(12) UK Patent Application (19) GB (11) 2 366 968 (13) A

(43) Date of A Publication 20.03.2002

(21) Application No 0022226.5

(22) Date of Filing 11.09.2000

(71) Applicant(s)
Intensiti Technologies Plc
(Incorporated in the United Kingdom)
12 Leadenhall Street, LONDON, EC3V 1LP,
United Kingdom

(72) Inventor(s)
Frankie Blaskovic

(74) Agent and/or Address for Service
Ipulse
26 Mallinson Road, LONDON, SW11 1BP,
United Kingdom

(51) INT CL^7
H04L 9/32

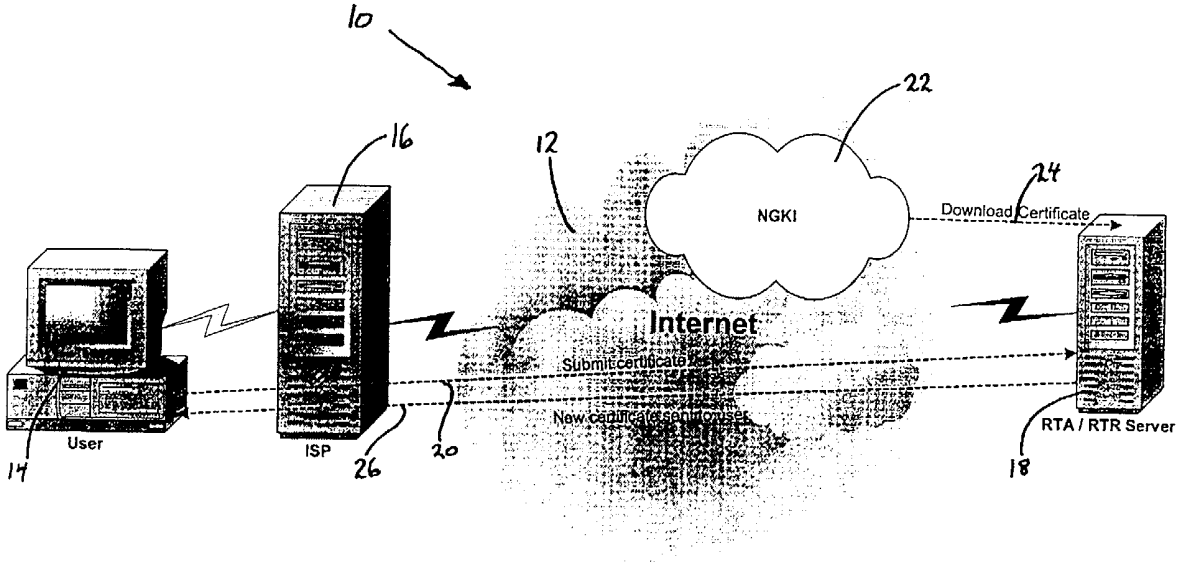
(52) UK CL (Edition T)
H4P PDCSA
U1S S2209

(56) Documents Cited
US 5687235 A

(58) Field of Search
UK CL (Edition S) **H4P PDCSA**
INT CL^7 **H04L 9/32**
Online:WPI,EPODOC,JAPIO,INSPEC

(54) Abstract Title
Digital certificate authentication and/or revocation

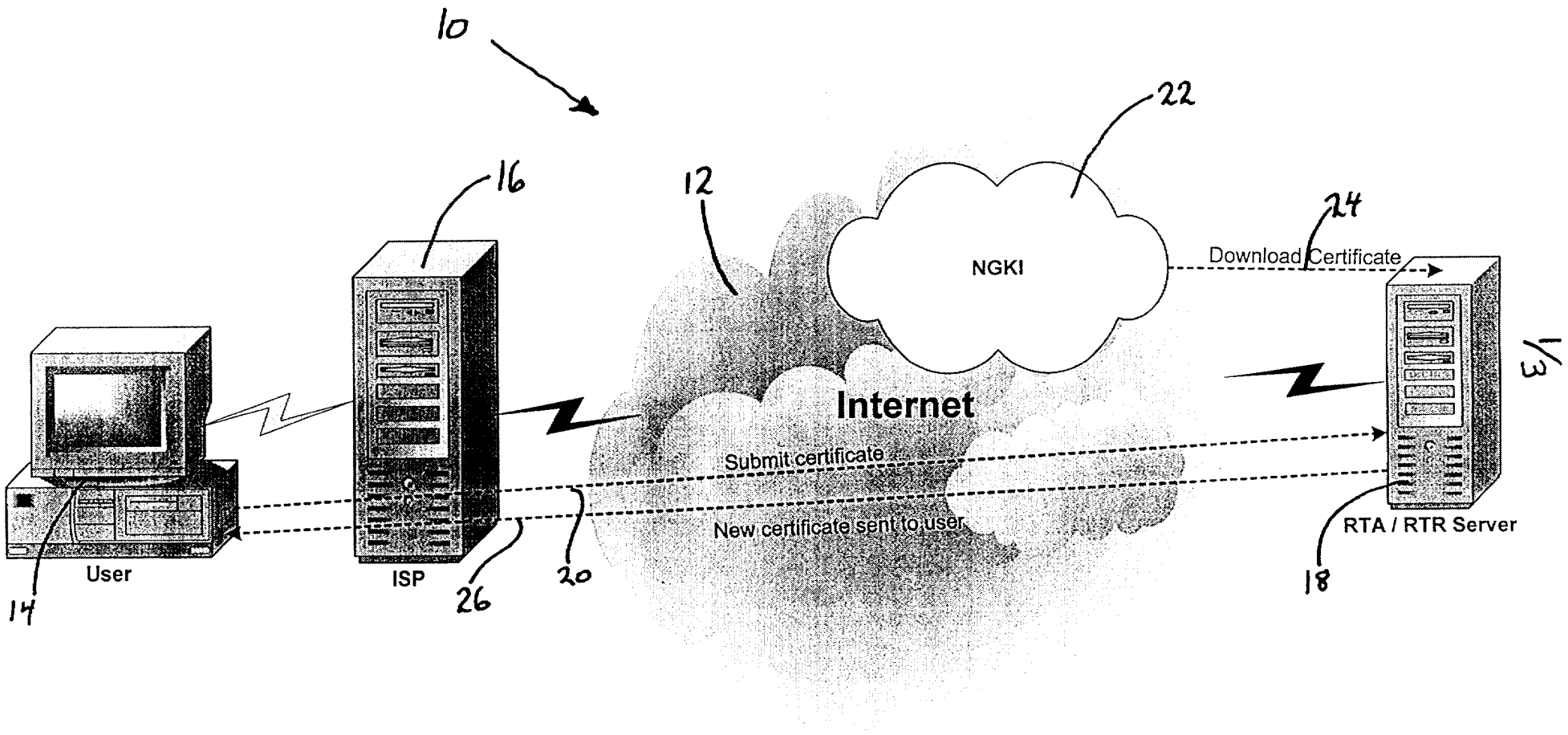
(57) A method for issuing digital certificates to end users, servers and systems. In particular the method embodies a method for authentication and/or revocation of digital certificates used in at least one electronic network for securing transmission of electronic messages, information and/or data between a user and at least one third party by a Certification Authority. The method is capable of facilitating faster and more reliable authentication and/or revocation of digital certificates as compared to known methods. It allows revoked certificates to be cancelled and updated in real time. The present invention permits checking of the validity of the digital certificates in order to ensure that each use is a valid one. There is also provided an electronic machine (eg computer) readable medium and a system to carry out this method.



1. User submits certificate to the RTA/ RTR server
2. RTA/ RTR server downloads user certificate from NGKI and checks against submitted cerificate
3. If user certificate valid then OK flag sent to user otherwise the updated certificate is sent to the user

FIGURE 1.

GB 2 366 968 A



1. User submits certificate to the RTA/ RTR server
2. RTA/ RTR server downloads user certificate from NGKI and checks against submitted cerificate
3. If user certificate valid then OK flag sent to user otherwise the updated certificate is sent to the user

FIGURE 1.

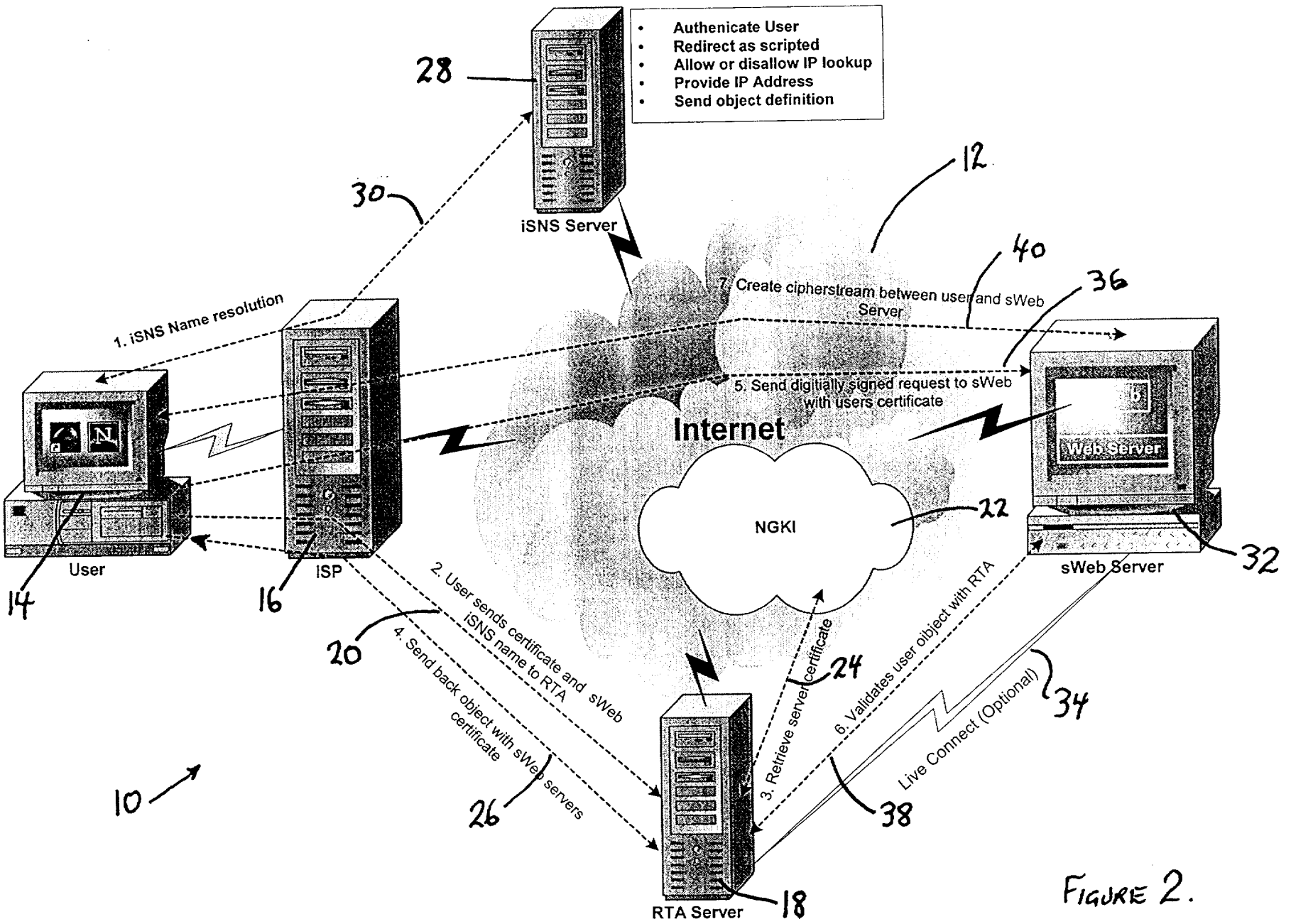
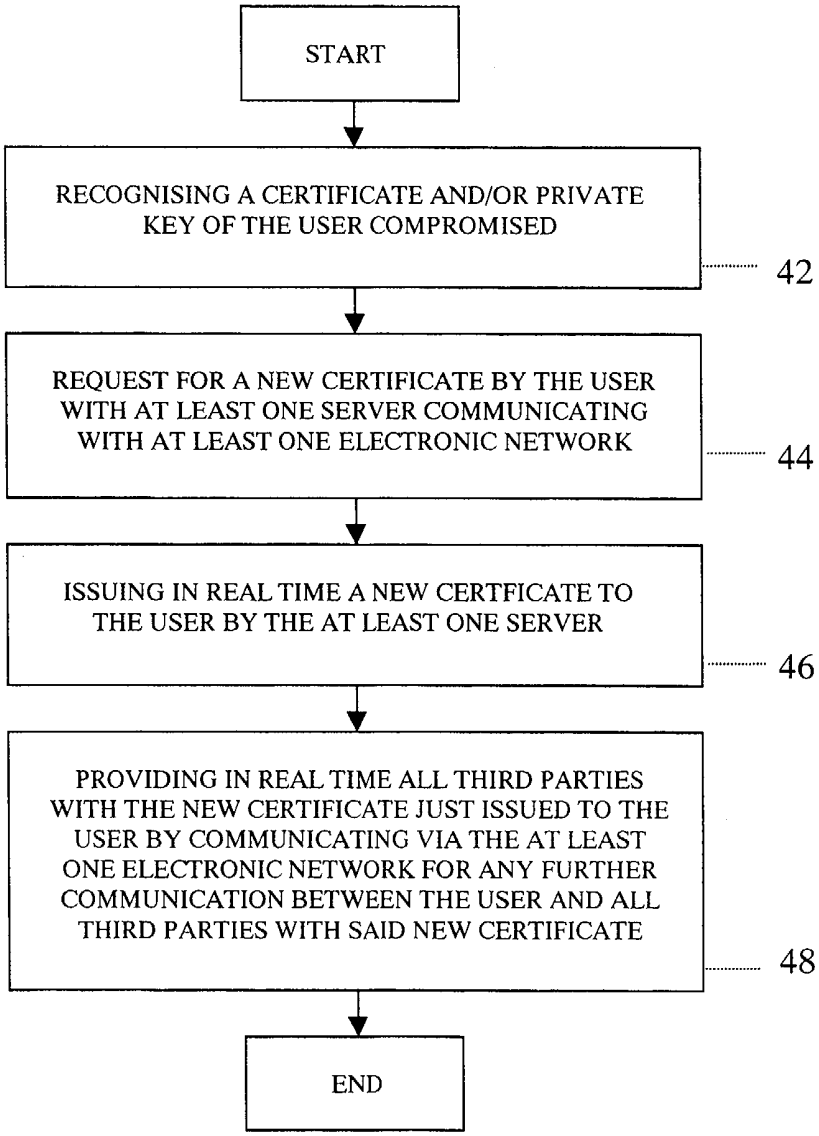

Authenicate User
Redirect as scripted
Allow or disallow IP lookup
Provide IP Address
Send object definition
28
30
iSNS Server
12
40
36
7. Create cipherstream between user and sWeb Server
1. iSNS Name resolution
5. Send digitally signed request to sWeb with users certificate
Internet
Web Server
NGKI
22
User
ISP
sWeb Server
32
14
16
2. User sends certificate and sWeb iSNS name to RTA
20
4. Send back object with sWeb servers certificate
26
3. Retrieve server certificate
24
6. Validates user object with RTA
Live Connect (Optional)
34
38
10
RTA Server
18

FIGURE 2.

Figure 3


START
RECOGNISING A CERTIFICATE AND/OR PRIVATE KEY OF THE USER COMPROMISED
42
REQUEST FOR A NEW CERTIFICATE BY THE USER WITH AT LEAST ONE SERVER COMMUNICATING WITH AT LEAST ONE ELECTRONIC NETWORK
44
ISSUING IN REAL TIME A NEW CERTFICATE TO THE USER BY THE AT LEAST ONE SERVER
46
PROVIDING IN REAL TIME ALL THIRD PARTIES WITH THE NEW CERTIFICATE JUST ISSUED TO THE USER BY COMMUNICATING VIA THE AT LEAST ONE ELECTRONIC NETWORK FOR ANY FURTHER COMMUNICATION BETWEEN THE USER AND ALL THIRD PARTIES WITH SAID NEW CERTIFICATE
48
END

METHOD, MEDIUM AND SYSTEM FOR ISSUING CERTIFICATES

The present invention refers to a method for issuing digital certificates to end users, servers and systems. In particular it embodies a method for authentication and/or revocation of digital certificates used in at least one electronic network for securing transmission of electronic messages, information and/or data between a user and at least one third party by a Certification Authority (CA).

Digital certificates are provided which are used for e-commerce within an Intranet, Extranet, Internet or other similar environment for services, for example Virtual Private Networks, Secure email, Secure Web Banking, Internet Shopping, Online Trading or the like. The digital certificates and/or digital signatures can be appended to messages, signals, information and/or data to authenticate them and the sender. The certificates, digital signatures and/or appended messages, signals, information and/or data can be encrypted using a so-called public key which can only be retrieved by using a complementary private key. Digital certificates operate as proof of identity and/or encryption.

Digital certificates can be obtained from CA's or their intermediaries (for example BT Trustwise).

Digital certificates are for example used within Public Key Infrastructures (PKIs) providing a framework by which users and/or entities are able to securely communicate with each other. PKI's can be of private or public types among other domains. A private PKI may be deployed by a corporation for securing transactions between its business and any related parties, e.g. customers, suppliers. Public PKI's, as for example Trusted Third Parties or Commercial Parties, are available on open networks, such as the Internet, and facilitate security between previously unrelated parties.

Within each PKI a CA and/or Route of Authority (RA) exists as a central controlling entity which is responsible for the authentication and revocation of users. This is achieved by the issuance and revocation of said digital certificates, which are memorized in directories, for example revoked certificate information is retained in Certificate Revocation Lists (CRLs).

CAs currently issue digital certificates, mostly based on X509 standard implementations, to end users, servers, and other systems.

Revocation of a certificate is a process whereby a corrupt/compromised/lost certificate key results in the corresponding certificate being invalidated from a digital security point of view. The process of revoking, i.e. invalidating, those certificates has been a problem to industry for a number of years. Currently CAs issue CRLs, which are then downloaded by end users, and parsed by the relevant software in order to invalidate those certificates with references in the. CRLs on that user's system (or network/machine..).

For example, current certificate revocation methods, typically used in X509 standard implementations and/or PKIs, put into effect in case a certificate and/or private key of a user is compromised are as follows: First, the user notifies the invalidity of the certificate and/or private key to the responsible CA. Then, the CA issues a new certificate to the user, adds the invalid certificate or certificate reference to a CRL and publishes a new or amended CRL. Subsequently, the one or more PKIs need to collect said new/amended CRL. Thereafter, each PKI revokes the invalid certificate and, as a subsequent step, downloads a new certificate and updates the directory services. It is only afterwards that the user can communicate with the new certificate.

There are many disadvantages and inconveniences resulting from the use of known state of the art methods, the methods in practice. Key problems with these known methods include but are not limited to the following. The users typically lack detailed technical knowledge about the CRLs, and/or simply do not update them regularly. The CRLs are becoming too big to manage. Download times and distribution times are increasing, making this method slow and impractical, hence a number of CAs do not publish them any longer. Another issue is that people who do not use a given certificate for some time, or who do not communicate with the systems/users whose certificates have been revoked, might not be aware of the fact that they have been revoked. Hence, the end result is that security and authenticity, which the digital certificates are meant to bring, is compromised. Using a revoked or invalid certificate in effect allows for proofs of digital signature, digital identity, and encryption stream to be used by either untrusted entities, or hackers in order to foil

someone's security, and other's reliance on it. Now that digital signatures are being recognized as legally enforceable, like ordinary signatures, this problem is further increased. Under present methods invalidated certificates can still be effective as if they were valid. Further, the present system requires users to request a completely new certificate and re-distribute those either manually, or through some form of automated systems, such as a PKI, to all the entities it communicates with in order for them to have the most up to date copies.

Consequently, it is a primary object of the present invention to overcome the aforementioned disadvantages and inconveniences, by providing a method which is capable of facilitating faster and more reliable authentication and/or revocation of digital certificates as compared to known methods described above, and an electronic machine (eg computer) readable medium and a system to carry out this method.

As used herein, the term computer system comprises systems using computers and other electronic devices for processing messages, signals, information and/or data.

In a preferred embodiment the present invention provides a method for authentication and/or revocation of digital certificates used in at least one electronic network for securing transmission of electronic messages, information and/or data between a user and at least one third party, comprising the following steps: a) recognizing that a certificate and/or private key of the user is compromised, b) requesting for a new certificate by the user with at least one server also communicating with the at least one electronic network, c) issuing a new certificate to the user in real time by the at least one server, and d) providing all third parties, preferably in real time, with the new certificate just issued to the user by communicating via the at least one electronic network for, any further communication between the user and all third parties with said new certificate.

The present invention provides a method which may allow revoked certificates to be cancelled and updated in real time. The present invention permits checking of the validity of the digital certificates in order to ensure that each use is a valid one. The invention deals with certificates in a new way compared to what is being done at the moment. Whereas

currently the users must go to the relevant CA and pick up a CRL, under the present invention the certificates may be checked transparently and in real time. There is no need for active user intervention; the users do not need to actively store or interactively download anything. The new certificates can be issued in real-time and are up-to-date. Therefore, a method of the present invention is referred herein as a Real Time Authentication (RTA) method. A method of the invention is more reliable than known methods, in that it may in real time revoke certificates, update them if need be, and distribute them without special intervention from the users.

In accordance with a preferred embodiment of the present invention, said recognizing according to step a) comprises the following steps: a1) sending an RTAObject to the RTA server with the certificate of the user following the RTAObject specification used by the server at the time, a2) connecting to at least one certificate store/database and/or distribution system by the server to collect that certificate, and a3)comparing of both the certificates on the fly.

In this context, said comparison according to step a3) can be carried out by way of a hash, by data comparison, by byte-code verification, as well as by byte date verification.

The RTA/RTR server can redefine the RTAObject from time to time to prevent people hacking into the RTA/RTR server. When the user sends the Object to the RTA/RTR server it sends it using the format as defined by the RTA/RTR server at that time.

According to yet a further preferred embodiment of the invention said recognizing according to step a) further comprises the following step in the event that the certificate is not valid: a4) returning an RTAErrorObject by the server to the client with an error message describing the reason for failure and/or return a failed/success (-1/O) exit code for the request.

In a further and most particularly preferred embodiment of the invention, said instantly issuing of the new certificate to the user according to step c) of the method comprises the following steps in the event that the certificate is valid: c1) generating a unique identifier

(ID) for that request by the server, and c2) encrypting that ID with a public key of all third parties.

Moreover, it is within the scope of this invention that in step c3) the ID encrypted with the public key of all third parties according to step c2) is added to the other parties live certificate being the most up to date to be checked for validity.

A further preferred embodiment of the invention provides step c4) wherein a sWebCertificateObject is built following its specification having the key elements, in particular the encrypted ID, the certificate of said third parties and a header of some type, in it.

Further, there may be provided step c5) wherein said sWebCertificateObject is returned encrypted or unencrypted to the user requesting the service.

Preferably, there is provided step c6) wherein the received certificate is validated against those in the at least one certificate store/database and/or distribution system.
The certificate is suitably replaced by the new certificate if this is a more up-to-date one.

A further preferred feature of the present invention is that the encrypted user ID is sent with the certificate of the user to all servers of said third parties, when the unique ID is decrypted by the relevant third party.

In a preferred embodiment of the invention the sWebCertificationObject is sent to all servers of said third parties, when the unique ID is decrypted by the relevant third party.

A particularly preferred feature of the present invention is that in step d) an RTAIDObject is built based on the sWebCertificationObject and sent back to the server in order to validate its existence, and to notify its validity and to deal with the ID as appropriate by the server.

According to the invention the invalidated certificate is preferably removed from the

relevant certificate store/database and/or distribution system if the certificate has been updated and/or cancelled when the -1/0 error code is issued to the client software.

Preferably, removal/revocation of an invalidated certificate comprises a method based on similar principles to Real Time Authentication. This method of removal/revocation is referred to herein as Real Time Revocation (RTR). The RTR method is used in a slightly different manner in order to allow for just revoking the certificates rather than checking their validity at the time. In the system, both client and server, real time revocation engines will call the Certification server/s, and check the validity of current certificates. Should any of those certificates be labeled as being revoked and/or invalidated they will be instantly deleted and replaced by the new version (if available), this will also enable users to update certificate information which is currently not possible without issuing a new certificate each time. As a result, the RTR process is similar to the RTA one, except that it is just single tier, the client systems communicating with the RTR server; as compared to RTA which is multi- tier, the client systems and merchants communicating with the RTA server.

In particular, a copy of the new certificate issued by the server is preferably added to the at least one certificate store/database and/or distribution system.

Another preferred embodiment of the present invention is an electronic machine readable medium, for example a computer readable medium, having stored therein instructions for causing at least one server to execute the method of the invention.

A yet further preferred embodiment of the invention is a system for authentication and/or revocation of digital certificates used in at least one electronic network for securing transmission of electronic messages, signals, information and/or data between a user and at least one third party, having in combination a computer system of the user communicating with a computer system of a Network service provider (for example an Internet service provider), and a server connected to the system of the Network service provider and the Network (eg. Internet), whereby the server and an Application server are directly communicating with each other and whereby the server of the Network service provider, the RTA/RTR server, the Application server and at least one system of a Network service

network system are connectable to each other for electronic transmission of messages, signals, data and/or information via the Internet or some other electronic communications network.

In this context, it is useful to provide the Internet or other electronic communications network with at least one certificate database/distribution system or Key Infrastructure, for example a Next Generation Key Infrastructure (NGKI), for storing and providing updated digital certificates to the at least one thi±d party.

Further technical features, advantages and details of the present invention will be more readily apparent, by way of example only, from the following detailed description of a preferred embodiment with reference to the accompanying drawings, in which:

Fig. 1 is a block diagram illustrating an example of an authentication and revocation system according to the invention,

Fig. 2 is a block diagram illustrating an example of an authentication and revocation system of the invention according to Fig. 1, included in a system of electronic networks, and

Fig. 3 is a flow chart illustrating an example of an embodiment of an authentication and revocation method according to the invention.

Fig. 1 is a block diagram illustrating an example of an authentication and/or revocation system 10 for a preferred embodiment of the invention. The system 10 is provided for authentication and/or revocation of digital certificates used in at least one electronic network 12, for example an Intranet, Extranet or the Internet and the like, for securing transmission of electronic messages, information and/or data between a user and at least one third party.

For this purpose, system 10 comprises a computer system 14 of a user (User). The User 14 communicates with a server 16 of an Internet service provider (ISP Server). Moreover, the

system 10 has a computer system (RTA/RTR Server) 18. The RTA/RTR Server 18 is connected to the electronic network 12 and the ISP Server 16 of the Internet service provider.

According to a preferred method of the invention, a digital certificate is submitted from the User 14 via the ISP Server 16 of the Internet service provider to the RTA/RTR Server 18 (arrow 20). Then, the RTA/RTR Server 18 downloads the relevant certificate from a Next Generation Key Infrastructure (NGKI) 22 (arrow 24) and checks this against the submitted certificate.

If the certificate of the user is valid, the RTA/RTR Server 18 sends then an OK flag to the User 14 via the ISP Server 16 to go ahead (arrow 26). Otherwise, an updated certificate, which is automatically prepared straight away, as will be described below in more detail, is sent to the User 14 (also arrow 24).

Now referring to Fig. 2, system 10 is integrated in a system of electronic networks for shopping via electronic network 12. The User 14 sends his name via ISP Server 16 of the Internet service provider to a computer system 28 of an Intensiti Secure Names Services (ISNS) system or other form of names service, for example a Domain Names service,(ISNS Server) for ISNS name resolution (arrow 30). The ISNS Server 28 communicates the following objects with the electronic network 12:

> authenticating the user, redirecting as scripted, allowing or disallowing Internet Protocol (IP) look up, providing IP address and, sending object definition

Afterwards, in particular in real time, User 14 also sends his certificate and sWeb ISNS name via the ISP Server 16 to the RTA/RTR Server 18 (arrow 20). In real time, as shown in Fig. 1, the RTA/RTR Server 18 retrieves the relevant server certificate from the Next Generation Key Infrastructure (NGKI) 22 (arrow 24) and checks this against the submitted certificate.

If the certificate of the user is valid, then the RTA/RTR Server 18 sends back the object with the certificate of a sWeb server 32 to the User 14 via the ISP Server 16 to go ahead

(arrow 26). Otherwise, an updated certificate, which is automatically and instantly prepared. is sent to the User 14 (also arrow 24).

The sWeb server 32 communicates with the RTA/RTR Server 18 and optionally is live connected to the RTA/RTR Server 18 (arrow 34). Moreover, the sweb server 32 communicates with the electronic network 12.

In the next step, the User 14 sends a digitally signed request to the sWeb server 32 via the ISP Server 16 and the electronic network 12 (arrow 36). Then, the sWeb server 32 validates the user object with the RTA/RTR Server l8 (arrow 38). Finally, a cypherstream between the User 14 and the sWeb server 32 is created for exchange of messages, signals, data, information etc. (arrow 40).

Fig. 3 illustrates a method of the invention which is started by sending a certificate and/or private key from the User 14. At step 42, the certificate and/or private key of the user is proved and recognized as compromised. At step 44, a new certificate is requested for by the user with the RTA/RTR Server 18 communicating with the electronic network 12. Instantly, a new certificate is issued to the User 14 by the RTA/RTR Server 18 at step 46. At step 48 finally, all third parties are provided in real time with the new certificate just issued to the User 14 by communicating via the electronic network 12 for any further communication between the user and all third parties with said new certificate.

In a preferred embodiment of the present invention, the functionality of components from Figs. 1 and 2 is provided with software using Java, in particular Java objects with specific format and specifications as set forth in Tables 1 to 4. However, other object-oriented programming techniques and languages, e.g. the C++ programming language, and non-object oriented programing languages, e.g. C programming language, could also be used.

Table 1 below illustrates an example directive RTAObject concerning step a) of a method according to one embodiment of the invention.

```
package intensiti.ObjectAgent.Objects;

import java.io.*;
import java.util.Vector;

public final class RTAObject implements Externalizable {
       private byte[] certificate = null;
       private byte[] signature = null; private String isnsName = null;
       private String isnsName = null;

       public RTAObject(){}

       private RTAObject(byte[] object) {
       }

       public static final RTAObject getInstance(byte certificate[]) {
       }

       public final String toString() {
              return "Intensiti RTAObject";
       }

       public final void readFromBytes(byte[] object) throws
       ClassNotFoundException,
              IOException {
       }

       public final void setiSNS(String iSNSName) {
       }

       public final void setSignature(byte data[]) {
       }

       public final byte[] getSignature(){
       }

       public final byte[] getCertificate(){
       }

       public final byte[] writeToBytes()throws lOException {
       }

       public final String getiSNSName(){
       }

       public final void writeExternal(ObjectOutput oout) throws IOException{
       }

       public final void readExternal(ObjectInput oint) throws
       ClassNotFoundException,
              IOException {
       }
}
```


Table 1

Table 2 below illustrates an example directive RTAErrorObject concerning also step a) of a method according to one embodiment of the invention.

E:\..\ObjectAgent\Objects\RTAErrorObject.java

```
package intensiti.ObjectAgent.Objects;

import java.io.*;
```

```
public final class RTAErrorObject implements Externalizable {
       private String RTAError = null;

       private RTAErrorObject(char[] error) {
       }

       public RTAErrorObject(String error) {
       }

       public RTAErrorObject () {}

       public final void setError(char[] ErrorMsg) {
       }

       public final void setError(String errMsg) {
       }

       public final void setError(byte[] errorMsg) {
       }

       public final String getRTAError(){
       }

       public final void writeExternal(ObjectOutput oout) throws lOException {
       }

       public final byte[] writeToBytes()throws IoException {
       }

       public final void readExternal(ObjectInput oint) throws
       ClassNotFoundException,
              IoException {
       }

       public final void readFromBytes(byte[] object) throws
       ClassNotFoundException,
              IoException {
       }

       public final String toString(){
       }
}
```


Table 2

Table 3 below illustrates an example directive sWebCertificateObject concerning step c) of a method according to one embodiment of the invention.

E:\..\ObjectAgent\Objects\sWebCertificateObject.java

```
package intensiti.ObjectAgent.objects;

import java.io.*;

public final class sWebCertificateObject implements Externalizable {
       private byte[] cert = null;
       private String EncrytedUID = null;
       private byte[] signature = null;
       private byte[] requestHeader = null;

       private sWebCertificateObject() {}

       public static final swebCertificateObject getInstance(byte[]
       CertificateData, String
              UID) {
       }

       public final void setHeader(byte[] requestHeader) {
       }
```

```
        public final byte[] getHeaderObject() {
        }

        public final String toString() {
        }

        public final String getEncryptedUID() {
        }

        public final byte[] getCertificateData() {
        }

        public final void Signature(byte[] data) {
        }

        public final byte[] Signature() {
        }

        public final void readFromBytes(byte[] data) throws
        classNotFoundException,
               IOException {
        }

        public final void readFromFile(String filename) throws
        classNotFoundException,
               lOException, Exception {
        }

        public final void writeToFile(String filename) throws Exception {
        }

        public final byte[] writeToBytes()throws IOException {
        }

        public final void readExternal(ObjectInput oin) throws
        classNotFoundException,
               IoException {
        }

        public final void writeExternal(objectoutput out) throws IoException {
        }
}
```

Table 3

Table 4 below illustrates an example directive RTAIDObject concerning step d) of a method according to one embodiment of the invention.

E:\Visual Studio Projects\..\ObjectAgent\Objects\RTAIDObject.java 1

```
package intensiti.ObjectAgent.Objects;

import java.io.*;

public final class RTAIDObject implements Externalizable {
       private byte[] RTAID = null;

       private RTAIDObject(String RTAID) {
       }

       public final static RTAIDObject getInstance(String RTAID) {
       }

       public final String getRTAID(){
       }
```

```
        public final byte[] getRTAIDAsBytes() {
        }

        public final void writeExternal(ObjectOutput oout) throws IOException {
        }

        public final byte[] writeToBytes()throws lOException {
        }

        public final void readExternal(ObjectInput oint) throws
        ClassNotFoundException,
               IOException {
        }

        public final void readFromBytes(byte[] object) throws
        classNotFoundException,
               IoException {
        }

        public final String toString() {
        }
}
```


Table 4

In view of the wide variety of embodiments to which the principles of the present invention can be applied, it should be understood that the illustrated embodiments are exemplary only, and should not be taken as limiting the scope of the present invention. For example, the steps of the flow diagrams may be taken in sequences other than those described, and more or fewer elements may be used in the block diagrams.

The claims should not be read as limited to the described order or elements unless stated to that effect. Therefore, all. embodiments that come within the scope and spirit of the following claims and equivalents thereto are claimed as the invention.

Claims

1. A method for authentication and/or revocation of digital certificates used in at least one electronic network for securing transmission of electronic messages, signals, information and/or data between a user (14) and at least one third party (28), comprising the following steps:

a) recognizing that a certificate and/or private key of the user (14) has been compromised,

b) the user (14) requesting a new certificate, certificate update or certificate renewal from at least one RTA/RTR server (18) communicating with the at least one electronic network (12),

c) issuing a new updated or renewed certificate to the user (14) in real time by the at least one RTA/RTR server (18), and

d) providing all third parties with the new updated or renewed certificate issued to the user (14) by communicating via the at least one electronic network (12) for any further communication between the user (14) and all third parties with said new certificate.

2. A method as claimed in claim 1 wherein the new updated or renewed certificate issued to the user (14) is provided to third parties in real time.

3. A method as claimed in claim 1 or claim 2 wherein said recognizing according to step a) comprises the following steps:

a1) sending an RTAObject to the RTA/RTR server (18) with the certificate of the user (14) using the RTAObject as published at that time by the RTA/RTR server (18),

a2) the RTA/RTR server (18) connecting with at least one certificate store/database and/or distribution system (22) to collect that certificate, and

a3) comparing both of the certificates on the fly.

4. A method as claimed in claim 3 wherein said comparison according to step a3) is carried out by way of a hash.

5. A method as claimed in claim 3 wherein said comparison according to step a3) is carried out by data comparison.

6. A method as claimed in claim 3 wherein said comparison according to step a3) is carried out by byte-code verification.

7. A method as claimed in claim 3 wherein said comparison according to step a3) is carried out by byte date verification.

8. A method as claimed in any one of claims 1 to 7 wherein said recognizing according to step a) further comprises the following step in the event that the certificate is not valid:

a4) the RTA/RTR server (18) returning an RTAErrorObject to the user (14) with an error message describing the reason for failure and/or returning a —1/0 exit code for the request.

9. A method as claimed in any one of claims 1 to 8 wherein issuing the new updated or renewed certificate to the user (14) according to step c) comprises the following steps in the event that the certificate is valid:

c1) the RTA/RTR server (18) generating a unique ID for that request, and

c2)encrypting that ID with a public key of all third parties.

10. A method as claimed in claim 9 further comprising step c3) wherein the ID encrypted with the public key of all third parties according to step c2) is added to the other parties live certificate being the most up to date to be checked for validity.

11. A method as claimed in claim 9 or claim 10 further comprising step c4) wherein a sWebCertificateObject is built using the specification published at the time by the RTA/RTR server or Application server, comprising as key elements the encrypted ID, the certificate of said third parties and a header.

12. A method as claimed in claim 11 further comprising step c5) wherein said sWebCertificateObject is returned encrypted or unencrypted to the user (14) requesting the service.

13. A method as claimed in claim 12 further comprising step c6) wherein the received certificate is validated against those in at least one certificate store/database and/or distribution system (22).

14. A method as claimed in any of claims 1 to 13 wherein the certificate is replaced by any more up-to-date certificate.

15. A method as claimed in any one of claims 1 to 14 wherein an encrypted user ID is sent with the certificate of the user to all servers of said third parties, when the unique ID is decrypted by the relevant third party.

16. A method as claimed in claim 15 wherein a sWebCertificationObject is sent to all servers of said third parties, when the unique ID is decrypted by the relevant third party.

17. A method as claimed in any one of claims 1 to 16 wherein in step d) an RTAIDObject is built based on a sWebCertificationObject and sent back to RTA/RTR server (18) in order to validate its existence, and to notify its validity and to deal with ID as appropriate by the RTA/RTR server (18).

18. A method as claimed in any one of claims 1 to 17 wherein the certificate is removed from the relevant certificate store/database and/or distribution system (22) if the certificate has been updated and/or cancelled when a -1/O error code is issued to client software.

19. A method as claimed in claim 18 wherein a copy of a new certificate issued by the RTA/RTR server (18) is added to the at least one certificate store/database and/or distribution system (22).

20. A method as claimed in any one of claims 1 to 19 wherein the at least one certificate store/database and/or distribution system (22) is a Key Infrastructure.

21. A method as claimed in any one of claims 1 to 20 further comprising use of object code as described in any one or more of Tables 1 to 4.

22. An electronic machine readable medium having stored therein instructions for causing at least one RTA/RTR server (18) to execute the method of claims 1 to 21.

23. An electronic machine readable medium as claimed in claim 22 wherein the medium is a computer readable medium.

24. An electronic machine readable medium having stored therein object code as described in any one or more of Tables 1 to 4.

25. A system for authentication and/or revocation of digital certificates used in at least one electronic network (12) for securing transmission of electronic messages, signals, information and/or data between a user (14) and at least one third party, comprising for executing the method of claims 1 to 21 in combination:

a) a computer system (14) of the user communicating with a server(16)of an Network service provider, and

b) an RTA/RTR server (18) connected via a network to a Network service provider (16) and a Network (12),

whereby RTA/RTR server (18) and an Application server (32) are directly communicating with each other and whereby Network service provider server (16), RTA/RTR server (18), Application server (32) and at least one server (28) of an Network service network system are connectable to each other for electronic transmission of messages, data and/or information via a network communications system (12).

26. A system as claimed in claim 25 wherein the Network is provided with at least one certificate database/distribution system or Key Infrastructure for storing and providing updated digital certificates to the at least one third party.

27. A system as claimed in claim 25 or claim 26 wherein the at least one certificate database/distribution system or Key Infrastructure is a Next Generation Key Infrastructure (NGKI) (22).

28. A system as claimed in any one of claims 25 to 27 wherein the Network is the Internet.

29. A system as claimed in any one of claims 25 to 28 comprising use of object code as described in any one or more of Tables 1 to 4.

30. A method for authentication and/or revocation of digital certificates used in at least one electronic network for securing transmission of electronic messages, information and/or data substantially as herinbefore described with reference to and/or as illustrated in one or more of the accompanying Figures and/or Tables.

31. A method for authentication and/or revocation of digital certificates used in at least one electronic network for securing transmission of electronic messages, information and/or data wherein a certificate and/or private key is recognized as

compromised using object code described in Table 1, Table 2 or both Tables 1 and 2.

32. A method for authentication and/or revocation of digital certificates used in at least one electronic network for securing transmission of electronic messages, information and/or data wherein a new certificate is issued to a user using object code as described in Table 3.

33. A method for authentication and/or revocation of digital certificates used in at least one electronic network for securing transmission of electronic messages, information and/or data wherein object code as described in Table 4 is used to provide third parties with new certificates which have been provided to users.

34. A method for authentication and/or revocation of digital certificates used in at least one electronic network for securing transmission of electronic messages, information and/or data comprising the use of object code as described in Tables 1 to 4.

20

Application No: GB 0022226.5 **Examiner:** B.J.SPEAR
Claims searched: 1-34 **Date of search:** 19 March 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): H4P (PDCSA)

Int Cl (Ed.7): H04L9/32

Other: Online:WPI, EPODOC, JAPIO, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	US5687235 (Novell)	-

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.