# Electronic Authentication System

## Background of the invention

The present invention relates to an electronic authentication system and an electronic authentication method. According to the popularization of an Internet, an electronic commerce in which a shopping or commerce is carried out through the Internet is generalized. Further, it has been necessary to make a contract on the Internet. Thus, to make it possible to safely perform an electronic commerce or contract on an electronic network, there appears an electronic authentication system for carrying out an authentication on the electronic network. The electronic authentication system is a system for registering, making reference to and verifying "when, who and what" about electronic information. Therefore, there are required a cryptographic technique for safely performing a communication on the electronic network, an electronic signature technique using a public key encryption system and a time stamping technique for verifying a correct time.

A usual electronic authentication system is carried out as shown in Fig. 5. An electronic authentication service trader 1 provides an electronic authentication service to an A company 2 and a B company 3 as users. For example, the trader 1 receives a registration of an electronic document 4 from the A company 2 and issues an electronic certificate 5 to the A company 2.

The electronic certificate 5 includes a unidirectional function value outputted in a unidirectional function based on the contents of the electronic document 4, for instance, a hash value, time information and an electronic signature or the like to these information. When the A company 2 and the B company 3 as the users perform an electronic commerce by using the electronic document 4 and the electronic certificate 5, the B company 3 transmits the electronic document 4 and the electronic certificate 5 to the electronic authentication service trader 1 to make reference thereto. Then, the electronic authentication service trader 1 verifies the electronic document 4 and the electronic certificate 5 to inform the B company 3 of its result.

In the above-described electronic authentication system, since there may possibly arise a doubt as to whether or not the time information included in the electronic certificate 5 for verifying the time that the electronic document 4 is registered, is preferably employed time stamping means which is managed by a third person independent of the electronic authentication service trader 1. However, if the above-described time stamping means is managed, there will arise a problem as to how a service fee is collected. With these circumstances taken into consideration, it is an object of the present invention to provide an electronic authentication system and an electronic authentication method in which the

reliability of time stamp information is improved and a service fee can be easily accounted.

Summary of the invention

For achieving the above-described object of the present invention, according to a first feature of the present invention, an electronic authentication system for performing an electronic authentication through a network comprises an electronic authentication center which receives a registration of electronic information from a user, issues an electronic certificate by using a time stamping unit and inspects contents based on the electronic certificate; and a time correction center which exists independently of the electronic authentication center to correct the time of the time stamping unit, and is characterized in that the time correction center includes a time correcting unit for correcting the time of the time stamping unit, a stamp issue log obtaining unit for obtaining stamp issue logs from which the number of the electronic certificates issued by the time stamping unit can be grasped from the time stamping unit and an accounting unit which grasps the number of the issued electronic certificates from the stamp issue logs obtained by the stamp issue log obtaining unit and accounts for the electronic authentication center in accordance with the number of issues.

According to a second feature of the present invention

described in the first feature, an electronic authentication system is characterized in that the stamp issue log obtaining unit accesses the time stamping unit through the network to obtain the specific ID of the time stamping unit and the stamp issue log.

According to a third feature of the present invention described in the first or second feature, an electronic authentication system is characterized in that the stamp issue log obtaining unit obtains the stamp issue log when the time correcting unit corrects the time of the time stamping unit.

According to a fourth feature of the present invention described in any one of the first to third features, an electronic authentication system is characterized in that the time correcting unit transmits a time correction certificate to the time stamping unit when it corrects the time and the time stamping unit issues the electronic certificate including the time correction certificate.

According to a fifth feature of the present invention, an electronic authentication method for performing an electronic authentication through a network comprises an electronic authentication center which receives a registration of electronic information from a user, issues an electronic certificate by using a time stamping unit, and inspects contents based on the electronic certificate; and a time correction center which exists independently of the electronic authentication

center to correct the time of the time stamping unit, and is characterized in that the time correction center corrects the time of the time stamping unit, obtains stamp issue logs from which the number of the electronic certificates issued by the time stamping unit can be grasped from the time stamping unit, and grasps the number of the issued electronic certificates from the stamp issue logs and accounts for the electronic authentication center in accordance with the number of issues.

According to a sixth feature of the present invention described in the fifth feature, an electronic authentication method is characterized in that the time correction center accesses the time stamping unit through the network to obtain the ID of the time stamping unit and the stamp issue log.

According to a seventh feature of the present invention described in the fifth or sixth feature, an electronic authentication method is characterized in that the time correction center obtains the stamp issue log when it corrects the time of the time stamping unit.

According to an eighth feature of the present invention described in any one of the fifth to seventh features, an electronic authentication method is characterized in that the time correction center transmits a time correction certificate to the time stamping unit when it corrects the time and the time stamping unit issues the electronic certificate including the time correction certificate.

Brief Description of the Drawings

Fig. 1 shows a schematic structural example of an electronic data authentication system according to one embodiment of the present invention,

Fig. 2 is a view for explaining a time stamp server and an electronic certificate in one embodiment of the present invention,

Fig.3 is a view for explaining a procedure for accounting an electronic authentication center from a time correction center according to one embodiment of the present invention,

Fig. 4 is a view showing a using state of the electronic certificate according to one embodiment of the present invention, and

Fig. 5 is a schematic structural example of an electronic authentication system according to a prior art.

Detailed Description of the Preferred Embodiment

In Fig. 1, the outline of an electronic data authentication system according to one embodiment is shown. As shown in Fig. 1, the electronic data authentication system of this embodiment provides an authentication service of electronic data to users 10 such as a user A and a user B by a paired electronic authentication center 100 and time correction center 200. Plural electronic authentication centers 100 are present for

one time correction center 200 to provide a service. The electronic authentication center 100 and the time correction center 200 are preferably managed by a main body independent of them. Further, each user 10 preferably registers in advance an electronic signature and a public key certificate used for a signature as well as a user's name and a specific ID, etc. in the electronic authentication center 100. Thus, an authentication can be smoothly carried out. Further, a communication between the user 10 and the electronic authentication center 100 can be completely carried out by the signature and encryption, and accordingly, a tampering, an eavesdropping, a successful impersonation, etc., during a communication step can be prevented.

In this case, the user 10 transmits electronic data 11 to the electronic authentication center 100, so that the user can receive an electronic certificate 101 to authenticate the contents and time of the electronic data 11. The user 10 preferably enciphers or encodes and transmits the electronic data 11 by using the electronic signature previously registered in the electronic authentication center 100.

The electronic authentication center 100 has an application server 110 for receiving an authentication from a user 10 and inspecting it. The application server 110 includes receiving means 111 for receiving the electronic data from the user 10 and transmitting the electronic certificate 101 to the

user 10, computing means 112 for receiving the accepted electronic data 11 to form a unidirectional function value for forming the electronic certificate 101 and inspecting means 113 for meeting a request for inspection from the user 10. Further, the electronic authentication center 100 is provided with a time stamp server 120 for applying time stamp information to the unidirectional function value to issue the electronic certificate 101.

Here, the receiving means 111 receives a request for connection from the user 10 to receive necessary information such as the specific ID of the user 10 as well as the electronic data 11. When the electronic data 11 is encoded, the electronic data is decoded and inspect whether a tampering or the like does not exist by the electronic signature.

The computing means 112 forms the unidirectional function value from the electronic data 11 received by the receiving means 111 and delivers it to the time stamp server 120. Here, the unidirectional function value designates, for instance, a (HASH) value which is also called as a message digest, that is, for instance, a pseudo-random number with a fixed-length generated by an irreversible unidirectional function such as a hash function. While the same unidirectional function value can be obtained from the same data, original data cannot be reproduced from the unidirectional function value.

The inspecting means 113 receives the electronic data

11 , the electronic certificate 101 therefor and the request for inspection from the user 10 to inspect whether there is no tampering therefor. The detail of the inspecting means will be described later.

As the time stamp server 120, any time stamp server which receives the unidirectional function value from the computing means 112 and applies time stamp information thereto to form the electronic certificate 101 may be employed without a special limitation. Further, the electronic certificate 101 is preferably encoded and signed by a prescribed procedure. Time information used by the time stamp server 120 is periodically corrected by the time correction center 200. These matters will be specifically described below.

The time correction center 200 for correcting the time of the time stamp server 120 includes time correcting means 210. The time correcting means 210 includes a cesium atomic clock 211 cooperative with an arranged universal time, a master clock 212 to which time source is supplied from the cesium atomic clock 211 and a time transmission server 213 to which time is transmitted from the master clock 212. The time transmission server 213 periodically corrects the time means of the time stamp server 120.

The time correcting means 210 of the time correction center 200 periodically accesses the time stamp server 120 to correct a clock contained therein, obtain the specific ID 102 of the

time stamp server 120 and the public key certificate 103 of a public key used by the time stamp server 120 and issue a time correction certificate 201 including the hash value as the unidirectional function value of the public key certificate 103.

Further, the time correction center 200 includes stamp issue log obtaining means 220 for obtaining a stamp issue log 107 which indicates the number of the electronic certificates 101 issued by the time stamp server 120 as well as the specific ID 102 of each time stamp server 120 and accounting means 230 for grasping the number of stamp issues based on the stamp issue log 107 obtained by the stamp issue log obtaining means 220 and accounting for the electronic authentication center 100 using the time stamp server 120 correspondingly thereto. The stamp issue log obtaining means 220 may obtain the stamp issue log 107 when the time correcting means 210 corrects the time of the time stamp server 120. Further, the time stamp server may be accessed periodically, for instance, at a prescribed timing such as once every month upon counting up accounts to obtain the stamp issue log 107. Furthermore, timing for accounting of the accounting means 230 is not also especially limited.

One example of such a time stamp server 120 and one example of the electronic certificate 101 issued by the time stamp server 120 are shown in Fig. 2. As shown in Fig. 2, the time stamp

server 120 has the specific ID 102 managed by the time correction center 200 and contains a clock 121 and includes electronic certificate forming means 122. Further, the time stamp server includes a secret key 123 used for encryption upon forming the electronic certificate 101 and a public key certificate 103 of a public key paired with the secret key 123. Further, the clock 121 of the time stamp server 120 is periodically corrected at a prescribed timing by the time correcting means 210 of the time correction center 200 as mentioned above, receives the time correction certificate 201 upon correction and keeps it. The time correction center 200 obtains the specific ID 102 and the public key certificate 103 from the time stamp server 120 to monitor whether or not the time stamp server 120 forms a proper electronic certificate 101 and authenticate the issued electronic certificate 101.

The electronic certificate forming means 122 receives the unidirectional function value 11A of the electronic data 11 of the user 10 from the computing means 112 to form time stamp information 104 obtained by adding time information got from the clock 121 thereto, encode the time stamp information 104 by the secret key 123 and form a signed electronic signature 105 and output them as the electronic certificate 101. Accordingly, the electronic certificate 101 includes the time stamp information 104 and the electronic signature 105, and further includes the public key certificate 103 for a secret

key for a time stamp and the time correction certificate 201.

A procedure in which the time correction center 200 accounts the electronic authentication center 100 using the time stamp server 120 for the rent is shown in Fig. 3. The time correcting means 210 of the time correction center 200 accesses the time stamp server 120 of the electronic authentication center 100 as described above to obtain the specific ID102 and the public key certificate 103, correct the clock 121 and issue the time correction certificate 201. Further, in this embodiment, at this time, the stamp issue log obtaining means 220 obtains the stamp issue log 107 from the time stamp server 120. The stamp issue log 107 shows the history in which the time stamp server 120 issues the electronic certificates 101. Further, the accounting means 230 grasps the number of issued electronic certificates 101 from the stamp issue log 107 and accounts the electronic authentication center 100 for the rent of the time stamp server 120 corresponding to the number of issues. At this time, it is to be understood that the electronic authentication center 100 may be accounted for the rent to which a basic rent is added.

Thus, the time correction center 200 can account the electronic authentication center for the rent of the time stamp server 120 and a fee for correcting time in accordance with the number of issues of the electronic certificates 101. Further, since the electronic authentication center 100 is accounted

for in accordance with the number of issues of the electronic certificates 101, the electronic authentication center 100 advantageously easily undergoes the time correction of the time correction center 200.

Since the time correction center 200 manages the time stamp server 120 as mentioned above, the time correction center grasps the electronic certificate 101 issued by the time stamp server 120, particularly, the time correction certificate 201 included in the electronic certificate 101 and the specific ID 102 of the time stamp server 120 which issues the electronic certificate 101, so that the time correction center can inspect whether or not the electronic certificate 101 is issued by the formal time stamp server 120 which the time correction center itself manages to correct time. Therefore, there may be carried out a service that the above-described inspection is received from the user of the electronic certificate 101 to certify that the electronic certificate 101 is a certificate issued from the formal time stamp server 120.

Ordinarily, whether or not the time correction certificate 201 is true is inspected to consider the electronic certificate 101 to be true. However, since the time correction certificate 201 itself may be possibly imitated and copied, the specific ID 102 included in the time stamp information 104 and the public key certificate 103 used when the time correction certificate 201 is formed are preferably stored to make reference

to them and inspect whether or not the time correction certificate is issued by the formal time stamp server 120. Further, the time correction certificate 201 is inspected to understand whether the time stamp server 120 issuing the electronic certificate 101 currently periodically undergoes a time correction. Thus, it can be decided whether or not the time stamp information 104 included in the electronic certificate 101 is correct. Further, by performing such an inspection, the electronic certificate issued by a false time stamp server holding a false specific ID and public key certificate can be seen through.

Now, an example in which the above-described electronic certificate 101 is used is shown in Fig. 4. In the example shown in Fig. 4, it is assumed that the user 10 (user A) who obtains the electronic certificate 101 from the electronic authentication center 100 employs the electronic certificate 101 together with the electronic data 11 to a user 20 (user X) and the user 20 carries out a request 301 for inspection to the electronic authentication center 100 by using the electronic data 11 and the electronic certificate 101. In this case, the user 20 performs an inspection request 301 for the electronic authentication center 100 by using the electronic data 11 and the electronic certificate 101 so that the user 20 can recognize that the electronic data 11 is not altered and the date is not changed based on a content certificate 302.

That is, the user 20 can see through an illegality due to the tampering of the electronic information only by transmitting and receiving the electronic information.

Means by which the electronic authentication center 100 certifies the content 302 is not particularly limited and the electronic authentication center may issue the certificate to the user 20 or communicate with the user by an electronic mail or the like or the user 20 may recognize on a Web.

In the electronic authentication center 100, the inspecting means 113 obtains a hash value from electronic data 11 received from, for instance, the user 20 like the above-described computing means 112. The inspecting means inspects whether or not the obtained hash value corresponds to the hash value included in the time stamp information 104 of the electronic certificate 101 to certify the contents 302. It is to be understood that the inspecting means 113 inspects not only the contents of the electronic data 11, that is, inspects not only whether or not the contents are altered, but also whether or not the time stamp information is altered.

When the time correction center 200 receives an inspection as to whether the electronic certificate 101 is formal as mentioned above, the user 20 carries out a time inspection request for the time correction center 200 by using the electronic certificate 101, so that the user can recognize that the electronic authentication center 100 uses the prescribed

time stamp server 120 which undergoes a time correction by the time correction center 200 and the electronic certificate 101 is issued by the prescribed time stamp server 120.

In such a manner, the user 20 can see through the illegality due to the alteration of the electronic information only by transmitting and receiving the electronic information.

As described above, the electronic authentication center 100 for performing an authentication based on the electronic certificate 101 of the electronic information is provided independently of the time correction center 200 for correcting the time stamp server 120 used by the electronic authentication center 100. Accordingly, the alteration of time can be prevented upon stamping the time and the reliability of the time stamp information can be improved. Thus, a new manner of use in which the time stamp information regarded as important can be met.

According to the present invention, the time correction center for correcting the time of the time stamp server used by the electronic authentication center is provided independently of the electronic authentication center for inspecting the contents based on the electronic certificate of the electronic information. Further, the time correction center accounts the electronic authentication center in accordance with the number of issues of the electronic certificates. Accordingly, the electronic authentication

system can be realized in which the reliability of the time stamp information is improved without generating doubts as to whether the correct time is stamped, whether the time is altered, or the like. Further the time correction center can account for the fee in accordance with the number of issues of time stamps.

What is claimed is:

1. An electronic authentication system for performing an electronic authentication through a network, said electronic authentication system comprising:

an electronic authentication center which receives a registration of electronic information from a user, issues an electronic certificate by using a time stamping unit and inspects contents based on the electronic certificate; and

a time correction center which exists independently of the electronic authentication center to correct the time of the time stamping unit, characterized in that the time correction center includes a time correcting unit for correcting the time of the time stamping unit, a stamp issue log obtaining unit for obtaining stamp issue logs from which the number of the electronic certificates issued by the time stamping unit can be grasped from the time stamping unit and an accounting unit which grasps the number of the issued electronic certificates from the stamp issue logs obtained by the stamp issue log obtaining unit and accounts for the electronic authentication center in accordance with the number of issues.

2. An electronic authentication system according to claim 1, wherein the stamp issue log obtaining unit accesses the time stamping unit through the network to obtain the specific ID of the time stamping unit and the stamp issue log.

3. An electronic authentication system according to

claim 1 or 2 wherein the stamp issue log obtaining unit obtains the stamp issue log when the time correcting unit corrects the time of the time stamping unit.

4. An electronic authentication system according to any one of claims 1 to 3, wherein the time correcting unit transmits a time correction certificate to the time stamping unit when it corrects the time and the time stamping unit issues the electronic certificate including the time correction certificate.

5. An electronic authentication method for performing an electronic authentication through a network, said electronic authentication method comprising: an electronic authentication center which receives a registration of electronic information from a user, issues an electronic certificate by using a time stamping unit, and inspects contents based on the electronic certificate; and a time correction center which exists independently of the electronic authentication center to correct the time of the time stamping unit, characterized in that the time correction center corrects the time of the time stamping unit, obtains stamp issue logs from which the number of the electronic certificates issued by the time stamping unit can be grasped from the time stamping unit, and grasps the number of the issued electronic certificates from the stamp issue logs and accounts for the electronic authentication center in accordance with the number of issues.

6. An electronic authentication method according to claim 5, wherein the time correction center accesses the time stamping unit through the network to obtain the ID of the time stamping unit and the stamp issue log.

7. An electronic authentication method according to claim 5 or 6, wherein the time correction center obtains the stamp issue log when it corrects the time of the time stamping unit.

8. An electronic authentication method according to any one of claims 5 to 7, wherein the time correction center transmits a time correction certificate to the time stamping unit when it corrects the time and the time stamping unit issues the electronic certificate including the time correction certificate.

9. A computer apparatus comprising means for carrying out all the steps of claim 5.

10. A computer program code means that when executed on a computer carryout all the steps of claim 5.

11. A computer program on a carrier code that when executed on a computer carry out all the steps of claim 5.