reference element includes attribute contents such as id, xlink-type, xlink:href, xlink:role in addition to the contents of the above-mentioned elements. Other effective name space attributes may be present. A receiving MSH may ignore an external name space attributes other than the attributes defined above. In this case, id is XML ID for Reference element, xlink-type defines the element as a XLINK simple link and has a fixed value of "simple". xlink:href is a URI value of the referenced payload object and based on the simple link of [XLINK] specification. xlink:role discriminates the payload object or a resource that describes the purpose of the payload object. If this attribute is present, this attribute needs to have an available URI value based on the [XLINK] specification.

If reference items have schema(s) that describes the

reference items (for example, XML Schema, DTD, or Database Schema), the Schema elements needs to be present as child elements of the Reference element. This is used to discriminate the schema from the version and defines the payload object which is discriminated by the parent Reference element. The Schema element has attributes such as location and version. In this case, location is an essential URI of the schema and version is a version identifier of the schema.

If the xlink:href attribute includes an URI which is content id(URI scheme "cid"), the MIME having the content-id needs to be expressed in the payload container of the message. Otherwise, an error having MimeProbem as errorCode and Error as severity needs to be transmitted to the transmitting party. If the xml:href attribute does not include an URI which is the content id(URI scheme "cid"), the URI is not interpreted and thus it is determined whether to transmit an error depending on the implementation. If it is determined to transmit the error, an error having MimeProbem as errorCode and Error as severity needs to be transmitted to the transmitting party.

The following Table 162 represents a typical Mainfest of the message having one payload MIME body part.

[Table 162]

```
<eb:Manifest eb:id="Manifest" eb:version="2.0">
  <eb:Reference eb:id="pay01" xlink:href="cid:pay load-1" xlink:role="http://regrep.org/gci/purchaseOrder">
    <eb:Schema eb:location="http://regrep.org/gci/purchaseOrder/po.xsd" eb:version="2.0"/>
    <eb:Description xml:lang="en-US">Purchase Order for 100,000 widgets</eb:Description>
  </eb:Reference>
</eb:Manifest>
```

(3) HTTP binding

An HTTP binding example in a method of transmitting a message through an HTTP will be described in the following Table 163.

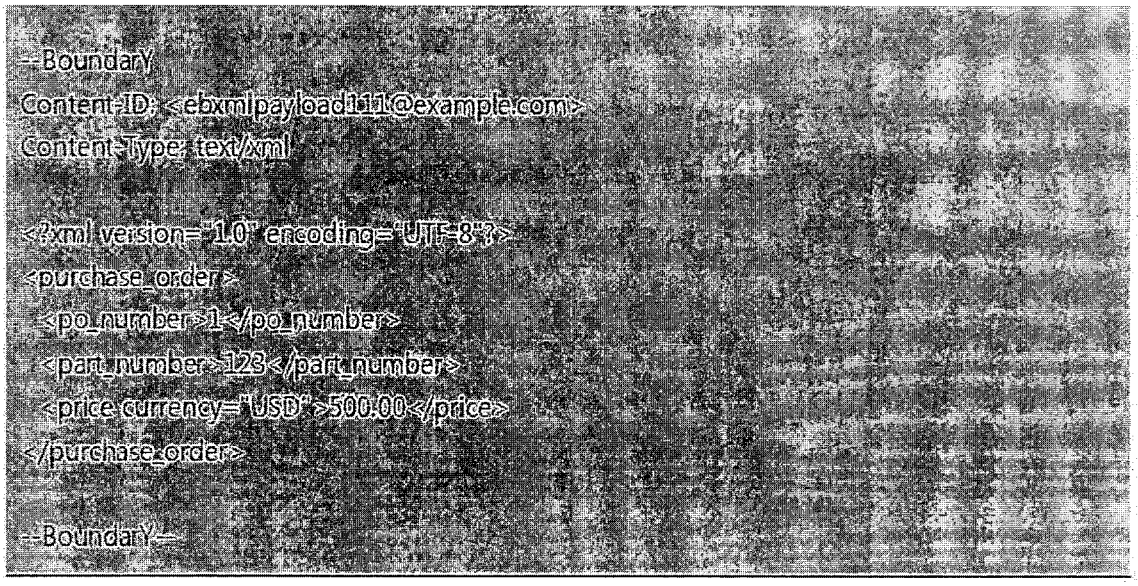
[Table 163]

```
POST /servlet/ebXMLhandler HTTP/1.1
Host: www.example2.com
SOAPAction: "ebXML"
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
    xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
    xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
    http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
    http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
    http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId>urn:duns:123456789</eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId>urn:duns:912345678</eb:PartyId>
      </eb:To>
      <eb:CPAId>20001209-133003-28572</eb:CPAId>
      <eb:ConversationId>20001209-133003-28572</eb:ConversationId>
      <eb:Service>urn:services:SupplierOrderProcessing</eb:Service>
      <eb:Action>NewOrder</eb:Action>
      <eb:MessageData>
        <eb:MessageId>20001209-133003-28572@example.com</eb:MessageId>
        <eb:Timestamp>2001-02-15T11:12:12</eb:Timestamp>
      </eb:MessageData>
    </eb:MessageHeader>
  </SOAP:Header>
  <SOAP:Body>
    <eb:Manifest eb:version="2.0">
      <eb:Reference xlink:href="cid:ebxmlpayload111@example.com"
          xlink:role="XLinkRole" xlink:type="simple">
        <eb:Description xml:lang="en-US">Purchase Order 1</eb:Description>
      </eb:Reference>
    </eb:Manifest>
  </SOAP:Body>
</SOAP:Envelope>
```



In this invention, in order to return the response code of the HTTP level, an HTTP response code defined in [RFC2616] needs to be used. Main response codes will be described in the following Table 164.

[Table 164]

State code	Related message	Meaning
200	OK	Request is successfully performed
400	Bad Request	Request has grammatical problem
401	Unauthorized	Client tries to access to a page that requires an approval without having proper approval
404	Not Found	No content is found in this address

500	Internal Server Error	Request is not normally processed due to error in server
503	Service Unavailable	Server currently cannot process requests due to excessive requests which exceeds available limit

[Electronic document form register]

Hereinafter, an electronic document form register of the electronic document distribution system according to the exemplary embodiment of the present invention as described above will be described in detail.

The electronic document form register is a system that allows a transceiving entity to create, register, and manage a form required to distribute a document in the electronic document distribution.

The electronic document form register includes a form creating unit, a form registering unit, and a form managing unit, and a standard connection module.

The form creating unit includes a PDF transforming module and a PDF form designer. The PDF transforming module provides a function of transforming a general form to a PDF (for example, create a standard PDF-A). The PDF form designer provides a function of creating an writable form PDF and a document security function such as two-dimensional barcode and copy prevention mark.

The form registering unit provides a function of allowing a user to register a form (for example, a general form such as HWP or MS-Word).

The form managing unit provides a function of allowing a form manager to register and manage a form and provides a registration function for every category and a record management function for every version. Further, a setting function to control a viewing period for every form, the number of viewing, and the number of printing is provided.

The standard connection module provides a function of connecting with the distribution client application. Further, a form list searching function and a file downloading function are also provided.

A form registering process of the electronic document form register according to the present invention is illustrated in Fig. 106.

A standard electronic document is created as a FormPDF using a Form designer and essential requirements will be described in the following Table 165.

[Table 165]

Classification	Description
Data input field	Data input field for

	inputting contents
Two-dimensional barcode	Original document and digital signature data of original document are inserted in order to certificate an original of a printed document
Copy prevention mark	Function for preventing the printed document from being copied. When the document is printed, an original mark disappears using a designated pattern
Information sentence	Expiration date of the document and verification method are included

In a structure of the standard electronic document, a space of approximately 5 cm from a lower edge of the document is required. A size of the barcode may be varied depending on the amount of data and a size of the copy prevention mark is 3>1.3 and appropriately disposed in accordance with a shape of the form. An example of the standard electronic document is illustrated in Fig. 107.

The standard connection module (standard interface)

allows a user to search and download the form and create a form in the distribution client application and is provided to a Web US (user interface) to be included in the distribution client application. The standard connection module provides a function of searching for every category, a form list, and file downloading.

[Electronic document packaging]

Hereinafter, the electronic document packaging which is applied to the electronic document distribution system and method according to the exemplary embodiment of the present invention as described above will be described in detail.

The electronic document packaging is a messaging system standard required to allow the transceiving entity to distribute a document in the electronic document distribution.

The electronic document packaging is configured by a standard electronic document and an attached document and configured by metadata for the standard electronic document. The standard electronic document is created based on PDF-A and the metadata is configured by information such as a document security function. The attached document is not transformed into a PDF but packaged into an original as it is.

The standard electronic document is digitally signed by the certificate of the user and the electronic document package is digitally signed after the packaging to be included in the package.

Fig. 108 illustrates an electronic document package structure. Referring to Fig. 108, the electronic document package structure according to the present invention includes a package header, metadata, a standard electronic document, an attached document, and digital signature data. Detailed components thoseof will be described in the following Tables 27 to 31.

The package header includes entire package structure information. The metadata includes information of the document security function of the standard electronic document and also includes information such as the number of document reading, the number of printing, and two-dimensional barcode information. The standard electronic document is configured in a standard PDF-A type and two-dimensional barcode data is included in an image region in a PDF file, and the digital signature data is included in a standard PDF Signed Data region. The attached document is not a standard electronic document, but atypical document. Therefore, the attached document is excluded from a target to which the document security function is applied. The digital signature data digitally signs the packaged data

using the certificate of the user to be included in the packaging.

[Table 166]

Number	Component	Remarks
1	Entire file size	
2	Size of Metadata	
3	Size of Standard electronic document	
4	Number of attached file	
5	Size of attached file	

[Table 167]

Number	Component	Remarks
1	Number of reading	
2	Number of printing	
3	Storing function	
4	Text extracting function	
5	Temporary storing/importing function	
6	Type of document	
7	2D barcode size (horizontal)	

[Table 168]

Number	Component	Remarks

1	PDF file	

[Table 169]

Number	Component	Remarks
1	Attached file	

[Table 170]

Number	Component	Remarks
1	Digital signature data	

A method of verifying the electronic document packaging includes (1) a method of verifying electronic document packaging digital signature, (2) a method of verifying a standard electronic document, and (3) a method of verifying a printed electronic document, which will be described below.

(1) Method of verifying electronic document packaging digital signature

- The client APP verifies the digital signature when processing the digital signature packaging. Only when the verification is successful, the client APP delivers the standard electronic document to an electronic document viewer.

- Further, the client APP supports a manual digital signature verifying function to verify the digital

signature when a dispute occurs.

(2) Method of verifying standard electronic document

-The electronic document viewer verifies the digital signature when reading the standard electronic document. Only when the digital signature verification is successful, the file is read in the electronic document viewer.

(3) Method of verifying printed electronic document

-Using additionally provided a verification program and a flat panel scanner, the digital signature data in the two-dimensional barcode is verified and contents of the original document and the contents of the printed document are compared by naked eyes.

In the meantime, since the copy prevention mark needs to be generated in accordance with the printer pattern of a user which finally receives the electronic document, the copy prevention mark is not included in the packaging.

[Distribution client application]

Hereinafter, the distribution client application of the electronic document distribution system according to the exemplary embodiment of the present invention as described above will be described in detail.

In order to allow the corporation or individuals to

transmit/receive a document (information) based on the certified electronic mailing address, an application that provides a user interface (hereinafter, abbreviated as UI) that supports the transmission/reception is required. As a messaging engine that sends/receives a message, if the distribution messaging server system serves as a mail server as compared with an email, the distribution client application (hereinafter, abbreviated as APP) serves as a user application likes a mail client which is provided to allow the user to send/receive an email in connection with the mail server.

Fig. 109 illustrates a structure diagram of the distribution client APP. Referring to Fig. 109, as an application under a UI environment for a general user who wants to exchange a document using the distribution messaging server system, the distribution client APP basically includes "(1) user authentication", "(2) message creation", "(3) message list inquiring and detailed contents reading function", and "(4) distribution messaging server system connection". In addition to the above basic functions, the client APP may provide a function of "(5) managing basic information and environmental information", "(6) managing a message folder", "(7) managing a document form, and "(8) a word processor" for transceiving a message and managing an application, which may be selectively

provided by an application developer.

(1) User authentication

- Before the distribution client APP is connected with the distribution messaging server system, the distribution messaging server system checks a user account and then receives login session information.

- A user authentication method of the distribution client APP includes user authentication based on a certificate (both public and private are allowed) and user authentication based on ID/PW.

(2) Message creating function

- The distribution client APP needs to provide a user interface that is capable of creating a new message and delivers the created document to the receiving party in connection with the distribution messaging server system.

- The message creating function is provided to input items other than a value which is set in advance by the environmental information among required basic information when a transmitting interface of the distribution messaging server system is called to transmit a message.

(3) Message list inquiring function and detaied contents reading function

- The messaging server system manages the message so as to be divided into a transmission message and a reception message. The distribution client APP necessarily provides a function of inquiring a list of the messages corresponding to the user account and a function of reading all detailed information of the message including the attached documents when the user wants to view the details of the message in connection with the distribution messaging server system based on the logged-in user account.

(4) Distribution messaging server system connection

- The most important function of the distribution client APP is a function of transceiving a message in connection with the distribution messaging server system. The distribution client APP transmits and receives the message based on the logged-in account through the message transmitting function and the received message reading interface provided by the distribution messaging server system.

(5) Basic information and environmental information management

- The client APP provides a function of managing environmental information basically required when transmitting a message. Since the distribution client APP

is not an independently existing application, the distribution client may participate in the distribution based infra in connection with the distribution messaging server system. Therefore, distribution messaging server system connection information (distribution messaging server system address information) which is required to be basically connected with the distribution messaging server system is basically set and managed.

- Additionally, management of register server information for the connection with the document form register or management of additional information for system environment of the distribution client APP may be defined to be provided in accordance with the development range of the application.

(6) Message folder management

- The message managed by the distribution messaging server system is basically divided into a transmission message and a reception message to be managed. The transmission and reception messages manage status information in accordance with the processing status. As the status information of each message, the transmission message manages the statuses such as before transmission, transmission completed, transmission failure, and reception completed by a person in charge. The reception message

manages the statuses such as the verification error, before reception confirmation, and reading confirmation. The distribution client APP manages the message folder based on the basic status information provided by the distribution messaging server system to provide the message folder to the user.

- The distribution client APP divides the transmission message and the reception message based on the transceiving folder to basically notify the status of the messages to the user in accordance with the status information provided by the distribution messaging server system. However, additionally, a deleted message mailbox such as a outbox or a trashcan is provided or a function of allowing a user to directly define and manage a folder is selectively provided by the application developer. Therefore, the description thereof will be omitted.

(7) Document form managing function

- The distribution messaging server system does not limit a format of a document which is attached to the message to be transmitted. Therefore, the transceiving target document includes any kinds of files such as a general text file, an office file, an XML document, or a multimedia file. However, for the convenience for users to utilize the distribution client APP in the task, a function

of supporting to create a document based on the form may be additionally provided to the basic document. The distribution client APP may provide a function of searching and downloading a document form provided by the document form register through a standard interface of the register and then creating a document based on the downloaded document form to be attached to the message.

- The distribution client APP manages the document form in a connection with the document form register provided by the electronic document distribution hub or independently builds a document form management system to manage the document in connection with this system. A method of searching and downloading the form in connection with the document form register provided by the electronic document distribution hub will be described with reference to the description of [Electronic document form register] as described above.

(8) Word processor

- A word processor is a creating unit that allows the distribution client APP to support the users to create a document based on a downloaded form through the document form managing function. The word processor is designed with reference to [electronic document form register] as described above when the document form register provided by

the electronic document distribution hub is used. If the document form management system is autonomously built, the word processor is designed in accordance with the form management system.

A basic process of the distribution client APP includes "(1) a document transmitting process" and "(2) a document receiving process". As an additional process, "(3) a electronic document form downloading process" is provided. The distribution client AP is connected with the distribution server system serving as a server in order to transmit and receive a document. Further, the distribution client APP is connected with the electronic document form register server in order to register a standard document form.

(1) Document transmitting process

A step in which the distribution client APP transmits an electronic document to other "transceiving entity" through the distribution messaging server system connected with the distribution client APP is illustrated in Fig. 110 and a processing procedure is as follows.

First, the distribution client APP creates a message to be transmitted to the receiver. In this case, a document that is created in advance by the transmitter or a document that is created by the word processor provided by

the distribution client APP is attached and a receiver is designated and then a message is created.

Next, after inputting receiver address information, the transmitting interface of the distribution messaging server system is called to request to transmit the message.

Next, the distribution messaging server system of the transmitter transmits the message to the receiver in accordance with the transmitting process and then receives the response message (reception certificate or reception error) for the reception from the receiver.

Next, the distribution messaging server system of the transmitter receives the response message for the reception and then delivers the response message to the distribution client APP as a response for the transmission.

Here, the first to fourth steps are essential and the second to fourth steps are synchronously performed.

Next, if the distribution messaging server system of the transmitter receives a message including a reading certificate that confirms the reading of a person in charge of reception from the receiver, the transmitting distribution messaging server system returns the response message for reception and stores the received message in the mailbox of the user.

Next, the distribution client APP of a first transmitter requests the connected distribution messaging

server system the received document.

Next, the distribution messaging server system of the transmitter delivers the list of received documents stored in the mailbox to the distribution client APP of a user who requests the received document.

Here, the fifth to seventh steps are selective and optional procedures which are performed only when the reading confirmation of a person in charge of reception is requested at the time of transmitting the first message.

(2) Document receiving process

A process in which the distribution client APP receives an electronic document from other "transceiving entity" is illustrated in Fig. 111 and the processing procedure thereof will be described as follows.

First, if the message is received, the distribution messaging server system of the receiver returns the reception response message for the received message to the receiver and stores the received message in the mailbox of the user.

Next, the distribution client APP of the receiver logs in the connected distribution messaging server system to request the received document.

Next, the distribution messaging server system of the receiver delivers the list of the received documents stored

in the mailbox of a user who requests the received document

Here, the second and third steps are synchronous.

Next, if the receiver requests to read detailed information of the message from the list of the received messages, the distribution client APP delivers transmit the detailed information including the attached document of the corresponding message to the distribution messaging server system.

Next, if an initial transmitter requests the reading confirmation of a person in charge of reception, the distribution messaging server system of the receiver transmits a message including the reading certificate to the transmitter of the corresponding message at the time when the user request the detailed information for the received document.

Next, the distribution messaging server system of the receiver receives the reception response message for the reading confirmation message (reading certificate) of a person in charge transmitted in the fifth step.

(3) Electronic document form downloading process

A process in which the distribution client APP dowlnoads the electronic document form is illustrated in Fig. 112 and the processing procedure thereof will be described as follows.

First, the distribution client APP is directly connected with the electronic document form register server to request searching a document form. In this case, the connection is performed based on the standard connection interface provided by the electronic document form register server.

Next, the electronic document form register server returns information on the searched document form as a result.

Here, the first and second steps are synchronous.

Next, the distribution client APP shows the searched form list to the user to select a form.

Next, the distribution client APP requests the electronic document form register server to download the selected electronic document form.

Next, the electronic document form register server returns the requested form to the distribution client APP.

Next, the distribution client APP registers the downloaded electronic document form to be plugged-in so as to be used in the word processor.

A type of interfaces provided by the distribution messaging server system for the above-mentioned distribution client APP includes a user authentication (login), logout, message transmission request, received message Get, detailed message information request, and

message deletion.

Connection methods (1) to (5) of the distribution client APP and the distribution messaging server system will be described as follows.

(1) Connection protocol of distribution messaging server system

A connection interface which is provided by the distribution messaging server system for the distribution client APP is based on the same protocol as the transceiving protocol of the distribution messaging server system. In this case, the distribution client APP and the distribution messaging server system provide one-way synchronous communication as illustrated in Fig. 113, which is different from the transmission/reception between the distribution messaging server systems and the digital signature authentication or user authentication method for the message is used therebetween.

The transmission message uses the message structure of the distribution messaging server system as it is and the user information and request and response messages are configured by the structure illustrated in Fig. 114. Detailed description thereof is as follows.

- SOAP Header: the distribution client APP and the distribution messaging server system may serve as a

transmitter or a receiver in accordance with the task type to be configured in accordance with [distribution protocol] as described above. SOAP Header includes messageHeader and Signature information.

- SOAP Body: includes Manifest element information and user login information defined in the above-described [distribution protocol].

- Transmission document container #1: includes message transmission request, received message Get, and a body document (contents) in case of receiving the detailed information of the message.

- Transmission document container #2 : includes message transmission request and an attached document in case of receiving the detailed information of the message from #2 sequentially.

A structure of SOAP Header will be described in the following Table 117 and a structure of MessageHeader will be described in the following Table 172, a structure of SOAP Body will be described in the following Table 173, and a structure of body message will be described in the following Table 174.

[Table 171]

Name of item	Description	Number of	Type	Length

		repetition		
MessageHeader	■ See following MessageHeader structure	1..1		
SyncReply	■ Synchronous transmission ■ See "distribution protocol standard"	1..1		
Signature	■ Digital signature element ■ See "distribution protocol standard	1..1		

[Table 172]

Name of item	Description		Number of repetition	Type	Length
From	■ message transmitter information		1..1		
	PartyId	Fixed value:"clientapp"	1..1	S	9
	Role	■ serve as transmitter ■ fixed value at the time of usage: 'sender'	0..1	S	6
To	■ message receiver information		1..1		

	PartyId	fixed value: "openapt"	1..1	S	7
	Role	■ serves as receiver ■ fixed value at the time of usage 'Receiver'	0..1	S	8
CPAId	■ ID of business cooperation protocol ■ necessarily use clientapp-openapl value		1..1	S	17
ConversationId	■ transceiving transaction identifier ■ set arbitrary value with length of 256 or shorter using English ■ ex> 2e2c2b1-4603-4919-9bef-ee435bc56cb3		1..1	S	Up to 256
Service	■ message service defined in CPA ■ necessarily use urn:ebxml:nipa:ClientToOa value		1..1	S	25
Action	■ identifier of specific task process in Service -document transmitting request: RequestSend -response for document transmitting request: RespondSend -document receiving request:		1..1	S	11

	RequestReceive -response for document receiving request: RespondReceive -receiving request for detailed information of document: RequestDetailInfo -response for receiving request for detailed information of document: RespondDetailInfo -document deleting request: RequestDelete -response for document deleting request: RespondDelete				
MessageData	■ data for discriminating message		1..1		
	MessageId	■ unique identifier of one message ■set arbitrary value with length of 256 or shorter using English ■ ex> 42e2c2b1-4603-4919-9bef-ee435bc56cb3	1..1	S	256
	Timestamp	■ message creating time ■ UTC type	1..1	S	24

		■ ex> 2008-07-31T06:29:39.724z			
	RefToMessageId	■ Only response message ■ MessageId of request message	0..1	S	Up to 256

[Table 173]

Name of item	Description		Number of repetition	Type	Length
Manifest	■ payload information ■ existed only when there is an attached document (message transmission, received message Get, detailed message information reception)		0..1		
	Reference	■ necessarily existed if there is Manifest ■ repeats as much as the number of payloads ■ see	0..∞		

		"distribution protocol standard"			
UserInfo	■ user information ■ necessarily existed only in case of message transmission request, received message Get, and detailed message information reception		0..1		
	Id	■ necessarily existed when there is user information ■ user ID registered in the distribution messaging server	0..1	S	20
	Password	■ necessarily existed when there is user information ■ password information set at the time of registering a user in the messaging server	0..1	S	15

		■ set after being encrypted with certificate of the distribution messaging server			

[Table 174]

Name of item		Description	Number of repetition	Type	Length
Content		■ detailed information of document ■ in case of document Get, existed as many as the number of document lists	1..∞	S	200
	Title	■ title of document ■ existed only in document transmission request, document Get response, detailed document information response	0..1	S	200
	Text	■ user comment	0..1	S	5000

		■ existed only in document transmission request, document Get response, detailed document information response			
	Sender	■ transmitter's reliable address ■ existed only in document transmission request, document Get response, detailed document information response	0..1	S	256
	Receiver	■ receiver's reliable address ■ existed only in document transmission request, document Get response, detailed document information response	0..1	S	256
	GetMessageID	■ detailed information request MessageId	0..1	S	256

		■ existed only in detailed information request			
	DeleteMessageId	■ delete request MessageId ■ existed only in deletion request	0..1	S	256

(2) Message transmission request

Basic information which is delivered by the distribution client APP to the distribution messaging server system at the time of transmitting a message will be described below. The transmission document which is stored in the mailbox after completely being transmitted has four steps of status information as described in the following Table 175.

[Table 175]

Status	Description
In the process of transmitting	■ a state when no response has been received from the receiver after transmitting a document
Transmission completed	■ a state when a response message (reception certificate) is received from the receiver

	for reception confirmation
Transmission failed	■ when SOAP Fault message is returned due to an error occurring in the receiving distribution messaging server system or a network error occurs in the transceiving process
Accepting completed	■ whether the reception user reads the details (including an attached file) of the received document

An example of the request message will be described in the following Table 176.

[Table 176]

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
```

```
    </eb:From>
    <eb:To>
      <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
        openapi
      </eb:PartyId>
    </eb:To>
    <eb:CPAId>clientapp-openapi</eb:CPAId>
    <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
    <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
    <eb:Action>RequestSend</eb:Action>
    <eb:MessageData>
      <eb:MessageId>20100209-133003-28572@example.com</eb:MessageId>
      <eb:Timestamp>2010-02-09T13:30:03</eb:Timestamp>
    </eb:MessageData>
  </eb:MessageHeader>
  <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
    SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
  <Signature ...> ... </Signature>
 </SOAP:Header>
 <SOAP:Body>
  <eb:Manifest eb:version="2.0">
    <eb:Reference xlink:href="cid:ebxmlpayload111@example.com"
      xlink:role="XLinkRole" xlink:type="simple">
    </eb:Reference>
    <eb:Reference xlink:href="cid:ebxmlpayload222@example.com"
      xlink:role="XLinkRole" xlink:type="simple">
    </eb:Reference>
  </eb:Manifest>
  <UserInfo>
      <Id>gazuo</Id>
      <password>FJDHS6IDFJFMCD</passwd>
  </UserInfo>
 </SOAP:Body>
</SOAP:Envelope>
```

--BoundarY

Content-ID:ebxmlpayload111@example.com

Content-Type:text/xml

<Contents>

<Content>

<Title>Test</Title>

<Title>It is test message</Title>

<Sender>gazuo#ceda001</Sender>

<Receiver>jnlee#ceda002</Receiver>

</Content>

</Contents>

--BoundarY

Content-ID:ebxmlpayload222@example.com

Content-Type:application/octet-stream

Actual attached document

--BoundarY--

An example of the response message will be described in the following Table 177.

[Table 177]

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RespondSend</eb:Action>
      <eb:MessageData>
        <eb:MessageId>20100209-133004-38572@example.com</eb:MessageId>
        <eb:Timestamp>2010-02-09T13:31:03</eb:Timestamp>
      </eb:MessageData>
      <eb:RefToMessageId>20100209-133003-28572@example.com</eb:RefToMessageId>
    </eb:MessageHeader>
    <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
      SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
    <Signature ...> ... </Signature>
  </SOAP:Header>
  <SOAP:Body/>
</SOAP:Envelope>

--BoundarY--
```

(3) Received message Get

An action of the distribution client APP that reads the received message through a logged-in user account in connection with the distribution messaging server system is separated from an action of deleting a message in the distribution messaging server system. The following two steps of status information are managed in accordance with the processes of the message reception.

- Whether the reception user reads the received document list in the mailbox

- Whether the reception user reads the details of the received document

An example of the request message will be described in the following Table 178.

[Table 178]

```
    <eb:To>
      <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
        openapi
      </eb:PartyId>
    </eb:To>
    <eb:CPAId>clientapp-openapi</eb:CPAId>
    <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
    <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
    <eb:Action>RequestReceive</eb:Action>
    <eb:MessageData>
      <eb:MessageId>20100209-133003-28572@example.com</eb:MessageId>
      <eb:Timestamp>2010-02-09T13:30:03</eb:Timestamp>
    </eb:MessageData>
  </eb:MessageHeader>
  <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
    SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
  <Signature ....> .... </Signature>
 </SOAP:Header>
 <SOAP:Body>
  <UserInfo>
      <Id>gazuo</Id>
      <password>FJDHS6IDFJFMCD</passwd>
  </UserInfo>
 </SOAP:Body>
</SOAP:Envelope>

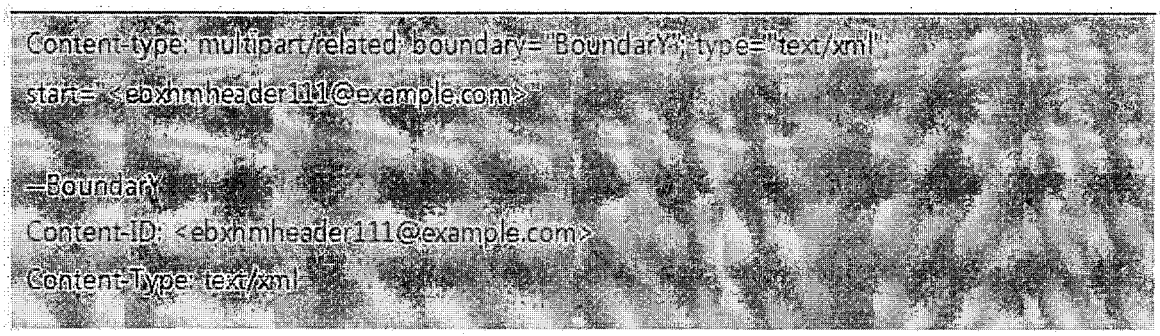
--Boundary--
```

```
    <eb:To>
      <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
        openapi
      </eb:PartyId>
    </eb:To>
    <eb:CPAId>clientapp-openapi</eb:CPAId>
    <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
    <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
    <eb:Action>RequestReceive</eb:Action>
    <eb:MessageData>
      <eb:MessageId>20100209-133003-28572@example.com</eb:MessageId>
      <eb:Timestamp>2010-02-09T13:30:03</eb:Timestamp>
    </eb:MessageData>
  </eb:MessageHeader>
  <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
    SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
  <Signature ...> ... </Signature>
 </SOAP:Header>
 <SOAP:Body>
  <UserInfo>
      <Id>gazuo</Id>
      <password>FJDHS6IDFJFMCD</passwd>
  </UserInfo>
 </SOAP:Body>
</SOAP:Envelope>

--Boundary--
```

An example of the response message will be described in the following Table 179.

[Table 179]


Content-type: multipart/related boundary="BoundarY"; type="text/xml"
start="<ebxhmheader111@example.com>"
--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

```
--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RespondReceive</eb:Action>
      <eb:MessageData>
        <eb:MessageId>20100209-133004-38572@example.com</eb:MessageId>
        <eb:Timestamp>2010-02-09T13:31:03</eb:Timestamp>
      </eb:MessageData>
      <eb:RefToMessageId>20100209-133003-28572@example.com</eb:RefToMessageId>
    </eb:MessageHeader>
    <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
      SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next" />
    <Signature ...> ... </Signature>
  </SOAP:Header>
  <SOAP:Body>
    <eb:Manifest eb:version="2.0">
      <eb:Reference xlink:href="cid:ebxmlpayload111@example.com"
        xlink:role="XLinkRole" xlink:type="simple">
      </eb:Reference>
```

```
</SOA:Body>

</SOAP:Envelope>

-BoundarY

Content-ID:ebxmlpayload111@example.com

Content-Type:text/xml

<Contents>

  <Content>

    <Title>Test</Title>

    <Title>It is test message</Title>

    <Sender>gazuo#ceda001</Sender>

    <Receiver>jnlee#ceda002</Receiver>

  </Content>

</Content>

  <Title>Test2</Title>

  <Title>It is test2 message</Title>

  <Sender>gazuo#ceda001</Sender>

  <Receiver>jnlee#ceda002</Receiver>

  </Content>

</Contents>


--BoundarY--
```

(4) Detailed message information request

If the user wants to read the details based on the received document list, the distribution client APP requests the detailed information of the message of the distribution messaging server system. The distribution messaging server system that receives the request of the detailed information delivers contents of all messages such as detailed attribute information of the message and the attached document of the message to the distribution client APP as a response message.

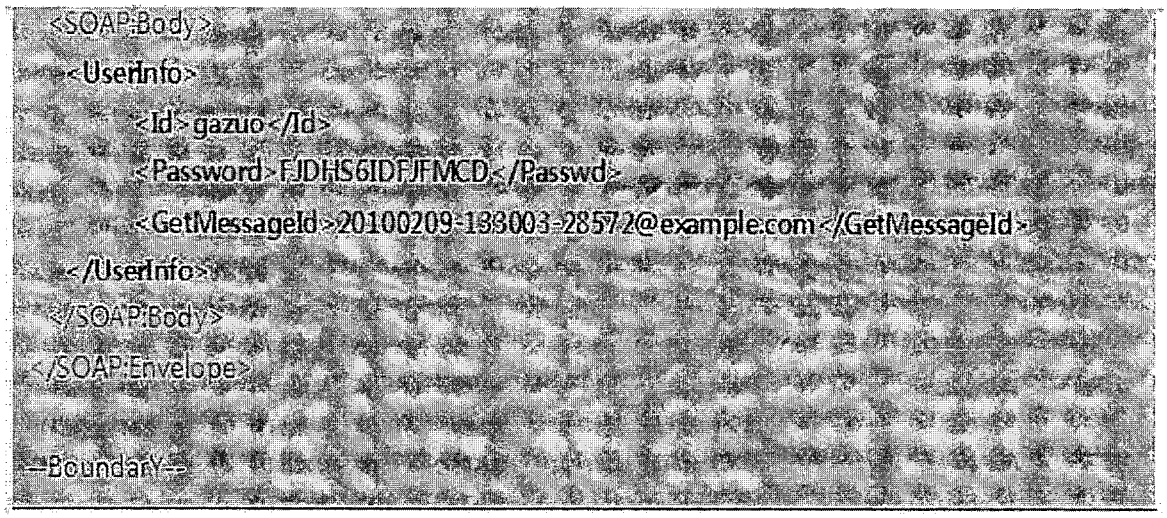
An example of the request message will be described in the following Table 180.

[Table 180]

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxmlheader111@example.com>"

--BoundarY
Content-ID: <ebxmlheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns ">
          clientapp
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns ">
          openapi
        </eb:PartyId>
      </eb:To>
      <eb:CPAId >clientapp-openapi</eb:CPAId>
      <eb:ConversationId >42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RequestDetailInfo</eb:Action>
      <eb:MessageData>
        <eb:MessageId>20100209-133003-28572@example.com</eb:MessageId>
        <eb:Timestamp>2010-02-09T13:30:03</eb:Timestamp>
      </eb:MessageData>
    </eb:MessageHeader>
    <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
      SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
    <Signature ...> .... </Signature>
  </SOAP:Header>
```



An example of the response message will be described in the following Table 181.

[Table 181]

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxmlheader111@example.com>"

--BoundarY
Content-ID: <ebxmlheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RespondDetailInfo</eb:Action>
```

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RespondDetailInfo</eb:Action>
```

```
    <eb:MessageData>
      <eb:MessageId>20100209-133004-38572@example.com</eb:MessageId>
      <eb:Timestamp>2010-02-09T13:31:03<eb:Timestamp>
    <eb:MessageData>
    <eb:Ref ToMessageId>20100209-28572@example.com</eb: RefToMessageId>
  <eb:MassageHeader>
```

```
<eb:SyncReplyeb:id="3833kkj9"eb:version="20"SOAP:must Understand="1"
    SOAP:actor=http://schemas.xmlsoap.org/soap/actor/next"/>
<Signature...>...</Signature>
</SOAP:Header>
<SOAP: Body>
  <eb:Manifest eb:version="20">
  <eb:Reference xlink:href=cid:ebxmlpayload111@example.com"
    Xlink:role="XlinkRole"xlink:type="simple">
    <eb:Reference>
  </eb:Manifest>
</SOAP:Body>
</SOAP:envelope>

--BoundarY
Content-ID:ebxmlpayload111@example.com
Content-Type:test/xml

<Contents>
 <Content>
  <Title>Test</Title>
  <Text>It is test message</Text>
  <Sender>gazuo#ceda001</Sender>
  <Receiver>jnlee#ceda002</Receiver
 </Content>
```

```
</Contents>
```

```
<Contents>
 <Content>Test</Title>
 <Text>It is test message</Text>
 <Sender>gazuo#ceda001</Sender>
 <Receiver>jnlee#ceda002</Receiver
 </Content>
</Contents>


--BoundarY
Content-ID:ebxmlpayload222@example.com
Content-Type:application/octet-stream


Actual attached document


--BoundarY--
```

(5) Message deletion

If the user requests the deletion, the distribution client APP delivers the deleting request of the document to the distribution messaging server system and notifies the result to the user. When the user deletes a document, whether to give a temporary deleting function which is a concept of a trashcan is an additional function of the

distribution client APP rather than an action on the actual server. Therefore, a developer of the distribution client APP may determine whether to provide the temporary deleting function but a function that requests the deletion to the distribution messaging server system is necessarily provided.

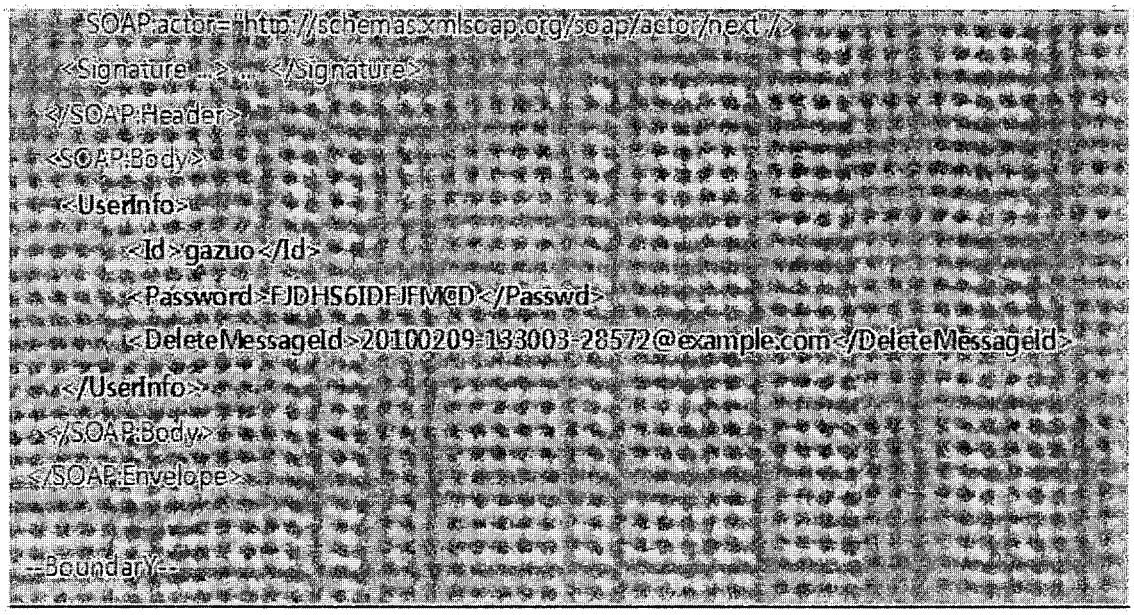
An example of the request message will be described in the following Table 182.

[Table 182]

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start= <ebxhmheader111@example.com>

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml-nipa:ClientToOa</eb:Service>
      <eb:Action>RequestDelete</eb:Action>
      <eb:MessageData>
        <eb:MessageId>20100209-133003-28572@example.com</eb:MessageId>
        <eb:Timestamp>2010-02-09T13:30:03</eb:Timestamp>
      </eb:MessageData>
    </eb:MessageHeader>
    <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
```



An example of the response message will be described in the following Table 183.

[Table 183]

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
```



[Recording medium]

The electronic document distribution method according to the present invention may be implemented in a general-purpose digital computer that operates a program using a computer readable recording medium which is created by a program which is executable in the computer. The computer readable recording medium includes a magnetic storage medium (for example, ROM, a floppy disk, a hard disk, or a magnetic tape), an optical reading medim (for example, CD-ROM, DVD, or an optical data storage device), and a carrier

wave (for example, transmission through Internet).

Hereinafter, another embodiment of the address directory server in the present invention as described above will be described below.

[Address directory server]

All users need to receive an unique electronic mailing address in order to participate in reliable electronic document distribution.

The electronic mailing address is represented by the following structure.

Electronic mailing address: internal separator + separation mark + unique registration address

An example of the electronic mailing address is "gdhong#nipa.kr".

The internal separator of the electronic mailing address is selectively added by an owner of the unique registration address for the convenience of internal processing and if necessary, the internal separator may be omitted.

The separation mark of the electronic mailing address is a mark which is located prior to the unique registration address or present between the inter identifier and the unique registration address. For example, "#" may be used and if necessary, other marks may be used.

The unique registration address of the electronic mailing address is a unique ID value which is requested to be issued by the corporation/institution/individual and the unit of the unique registration address is a legal responsible unit for the transmission and reception. The unique registration address is a unique registration address which is issued after the transceiving entity autonomously builds the distribution messaging server or through the electronic document third party distribution agency and is an essential configuration of the electronic address.

The transceiving entity has an actual physical address (IP address) for its own distribution messaging server system. However, the physical address does not correlation relationship with the electronic mailing address and the physical address and the electronic mailing address have 1:N relationship. One electronic mailing address does not have a plurality of physical addresses.

The corporation/institution/individual which is present next to the separation mark is responsible for legal reception of the information (electronic document) on the electronic mailing address and the distribution by the internal identifier is divided for the convenience of the corporation/institution/individual. Therefore, the corporation/institution/individual is responsible therefor.

The meaning of the electronic mailing address in the electronic document distribution system is represented as a relationship chart of the electronic document distribution system participant illustrated in Fig. 3.

As described above, the electronic mailing address including the internal identifier and the unique registration address will be described again as follows.

(1) Internal identifier

- The internal identifier is autonomously issued and managed by the transceiving entity regardless of the address directory server.

- The internal identifier is a unique value in the transceiving entity and may be omitted.

- The corporation/institution/individual is basically responsible for a method of assigning the internal identifier and the distribution of the electronic document by the internal identifier does not have an official meaning in the electronic document distribution based infra system.

- If the unique registered address is an entity which is officially registered in the address directory server such that the government/public sector/corporation/institution/group/individual that is responsible for the reception opens an account in a third

party distributing transceiving entity, the internal identifier is used to distribute the electronic document for the convenience of the task of the corporation and is not registered in the address directory server but used only as information inside the corporation.

(2) Unique registered address

- The government/public sector/corporation/institution/group/individual that participates in the electronic document distribution system to distribute the electronic document autonomously builds the distribution messaging server system and then receives the unique registered address as a transceiving entity or receives the unique registered address through a third party distribution (distribution by proxy) agency.

- The uniqueness of the unique registered address is confirmed by the address directory server at the time of issuance so as not to be redanduntly issued.

- The configuration method of the unique registered address of the government/public sector/corporation/institution/group/individual is determined by the policy of institution of the certified electronic mailing address management.

The electronic mailing address as described above is basically managed in two levels. At the highest part of

the certified electronic mailing address, institution of the certified electronic mailing address chief manager (for example, National IP Industry Promotion Institution) that manages the address directory server is present and the certified electronic mailing address chief manager issues and manages the unique electronic mailing address for a lower transceiving entity. Among the lower transceiving entities of the certified electronic mailing address chief manager, a transceiving entity that is capable of performing the third party distribution (distribution by proxy) opens a registered address for a user who wants the third party distribution and then registers the address information in the address directory server. In this case, in order to guarantee the uniqueness of the unique registered address value of the user, it is required to confirm the redundancy from the address directory server.

Among the electronic mailing addresses, an internal identifier which is not an official user but is internally issued and used for the convenience of the task is autonomously issued and managed by the transceiving entity regardless of the address directory server.

A system of issuing the electronic mailing address is illustrated in Fig. 4 and roles of the components illustrated in Fig. 4 will be described in the following Table 184.

[Table 184]

Component	Role
National IP Industry Promotion Institution (electronic mailing address chief manager)	- NIPI manages all certified electronic mailing address information as highest managing agent of certified electronic mailing address - Issues unique ID for transceiving entity - when certified electronic mailing address for user account is required to be registered, notifies whether to be newly registered, or change of an existing address - when user account is newly registered, notifies whether the account ID is unique -delivers result value for physical address information searching request of a user
Transceiving entity	-basic unit of physical certified electronic mailing address -issues and manages user account or internal identifier information for a plurality of users at the lower level of one certified electronic mailing address

	and guarantees the uniqueness of the user account or the internal identifier in one certified electronic mailing address
User (individual, corporation, or institution) account or ID for internal identifier	-an actual user which participates in the electronic document distribution and if ID is issued from the same transceiving entity, even though the physical certified electronic mailing address is identical, the user becomes a unit of an actual basis of the reliable distribution -user account is a legally responsible transceiving unit as an electronic mailing address open through a transceiving entity which is capable of third party distribution and should be registered in the electronic mailing address directory server -the internal identifier is information that is managed by the transceiving entity which is legally responsible for the transmission/reception for the convenience of the task and the transceiving entity which is at a higher level than the internal identifier has a legal

	responsibility and is not registered in the electronic mailing address directory server

A process of issuing an electronic mailing address is illustrated in Fig. 5. The user (corporation) may directly access to a screen that is provided by the address directory server to register or edit the address or receives the electronic mailing address through a distribution messaging server system (web site provided by the system) that issues the certified electronic mailing address by proxy.

The user that participates in the distribution needs to know physical actual address information based on the electronic mailing address before transmitting a message to the other party and further acquires public key information of the receiver in order to encrypt the attached document.

A procedure of acquiring a physical address of the electronic mailing address in the electronic document distribution process is an essential step and the transmitter inquires the address directory server in order to acquire the physical address information and the security information for the receiving party based on the address information of the receiver. If the transmitter delivers the transmission document to the receiver based on

the physical address, the distribution messaging server system of the receiver receives the transmission document to internally distribute the received document in accordance with the user account or the internal identifier based on the receiver address information.

A process of acquiring the physical address of the electronic mailing address and the security information is illustrated in Fig. 6. In order to transmit a document to the receiver based on the certified electronic mailing address in the electronic document distribution, there are two methods as follows: (1) the distribution client APP acquires necessary information in connection with the address directory server at the time of inputting address information of a receiving party and then requests the distribution messaging server to transmit the document based on the searched actual physical address information and (2) the distribution client APP requests the distribution messaging server to transmit the document based on the certified electronic mailing address for the receiver and the distribution messaging server acquires the physical address and the security information to the address directory server before the distribution messaging server transmits the document and then transmits the document to the receiver. The procedure for the two methods are illustrated in Fig. 7

The address directory server provides a remote service so that the distribution messaging server system searches the address information or issues an address by proxy. The services provided by the address directory server include an address searching service, an address registering service, and address changing service and provides the following service interfaces based on the distribution protocol standard.

The address searching service is a service that the address directory server returns the physical address information (for example, IP address and a Domain address) corresponding to the certified electronic mailing address and the public key information to the searching requestor. Generally, the address searching service is used to acquire the actual address information of the receiver and the security information for encryption before the transmitter transmits the document. In this case, the roles of the request message and the response message will be described in the following Table 185.

[Table 185]

Component	Role
Request message	Whether receiver is individual, corporation/institution, unique ID of the

	receiver (resident registration number, business registration number, foreigner registration number), whether to request public key
Response message	Unique ID of receiver, receiver address, public key (optional if requested)

The address registering service is a service that is provided to register the certified electronic mailing address of the user not only through the UI provided by the address directory server but from a remote location. The address directory server receives user information and certified electronic mailing address information as a request message to register the information and then receives the result as a response message. The request message for the address registering service needs to be delivered so as to include the digital signature information for the requester and the address director server verifies whether the user information included in the request message is identical to the certificate information used for the digital signature. In this case, the roles of the request message and the response message will be described in the following Table 186.

[Table 186]

Component	Role
Request message	User unique ID, user additional information structure (user name, contact information) whether receiver is individual, corporation/institution, user address information, public key information (optional), structure that defines scope to open address information
Response message	User unique id, registration result value (successful, failed-request information error, failed-already registered, failed-not an authenticated transceiving entity, or address directory server error)

The address changing service is a remote service that provides a function that allows the user to directly and remotely change the address information of the registered user. The address changing service transmits a changing request message to the address directory server together with information to be changed and receives the result as a response message. The request message for the address changing service needs to be delivered so as to include the digital signature information for the requester. The address director server verifies whether the user information included in the request message is identical to

the certificate information used for the digital signature. In this case, the roles of the request message and the response message will be described in the following Table 187.

[Table 187]

Component	Role
Request message	Only changed information among user unique ID and user additional information structure (user name, contact information) whether receiver is individual, corporation/institution, user address information, public key information (optional), structure that defines scope to open address information
Response message	User unique id, information changed result value (successful, failed-request information error, failed-unregistered user, failed-no changing authority, or address directory server error)

[CLAIMS]

1. An electronic document distribution system, comprising:

a transceiving entity that transmits and receives a message based on an electronic mailing address and distributes the electronic document through a distribution messaging server that issues and manages a distribution certificate for message transmission/reception;

a distribution hub that registers/manages the electronic mailing address of the transceiving entity, sets an electronic document distribution route between the transceiving entities, provides a standard form of the electronic document to the transceiving entity, transmits the message by proxy when an error occurs in the process of distribution the electronic document between the transceiving entities and issues a distribution certificate; and

a reliable third party storing institution that receives and stores the distribution certificate.

2. The electronic document distribution system according to claim 1, wherein the distribution messaging server of the transceiving entity stores the transceiving message in a mailbox so as to include status information

for every user,

stores a message transceiving record in a medium that is not allowed to edit and delete the message transceiving record for a predetermined period of time,

issues the distribution certificate for the message transmission/reception to request the third party storing institution to store the distribution certificate,

allows the transceiving entity to use function of registering, searching, editing, and deleting the electronic mailing address in connection with the address directory server of the distribution hub, and

moves messages which are stored for a predetermined period of time or longer to an external storage device to be stored.

3. The electronic document distribution system according to claim 1, wherein the electronic mailing address includes:

a user identification mark that is issued to the transceiving entity through the address directory server of the distribution hub;

an additional identification mark which is an unique value autonomously assigned by the transceiving entity if necessary and a unique value in the transceiving entity; and

an identification mark disposed between the user identification mark and the additional identification mark.

4. The electronic document distribution system according to claim 3, wherein a principal agent for the electronic document distribution is a user that receives a unique registration address.

5. The electronic document distribution system according to claim 3, wherein the identification mark is "#".

6. The electronic document distribution system according to claim 1, wherein the distribution hub includes an electronic document format register, and

the electronic document format register performs the management including registration, deletion of the electronic document standard form, and information edition. Further, the electronic document format register additionally classifies the electronic document standard form in accordance with a context and performs management including registration and edition of a context in which the electronic document standard form is used.

7. The electronic document distribution system

according to claim 6, wherein the electronic document form register includes a server engine that manages a document format and a standard interface that allows a user who uses the transceiving entity to search and download the document format to use the document format,

the transceiving entity further includes a distribution client application which is a user interface that allows the user who uses the transceiving entity to transmit/receive the message through the distribution messaging server, and

the user who uses the distribution client application searches and downloads the document format through the standard interface of the electronic document form register and then creates an electronic document using the document format.

8. The electronic document distribution system according to claim 1, wherein the distribution hub includes a distribution relay server that transmits a message by proxy when error occurs during the process of distributing the electronic document between the transceiver entities and issues a distribution certificate,

when the distribution relay server is requested by the transceiving entity to transmit the message, the distribution relay server issues a transmission certificate

to the transceiving entity that requests the message transmission after transmitting the message by proxy and if the requested message transmission is failed, transmits an error message to the transceiving entity that requests the message transmission.

9. The electronic document distribution system according to claim 1, wherein the distribution hub includes an externally connected gateway server for connection with an external system, and

the externally connected gateway server includes a distribution messaging server that transmits/receives a message based on an electronic mailing address, provides an electronic mailing address verification/conversion function between the connected external system and the electronic document distribution system, a message verification/conversion function between the connected external system and the electronic document distribution system, a verification/conversion function of security which is applied to an electronic document between the connected external system and the electronic document distribution system, and a function that verifies and transforms a compatibility of the electronic document between the connected external system and the electronic document distribution system.

10. The electronic document distribution system according to claim 1, further comprising:

a first interface which is used for an electronic mailing address registration agency to request the address directory server to register the electronic mailing address and receive the response, a second interface which is used for the electronic mailing address registration agency to request to change the electronic mailing address registered in the address directory server and receive the response, and a third interface which is used for the electronic mailing address registration agency to request to delete the electronic mailing address registered in the address directory server and receive the response,

wherein the electronic mailing address registration agency transmits the request message including electronic mailing address registrant information and electronic mailing address information through the first interface and then receives the registration result of the address directory server as a response message, transmits the request message including electronic mailing address registrant information and electronic mailing address information to be changed through the second interface and then receives the changing result of the address directory server as a response message, and transmits the request

message including electronic mailing address registrant information and electronic mailing address information to be deleted through the third interface and then receives the deleting result of the address directory server as a response message.

11. The electronic document distribution system according to claim 10, further comprising:

a fourth interface that is used for the electronic mailing address registration agency or the transceiving entity to request the address directory server for physical address information corresponding the certified electronic mailing address information of the receiver of the electronic document and certificate information for message secure processing and receive the response,

after transmitting the request message including the certified electronic mailing address of the receiver of the electronic document and whether to request the certificate, the electronic mailing address registration agency or the distribution messaging server of the transceiving entity receives the physical address information of the receiver of the electronic document and the certificate information from the address directory server as a response message.

12. The electronic document distribution system

according to claim 1, wherein the distribution messaging server of the transceiving entity and the distribution messaging server of the electronic mailing address registration agency includes a fifth interface that is used to transmit a message, deliver the distribution certificate, request to store the distribution certificate, and deliver the storage result of the third party storing institution.

13. The electronic document distribution system according to claim 1, wherein the user in the transceiving entity includes a distribution client application which is a user interface,

the distribution messaging server of the transceiving entity includes a sixth interface that provides a document transceiving function to the user in connection with the distribution client application for a user who requests the electronic document distribution, and

the sixth interface provides a function of requesting to transmit a message, requesting a list of the message, requesting detailed information of the message, reporting a spam message and searching the physical address information to the distribution client user.

14. A method of distributing an electronic document in an electronic document distribution system including a

transceiving entity and a distribution hub, comprising:

(a) a step of allowing a transmitting entity to acquire physical address information corresponding to address information of a receiving entity and then transmit a message with an attached electronic document to the physical address;

(b) a step of allowing the receiving entity that receives the message to issue a reception certificate or an error certificate in accordance with compatibility verification result for a received message and the transmitting entity and deliver the certificate to the transceiving entity; and

(c) a step of allowing a transmitting entity that transmits the message to the receiving entity but fails the transmission to request the distribution hub to transmit the message by proxy and allowing the distribution hub that receives a request to transmit the message by proxy to issue the transmission certificate to deliver the certificate to the transmitting entity and transmit the message to the receiving entity and then perform the step (b).

15. The method according to claim 14, wherein the step (a) includes:

(a1) a step of allowing the transmitting entity to

inquire inquires an address directory server for physical address information and security information based on the address information of the receiving entity;

(a2) a step of allowing the address directory server to receive/verify the inquiry of the transmitting entity and then provide the physical address information corresponding to the electronic mailing address to the transmitting entity if the electronic mailing address is included in a whitelist; and

(a3) a step of allowing the transmitting entity to set a route based on the physical address received from the address directory server to transmit a message with an attached electronic document to the receiving entity.

16. The method according to claim 14, wherein after the step (b), the transceiving entity that receives the reception certificate verifies the validity of the reception certificate and attaches the verified information to the reception certificate and then stores the reception certificate therein and requests a third party storing institution to store the reception certificate.

17. The method according to claim 14, wherein the step of (c) includes:

(c1) a step of allowing the transceiving entity that

transmits a message to the receiving entity but fails the transmission to request the distribution hub to transmit the message by proxy;

(c2) a step of allowing the distribution hub to start the message transmission and retry the transmission at a predetermined interval when the transmission is failed, and if the message transmission is finally failed, transmit the transmission failure message to the transmitting entity;

(c3) a step of allowing the receiving entity that normally receives the message to issue the reception certificate and transmit the reception certificate to the distribution hub; and

(c4) a step of allowing the receiving entity to issue a reading certificate to directly transmit the transmitting entity without using the distribution hub if the receiver of the electronic document reads the electronic document.

18. A method of distributing an electronic document in an electronic document distribution system including a transceiving entity that serves as a transmitter or a receiver and an electronic document distribution hub, comprising:

(a) a step of allowing the transmitter to acquire electronic mailing address information of the receiver;

(b) a step of allowing the transmitter to create a

message obtained by packaging a document to be transmitted with a predetermined message structure and then transmit the document to the electronic mailing address of the receiver;

(c) if the transmission of the step (b) is failed, allowing the transmitter to request the electronic document distribution hub to transmit the message and allowing the electronic document distribution hub to issue a transmission certificate and deliver the transmission certificate to the transmitter and then transmit the message by proxy;

(d) a step of allowing the receiver to verify the message received from the transmitter or the electronic document distribution hub and if the verification is passed, extract a document from the received message and issue a reception certificate to deliver to the transmitter;

(e) a step of allowing the transmitter to store the delivered reception certificate utilizing a reliable third party storing INSTITUTION; and

(f) a step of allowing the receiver to deliver the extracted document to a person in charge of document.

19. The method according to claim 18, further comprising: prior to the step (a),

(g) a step of allowing the transmitter and the

receiver to determine whether to build a distribution messaging server for the document distribution or use a transceiving entity that includes a distribution messaging server which is capable of performing the third party distribution;

(h) if it is determined to build the distribution messaging server for the document distribution in the step (g), a step of allowing the transmitter and the receiver to build the distribution messaging server for the document distribution and then perform authentication test of the distribution messaging server through an authentication institution and register and manage an internal identifier for an internal actual user after receiving an electronic mailing address as a transceiving entity by accessing to the address directory server of the electronic document distribution server;

(i) if it is determined to use the transceiving entity that includes a distribution messaging server which is capable of performing the third party distribution in the step (g), a step of allowing the transmitter and the receiver to request to open an electronic mailing address through the distribution messaging server which is capable of performing the third party distribution and then register the electronic mailing address information in the address directory server of the electronic document

distribution hub; and

(j) a step of allowing the transmitter to search, download, and register a document format from an electronic document form register of the electronic document distribution hub after the step (h) and the step (i);

before the step (b), further comprising (k) a step of selecting a document to be transmitted or created a document to be transmitted using the document format registered in the step (j).

20. A computer readable recording medium, in which a program that executes a method according to any one of claims 14 to 19 is stored.